Methods and Factors Affecting Digital Forensic Case Management, Allocation and Completion

by

Ibtesam Mohammed Alawadhi

A thesis submitted in partial fulfilment for the requirements for the degree of Doctor of Philosophy at the University of Central Lancashire

May 2019

University of Central Lancashire

STUDENT DECLARATION FORM

Concurrent registration for two or more academic awards

I declare that while registered as a candidate for the research degree, I have not been a registered candidate or enrolled student for another award of the University or other academic or professional institution

Material submitted for another award

I declare that no material contained in the thesis has been used in any other submission for an
academic award and is solely my own work

(state award and awarding body and list the material below):

Collaboration

Where a candidate's research programme is part of a collaborative project, the thesis must indicate in addition clearly the candidate's individual contribution and the extent of the collaboration. Please state below:

Signature of Candidate ____

Type of Award ____**Doctor of Philosophy** ____________________________

School ____**School of Physical Sciences and Computing**____________

ABSTRACT

Modern Digital Forensic (DF) departments/sections are witnessing rapid increases in digital forensic cases through the years. The challenges of DF cases investigation are getting more robust and they are affecting digital forensic investigation processes. Accordingly, understanding different factors affecting Person-Hours of investigation from real cases records, and recognising the context of work with different strategies and practices performed in different departments is necessary to create a stable ground to face all the factors affecting the investigative processes.

This research details the cases' trends in the Dubai Police. It also identifies the main challenges encountered by DF including rising volumes of data and case complexity, using real case records from the Dubai Police. This extensive research explains the contribution of several factors to the delay in the DF investigation process. The research also explores the context of work of DF departments in other locations and other countries to understand a range of case allocation strategies and case management procedures. The research contributes a set of Decision Tables that could be used by DF managers and supervisors to select best proposed case allocation strategies and case management procedures.

The research is accomplished through a series of three studies referred to as Study One, Study Two, and Study Three. Study One (Investigation of the Dubai Police Records) involves a quantitative analysis of secondary data in the form of case records from the Dubai Police (DP) Database and associated reports. This study addresses the first research question (RQ1): "*What are the trends and challenges encountered by practitioners faced with large volume/heterogeneity DF investigations*?" by measuring the growth of cases and identifying the main factors for the delay in DF investigations. Study Two (Interviews with DF managers) follows a qualitative approach using the phenomenological model, and covers the second research question (RQ2): "*What are the effect of different factors behind the delay of DF investigation process?"* The study identifies the common factors affecting delay in DF investigations, from the diverse experiences and backgrounds of DF decision makers around the world. Study Three (Confirmation of the Interviews) again uses the phenomenological model, and covers the third research question (RQ3): "*What are the different case management procedures and workflow implementation practices currently used?"* This study evaluates the efficacy of different case allocation strategies and workflow implementation practices with selected participants and results in a contribution to DF in the form of a series of Decision Tables for case allocation.

The main findings of the research explain the main factors that lead to the creation of delay in DF investigation and thereafter affect the DF investigation process. Moreover, this research identifies case management strategies and workflow implementation practices. The research also contributes Decision Tables to allow managers and others to select a case management strategy and workflow implementation depending on several conditions.

ACKNOWLEDGEMENT

I would like to express my appreciation to my supervisors Prof. Janet C. Read, Dr. Andrew Marrington and Dr. Virginia N. L. Franqueira for their guidance, patience, commitment, and tolerance when advising me, reading my draft chapters and thesis, and for encouraging me to publish articles.

My thanks also go to all the participants of this research for their kindness and cooperation, and to the support staff and colleagues in the School of Physical Sciences and Computing at the University of Central Lancashire.

Finally, I would like to thank the Dubai Police for providing me a scholarship to pursue my Ph.D. studies.

DEDICATION

I dedicate this thesis to my parents, husband and my precious kids
for their endless support.

DECLARATION AND PUBLICATION

Concurrent registration for two or more academic awards

I declare that, while registered as a candidate for the research degree, I have not been registered as a candidate or enrolled as a student for another award of the University or other academic or professional institution.

Material submitted for another award

I declare that I did not use any material contained in the thesis in support of an application for another degree, or qualification, to any other university, or institute of learning; and is solely my own work.

Some of the material contained here has been presented in the form of the following:

Journal Publication:

Al Awadhi, I., Read. J.C., Marrington, A., Franqueira, V.N.L. (2015). Factors influencing digital forensic investigations: Empirical evaluation of 12 years of Dubai police cases. Journal of Digital Forensics, Security and Law (JDFSL), 10(4), pp. 7-16. ADFSL Press.

Signature of Candidate

Type of Award:	Ph.D.
School:	Computing, Engineering and Physical Sciences

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF Equations

LIST OF ABBREVIATIONS

ABBREVIATION	MEANING
ACPO	Association of Chiefs of Police Officers
CSI	Crime Scene Investigation
DDF	Distributed Digital Forensics
DF	Digital Forensics
DFD	Digital Forensics Department
DP	Dubai Police
FBI	Federal Bureau of Investigation
IoE	Internet of Everything
IoT	Internet of Things
MEMS	Micro Electro Mechanically Systems
NFI	Netherlands Forensic Institute
UK	United Kingdom
USA	United States of America

CHAPTER 1: RESEARCH INTRODUCTION

The chapter provides a general background in Digital Forensics (DF), and discusses related studies on the trends in DF. The chapter then discusses the statement of the problem and the different factors that affect the investigation process; specifically, the Total Evidence Volume per Case and the Heterogeneity of Evidence Items per Case.

The chapter then discusses the research aims, questions, and objectives, separating out the aims and research questions of each of the studies conducted in the research. The chapter also gives an overview of the research design and methodology and explains the thesis' contribution to knowledge. Finally, the chapter explains the organisation of the thesis.

1.1. Research Background

Digital Forensics (DF) is the process of investigating cybercrimes where several digital devices might be key sources of evidence in different cases. Whilst personal computers spread widely in the 1980’s, the importance of DF was not recognized until the 1990's, when internet use increased and people started to perform illegal activities online (Mohay, 2005). The timeline of DF can be described in three main phases: the ad-hoc phase, the structured phase, and the enterprise phase (Forensics-Research). The ad hoc phase lacked structure, clear goals, adequate tools, processes and procedures. The structured phase was the complex era when DF practitioners developed accepted procedures, and special tools, and criminal legislation of digital evidences became the norm. DF is currently in the enterprise phase, involving real-time collection of evidence and the further development of field collection tools.

In just two decades, DF has become a valued field in forensic science, playing an important role in many criminal and civil investigations. One of the reasons for the rapid prominence of DF investigations is the increase in digital evidence in proportion to the amount of digital data generated by people, computers, devices, and things. Simply put, there is a mammoth amount of digital data generated daily. Several years ago, IBM reported that the world created around 2.5 Exa-bytes of data per day (Thomas, 2011). As shown in Figure 1 below from CISCO’s Global Cloud Index, data is growing at a 40 percent compound annual rate, and is expected to reach nearly 45 Zettabyte by 2020 (CISCO, 2016).

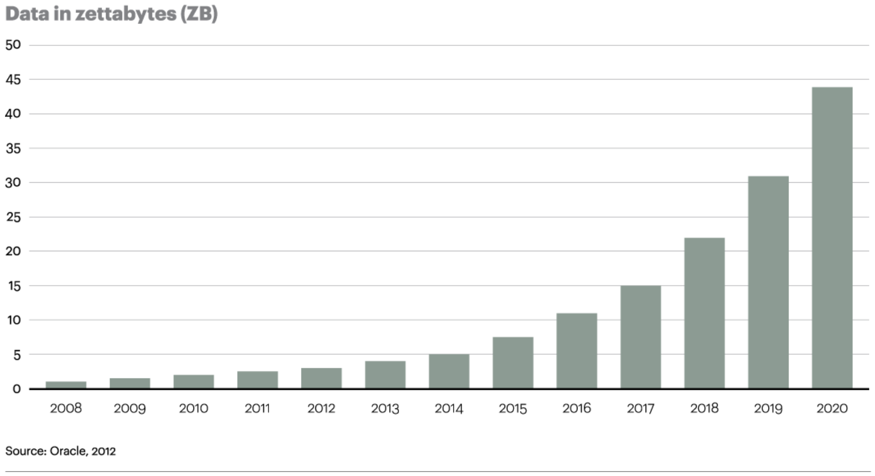


Figure 1. CISCO Global Cloud Index (CISCO, 2016).

One of the pressing problems facing DF investigation is the rise of Big Data. Collections of datasets that are too complex and large to be processed with normal management tools and Databases are known as "Big Data”. The term was first introduced by Doug Laney in 2001 (Wigmore, 2013). Big Data results from the combination of structured and unstructured data (Johnson, 2013), and its complexity derives from three main properties: velocity[1], volume and variety (3Vs). The Big Data challenge is more about the combination of those properties rather than just big volume alone. Figure 2 below shows the 3V properties associated with growth in Big Data.

[1] Velocity: Speed of data created, stored, analyzed and visualized

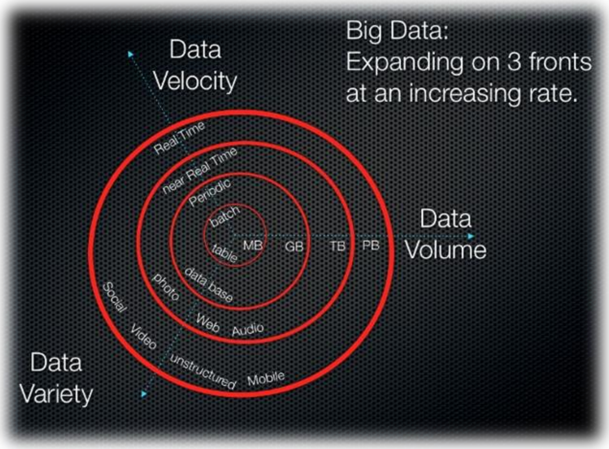


Figure 2. 3V properties of Big-Data (Thomas, 2011)

Aside from Big Data, other trends increase the volume, velocity, and variety of data that DF investigations have to tackle. Currently, most data come from human beings as they type, press, record, take a picture, scan a bar code, or do some other action (Wigmore, 2013). However, increases towards autonomous machines and systems, as described in the Internet of Things (IoT) and the Internet of Everything (IoE) also result in data being created from non-human actions (Evans, 2013).

The Internet of Things (IoT) is the scenario where objects, animals or people are given unique identifiers and can transfer data over the network without the need of human-to-human or human-to-computer interaction. The IoT was constructed from the combination of wireless technologies, micro electromechanically systems (MEMS), and the internet. The first implementation of an IoT type technology was in the 1980s at Carnegie Melon University. The programmers were able to connect to a Coke machine over the Internet to check the status of the machine and allow humans to determine if they could find a cold drink waiting for them (Wigmore, 2013). IoE is the next evolutionary extension of IoT (ABIresearch, 2013). Further implementation of this technology in the future is expected. (Barrett, 2012). You could visualize the technology in many forms like the heart monitor implant transmitting details about heart functions, connected cars informing the driver of needed vehicle services, water delivery systems locating leaky pipes and many other “things” that transmit data wirelessly to the internet to provide better and more reliable services to humans. This technology is spreading wider every day.

As these innovations transmit and create data, adding to the human generated data, traditional digital forensic methods face several challenges especially in the light of more and various digital evidence (DE).

1.2. Studies Related to Trends in DF Cases

Several studies have examined the trend of increasing data. These studies, discussed further below, include the Gogolin Study, the SANS Study, the NFI Study, the Dezfoli Study, and the Irons and Lallie Study. These studies confirm an increase in digital crimes and digital data and highlight some of the challenges DF organizations and investigation processes must overcome considering the increase in the volume, variety, and velocity of digital data. Several studies suggest that the DF field must adopt new technologies and techniques and improve DF resource and capabilities to address the challenges to DF.

1.2.1. Gogolin Study

This research project studied more than 45 agencies in Michigan, USA (Gogolin, 2010). The aim was to study the experiences and investigation capabilities of law enforcement using an interview methodology. The researcher later extrapolated from the study using Federal Bureau of Investigation (FBI) crime reports. Although FBI reports indicate only general information about annual crime statistics, the study used a series of scenarios to extrapolate how many crimes involved a digital device. The study found that digital crimes increase rapidly each year. The study also cited a previous study conducted in 2009 by Michigan law enforcement showing that investigators could process an average of 35 cases annually. The study estimated that as only 70 investigators were working in Michigan law enforcement at that time, it was likely that case backlogs would increase. The study concluded that the problem would only worsen. For example, New York City law enforcement investigated about 200,000 crimes in 2008. If 10% of those crimes involved digital devices, then digital forensic departments were facing a vital problem that needed urgent solutions. Additionally, the study found that only 34% of the digital forensic investigators had received training. This situation had also contributed to the reduced capability of DF investigators.

1.2.2. SANS Study

The SANS analyst program (SANS, 2013), conducted a statistical study on the problems of DF and incident response. Noting that DF is changing rapidly, SANS revealed that some of the difficulties in this field included dealing with non-traditional devices (e.g. virtual, cloud and embedded devices), platforms and systems. The study also found that practitioners engaged in several different types of DF practice: 79% investigated internal network systems and applications, 60% investigated virtual systems and networks, 45% investigated web applications, and 15% investigated server infrastructure in the cloud. SANS researchers also found that when dealing with non-traditional devices, most practitioners did not use tools specifically designed for those devices.

SANS researchers also conducted a further statistical study to identify the challenges encountered by practitioners when dealing with non-traditional devices. The researchers identified legal issues of ownership and privacy, a lack of standards and tools, a lack of skills training and certification, a lack of established police, and a lack of visibility as the primary challenges. Moreover, the researchers concluded that the most difficult activity faced is obtaining a forensically sound copy of the digital evidence item.

1.2.3. NFI Study

An extensive study was conducted by the Netherlands Forensic Institute (NFI) to cover current and future trends and challenges affecting different disciplines of forensic investigations, including digital crimes (Tjin-A-Tsoi, 2013). The study showed that crimes had increased remarkably in the past 15 years, with the number of 2013 cases increasing six-fold over that time. The Dutch workforce had also increased in this period from 200 to 600 people Two main factors were found to contribute to the growth of number of forensic cases: capabilities of new technology and increased awareness about the importance of forensic science. The needs of many government and private organizations drove the increase in cases.

1.2.4. Dezfoli Study

In 2013, there was another statistical study conducted to cover the trends of all the aspects of DF and security (Dezfoli et al., 2013). The study provides some estimation about future research trends in this area. It is important to mention that this study's main limitation is the use of different research papers for data analysis. This fact hinders the attainment of a higher accuracy of the statistical data. The study illustrates that many tools facilitate digital forensic investigations. Some of the tools increase the efficiency of acquiring digital evidence items, while other tools are very powerful to extract the evidence from, and reduce the duration of, analysis. However, the study suggests some factors, which needed to be adopted by digital forensic investigations, to adapt to new challenges in the field. For example, the study proposed the adoption of new technologies and techniques in acquisition, rather than traditional methods, and the expansion of the investigation procedures of cloud computing and peer-to-peer networking.

1.2.5. Irons and Lallie Study

In 2014 a research study, using the annual data published by the FBI from 2007 to 2011, demonstrated year on year growth in numbers of forensic investigations, in the amount of data being investigated and in the amount of data being investigated per case (Irons & Lallie, 2014). All the trends increased radically over the years. The study suggested the need to consider more effective and efficient procedures in different processes of digital forensic investigations to cope with the growing scale of cybercrimes. In addition, the study suggested the need to improve the use of resources available and to move beyond the capabilities of the current forensic tools. The study suggested the use of artificial intelligence to address various challenges in DF.

1.3. Statement of the Problem

In the field of DF, which is sure to get more complicated in the future. numerous challenges have emerged over time, For DF practitioners, the most notable consequence of technological advances like the IoT and the IoE that further increase Big Data is the resulting extensive increase in the potential Total Evidence Volume per Case and in Heterogeneity of Evidence. The challenges come from an increase in velocity, volume, and variety (the ‘3Vs’) of data coming into digital forensic investigations (Johnson, 2013). As Jusas et al. (2017) states, “the evolution of modern digital devices is outpacing the scalability and effectiveness of the digital forensic techniques.”

There are examples of criminal investigations where forensic examiners had to acquire thousands of gigabytes from diverse devices to process the DF investigation. To give some quantitative examples, the Royal Military Police in the United Kingdom collected 75 terabytes of data when investigating allegations of abuse of British soldiers in Iraq between 2003 and 2008 (Bowcott, 2013). The FBI compiled one million gigabytes (1 PetaByte) (Konkel, 2013), in the aftermath of the Boston Marathon bombing incident. Generally, these trends will keep increasing steadily in the future.

The growth in volume and variety of digital data, as well as many other factors, poses delays to DF investigation processes. Consequently, management strategies and practices need to consider all those challenges to mitigate DF investigation delays.

It is important to research the impact of data volume and variety on DF investigation processes. Furthermore, understanding the management procedures and practices is very important to absorb the different challenges occurred in the field. The research questions and hypotheses that address this problem are presented and discussed in the next section.

1.4. Research Aims, Questions and Objectives

1.4.1. Overall Aims of the Research

The overall aim of the research is to measure the growth of DF investigation and illustrate the challenges in order to identify several factors that affect the delay in the DF investigation process. The research will specifically consider Total Evidence Volume per Case and Heterogeneity of Evidence Items per Case. Furthermore, the research aims to illustrate several case management strategies and workflow implementation practices in order to propose solutions to assist the profession to go forward.

The following research questions will drive the inquiries throughout the entire research:

Research Question 1:
What are the trends and challenges encountered by practitioners faced with large volume/heterogeneity DF investigations?

Research Question 2:
What are the effects of different factors behind the delay of DF investigation process?

Research Question 3:
What are the different case management strategies and workflow implementation practices currently used?

These questions are investigated in three studies. Study One (Investigation of the Dubai Police records) will deal primarily with Research Question 1 and partially Research Question 2. Study Two (Interviews with DF managers) will deal primarily with Research Question 2. Study Three (Confirmation of the Interviews) will deal primarily with Research Question 3.

1.4.2. Study One (Investigation of the Dubai Police Records) Aims and Questions

The aim of the first study is to measure the growth of cases and extrapolate the main factors behind the delay of digital investigations. The factors will relate to Number of Cases, Total Evidence Volume per Case, Number of Evidence Items per Case and Heterogeneity.

The following research questions will drive the inquiries in the first study:

Research Question 1.1
What are the trends for the cases investigated by practitioners over the past twelve years?

Research Question 1.2
What influence does Total Evidence Volume per Case have on the investigation processes?

Research Question 1.3
What influence does Heterogeneity of Evidence Items per Case have on the investigation processes?

Before collecting and analysing the data, this study posits the following hypothesis:

Hypothesis 1
There is an increase on the cases trends over the past 12 years.

Hypothesis 2
The Total Evidence Volume per Case affects the time required for the examination process.

Hypothesis3
The Heterogeneity of Evidence Items per Case affects the time required for the examination process.

1.4.3. Study Two (Interviews with DF managers) Aims

The aim of this study is to understand the context of work in various government and private digital forensic laboratories in different countries. The status of work processes in those laboratories is illustrated and the different strategies of assigning digital forensic cases among examiners are also discussed. This study also explores the different workflow implementation practices, which are adopted by different departments/companies. This study will also intensively highlight the different factors and trends likely to affect the Person-Hours of investigation.

The main contribution of this study is to bring together decision makers from different experiences and backgrounds to identify and understand various strategies of assigning, and management of, cases. This study also elicits reflections from professionals in the field to identify the main factors affecting the Person-Hours of investigation and to summarise what they suggest to overcome those effects.

1.4.4. Study Three (Confirmation of the Interviews) Aims

The aim of this study is to validate the findings of the second study. The researcher conducts Semi-Structured Email Interviews with the participants to evaluate the potential applicability of different case management strategies and the implementation practices of the workflow. This study will highlight the pros and cons of the different strategies and practices.

The main contribution of this study is to get feedback from the decision makers on the different strategies, practices and techniques applied in various departments and companies.

1.5. Research Design and Methodology

A mixed methods case study and sequential explanatory design frame the research, using both quantitative and qualitative methods. Study One (Investigation of the Dubai Police records) involves a quantitative analysis of case records collected from the Dubai Police (DP) Database and reports. The second and third studies follow a qualitative approach using the phenomenological follow-up explanation model.

1.6. Contribution to Knowledge

The main contributions of this research are; illustrating the trends of DF cases and identifying digital forensic factors that affect the investigation processes by using thousands of records stored in the Dubai Police (DP) Databases and reports by giving the researcher a unique access to secondary data. Employing the quantitative methodology, the research first develops a clear vision of the cases trends in DP throughout 12 years based on the evolution of Total Evidence Volume per Case and Heterogeneity of Evidence Items. This research also contributes to knowledge by defining a number of equations to calculate several variables corresponding with the digital forensic investigation processes.

In addition to the quantitative data, the research then uses qualitative methodologies to identify the challenges and factors affecting DF processes, and enriches the research with the experiences of interviewed practitioners to categorise different case management strategies and workflow implementation practices.

Additionally, this research is distinctive as it suggests several Decision Tables to assist DF managers and supervisors to choose best case management procedures and workflow implementation.

The outcome of this research will be relevant to researchers, DF investigators, DF case managers, DF laboratories, governments, law enforcement agencies, and businesses. The research will increase efficiencies and effectiveness in DF organisations, case management, and processes by identifying factors that contribute to delay in DF investigations, identifying existing gaps in the current research regarding these factors, and proposing Decision Tables for suggesting which case management procedures and workflow implementation practices to use depending on several conditions. Being a digital forensic examiner for more than nine years at the Dubai Police, gave me the privilege to interpret the research and bring together the results in a practical manner.

1.7. Organization of the Thesis

The thesis is organised into seven chapters as follows:

Chapter 1 – Introduction – including the research problem, aims, objectives, and contribution to knowledge.

Chapter 2 – Literature Review - with a focus on literature that has addressed the challenges of DF investigation case management, and proposed solutions to those challenges.

Chapter 3 – Research Methodology - describes research methodologies and provides justification for the methods used. The chapter also discusses and justifies the research design and strategy, Finally, the chapter discusses and justifies the data collection method implemented in the research.

Chapter 4 – Data Collection - describes the data collection methods of each of the three studies separately, including a discussion of participant selection, data gathering procedure, and sampling design.

Chapter 5 – Data Analysis - including the hypotheses and observations from Study 1 (Investigation of the Dubai Police records), the use of the phenomenological methodology to analyse qualitative data in the second and third studies, and the use of the deductive approach in Study 3 (Confirmation of the Interviews).

Chapter 6 - Outcomes – a discussion of the principal findings and lessons learned from the studies. The chapter ends with a discussion of a series of case management strategies and workflow implementation practices and a set of Decision Tables.

Chapter 7 – Conclusion – summarises the contributions, revisits the research questions and discusses research limitations and potential for future work.

CHAPTER 2: LITERATURE REVIEW

2.1. Introduction

This chapter discusses the review of the literature undertaken with the aim of exploring the general background of Digital Forensics (DF), and the current state of the literature on the challenges and solutions around the management of large-scale investigations with an increasing volume of data. The chapter is divided into seven sections. The first section provides a general background on DF and its development as a field and then the second section of the chapter discusses the DF investigation process and presents various DF investigation models as proposed in the literature. The third section of the chapter discusses the various challenges to DF identified in the literature that affect DF investigations and case management. These challenges include (1) heterogeneous sources, (2) data diversity, (3) anti-forensics, (4) Big Data, (5) legal requirements, and (6) DF department efficiencies. This exploration is followed, in section four, by an investigation of the solutions that researchers have proposed to overcome the identified challenges. These solutions include (1) DF tool features, (2) random sampling, (3) triage, (4) enhanced previewing, (5) information visualization, (6) distributed DF, and (7) data mining tools. The fifth section discusses the experience of others in tackling the challenges and leads onto a sixth section that reviews the literature on case management and assignment, with a discussion of solutions to case management challenges that include workflow. Finally, the seventh section discusses the identified gaps in the literature relevant to the research.

2.2. Digital Forensics

Digital Forensics (DF) is seen as a new area of IT but in fact has been known as a discipline for over forty years (Jawale 2010). In that time, DF has undergone, and continues to undergo, constant technological updates that pose increasingly novel and complex challenges. The impetus that drove the formation of DF as a scientific field of study was the observed increase in computer crime rates immediately after the introduction of personal computers, which criminals used as a tool to perpetrate crimes (Jones et al. 2009). In the 1970’s, investigators first applied DF techniques to recover unintentionally erased data from highly fragmented Database files (Jawale 2010). By the 1980's, software utilities had become available with the rudimentary capability of data recovery.

In 1984, the Metropolitan Police in the UK established the first computer crime unit dedicated to the field of DF, consisting of investigation units including the Forensic Science Unit, the Computer Crime Working Group, and the Association of Chief of Police Officers (ACPO), (Goodwin, 2003). It took another fourteen years before the ACPO issued the first guidelines for computer crime investigations (Pollitt 2001, Sommer 2011). Most of the other parts of the world did not engage in dedicated DF investigations until the early part of the 21st century (Pollitt, 2010). By then, the rapid development of DF investigation had become apparent, along with the need to prevent, investigate, and prosecute cybercrimes. Today, researchers divide DF into three sub-fields of specialization: Database forensics, mobile device forensics, and network forensics (Jawale 2010).

As technology has advanced, cyber criminals use more advanced tools to commit crimes, posing additional challenges and pressures to improve DF investigation tools, processes, and techniques and to promote further specialization in the sub-fields of DF. Among the most persistent challenges in DF is how to deal with the increasing volume of digital evidence and cases processed through traditional DF investigation methods.

2.3. DF Investigation Process

Many DF investigation process models have been proposed, but no single model has yet emerged as a global standard for DF investigation (Pollitt, 2007, Casey, 2009). Still, the various proposed models for DF investigation typically consists of the following four foundational elements: (1) collection or acquisition, (2) examination or identification, (3) analysis or evaluation, and (4) presentation (Baryamureeba & Tushabe, 2004, Pollitt, 1995, Harrell, 2010). Collection or acquisition is the process of using standardized and accepted procedures to maintain a duplicate of the digital evidence. Examination or identification is the process of a comprehensive systematic search of electronic evidence relating to the suspected crime. Analysis or evaluation is the process where the examiner quantifies and reconstructs fragments of data to come up with logical conclusions based on the evidence found. Presentation is the process to summarize the findings and clarify the conclusions for admission of evidence.

As DF investigations have evolved, taking into consideration the challenges of evolving technologies, researchers have proposed DF investigation models that incorporate additional stages and additional DF devices. In practice, there may be hundreds of variations of the DF investigation process, with each organisation possibly developing its own procedures based on the technological requirements of the investigation (Selamat et al., 2008). Due to the variety of digital crimes, DF investigators will likely select the applicable framework on a case-by-case basis, often revising the methodology to fit the needs of the case (Sanya-Isijola, 2009). Still; it is worth examining proposed and published DF investigation models. See Table 1 below.

Model or Framework Name	Researcher (Year)	No. of Stages
Computer Forensic Investigative Process	Pollit (1995)	4 processes
DFRWS Investigative Model	Palmer (2001)	7 steps
Abstract Digital Forensic Model	Reith, Carr & Gunsch (2002)	9 components
Integrated Digital Investigation Process	Carrier & Spafford (2003)	17 phases
End-to-End Digital Investigation	Stephenson (2003)	9 steps
Enhanced Digital Investigation Process	Baryamureeba & Tushabe (2004)	21 phases
Extended Model of Cybercrime Investigation	Ciardhuáin (2004)	13 activities
Hierarchal Objective Based Framework	Beebe & Clark (2005).	6 phases
Forensic Process	Kent, Chevalier, Grance & Dang (2006)	4 processes
Investigation Framework	Kohn, Eloff, & Oliver (2006)	3 stages
Cyber Forensic Field Triage Process Model	Rogers, Goldman, Mislan, Wedge, & Debrota (2006)	
FORZA Model for Cloud Forensic	Leong (2006)	
Common Process Model for Incident and Computer Forensics	Freiling & Schwittay (2007)	4 phases
Live and Static Data Acquisition Model	Perumal (2009)	
Relational Reconstruction Model	Ademu, Imafidon & Preston (2011)	
Big Data Framework	Adedayo (2016)	

Table 1. DF Investigation Models or Frameworks

2.3.1. Computer Forensic Investigative Process

Pollit (1995) proposed a four-step DF investigation model called the Computer Forensic Investigative Process (CFIP) that consists of (1) acquisition, (2) identification, (3) evaluation and (4) admission of evidence. CFIP is widely recognized as the first proposed methodology for the DF investigation process.

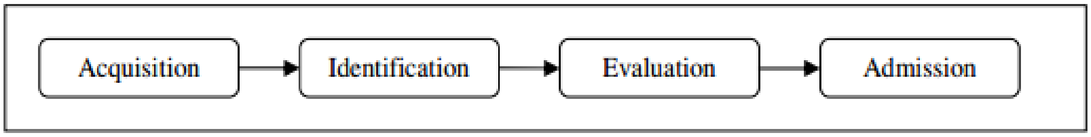


Figure 3. Computer Forensic Investigative Process.
Source: INFOSEC Institute (2016).

2.3.2. DFRWS Investigative Model

In 2001, a group of researchers presented a seven-step DF investigation process at the 1st Digital Forensic Research Workshop (DFRWS). The seven-step process includes (1) identification, (2) preservation, (3) collection, (4) examination, (5) analysis, (6) presentation, and (7) decision (Palmer, 2001). The model starts with the identification phase, which detects the systems and evidence items. Second, the preservation phase includes tasks such as following the required processes to maintain the chain of custody. The collection phase includes tasks that entail the collection of the required data. The examination and analysis phases include tasks like evidence trace, validate, recovery, data mining, and timeline. Finally, the presentation phase includes tasks like documentation and expert testimony. Most researchers later extended and enhanced their models from the DFRWS investigative model (Palmer, 2001).

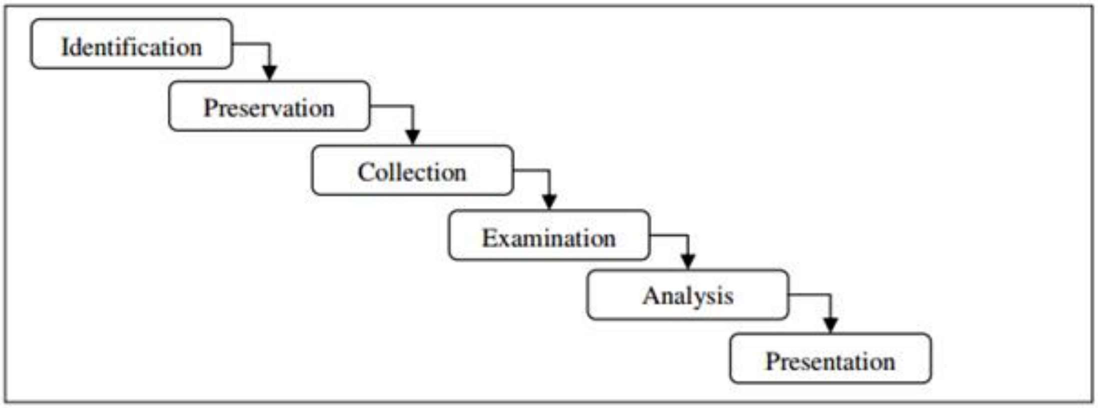


Figure 4. DFRWS Investigative Model. Source: INFOSEC Institute (2016).

2.3.3. Abstract Digital Forensic Model

The following year, Reith et al. (2002) proposed a model called the Abstract Digital Forensic Model (ADFM) that he argues is an improvement from the DFRWS model for DF investigation because the researchers built it on the classic strategy for DF investigation as conducted by police departments.

ADFM added three significant phases to the DFRWS model. Those phases are preparation, approach strategy, and returning evidence. The preparation phase comes after the identification phase, then approach strategy, preservation, collection, examination, analysis, presentation, and finally the returning phase. The preparation phase includes tasks like tools preparation, technique identification, and securing necessary management support. Reith et al. (2002) introduced the approach strategy phase to maximize the acquisition of evidence items and minimize any negative impact to the victim and surrounding people. Finally, the returning phase aims to ensure that the evidence items return to the owner in the required condition (Yusoff et al., 2011).

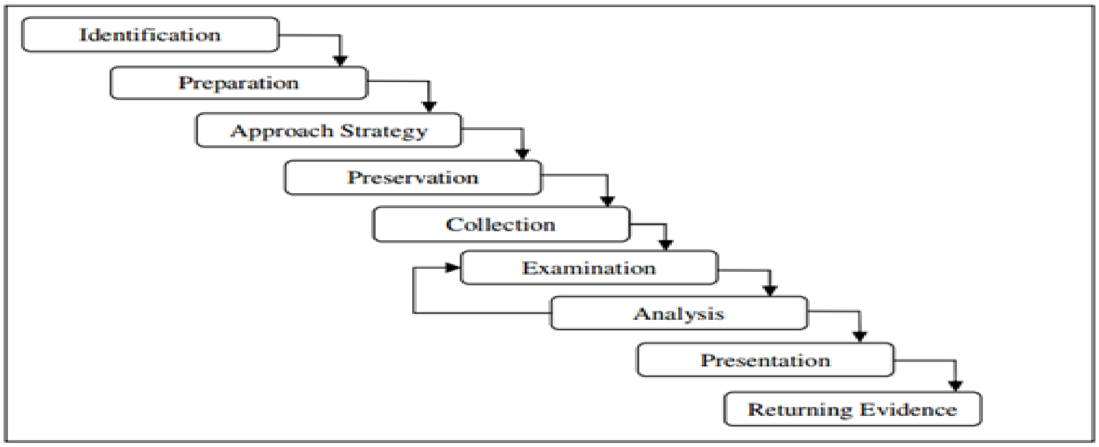


Figure 5. Abstract Digital Forensic Model. Source: INFOSEC Institute (2016).

2.3.4. Integrated Digital Investigation Process

In 2003, Carrier and Spafford (2003) proposed the five-group, seventeen-stage Integrated Digital Investigation Process (IDIP), integrating and building on previous models to combine the physical and digital forensic investigation processes. The five groups include; (1) the readiness phases, (2) the deployment phases, (3) the physical crime scene investigation (CSI) phases, (4) the digital CSI phases, and (5) the review phase.

The readiness phases' main goal is to ensure that the DF organisation supports the investigation by obtaining the required operations and infrastructure. The deployment phases include the mechanism for a DF investigator to detect and confirm an incident. The physical and digital CSI phases introduce the processes of preservation, survey, documentation, search and collection, reconstruction, and presentation. Physical CSI intends to deal with physical evidence items, and digital CSI intends to deal with digital evidence items. The review phase includes the processes of revisiting the whole investigation process.

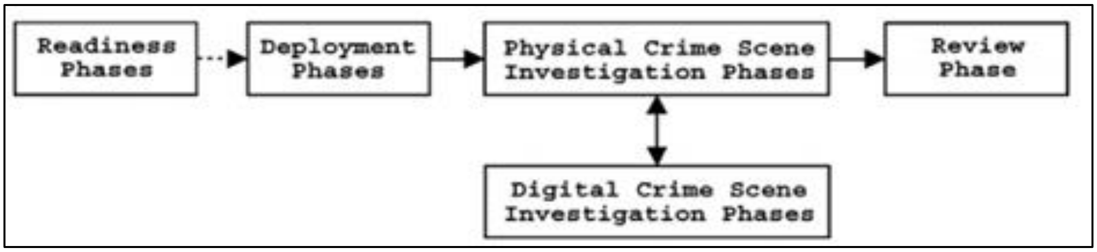

Readiness Phases
Deployment Phases
Physical Crime Scene Investigation Phases
Review Phase
Digital Crime Scene Investigation Phases

Figure 6. Five groups of Integrated Digital Investigation Process. Source: INFOSEC (2016).

2.3.5. End-to-End Digital Investigation Process

Stephenson (2003) merged the DF investigation process into nine stages in the proposed End-to-End Digital Investigation (EEDI) model. The EEDI identified critical activities during the collection process that included the collection of images of affected computers, collection of logs of intermediate devices especially those on the internet, collection of logs of affected computers, and collection of logs and data from intrusion detection systems, firewalls, etc. EEDI is an analysis driven model that merges events from multiple locations.

2.3.6. Enhanced Digital Investigation Process

Baryamueeba and Tushaba (2004) argued for an amendment of the IDIP model, proposing the Enhanced Digital Investigation Process (EDIP) model. This model is the most complex of those reviewed here. The EDIP added two stages to IDIP (trace back and dynamite) to separate the investigation from the digital device and the physical crime scene in order to avoid inconsistencies (Baryamueeba and Tushaba, 2004, Selamat, et al., 2008).

2.3.7. Extended Model of Cybercrime Investigation

Ciardhuáin (2004) proposed the Extended Model of Cybercrime Investigation (EMCI), which consists of thirteen activities: awareness, authorisation, planning, notification, search and identify, collection, transport, storage, examination, hypotheses, presentation, proof/defence and dissemination. EMCI provides clear steps that make it easier to understand the process of cybercrime investigation as it focuses on specific 'action' steps such as presenting the information flow in an investigation rather than focusing on evidence related nomenclature.

In this model, awareness is about the creation of awareness that an investigation is required, authorisation is concerned with getting permission to carry out the DF investigation and the planning phase suggests the DF investigator plans the activities needed and identifies if further authorisation might be required. The notification phase starts the process of action by requiring the DF investigator to inform all the required parties that an investigation is underway. This is followed by the search and identification phase which deals specifically with locating and identifying the required exhibits and then the collection phase, when the images and evidence items are seized. In the transport phase, the DF investigator transfers the seized evidence items to the lab before safely storing and labelling them in the storage phase. The examination phase includes the techniques to find and interpret significant data. The hypothesis phase is when the DF investigator must construct a hypothesis of what occurred based on the examination of the evidence items. In the presentation phase, the DF investigator must illustrate the hypothesis for somebody else other than the investigators and then in the proof/defence phase, the DF investigator must prove the validity of their hypothesis and defend it against any challenge or criticism. The final phase indicates the dissemination of information from the investigation. This model aims to help the investigators with their future tasks and help in the development of policies and procedures. The dissemination activity can be provided by real time support for investigators or by providing archives of knowledge and experience of the investigators for the examiners to refer to when needed.

2.3.8. Hierarchal Objective Based Framework

Beebe & Clark (2005) proposed the Hierarchal Objective Based Framework (HOBF), a multi-tier process model that aims to be practical and specific. Each tier is based on objectives rather than tasks. This model suggested three tiers with sub phases. The first-tier phases include preparation, incident response, data collection, data analysis, presentation and incident closure, while the second-tier phases are objective based tasks that include the survey phase, extract phase and examine phase. The final tier phase is mainly concentrated on the examination of extracted data to reach the confirmation and reconstruction goals. HOBF is flexible and can be applicable to any future need by adding new layers and new sub-categories.

2.3.9. Forensic Process

Kent et al. (2006) introduced a four-stage DF investigation model called the Forensic Process (FP), resembling the CFP proposed by Pollit (1995). The four stages include; (1) collection, (2) examination, (3) analysis, and (4) reporting. The forensic process transforms media into digital evidence by extracting data into a format compatible with forensic tools. The process transforms the data into information through the analysis phase, and into evidence through the reporting phase.

2.3.10. Investigation Framework

Kohn et al. (2006) proposed a three-stage model called the Investigation Framework (IF) that draws from previous experiences of researchers in the field. IF identifies three stages as minimum requirements to qualify under the definition of “forensics”. These three stages are; (1) preparation, (2) investigation, and (3) presentation. Importantly, IF highlights the need to base the framework on the relevant legal requirements prior to the investigative process, and the importance of documentation during the investigative process.

2.3.11. Common Process Model for Incident and Computer Forensics

The most recent framework in this review is one to conduct cybercrime investigations that was proposed by Freiling et al. (2007) called the Common Process Model for Incident and Computer Forensics (CPMICF). This is a cybercrime investigation process that combines incident response and computer forensics. CPMICF aims to enhance DF investigation through an analysis driven model that consists of the following four stages: (1) Pre-Incident Preparation, (2) Pre-Analysis, (3) Analysis and (4) Post-Analysis.

2.3.12. Other Proposed DF Investigation Models

Other DF investigation models focus on aspects of the investigation process that could be improved or focus on extending the application of the DF investigation process to unique technological demands. For example, Rogers et al. (2006) proposed the Computer Forensic Field Triage Process Model (CFFTPM), which focused on a field approach to identification, analysis and interpretation within a short time frame, and abandoning the in-depth lab examination or forensic imaging. Leong (2006) proposed the FORZA Model, a cloud forensic framework that does not follow the typical DF investigation elements but is instead a technical-dependent framework. Likewise, Perumal (2009) proposed a model that highlights the importance of live and static data acquisition in the investigation process. Ademu et al. (2011) proposed the Relational Reconstruction Model, which addresses the necessity for reconstruction and interaction, highlighting the regular interaction of all investigation resources. More recently, Adedayo (2016) proposed a Big Data Framework that contributes to already existing frameworks by introducing more efficient collection, preservation, analytical, and presentation techniques.

2.3.13. Implications of the DF Investigation Models

There are many suggested Digital Forensics processes. All the described frameworks/processes draw on the experience of the authors and each author highlights his perspectives. It is clear from all the suggested processes that having a relevant legal basis is an important aspect to consider before setting up a framework because it will affect the entire DF investigation process. Furthermore, the processes show that they need to have the basic forensic requirements such as preparation, investigation, and presentation (Kohn et al., 2016). The aim of all those suggested processes and frameworks is to establish a clear guideline of DF investigation.

All these studies illustrate the fact that plenty of research has been conducted to identify guidelines for DF investigation. However, there is little research identifying the DF processes that take place prior to the DF investigation itself, such as DF case management and workflow implementation practices. As such, little is known as to whether the most appropriate decisions have been made when allocating cases and whether, and to what extent, those decisions affect the later DF investigation processes.

2.4. Challenges to DF Investigation and Case Management

As is clear from the models outlined above, there is a consensus as to the main elements of a digital forensic investigation. This section discusses the challenges highlighted by researchers with respect to the four foundational elements of the DF investigation process: collection, examination, analysis and presentation.

A review of the DF investigation challenges shows a close link to case management challenges, especially the challenges related to heterogeneous sources, data diversity, Big Data, and DF department efficiencies. These challenges, whether separately or cumulatively, seem enough to create substantial delay in DF investigation, and increase backlogs and Person-Hours.

2.4.1. Heterogeneous Sources

Heterogeneous sources have become a very critical aspect to consider in DF. Digital Forensic Departments are receiving an extraordinary number of digital devices yearly. For instance, every year the London Metropolitan Police (MPS-DEFS, 2015) receives more than 38,000 digital devices, which a team of about 80 practitioners must investigate (Overill, Silomon, & Roscoe, 2013). Forensic practitioners are required to obtain correlated data from diverse sources (Mohay, 2005). Heterogeneous sources include, but are not limited to, personal and corporate computers, servers, networks, social networking web pages, IoT, IoE, cloud computing, and embedded devices. Cloud computing - "a large-scale, distributed computing model driven by economies of scale, which provide the abstract, virtualized, dynamically scalable, and effective management of computing, storage, the pooling of resources and services, and an on-demand model via the Internet to external users" (Tian & Zhao, 2015) - is a major provider of data to DF investigations. Embedded devices (e.g. smart phones, mobiles, smart watches and health devices etc...) transmit data to smart homes or industrial control systems and create data. One example is the transmission to SCADA which is a software package, positioned on top of hardware to monitor and control very large processes (Boyer, 2009; Daniels & Salter, 1999), and used in many industrial and experimental facilities like steel making, power generation and distribution, chemistry and nuclear fusion.

The heterogeneous sources of data and the expanding diversity of digital devices create a wealth of opportunities for criminals and terrorists to perform illegal activities. The sources of data will only increase tremendously in the future. For example, an estimated 30 billion devices will connect wirelessly to the IoE by 2020 (ABI Research, 2013).

2.4.2. Data Diversity

Forensic examiners are also encountering the challenge of diversity in data types, formats and standards (Anderson, 2004). DF investigators could extract data from Databases, system logs (e.g. event log, Linux system log), software logs (e.g. installation log, transactions log), documents, spreadsheets, backup files and many other file types and formats. In addition, forensic practitioners are not only interested in extracting the standard data, but are also looking for corrupted, encrypted and invalid data to retrieve as much evidence as possible. Typically, DF examiners are searching for tiny pieces of digital evidence or files, most of which are hidden in a chaotic environment. It is also true that development and adoption of new technologies (e.g., self-destructive content, anonymous communication) is increasing dramatically compared to the limited development of digital forensic tools. Forensic tools are incapable of recognizing all data types, a limitation that will likely exacerbate over time (Garfinkel, 2012).

2.4.3. Anti-Forensics

DF practitioners are defeating the tricks and techniques that criminals use to forestall forensic investigations. Known as Anti-forensics, these tricks and techniques come in many forms such as artefact wiping, data hiding, trail obfuscation, data encryption, and attacks against computer forensics tools and processes (Jain & Chhabra, 2014).

Artefact wiping is the deliberate sanitation of data, for example, by removing or destroying the data that resides in the memory. Data hiding is another anti-forensics technique that ensures data becomes undetectable to DF investigators. Examples of data hiding include the relocation of data to locations that DF practitioners will likely ignore from the investigation, or the hiding of files in other file types, known in DF practice as steganography (Johnson & Jajodia, 1998). Trail obfuscation, also known as evidence counterfeiting, is another type of anti-forensics, employed to confuse and disorient the DF investigator. An example of trail obfuscation is the modification of metadata (data about data that a computer or software generates upon file creation).

The ultimate anti-forensics technique is cryptography (Kessler, 2007). Many cryptographic tools make digital investigations difficult, or perhaps, impossible. While cryptography is easy for the user to employ, it increases the time and effort practitioners spend to defeat the encryption and thereafter start the investigation process. Criminals can employ encryption on file systems, whole disk, or Internet based communications and while DF investigators can easily overcome some encryptions like Wired Equivalent Privacy [WEP], other encryptions such as Pretty Good Privacy (PGP) are more challenging.

In an affront to the DF business, criminals may also attack computer forensics tools and processes by exploiting tool vulnerabilities. For instance, attackers may use the bugs in the validation process of select tools to perform a buffer overflow attack (Garfinkel, 2007).

2.4.4. Big Data: Volume of Digital Evidence

The ever-increasing volume of digital evidence, what some have called "the digital tsunami" (Gogolin, 2010), and the spectacular cost drop of hard drives and solid-state storage capacities have created another challenge in DF: investigation performance. According to Leong (2006), performance has direct implications for the DF workflow. The remarkable growth of digital evidence capacity has resulted in an increasing backlog due to the length of time required to obtain a forensic image, and to investigate all the data in the evidence.

As an example, the cybercrime unit at the Iowa Division of Criminal Investigation (DCI) in the United States had a backlog of 12 to 18 months in child exploitation cases in 2010 (Raasch & Geary, 2010). Delays in many digital crime labs in Michigan exceed two years (Gogolin, 2010). Because of such backlogs, forensic practitioners are increasingly under pressure to improve performance, becoming highly dependent on the automated "push-button forensics" (James, Joshua, & Gladyshev, 2013) to be able to investigate large-scale evidence rapidly. Many digital investigation tools, such as FTK and Encase (Access Data, 2013; Guidance, 2014), provide features to conduct initial and complex investigation tasks that only require pressing one or several buttons. Over time, such practices will diminish the ability of expert investigators, and force forensic practitioners to confine their work to those forensic tools, instead of searching for alternative and creative solutions and techniques.

It is important for DF to adopt new techniques and tools. Thus, it is essential for forensic departments to ensure a balance between push-button and manual forensics in order to maintain the foundation of the practitioners' forensic experience. This is also important to ensure the quality and legal admissibility of the extracted digital evidence (ACPO, 2007; ISO -27037, 2012).

2.4.5. Legal Requirements

In most cases, DF investigators must ensure that there is compliance with the law, legal procedures, and the deployment environment (Palmer, 2001; Quick & Choo, 2014). ISO 27037 provides a list of the legal considerations when dealing with digital evidence. According to Brezinski and Killalea (2002), it is important for the DF investigator to ensure admissibility, authenticity, completion, reliability and believability of the digital evidence. Thus, completion is an important consideration for admissibility of the evidence. It is true that complete does not necessarily mean that everything in the evidence items is imaged but it is a fact that a representation of the whole story needs to be illustrated, and not only a specific perspective. Thus, any proposed solutions to reduce the time to conduct the DF investigation must also ensure the implementation of necessary legal requirements.

2.4.6. Efficiency in DF Departments

Another challenge faced by each digital forensic department is maintaining their unit's efficiency level in the face of growing digital data volume and heterogeneity. Many factors contribute to the efficiency challenge, including the volume of cases, work pressure, insufficient funding, and lack of ongoing training and participation in professional events. It has become more and more difficult for DF practitioners to develop the skills and knowledge needed to cope with improvements and changes in technology. Reducing the work pressure, providing generous funding, and encouraging ongoing training and professional event participation are key factors to increase the efficiency of the investigation process. The lack of enough funding affects many aspects such as training, maintenance, and purchase of equipment, and software (HTCIA, 2010). Logically, improvement of practitioners' knowledge, work environment, tools and solutions would take digital forensic departments to a new level of investigative capability.

2.5. Proposed Solutions to the Challenges

Researchers have proposed a few solutions to overcome the myriad challenges encountered in DF investigations. Additionally, different digital forensic departments have implemented many practical solutions to mitigate or eliminate the challenges. The following section will introduce some of the proposed solutions, which include; (1) DF tool features, (2) random sampling, (3) triage, (4) enhanced previewing, (5) information visualization, (6) distributed DF, and (7) data mining tools.

2.5.1. DF Tools Features

There is no standard to follow when dealing with various types of digital forensic sources and data types (Garfinkel, 2010). However, to mitigate the challenge of Heterogeneity of Evidence Items, many tool vendors are trying to evolve a way out of this problem. Some tools such as Guidance Software, Encase, and FTK (Access Data, 2013; Guidance, 2014) are well known in DF, and others such as Nuix (Nuix, 2013) and Spektor (Spektor, 2013) are new. Guidance Software can obtain a forensic image from a wide array of tablets/smart phones, removable media and hard drives. Encase also provides search and disk level forensic analysis to multiple drives or media simultaneously. Moreover, Encase offers the facility to perform a quick triage by viewing the images. This allows practitioners to eliminate any devices that are not relevant to a case. It is also capable of producing inclusive reports of the findings.

Nuix has launched a tool called “the investigative lab”, a digital analysis tool for use after forensic acquisition. The user must import the forensically sound image into the tool in order to start the analysis procedure. Nuix suggests a solution to data diversity and claims the ability to support a huge range of today's most common data types (Nuix). It can classify virtually any data set including images, videos, documents, spreadsheets, emails and financial records by indexing and filtering the results allowing practitioners' immediate review using a variety of data visualization techniques. Nuix states that this virtual indexing of data allows searching and filtering processes to be extremely quick as it can deal with the complexity of data storage with its ability to export and make searchable items for data stored 100+ levels deep. This means that practitioners can search for data embedded in another file (100 + times) such as an image in a document stored in a PST file. The main concern with Nuix is the lack of scientific papers reporting test results; thus, it becomes important to examine it to determine its compatibility with fundamental forensics procedures. It is also important to find out the efficiency of the product, and to compare its performance with traditional DF tools.

Another relevant tool is Spektor, a DF solution supported by Dell (Dell, 2011). Dell developed the software for law enforcement, corporate and government security agencies, and e-discovery organizations. Spektor is mainly used for CSI or in triage and has features for collecting, triaging, imaging, storing, analysing, reporting and archiving digital evidence. It claims the ability to take a forensically sound image from various types of sources such as a MacBook and devices with multiple disks or solid-state storage (Spektor). It is important to mention that Spektor can deal with heterogeneous data sources such as computers, removable media and mobile phones. It claims to be able to run forensic investigations of over 6000 handsets and uses triage techniques to give practitioners the ability to make decisions about whether a device contains important evidence artefacts and needs seizing. Spektor claims that it is faster than other triage solutions because it does not triage the data using the target device's resources; rather, it uses the examination's device resources. Despite these claims, there are no scientific papers or research reporting results of experimentation with Spektor (e.g., its strengths, weaknesses and the admissibility of the investigation process using it). If those features are confirmed and work efficiently, Spektor would be an effective tool for decision making whether the digital evidence item is important for the suspected crime or not. This feature would reduce the number of digital items collected and would restrict the extensive analysis procedure to devices that, for sure, include important data to the corresponding case.

From all the features introduced by those three tools (i.e., Encase v7, Nuix and Spektor), it is essential to start examining them with a predefined methodology to test their efficiency and effectiveness in dealing with heterogeneous evidence and various data types.

2.5.2. Random Sampling

To overcome the problem of large-scale evidence storage, random sampling is an-approach recommended by researchers to reduce the Number of Evidence Items per Case to be analysed, and collected from different devices (Mora & Kloet, 2010). Indeed, sampling is a well-grounded scientific technique that experts have used in multiple fields including physics and sociology (Bohm & Zech, 2010; Browne, 2006). In forensic sciences, Deoxyribonucleic Acid (DNA) and chemistry forensics extensively use random sampling (Fraser, 2010; Saferstein, 2004). In DF, random sampling is a technique applied to overcome the problem of the ever-increasing size of digital forensic devices when time is a crucial factor. Mainly, a combination of sector hashing and random sampling could determine if certain evidence is in the device (Roy, 2014).

Unlike sector-based hashing, random sampling uses randomly selected sectors to read, hash, analyse and check. To verify the reliability and confidence of the search results, DF investigators use probability and statistics. Random sampling works by breaking the target data into blocks that match the sector size of the digital media. It calculates the hash values of those blocks and stores these in a Database. Then, the process checks the randomly selected sectors by comparing the hash value of those sectors to the hash value of the matched blocks. Because the DF investigator reads the sectors directly from the media, this indicates that the matched files exist at some point in this media. Moreover, random sampling will significantly reduce the time of investigation because reading and hashing is not required for every sector on the digital media.

Research conducted by Taguchi explored a method to provide a balance between high probabilities of random sampling detection and speed (Taguchi, 2013). He developed a program that automates the process of hash based random sampling. Taguchi was able to show that the random sampling on a 1 TB drive is possible with a confidence of 90 % when finding one block of 10 MB of target data in 26 minutes.

Earlier, the Australian New South Wales police force (NSW) conducted research on the application of random sampling to child abuse materials (CAM) (Jones, Pleno, & Wilkinson, 2012). The researchers' main objective was to view a sample of the files on an evidence device and predict the percentage of CAM in other files. They followed a statistical methodology and confirmed the reliability and validity of the experiment. They applied the recommendation of sample size using Yamane's formula, which provides a simplified equation for calculating sample sizes (Yamane, 1967). The implementation of this random sampling resulted in the reduction of the response time from 3 months to 24 hours, and consequently the reduction of CAM cases backlogs.

DF investigators could implement random sampling in other case types. However, more research is necessary in this area to form a reliable procedure for use in DF investigations, and to calculate the difference on time spent between extracting all evidences and extracting random samples.

2.5.3. Triage

Triage is a procedure suggested by researchers to defeat the ubiquitous problem of large-scale investigation. Medical doctors first introduced triage to prioritize the treatment of patients depending on the severity of their conditions (Hogan & Burstein, 2007). Due to time constraints, DF adopted the triage technique to reduce the amount of evidence to be analysed. In contrast to random sampling, in which the DF investigator selects specific records depending on a mathematical calculation, triage prioritizes records according to their importance.

One could divide the triage technique in DF into administrative and technical triage (Shaw & Browne, 2013). In the administrative triage, usually digital forensic laboratories evaluate new cases in order to prioritize them depending on different facts such as type of crime or seriousness of crime. It is true that sometimes media attention may affect case priority, or higher-ranking officers may push the priority of some cases for various reasons. Thus, some researchers suggested having control over those situations by adapting a solid case prioritization method (James, 2014). One of the researchers suggests a method to identify and measure the priority of factors based on the input from multiple stakeholders. This can help to calculate the priority of incoming cases based on the organization's (digital department's) exact needs (James, 2014).

Technical triage prioritizes files in the original evidence, which are likely to be more important. The DF investigator accomplishes prioritisation by targeting available files not yet deleted from the system. For example, when a user deletes a file from the system it does not delete from the hard drive; it goes, and remains, in the recycle bin to give the opportunity for restoring it in the future (Garfinkel & Shelat, 2003).

DF investigators could use the triage technique throughout the various processes of digital investigations. One proposed approach of technical triage is to categorise automatically digital media (Marturana & Tacconi, 2013); another concentrated-on triage based on the importance of evidence at the crime scene (Moser & Cohen, 2013). DF investigators could apply triage in the crime scene to prioritize digital evidence depending on its volatility (Brezinski & Killalea, 2002) and the occurrence of potential evidence. This will allow the practitioner to classify the evidence into three groups: a) the device probably contains important evidence but it is not under immediate threat of destruction, b) the device probably contains important evidence and is under immediate threat of destruction, and c) the device probably does not include any important evidence (Moser & Cohen, 2013). As a result, the devices with important evidence and high volatility (group b) need to be forensically copied and analysed first. To give an example, memory cache is highly volatile and could be lost if the system power shuts down (Schuster, 2008). Next, devices with no volatility threat (group a) must be acquired and analysed. Finally, the devices with no important evidence (group c) should not be forensically copied and analysed. This process will reduce investigation-processing time by eliminating devices with no evidence.

Different digital forensic departments have implemented many practical responses to mitigate the challenges encountered in digital forensic investigations using the triage technique. For instance, the Forensic Institute used several measures to reduce their backlog of cases (Tjin-A-Tsoi, 2013). They used an annual Service Level Agreement (SLA) with their customers (police and prosecution) that set a limit on the number of investigations that NFI had to complete yearly. This gives a clear vision of the department's limits and capabilities and with this agreement, customers are required to triage the cases the forensic department will investigate. Some might argue that the forensic department should treat all cases equally; however, to investigate all cases would be difficult or impossible. Accepting more cases would increase the backlog and delay delivery of results.

Although triage may look like a promising approach to overcome large-scale investigations, it raises completeness issues (Casey, 2011). This means there is a high risk of missing important potential evidence artefacts: evidence residing in encrypted files, emails, unallocated space, swap and mounted file systems. An additional disadvantage of triage is the added cost for further technical triage software or tools (Shaw & Browne, 2013).

2.5.4. Enhanced Previewing

As an alternative to triage, researchers suggested enhanced previewing, which claims the ability to overcome the weaknesses of triage (Shaw & Browne, 2013). Researchers argue that enhanced previewing is useful in large-scale investigations and in examining evidence devices in a forensically sound way.

Shaw and Browne used the GNU/Linux forensic bootable CD (CAINE, 2012), built with open source forensic tool plus forensic analysis tool to allow enhanced previewing features. Enhanced previewing helps to reduce the time for the examination process because it simplifies the ability to reach the data. For example, enhanced previewing provides several configurations that make it easy for the examiner to select the types of file (e.g., email, chat) depending on the case type (e.g., fraud, child indecency). The tool can extract the most common files that usually appear in different case types. Enhanced previewing increases the forensic practitioners' confidence about their investigation because of its capability to search a whole disk, including allocated files, deleted, unallocated space; swap files; full file systems; raw data; encoded data (i.e. email attachments); and memory dump.

In principle, enhanced previewing potentially balances the risks between triage and full forensic investigations. It can generate a very simple output report, which an examiner can later review in any computer platform. On the other hand, this tool has its own weaknesses. For example, the system is not suitable for live investigation. Moreover, no other researchers have used enhanced previewing in their experiments to determine the efficiency of this tool. Thus, future independent study is necessary to determine its strengths and weaknesses in DF investigations.

2.5.5. Information Visualization

Information visualisation is another approach proposed to overcome the problem of huge capacity and Heterogeneity of Evidence Items. The technique is mainly concerned with processing data and presenting visual forms of abstract data using interactive and adjustable mapping techniques. Hence, the overload of digital evidence data received by practitioners could be reduced using information visualisation techniques. Potentially, such techniques enhance efficiency and extracted data appearance while analysing evidence.

The EIC (Explore, Investigate and Correlate) framework (Prefuse, 2013) integrates information visualisation techniques with a web-based application. This open source software has been demonstrated with a practical examination (Osborne, Turnbull, & Slay, 2010) mainly focused on social interaction entities, e.g. emails and phone calls, from different sources of evidence. In general, this empirical study was preliminary because the researchers based it on personal observations, rather than real forensic cases. Further work is necessary in this area to examine its efficiency when applied to real-life digital forensic investigations.

In 2008, Vond, a software developer company, specialized in digital investigations and eDiscovery solutions, introduced Intella, another information visualization tool, to the DF investigations market (Intella, 2013). Intella is an open source product that improves the visualization of data and the social mapping for examiners. Rather than using the traditional tree and table-based approach to display information extracted from devices, Intella uses clusters at different levels of abstraction, potentially making it easier to identify outliers.

The company claims that this tool can improve staff productivity by reducing the costs and time required to carry out an investigation process. Intella has, in principle, a search engine where users can quickly find sampling terms by selecting related terms and eliminating non-related terms. Another supposed strength of Intella is its ease of use. Intella's yearly license and maintenance costs is famously inexpensive in comparison to other digital forensic investigation tools in the market.

Vaidya (2013) conducted a pilot test and two major test case scenarios that demonstrated that Intella can produce quick results with enhanced visualization features. However, Vaidya mentioned that it (Intella) was more complex and time consuming when compared to the closed source tools like Encase and FTK. Moreover, Vaidya mentioned that to be able to install and process the cases using the open source tool, the digital forensic examiner needs comprehensive knowledge. Vaidya conducted the research under several constraints. First, the test was limited to one test and two case scenarios. Secondly, the researcher used a trial version of the tools. Finally, not all the functionalities of the Intella tool were tested. Thus, further tests are required in this area to confirm clearly the efficiency of applying this tool in real-life digital forensic examinations.

2.5.6. Distributed DF

The problem of vast amounts of disk storage and the inadequacy of some DF tools was reported over ten years ago (Vassil & Golden, 2004). This research suggested an early prototype for distributed DF (DDF). They used a six Gigabit hard drive image and examined it over eight nodes. The focus was only on the initialization of the image and the searching process. They found that using DDF tools was faster than using a single workstation. DDF reduced the time from hours to minutes. However, the proposed solution did not address the problem of evidence variety; time consumed in the acquisition, and did not use data from actual cases.

DDF uses the resources of a pool of computer systems in order to manage digital forensic investigation tasks (Roussev & Golden, 2004). It was one of the early suggestions proposed to ease the challenge of vast capacity of storage devices (Roussev & Golden, 2004). Roussev and Golden conducted an empirical study using a 6 GB forensic image against single (one resource) and distributed workstations (multiple resources). The targeted machine had a 6 GB Western Digital IDE hard drive formatted with NTFS, and it had a single partition with windows 2000 system. The hard drive had 110,000 files distributed in 7800 directories. The initialization process (loading the image from disk into the internal memory cache) was the main target of the test. Roussev and Golden used FTK to load the image (Access Data, 2013). In the first experiment with a 3GHz Pentium 4 workstation, it took 1:38 hours to initialize the image. Using similar specifications but with eight workstation nodes, the initialization process took only 9:36 minutes. Thus, they found that using distributed digital resources was much faster than using a single workstation.

Later, many tools were introduced to perform distributed computing such as web analysis tools. The use of technologies developed for Web-centric purposes was a non-forensic tool suggested to overcome the problem of examining huge volumes of data in DFs (Roussev, 2011). An example is the web domain Google's Map-Reduce framework, which is a programming model able to process large data sets in distributed computing environments. Google developed Map-Reduce as a distributed programming paradigm to be scalable where massive parallel applications with terabytes of data could be processed using large commodity clusters (Roussev et al., 2009). One of the most popular implementations of Map-Reduce is Apache Hadoop (Hadoop, 2014). Hadoop is an open source Java implementation of Map-Reduce that provides the necessary minimum functionality by merging simplicity of use with scalable performance (Papadimitriou & Jimeng, 2008). DF investigators have used Hadoop/Map-Reduce in numerous practical examinations, especially for cloud investigations (Xiao & Xiao, 2014).

There are some concerns of applying Hadoop in DF (Roussev et al., 2009). Firstly, it is not efficient enough when attempting to utilize relatively small clusters. Secondly, in order to implement Hadoop, one must use the Hadoop File System (HDFS), and as this works as an abstraction layer on top of the existing file system and it leads to reduced efficiency. Roussev et al. (2009) developed the Message Passing Interface (MPI) Map-Reduce to resolve those concerns. This gives the ability for the Map-Reduce framework to realize efficiently the basic building blocks of many forensic tools. Their experiment indicated that MPI Map-Reduce provides a good platform to develop large-scale forensic processing tools. However, research is necessary to determine whether it has validity within guidelines set for DF.

Recently, most of the commercial forensic tools such as FTK and Encase (Access Data, 2013; Guidance, 2013) have introduced DDF into their products. In 2011, Roussev (2011) conducted an empirical study to test data scalability using the distributed resources in

FTK. The study comprised of a test for four image files. The total size of these four image files equalled 475 GB. The test showed that the full forensic process using one node took 38:09 hours. When Roussev performed the same test on three nodes, it lasted only 12:19 hours.

Practitioners have registered several complaints about implementing DDF: saying it is difficult to apply and very expensive and that additional personnel were needed to adapt the technology (Garfinkel, 2012). Therefore, it becomes very important to test the efficiency and effectiveness of this feature further in real cases following forensically sound procedures to document the results and lessons learned.

2.5.7. Data Mining Tools

Researchers have also introduced tools that implement data mining techniques in the field of DF. Many digital forensic techniques could be conducted using data mining tools such as data recovery, data generation, pre-processing and data analysis (Nirkhi, Dharaskar, & Thakre, 2012). Data mining applications have many advantages, such as the ability to minimize the complexity of investigation, speed up the process of investigation, and improve the quality of the processed data. DF practitioners use data mining extensively for large data sets (Lanka, 2011).

Different DF processes have adopted the technology of data mining by using several tools like Recuva, FTK Encase, Sleuth kit/Autopsy or Pro-Discover for data recovery, data generation and pre-processing (Piriform, 2014; Pro-Discover Forensics; Sleuthkit, 2013). Other tools, such as Waikato Environment for Knowledge Analysis (Weka), Cyber Forensic Time lab, Invisible Witness and LingPipe, are open source data mining tools that could be used to enhance the analysis stage of DF investigations using the methodology of data mining (i.e. association, classification, clustering and regression) (Nirkhi, Dharaskar, & Thakre, 2012). Thus, data mining techniques can benefit digital forensic investigations to reduce the processing time, improve the information quality, reduce the cost of analysis and improve the ability to discover patterns (Quick & Choo, 2014).

Lanka (2011) investigated the application of data mining tools to digital forensic investigations. He compared two data mining tools Weka and Rapid Miner against the well-known digital forensic tool FTK. Using two predefined data sets and two types of digital sources, i.e., thumb drive and a hard drive; he found that such tools could be a better solution for large volume digital device investigation than digital forensic tools such as FTK. However, he declared that researchers should conduct further examination in this area to be sure that DF investigators could implement all the requirements of DF investigation with open source data mining tools. In general, there is a limitation of applying the data mining tools in DF because there is lack of real implementation of data mining techniques on forensic data (Quick & Choo, 2014). Researchers suggest raising awareness and understanding of data mining techniques, training digital forensic practitioners in the use of those techniques, and creating a manageable framework to use data mining techniques in digital investigations (Beebe & Clark, 2005).

2.6. Experience of Others

The Legal Electronic Discovery project (e-Discovery) was a project that investigated large datasets (Sondhi & Arora, 2014). Briefly, they found that for selective handling they could use multi-pass approaches to help in segmentation and qualification of data. They also learnt the value of the early content analysis in helping to quantify the examined data at a given time. Moreover, they found out that visualization is the main factor for fast and interactive analysis. Their work stressed the importance of parallel and pipelined I/O to sustain the processing power of high-end computing platforms and they proposed that predictive coding and predictive analytics techniques could be very helpful when applied to subsequent query, search and processes. Importantly, as one of the few studies into the human impact on DF, they found that both human power and computational power are required for high quality reviews or large-scale processed data. This means that case management and assignment, as discussed in the next section, will play a very important role when investigating large data sets.

2.7. Case Allocation Practices

Several human aspects such as work choices, work assignment, and work autonomy are shown to lead to higher levels of job satisfaction for employees. Research has shown that giving employees more work autonomy results in higher levels of job satisfaction (Wheatley, 2017). Further, research has also showed a clear link between job satisfaction and organisation performance (Bakotić, 2016). High work satisfaction for DF investigators may result in faster investigation or improved DF organisational performance. Thus, it is important to examine job stress and satisfaction among DF practitioners to be able to examine their performance. While DF job satisfaction is beyond the scope of this research, the research does begin to examine DF organisational performance through case allocation practices.

Aside from the challenges around the DF investigation process it is important to review the literature on case allocation practices in DF departments or organisations in order to understand the practical implementation of case delegation, the Person-Hours of investigation and the suggested solutions.

Different workplaces have different structures to some extent. There are organisational cultural differences which cause variation in how organisations perform; and the work delegation process varies from one department or company to another (Allard, 2010; Petty et al., 1995). The unique job in a DF investigation lab requires unique delegation processes. There are legal requirements and rules that each examiner needs to follow. These work practices are further examined in the following sections.

2.7.1. Work Allocation and Productivity in Other Industries

Psychology and strategic human resource management literature have a rich source of research suggesting that human resource management plays an important role in creating competitive advantage for an organisation (Kim and Ployhart, 2014). According to Ployhart and Moliterno (2011), the knowledge, skills, abilities and other characteristics of employees "comprise organisational level forms of human capital resources that contribute to a firm's performance."

Aside from human resources management, it is also necessary to examine case allocation practices. Other industries, like in a variety of health and behavioural settings, have done research and created strategies for case management and case allocation or caseload. (CMSA, 2008). Research in industries that use cases has shown a correlation between productivity and work allocation (sometimes called case allocation or caseload). In the legal setting, a study indicated that the caseload has a direct and positive effect on court's productivity. (El Bialy, 2011). In social work, caseload is used as a productivity index. (Harvey, 1987). In the field of forensic science, much closer to DF, researchers have examined the effect of caseload on operational performance and productivity. (Venter, 2010). There is also research in forensic science on the efficient delivery of forensic science services (Maguire et al., 2012).

In IT, software developers have studied how to make task or work scheduling and resource allocation more efficient and have proposed several project management frameworks that covers work allocation to increase productivity (Monica et al., 2014). In software development, researchers have proposed the use of a task allocation optimizer (Duggan et al., 2004), a tool that supports human resource planning, monitoring and evaluation (Schnaider, 2003), a risk-driven model for work allocation (Lamersdorf et al., 2011), a queuing theory-based approach (Antoniol et al., 2001), and a fuzzy logic based system for human resource selection and evaluation (Ruskova, 2002). In the software development industry, such work allocation strategies are often the difference between success and failure. As Baretto et al. (2007, p. 3074) stated, "optimizing the allocation of available developers in accordance to the constraints imposed to (e.g., such as schedule deadline, project budget, and head-count) or by (maximum allocation, minimum effort to participate, among others) the development organization may determine whether a project will be profitable or not."

2.7.2. Case Allocation in DF

Unlike the other industries discussed above, a systematic review of DF literature shows that research into case allocation practices to increase efficiency or productivity in DF organisations has been limited. According to Barbara (2014), "finding the critical probative data faster in a cost-effective manner while reducing or eliminating case backlogs is going to require a more efficient methodology." Such methodology should include case, work or task allocation in a DF organisation. One of Barbara's proposals, for example, for streamlining workflow to create efficiencies is to "divide the evidence among multiple investigators for further analysis". In other words, Barbara proposes that case or work allocation among DF investigators affects performance. Barbara, however, does not go further, and does not delve into how work or case in DF organisation is to be allocated.

Minimal research exists that explores the techniques to optimize the complicated and timely process of case allocation (James, 2014). Likewise, DF guides or standards such as the ACPO Managers Guide: Good Practice and Advice Guide for Managers of e-Crime Investigation, regarded as the conclusive and best practice guide for computer forensics in the UK, while recognising the importance and complexity of productivity, do not address case allocation and productivity. The ACPO Managers Guide only states that "It is not the intention of this Guide to prescribe exactly how to increase productivity, as there are clearly a number of factors which can and do affect any method of trying to do so." (ACPO Managers Guide, 2011).

Without much guidance for DF managers, case allocation practices in DF have been ad hoc. While no study has been done to measure the effect of a lack of a case allocation strategy optimized for DF, research suggests that the lack of research into this area goes against the practice in other similar industries that have aimed for organisational efficiency. Because research in other similar industries have suggested a link between work allocation and productivity, it is very likely that creating case allocation strategies could improve DF organisational productivity and efficiency.

Due to the inexistence of research papers that explicitly talk about case assignment and management in DF departments or organisations, this section introduces different techniques used to delegate tasks in related work environments. It is known that good work allocation increases productivity in any work environment. Generally, in most work settings, individuals are not entirely free to select which activity to conduct as supervisors assign tasks to their employees (Athanasou & Van Esbroeck, 2008). Supervisors are reported to distribute tasks depending on the subordinate's skills, knowledge, and self-confidence both to increase their job satisfaction and improve their organizational commitment (Vinton, 1987). Supervisors usually pay more attention to delegating challenging tasks as such tasks represent greater risk for the superiors (Van de Vliert & Smith, 2004). To reduce the risk, supervisors usually intend to assign challenging tasks to those who are willing and able to perform well.

Supervisors have different delegation behaviours that mostly associate with the subordinate's job performance and their ambition. Habitually ambitious subordinates are more eager to perform challenging tasks (DeMers, 2014). Strategies include knowing when to delegate tasks and when to tackle them on their own, ensuring that people have a clear set of objectives for every task and making sure the employee is aware of his/her expectations while performing a delegated task. Supervisors need to increase the overall efficiency by taking advantage of the unique skill sets, unique preferences and unique talents that every co-worker has.

Managers use many management systems/tools to facilitate the process of work distribution among the subordinates and supervise their progress. Those systems are used in different work environments (Kumar et al., 2002). Examples of some of those management tools are Microsoft Project Management (Microsoft, 2017), Genius Project (Genius-Project, 2017), Wrike (Wrike, 2017), Smart Sheet (Smart-Sheet, 2017) and Project Management Cloud (Oracle, 2017). Those tools have different features but primarily provide the supervisors with workload management features, cross team collaboration, custom features, workflows, real time status updates, visual dashboards, reports and other features.

DF departments have been shown to use common project management tools and customise them to fulfil their main requirements, or to use the management tools built specifically for them such as Lima Forensic Case Management (Lima, 2017) or Sentinel Data (Atlas, 2017). These tools are particularly designed to simplify and consolidate the digital forensic case management processes. They provide features like global collaboration any case, unlimited client base, permanent case archives creation, chain of custody maintenance, complete exam documentation, assets management, full task management, forensic tools compatibility, local or remote browser access, consolidation of all case information, management of financial information, analysis of lab expenses, project expense accountability, invoice generation, high reporting standards, and process review facilitation. A lack of studies of practical implementation of cases assignment and management strategies would explain why there are no standardization and adaption of the management processes in the digital forensic departments/companies.

2.7.3. Organisational Workflow in DF

The researcher found limited discussions in the DF literature that covered the practical implementation of organisational workflow in the field of DF. This contrasts with the many models for crime scene and DF investigation processes, as discussed above, and coincides with the limited amount of research on the workflow of the DF investigation process. Much of the discussion on workflow in DF organisations deals with the DF investigation workflow, rather than organisational workflow (Mueller, 2013; de Braekt et al., 2016). While DF investigation workflow deals with the steps in the DF investigation process, an organisation's workflow may consist of "the set of processes it needs to accomplish, the set of people or other resources available to perform those processes, and the interactions among them" (Caine & Haque, 2008). In other words, organisational workflow is the interplay between people and process in order to increase productivity.

Research has found operational performance improvement due to the effective use of workflow systems. (Keung, 2000; Vanderfeesten & Reijers, 2005). Workflow systems also have the potential to positively change organisational culture by improving the organization's customer orientation, flexibility, quality focus, job satisfaction, and quality of business processes output. (Doherty & Perry, 2001; Keung, 2000).

While ISO (27037:2012) provides guidelines for handling the different processes of digital forensic investigation such as identification, collection, acquisition and preservation of potential digital evidence (ISO, 2012), and while these processes are well understood, few people have looked at the human processes that align to these activities.

Barbara (2014) proposed the concept of streamlining the workflow to deal with the challenges of Big Data in DF investigation. Barbara proposed streamlining the workflow by; (1) using a triage tool to identify the most likely evidence sources, (2) seamlessly exporting the work product into another tool to process the data and cross-reference the sources, (3) divide the evidence among multiple investigators for further analysis, and (4) export any relevant data found into reports. (Barbara, 2014). Barbara's discussion of streamlining the workflow in DF focused on the use of triage and upgrading DF tools, and not so much on work or case allocation among DF investigators. In other words, Barbara focused on the DF investigation process rather than creating efficiencies through organisational workflow. Importantly, however, is Barbara's suggestion of dividing the Number of Evidence Items among multiple investigators, a point that addresses one of the aims of this research, which is to determine the impact of DF case management strategies and organisational workflow implementation practices on Person-Hours.

Like Barbara, de Braekt et al. (2016) also proposed a way for streamlining workflow. However, de Braekt et al. only focused on the DF investigation and not on the organisational workflow.

There is also some literature on workflow in DF that focuses on the use of technology like NUIX and collaborative workflow (Jeffries & Jewell, 2015). Collaborative workflow discusses increasing efficiencies by adopting new workflows, increasing the number of people working on cases, getting information to DF investigator quicker, and bridging the gap between technical and non-technical DF practitioners. (Jeffries & Jewell, 2015).

Additionally, Grispos et al. (2017), recognising literature in DF that discuss the need to create a DF organisational structure that will align with DF efforts (Grobler & Louwrens, 2007), proposed the use of a workflow typology to create a forensics-enabled DF organisational structure. The workflow typology proposed, however, is geared toward the creation of an organisational structure rather than the creation of a more efficient and productive organisational workflow.

There has been no study, o date, that tries to identify the types of organisational workflow various DF organisations employ and to try to propose a way for DF managers to assess to adopt alternative workflows.

2.7.4. Case Management in DF

There are studies that claim that case management is a critical issue in investigation (James, 2014). Nevertheless, few offer solutions; Jones and Valli described the importance of standardized case prioritization, but they did not suggest how prioritization should be conducted (Jones & Valli, 2011). Likewise, Shaw and Browne (2013) discussed the concept of administrative triage using a matrix system that eliminates exhibits before conducting the actual forensic analysis using what they called a pre-analysis team but there is no amplification on the construction and use of this matrix.

James (2014) proposed a novel multi-stakeholder case prioritization method, which helps reduce risk to the organization adopting this method. His study focused on forensic investigation laboratories and he gave several examples of case categorization and prioritization in practice from several law enforcement organizations. He identified that different organizations use different methods of prioritization even if they are in the same country. James later highlighted the common challenges observed in case prioritization such as wasting resources and increasing stress within the organization because of not having an objective case prioritization model to pursue (James, 2014). Another challenge comes from higher-ranking officers pushing certain cases, which leads to a delay in other cases. James illustrated his proposed case prioritisation method which is made up of four main steps these being; categorizing crime types, identifying prioritization factors, determining the priority of factors, and assigning a weight to each factor to apply desired prioritization algorithm. This is quite a mathematical and stochastic solution to work allocation. Later, James suggested a prioritization formula by weighting factors and applying them on a scaling model. This work mainly highlighted case management challenges while many works focus on enhancing the investigation process. This work helps laboratories to learn and incorporate from others' experiences and implement it in their own organisation.

2.7.5. Proposed Solutions to Lengthy DF Investigations

A more human centred approach is to shift decision-making and autonomy to the investigators through improved DF case management and workflow implementation. However, the researcher has not found a study that proposes DF case management and workflow implementation as potential solutions to lengthy DF investigations.

Casey et al., (2013) studied the bottlenecks in the DF process and evaluated the complete forensic procedure (preparation, preservation/storage, extraction/survey, examination/analysis and reporting) before honing DF processes to develop tools that recognize the interconnectivity of the examiner tasks in the digital forensic lab. The work aimed to increase the overall efficiency and effectiveness of forensic examination.

Researchers have conducted many studies that aim to trim down the lengthy Person-Hours of investigation. James and Gladyshev (2013) conducted two studies aiming to reduce the time spent in investigation by eliminating a digital item from further investigation. Their first study was a survey of digital forensic examiners' investigation and decision process. They then studied the accuracy of decisions taken to exclude a digital item from receiving further in-depth analysis based on an enhanced preview. They found that DF investigators are not always conducting a complete in-depth analysis of each evidence item when the preliminary analysis reveals nothing. To exclude a digital evidence item, digital forensic examiners claim that the investigator requires high levels of training, education and experience. They do not trust the results from automated solutions, which do similar functions to exclude or to stop an evidence item from further analysis. However, the study was able to show that excluding a digital evidence item using enhanced preview could reduce the number of items to be fully analysed. They compared their findings to the outcome from manual examination of digital forensic items in order to strengthen their conclusions.

.8. Gaps in the Literature

After a review of the literature, the researcher identified the following gaps:

1. Researchers typically collected data on the challenges related to the increase of 3Vs in DF investigations. Specifically, Total Evidence Volume per Case and Variety (Heterogeneity of Evidence Items).
2. There exists a significant lack of research that use real cases and Databases from DF departments around the globe to identify trends related to the increase of large-scale investigations and predict the consequences of this phenomenon for practitioners.
3. Guidelines and best practices available for DF practitioners do not provide specific guidance for case allocation.
4. While researchers have introduced several models or frameworks for the DF investigation process, there has been a lack of proposals covering the DF case allocation process. Other industries, specifically IT and forensics sciences, have recognised the relationship between work allocation and productivity, but DF lacks strategies for case allocation to increase productivity.
5. While other industries have recognised the increase in operational performance due to efficient organisational workflow, research in the DF field has focused primarily on DF investigation workflow and has largely ignored organisational workflow. There has been no

study in DF that tries to identify the types of organisational workflow various DF organisations employ and to try to propose a way for DF managers to assess or adopt alternative workflows.

6. While there are studies that claim that case management is a critical issue in DF investigation, few offer solutions and no research has been done to identify and evaluate the types of case management strategies employed by DF organisations.

7. The proposed solutions to the challenges facing DF investigations focus on DF investigation, tools and techniques, but have not combined quantitative and qualitative methods to determine the relationship between productivity measured in Person-Hours and case management strategies and workflow implementation practices.

8. The researcher has not found any study that covers the practical implementation of case allocation in the field of DF.

CHAPTER 3: RESEARCH METHODOLOGY

3.1. Introduction

This chapter explains the research methodology implemented in this research to investigate the research aims and objectives, primarily the factors affecting digital forensic case management with a particular emphasis on the allocation and completion of DF cases and the causes for delay in DF investigations. The chapter follows a hierarchal structure of approaching the research methodology inspired by Pickard (2007), starting with the research paradigm, followed by the research methodology, then the research strategy, then the research method, and finally the research instruments. This chapter's approach adds research design between research methodology and research strategy. Almarzooqi (2016) used this hierarchical approach in a DF research. Figure 7 shows the hierarchical research methodology.

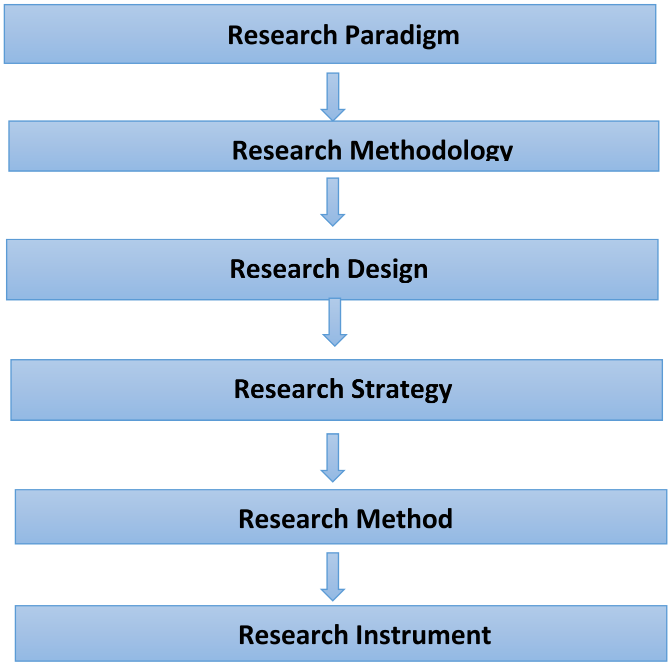


Figure 7. Hierarchy of Research Methodology.
Adapted from (Almarzooqi, 2016).

The chapter discusses and justifies the research paradigms and then discusses the types of research methodologies, including quantitative, qualitative and mixed methods research before setting out the factors to consider when choosing a methodology. After justifying the methodology applicable to the research at hand, the chapter then discusses the research design according to mixed methods research designs as outlined by Creswell (2014) and defends the choice of sequential explanatory design. Further, the chapter explains several research strategies, including case study, phenomenological, experimental, ethnographic, grounded theory, action research, and narrative research, and then provides justification for the chosen design and strategy applicable to the research. Finally, the chapter explains and justifies choices made for the data collection methods used.

3.2. Research Paradigm

A variety of research paradigms underlie information technology and information systems research (Clarke 2005). Each describes a basic set of beliefs about the world, or a philosophical worldview, that guides the researcher's actions and choices about the research and the gathering of information. Similar terms researchers have used to refer to a research paradigm (Mertens 1998; Lincoln & Guba, 2000; Clarke 2005) include epistemologies and ontologies (Crotty, 1998), broadly conceived research methodologies (Neumann, 2000), and philosophical worldview (Creswell, 2014).According to Kuhn (1970), a research paradigm is "the underlying assumptions and intellectual structure upon which research and development in a field of enquiry is based". Brewer (2001) defines paradigm as "a research culture", thereby influencing the choices a researcher makes about the research "question or hypotheses, research methods, and outcomes and interpretations." A paradigm is a way of simplifying or "breaking down the complexities of the real world" (Patton 1990). According to Orlikowski and Baroudi (1991), a researcher should base the research interests, aims, objectives, and assumptions on an appropriately chosen research paradigm. The research paradigm will later inform the researcher on whether to pursue quantitative, qualitative, or mixed methods research (Creswell, 2014). The traditional research paradigms are positivist, interpretive and critical (Orlikowski and Baroudi, 1991; Almarzooqi,2016). Whether as a reaction to, or as a refinement of, traditional research paradigms, additional paradigms or philosophical worldviews have since emerged, namely post-positivist, constructivist, and pragmatic (Creswell, 2014; Guba & Lincoln, 1994). This section will briefly discuss each of these paradigms and explain the justification for choosing pragmatism as a paradigm for this work.

3.2.1. Positivism

Positivism has been a leading research paradigm under the scientific method for several centuries (Oates, 2006; O'Brien, 2001). Ontologically speaking, positivists are realists, and assume a separation between the researcher and reality (Stahl 2008). Concerning knowledge or theory of knowledge, positivists assume that an objective reality exists beyond the human mind, believing in an objective reality that independent observation can directly verify through logic and empirical testing (Choudrie and Dwivedi, 2005). Positivists assume that objects of the research or phenomena have qualities subject to natural laws and that these are independent of the researcher. The research methods positivists use include laboratory experiments, surveys, and field studies that usually involve large data sets analysed statistically to detect existing regulations (Choudrie and Dwivedi, 2005). Because positivists use precise empirical observations (Neumann, 2011), they view data collection as a true measure of reality, thereby making the data valid, if internal and external validity checks are in place such as construct validity and statistical significance. Through inductive and deductive reasoning, positivists aim to discover and confirm a set of probabilistic causal rules or laws about human activity from these quantitative data, derived through mathematically determined statistical relationships. (Oates, 2006; Neumann, 2011). In so doing, positivists determine the reliability of the research outcomes based on the repeated consistent and accurate results over time, especially when verified by others. The strength of positivism is its ability to minimise bias and increase reliability through large sampling (Gable, 1994; Chen and Hirschheim, 2004). However, researchers criticise positivism for ignoring historical, cultural, social, political, and contextual factors that shed light on quantitative data. (Orlikowski and Baroudi, 1991; Neuman, 2006; Collis and Hussy, 2003).

3.2.2. Interpretivism

Unlike positivism, interpretivist or social constructivism focuses on the influence society, history, culture, politics, economics, and context have on language and concepts (Creswell, 2014; Guo and Sheffield, 2008). Ontologically speaking, interpretivists are relativists and believe in multiple constructive realities that cannot exist outside the social world that creates them. (Pickard, 2013). They assume that the researcher is inseparable from reality (Stahl 2008). Interpretivists assume that a researcher intentionally builds knowledge through lived experiences or social constructs about the world in which knowledge and reality are social and language constructs (Almarzooqi, 2016; Guo and Sheffield, 2008). However, the researcher must remain objective like a passive collector interpreting subjective data (O'Brien, 2001). Interpretivists prefer a direct, natural, and detailed observation of the human environment to better understand and interpret "how people create and maintain their social world" (Neuman, 2011, p.102; Saunders et al., 2003), rather than through quantitative and mathematical methods. The research methods interpretivists employ include case studies, ethnographic studies, hermeneutics, grounded theory, participant observation, ethnomethodological studies, and phenomenology to analyse indirect meanings and uncover hidden ones (Choudrie and Dwivedi, 2005). In terms of validation, interpretivists focus on the defensibility of the knowledge acquired, and assume that the researcher must produce evidence to support any claims the researcher makes. Interpretivists consider the process and the research context when determining the validity of the knowledge the researcher claims. A researcher establishes reliability by demonstrating interpretive awareness. Researchers have criticised interpretivists for making over generalisations that lack a wider sampling of a population and by ignoring historical changes as date may evidence over time. (Orlikowski and Baroudi, 1991).

3.2.3. Critical/Advocacy/Participatory

Ontologically, a critical, advocacy, or participatory paradigm, follows historical realism, where social, political, cultural, economic, ethnic, and gender values shape reality (Guba & Lincoln, 1994). Epistemologically speaking, critical paradigm is transactional and subjectivist. There is an interactive link between the researcher and the research object, with the values of the researcher inevitably influencing the inquiry (Guba & Lincoln, 1994).

Critical paradigm is evaluative, critical, and aims to change the social reality of the research subject. (Choudrie and Dwivedi, 2005; Orlikowski and Baroudi, 1991). Because critical paradigm is transactional, there must be dialogue between the researcher and the research subject, and the dialogue is dialectic in nature with the aim of criticising and changing relationships, conflicts, and contradictions that the researcher views as restrictive and alienating. (Myers, 1997; Guba & Lincoln, 1994; Oates, 2006). Critical paradigm is often associated with action research.

3.2.4. Post positivism

Post positivism is an extension of positivism, through challenging the positivists' traditional notion of absolute truth and knowledge. (Creswell, 2014; Phillips & Burbules, 20000). Unlike the traditional realism of positivists, post positivists are critical realists, and claim that a researcher must subject reality to the widest possible critical examination to have the closest possible understanding (Guba & Lincoln, 1994; Cook & Campbell, 1979). Still, post positivists hold a deterministic philosophy where causes probably determine outcomes. (Creswell, 2014). Post positivists abandon strict dualism but maintain objectivity as an ideal. Post positivists go beyond quantitative methods, and increasingly employ qualitative methods in their inquiry, even contributing to grounded theory (Strauss & Corbin, 1990). They follow a modified experimental methodology, with the aims of falsifying rather than verifying a hypothesis (Guba & Lincoln, 1994).

3.2.5. Constructivism

Constructivists view reality as individual or group constructions that may be understood in a social or experiential setting in the form of multiple, intangible mental constructions (Guba & Lincoln, 1994). Individuals develop subjective meanings, the complexity of which only the individual can construct (Creswell, 2014). Constructivists view reality as alterable, not measured by truth but by the extent to which the construction is informed (Guba & Lincoln, 1994). Like critical theorists, constructivists are transactional and subjectivist, and assume an interactive link between the researcher and the research object. Constructivists believe that researcher can better understand and refine constructions through interactions with the respondents, using broad, general, and open-ended questions (Creswell, 2014; Guba & Lincoln, 1994). Constructivists aim to make sense of the meaning or constructions respondents have about the world, and then interpret the constructions using hermeneutical and dialectic techniques. Through the process, constructivists develop a theory or pattern of meaning, and the outcome is a consensual construction that becomes more sophisticated than the previous construction.

3.2.6. Pragmatism

Pragmatists do not subscribe to only one philosophical worldview. Instead, pragmatists are concerned with solutions to problems, wanting to know what works best and what does not (Creswell, 2014). Pragmatists use all approaches available to understand and find solutions to a problem, rather than focusing on the process and methods (Patton, 1990; Rossman & Wilson, 1985; Creswell, 2014). Pragmatists posit that the value of any given research methodology is based solely on its empirical and practical efficacy (Johnson & Onwuegbuzie, 2004). However, like interpretivists, pragmatists view research as occurring in social, historical, political, and other contexts.

Pragmatism allows the researcher to focus on the research problem, and then use pluralistic approaches to understand the problem and arrive at solutions. Pragmatism, therefore, is best suited for mixed method research, where the researcher may employ both quantitative and qualitative methodologies because the use of both provides the best path to understanding the problem. (Creswell, 2014). In addition, pragmatism gives the researcher freedom to design the research, including the methods, techniques, and procedures.

3.2.7. Justification for Research Paradigm

At first glance, the positivists and post positivists' use of quantitative methods seem the most applicable to the research's aim of determining the effects, like DF investigation delay and lengthy Person-Hours, of increasingly voluminous and heterogeneous digital data and sources of such data – the cause. In this regard, the research does take on a post positivist, though not a strict positivist, worldview in some aspects of the research. However, engaging in the inquiry through the limited lens of post positivism would ignore a key component of the research: an inquiry into DF organisations, the people involved in such undertakings, and the various DF environments. In other words, this research is not only about the verification (positivists) or about the falsification (post positivists) of reality through quantitative methodology; quantitative secondary data from Dubai Police is certainly an essential element of the research to create a robust basis for later conjecture. However, the research must also consider the historical, cultural, social, political, and contextual nature of the DF work environment. The research is also about case management strategies and workflow implementation practices which all relate to actions and decisions of people within a given environment.

In this sense, the research also engages in an interpretivist paradigm. The interpretive paradigm, according to Almarzooqi (2016), is appropriate in a research in DF and DF organisations because the practice of DF deals mostly with a system composed of people's interactions with information or data, which is social in nature. For this reason, qualitative research's focus on social interactions has made it compatible with research in the field of information technology (Fernandez, 2004; Almarzooqi, 2016). Research methods followed by interpretivists like case studies, grounded theory, and phenomenology would certainly add depth to the quantitative secondary data from the Dubai Police Database. The research must, therefore, be engaged in the interpretivist methodology of direct, natural, and detailed observation of the DF work environment to better understand and interpret the causes of delay in DF investigations and increase in Person-Hours. The research aims to indicate if Total Evidence Volume per Case and Heterogeneity of Evidence Items per Case causes delay in DF investigation process. Since the researcher values quantitative data from the Dubai Police Database, the interpretivist paradigm alone would be insufficient.

Certainly, the critical paradigm is inapplicable to the research at hand because the researcher here does not aim to change how DF investigators and DF managers view their reality and relationships. For the same reason, constructivism is inapplicable because constructivism follows a transactional and dialectical approach like the critical paradigm, aiming to understand and refine, along the process, the respondents' constructions of meaning. The objective of this research is not to refine the meanings DF investigators or managers have about the world and the DF work environment. Rather, the researcher will remain objective as consistent with post positivism and interpretivist.

Having considered the above, the most suitable paradigm to the research problem is pragmatism. The research problem requires inquiries into both quantitative and qualitative data. Quantitative data is necessary to establish the causal relationship between Total Evidence Volume per Case/ Heterogeneity of Evidence Items per Case and lengthy DF investigation process using secondary data provided from the Dubai Police Database. The use of the quantitative data is one of the strengths of the research, making it unique among existing research that aim to tackle the challenges posed by Big Data. Likewise, qualitative data is necessary to discover other potential factors that may substantially affect DF investigation delay and lengthy Person-Hours. Qualitative data will give a valuable window into the historical, cultural, social, political, and contextual nature of the DF work environment.

The differences in the choice of paradigm, according to Weber (2004), truly lie in the choice of research methods, which may be determined by a variety of factors such as the researcher's training, recommendation from faculty or peers, pressure from advisors or colleagues, time, money, and so on. In this instance, however, the research problem itself is the primary driver in choosing the pragmatist paradigm. The research focuses on understanding a problem in DF investigations and DF case management that has remained elusive despite proposed solutions. The failures of the other research paradigms to provide the optimal means for understanding the problem posed in this research make the pragmatist paradigm most suitable for the research at hand. Following Pickard's hierarchical structure, the chapter next examines the research methodologies.

3.3. Research Methodologies

A research methodology is a scientifically accepted approach to collect, interpret and analyse a set of data. There are generally three types of research methodologies: quantitative research, qualitative research, and mixed methods research.

3.3.1. Quantitative Research

Quantitative research aims to use numerical data to create generalizable results or confirm a theory (Reinard, 1998). Quantitative research includes the use of deductive reasoning, large random samples, the use of formal instruments, and the collection and analysis of numerical data (Reinard, 1998; Patten 1997). Quantitative research employs standardized data collection methods, such as closed ended questionnaires and structured interviews, and the data is interpreted using statistical analysis. There exists an assumption in quantitative research that a researcher can isolate and thereby examine variables within a research problem, while other variables remain intact (Salomon, 1987; Brewer, 2001).

3.3.2. Qualitative Research

Qualitative research focuses on describing, interpreting, and evaluating complex social environments with the aim of answering questions or a set of questions to develop new insights or theories about human experiences or a phenomenon (Leedy, 2005). According to Brewer (2001), qualitative research is “interested in how people interpret their own experiences” in a social world.

Qualitative data could derive from published documents, interviews, and observations, but the researcher is the primary instrument in data collecting and theory building. Therefore, “qualitative researchers tend to spend a great deal of time in the settings they study” (Gay & Airasian, 2000, p.19), and in face-to-face interaction with respondents (Brewer, 2001). Qualitative research uses techniques like in-depth interviews, semi-structured interviews, ethnographic studies, historical research, phenomenology, grounded theory, and focus groups to arrive at findings that are not determined in advance, and that the researcher must discover, explore, and induce throughout the process. (Cohen et al., 2011; LoBiondo-Wood & Haber, 1998). According to Fraenkel and Wallen (1996), qualitative research characteristics may include the following: (1) use of evolving definitions, (2) use of inductive reasoning, (3) use of narrative data, (4) assumes the reliability of inferences, (5) use of purposive sampling, (6) imprecise discussion of procedures, and (7) narrative discussion of results.

3.3.3. Mixed Methods Research

Mixed methods research is "research in which the investigator collects and analyses data, integrates the findings, and draws inferences using both qualitative and quantitative approaches and methods in a single study or program of inquiry" (Tashakkori and Creswell, 2007). A simpler proffered definition of mixed methods research states that it is a "type of research in which a researcher…combines elements of qualitative and quantitative research approaches" (Johnson et al. 2007).

Campbell and Fiske (1959) were probably the first to mix research methodologies when they used multiple methods in a study of psychological trait validity (Creswell, 2003). Since then, researchers have come to recognize the value of mixing both quantitative and qualitative research. Mixed methods are not new to the information systems/information technology (IS/IT) field. Several IS/IT researchers have used mixed methods (Peng et al., 2011; Arpaci et al., 2015; Peng & Annansingh, 2015; Wu, 2012). In the field of DF, Pooe and Labuschagne (2013) and Altiero (2015) are examples of researchers who have used mixed methods research to tackle DF forensics research problems.

According to Pooe and Labuschagne (2013), there is a philosophical assumption that gives direction to a mixed methods research. In the research at hand, the author has explained her philosophical worldview as the pragmatist paradigm. Mixed methods have been formally linked to pragmatism (Tashakkori & Teddlie, 2003).

An advantage of mixed methods research is that the combination of quantitative and qualitative research in a single or series of studies offers a better understanding of the research problem than each method on its own (Pooe & Labuschagne, 2013). For instance, mixed methods may use both deductive and inductive reasoning. Further, the researcher can understand the strengths and weaknesses of both quantitative and qualitative research, and thereafter combine strengths and non-overlapping weaknesses (Johnson and Turner, 2003). According to Mertens (2003) and Punch (1998), a researcher may use mixed methods to arrive at a better understanding of the research problem through the convergence of numeric trends from quantitative data and specific details from qualitative data. Mixed methods may even uncover the need for further study, confirm hypotheses, and add texture (Brewer, 2001).

Green et al. (1989) suggested four reasons to justify the researcher's combination of quantitative and qualitative research: (1) to complement, (2) to develop, (3) to initiate, and

(4) to expand. The rationale for mixing is to complement when the researcher uses results from one method to elaborate on results from the other method. This complementarity of results can be a positive outcome for mixed methods research (Brewer, 2001; Green et al., 1989). The rationale is to develop when the researcher uses results from one method to inform the other method. In sequential design, mixed methods may even reveal the development of a phenomenon under inquiry. (Brewer, 2001). The rationale is to initiate when the researcher recasts results from one method to questions or results from the other method. Finally, the rationale is to expand when the researcher extends the range of inquiry by using different methods for different inquiry components. In other words, the results of mixed methods research increase the researcher's scope of knowledge about the research problem (Brewer, 2001; Creswell, 1994).

There are certainly disadvantages to mixed method research, namely its complexity, that it is time consuming, and in using it, the researcher may find it difficult to avoid bias, especially when the researcher has examined the quantitative data prior to the qualitative research. Although a mixed methods research will likely be more time consuming than a mono-methodological research, mixed methods research will likely produce a richer set of data. Data acquired through qualitative research could provide baseline information and help avoid bias (Brewer, 2001), while qualitative research could help the researcher assess the quantitative data and offer a new perspective on the research problem.

3.3.4. Justification for Mixed Method Research

This research adopts a mixed method approach to understand better the research problem consistent with the pragmatist paradigm of the research. Under the pragmatist paradigm discussed above, researchers should choose methods that offer the best opportunities for answering the research question under investigation (Trahan & Stewart, 2013). Mixed methods are best suited under the pragmatist paradigm (Creswell, 2014).

According to Creswell (2003, p. 22), "a mixed methods design is useful to capture the best of both quantitative and qualitative approaches." The research problem and personal experience play into the decision on whether to use both quantitative and qualitative research. (Creswell, 2003). The research problem should be the primary driver in the decision to apply mixed methods research. The collection and analysis of both quantitative and qualitative data prove advantageous in arriving at a better understanding of a research problem (Creswell, 2003). Though not as common, researchers in IS/IT and even the DF field have used mixed methods research when appropriate to the research problem.

In this case, the decision to use mixed methods was primarily to understand better the research problem. The research problem requires an analysis of quantitative secondary data, such as Person-Hours spent in DF investigations, to test the hypothesis that the Total Evidence Volume per Case and Heterogeneity of Evidence Items per Case are the likely causes of DF investigation delay and lengthy Person-Hours. In other words, the researcher wanted to isolate variables like Person-Hours to understand the research problem. However, the research also required analysis of the human, technological, and resources-based factors behind the problem, especially as the research wanted to look into the case management and case allocation aspects of a DF organisation. The second aspect required a qualitative approach to the problem so that the researcher can analyse the complexities of the DF work environment that may contribute to DF case management strategies and workflow implementation practices. The solution was to use both quantitative and qualitative studies to understand better the research problem.

The research problem itself arose from the author's personal experience working at Dubai Police. The author's access to the Dubai Police Database gave the author a unique opportunity to analyse quantitatively the factors influencing lengthy Person-Hours, delay in DF investigations, and DF cases backlogs. These phenomena have been the target of other studies in DF, but most prior researchers did not base their studies on quantitative data, but rather largely on qualitative data. As such, the researcher was prompted to begin the study with a quantitative analysis of secondary data from the Dubai Police Database, and to later complement, develop, initiate, or expand the result of the quantitative data with the result of the qualitative data. In so doing, the author benefited from the mixed method research by increasing the author's scope and understanding of the research problem – that there were other factors involved other than the Total Evidence Volume per Case.

While the author does not regret having used the mixed method approach, the author must note, for the sake of future researchers, that the one primary disadvantage of mixed methods research is that it is time consuming.

3.4. Mixed Methods Research Design Strategies

After choosing mixed methods research, it is essential to explain and justify the mixed method design strategy for the research. Since mixed methods uses both quantitative and qualitative research, the researcher must decide whether to present the studies sequentially, in what order, or concurrently. There is no single design for a mixed methods research (Pickard, 2013; Johnson & Onwuegbuzie, 2004). For example, quantitative research may be undertaken first, followed by qualitative research, or vice versa (Creswell, 1995; Flick, 2011). While there may be more than forty different mixed methods designs (Tashakkori & Teddlie, 2003), Creswell's six methods are the most commonly used in mixed methods research. (Ivankova et al., 2006; Peng et al, 2011). Creswell (2003) proposed six mixed methods design: (1) sequential explanatory, (2) sequential exploratory, (3) sequential transformative design, (4) concurrent triangulation design, (5) concurrent nested (embedded) design, and (6) concurrent transformative design.

3.4.1. Sequential Explanatory Design

Sequential explanatory design consists of two distinct phases of data collection, where the researcher first collects, and analyses, quantitative data followed by qualitative data collection and analysis. (Peng et al, 2011). The design gives priority to the qualitative portion. The purpose of the design is to use the qualitative results to further explain and interpret the findings from the initial quantitative phase. For example, a researcher may first conduct a survey to collect a large set of quantitative data, followed by the collection of qualitative data by interviewing selected survey participants, who can give detail and further insight into the survey answers.

There are two subtypes of the sequential explanatory design: the follow-up explanation model and the participation selection model (Creswell & Clark, 2007). In the follow up explanation model, the research uses the qualitative data to explain or expand the quantitative data. In the participation selection model, the researcher uses quantitative data to identify and purposefully select participants for a follow up, in-depth qualitative study.

3.4.2. Sequential Exploratory Design

Sequential exploratory design consists of two distinct phases of data collection as well, but the collection of quantitative and qualitative data is reversed from sequential explanatory design. Qualitative data precedes quantitative data collection and analysis, with priority given to the initial qualitative research. The aim is to increase the generalisability of the findings in order to develop a later instrument to develop a classification for testing, or to identify variables (Peng et al, 2011). Researchers, for example, may use qualitative data from journals or diaries to develop a survey design to administer to a larger population.

3.4.3. Sequential Transformative Design

Sequential transformative design also consists of two distinct phases of data collection, but the researcher may give priority to either qualitative or quantitative research, or even to both concurrently, given enough resources (Peng et al, 2011). The theoretical perspective of the researcher may guide the study and determine the order of the data collection. At the end of data collection, the researcher integrates the results of both qualitative and quantitative research with the interpretation phase.

3.4.4. Concurrent Triangulation Design

The most common and well-known mixed method design is triangulation. (Creswell, Plano Clark et al, 2003). In concurrent triangulation, the researcher concurrently or simultaneously collects qualitative and quantitative data in one phase, giving either type equal priority or importance. The researcher analyses the results of the data collection separately, where the researcher compares and/or combines the results in order to confirm, cross-validate, or corroborate the findings within the same single study (Peng et al, 2011). The use of both qualitative and quantitative research aims to overcome the weaknesses in one method with the strengths inherent in the other method. A researcher, for example, may collect experimental data and interview data concurrently and thereafter compare the results.

3.4.5. Concurrent Nested (Embedded) Design

Concurrent nested design consists of one phase of data collection, where the researcher collects quantitative and qualitative data simultaneously or concurrently. The research, however, gives priority to one method that guides the research while the researcher embeds or nests the other supporting method within the predominant method (Peng et al, 2011). The supporting method will address a different question than the predominant method, which addresses the main research question. The design may also aim to discover information at different levels.

3.4.6. Concurrent Transformative Design

Concurrent transformative design consists of one phase of data collection. The design combines the best features of concurrent triangulation and concurrent nested designs (Peng et al, 2011). The researcher collects quantitative and qualitative data concurrently or simultaneously, guided by the researcher’s theoretical perspective on the research question or purpose of the research. The researcher aims to evaluate the theoretical perspective at various levels of analysis. The researcher may use triangulation of equally important quantitative and qualitative data results. The researcher may additionally embed or nest a supplemental method to explore further the research with a separate question.

3.4.7. Justification for Research Design

One design is not necessarily better than other designs, and the researcher’s selection of the design should depend on the research question and the research context the researcher aims to investigate. (Peng et al, 2011). Creswell and Clark (2007) identified three factors a researcher must consider when deciding which mixed methods research design to apply: timing decision, weighing decision, and mixing decision. When considering these three factors, it becomes apparent that the sequential explanatory design is most applicable to the current research.

This current research does not use any of the concurrent designs since the researcher does not conduct the quantitative and qualitative data collection simultaneously. In other words, concerning timing, the design must be sequential.

In terms of weighing, the research prioritizes the quantitative data, which thereafter drives the qualitative research. In terms of mixing, the secondary data from the initial quantitative research connects to the qualitative research data. Further, the purpose of the research is not to explore variables related to the delay of DF investigations or long Person-Hours. Instead, the research focuses on the variables of Big Data, mainly volume and variety, as they affect DF investigation. Therefore, the research does not begin with a qualitative data collection and is therefore not a sequential exploratory design. It is also not a sequential transformative design because the theoretical perspective does not drive the research. Rather, the research problem drives the theoretical perspective since the aim of pragmatism is to use any approaches to find solutions to the research problem, and not the other way around.

Therefore, this research uses the sequential explanatory approach; qualitative research (personal experience) follows the initial quantitative research (numerical) (Creswell, 2013). The purpose of the two-phase explanatory design is for the second qualitative method to help develop, inform, contextualise, and analyse the first quantitative method. (Creswell, Plano-Clark, Gutmann and Hanson, 2003). Qualitative data can also enhance and enrich the findings (Taylor and Trumbull, 2005; Mason, 2006), and help generate new knowledge (Stange, 2006). Sequential explanatory design has been used in IS/IT organisation research (Arpaci et al, 2015).

Such a design became evident in this research after the first method resulted in findings that contradicted the assumptions behind and revealed that the Total Evidence Volume per Case was not the only factor that caused DF investigation delay or lengthy Person-Hours. Quantitative methods became insufficient for measuring the other factors as they related to the interactions of people and phenomena in the DF environment, including such aspects as case management, case allocation, case completion, DF investigator training, and resource needs of the DF organisation.

A sequential explanatory design is appropriate for this study because the latter qualitative studies helped the researcher explore details that were lacking in the first quantitative study. In other words, the qualitative data helped the researcher better understand

and interpret the quantitative data, and therefore the research problem at large. An analysis of quantitative data in the first study helped determine that later interviews had to involve case managers from the same and other organisations, to determine whether the results of the quantitative studies applied in other organisations as well. The follow up interviews provided more insights about the role of various factors in DF case management strategies and workflow implementation practices.

3.5. Research Strategy

The research strategy is the researcher's approach to answering the questions and aims of the research (Saunders et al., 2003; Robson, 2002). In the field of DF, researchers have used the following various types of research strategies: case study, phenomenology, experiment, survey, ethnography, grounded theory, action research, and narrative research (Almarzooqi, 2016; Johansen & Perjons, 2014). After explaining the various types of research strategies, the researcher provides justifications for adopting the case study and phenomenological research strategies.

3.5.1. Case Study

According to Creswell (2014), a researcher engages in a case study through an in-depth exploration of a program, phenomenon, event, activity, process, or one or more individuals to find underlying principles. A case study is suitable for collecting descriptive data (Powell & Connaway, 2004). A researcher uses a case study, according to Pickard (2007), to develop an in-depth analysis of a single case by visiting a case site multiple times at regular intervals. A case study provides "a holistic account of the case and in-depth knowledge of the specific through rich description situated in context" (Pickard, 2007, p.86). According to Stake (1995), the researcher collects detailed information using a variety of data collection procedures. Case study data largely comes from documents, archival records, interviews, direct observations, participant observation and physical artefacts (Yin, 1994).

There are three types of case studies: intrinsic, instrumental, or collective. (Pickard, 2007). An intrinsic case study aims to acquire a deeper understanding of an individual case, an instrumental case study focuses on a phenomenon, and a collective case study combines both intrinsic and instrumental approaches to investigate a phenomenon through multiple cases.

In research relating to an organisation, a case study allows the researcher to identify common or unique organisational features, or the interaction and influence of processes on the organisation's functions (Bell, 2005). The researcher can then make cross-contextual generalisations where the findings of the cases study will be relevant and transferable to similar contexts and organisations (Mason, 2002).

3.5.2. Phenomenological Approach

Edmund Husserl first introduced phenomenological research (Husserl, 1970). The German philosopher focused on personal experience. In phenomenological research, the participants in the study describe rather than explain the essence of human experience concerning the studied phenomenon (Creswell, 2003).

Van Manen (1990, p.9-10) described the phenomenological approach as "a deeper understanding of the nature or meaning of our everyday experiences". The researcher aims to understand the “lived experiences” of individuals related to a specific phenomenon by studying a small number of subjects to develop patterns and relationships of meaning (Moustakas, 1994; Creswell, 2003; Creswell 2007). In phenomenological research, the researcher aims for descriptive answers to the research questions by conducting interviews or observations of participants closest to the phenomenon (Davison, 2014). The researcher can use a variety of methods ncluding interviews, conversations, participant observation, action research, focus meetings, and analysis of personal texts. The researcher uses the phenomenology for analysing the collected records, and then develops a composite description of the phenomenon (Davison, 2014).

Usually, the phenomenological approach is discovery oriented rather than hypothesis proving or theory testing (Giorgi, 1986). This type of research starts with perspectives that are free from hypotheses. It is important to start the research without preconceptions or bias.

3.5.2.1. Phenomenological Reduction and Epoché

As such, phenomenological research involves the use of epoché and phenomenological reduction (Appendix 1). In epoché, a Greek word used by Husserl, the researcher is to stay away, or abstain, from presupposition or judgments about the phenomena under investigation (Langdridge, 2007; Moustakas, 1994). In phenomenological reduction, the researcher suspends judgment about the existence, or non-existence, of the natural external world in order to focus on analysis of experience. The task in phenomenological reduction is to describe individual experiences through textural language. Researchers are required to consider the external object related to their perception when describing what they see (Moustakas, 1994). In other words, the researcher must aim to remove theory from the description of the phenomenon, or to bracket perceived notions and prejudices.

3.5.2.2. Imaginative Variation

Phenomenology also involves the use of imaginative variation, a phenomenological analysis process that follows phenomenological reduction and depends purely on the researchers' imagination rather than on empirical data. The researcher drives structural themes through the imaginative variation process. According to Moustakas (1994, p. 85), imaginative variation requires the researcher "to seek possible meaning through the utilization of imagination, varying the frames of reference, employing polarities and reversals' and approaching the phenomenon from divergent perspectives, different positions, roles, or functions." The imaginative variation process aims to remove unnecessary features by finding a possible meaning of the phenomenon and asking question about the phenomenon (Beech, 1999). The process continues until the shared meaning of the phenomenon of interest is found (Streubert & Carpenter, 1995).

3.5.2.3. Individual Textural and Structural Description

Textural and structural description is the process of writing the experiences of individual participants in relation to the subject being investigated. The textural description gives the "what" of the experience, and the structural description gives the "how" of the experience.

3.5.2.4. Composite Textural and Structural Description

In this stage of the data analyses, each individual experience will be represented in the composite textural and structural descriptions.

3.5.2.5. Synthesis

Synthesis is the process of combining the textural and the structural descriptions into the essences of the phenomenon. The accuracy of the findings is substantiated by revisiting the raw data descriptions to justify the understanding of both the essential meanings and the general structure.

3.5.3. Experiment

Experiments, as a part of any research strategy, include both true experiments and quasi-experiments (Creswell, 2003). True experiments use a random assignment of subjects to treatment conditions while quasi-experiments use nonrandomized designs, including single-subject designs (Keppel, 1991). In the experiment method, the researcher studies an existing theory to make a prediction, designs an experiment to test the prediction, and then observes the experiment. The researcher, thereafter, can use the experiment's results to modify a theory.

3.5.4. Ethnography

In the ethnographic method, the researcher studies or observes the behaviour or culture of people, or an intact cultural group, in a natural setting. Ethnography allows a researcher to examine complex cultural phenomena. The researcher primarily collects observational data over a prolonged period (Creswell, 2003). In the IS/IT field, researchers have used this method to observe human interaction with systems or technologies. Ethnography is flexible, and usually evolves contextually as the researcher responds to the lived realities encountered in the field setting. (LeCompte & Schensul, 1999).

3.5.5. Grounded Theory

In grounded theory, the researcher aims to generate, or discover, a general, abstract theory of a process, action, or interaction (Glaser & Strauss, 1967; Creswell, 2003). The researcher must ground the theory in the views of the participants in the research based on an analysis of the data. According to Martin and Turner (1986), grounded theory is "an inductive, theory discovery methodology that allows the researcher to develop a theoretical account of the general features of a topic while simultaneously grounding the account in empirical observations or data."

Grounded theory involves multiple stages of data collection. The researcher must select data, use theoretical sampling of data to maximise similarities and differences, and then group and code data into categories of information (Strauss & Corbin, 1990). There must be a constant comparison of data with emerging categories. When grouping data into categories, the researcher must identify categories from the data, build relationships between categories, and group the categories further into theoretical constructs. Primary data collection methods for grounded theory are interviews, observation and document analysis. The data collected is typically large, making it difficult to manage the data.

3.5.6. Action Research

Action research involves a loop or circular process. It is an iterative research methodology, which starts with the researcher defining the problem, taking steps to resolve the problem, and then carrying out an evaluation of the results. The process then restarts and continues until the researcher achieves a satisfactory result (O'Brien, 2001). In the information security field, the action research process has been described as the planning of an intervention, carrying it out, analysing the results of the intervention, and reflecting on the lessons learned that might contribute to the redesign of the social action, and the planning of a new intervention (Faily, & Fléchais, 2011). The process for action research requires the researcher to learn by engaging in the experiment.

3.5.7. Narrative Research

In narrative researcher, the researcher studies the life or experience of one or more individuals through life stories, biographical data, text and semantic field analysis, or the reconstruction of the individual's life story (Creswell, 2003). The researcher retells the narrative information into a collaborative narrative chronology that ultimately combines the views from the participant's life with those of the researcher's life (Clandinin & Connelly, 2000; Creswell, 2003).

3.5.8. Justification for Research Strategy

A researcher should consider the questions and aims of the research before choosing the appropriate research strategy (Sekaran, 2003). The researcher conducted a mixed method sequential explanatory research that met the needs of the research.

In the first study, the researcher uses existing secondary data, applying statistical analysis and secondary data analysis to the quantitative data obtained from the Dubai Police Database, as consistent with quantitative research. The next section further discusses the use of secondary data.

The research employs the phenomenological approach (transcendental phenomenology) in Study Two (Interviews with DF managers). The phenomenological approach fits well with the objectives of this research. This qualitative approach allowed the researcher to gain a deeper understanding of the tasks that the decision makers enact in their everyday routines. This also helped the researcher to identify the common factors behind the decision of assigning the cases in a DF department or organisation. The phenomenological approach also helped to identify a list of common-sense decision influences. This study emphasized the experiences of decision makers around the world in managing the digital forensic departments/companies.

This research also follows an approach where the focus is on specific phenomena – case management strategies employed by DF organisations, workflow implementation practices, and the solutions used by these DF organisations to overcome lengthy Person-Hours. In this study, the data collection method employed was archival data, semi-structured interviews and semi-structured email interviews. The research looked at archival data of the Dubai Police through their Database to get a better understanding of the individual case of the Dubai Police. Afterwards, the researcher conducted semi-structured interviews with various DF organisation case managers, and semi-structured email interviews of selected participants of the prior interview.

Ethnographic research was not the most applicable method for the research. While ethnography could give valuable insight into the human interaction with DF systems and technology, the current research does not focus on the cultural aspects of the DF work environment or its work culture. Rather, the current research examines the cause and effect of DF investigation and case management.

Action research is not applicable in the current research because the researcher does not aim to find a solution to the challenges posed by Big Data to DF investigations, by engaging in DF investigations in order to resolve the problem. Such a herculean task would be impossible involving Big Data and designing such an experiment to understand the impact of Big Data on DF investigation delay and case management would be quite different from starting with an analysis of the Dubai Police Database.

Likewise, narrative research is largely inapplicable to the research at hand because this research is not interested in the life stories of DF investigators or DF case managers, but rather at the effect of external factors like Total Evidence Volume per Case and Heterogeneity of Evidence Items per Case. The personal stories of the individuals involved are largely irrelevant without data pointing to their relevancy as a factor. The research did not show any data indicating the existence in the personal life stories of individuals involved that become a significant factor in determining DF case management and DF investigation delay.

3.6. Data Collection Methods

This section discusses the difference between quantitative and qualitative data collection methods, and the difference between primary and secondary data collection. Then, the section discusses the various types of data collection methods before discussing the justification for the data collection methods used in this research.

3.6.1. Quantitative and Qualitative Data Collection Methods

Since the research is mixed methods, it is necessary to discuss data in terms of its origin and quantitative and qualitative data collection methods. This section considers types of data as well as the classic means by which data is gathered and collected.

3.6.2. Primary and Secondary Data

Primary data is data that a researcher collects directly from individuals, objects or processes. It is data collected for a specific research goal (Hox & Boeije, 2005). A researcher may collect primary data in both quantitative and qualitative research. The advantages of primary data collection are that the researcher has already tailored the research question and procedure to fit the research problem and the researcher controls the collection of the data, adding to its reliability.

Secondary data, on the other hand, is data originally collected for a different purpose and reused for a (different or new) research question (Hox & Boeije, 2005). Secondary data can either be quantitative or qualitative data, though most are quantitative data (Hox & Boeije, 2005). The most obvious advantage of secondary data is its low cost and faster access to an already compiled relevant data. However, secondary data was originally collected for a different purpose, and it may not be optimal for the research problem. Nevertheless, the practicality of utilizing existing data for research is becoming more prevalent (Johnston, 2014; Andrews et al., 2012; Smith, 2008; Smith et al., 2011).

3.6.3. Experiment

In experimental data collection, the researcher has full control of who participates in the experiment. In collecting data, the researcher manipulates one or more of the predictor variables, observing its effect on the outcome variable (Hox & Boeije, 2005). Because the researcher exerts overt control over the planning and procedures of the experiment, the outcome allows for a causal interpretation. An experiment is normally concerned with numbers and is associated with quantitative data collection.

3.6.4. Interview

A researcher may use interviews for either quantitative or qualitative data collection, though it is most common in qualitative research for drawing out descriptive data. Marshall and Rossman (1999) define an interview as "an interaction between an interviewer and a respondent, from which the interviewer can infer whether the answers have relevance to the research questions." Because of the face-to face interaction, the interview can be very effective and get the most relevant and credible data. In qualitative research, the interview can allow the researcher to ask for follow up, clarification, or add in impromptu questions, while at the same time the participant can ask the researcher to explain unclear questions. An interview is, therefore, flexible, and allows the researcher to get an in-depth understanding of a phenomenon by probing the participant (Neuman, 2004). Another advantage of the interview method is that it allows the researcher to assess the participant's knowledge level through the participant's answers and reactions to the questions.

The interview can be either structured or semi-structured. In a structured interview, the researcher uses standardised questions ideal for many participants (Denscombe, 2007). In a semi-structured interview, the researcher has flexibility to use non-standardised questions. The main disadvantages to the interview method are possible high cost, time consuming, and prone to interview bias (Robson, 2002).

3.6.5. Observation

A researcher may use observation as a data collection method in both quantitative and qualitative research; the difference between the two lies in the type of data the researcher collects. According to Creswell (2005, p. 211), observation is the "process of gathering open-ended, first-hand information by observing people and places at a research site." The researcher uses the senses, including sight, hearing, touch, and smell to observe, document, explore, and understand activities, actions, relationships, culture, or ways of doing things (Paridis et al., 2016). Observation allows the researcher to collect large Total Evidence Volume per Case data.

Observation can be participant or direct. In participant observation, the research participates, or immerses, in the action or events over time to gain first-hand experience in the setting. Through participation or immersion, the researcher aims to elicit meanings and understand nuances of behaviour, ideas or emotions. Participant observation is often associated with qualitative methods. Direct observation occurs when the researcher observes interactions, processes, or behaviours as they occur, while indirect observation occurs when the researcher observes the results of interactions, processes, or behaviours possibly using video playback1. Unlike participant observation, in direct observation, the researcher does not participate or interferes in the actions of people or processes observed.

3.6.6. Content or Textual Analysis

Content or textual analysis deals with textual or visual data in documents, as such it is associated with qualitative data collection, though it can be used for quantitative data collection as well. Due to the ready accessibility and availability of documents, content analysis has grown in popularity. The research question largely guides the type and number of documents the researcher will analyse. Documents could include letters, minutes of meetings, notes, lab manuals, electronic documents, web pages, newspapers, research articles, governmental reports, records, policies, protocols, films, photographs, art, or any other type of useful document (Marshall and Rossman, 2006). The researcher can use content analysis as the main data collection method, or as a supplementary collection method to contextualize findings from another method.

Content analysis involves coding textual data, the approach to which delineates the three types of content analysis: conventional, directed, or summative. In conventional content analysis, the researcher derives coding categories directly from the textual data. In directed content analysis, on the other hand, the researcher uses a theory or research finding to guide the coding. The research question guides the development of an analytical coding grid, which the researcher iteratively applies to selected documents (Paradis et al., 2016). In a summative content analysis, the researcher counts and compares keywords, and thereafter interprets the underlying context.

3.6.7. Survey

A researcher may use a survey or questionnaire in either quantitative or qualitative data collection. Surveys are ideal for documenting perceptions, attitudes, beliefs, or knowledge within a clear, predetermined sample of individuals (Paradis et al., 2016). A researcher may conduct a survey to gather data not readily available in the literature (Remenyi et al., 1998) with the intent of generalising the results to a population (Creswell, 2003).

A researcher may conduct a survey in-person, via email, telephone, or the use of a website such as Survey Monkey. Surveys may include cross-sectional and longitudinal questionnaires, or structured interviews (Babbie, 1990). Well-constructed survey questions are essential was it is important that the researcher needs to be careful to avoid leading or biased questions.

The advantages of the survey method include that it is low cost and not as time consuming as an interview or other methods; the researcher can still gather enough data. Surveys, however, have the disadvantage of not being able to ask lengthy or probing questions. In addition, the credibility or trustworthiness of survey responses may be questioned, and there may be difficulty with a low rate of survey response. (Denscombe, 2007; Neuman, 2004).

3.6.8. Focus Group

Focus groups are used in qualitative research. In a focus group, a researcher invites a small group of participants to engage in a discussion designed to generate data relevant to the research question. (Yates, 2004). The researcher may use predetermined questions that a moderator asks participants in order (group interview), or the researcher may use a script to generate undetermined group conversations about the research question or set of questions (group discussion) (Paridis et al., 2016). A focus group is ideal when the researcher wants to capture the collective experiences of a group of people, especially when an individual experience would be insufficient to understanding a phenomenon. Researchers have also used the focus group method to supplement or verify a previously completed data collection method. Unfortunately, a focus group may be costly, and could pose scheduling challenges, when an ideal number of eight to ten participants must be present at the same time. (Bryman, 2008; Paridis et al., 2016).

3.6.9. Justification for Data Collection Method

The researcher uses secondary data for the quantitative research. The researcher obtained permission to access and use data from the Dubai Police Database. The data is secondary because the data was originally collected for a different purpose; for recordkeeping of the Dubai Police, and the researcher will reuse the data to address the research questions of this thesis. The researcher will apply secondary analysis and statistics to interpret the secondary data obtained from the Dubai Police Database. A main advantage of using the Dubai Police Database as secondary data is that it is low cost, and provides speedy access to an already compiled data about the Dubai Police DF department, a second advantage is that this allows the research to investigate real cases that have occurred over more than ten years: this makes the data highly relevant to the research.

The primary data collection method for the qualitative portion of the research will be semi-structured interviews to reflect the qualitative aims and objectives of the research. The interview method can be used to great effect for the purposes of qualitative studies (Hardy & Corrall, 2007). Many researchers following the case study and phenomenological approaches have used the observation and interview techniques. (Leedy & Ormrod, 2005). The observation method, while allowing for random visits and a view of management operations in organisations that may produce better information, would not be practical for the current research because it would be impossible for the researcher to conduct observations of the various DF case managers in different organisations and countries.

The interview method gives the researcher flexibility in understanding the DF organisations' case management procedure and allows the researcher to probe participants with regards to questions for a deeper understanding of the effects of Big Data on DF investigation delay and lengthy Person-Hours. In this regard, the semi-structured interview's adaptability and opportunities for exploring responses and ideas makes it most appropriate with the researcher's strategy of better understanding the results of quantitative research with the results of qualitative research. According to Almarzooqi (2016), the rich data derived from an in-depth interview will help to unmask the complexities of a new field of study such as DF.

CHAPTER 4: DATA COLLECTION PROCESS

4.1. Introduction

The main aim of this research is to identify the most common factors, challenges, and trends that DF investigators and DF case managers encounter due to increasingly voluminous and heterogeneous digital data. In this investigation the aim is to then consider how such managers can best manage those challenges systematically, especially in relation to the allocation and completion of DF cases. This chapter will explain how the researcher conducted the data collection in each of the three studies, according to the mixed methods sequential explanatory design, and the appropriate research method for the corresponding research strategy. The chapter, therefore, is divided into (1) Study One (Investigation of the Dubai Police Records) data collection, (2) Study Two (Interviews with DF managers) data collection, and (3) Study Three (Confirmation of the Interviews) data collection.

4.2. Study One (Investigation of the Dubai Police Records) Data Collection

Data for this study was derived from the Databases and reports of the Dubai Police. The researcher used this data because of its availability, its size (many records over many years) and its fit to the research aims. In so doing, the researcher used empirical research methods (Wohlin, Höst, & Henningsson, 2003). Quantitative research methods are the most appropriate for this work because this study is mainly concerned with different trends in cases that influence the DF investigation processes. According to Johnston (2013), secondary data analysis is a viable method to utilize in the process of inquiry when the research follows a systematic procedure. Johnston (2013) suggested the following systematic procedure for secondary data analysis, which this research applies: (1) development of the research question, (2) identification of the dataset, and (3) evaluation of the dataset.

4.2.1. Research Question Development

In this first study, the researcher aims to measure the growth of cases and extrapolate the main factors behind the delay of digital investigations including the Total Evidence Volume per Case and Heterogeneity of Evidence Items per Case.

To this effect, the researcher stated the following research question for the first study:

Research Question 1.1:
What are the trends for the cases investigated by practitioners over the past twelve years?

Research Question 1.2:
What influence does Total Evidence Volume per Case have on the investigation processes?

Research Question 1.3:
What influence does Heterogeneity of Evidence Items per Case have on the investigation processes?

Further, the researcher posited the following hypotheses prior to data collection:

Hypothesis 1
There is an increase on the cases trends for the past 12 years.

Hypothesis 2
The Total Evidence Volume per Case affects the time required for the examination process.

Hypothesis 3
The Heterogeneity of Evidence Items per Case affects the time required for the examination process.

4.2.2. Evaluation of the Dataset

In evaluating the dataset in secondary data analysis, a researcher should identify; (1) the purpose for collection of the original data, (2) who was responsible for collecting the original data, (3) what original data was actually collected, (4) when the original data was actually collected, (5) what methodology was employed in obtaining the data, (6) management of the original data, and (7) consistency of the information obtained with other sources (Johnston, 2013).

The researcher has the benefit of her work affiliation with the Dubai Police to be able to conduct a proper evaluation of the secondary data. This data was collected by the Dubai Police as part of its process and documentation as a government department. The purpose for the collection of the data, therefore, was for government record keeping. The personnel or a staff of the DF Department was responsible for collecting the data as part of the documentation process of the Dubai Police. Third, the type of data collected were (1) case records Database and (2) Acquisition Verification Reports. These types of data are described further below under the section on sampling design. Fourth, the original data was collected between January 2003 to February 2015, as discussed in more detail further below under the section on sampling design. Fifth, the methodology employed to collect the data is inapplicable here since the data was not initially collected for research but as part of a government agency's record-keeping procedures. Sixth, the original data is managed by the Dubai Police and kept in the Dubai Police Database. Finally, the data's consistency with information obtained from other sources is inapplicable here since the researcher has no access to datasets from other police departments.

Since the researcher followed a systematic procedure for collecting the secondary data, secondary data analysis was a viable method for use in this research. The succeeding sections explain further the methodical process employed for collecting the secondary data.

4.2.3. Participant Selection

The researcher selected the Dubai Police - DF Department to study the trends in digital forensic crimes for several reasons. First, the UAE government is sponsoring the researcher's study. Second, the Dubai Police supports this research by allowing the researcher access to their Database records, cases, workstations, and DF investigation tools; and by allowing DF investigators and case managers to participate in the study. Moreover, and as it is important for any Digital Forensic Department around the world, the Dubai Police are investing in this research to gain better knowledge about the data that they have. This research will guide the Dubai Police to determine the possible factors behind the delay of investigation. The knowledge that they will gain from this research will be akin to a guide to take decisions that decrease the time of the DF investigation process. Additionally, Dubai is a high-profile global city, with more than 200 nationalities comprising a population of approximately 2,213,000 people in 2013, the last year for which reliable data exists (DSC, 2013). Thus, digital crimes are committed in Dubai by people with different backgrounds, capabilities and experiences. Moreover, the Dubai Police is one of the leading organizations in the Middle East providing DF investigations.

By way of context, DF investigations started in a small section of the Dubai Police in 2000. At that time the section had only four employees, including the section head and a small lab with a few tools. By 2008, with the development of the DF field and a flood of digital forensic cases in Dubai, the Dubai Police enlarged the DF Department to become a sub-department under the General Department of Forensic Science and Criminology. Today (2018), the DF Department includes a core of 52 employees in several sections. The DF Department expects to double this number within the next few years because the Dubai Police is sponsoring many students to study in different DF disciplines. The DF Lab has up to-date-tools and devices to cope with the accelerated growth of digital forensic cases. The researcher of the current study has been working in the Dubai Police as a DF examiner for over nine years. Thus, the Dubai Police is the most convenient primary organisation for the quantitative portion of this study.

4.2.4. Data Gathering Procedure

The original records in the Databases were written in Arabic. The researcher manually collected all the records for this study from Databases and reports in the Dubai Police - DF Department; this took around two and a half months. Next, the researcher translated the original records from Arabic into English and inserted the translated records into a new Database that the researcher specifically built for this study. The researcher named the new Database [DATASET 1].

The following are the sources of the collected data case records Database and Acquisition Verification Reports. Figure 8 shows the relationship between those data sources. Each of these data sources are described in the following section:

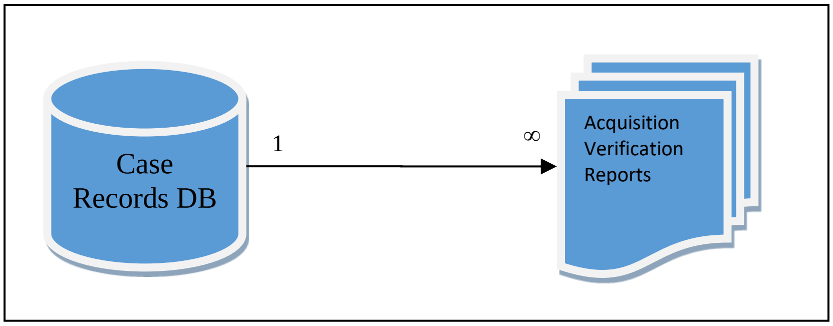


Figure 8. Relationship between the data sources

The resource, Case Records DB holds 8620 records and has Case, Evidence and Examiner tables as illustrated in Table (2). The highlighted variables are the ones which are used in the thesis study either directly or in a calculation to create a new variable. Figure 9 below shows the relationship between the tables in Case Records DB.

Table Name: Case				
Variable Name	Abbreviation	Description	Data Type	Example
CaseNumber	CNo	Unique number assigned to each case	Numerical	20181
CaseReceivedDate	CRD	The date of receiving the case	Date	13/6/2013
CaseSentDate	CSD	The date of closing/sending the case	Date	14/6/2018
Number of Evidence Items per Case	NEI	Number of Evidence Items per Case	Numerical	4

ExaminersIDs	EIDs	The list of examiners IDs who are assigned for this case	Numerical	17514
Case Request Details	CRD	Case request details to indicate what is needed to be done to proceed investigating the case.	String	Extract all the .jpg files.
Heterogeneity of Evidence Items per Case	H	A count of the number of unique evidence item types per case	Numerical	4
Table Name: Evidence				
Variable Name	Abbreviation	Description	Data Type	Example
Case Number	CNo	Unique number assigned to each case	Numerical	20181
Evidence Serial Number	ESNo	Serial number of the evidence item	String	TH-112-398-211-2
Evidence Description	ED	Description of the evidence item	String	A laptop with two hard drives
Evidence Type	ET	The type of the evidence like Laptop, Desktop, Hard Drive, Flash Drive, CD, DVD…etc	String	Mobile
Examiners IDs	EIDs	The list of examiners IDs who will work on this specific evidence item	Numerical	17514
Total Evidence Volume per Case	TEV	The logical size of the evidence calculated in GB.	Numerical	1024
Table Name: Examiner				
Variable Name	Abbreviation	Description	Data Type	Example
Examiner ID	E ID	The examiner ID number	Numerical	17514

Examiner Name	EN	The name of the examiner	String	Ibtesam
Join Year	JY	In which year the examiner joined the department	Numerical	2004
Earlier Experience	EE	Number of experience years in the field before joining the department	Numerical	8
Section ID	SID	A unique number of each section in the department	Numerical	1
Table Name: Section				
Variable Name	Abbreviation	Description	Data Type	Example
Section ID	SID	A unique number of each section in the department	Numerical	1
Section Name	SN	The name of the section in the department - Dubai Police has six sections and they are Computer, Network, Mobile, Programs &Databases, Photos & Videos Analysis and the Voice Analysis Section	String	Computer Investigation
Description	Desc	Brief description of each section	String	Investigating all the cases including computers or laptops

Table 2. Tables and Variables in Case Records DB (the resource DB)

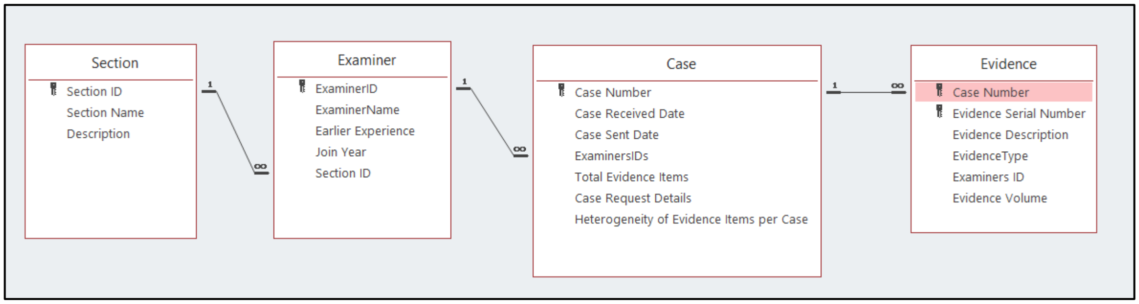


Figure 9. Relationships Between the Tables in Case Records DB.

Following this, 4398 Acquisition Verification Reports were collected. In DF, Acquisition refers to the process of duplicating or imaging the seized digital forensic evidence using a duplicator or a software-imaging tool with a write-blocking device to create an identical copy of the evidence item and preserve the original drive safe from any tampering (Leong, 2006). Thus, the Acquisition Verification Reports is the document that verifies the imaged copy of the evidence using one of the hashing methods Sha-1 or MD5 functions. The researcher collected the following variables from the reports and as described in the previous section, the highlighted variables are the ones which were later used in the thesis work.

Variable Name	Abbreviation	Description	Data Type	Example
Case Number	CNo	Unique number assigned to each case	Numeral	20181
Total Evidence Volume per Case	TEV	The logical size of the evidence in Mega Bite	Numeral	1024
Acquisition Date	AD	The date the acquisition process conducted in	Date	6/6/2017
Evidence Serial Number	ESNo	Serial number of the evidence item	String	TH-112-398-211-2

Table 3. Variables from Acquisition Verification Reports (the resource reports)

To validate the data gathering procedure, the researcher made sure that the data translation and transfer of each record was accurate by having one of the Dubai Police Digital Forensics department's employees check a selection of the records.

Approximately 15% of the Total Evidence Volume per Case in Cases Records DB were not recorded. The missing values were found in the collected Acquisition Verification Reports and filled in in the new Database [DATASET 1].

The researcher collected 8620 records stored in [DATASET1] from December 2014 to February 2016, and the researcher obtained records from January 2003 to February 2015. However, the data used for the study was selected from February 2003 to December 2014 to make sure that the examiners are not working on pending cases before 2003, and to be sure that all the selected cases are completed by the end of 2014. The researcher also selected only cases received by the Computer Section, Network Section, Mobile Section, and Programs and Databases Section. Classified Cases were not included as their records held no useful data.

Outliers were removed from the Databases using interquartile ranges (IQRs). Any data point more than 1.5 IQRs below the first quartile or above the third quartile was considered as an outlier (Ghasemi et al., 2012). The interquartile range was measured for the Total Evidence Volume per Case, Total Evidence Items and Number of Working Days (The calculation of this variable will be illustrated in the next section).

Following this cleaning of the Database, there remained 3353 records [DATASET 2]. Later, the researcher selected only the cases that were examined by a single examiner and excluded all the cases with more than one examiner - this resulted in 277 additional records being removed leaving 3076 records remaining for [DATASET 3].

4.2.5. Defining and Designing Study Variables

The researcher wanted to see how the predictor variables affected the outcome variables in order to understand cause and effect relationships between the variables. This suggests a factorial design as described by Vogt, (1999). The researcher identified predictor and outcome variables. The following section will identify the details of the study variables, see Table 4, some of those variables were collected directly from the data sources and other variables were calculated (the calculated variables are highlighted).

Hypothesis #	Predictor Variable	Outcome Variable
Hypothesis 1	Year	Number of Cases
Hypothesis 2	Total Evidence Volume per Case	Person-Hours
Hypothesis 3	Heterogeneity	Person-Hours

Table 4. Predictor and Outcome Variables

Different equations were used to calculate the highlighted variables above. To identify Number of Cases per Year (NCY) it is a simple sum of all the number of records in that specific year (i). Equation 1. was used to calculate the Number of Cases.

$$Number\ of\ Cases = \sum_{i=1}^{NCY} i$$

Equation 1. Number of Cases

The researcher considered two different ways to calculate Person-Hours of investigation (Equations 3 and 4). In each case she first needed to identify the Number of Working Days (NWD) by calculating the number of days between the Case Received Date and Case Sent Date (i). Weekends and national holidays had to be excluded (H). This calculation is found in Equation 2.

$$Number\ of\ Working\ Days\ (NWD) = (Case\ Sent - Case\ Received - H)$$

Equation 2: Number of Working Days

Given that an examiner could be working on more than one case at a time, an estimate had to be calculated to determine the Person Hours on a Case. Two possibilities were considered. The first (Equation 3) assumes that an examiner shares his / her time equally over all cases.

This uses the Number of Active Cases each Examiner had (NACPE) to determine the Average Number of Cases per Examiner (ANCPE) on a received date.

$$Person\ Hours\ of\ Investigation\ = \frac{1}{ANCPE} \times 7\ \times NWD$$

Equation 3. Person Hours of Investigation (1)

An improved Equation (4), weights the hours according to the evidence items of a case. This uses the Number of Evidence Items per Case (NEI) and the Total Number of all Evidence Items (TEI) an examiner has on a case received date.

$$Person\ Hours\ of\ Investigation = \left(\frac{\mathrm{NEI}}{\mathrm{NEI} +\ \sum_{\mathrm{i}}^{\mathrm{N}} \mathrm{Ei}} \times 7\right) \times \mathrm{NWD}$$

Equation 4. Person Hours of Investigation (3)

Equation 4. models complexity by taking into consideration the number of evidence items the examiner is working on when he / she receives a new case. This is, therefore, a closer fit to the reality as experienced by the researcher, hence Equation 4. is the chosen one.

4.2.6. Validating Choice of Measures

As outlined above, Person-Hours of Investigation had to be estimated. To justify the methodology used in Equation 4., the researcher randomly collected 24 case records and gathered the details of Person-Hours from each examiner manually in order to compare the accurate Person-Hours against the estimated amount (Creswell, 2015).The researcher made a comparison between the reported total number of hours per case and the predicted value from the methodology, see Figure 10. The researcher calculated the comparison using the following:

$$Percentage\ Error = \left(\frac{Prediction\ Time - Real\ time}{Prediction\ Time}\right) * 100$$

Equation 5. Percentage Error

The comparison between the accurate data and the estimated data shows that the mean absolute percentage error (MAPE) equals 20.26%, which means that the accuracy percentage is 79.74%, as shown in Table 5. This comparison justifies the proposed methodology.

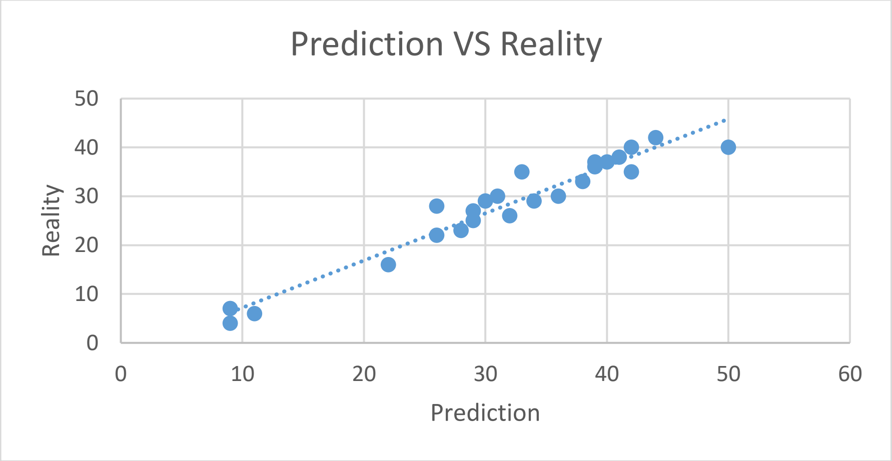


Figure 10. Prediction VS Reality of Person-Hours of Investigation

Prediction	Reality	Percentage Error (rounded to 2 decimals)
44	42	4.55
50	40	20
36	30	16.67
34	29	14.71
26	22	15.38
28	23	17.86
38	33	13.16
33	35	6.06
39	36	7.69
40	37	7.5
42	35	16.67
39	37	5.13
41	38	7.32
29	25	13.79
22	16	27.27
32	26	18.75
29	27	6.9
42	40	4.76
31	30	3.23
26	28	7.69
30	29	3.33
11	6	45.45
9	4	55.56
9	7	22.22
	MEAN	20.26

Table 5. The Mean Absolute Percentage Error

4.2.7 Data Measurement Scale

Table 6 summarises the constructs being studied, and the variables used.

Construct being studied	Variable Name	Abbreviation	Data Type	Variable Type	Example
Volume of work to be done	Number of Cases	NoC	Numerical	Outcome	60
Age of a case – possibly suggesting simplicity	Year	Y	Numerical / Interval	Predictor	2006
Effort associated with a case	Person-Hours	PH	Numerical / Interval	Outcome	32
Complexity of a case	Total Evidence Volume per Case	TEV	Numerical / Interval	Predictor	1024
Diversity of a case	Heterogeneity of Evidence Items	HEI	Numerical/ Interval	Predictor	6

Table 6. Measurement Scale of the Collected Data

The assumption was that complexity, size, and diversity of a case (predictors) would affect the effort / work needed to solve cases (outcomes). There was also an assumption that the Number of Cases (outcome) would rise with the year of consideration (predictor).

4.2.8. Data Collection Instruments

The researcher used SPSS to examine all the collected records from the Cases Records Database and Acquisition Verification Reports from the Dubai Police Computer

Section. The workstation which was used to store the selected report is provided from the Dubai Police and it provides full security restrictions to ensure the safety of the data.

4.2.9. Limitations

The data chosen for study generally covered most of the sections within the Dubai Police Digital Forensic Department. However, cases from the Photos and Videos Analysis Section and Voice Analysis Section were not included since, prior to 2013, they were under the Fingerprint Department and so not held in the Case Records Database. Given that cases were only being gathered to 2014, excluding this small number between 2013 and 2014 was not considered to be problematic. If data had been available for years prior to 2013, it would have been interesting to see if these data would have changed the findings as to the Heterogeneity of Evidence Items per Case, and whether there is an increase in the number of evidence items in photo, video, or voice format.

4.3. Study Two (Interviews with DF managers) Data Collection

The researcher primarily derived the data in this study from semi-structured interviews; a qualitative data collection method. The qualitative research method was most appropriate because Study 2 was mainly concerned with understanding how DF organisations work to handle lengthy DF investigations. The second study investigates the context of work in various government and private DF organisations in different countries, examining the different factors likely to affect the Person-Hours of investigation, the case management strategies employed by DF organisations, workflow implementation practices and the solutions used by these DF organisations to overcome lengthy Person-Hours.

4.3.1. Sequential Explanatory Design: Follow Up Explanation Model

In the sequential explanatory design's follow up explanation model, the researcher uses the qualitative data to explain or expand the quantitative data. As such, the second study aims to collect qualitative data through semi-structured interviews to explain or expand the results of the quantitative secondary data from Study 1 (Investigation of the Dubai Police records).

The researcher derived the questions used in the second study from the literature, and from the factors identified in the first study. Study 1 (Investigation of the Dubai Police records) mainly highlighted the factors that influence the total Person-Hours of DF investigation. In Study 2 (Interviews with DF managers), the researcher sought to compare the factors so found, to those that the participants in the interviews really encounter in practice. This study contributes knowledge that could help decision makers to perceive the context of the work, the distribution process and the management of the workflow used in other digital forensic departments/companies.

4.3.2. Phenomenological Approach

The researcher used a phenomenological approach in the second study because the researcher wanted to understand better the experiences of decision makers around the world in managing a DF organisation, in order to identify a list of common sense decision influences and the common factors behind the decision of assigning the cases in the DF organisation. In other words, the researcher wanted to understand the "lived experiences" of individuals in DF organisations.

4.3.3. Semi-Structured Interviews

Following the phenomenological approach, the researcher used the semi-structured interview as the data collection method. A phenomenological interview aims to describe the meaning of a phenomenon shared by several individuals (Marshall & Rossman, 2006; Yüksel & Yildirim, 2015). The semi-structured interview is appropriate here because the researcher can get descriptive data from DF investigators and DF investigators – participants closest to the phenomenon under investigation, which is the effect of Big Data on lengthy DF investigation. The researcher collected the data utilized for analysis from April- 2016 to October- 2016.

4.3.4. Participant Selection Criteria and Sampling Design

Following the phenomenological tradition, the researcher selected participants who had experienced the phenomenon (Moustakas, 1994). In a phenomenological inquiry, the participants should consist of a homogeneous group who have a shared experience, that is significant and meaningful, with the same phenomenon (Creswell, 2007). The participants in the second study had a shared experience as managers of DF departments or sections. These participants had meaningful and significant experience since they were, at the time of interview, active decision makers in DF departments or sections.

Each was willing to describe their experience and agreed to have the interviews recorded. A small sample size; between eight to fifteen participants is common in this type of study as the main purpose of a qualitative study is the depth of understanding not generalization (Quinn, 2002). However, those kinds of studies require enough participants to offer different experiences of the phenomenon (Moustakas, 1994). Creswell (2013) suggested that the sample size of a phenomenological study is usually between one and ten. This study had 12 participants.

Purposeful sampling was used; this is common in qualitative studies. In a phenomenological study, Creswell (2007) explained that purposeful sampling involves the researcher purposively selecting participants who can understand the phenomenon; and whom the researcher determines share significant and meaningful experience concerning the phenomenon under the investigation. (Yuksil & Yildirim, 2015).

The researcher therefore selected participants who were decision makers in DF departments or sections (government or private sector). Participants were either head of the department or head of a section under a department. To ensure reasonable depth for the analysis, the researcher selected participants from nine different countries. The researcher also selected managers or section heads that were responsible for allocating digital forensic cases among DF investigators. To recruit participants, the researcher created a list of decision makers (potential participants) from different DF departments or sections. The researcher's potential participants list included DF managers from the following countries: United States of America, United Kingdom, Sweden, Netherlands, Spain, Pakistan, Malaysia, Singapore, Ireland, Kingdom of Saudi Arabia, Kuwait, and United Arab Emirates. Dr. Ibrahim Baggili, an Assistant Professor of Computer Science at the Tagliatela College of Engineering, University of New Haven, and the researcher's previous instructor in a master's degree program, helped the researcher reach out to the potential participants. The researcher also used LinkedIn (www.linkedin.com) to contact professionals in the field of DF investigations. The researcher invited 19 DF managers to participate in the research; however, only 12 DF managers showed interest to participate.

4.3.5. Participation Process

As known in phenomenological studies, the interview transcripts form the basis of the data. All interviews followed the transcendental phenomenological tradition. The researcher approached potential participants via email or telephone (office numbers). The researcher emailed an information sheet to all participants for review (Appendix 2). The researcher then gave potential participants up to two weeks to reply via email or telephone to confirm whether they would be interested in participating or not. The researcher sent consent forms to potential participants via email (Appendix 3) and gave the participants two weeks to sign, and email, the consent form. Once a participant signed the consent form, the researcher arranged interview dates with the participant based upon the participant's availability and preference. The timeframe for the interview was usually within four weeks from the signing of the consent form.

4.3.6. Ethical Consideration

As the research involved interaction with humans, the researcher conducted the interviews after obtaining ethical approval from the University (Appendix 4); especially the researcher did not encounter any ethical issues in the research project as the researcher obtained informed consent from participants and safeguarded the participants' information through confidentiality safeguards.

4.3.7. Pilot Interviews

The researcher tested the research protocol by conducting pilot interviews to enhance and ensure the efficiency of the interview questions. These interviews were with a member of the advisory committee, Dr. Virginia N. L. Franqueira; a manager of the Dubai Police DF department, Major/Eng. Rashid Lootah; and the Head of the Voice Comparison Section of the Dubai Police DF department, Major/ Eng. Hamad Juma'. All the participants gave the researcher verbal permission to share their names. Following these pilot interviews, some questions were reordered, and others had the words changed to ensure they were meaningful.

4.3.8. Interview Procedure

The researcher shared a summarized version of the first study with the interviewees ahead of time, and if interviewees needed further details, the researcher referred the interviewees to the following published paper relating to the first study:

Al Awadhi, I., Read. J.C., Marrington, A., Franqueira, V.N.L. (2015). Factors influencing digital forensic investigations: Empirical evaluation of 12 years of Dubai police cases. Journal of Digital Forensics, Security and Law (JDFSL), 10(4), pp. 7-16. ADFSL Press.

At the start of the interview, the researcher shared a common definition list with the participants to ensure clarity of terms as some named things differently from one department to another. The researcher then briefed the participants going over the information sheet and confirming that the participant understood. The researcher gave the participants a further option to withdraw from the interview prior to the start. Thereafter, the researcher confirmed receipt and signature of the consent form.

The interview started, and it was expected to last for approximately one hour. The researcher recorded all the interviews using the recording application on the workstation and they were all conducted in the English language. The first set of questions started with the context of work in every DF department. The second set of questions covered the status of DF case assignment process in the participant’s respective DF department or section. Afterwards, the interview focused on the trends and factors that affect the Person-Hours of investigation. Finally, a set of questions covered the techniques used to overcome the lengthy process of DF investigations. The question list can be seen under Section 4.3.11 below.

At the end of the interview, the researcher again gave the participants an option to withdraw. The researcher also gave participants an opportunity to discuss any issues and questions with the researcher. The researcher then gave the participants the contact details of the researcher and the Director of Studies who could answer any questions that any participant may have about the researcher and the research. The researcher then explained that the participant had the ability to withdraw within two weeks after the interview. Finally, the researcher kept the participants updated with the outcome of their participation in the interviews in a timely manner.

4.3.9. Epoché

Since phenomenological research requires the researcher to conduct the interview without preconception or bias, the researcher used epoché. Epoché is the act of clearing all suppositions from the mind of the researcher to be able to view the phenomena as a fresh experience (Moustakas, 1994). In the second study data collection, the researcher freed herself from any presuppositions and biases related to the study's phenomena. The researcher set aside prior knowledge and experience, including what the researcher learned from the first study. This was conducted by writing a personal epoché to include all the background, knowledge and experience that the researcher obtained to be available for the reader to compare between the findings of this research and the researcher's own beliefs and expectations. Moustakas (1994) suggests that "no position whatsoever is taken...Nothing is determined in advance". Thus, the epoché process frees the researcher from previous experiences and predetermined thoughts to be able to describe accurately the characteristics of the phenomena as it is away from the researcher’s personal beliefs or illusions. The personal epoché of the researcher is in (Appendix 1).

4.3.10. Data Gathering Procedure

All the interviews were audio recorded in English. Then, the researcher transcribed all the recordings and stored them in Microsoft Word on the workstation of the Dubai Police.

4.3.11. Common Definitions Shared

The researcher shared a list of common definitions with the interview participants prior to the interview. The common definitions, used in the Dubai Police, included the following:

1. Expert/Examiner/Practitioner: Digital forensic investigators who are experts in gathering, recovering, and presenting data evidence from digital devices.
2. Analysts: analyse the data exported depending on the case factors and represent a complete report.
3. Technicians:

a. Forensic technicians who complete certain tasks under the supervision of the experts. They might help in taking pictures of the digital forensic evidence, open the digital forensic evidence to extract the hard drive...etc.

b. IT technicians who are providing maintenance for Digital Forensics workstations, devices and servers. They make sure that everything is up to date, licensed and fully functional.

4. Administrative: complete administrative tasks in the department such as secretary, follow up with purchases, organize training programs...etc.

4.3.12. Initial Questions

The following were the set of questions that the researcher used to guide the interview:

1. What was your experience before being the manager of the digital forensic department?
2. What different job descriptions there are in your department? [experts, analysts, technicians, administrative employees]
3. Roughly, how many staff member is there in each job description?
4. Describe the background/experience, skills, abilities and individual characteristics of experts in your department.
5. Do you get enough budget support for new equipment, software licenses and training programs? [Make sure to get information about the cases that they don't deal with because of lack of equipment, software licenses, skills and experience.]

6. What is the process followed to accredit an examiner?

7. Does your department deal with criminal cases only, civil cases only, or criminal and civil cases?

•If both: Do considerations differ when dealing with criminal cases as compared to civil cases? If so, how?

8. What are the different types of case that your department deals with?

9. How do you rate the complexity of this type of case?

10. How do you rate the effort required to complete this type of case?

11. Which cases does your department deal with most?

12. Which case does your department find to be challenged?

13. If the cases that you find to be challenged to your department are the most frequent cases, what would be your plan to overcome this challenge?

14. What strategy is followed when assigning a digital forensic case?

15. When, if ever, is this strategy bypassed? [Make sure that the interviewee talks about the effect of very important/high-profile cases on the distribution process and the work of examiners.]

16. How do different types of cases affect the distribution process?

17. How do you decide on the composition of a team of examiners if you want to assign a case to a team?

18. What do you think, when a case is assigned to a team is more/less efficient than assigning it to one examiner?

19. What are the circumstances that allow decision maker and/or examiners to change case assignments? [Make sure that the interviewee talks about the examiners' ability to freeze or switch cases.]

20. How do you describe the yearly trend (increase/decrease/steady) in the Number of Cases at your department?

21. In Study 1: We highlighted the factors affecting Person-Hours of work:

Make sure to cover Total Evidence Volume per Case, Number of Evidence Items per Case, Heterogeneity of Evidence Items per Case]

• What is the effect of Study 1 factors on Person-Hours of investigation in your department?

a. What is the effect of Total Evidence Volume per Case on Person-Hours of investigation in your department?

b. What is the effect of Number of Evidence Items per Case on Person-Hours of investigation in your department?

c. What is the effect of Heterogeneity of Evidence Items per Case on personal hours of investigation in your department?

22. In your opinion, what other factors affect the Person-Hours of investigation?

23. Do you estimate the Person-Hours of investigation for the cases?

    • What are the factors that you rely on to make your estimation?

    • How effective is this estimation for the distribution process?

24. The statistics showed an incremental increase in Number of Cases:

• If the current Number of Cases doubled or tripled, how the department will be affected? And how do you think the distribution process will be impacted?

• With this increase in Number of Cases, what are your plans to overcome this challenge?

25. What are the techniques used to overcome the lengthy digital forensic investigation process?

4.3.13. Validity and Reliability

The scientific procedures in qualitative research are different from quantitative research. Thus, the concern for validity is common in qualitative research. To strengthen the study's validity, the phenomenological methods and philosophical assumptions needs to be strictly followed (Cilesiz, 2011). The bracketing / epoché concept of phenomenological research also increases data validity (Laverty, 2003). Bracketing is the act where the researcher's own experience, biases, and preconceived notions are set aside. It is important to implement bracketing in this type of research, as understanding the views of the participants is the main target of the research instead of manipulating their views to fit the researcher’s own views.

This study followed strictly the phenomenological methods and applied the bracketing to isolate the phenomenon from the outside world.

4.3.14. Limitations

The main limitation with the data collection had to do with the number of interviewees. This study used semi-structured interview with digital forensic leaders/managers in both government and private. Twelve participants divided between government (7) and private (5). It was difficult to reach to more managers as some of them gave appointments but kept postponing due to their workload. Moreover, there are some responders who represent departments or companies, which are too small – with one, two or three examiners in the department/company. The researcher eliminated those participants as the case allocation strategies and workflow implementation practices are constrained to the low number of examiners. Therefore, if there were more participants, the research results would include more strategies of case allocation and workflow practical implementation.

The main limitation of this research is the lack of prior research studies that cover the work strategy followed by government or private DF departments or organisations. There is also a lack of understanding of the procedure followed when assigning DF cases. Thus, this research typology requires an initial collection of data to maintain a Database of strategies and techniques used to manage different DF departments or organisations.

4.4. Study Three (Confirmation of the Interviews) Data Collection

The main goal of this research was to make sense of the feedback from the participants regarding their practical experiences in DF case allocation and workflow. This study primarily aimed to validate the findings in the second study by focusing on the pros and cons of different assignment strategies and the pros and cons of different management procedures.

4.4.1. Sequential Explanatory Design: Follow Up Explanation Model

Like the second study, the researcher used the sequential explanatory design's follow up explanation model in the third study because the researcher used qualitative data to explain or expand the previous quantitative and qualitative data. As such, the third study aimed to collect additional qualitative data through Semi-Structured Email Interviews to explain or expand the results of the qualitative data from Study 2 (Interviews with DF managers), which in essence also explains or expands the results of the quantitative data from Study One (Investigation of the Dubai Police Records).

The researcher used the findings in Study Two (Interviews with DF managers) to inform the Initial Questions in Study 3 (Confirmation of the Interviews). In Study Three (Confirmation of the Interviews), the researcher asked the participants to evaluate the strategies and the implementation practices applied in different DF departments or organisations. This Study Three (Confirmation of the Interviews) encouraged the participants to think of other possible techniques in leading and managing a DF department or organisation.

4.4.2. Semi-Structured Email Interviews

Like Study Two (Interviews with DF managers), Study Three (Confirmation of the Interviews) is a qualitative research and uses Semi-Structured Email Interviews as a data collection method. Study Three (Confirmation of the Interviews) is a follow up or validation of the second.

4.4.3. Participant Selection

Participants in Study Three (Confirmation of the Interviews) were the same as the participants of Study Two (Interviews with DF managers). In Study Two, there were twelve participants and they all gave the researcher permission to contact again for any further interview questions to enhance the research. The researcher sent all the potential participants with the findings of Study Two and asked them if they were willing to participate in an email interview for Study Three. Out of the twelve participants, nine replied and agreed to participate in Study Three. However, two participants asked to get between three to four weeks before they can submit their answers as they were about to start their holiday break.

4.4.4. Participation Process

The researcher contacted the participants from Study Two (Interviews with DF managers) via email to indicate the need for a further interview in Study Three (Confirmation of the Interviews), and the researcher asked if the participants were willing to participate. The researcher sent the Confirmation Questions for Study Thereto the participants via email and asked them kindly to answer them within two weeks. The researcher already obtained consent forms from the participants in Study Two that covered a subsequent follow up interview. One week later, the researcher sent a reminder email to the participants regarding the email interview.

4.4.5. Data Gathering Procedure

The researcher asked all the Confirmation Questions via email, and the participants sent answers back to the researcher by email as well. The researcher then archived all the email interviews.

4.4.6. Email Interview Process

The researcher sent ahead of time the results from the second study to all the potential participants in the third study, who were also participants in Study Two (Interviews with DF managers). The researcher then sent invitations to all potential participants to participate in the Study Three (Confirmation of the Interviews) follow up email interviews.

The researcher again shared a common definition list to the participants to remind the participants and again included a briefing about the research and gave the participants an option to withdraw prior to the start. The researcher confirmed receipt and signature of the consent form from the previous study, and agreement to participate in Study Three (Confirmation of the Interviews) via email.

The researcher listed the interview Confirmation Questions in the email interview sent to the participants who consented to participate in the third study. The first set of questions dealt with the pros and cons of using different assignment strategies and different management procedures. The second set of questions covered strategies and procedures related to workflow. The researcher again gave the interviewee an option to withdraw at any time.

The researcher then gave the participants the contact details of the researcher and the Director of Studies who can answer any questions that a participant may have about the researcher and the research. The researcher then explained that the participant had the ability to withdraw within two weeks after the interview. Finally, the researcher kept the participants updated with the outcome of their participation in the interviews in a timely manner.

4.4.7. Transcription of Interviews

The main advantage of an email interview is that the interview is already transcribed. Thus, there is no additional effort to spend in this step. The interviewed emails are already the transcribed reports.

4.4.8. Sampling Design

The researcher collected the data utilized for analysis from 6 June 2017 to 20 June 2017. There was no purposive sampling, except that participants chose to continue in the study from Study Two. Thus, it could be described as a convenience sample.

4.4.9. Common Definition Shared

The researcher shared the list of common definitions as seen in section 4.3.11.

4.4.10. Confirmation Questions

The following were the set of questions that the researcher sent to the participants:

4.4.10.1. Cases Assignment and Management

1. What are the pros of depending on the number of exhibits when assigning the case to one or more examiners?
2. What are the cons of using that strategy?

3. What are the pros of assigning the cases to examiner(s) with the least number of caseloads without paying attention to their skills, knowledge or capabilities?
4. What are the cons of using that strategy?
5. If you are not already using this strategy, what are the outcomes if you applied it at your department/company?
6. What are the pros of using the urgency of case as a decision factor for assigning cases? (depending on the availability: urgent cases for senior examiners and normal cases for junior examiners)
7. What are the cons of using this procedure?
8. Do you agree that the number of exhibits is the factor that the managers need to rely on when deciding to assign the case to one or a team of examiners?
9. If you are not already using this strategy, what are the outcomes if you applied it at your department/company?
10. What are the pros of depending on the examiner's experience, skills, knowledge, capability and availability when assigning a case?
11. What are the cons of using this procedure?
12. If you are not already using this strategy, what are the outcomes if you applied it at your department/company?
13. What are the pros of assigning similar case to two teams and each team will work in parallel to ensure the speed in getting the results?
14. What are the cons of using this procedure?
15. If you are not already using this strategy, what are the outcomes if you applied it at your department/company?

4.4.10.2. Workflow

1. What are the pros of letting the examiner or the team that receives a case is required to work on the case from the start to end?
2. What are cons of using this procedure?
3. If you are not already using this procedure, what are the outcomes if you applied it at your department/company?

4. What are the pros that the case leader and his team if available are responsible of a case, but the whole department help in the pre-incident preparation, pre-analysis phase and the beginning of the analysis stage and then the case leader and his team will be responsible to complete the case analysis?
5. What are the cons of using the procedure?
6. If you are not already using this procedure, what are the outcomes if you applied it at your department/company?
7. What are the pros of letting two teams to work on parallel on the same case and giving a bonus to the team who will finalise the analysis of the case first?
8. What are the cons of using this procedure?
9. If you are not already using this procedure, what are the outcomes if you applied it at your department/company?
10. What are the pros of using contractor examiners, and selecting them depending on their skills and experience?
11. What are the cons of using that procedure?
12. If you are not already using this procedure, what are the outcomes if you applied it at your department/company?
13. What are the pros of assigning each case to junior and senior examiners and letting the junior to conduct the pre- analysis and initial analysis phase and the senior examiners to complete the analysis and post analysis phase?
14. What are the cons of using this procedure?
15. If you are not already using this procedure, what are the outcomes if you applied it at your department/company?

4.4.11. Validity and Reliability

To ensure research validity and reliability, the researcher used the results of the interviews in Study 3 (Confirmation of the Interviews) to evaluate the results found from the previous two studies, with the focus being on validating the second study. Thus, each participant in Study 3 evaluated the entire findings. Then, the researcher compared the results to each other to ensure the validity and reliability of the findings.

4.4.12. Limitations

Since the researcher used semi structured email in the third study, there were several limitations. First, the research required online communication skills for both the interviewer and interviewees. Second, it was anticipated that a lack of communication between the interviewer and interviewee might lead to a misunderstanding of the Confirmation Questions. Third, the questions needed to be extra clear for the interviewee to understand and answer. Although the research methodology had several limitations, its advantages such as the ability to work in parallel with more than one interviewee, made it easy for the interviewee to select the time to answer and avoided time constraints.

CHAPTER 5: DATA ANALYSIS

5.1. Introduction

This chapter explains how the researcher analysed both quantitative and qualitative data in a mixed methods sequential explanatory design research. The chapter explains how the researcher used statistical techniques to analyse the quantitative secondary data collected in Study One (Investigation of the Dubai Police Records). The chapter also explains how the researcher used the phenomenological approach to analyse the qualitative data collected in Study Two (Interviews with DF managers). Finally, the chapter explains how the researcher used deductive reasoning to analyse the qualitative data collected from Study Three (Confirmation of the Interviews).

5.2. Study One (Investigation of the Dubai Police Records) Analysis

The purpose of this study is to examine the increase in the Number of Cases received by the DF Department of the Dubai Police for the past twelve years. Since Study One involves the statistical analysis of collected secondary data, the study aims to understand the effects that predictor variables cause to outcome variables. This section first discusses the data analysis and statistical data treatment conducted on the collected secondary data. The section then provides a general description of the collected secondary data. The study used [DATASET2] and [DATASET3]. The study demonstrates the correlation coefficient between the variables in hypothesis one and multiple linear regression in hypothesis two and three. Then the section discusses observations that describe further factors behind the lengthy Person-Hours. Overall, the researcher presents the results of the entire hypothesis with the aim of highlighting the factors behind the time spent in DF investigation.

5.2.1. Data Analysis and Statistical Data Treatment

The researcher conducted data analysis, of the secondary data collected in Study One (Investigation of the Dubai Police records), using a variety of statistical techniques. The researcher analysed data using the computerised statistical analysis program, SPSS (Version 20). The researcher used Pearson's Correlation for hypothesis number one to measure the linear correlation between two variables (Number of Cases versus Years). The measurement result will be between +1 and -1, where 1 represents a total positive correlation and 0 represents no correlation. For the second and third hypothesis, the researcher conducted the multiple linear regression to indicate the effects of two variables which are Total Evidence Volume per Case and Heterogeneity of Evidence Items per case on the Person-Hours of investigation.

5.2.2. General Description of Data

The complete descriptive statistics, which provides minimum, maximum, mean, skewness, kurtosis and standard deviation for all the variables in Study One (Investigation of the Dubai Police Records) are illustrated next. The normality of the outcome variables is also listed. The first table refers to the data elements in [DATASET2] and the second table refers to [DATASET3]. Figures, 11 and 12 show the histograms for the outcome variables.

Variable Name	Mean	Min	Max	Skewness	Kurtosis	Normal
Number of Cases (NoC)	425.42 (SE=252.99)	150	909	.929 (SE=.64)	-.261 (*SE* = 1.23)	YES
Year (Y)	n/a	-	-	-	-	-
Total Evidence Volume per Case (TEV) (GB)	1111513.689 (SE = 90244.644)	750	128144000	18.81 (SE= 0.042)	399.84 (SE- 0.085)	-
Number of Evidence Items per case	-	-	-	-	-	-

Table 7. Description of Data – [DATASET2]

Variable Name	Mean	Min	Max	Skewness	Kurtosis	Normal
Person-Hours (P.H.)	211	7	1911	.01 (*SE* = .04)	-0.18 (*SE* = 0.09)	YES
Year (Y)	n/a	-	-	-	-	-
Total Evidence Volume per Case (TEV) (GB)	635	75	16000	-0.26 (*SE* = 0.04)	-0.18 (*SE* = 0.09)	-
Heterogeneity of Evidence Items (HEI)	1.83	1	9	1.389 (*SE* = .04)	0.82 (*SE* = 0.09)	-

Table 8. Description of Data – [DATASET3]

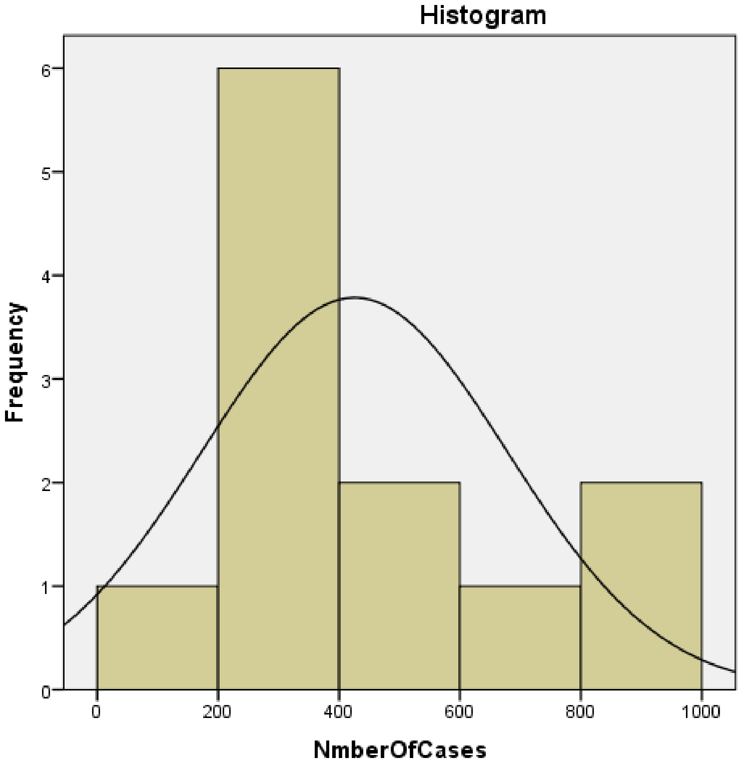


Figure 11. Number of Cases Histogram

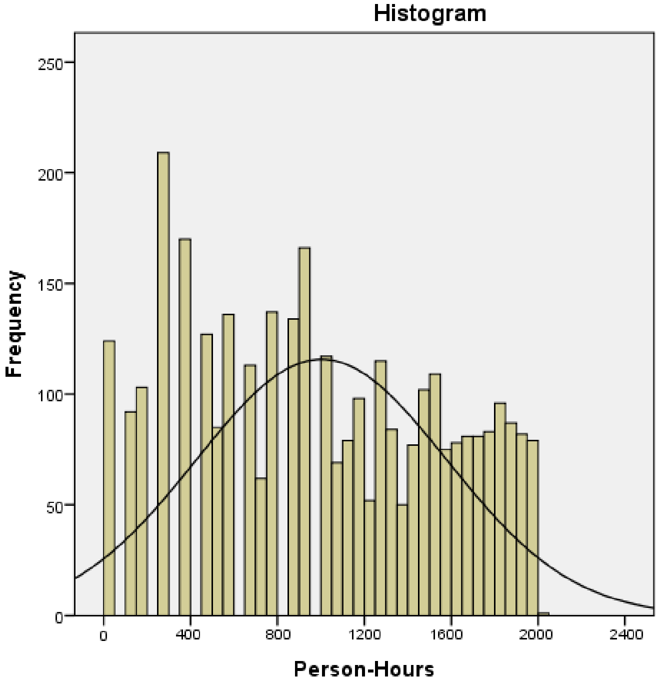


Figure 12.Person-Hours Histogram

5.2.3. Hypothesis Presentation and Analysis of Data

5.2.3.1. Hypothesis 1

[Hypothesis 1: There is an increase on the cases trends for the past 12 years.]

The first hypothesis of the study uses [DATASET 2] and is aimed at understanding better the trends of cases investigated by Dubai Police DF Department practitioners in the past twelve years.

As shown in Figure 13 below, the Number of Cases increased every year. There were 51 cases in year 2003 and more than 900 cases by 2013. It is also clear from Figure 13 that in 2010 there was an unexpected increase in the Number of Cases. A senior officer in the Dubai Police mentioned that there were high profile crimes in 2010, which led to pulling more cases. Generally, the Number of Cases increased linearly through the twelve years.

As this research is mainly concerned about the time DF examiners spent in investigations, it is important to identify if the outcome variable Number of Cases changed through the years. The researcher chose a correlation coefficient to quantify the extent and nature of the linear relationship between the Number of Cases and the Year. The Pearson

Correlation between Number of Cases and the Year was positive with strong correlation, Pearson's r (12) = .88, p< .001. r^2 = .77.

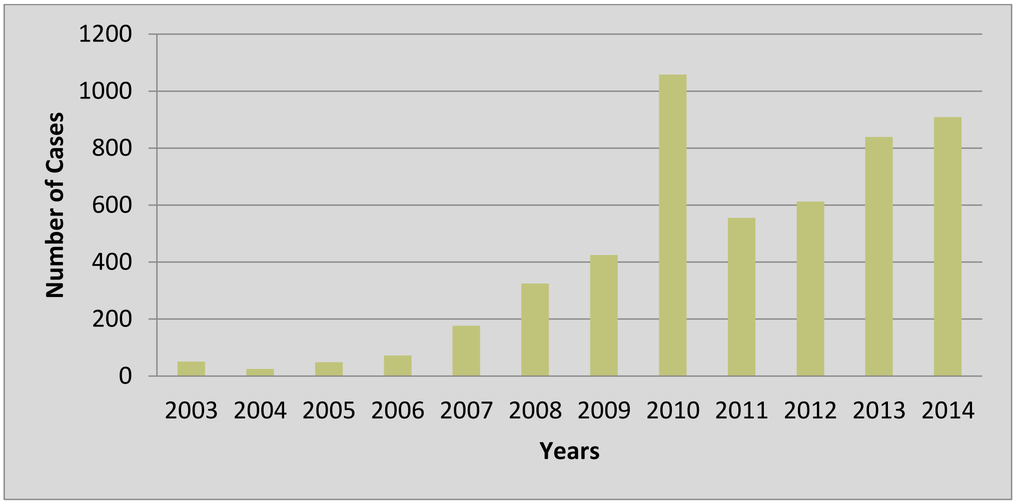


Figure 13.Year by year totals of Number of Cases

For further factors correlated with years, the researcher used [DATASET 2] to detect the rate of change in the Total Evidence Volume per Case throughout the Years. The average of the Total Evidence Volume per Case increased between 2003 and 2009, except for the year 2004 were it decreased, as shown in Figure 14 below. The average dropped in 2010 and started to increase later to reach a peek by 2014 with the average of 8000 GB per case.

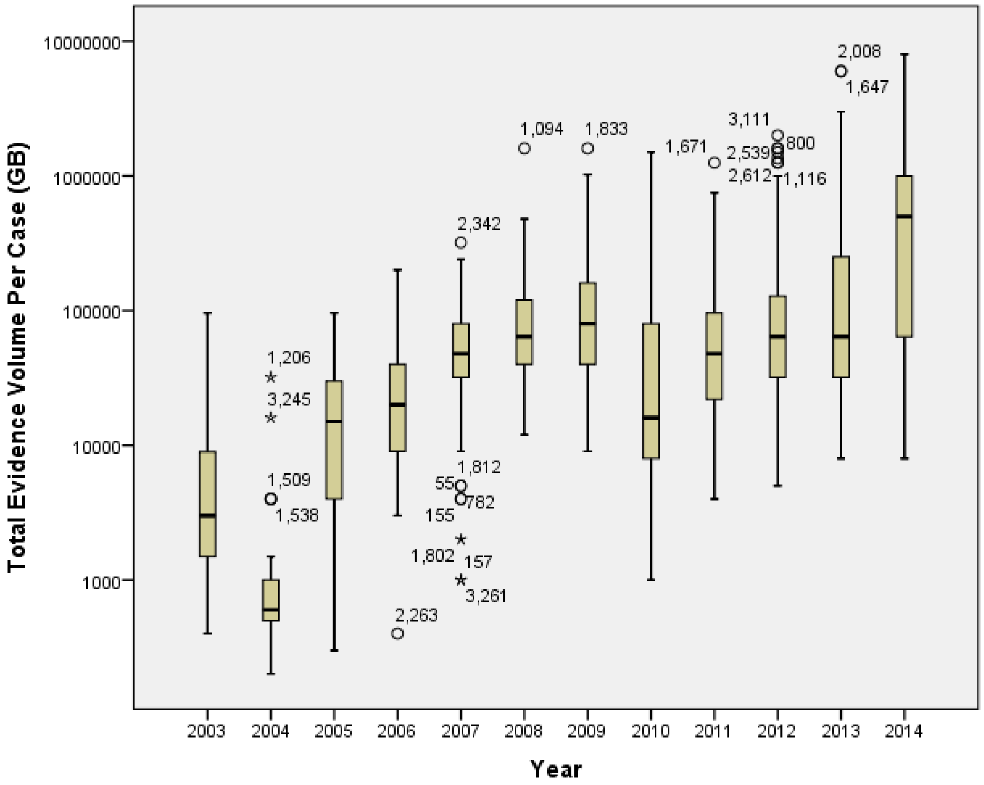


Figure 14.Year by Year Trends of Evidence Volume per Case (Calculated in GB)

Also from [DATASET2], Figure 15 below shows that the Number of Evidence Items per Case remained between 1 and 2 items except in 2003 and 2005 where it reached between 3 and 4. The data has not been specifically examined as to why the number of evidence items per case was higher than for the rest of the years. From the researchers own experience, in the early years in the DF department, the first responders in the crime scene tended to collect all the items that were at a scene, a practise that is less common now as the first responders now are better trained and more able to choose evidence items according to the crime.

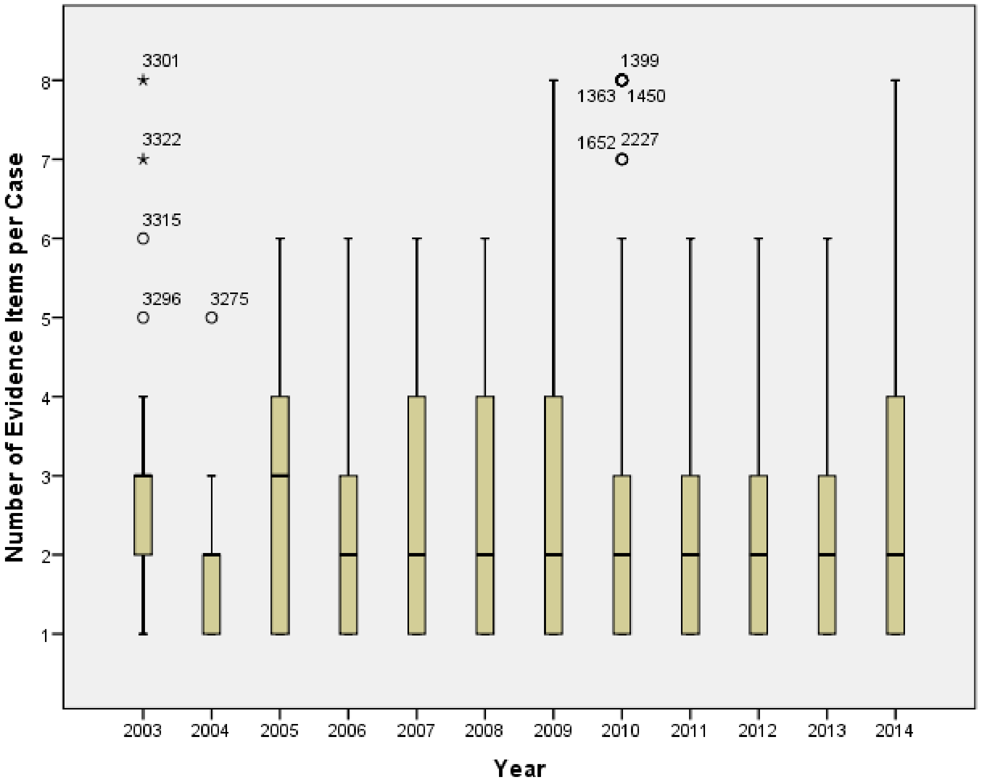


Figure 15.Year by Year Trends of Number of Evidence Items per Case

In summary, an analysis of data concerning the first hypothesis shows an increase in the Number of Cases, Figure 13, and a yearly increase in the Total Evidence Volume per Case, (Figure 14), over the past twelve years in the Dubai Police DF Department. The Number of Evidence Items per Case has remained static over the years (Figure 15).

5.2.3.2. Hypotheses 2 & 3

[Hypothesis 2: The Total Evidence Volume per Case affects the time required for the examination process.]

[Hypothesis 3: The Heterogeneity of Evidence Items per Case affects the time required for the examination process.]

As the main purpose in this section is to determine if the Total Evidence Volume per Case and the Heterogeneity of Evidence Items per Case affects the Person-Hours of investigation, multiple linear regressions was conducted on [DATASET 3] to predict Person-

Hours based on Total Evidence Volume per Case and Heterogeneity of Evidence Items per Case.

The descriptive statistics are listed previously under sections (5.2.2. General Description of Data).

A significant regression equation was found (*F* (2,2979) =724.66, *p*< .000), with an *r*^{2} of .327 (33%). The predicted Person-Hours are modelled by the following equation:

$$Person_{hours} + 10.308 + 1.539(Heterogeneity\ of\ Evidence\ Items\ per\ Case) + .004(Total\ Evidence\ Volume\ per\ Case)$$

Equation 6. Number of Cases

Heterogeneity of Evidence Items per Case is a count of the number of unique evidence item types per case and Total Evidence Volume per Case is measured in GB. Heterogeneity of Evidence Items per Case is the significant predictor of Person-Hours with moderate correlation. The Total Evidence Volume per Case doesn't play a separate role once its correlation with Heterogeneity of Evidence Items per Case is considered. This is because the Total Evidence Volume (B = .004): as Total Evidence Volume increases by one unit (i.e. by one GB), Person-Hours increase by 0.004 units. Furthermore, Heterogeneity (B = 1.54): as Heterogeneity increased by one unit on the Heterogeneity scale, Person-Hours went up by 1.54 units (Table 9). Thus, Heterogeneity contributed significantly to the Person-Hours (B = 1.54, p<.00), Total Evidence Volume did not (B = .004, p<.00).

Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	10.308	.313		32.937	.000
	TotalEvidenceVolume	.004	.000	.457	29.804	.000
	Heterogeneity	1.539	.089	.265	17.264	.000

a. Dependent Variable: PersonHours

Table 9

Table 10 below shows further explanation of the results. Table 10 shows that most of the cases spent between 11 to 42 hours in investigation process. The scatter plot in Figure 16 shows the moderate correlation between the Heterogeneity of Evidence Items per Case and Person-Hours.

As a summary, an analysis of data concerning the second and third hypotheses shows that Heterogeneity of Evidence Items effects the time of investigation (Person-Hours). There is a moderate relationship between the predictor variable Heterogeneity of Evidence Items and the outcome variable where an increase of the predictor variable will result in increase of Person-Hours of investigation. As this is only moderate, we can conclude that there are also other factors that affect the Person-Hours of investigation.

Total Evidence Volume Person Hours	**.75 to 2.5**	**2.5 to 4**	**4 to 8**	**8 to 19**	**19 to 48**	**48 to 96**	**96 to 768**	**1000 to 8000**	**Mean**
1 to 10	22	41	25	98	107	139	21	20	59.125
11 to 20	19	87	82	88	305	156	198	39	121.75
21 to 30	9	58	29	67	200	161	150	33	88.375
31 to 42	6	28	25	246	56	113	299	55	103.5
Total	56	214	161	499	668	569	668	147	372.75

Table 10.Number of Cases under categorized Person-Hours and Total Evidence Volume per Case

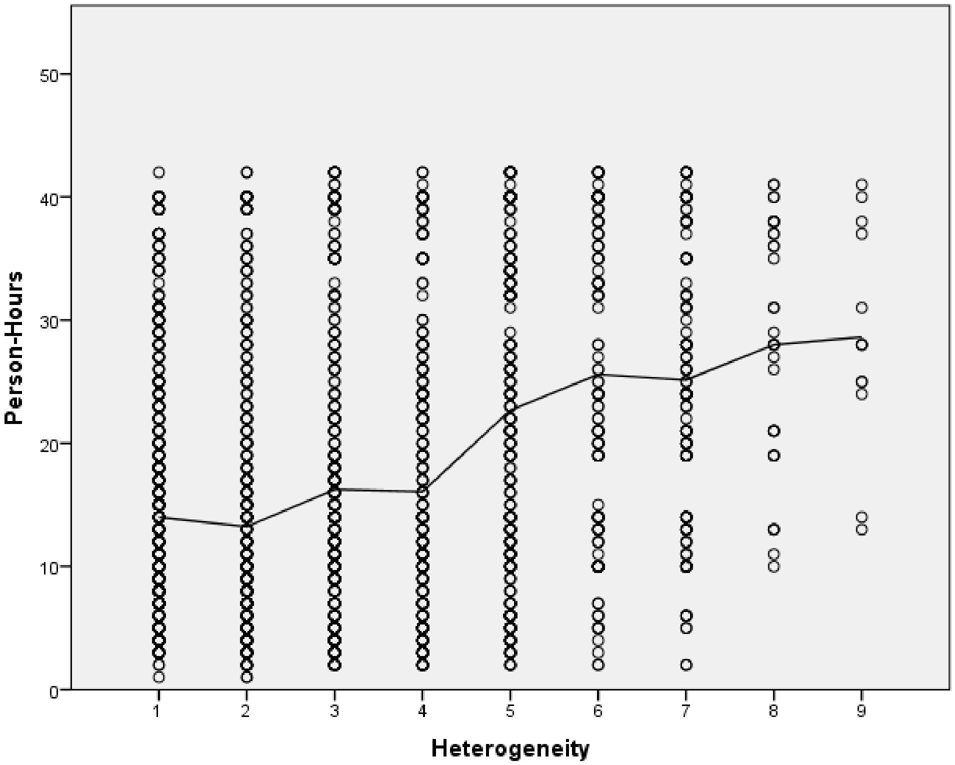


Figure 16.Person-Hours and Heterogeneity

5.2.4. Observations Exploring Factors Behind Lengthy Person-Hours

The researcher wanted to understand the data better and conducted a series of three observations. These observations highlight, by statistical methodology, several factors (predictor and outcome variables) that might increase Person-Hours. It was noted above that Person-Hours appeared to increase as the heterogeneity of evidence items increased but, as shown in the regression equation above, additional factors must also influence the Person-Hours. These additional factors may include the Number of Evidence Items per Case, Workstation Specifications, Digital Forensic Tools Version and Availability, Number of Examiners Working per Case, Examiner Experience, Complication, and the Availability of Case Details. The potential increase in Person-Hours is likely to be a result of a combination of these factors. The following observations represent some of the researcher’s assumptions.

5.2.4.1. Observation 1 – Evidence Volume does not correlate with Person Hours

It is noticeable from Table 10 above that there are cases where the Total Evidence Volume per Case varied while Person-Hours were similar. To study this, the researcher decided to examine cases with quite different Volumes and see how the Person-Hours varied.

The researcher applied several filters on the [DATASET 2] to select only these records of cases with a Total Evidence Volume per Case equalling 4 GB or500 GB. The researcher selected this filter of records as she had worked previously on several cases with those two Total Evidence Volumes per Case and had observed, in her work, that these had similar Person-Hours of investigation. The filter resulted in1,098 records out of 3353 records being included in the examination. Figure 17 below shows the Person-Hours per Volume of the evidence items at 4 GB and 500 GB.

An independent samples t-test was conducted to compare Person-Hours for Total Evidence Volume per Case of 4 GB and the Total Evidence Volume per Case of 500 GB. There was no significant difference in the Person-Hours of investigation for Total Evidence Volume per Case 4 GB (*M*= 18.91, SD= 9.56) and 500 GB (*M*= 20.59, SD=13) Conditions; *t* (547) = -1.53, p=.126.

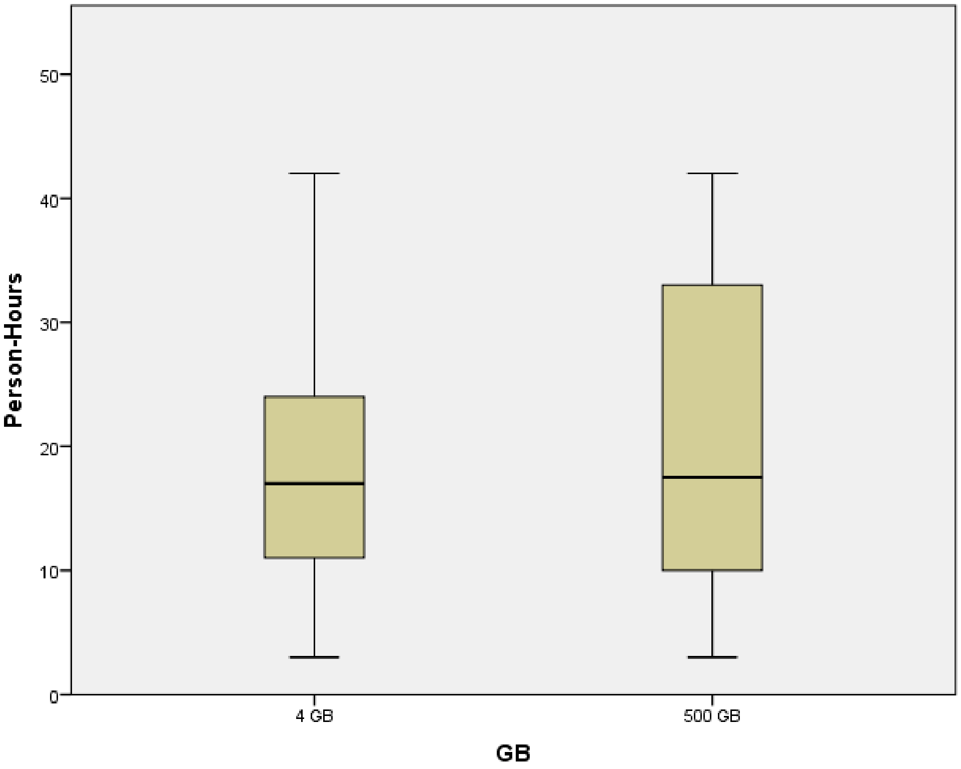


Figure 17.Person-Hours and Total Evidence Volume per Case

By analysing each group, the researcher found that most of the cases with Total Evidence Volume per Case of 4 GB were received between the years 2003 to 2011, and most of the cases with 500 GB Total Evidence Volume per Case were received between the years 2012 to 2014.

That there was no significant difference, suggests that over time, other influences have helped keep the Person-Hours low. This is likely to be a result of several factors, including better workstation specifications, more effective triage, improved digital forensic tools, and better digital forensic practitioners' experience. These improvements could explain the circumstance of spending a similar total number of Person-Hours in cases with Total Evidence Volume per Case of 4 GB and 500 GB.

5.2.4.3. Observation 2 - Experienced Examiners are more Efficient

One explanation for what is seen in Observation 1, is that examiners with more experience are faster at dealing with cases. To test this, the researcher chose to look at cases with a controlled (512GB) Volume and look at the effect of examiner experience. To study this, it was important to only look at records of cases with a single examiner working per case [DATASET 3] and to look only at a single year, given that the year was known to have an effect. 2013 was chosen as a suitable year to examine as the researcher was aware that in that year there was a range of experience across the DF team in the Dubai Police. 512 GB was selected as this was the most common volume in that year.

The researcher identified 255 records meeting the criteria. The Mean of the Person-Hours was (*M*= 92.95), minimum value of the Person-Hours = 20 and the maximum value = 300. The Mean of the Experience (in years) was (*M*= 6.79), the minimum value of the experience is 2 and maximum is 10.

An analysis of those records revealed that there is an effect of experience on the total number of Person-Hours as shown in the Box and Whisker graph in Figure 18 below. The Figure clearly shows that examiners with 2 and 3 years of experience spent more time in Person-Hours than the other examiners, while examiners with more than 7 years of experience spent the least amount of time in Person-Hours on investigations. So, examiners with few years of experience (2, 3 and 4 years of experience) spent more time in investigation than the rest of experts.

A one-way ANOVA was conducted to compare effect of the Experience on the Person-Hours. An analysis of variance showed that the effect of Experience on Person-Hours was significant, F (8, 246) = 7.97, p= .000

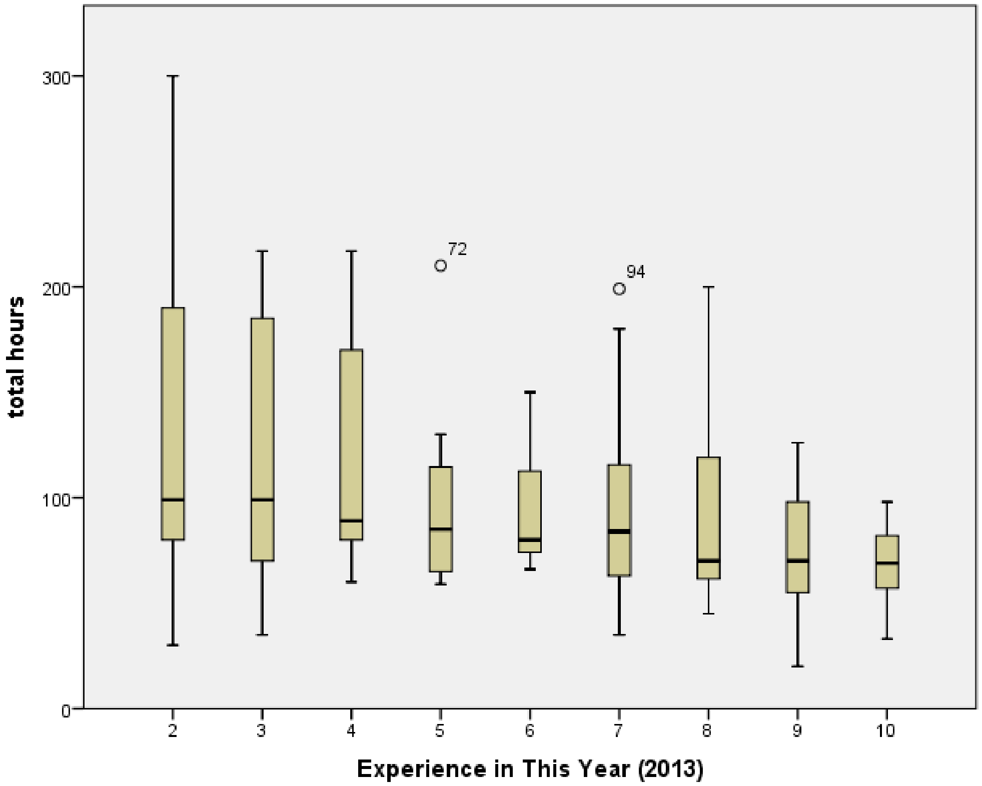


Figure 18.Person-Hours and Examiner's Experience in Years

5.2.4.4. Observation 3 – The Effect of Detail

DF practitioners know well that the amount of details that come in the case request to describe what is required from the examiner to search for in the case affects the Person-Hours. The researcher assumed that examiner could investigate cases with more details and specifications faster than cases with general or only little information. This observation intends to understand the effect of the case details variable on Person-Hours. To eliminate the confound of multiple investigators working on a single case, the researcher again used [DATASET 3] to conduct this observation.

For purposes of the observation, the researcher added the Case Request details field in the Database to designate the amount of information in a case request the DF Department received. To populate this field, the researcher used the case request description. Case details values could be either specific or general. "Specific" indicates that the case request had specific request details. For example, the case request could ask for a specific type of file in the hard drive to check if it exists or not, or the case request could provide the DF examiner with personal details of the criminal. On the other hand, "General" referred to cases with general information in the request details. One example is to ask the DF examiner to extract all the personal pictures from the hard drive without specifying the age or gender. Another example is to ask for extracting evidence, which indicates that the owner of the hard drive committed a fraud crime without indicating specifically what type of fraud crime has been committed.

For this observation, the researcher set the following filter to get 658 records (280 records for General and 378 records for Specific) the records are identical in the following variables: Total Evidence Volume per Case is 512 GB, Number of Evidence Items per Case is 1, single examiner, all cases that include a Mobile Device, and cases received in the year 2014. Those criteria were selected as 2014 was the most recent year in the DB records. The rest of the filters were chosen as they represented the most records complete in the Database, in other words, they allowed a useful and large enough sample of controlled records to be compared.

As shown in Figure 19 below, there did not appear to be a difference in the time taken according to the Case Details. An ANOVA test was conducted for equality of two variances of General and Specific to indicate if the Person-Hours differs between cases with General details and cases with Specific Details. There was a significant effect of the Details (General, Specific) received in a case, p level < .05 for the F (1,656) =3.99, p=.046.

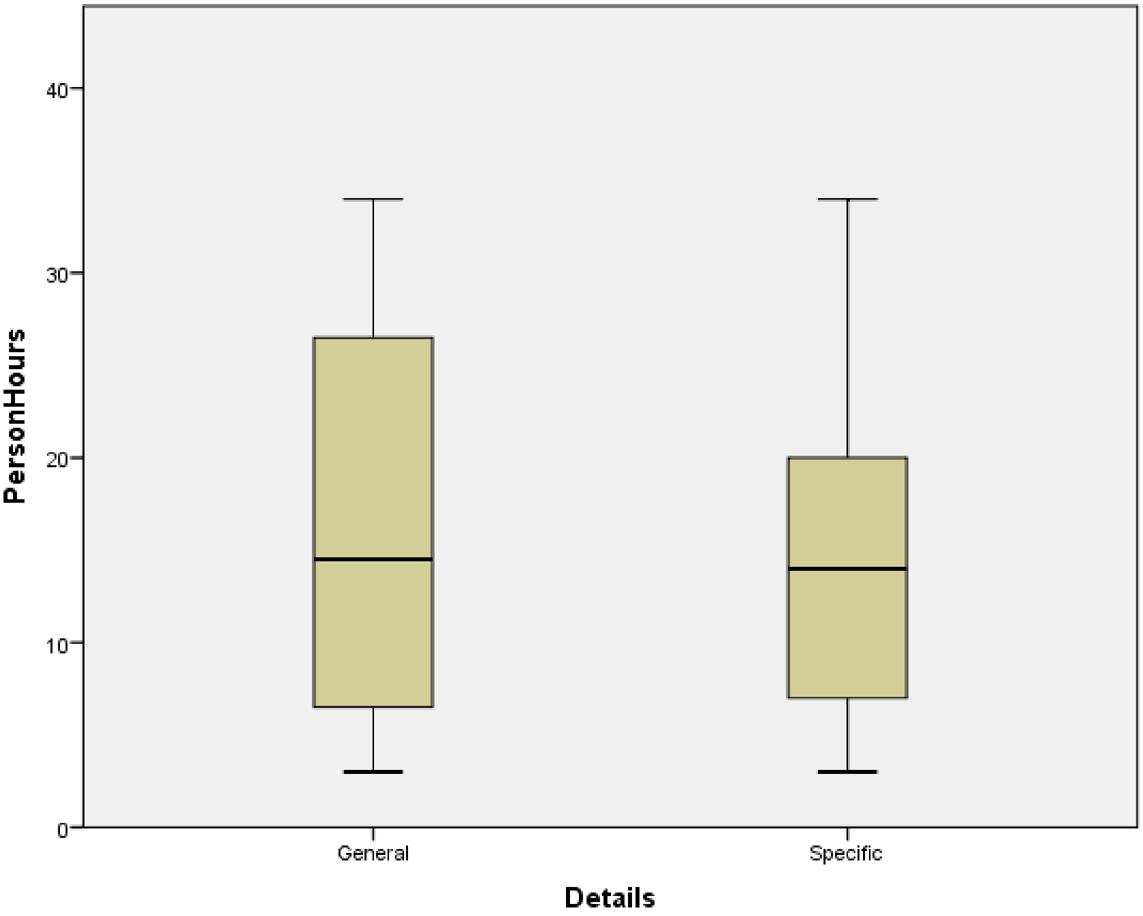


Figure 19.Person-Hours and Case Request Details

From Figure 19, it is noticeable that there is greater variance in Person-Hours for the cases with General details compared to the cases with Specific details. When the case request comes well specified, the examiner can target the required evidence easily from the investigated device. However, if the case request provides little information or only general information, then the digital forensic examiner will spend more time extracting everything that he thinks might be relevant to the case.

5.2.4.5. Observations Overview

As a summary, the observations suggest that while Volume is rising, the Person-Hours needed are staying the same. Heterogeneity of Evidence Items seems to be a partial predictor of expanded Person-Hours. That Person Hours hasn’t expanded in correlation with rising Volume is probably as a result of other factors that speed up elements of the DF process. From the small follow on studies reported here, there appears to be an effect of the Experience of the investigator, and of the Detail included in the request for investigation, on Person-Hours.

5.3. Study Two (Interviews with DF managers) Analysis

This study aimed to highlight intensively the different factors and trends likely to affect the Person-Hours of DF investigations. As you may recall, Study One (Investigation of the Dubai Police Records) analysis found that the Heterogeneity of Evidence Items per Case affects the time of investigation moderately. The researcher's further observations conducted in Study One (Investigation of the Dubai Police Records) analysis suggested that Experience of the examiners had an affect whilst also pointing to changes over time, with improved technology and tools that may be speeding up the process of investigation, even as Volume is increasing. In this regard, Study Two (Interviews with DF managers) aimed to extend the researcher’s understanding of the various factors that may affect Person-Hours in DF investigations.

Study Two (Interviews with DF managers) also aimed to understand the context of work in various government and private digital forensic laboratories in different countries. The researcher illustrates the status of work processes in those laboratories. Study Two discusses the different strategies of assigning digital forensic cases among examiners. The study exemplifies the different implementation practices of the workflow processes that different DF departments or organisations adopt. Study Two, therefore, also aims to help the researcher understand the bigger picture relating to workflow.

The main contribution of this study is to bring together decision makers from different experiences and backgrounds to exemplify various strategies of assigning and managing cases. The study also obtains reflections from professionals in the field, to identify the main factors affecting the Person-Hours of investigation, and to suggest ways to overcome those effects. This study utilized the guidelines suggested by Moustakas for the phenomenological analysis procedures of interview data (Moustakas, 1994).

5.3.1. Phenomenological Reduction

As preparation for the phenomenological reduction, the researcher started with transcription which made it handy for the researcher to note what is important. Then, the researcher listened to the entire interview to obtain a general sense of the whole interview. Afterwards, the researcher read the interview transcript in its entirety (Appendix 5) before re-reading the transcript to divide the data into meaningful sections or units in order to cluster units of relevant meaning. Later, the researcher eliminated redundancies and then conducted the horizontalization, which is when the researcher took significant statements from transcripts to describe elements of experience in the phenomenon.

5.3.2. General Description of Data

The researcher interviewed twelve DF managers from both government and private sectors from seven countries. These included:

a. United States of America (Delaware State Police, Georgia Private Investigator, Bunting Digital Forensics, Berryhill Computer Forensics)
b. United Kingdom (Competition and Markets Authority, CYFOR)
c. Sweden (Athena Labs)
d. Kingdom of Saudi Arabia (Computer Crimes at Public Security General Directorate of Criminal Evidence Computer Forensics)
e. United Arab Emirates (Computer Emergency Response Team in Dubai, Abu Dhabi Police Digital Forensics Department).

The researcher listed only the managers who approved sharing their information in this study. However, two government DF departments requested to keep their name anonymous.

5.3.3. Transcription of Interviews

The researcher personally transcribed and analysed the interviews. Listening to each interview repeatedly helped the researcher understand what the participants experienced while being a leader of a DF department or organisation, and the researcher became familiarised with how the participants experienced the phenomenon. When reading the transcripts, the researcher made sure to apply the phenomenological process of Epoché (Appendix 1) shows the process.

5.3.4. Data Analysis

The data analysis started with horizontalization. In horizontalization, the researcher coded the data from the interview transcripts into meaningful statements. As the researcher used semi-structured interviews in this study, the transcripts included some unrelated data which was eliminated at this stage. The collected meaningful units from the interviews were the source of textural descriptions. Then, the researcher developed the structural descriptions from the textural descriptions by deploying imaginative variation (Moustakas, 1994). This research included twelve textural descriptions and twelve structural descriptions (Appendix 6 & 7). Later, the researcher created a single composite textural description and a single composite structural description. Reading through the data analysis processes shows that the researcher built on and interconnected each step to the next one.

5.3.5. Data Horizontalization

The first step in the phenomenological reduction process is horizontalization of the data. The researcher identified the significant statements from the transcripts to provide information about the experiences of the participants. According to Moustakas, "these significant statements are simply gleaned from the transcripts and provided in a table so that a reader can identify the range of perspectives about the phenomenon" (Moustakas, 1994). The researcher freed her mind when examining each statement. Those meaningful statements are the horizons or as Moustakas described as "the textural meaning of the phenomenon" (Moustakas, 1994).

5.3.6. Meaning Units or Themes

As every significant statement has equal value, the researcher started the reduction and elimination process to quantify any irrelevant, repeated or overlapped statements. All the remaining statements are the horizons. As Moustakas recommends, a researcher should follow two questions in this process. Those questions are as follows: "Does it contain a moment of the experience that is a necessary and sufficient constituent for understanding it?" and "Is it possible to abstract and label it?" (Moustakas, 1994). All the horizons for each participant met these questions and created the invariant constituents of the experience. It is important to mention in this stage that the researcher conducted all the processes following the participants' descriptions rather than the researcher's own perceptions.

The next step is to use the results from the horizontalization to reveal structural elements that defines each experience. First, the researcher clustered the invariant constituents into meaningful unites or themes. In this stage of the reduction process, the researcher carefully clustered all the invariant constituents. The researcher identified the themes by combining similar content to analyse the phenomena in DF management through understanding the implementation practices of the workflow processes in each DF government department or organisation.

5.3.7. Imaginative Variation

The researcher started the process of free imaginative variation by determining which of the integrated meaningful units are essential for and made up of a fixed identity for the phenomena in the study (Dowling, 2007). Both context and setting influence "how" the participants experienced the phenomenon. The researcher then elaborated the findings from the process of free imaginative variation.

This step-in data analysis emphasises each participant's individual experiences. The researcher gathered and categorised all the invariant constituents for each of the twelve participants in the study.

The researcher then provided a description of what was experienced in the textural description, and how the participant experienced it in the structural descriptions. Each of the participants will have one textural description and structural description. Thus, this study resulted in twelve textural descriptions and twelve structural descriptions.

In the textural description, Moustakas advised to use the participant's own words to ensure the perceptions of the phenomenon investigated (Moustakas, 1994). In this study, there were twelve individual textural descriptions.

5.3.8. Synthesis

The researcher synthesized both textural and structural descriptions of the experiences to build the composite description of the phenomenon, which Moustakas refers to as intuitive integration (Moustakas, 1994). This description is the core that captures the experiences and describes the phenomenon of the work process in DF departments or organisations.

5.3.9. Composite Textural Description

The final step in this transcendental phenomenological study was to write the composite textural and structural descriptions. The aim here is to identify the working process in the DF departments or organisations and to have a better understanding of the difference between government and private sectors. This section describes the composite textural description relating to (1) the context of work, (2) case assignment and management, and the workflow, and (3) challenges and suggested solutions.

5.3.9.1. The context of work

All the participants in the study were heads or managers of a DF department, section, or organisation. The researcher interviewed seven from the government sector and five from the private sector. All participants had experience in one of the computer science fields in the range of 11 to 22 years and in the DF field in the range of 9 to 20 years.

Out of seven digital forensic government departments, only two are not satisfied with their yearly budget, and stated that there is never enough budget to support their department requirements from new forensic devices, licenses, and training programs. In the private sector, it is slightly different, as the DF organisation will bill completely to the client the required budget for any investigation.

All the government and private sectors have no recognized accreditation requirements when hiring or promoting any of the DF practitioners. At the time of hiring, the government departments usually depend on the type of education the applicants have. They are flexible in hiring employees who have related certificates. They do not always require experience; fresh graduates can work directly in any of the government DF departments. However, some government departments require that no civilian employee may be hired, and they can only hire police officers whenever there is a vacancy. Private companies are stricter about hiring DF examiners. They usually look for examiners with experience, and rarely hire fresh graduates.

Most government departments provide clear prerequisites for the examiners to transfer from an entry level to a higher level of pay, skills, authority or responsibility. The requirements include the Number of Cases the examiner has previously completed, the types of cases the examiner previously worked on, the training programs the examiner has attended, and the number of examinations or tests the examiner has passed. In contrast, four out of five private companies interviewed do not have a clear career ladder for their DF examiners.

ISO 17025 (Watson & Jones, 2013) accredits the general requirements for the competence of testing and calibration laboratories. Only two government departments obtained ISO-17025, and two are in the process of obtaining the certificate. However, all the private organisations obtained this accreditation.

All the government and the private departments or organisations work on both civilian and criminal cases except for two (one from the government and one from the private) that work only on civilian cases. Government departments either generate their own cases by searching for predators, hackers, policy violators, and so on; by trolling social media applications; reviewing reports; or receive cases from other sources such as police stations, public prosecutions, defence sector, attorneys, and criminal investigation department. Private companies do not create their own cases; they receive cases from different sources like the defence sector, attorneys, and individuals.

5.3.9.2. Case assignment and management, and the workflow

The case assignment and management processes in both government and private sectors match each other on fixed assets and vary in the process of implementation. Most government sectors follow similar implementation techniques, but private companies come up with a variety of implementation methods. It is true that there is no right or wrong path to assign or manage DF cases. However, familiarity with different case assignment strategies and implementation practices of the case workflow would enrich the knowledge of managers and keep them aware of other possible techniques that might help in assigning cases and managing the department.

5.3.9.3. Challenges and suggested solutions

Both government and private sectors agree that a combination of factors affect the Person-Hours of investigation. Some factors match the factors found in Study 1(Investigation of the Dubai Police records) and some do not. The researcher divided the factors identified by participants into administrative and investigative factors as discussed more fully below in section 5.3.11. Additionally, the researcher discusses below the different techniques followed by some of the departments or organisations to reduce the Person-Hours of investigation.

5.3.10. Composite Structural Description

This section describes the composite textural description relating to (1) the context of work, (2) case management strategies, and (3) the workflow implementation practices.

5.3.10.1. The context of work

All government department managers had years of experience in the field of DF, and they were promoted to reach to their current positions. Most of the managers (four out of five) in the private companies worked before in one of the government DF departments, though not necessarily with a high position, but they had obtained the requisite experience.

After gaining experience in the government sector, the participant shifted to work in a private organisation, or they started their own company.

As DF is playing an important role in most of the current cases, they are getting the highest budget among other departments. In private organisations, an examiner must obtain permission from the customer for any extra tool required or volume capacity needed to process the case, and the examiner must append the cost to the total fees.

Although there are no clear accreditation requirements for DF examiners, government departments have certain prerequisites to complete in order to progress in their career. Usually new employees are fresh graduates with a background in one of the IT fields, examiners with experience from another department or company, or employees who shifted from another department to the DF department. In the government department, the practitioner will start as a junior examiner. After a couple of years and depending on the Number of Cases the examiner worked on, the types of cases the examiner worked on, and the ability to learn all the required skills, the examiner will be examined and interviewed to be promoted into senior examiner.

On the other hand, most private organisations do not have a clear path for DF examiner promotion. Private DF organisations promote examiners after years of experience, but usually depending on the amount of time the examiner spends to extract the evidence. Thus, knowing what to examine and how to examine is important, but reducing the Person-Hours of investigation is vital in private organisations. Examiners who spend the least amount of time to examine an exhibit have a better chance of earning a promotion to senior examiner.

As ISO 17025 is applicable to all organizations performing tests or examination regardless of the number of personnel, all private companies obtained the certificate to ensure their work quality. However, most government departments that obtained the certificate, or are currently working on obtaining the certificate, have been asked to do so or their evidence will no longer be admissible in court. Thus, it is a self-development requirement in private organisations, while a compulsory requirement for government departments.

Government departments can generate their own cases if there is any suspicion of illegal activity. They can thus develop their pipeline of cases either by letting specific employees trace predators in certain companies, or over the internet. They use data mining products and other open source tools to find out breaches and generate the cases. Usually, such practices are inapplicable in private companies. Private companies usually wait for a customer request to start a new case.

5.3.10.2. Case management strategies

Managers follow different strategies when assigning cases to examiners. They have different motivations about those strategies. They even have expectations regarding their selected strategy's applicability in the future. The researcher grouped the different strategies into three main categories: (1) caseload strategy, (2) ability strategy, and (3) parallel team strategy. It is important to mention here that the strategies discussed are the manager's first option to rely on when assigning and managing cases.

5.3.10.2.1. Strategy 1: Caseload Strategy

In the first strategy, the manager allocates according to the caseload that the examiners have. Once the manager receives a case, he will read the details and identify the number of exhibits. Depending on the manager's analysis of the case, the manager will decide whether to assign the case to an individual or a team based on the number of exhibits. Then the manager will check the examiners' existing caseload. The manager will assign the new case to the examiner with the least Number of Cases.

The manager following this strategy is not paying attention to any other factor. He believes that all his employees have similar skills, capabilities and knowledge because he provides similar training opportunities to all examiners. Thus, all the examiners receive similar training programs, courses and they all have the required skills to deal with different types of cases.

From the sample, there were four departments or organisations that follow this strategy and the managers are confident about their selection of strategy. Two of them are manually following this procedure, while the other two use case management tools, which allow the managers to view the status of cases: in progress, on hold, just assigned, or completed. The case management tools make the work more convenient as they can view the examiner's progress, view the caseload that each examiner has, and select the examiner with the least number of pending cases. The examiners in those departments usually can receive up to 10 cases at a time but not more than that. The managers anticipated that they could still rely on this strategy if the Number of Cases increased doubly in the future. However, if the Number of Cases tripled in the future, they will be requiring more manpower.

5.3.10.2.2. Strategy 2: Ability Strategy

The manager using this strategy relies on the examiner's experience, skills, knowledge, capability and availability. The manager decides whether to assign the case to an individual or a team, depending on the exhibits received. The manager reads the details of the case and with the initial understanding of the case weight, type, requirements, and exhibits types; the manager chooses who is best suited to investigate the case. The researcher divided the managers who applied this strategy into two groups, depending on how the manager applies the strategy:

5.3.10.2.2.1. Group 1 Managers

Some managers check the weight of the case, whether it is ordinary or urgent. Often, managers will assign ordinary cases to junior examiners (examiners who worked in the field for less than three years) and will assign urgent cases to senior examiners (examiners who worked in the field for more than three years). Then, the manager makes the decision depending on the availability of the examiners and the number of exhibits. For example, for an urgent case with many exhibits, the manager will assign the case to a team of senior examiners, or a team of senior and junior examiners, if senior examiners are not available.

Two government departments applied this strategy. Their main motivation to follow this strategy is to improve the skills and experience of the junior examiners. The managers who selected this strategy believe that the strategy allows the junior examiners to experience different types of cases. The managers understand that junior examiners might spend more time than senior examiners, but as managers assign them the ordinary cases, it would be fine. The managers expect that this strategy will remain valid in the future with the increase in the Number of Cases and they feel that it is the best for their department.

5.3.10.2.2.2. Group 2 Managers

Some managers will directly check the experience, skills, knowledge and capability of the examiner either by checking the matrix sheet or by relying on their familiarity about the capabilities of each single examiner in the department or organisation. The matrix sheet usually includes all the experience and skills obtained by the examiners. The examiners update this sheet after each new skill learnt, knowledge obtained, or training course attended.

Five departments or organisations use this strategy. The manager's main motivational aspect for selecting this strategy is that even if all examiners receive similar courses and training programs, they have different strengths in different areas. Regardless of whether the examiner is senior or junior, the skills and knowledge obtained is the main factor. There are examiners who are very good in solving networking issues, while others are more confident working in cases with social media applications, and still others are better at working with cases that include anti forensics techniques, and so on.

Moreover, managers believe that assigning examiners the cases depending on experience will enhance the examiners’ knowledge and improve their work, allowing examiners to solve cases faster.

Of the five departments or organisations that use this strategy, only two departments use the competency matrix sheet to include all the experiences and skills of the examiners. The examiners update the competency matrix every time they gain a new skill, attend a new training course, or work on a new type of case. The competency matrix sheet makes it easier for the managers to assign the cases depending on the examiner’s experience. The managers who selected this strategy believe that assigning the cases depending on skills is the most appropriate way, as the person who has the required skills will know how to investigate and what to extract. Managers expect that they can handle any increase in future cases, and that their choice is the most suitable to their work environment.

5.3.10.2.2. Strategy 3: Parallel Team Strategy

The manager will assign each case to two teams and they will work in parallel. Each team consists of three to five examiners. Each examiner has different capabilities, experience, knowledge, skills; and receives different types of courses and training programs. Each team has a team leader. When the manager receives a case, the manager will have a meeting with all the team leaders. They will take into consideration the case type, exhibits types, examiner's experience and caseload; and they will decide which teams will receive the case.

One private company uses this strategy. They receive only high profile, big cases. The main motivation for the company manager to select this strategy is the business needs. The most important factor in a company is the time to complete the case. The company can charge higher fees for cases that the company conducts faster. Thus, the company came up with this strategy to increase competition between the employees, and the manager believes that this strategy increased the speed. The manager is satisfied with the outcome of this strategy and expects that this strategy can remain valid if the Number of Cases doubled or tripled in the future.

5.3.10.3. The workflow implementation practices

After the assigning process, the work procedure starts. Each department or organisation has its way to manage cases. Before illustrating the different implementation practices of the workflow processes, it is important to exemplify the different process models. As discussed in the literature, various researchers have suggested several DF crime-scene process models and DF investigation process models. For purposes of this research, the researcher will use the DF crime-scene process model with six phases as suggested by the Massachusetts Digital Evidence Consortium (MDEC, 2015). The researcher selected the MDEC process because it represents the basic resource for law enforcement officers encountering digital evidence in different crime scenes. The details of those phases vary depending on the seized devices in the crime scene: whether they are smart phones, other mobile devices, laptops, desktop computer systems, or other digital storage evidence. A DF investigator conducts the following main steps at the crime scene after obtaining the search warrant:

1. Document the evidence items and all collection procedures and information.

a. Photograph

b. Video

c. Sketch

d. Notes

e. Chain of custody

2. Check if the device is on or off.

3.If the device is off, do not turn it on.

4.If the device is on, proceed with caution.

5.Collection and package.

a. Collect the power cables

b. Consider collecting devices that may contain backups

c. Ensure physical security from any damages of collected items

d. Transport by protecting all the evidence items from any damage and deliver it to the secured law enforcement facility as soon as possible.

For the DF investigation model, the researcher selected the DFRWS model, as it is the main model that researchers based most other derivative models (Yusoff et al., 2011) (Palmer, 2001). This model has six main processes and they include the following:

1. Identification: identify an incident and determine its type.

2. Preservation: include tasks such as

a. Set-up proper case management.

b. Apply different imaging technologies.

c. Ensure acceptable chain of custody.

3. Collection: The examiner collects relevant data by using approved methods, software and hardware. The examiner also applies any sampling techniques or data reduction in this process.

4. Examination: apply different tasks such as

a. Trace and validation techniques

b. Apply filter techniques

c. Uses pattern matching

d. Discover and extract any hidden data.

5. Analysis: Uses data mining techniques and link the findings.

6. Presentation: include tasks such as

a. Documentation

b. Expert testimony

c. Clarification

d. Mission impact statement

e. Recommended countermeasure

f. Statistical interpretation

All the departments or organisations apply the main processes of crime scene and investigative process models. This section highlights the practical implementation of those processes, and who is responsible to perform them in different departments or organisations. The researcher grouped the different organisational workflow implementation practices into five categories: (1) traditional workflow, (2) team workflow, (3) parallel team workflow, (4) outsourced workflow, and (5) tiered workflow.

5.3.10.3.1. Traditional Workflow

In the traditional workflow, the examiner or team that receives a case is required to work on the case from start to the end. The examiner will be responsible for the crime scene and investigation processes, which include documenting the evidence items and all collection procedures and information, checking if the device is on or off, collection and package, transportation of evidence, identification, preservation, collection, examination, analysis and presentation. Seven departments or organisations use this procedure.

5.3.10.3.2. Team Workflow

In the team workflow, the manager assigns the case to one examiner or a team of examiners with a case leader using one of the case assignment strategies discussed previously. However, the entire lab will participate in the crime scene processes. They will also conduct the identification and preservation processes of the DF investigation model.

The case leader assigned to this case will be responsible for continuing the rest of the process of investigation, which are collection, examination, analysis and presentation. At the site, each person has a different role. For example, one examiner will take photographs and videos of the scene and evidence seized, while another set of examiners, assigned to different rooms in the scene, will be responsible for collecting all the evidence items from the assigned room. They start previewing and collecting the evidence items.

The case leader applies a set of rules on what to collect from the scene, and what to leave. Once the case leader and his team have seized a couple of exhibits from the scene, they can go back to the lab and start working on those evidence items. The rest will remain at the crime scene and continue to collect evidence items and seize all the desired exhibits. Upon return to the lab, the team will start a forensic duplication process. As the team is connected in a secure internal network in the lab, they all put the forensically duplicated files in one case so the lead investigator and his team, once available, can start the collection and examination. They will bookmark data, conduct keyword searching, prepare the forensic report, and later they will be responsible for the persuasion and testimony. This process is a total team effort when conducting search warrant and pre-processing of the exhibits, but in the examination and analysis stages, the process goes back to the team in charge of the case. One government department uses this procedure.

5.3.10.3.3. Parallel Team Workflow

In the parallel team workflow, two teams compete and are rewarded based on team performance. The examiners will receive the evidence items, and they will not go to any crime scene. They only accept big cases with plenty of evidence items. Their most important factor when dealing with each case is the time spent to examine the case. For each case, they assign two teams consisting of three to five members in each team. Both teams will receive similar forensically sound images of the case evidence items. Those two teams are opposing each other. Both teams have members with different skills, background and experience. They will work in parallel to extract the evidence items. The team that extracts the evidence faster will gain the bonus from that case. There are times where one team reaches 40 percent of the case and the other team reaches another 60 percent of the case. In this situation, the manager can let both teams combine their findings and they will share the bonus depending on the percentage of findings they accomplished, per Figure 20 below. There is one private company using this procedure.

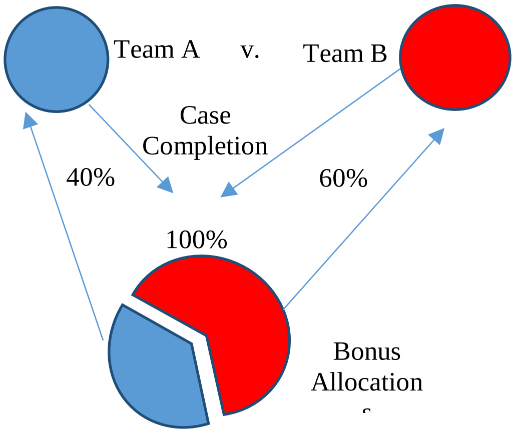


Figure 20. Parallel Team Workflow

5.3.10.3.4. Outsourced Workflow

In the outsourced workflow, the manager will outsource to, or have the work done externally by, a contractor examiner or a team as required. Contractor examiners have their own business or work, and the manager will contact them depending on their skills and experience related to the case. Moreover, the examiner will not go to the crime scene, but will receive the evidence items in the examiner's department or organisation. The DF department or organisation has a matrix sheet of their examiners' experiences and capabilities. The DF department or organisation selects the preferred examiner to assign for that specific case. After selecting the most suited examiner, the DF department or organisation will contact the examiner to discuss the case, and if the examiner agrees, the DF department or organisation will assign the case. The examiner will receive the forensic duplicated files and start the pre-analysis, analysis and post-analysis phases. Upon completion, the examiner submits the results back to the DF department or organisation. One organisation applies this procedure.

5.3.10.3.5. Tiered Workflow

In the tiered workflow, managers assign simple tasks, such as conducting the forensic duplication process, to all the junior examiners. Afterwards, the junior examiners will load the case into the server and the senior examiners will complete the collection, examination, analysis and presentation. The junior examiners could be involved in other processes for training purposes. However, the senior examiners conduct the main tasks, per Figure 21 below. One government department applies this procedure.

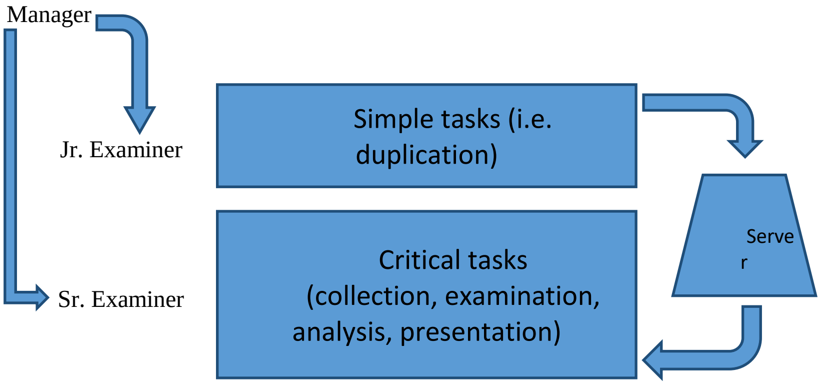

Manager
Jr. Examiner
Sr. Examiner
Simple tasks (i.e. duplication)
Critical tasks (collection, examination, analysis, presentation)
Serve
r

Figure 21.Tiered Workflow

5.3.11. Factors behind the lengthy Person-Hours of investigation and suggested solutions

Besides case assignment and case management, managers are responsible for maintaining reasonable Person-Hours of investigation. The managers noticed different factors that affect the Person-Hours of investigation. The researcher divided the reasons behind the delay in investigation and lengthy Person-Hours into administrative factors and investigation factors

5.3.11.1. Administrative Factors

The participants indicated many administrative factors that cause delay in investigation. One factor is staffing fluctuations or shortages due to holidays, absences, sick leaves, or attending conferences and training courses. The managers also agreed that cases assigned to one examiner would consume more time than cases assigned to a team, a direct effect of case management and case allocation strategy.

Managers also noticed that the length of time in receiving the exhibits might cause some delays. Typically, when the DF department receives a case, the DF department has not yet received the exhibits because transferring the exhibits from one department to another takes time, approximately two days. Such inter-department processes cause additional delay.

Another administrative factor is the time it takes to receive the case description from the public prosecution. There are many times where the case request is made but the report from the public prosecution takes a couple of days to append. Some participants mentioned that if the case descriptions and requirements were clear for the examiner, the findings would be faster and more critical. However, if the examiner were given less details about the case requirements, the practitioners will spend more time to extract the evidence.

Moreover, managers had different views regarding the relation between the experience of the examiner and the Person-Hours of investigation. Some managers believe that examiners with 3 years and above spend a similar amount of time in DF investigations. They receive similar training programs and have similar skills and backgrounds. Other managers see the variation in time spent in investigation depending on experience. Examiners with less than 3 years of experience take more time than examiners between 3 to 7 years of experience, who in turn will spend more time than examiners more than 7 years of experience. Other managers suppose that experience does not affect the amount of time spent in DF investigations. They gave examples of cases that require specific skills that the beginner examiner just studied in university, giving the examiner with less than 3 years of experience the advantage to conduct the investigation faster than other practitioners who will spend time searching and learning about the specific skill. Thus, some managers believe that regardless of the experience, skill, knowledge or background a DF practitioner possess, they will nevertheless face novel challenges as the DF field is developing rapidly.

5.3.11.2. Investigative Factors

The participants mentioned several investigative factors like DF workstations and tools, specialized DF challenges, the volume of exhibits, the Heterogeneity of Evidence Items per Case, and number of exhibits.

Most participants agree that the development of the forensic workstations and tools increased efficiency and reduced the time of the investigation. For instance, examining a 1 GB a hard drive in 2008 would take longer than today. The speed of computers and the volume of data are chasing each other. Thus, as technology develops, data storage increases. In the early days of DF, participants used to receive exhibits with megabytes of storage, then, it increased to gigabytes with most exhibits, and nowadays most cases come with terabytes of storage.

However, participants also noticed that the capability of DF software tools affects the Person-Hours of investigation. They find that several tools struggle when they pass a specific volume or amount of data. For example, Xways struggles past 15 million documents/images/messages.

Moreover, cases with anti-forensic techniques, cloud computing, password protected files/drives/mobiles, social media applications, and the uses of network intrusions usually cause delay in the DF investigation as they require special handling techniques.

To reduce the length of time the investigation takes, participants use a variety of techniques to trim down the Person-Hours. Some departments spend days on-site trying their best to reduce the number of seized exhibits. These departments conduct several processes on-site like preview, triage and elimination of evidence items. They would use Nuix portable or other portable tools on- site to conduct initial keyword searches to decide whether they need to seize the device or not.

Other departments use a tiered structure of technicians to manage and start pre-processing the evidence items. Thus, once the case reaches the examiners, technicians have already done all the pre-processing.

Case processing methodologies were used in some places to reduce the time of investigation. The organisations using this are developing the case process methodology as they go along. Such a methodology could suggest the best way to solve each specific case type with a certain volume/type and number of evidences. Thus, all their examiners will follow the suggested case process methodology. They are currently developing the best process methodology to solve cases that include cloud computing.

Some departments studied the capability of current DF software tools. These departments know that a case exceeding a specific data volume will slow down the software tool during examination. They suggest splitting the case into two and putting the data into two analysis machines for faster results.

5.4. Study Three (Confirmation of the Interviews) Analysis

The aim of this study was to generalise the findings and evaluate the outcome from Study Two (Interviews with DF managers). The researcher conducted Semi-Structured Email Interviews with participants to evaluate the applicability of different case allocation strategies and case management procedures, which the researcher analysed in Study Two. The research highlighted the pros and cons of the different strategies and procedures. In general, this study uses the deductive approach to analyse the data collected.

The main contribution of this study is to evaluate the findings from the previous study, and to introduce a set of Decision Tables that could be beneficial for new managers working in the field and facing similar situations.

5.4.1. Deductive Approach

This study uses a deductive approach to analyse the data, with the aim of evaluating the findings from the second study.

5.4.2. General Description of the Data

The participants had all participated in Study Two (Interviews with DF managers). However, not all the participants from Study Two participated in Study Three (Confirmation of the Interviews). Seven participants replied and completed the emailed semi-structured interview. They are all managers working in public or private sectors of DF departments or organisations. Participants are from different countries including the United States of America, United Kingdom, Kingdom of Saudi Arabia, Sweden and United Arab Emirates. The researcher listed above only the managers, who approved sharing their information in this study. Two government DF departments requested to keep their names anonymous.

5.4.3. Analysis of Data

The researcher used the deductive approach in this study to provide reasons for the strategies and implementation practices employed in the previous study and to reach a logical conclusion. Since the researcher used a semi-structured email interview in this study, the researcher did not need transcription of the emails received from the participants after they answered the Confirmation Questions. The Data coding was therefore the first step the researcher conducted using the interview transcripts. One benefit from this type of interview is that answers tend to include information that is relevant to the study so not much irrelevant data was found. Thereafter, the researcher conducted the analysis of the data. This section discusses the analysis of the data within the framework of these two hypotheses.

The researcher dedicated the first portion of the third study to identifying the opinion of managers regarding the different case allocation strategies used by different DF departments or organisations. Then, the researcher wanted to determine whether managers would be enthusiastic in changing their case allocation strategies. The researcher also aimed at identifying the different factors that influence managers to change their routine strategy.

As discussed above, managers tended to use three strategies for case management: (1) caseload strategy, (2) ability strategy, and (3) parallel team strategy. The following points provide a quick summary of the different strategies:

1. Caseload strategy: Relying on the caseload that the examiner has. Not paying attention to experience, skills and selecting examiners with the least number of pending cases.
2. Ability strategy: Relying on the experience, skills, knowledge, capability and availability of the examiner when assigning. Some managers check the weight of the case first and see if it is ordinary or urgent then decide. Some other managers will directly check the required experience.
3. Parallel team strategy: Relying on the competition between the examiners. Each team has different knowledge, skills and experience.

For the caseload strategy, most managers (five out of seven) suggested that using the number of exhibits at the beginning of the case, as an initial factor to choose if the case will be assigned to a single or multiple examiner, improves the processing time later. They also agreed that putting experience aside from the decision and selecting the examiner depending on the number of pending cases is not generally a wise plan. The managers agreed on the necessity in understanding the examiner's experience when assigning a case. Even when examiners had similar background and experience, and had received similar training, there could still be differences in the implementation of their knowledge. Thus, there are examiners who will be faster, more accurate or precise when investigating a case type than other examiners with similar knowledge. Therefore, the managers agreed that they can apply a caseload strategy in their departments or organisation as an initial decision factor, abut would favour later combining it with the experience factor. One example that was mentioned was where a case can be assigned to an examiner, with the least number of pending cases and least experience, for training purposes. In this way, the manager can improve the skills of an examiner in a specific area when the examiner has a small caseload.

The second strategy, the ability strategy, focusses on the experience, skill, knowledge, capability and, to a lesser extent, the availability of the examiner. The rationale for choosing based on experience is that experienced staff will typically be quicker and more thorough than their less experienced counterparts. These two motivations suggest two variations.

In the first variation, the urgency of a case is the driving factor. In these instances, the managers check the urgency of the case and assign urgent cases to the senior examiners and normal cases to junior examiners. Six out of seven managers reported that they would apply this type of strategy with urgent cases as it is highly effective and is also a good decision because the senior examiners have the experience to deal with the external and internal pressures that come with those types of cases. That said, the managers also suggested that junior examiners need to, at some point, be exposed to urgent cases in order to be able to deal with them appropriately when they become senior examiners. Thus, urgency would typically suggest a decision based on ability.

A second approach to case management based on ability is to consider the skills of the examiners. In this case the manager considers the case and directly evaluates the required experience, skill, and knowledge, before deciding on the best-qualified examiner to handle the case. Four of the seven managers questioned considered experience, skill and knowledge to be a core factor to consider when assigning cases. Interestingly, these four managers had teams with examiners of roughly equal ability and skill. The other managers felt less able to apply this strategy, because training junior examiners and giving them the chance to develop their knowledge, was vital for their work situations. Thus, they might almost take an alternative approach and evaluate the case and try to distribute the cases in a way to enhance the examiners' skills.

The third strategy that was considered in Study Three was the parallel team strategy, where two teams were given the same case and they worked in competition. Most of the participants (6 out of 7) rejected this strategy. These considered that this type of strategy could not be applied in their workplaces as it overuses resources and wastes manpower in duplicative work. Moreover, these managers opined that if they were to apply this strategy it would increase the pending case list. The manager who felt this strategy could be applied thought it could possibly be used - he suggested having two small groups try it on urgent cases to see if this sped up the investigation process.

From analysing the collected data, the researcher found that most managers had a preferred strategy and that they used this most of the time. However, some did alter their habits in the presence of factors like urgency of cases, training purposes, high numbers of evidence items in a single case, number of available examiners and the number of pending cases. The existence of one of those factors usually leads the managers to find or use other strategies, depending on different manpower, goals, visions, and work policies.

Thus, most managers are flexible to change their main strategy of case allocation depending on the factors provided by each case. As most managers are enthusiastic in changing their case allocation strategies depending on several factors.

The researcher then considered workflow as opposed to case allocation. As discussed above, managers reported five categories of workflow implementation practices: (1) traditional workflow, (2) team workflow, (3) parallel team workflow, (4) outsourced workflow, and (5) tiered workflow. These are briefly summarised here:

1. Traditional Workflow: One examiner will work on a case from start to end.
2. Team Workflow: One examiner will work on a case, but everybody in the lab will help in the crime scene and in forensic duplication/ pre-processing of the case.
3. Parallel Team Workflow: Two opposing teams will work on the same case, aiming to get the results as fast as possible.
4. Outsourced Workflow: Practitioners with contracts who have the required experience will work on the case.

5. Tiered Workflow: Basic tasks are done by some (typically junior) examiners whilst others (senior) examiners complete critical tasks.

All the managers agreed that the traditional workflow implementation practice of letting the examiner handle the case from the start to the end is good practice. This is because the examiner knows the case better than anyone else does, which should result in more coherence and consistency in the workflow. This implementation practice is also ideal for the examiner when testifying in court as he/she will know the case inside out.

Most of the managers saw few disadvantages in this practice considered that the advantages for outweighed any disadvantages. However, some managers indicated that this practice squanders the ability of senior examiners with routine tasks that managers cold better assign to junior examiners or technicians. For those managers who were not using this implementation practice, they gave positive feedback about it as a practice but did not think that it was a possible option for them to apply in their department. They cited the single case allocation as being time consuming for the senior examiners, who they preferred focusing just on critical tasks regarding the case.

The second implementation practice, full team workflow, requires the examiner and his group, if available, to work on a case, with the entire lab going to the crime scene and helping in the acquisition and initial previews of the case. None of the managers questioned applied full team workflow. They all could see some positives in this practice, like the ability to eliminate any unrelated exhibits because everybody is involved in this step. Thus, the team will immediately know which exhibits need full investigation. At the same time, they could not see how it could be applied in their departments or organisations. Managers explained that they seldom went to crime scenes, more usually receiving exhibits in their labs except for cases that require live investigation. Moreover, some departments consisted of 80 or more examiners, working on numerous cases that could not be put on hold pending examiners going to the crime scene. Additionally, many managers had cases arriving daily so team workflow would be difficult to schedule.

In the third implementation practice, the parallel team workflow, the process consists of two teams competing. Only the manager already implementing this technique, saw any advantage of using two opposing teams to conduct the same job and to create a competition environment for the investigator to speed up their investigation processes. Others thought that this practice is insufficient and impractical. It consumes time in duplicative work; it also consumes limited resources and budget. One of the participants said that this practice could only be implemented in one way, by evaluating the work of one team against the other for training purposes. However, in real work it is still very difficult to facilitate. Implementing the parallel team workflow seems to likely result in counterproductive results and not to any productive outcome.

Outsourced workflow was the fourth practice; all the participants agreed that dealing with contractor examiners could add great value especially with cases that include device items that are new or with which they are unfamiliar. Two of the managers were already partially implementing this practice. These two mainly took advantage of somebody's experience, using outsourcing in specific cases. Other managers mentioned that the implementation of outsourced workflow would be impossible as their policy allowed only law enforcement staff to be in the lab and work on cases. It was noted by some managers that they might like to do this but did not have trusted, licensed examiners to outsource to, making it difficult to implement the practice.

In the last implementation practice, the tiered workflow, the manager assigns basic tasks such as acquisition, preview, and keyword search to the junior examiners and the senior examiners conduct the critical tasks like the advanced search, analysis, writing of the report and testifying. All the managers found many advantages of this practice. The junior examiners would be able to develop their basic skills by conducting the basic tasks in the cases and the dyad of senior and junior examiner one case would lead to exchange of skills. All the managers who responded to the questions agreed that they could try the tiered workflow in their departments or organisations with some of their cases so they could assess the benefits. It was noted that this approach could be counterproductive as it was also important for junior examiners to work on the more critical work to gain experience.

5.5. Summary

Chapter 5 discusses the hypotheses and observations from Study One (Investigation of the Dubai Police Records), the use of the phenomenological methodology to analyse qualitative data in the second and third studies, and the use of the deductive approach in Study Three (Confirmation of the Interviews).

In Study One (Investigation of the Dubai Police Records), the observations suggest that while Volume is rising, the Person-Hours needed is staying the same, probably as a result of other factors that speed up elements of the DF process. There appears to be an effect of Experience and details given on Person-Hours.

Study Two examined the types of case assignment and case management strategies and discussed the reasons behind the delay in investigation and lengthy Person-Hours into two factors: administrative and investigation.

Finally, Study Three (Confirmation of the Interviews) evaluated the findings from the previous studies and introduced a set of Decision Tables that could be beneficial for new managers working in the field and facing similar situations.

CHAPTER 6: RESEARCH DISCUSSION

6.1. Introduction

This chapter discusses the research outcomes and the relationships among the data that the researcher identified after conducting the data analysis of the three case studies in the previous chapter. The chapter begins by providing a summary of the research problem and the methodology the researcher applied. The chapter then discusses the concept of integration and synthesis and its importance in a mixed methods sequential explanatory design. Next, the chapter discusses the lessons from each of the three case studies, including a discussion of the principal findings, interpretation in the context of the literature, and implications of the case studies. Further, the chapter integrates and synthesises the three case studies. The chapter then reviews and discusses how the researcher findings have answered the research questions. Finally, the chapter proposes a series of DF case management and case allocation Decision Tables that the researcher hopes will guide DF managers and practitioners.

6.2. Summary of the Research Problem and Methodology

Before engaging in a discussion of the research and the three studies, it is necessary to summarise the research problem and the methodology the researcher applied. As stated in the first chapter, this research tackles the problem posed the different factors that causes delay in digital forensic investigation process. More specifically, the research aims to gain a better understanding on how Total Volume per Case and Heterogeneity of Evidence Items per Case may affect DF investigation delay. Furthermore, DF manager may in turn address case management strategies and workflow implementation practices to encounter the various challenges occurs by those different factors.

To understand better the research problem, the research used a mixed methods sequential explanatory design, as explained in more detail in the third chapter. The research problem required an analysis of quantitative secondary data, such as Person-Hours spent in DF investigations, to test the hypothesis that the Total Evidence Volume per Case and variety of digital data are the likely causes of DF investigation delay and lengthy Person-Hours.

However, the research also required analysis of the human, technological, and resources-based factors behind the problem, especially as the research wanted to look into the case management strategies and workflow implementation practices aspects of a DF organisation. The second aspect required a qualitative approach to the problem so that the researcher can analyse the complexities of the DF work environment that may contribute to DF case management and case allocation.

6.3. Integration and Synthesis in Mixed Methods Research

In mixed-methods sequential explanatory design, integration refers to a stage or a series of stages in the research process where the researcher mixes, integrates, or synthesise the results of the quantitative and qualitative methods (Tashakkori & Teddlie 2003; Creswell et al.. 2003; Ivankova et al., 2006). The researcher may conduct the integration at the beginning, middle, or end of the research process (Ivankova et al., 2006).

Integration occurs in the beginning when the researcher discusses the mixing within the context of the purpose or aims of the research (Tashakkori & Teddlie 2003). Here, the researcher first integrated the research at the beginning when the researcher discussed the research design and methodology in the first chapter within the context of the purpose and aims of the research. In designing the research, the researcher proposed quantitative research questions in Study 1 (Investigation of the Dubai Police records), and qualitative research questions in the second and third case studies.

Further, the researcher integrated or connected the quantitative and qualitative methods in the middle of the research process. In the mixed methods sequential explanatory design, integration may occur at the intermediate stage (Hanson et al., 2005; Ivankova et al., 2006). Here, the researcher conducted an integration when the quantitative results of Study 1 (Investigation of the Dubai Police records)'s data analysis informed and guided the qualitative data collection in the second and third case studies, which the research used to get an in-depth understanding of the results of the first study. Additionally, the researcher integrated the research by selecting participants for the follow-up qualitative Study 3 (Confirmation of the Interviews) from the participant pool in Study 2 (Interviews with DF managers), which can occur in a mixed methods sequential explanatory design (Creswell et al.. 2003).

Integration of the quantitative and qualitative results may also occur towards the end of the research process when the researcher discusses and interprets the findings of the data analysis (Onwuegbuzie & Teddlie 2003; Ivankova et al., 2006). In this chapter, the researcher integrates the results of the quantitative and qualitative studies by discussing the outcomes of the entire study, and then connecting and synthesising the three case studies. The researcher discusses the principal findings of each of the studies, and then combines the results of the three case studies to provide an in-depth answer to the research questions and gain a better understanding of the phenomenon. An interpretation of the results in the context of the literature adds further depth to understanding the phenomenon. The integration and synthesis process of this chapter allows for further explanation of the results of the quantitative Study 1 (Investigation of the Dubai Police records), and a verification of the results of the qualitative Study 2 (Interviews with DF managers). In the end, integrating the quantitative and qualitative findings helps the researcher explain the quantitative results, and underscores the elaborating purpose for a mixed-methods sequential explanatory design (Creswell et al., 2003; Ivankova et al., 2006).

Additionally, in a phenomenological study, the researcher must conduct a synthesis of textural and structural descriptions into essences of the phenomenon. The researcher must integrate the phenomenological research by interpreting and justifying the researcher’s understanding of both the essential meanings and the general structure of the descriptions.

6.4. Lessons from the Case Studies

In this section, the chapter discusses the lessons from the three studies. The researcher organises the section according to the studies. The discussion of each of the studies include a discussion of the principal findings, an interpretation in the context of the literature, and the implications of the findings.

6.4.1. Discussion of Study 1 (Investigation of the Dubai Police records)

Study 1posed three hypotheses that aim to evaluate the relationships among several different factors (predictor variables) and the total number of Person-Hours per case (outcome variable). In other words, the researcher wanted to determine the significant factors that cause delay in DF investigation as measured in Person-Hours. The researcher posed the following three hypotheses:

Hypothesis 1
There is an increase on the cases trends for the past 12 years.

Hypothesis 2
The Total Evidence Volume per Case affects the time required for the examination process.

Hypothesis 3
The Heterogeneity of Evidence Items per Case affects the time required for the examination process.

Hypotheses one and three were confirmed. The researcher found a relationship between predictor variables (Number of Cases and Heterogeneity) and the outcome variable (Person-Hours) per Case. For the second hypothesis, the researcher didn't find an effect of the predictor variable Total Volume per Case on the outcome variable Person-Hours. However, the findings of this study justify the research questions posed and the mixed methods employed to answer the research question. From the statistical analyses and observations conducted in this study, the researcher found that a combination of factors affects the time of investigation, rather than merely the Heterogeneity of Evidence Items per Case, as its effect is only moderate. The results of Study 1 (Investigation of the Dubai Police records) also underscores the need for qualitative study to provide an alternative and perhaps more in-depth view of the human and social factors that affect DF investigations.

First, analysis of the data revealed a significant increase in the Number of Cases throughout the Years, and therefore confirmed hypothesis one, namely that "*there is an increase on the case trends for the past 12 years."* The analysis also showed that the Total Evidence Volume per Case increased over years. Moreover, the Number of Evidence Items per Case remained between 1 and 2 in most of the years.

The researcher initially expected that the increase in the Total Volume per Case and Heterogeneity of Evidence Items per Case would lead to an increase in the number of Person-Hours. The researcher hypothesised that "*the Total Volume per Case affects the time required for the examination process*." And "*the Heterogeneity of Evidence Items per Case affects the time required for the examination process*." The multiple linear regression showed moderate relation only between the increase in Heterogeneity of Evidence Items per Case and Person-Hours of investigation, Total Volume per Case was quite insignificant.

To integrate and synthesise the results of the hypotheses in Study 1 (Investigation of the Dubai Police records), the researcher found that Heterogeneity of Evidence Items per Case increased over the years, with moderate correlation with Person-Hours. Although, there is moderate effect of the Heterogeneity of Evidence Items per Case and Person-Hours of investigation, the research found that there are other factors, aside from Heterogeneity of Evidence Items per Case may affect the length of time in DF investigations.

6.4.1.1. Principal Findings from the Observations

The researcher tried to understand further the results of the data analysis and observations of the results through further observations to see other factors affect the DF investigation time in Person-Hours.

In the first observation, the researcher examined selected cases with similar investigation time but with two Total Evidence Volume per Case sizes. The researcher found that most of the cases with a lower Total Evidence Volume per Case were received between 2003 and 2011, while cases with a higher Total Evidence Volume per Case were received between 2012 and 2014. Based on the separation of the case sizes pre 2011 and post 2011, the researcher concludes that several factors more significant than Total Evidence Volume per Case may be behind the number of Person-Hours. One reasonable explanation is that changes in technology post 2011 may have reduced Person-Hours through improved workstation specifications, digital forensic tools version, or even DF practitioners' experiences. As a corollary, those factors may also lead to a delay in DF investigations.

In the second observation, the researcher tested the examiners' experience. The observation proved that experience has significant impact over the total time of investigation.

The observation revealed that most examiners with less experience spent more time on the investigation overall.

The third observation examined how the amount of information, which comes with the case request, affects the Person-Hours. The observations show that it is most likely to take less time if enough specifications in the request details are provided to the DF examiner.

These observations found that other factors would significantly affect the Person-Hours of investigations. These factors include, but are not limited to, the workstation, the digital forensic tools, the examiner's experience, the number of examiners assigned to a case and the amount of information provided to the examiner in the case request. The findings in Study 1 (Investigation of the Dubai Police records) underscored the need to conduct a qualitative study to determine if participants who experienced the phenomenon could confirm the quantitative findings in Study 1 (Investigation of the Dubai Police records), and shed light on understanding other factors that may affect the Person-Hours in DF investigation.

6.4.1.2. Interpretation in the Context of Literature

In order to compare the findings of this study with research papers, there are important facts that need to be illustrated. This research uses actual data from the DF Department of the Dubai Police. However, most research papers found on DF organisations used data from yearly reports published by different DF departments, cases announced in the media and introduced publicly, or by using records from private digital forensic departments. Moreover, the amount of data used in this research qualifies the results to be more robust with high accuracy compared to the amount of data used in other research papers. This research follows and further builds on literature like the research paper, "Digital Forensics to Intelligent Forensics" (Irons & Lallie, 2014), in proving that the number of DF cases and the volume of digital evidence is increasing roughly over the years. However, none of the research papers discussed the effect of Total Volume and Heterogeneity of Evidence Items on the Person-Hours spent in DF investigation. Generally, research papers discussed the backlogs that DF departments face, and assume the delay in investigation process. Like the researcher, there seems to have been an expectation that the increased volume and heterogeneity would increase the Person-Hours and would be a significant factor in DF investigation delay.

This research demonstrates in substantially more detail the relationship between those variables. Most importantly, this research paper shows that the Total Evidence Volume per Case is not directly affecting Person-Hours of investigation and Heterogeneity of Evidence Items per Case is affecting Person-Hours of investigation moderately. Reducing Person-Hours requires looking at a whole set of several factors other than the Total Evidence Volume per Case and Heterogeneity of Evidence Items per Case. To determine what some of these factors may be, this research conducted several observations that start identifying and highlighting some of the potential significant factors that affect Person-Hours.

6.4.1.3. Implications

Study 1 (Investigation of the Dubai Police records) has both academic and practical implications on DF investigations research and practice. The research reveals the benefits in using quantitative research to understand DF organisations and processes, but at the same time reveals the limitations of quantitative research. The Study revealed that additional qualitative research would further benefit a researcher in understanding and interpreting the quantitative results. The study, therefore, highlights the benefits of a mixed methods research when conducting research into DF organisations and processes.

Importantly, the study has found that Total Evidence Volume per Case is not directly affecting the Person-Hours per Case; also, that Heterogeneity of Evidence Items per Case has an effect, albeit moderate, on Person-Hours. This opens further potential in researching other factors that may affect Person-Hours. If researchers before were making assumptions about the role of Total Evidence Volume per Case and Heterogeneity of Evidence Items per Case on case back logs and lengthy DF investigations, this study shows that it is important for researchers and practitioners to consider the interplay of other factors such as DF tools, DF case management strategies, the experience and number of DF examiners, among others.

6.4.2. Discussion of Study 2 (Interviews with DF managers)

Study 2 (Interviews with DF managers) combined the context of work in various government and private digital forensic laboratories with the practical experience of the participants in order to arrive at a better understanding of the phenomenon of DF investigation delay and the management and allocation of DF cases. The researcher has come to understand from the descriptive answers of the participants that DF managers follow different strategies when assigning cases to examiners. The researcher has also come to understand that DF managers follow different workflow implementation processes. The findings of Study 2 (Interviews with DF managers) indicate that there is no standard strategy or practice in managing DF cases assignment or the workflow of the DF departments or organisations. Additionally, the researcher discovered different factors affecting the Person-Hours of investigation and the practical solutions the participants use to reduce the time of DF investigation.

6.4.2.1. Principal Findings

The researcher mainly aimed the study at understanding the context of work in various government and private DF laboratories in different countries. The study identified the diverse experiences that the participants have in leading and managing DF departments or organisations. It also focused specifically on their decisions when assigning cases to examiners, further elaborating on Study 1 (Investigation of the Dubai Police records)'s findings relating to the number of examiners assigned to a case. The study also came to understand better the motivations, expectations, and feelings behind a DF manager's choice of assignment strategy. The interview process gave the researcher the opportunity to understand the various aspects of managing DF departments or organisations. The textural and structural descriptions of the interviews enrich this study with personal perspectives from managers serving the field of DF for plenty of years. Finally, the researcher identified and represented the essence of the experience, as the phenomenological research process requires (Patton, 2002).

Through the phenomenological process, the research identified principal findings related to DF case management strategies, DF implementation practices, and various factors that affect the Person-Hours of DF investigation. The researcher discovered that DF managers rely on different DF case management strategies that the researcher grouped into the following categories: (1) caseload strategy, (2) ability strategy, and (3) parallel team strategy. Additionally, the researcher identified that DF managers use different DF implementation practices that the researcher grouped into the following categories: (1) traditional workflow, (2) team workflow, (3) parallel team workflow, (4) outsourced workflow, and (5) tiered workflow. This research, therefore, has contributed to the literature by identifying some of the existing DF case management strategies and implementation practices that can be a basis for further research in this area.

Further, the researcher identified administrative and investigative factors affecting the Person-Hours of investigation, further enhancing the findings in Study 1 (Investigation of the Dubai Police records) as to potential factors.

6.4.2.2. Interpretation of Findings

The participants had comprehensive answers to the questions corresponding to this research. The researcher discovered various essences from the participants' interviews and arrived at a better understanding of the background of DF managers, hiring practices, promotion practices, ISO certification, case generation, DF case management, DF workflow implementation practices, and factors that affect Person-Hours of investigation. In integrating the above essences, the researcher interpreted and justified the essential meanings and the general structure. The researcher, therefore, explains in this section how the discovered essences fit together. In so doing, the researcher highlights two factors common to the discovered essences: people and process.

The researcher found that the identified essences fit within the sphere of interaction between people and process involved in a DF department or organisation. The researcher identified two types of interplay between people and process: administrative and investigative. Administrative interplay deals with management methods DF managers apply in a DF department or organisation, including the allocation of human and technical resources. Investigative interplay deals with investigative methods DF investigators apply in a DF department or organisation, including the use of certain DF tools or workstations and the use of certain DF investigation models. Both administrative and investigative interplay affect the Person-Hours of DF investigation.

In administrative interplay, for example, the core of work in DF departments or organisations is similar but the DF case management strategies and workflow implementation practices vary. The process of assigning DF cases, and the workflow of the DF cases, differs from one DF department or organisation to another. Different DF case management and implementation practices will approach management of Person-Hours differently from an administrative perspective. Hiring and promotion practices affect DF case management and workflow implementation; which in turn affect allocation of experienced examiners and the number of examiners assigned to a case. There are also unique administrative processes that a DF department or organisation may face based on its organisational structure and process that could contribute to lengthy Person-Hours.

In investigative interplay, the DF tools, workstation, unique DF investigation or academic experience of DF investigators, and administrative interplay may combine to affect the Person-Hours of DF investigations. Administrative interplay that affects investigative interplay includes, among others not discovered in this research, how DF examiner experience affect case assignment and allocation, the number of examiners assigned to a case, and incentives for examiner performance such as promotion or bonus.

This section discusses each of the essences discovered in the research and explains how each of the essences relates to one another, to administrative and investigative interplays, and to Person-Hours.

6.4.2.2.1. Background of DF Managers

All the interviewed managers come from technical backgrounds, not administrative. They gained their forensic skills by practice. All the participants have experiences of more than nine years in the field of DF. It is perhaps because of the general lack of administrative background that the hiring and promotion practices, as explained next, seems so unique for each participant. Overall, the DF field has yet to develop a standard for who qualifies as a DF manager, although experience is what the participants have in common.

It was interesting to find that most of the participants were satisfied with their yearly budget. They are getting enough to support their new licenses, tools and training programs. Perhaps because of this relative satisfaction with the availability of funding, the research did not discover essences relating to the allocation of resources concerning DF tools and equipment.

6.4.2.2.2. Hiring of Examiners

Across the different departments and companies, there are no recognized accreditation requirements for hiring new practitioners. Most of the departments and companies developed their own internal examination or interview to rate the capability of the job candidates. The lack of a recognized standard for hiring creates an added staffing challenge for DF managers that could affect Person-Hours at the administrative interplay.

The researcher also discovered that most of the government departments accept candidates with experience if they are available, as well as fresh graduates with the required skills and knowledge. However, private companies mostly would rely on the experience that the candidate has before hiring. Most of these will not prefer hiring graduates as this would require effort in training and improving their skills and knowledge. In general, it would be beneficial to have definite accreditation requirements such as certain courses taken, training programs attended, or certificates obtained by the candidates when applying for the digital forensic examiner job.

The differences in hiring practices between government departments and private companies affect the DF case management and workflow implementation practices of participants. Government departments that hire fresh graduates are more concerned with providing experience to those hires and favour a case management and workflow that allows for such training and experience sharing. That private DF organisations prefer to hire DF examiners with experience also signals that these private DF organisations, which are more drive by profit than their government counterpart, may have done the cost-benefit analysis and see a link between experience and productivity. Certainly, Study 1 (Investigation of the

Dubai Police records) partially supports such a view since examiners with less than three years of experience, according to the first study, will be less productive in comparison to examiners with more than three years of experience.

A possible takeaway here is that both public and private DF organisations should consider the lessons from Study 1 (Investigation of the Dubai Police records) and set a standard for hiring examiners that begin with three years of experience. One may argue, however, that not allowing fresh graduates the opportunity to join a DF organisation would lower the pool of DF practitioners. Perhaps, DF organisations can adopt a two to three-year internship or training requirements for all fresh graduates as a standard for hiring.

6.4.2.2.3. Promotion of Examiners

Like hiring, there are no recognized requirements on the development path of the employees. Rising from one position to another as an expert would be efficient if there is a standard to follow among all the departments and companies. The researcher observed that most government departments have a clear career promotion path. However, private companies do not have a clear strategy for job promotion. Having clear accreditation requirements for hiring and promotion will increase the awareness among DF examiners about the importance of keeping up to date with new development in the field of DF and making sure that examiners are coping with new technologies and the best practices of investigation.

Usually in the government department, the junior examiner will be required to complete a certain number of years to earn promotion to senior examiner. The junior examiner will be required to work on a specified number of cases, attend several training programs, attend several courses and pass examinations and interviews to ensure the capability of the knowledge obtained.

In private companies, there is no clear path for junior examiners to follow to attain promotion. As time is a very important factor for companies, they depend mainly on the examiners' experience, skills and knowledge, and the application of these factors to reduce the Person-Hours of investigation. Thus, examiners who can complete tasks efficiently and spend less time have a higher chance of earing a promotion. Thus, there is a clear path for promotion in the government departments, however, in the private companies interviewed there is no clear strategy for promotions.

Lack of a clear promotion path is troublesome and may affect DF practitioner performance because of unclear incentives. It would be interesting to study, for example, how performance incentives tied to Person-Hours may change DF investigation delay, or to study whether DF departments or organisations have proper performance incentives in place that would result in lower Person-Hours.

6.4.2.2.4. ISO Certification

At the time of the interviews, there were still a few departments that had not obtained ISO 17025 certification. The fact that courts do not accept reports from uncertified departments or organisations is the principal motivator for all departments and organisations to swiftly obtain ISO certification. It is interesting to note, however, that ISO 17205 only deals with standardisation of testing and calibration processes. Interestingly, none of the participants mentioned other types if ISO certification or creating documented processes concerning administrative and investigative interplays.

6.4.2.2.5. Case Generation

Most participants work on criminal and civilian cases. Government departments can generate their own cases, which also increases the Number of Cases. They can find online offenders by using data mining products, for example by trolling Twitter, Facebook, or Instagram. This feature increases the Number of Cases that government or public DF departments receive in comparison to the Number of Cases that independent or private DF organisations receive.

Interestingly, the amount of cases a DF department or organisation receives will also influence its DF case management and workflow implementation practices. Certainly, the Number of Cases a DF department or organisation receives will influence the caseload on DF examiners. Those with lower caseloads, for example, may be more inclined to create DF examiner teams, and thereby reduce Person-Hours with such administrative interplay. Still, the Number of Cases is not the determinative factor in a DF manager's decision to assign a case to one or more examiners, as shown in Study 1 (Investigation of the Dubai Police records), but rather the Number of Evidence Items per Case. In this regard, some private DF organisations may take fewer cases but take on cases with a higher Number of Evidence Items per Case, and therefore be more inclined to create DF examiner teams, in comparison to the government counterpart.

6.4.2.2.6. DF case management strategies

For DF case assignment, different managers rely on different strategies such as caseload, examiner's experience, skills, knowledge, availability and competition among the examiners. There is no standard for determining the most efficient DF case management strategy.

The researcher categorised the three main strategies that the departments/companies follow when assigning cases as follows: (1) caseload strategy, (2) ability strategy, and (3) parallel team strategy.

In the caseload strategy, the DF manager relies on the caseload that the examiner has. The DF department or organisation's hiring and case generation capacity, as discussed earlier, will certainly influence such a strategy. DF managers who use the caseload strategy, however, do take into account the number of exhibit when assigning the case to a DF examiner, which supports the finding in Study 1 (Investigation of the Dubai Police records) as to relationship between the number of examiners and the number of exhibits items. That the caseload strategy treats all examiners as having similar skills, capabilities and knowledge because of the similar training opportunities provided to all examiners, may be generally supported by the finding in one of Study One (Investigation of the Dubai Police records)'s observation that there is no strong relationship between the examiner's years of experience and the Person-Hours. However, the same observation did show that examiners with less than three years of experience do tend to take longer to conduct a DF investigation in comparison to those with more than three years of experience. Government DF departments that hire fresh graduates and use the caseload strategy will be more likely to find an increase in Person-Hours for those examiners with less than three years of experience. Yet, such

Person-Hours could also be offset by other factors such as new techniques learned in school or training, or the use of faster technology or equipment.

In the ability strategy, the DF manager relies on the experience, skills, knowledge, capability and availability of the examiner when assigning a case. DF managers using the ability strategy also consider the number of exhibit items, again supporting the findings in Study One (Investigation of the Dubai Police records) as to the role of the number of exhibit items. Some managers consider the urgency of the case, while other managers put more emphasis on the DF examiner's ability according to a matrix. The DF department or organisation's hiring and promotion policies will certainly affect the ability strategy. In general, the DF department or organisation should rely on a broad range of abilities, and should value diversity in experience, skills, and specialisation. The case generation process of the organisation will also play a role because a DF organisation with a case generation process that overproduce cases that fit only certain DF examiner abilities may overburden a certain segment of the DF examiner pool in the organisation. DF managers who employ the ability strategy stated that assigning cases based on the DF examiner's ability will allow DF examiners to work faster in the face of heterogeneous case types. However, Study One (Investigation of the Dubai Police records) support such a view because the researcher found in approving the third hypothesis in Study 1 that the Heterogeneity of Evidence Items per Case does affect moderately the Person-Hours spent in an investigation.

In the parallel team strategy, the DF manager relies on the competition between the examiners when assigning cases. However, only one private DF organisation employs this strategy, a company that receives only a small number of high profiles, big cases. The parallel team competition is a creative solution to incentivise performance and possibly lower the Person-Hours of DF investigation. The competition seems to focus on the volume or complexity of the case the team competes for, and perhaps forces the team to complement each other's abilities. Competition as a motivating factor to lower the Person-Hours requires further research, and the findings in the first study supports the underlying premise behind the strategy. If Heterogeneity of Evidence Items per Case was the underlying assumption behind the parallel team strategy, then the findings in Study One (Investigation of the Dubai Police records) would certainly support such an assumption. Additionally, the hiring and promotion policy of a DF organisation applying the parallel team strategy would also correlate with the strategy since the DF manager would want to create teams based on the examiners experiences and abilities. The DF organisation's case generation process would also have an impact on the feasibility of a parallel team strategy, making it less likely to occur in DF departments or organisations that have high caseload.

The researcher would be interested to see how the managers themselves would evaluate these three case management strategies and the strategies' applicability in their respective organisations, which this researcher will validates through Study 3 (Confirmation of the Interviews).

6.4.2.2.7. DF workflow implementation practices

The workflow implementation practices also vary. Each DF manager who participated in the study had his own principles and views as to workflow implementation. Thus, there is also no standard for workflow implementation practices.

DF managers built their own unique workflow implementation practice from their respective experience during the long years they spent leading the department. All the participants obtained their strategies and workflow implementation practice either from the managers working in that position before them or applied the techniques depending on their own understanding of the requirements of their departments. Each department or organisation has its own method of workflow implementation practices. The researcher grouped the workflow implementation practices into five main categories: (1) traditional workflow, (2) team workflow, (3) parallel team workflow, (4) outsourced workflow, and (5) tiered workflow.

In the traditional workflow, the examiner will work on a case from start to end, and the DF manager assigns the case under either the caseload or the ability strategy. The traditional workflow, however, should at times employ a team approach because of the advantage of lower Person-Hours with a higher number of examiners. The traditional workflow would also benefit more when there is a clear promotion policy that incentivises an examiner who bears the burden of a DF investigation from start to end. In government DF departments that hire fresh graduates, the traditional workflow will require less experienced examiners to undergo training and gain a solid experience before the DF manager assigns to complete a case from start to end. The traditional workflow would also benefit from an ISO certification since the examiner follows a specific process as determined by the DF department or organisation. In this regard, investigative interplay will play a significant role for the DF examiner to lower the Person-Hours.

In team workflow, the examiner will work on a case, but everybody in the lab will help in the crime scene and in forensic duplication/ pre-processing of the case. The DF investigation framework or model adopted by the DF department or organisation seems to drive the team workflow because the tasks assigned to team members correspond to the DF investigation process. Each participant is assigned some aspects of the DF investigation process. This signals that perhaps the type of DF investigation model chosen by the DF department or organisation could also affect the Person-Hours. Additionally, the investigative interplay plays a pivotal role in this workflow.

In the parallel team workflow, two opposing teams will work on the same case, aiming to get the results as fast as possible. This workflow corresponds with the parallel team strategy, which one private DF organisation employed. The same interpretation relating to the parallel team strategy applies to the parallel team workflow.

In the outsourced workflow, external or outsourced practitioners with contracts and have the required experience will work on the case. This workflow practice likely follows the caseload strategy and does not likely follow a hiring or promotion practice beneficial to the long-term career of DF examiners within the DF department or organisation, since the DF department of organisation outsources most of the work, except for the initial duplication to external practitioners who have their own businesses. This workflow approach also does not consider the benefits of multiple examiners working on a case to lower the Person-Hours since the outsourced practitioner will likely make that decision and will likely not have the luxury of having multiple examiners working on a case. On the other hand, the outsourced workflow may be a work around for the concern relating to Person-Hours, since the DF department or organisation could require the outsourcing practitioner to complete the task within a given timeframe.

In the tiered workflow, junior examiners start with the basic tasks in the case, then the senior examiners will work in the investigation. This workflow likely follows the ability strategy and determines who becomes junior versus senor examiner based on ability. Because ability is essential, there should be a clear policy for promotion and hiring to determine who is junior versus senior. In addition, according to the findings of the first study, senior examiners should be required to have at least ten years of experience. However, none of these proposals regarding promotion, hiring, and experience of examiners is likely being applied by the participants, and certainly did not emerge from the lived experiences of the participants in the interviews. There seems to be an assumption underlying the tiered workflow that basic tasks require less experience, while critical tasks require more experience. This means that the DF investigative framework or model is what drives the thinking behind the tiered workflow, and signals that perhaps the type of DF investigation model chosen by the DF department or organisation could also affect the Person-Hours.

The DF managers were all convinced that their selected way of assigning cases and processing the work in the department is the best, and they do not think that changing the techniques to another way would be a good idea. The numbers of cases are increasing rapidly in all the DF departments or organisations, and perhaps it would be interesting to see whether changing strategies would improve efficiencies and perhaps lower Person-Hours in the process. The researcher would be interested to see how the managers themselves would evaluate these five workflow implementation practices and the applicability of other workflows in their respective organisations, which this researcher will validates through Study 3 (Confirmation of the Interviews).

6.4.2.2.8. Factors affecting Person-Hours

Finally, the researcher discovered additional potential factors that may affect Person-Hours from the lived experiences of the participants. All the DF managers agree that a combination of factors affect the Person-Hours of investigation. It is also true that the literature suggests different factors that could affect the Person-Hours of investigation. However, the managers provide factors that are more specific by reflecting on their lived experiences in the DF department or organisations. It should be emphasized that the identification of these additional factors supports the findings and observation s in Study One (Investigation of the Dubai Police records) and shed light on the administrative and investigative interplay identified in the general structure of the identified essences in this study. The researcher grouped the discovered additional factors into two categories: administrative and investigative, as consistent with the administrative and investigative interplays between people and process.

The participants identified the following administrative factors that may affect the Person-Hours in DF investigations:

a. Lack of staff

b. One examiner working on a case instead of a team

c. There are some participants who believe that the experience affects the Person-Hours of investigation and there are others who do not.

d. The delay time to receive the public prosecution report.

e. The delay time to shift the exhibits from one department to another.

f. The case details, if the case is requested and the requirements are not clear it will extend the Person-Hours of investigation.

Some of the administrative factors support the findings in Study One (Investigation of the Dubai Police records) and justify the general meanings identified from the other essences. That participants expressed that one examiner working on a case instead of a team supports the finding in the first cases study that a higher number of examiners lead to lower Person-Hours. The split among participants as to the role of experience on Person-Hours is also reflective of the finding in Study One (Investigation of the Dubai Police records) regarding the general relationship between the experience of examiners and the Person-Hours. The split in view may be because of experience that is less than three years or more than ten years being conflated with the overall effect of experience. Additionally, that the participants expressed the case details as a factor in Person-Hours also supports the findings in the Study One (Investigation of the Dubai Police records) observations that more case details may lower the Person-Hours. The factors concerning lack of staff does relate to the hiring, promotion, and DF case management and workflow essences discussed above. The factors relating to delay in receiving reports or exhibits also relate to the administrative interplay.

The participants also identified the following investigative factors that may affect the Person-Hours in DF investigations:

a. Volume of the exhibits

b. Heterogeneity of exhibits

c. Number of exhibits

d. Cases uses anti forensic techniques

e. Cases uses cloud computing

f. Cases has password protected in the files/drive or mobiles

g. Cases use social media applications.

h. Cases uses network intrusions

i. Capability of the digital forensic software.

Since the DF managers identified these as factors, this underscores the need to continue to do quantitative and qualitative studies side by side to verify and correct assumptions about the DF field. The participants also identified the number of exhibits as a factor in Person-Hours. However, as found in the Study One (Investigation of the Dubai Police records), Number of Evidence Items per Case does not affect the Person-Hours.

The participants expressed factors relating to the ‘type’ and the ‘needs’ of cases as potential factors affecting Person-Hours. While Study One (Investigation of the Dubai Police records) found that the types of cases do not affect Person-Hours, there is no specific data regarding the unique needs of cases relating to ant-forensics, cloud computing, social media, or network intrusions. The literature does suggest that there are additional challenges posed by anti-forensics, cloud, password protection, and social media, as discussed in the literature review.

Although, the participants related certain factors as affecting throughput, they did not provide any solutions. The participants each used a variety of different techniques to reduce some of the investigative barriers to investigation completion. The participants reported using the following different techniques to reduce the time spent in DF investigation:

1. Spend days on site to triage, preview and eliminate the number of exhibits.
2. Using tiered structure of techniques.
3. Develop case process methodology for the examiners to follow.
4. Study the capability of the current digital forensic software tools.

These techniques seem to follow the literature on DF investigation techniques and since there is a lack of literature on administrative interplay, then participants are lacking in expressing experiences with administrative solutions.

6.4.2.3. Interpretation in the Context of Literature

There are similarities between the findings from the current study with the literature. First, DF managers depend mainly on the load of cases, examiner's experience, skills, knowledge, availability and the rivalry between the examiners. This is like which most supervisors rely on when delegating tasks to their subordinates (Vinton, 1987). The managers in some of the departments will rely on assigning the urgent cases to senior examiners and the normal cases to junior examiners. This finding also reflects the findings in the research where assignment of tasks might include both challenging and routine tasks and supervisors usually are careful in delegating challenging tasks and trying to assign those tasks to employees with higher experience (Van de Vliert & Smith, 2004). Furthermore, the interviews also exposed the existence of numerous management tools that DF managers can use to assign tasks and follow up with their employees' accomplishments. As discussed in the literature, DF managers can use variety of management tools in their departments, and there are specific management tools built specifically for the DF field such as Lima Forensic Case Management (Lima, 2017). However, none of the interviewees used the specified management tool for forensics and they were using management tools that they can customise to their requirements.

The outcome of the practical implementation practices of cases workflow did not reflect the general findings in the literature. Yet, there are plenty of studies that discussed in detail the methodologies to be followed at a crime scene by first responders and the methodologies used by DF investigators while examining the digital evidence. The findings from this study came from the practical experience of digital forensic managers. The different implementation practices, which were defined in this study, depended on the DFWS model of case investigation (Palmer, 2001). The researcher specifically chose this model because it is the main model that most of enhanced methodologies rely on.

6.4.2.4. Implications

The findings from this study have implication for managers, supervisors, decision leaders working in DF departments or companies in practices related to case management, allocation and completion. This section will provide these suggested implications for practical execution in leading any DF department or organisation. The overall finding of case assignment indicates that the managers rely on three main strategies to assign the cases. Those strategies are guided by the different factors such as caseload, experience, skills, knowledge, capability, availability and competition. These factors affecting cases assignment strategies can be incorporated to broaden the manager's personal experience with the different available strategies.

The workflow implementation practices may be particularly important in introducing the experience of other managers. The workflow implementation practices vary from one department or organisation to another. Some let the examiners complete all the tasks in each case from start to the end. Others might divide the tasks between the employees in the department and then complete the rest of the tasks according to the case leader and his team. Some departments depend on competition between two groups to accomplish the cases. Further, some departments use contractor examiners to accomplish the cases. Thus, DF departments should operate in a way that reflects their vision and mission and put in consideration the different variables that influence the decision. Illustrating the different workflow implementation practices help the managers to encounter work in various DF departments or organisations. Thus, this study defined the experiences of DF managers working in the field for 9 to 22 years. This also develops the strength and confidence of the managers that there are others following similar implementation practices.

Representing the different factors that affect the Person-Hours of investigation and grouping them by administrative and investigative factors is beneficial as it highlights the practical factors that managers deal with. These factors imply the importance of further research on the factors affecting Person-Hours. Moreover, this study also covered the precaution techniques that managers apply to minimize the effect of the factors, which are also beneficial for the researchers to be aware of the current implemented and approved techniques. In general, the findings of this study are very beneficial for academics. It can help researchers become aware of the DF case management and workflow implementations practices in DF departments or organisations. Thus, this study also supports the new leaders and managers in the DF departments or organisations to encounter the various experiences and practical observations. This will enrich their knowledge of the practical management experiences and prevent several obstacles that might result when implementing new strategies and techniques.

6.4.3. Discussion of Study Three (Confirmation of the Interviews)

This study aims to evaluate the findings from the previous study. The participants in this study expressed what they deemed as the advantages and disadvantages of the different DF case management strategies and workflow allocation practices the researcher discovered from the lived experiences of participants in the second study. As the researcher selected the participants in Study Three (Confirmation of the Interviews) from the same pool of participants as those in Study Two (Interviews with DF managers), Study Three (Confirmation of the Interviews) was essentially a peer review of the discovered strategies and practices from Study Two (Interviews with DF managers). This section, therefore, discusses the principal findings in Study Three (Confirmation of the Interviews), the interpretation of the findings, the interpretation of the findings in the literature, and the implications.

6.4.3.1. Principal Findings

As to the first hypothesis, participants weighed the applicability of the three types of case management strategies the researcher identified: caseload, ability, and parallel team strategy. Most participants stated that the caseload strategy would be beneficial as an initial factor in case management and allocation. The participants overwhelmingly rejected the parallel team strategy and found it inapplicable and inefficient. Participants divided the ability strategy into one that DF managers apply to urgent cases and one that evaluates the experience, skills, and knowledge of the examiner. Most participants favoured the use of the ability strategy on urgent cases but did not feel as strongly about the use of the ability strategy that evaluates the experience, skills, and knowledge of the examiner.

Managers were enthusiastic in considering other case allocation strategies especially for training purposes and improving efficiency concerning the urgency of cases. Thus, most participants stated that they could continue their current case assignment strategy for normal cases. However, participants are willing to change strategy for urgent cases and to train and develop the skills of their examiners. Additionally, participants are willing to change strategy considering factors like the Number of Evidence Items per Case, number of available examiners and the number of pending cases.

As to the second hypothesis, participants weighed the applicability of the five types of workflow implementation practices: (1) traditional workflow, (2) team workflow, (3) parallel team workflow, (4) outsourced workflow, and (5) tiered workflow. All the participants favoured the traditional workflow implementation practice with some stating that it is nevertheless inapplicable or not implementable in their respective departments or organisations. Participants found some advantages to the team workflow but found it inapplicable in their respective departments or organisations. The participants overwhelmingly rejected the parallel team workflow. All the participants recognized the advantages of the outsourced workflow, but some cannot implement it because of policy limitations in their respective departments or organisations. Finally, all the participants favoured the tiered workflow's advantages.

Most of the participants are open to new ideas about workflow implementation. However, they do not imagine applying them in their workplace for several reasons such as the workflow practice consumes time, resources and effort on the senior examiners while conducting routine tasks. Moreover, some workflow practices would be inapplicable in their departments due to the nature of their work, policy, manpower availability, and resources. Participants stated that they could not implement some workflow practices on a huge Number of Cases that some of the departments have. Furthermore, the workflow practice may not give the junior examiners the required training.

6.4.3.2. Interpretation of the Findings

The researcher concludes that the parallel team strategy and workflow are not viable types of strategies and practices for the majority of DF department or organisations. The findings in the third cases study show that the participants overwhelmingly reject this parallel team strategy and workflow. However, there may be unique circumstances such as training purposes or business performance enhancement where a DF manager may choose to apply the parallel team strategy and workflow.

The findings suggest that there may be several other DF case management strategies, and further research on the phenomenon involving a larger number of participants is necessary, though beyond the time and resource limitations of this thesis. In interpreting the findings in Study Three (Confirmation of the Interviews), it becomes evident that DF managers could develop a combination or matrix of DF case management strategies to determine what is most applicable in a given DF department or organisation given a number of factors like resources, policy, type of DF organisation, time requirements, among others. In the limited findings of the second and third case studies, the researcher finds, for example, that a combination of the caseload and ability strategy would be effective and likely favoured by DF managers. The DF manager could apply the caseload strategy as an initial factor but switch to the ability strategy for urgent cases. However, the researcher realizes that there may be many other DF case management strategies yet to be discovered and could create a more effective set of choices for DF managers.

As to the workflow implementation practices, the findings suggest that most DF managers would agree to adopt the tiered workflow. The traditional, team, and outsourced workflows also have advantages, but DF managers are likely to reject these types if they do not fit with the needs, framework, and policy of the DF department or organisation. In this regard, it is likely that there are other workflow implementation practices not identified by this research. Additionally, DF managers could develop a combination or matrix of the four workflows to determine what works best for their respective DF department or organisation.

The researcher concludes that risk strategies should be developed in DF departments or organisations in order to evaluate the risks of each case assignment and workflow implementation practices. Moreover, risk strategies would help DF managers identify various case management strategies and workflow implementation practices and determine their advantages and disadvantages.

6.4.3.3. Interpretation in the Context of Literature

Because minimal research exists that explores the techniques to optimize the complicated and timely process of case management prior to the start of the investigation process (James, 2014), Study Three (Confirmation of the Interviews) contributes to a gap in the literature. While there are numerous papers proposing DF investigation models, no research paper that the researcher is aware explicitly talks about DF case management in DF departments or organisations. Additionally, there has been a lack of studies concerning DF workflow implementation practices. The researcher's identification of the various DF case management strategies and workflow implementation practices is, therefore, an important contribution to the DF literature.

When examining non-DF literature regarding strategies and implementations for work allocation, management, delegation, assignment, the researcher found similarities with the findings in the second and third case studies.

The literature supports that proper work allocation is necessary to increase productivity in any work environment. Research also agree that managers need to pay attention to various strategies before assigning tasks to employees. Therefore, the literature supports the idea of using a matrix or combining case management strategies and combining workflow implementation practices.

The literature supports the ability strategy that the researcher discovered. According to the literature, supervisors usually delegate tasks depending on the subordinate's skills, knowledge, and self-confidence thus increasing their job satisfaction and organizational commitment (Vinton, 1987). While the second and third case studies did not discover such descriptions as self-confidence and organizational commitment, skill, knowledge, and experience were recurrent descriptors in the ability strategy. The literature discusses taking advantage of unique skill sets, unique preferences and unique talents that every co-worker has, which also supports the caseload and ability strategies, and the traditional, team, and tiered workflow implementation practices.

The literature discusses the delegation of challenging and routine tasks like the basic task assigned to junior examiners and critical tasks assigned to senior examiners described by DF managers in the tiered workflow. According to the literature, supervisors usually are careful in delegating challenging tasks because challenging tasks assigned to subordinates might cause certain risk for the superiors (Van de Vliert & Smith, 2004). To reduce the risk, supervisors usually intend to assign challenging tasks to those who are willing and able to perform well, just like in the ability strategy and tiered workflow.

The literature even supports the parallel team strategy and workflow overwhelmingly rejected by the participants in Study Three (Confirmation of the Interviews). The literature states that supervisors mostly rely on the subordinate's job performance and ambition, where habitually ambitious subordinates are more eager to perform challenging tasks. The same concepts of ambition and rewarding DF examiners for performance may underlie the thinking behind the parallel team strategy and workflow.

The literature also supports the team workflow. The literature states that managers, who are unsure who to assign a task to, could present the task to a group of co-workers and ask who has the required skills to handle the task. Managers can also encourage the co-workers to use a constructed timeline from the beginning of the task delegation to its final execution to maintain focus and accountability. This is like the team workflow and the ability strategy.

Overall, the non-DF literature on strategies for work management supports the discoveries and evaluations in the second and third case studies on DF case management strategies and workflow implementations practices.

6.4.3.4. Implications

Study Three (Confirmation of the Interviews) has implications for both academics and practitioners. For academics, Study Three (Confirmation of the Interviews) reveals the further need to discover the various DF case management strategies and workflow implementation practices employed by DF managers. A qualitative study involving a larger population would likely reveal additional strategies and practices. The strategies and practices that the participants evaluated in this study is a promising starting point for further research and theory development. While the researcher initially planned to conduct a grounded theory study towards theory building, the researcher’s time and resource limitation made further study difficult, especially in an already challenging multi-staged mixed methods research.

For practitioners, Study Three (Confirmation of the Interviews) has implications because it suggests that DF managers should pay attention to, and weigh the advantages and disadvantages of, various DF case management strategies and workflow implementation practices. Study Three (Confirmation of the Interviews) also eliminates the parallel team strategy and workflow since it does not seem viable for most DF managers. Of the remaining strategies and practices, the study suggests for DF managers to combine or create a matrix to determine what fits best with the DF department or organisation.

6.5. Integration and Synthesis of Case Studies

While the researcher has integrated the studies throughout the thesis, it becomes necessary to conduct an explicit and separate integration and synthesis of the case studies in order to justify the researcher's understanding of both the essential meanings and the general structure of the descriptions, and to arrive at a better understanding of the relationships among the three case studies. This section, therefore, explicitly integrates and synthesises the first and Study Two (Interviews with DF managers), the Study Two (Interviews with DF managers) and Study Three (Confirmation of the Interviews), and all the case studies.

6.5.1. Integration and Synthesis of Study One (Investigation of the Dubai Police records) and Study Two (Interviews with DF managers)

In Study One (Investigation of the Dubai Police records), the researcher tried to find the relationship between different factors and the Person-Hours of investigation. The factors considered were Total Evidence Volume per Case, Number of Evidence Items per Case, and Heterogeneity of Evidence Items per case. The analysis showed that there is a moderate relationship between Person-Hours and Heterogeneity of Evidence Items per Case.

However, Study One (Investigation of the Dubai Police records) illustrated that a combination of factors affects the time spent on DF investigation. Some of the factors discussed in Study One (Investigation of the Dubai Police records) include workstation specifications, DF tools version and DF practitioner's experience, number or examiners working on the case, and case details.

In Study Two (Interviews with DF managers), the researcher discovered from the lived experiences of the participants that a combination of factors affects the Person-Hours of investigation, supporting the findings in Study One (Investigation of the Dubai Police records). The researcher grouped the factors into either administrative or investigative factors. Most of the participants expressed that the volume of exhibits, Number of Evidence Items per Case, and the Heterogeneity of Evidence Items affect the Person-Hours of investigation. The findings in Study One showed that only Heterogeneity of Evidence Items per Case affects the Person-Hours of investigation moderately.

Most of the managers agree that the amount of time spent on investigation has remained the same throughout the years even when the Total Evidence Volume per Case increased because of the development of DF investigation tools that help alleviate the challenges of new digital evidence items.

The participants in the Study Two (Interviews with DF managers) also agree with another factor shown in Study One (Investigation of the Dubai Police records): that the caseload has increased over the years. However, some of the managers put a cap on the maximum Number of Cases that each examiner can receive at once; this has the effect that even if the Number of Cases keeps increasing in the future, the caseload for an individual will not exceed a certain number.

All the participants agree that a group or team of examiners will complete an assigned case faster than a single examiner assigned the same case. Working in a team strengthens the investigation process because each examiner has a different background, experience and knowledge.

Lastly, Study One (Investigation of the Dubai Police records)'s findings indicated that experience affects the amount of time spent in a DF investigation. However, participants, when queried in the follow-on studies, had different point of views. Some believe that experience affects the time of DF investigation, while others do not.

Overall, Study Two (Interviews with DF managers) expanded the researcher's understanding of the factors affecting the Person-Hours of investigation due to the lived experiences of the participants, who have years of experience in the field, with the phenomenon.

6.5.2. Integration and Synthesis of Study Two (Interviews with DF managers) and Study Three (Confirmation of the Interviews)

The researcher discovered in Study Two (Interviews with DF managers) that DF managers rely on different DF case management strategies that the researcher grouped into the following categories: (1) caseload strategy, (2) ability strategy, and (3) parallel team strategy. In Study Three (Confirmation of the Interviews), the participants evaluated these strategies, the result of which led the researcher to eliminate the parallel team strategy, and to identify the caseload and ability strategy as the most viable of the discovered factors.

Additionally, the researcher identified that DF managers use different DF workflow implementation practices that the researcher grouped into the following categories: (1) traditional workflow, (2) team workflow, (3) parallel team workflow, (4) outsourced workflow, and (5) tiered workflow. In Study 3 (Confirmation of the Interviews), participants evaluated these workflow practices. The researcher found that the parallel team workflow should probably not be considered as viable and that tiered workflow is the most viable option, with team, parallel and outsourced workflows being good alternatives that DF managers may or may not adopt based on several factors unique to each DF department or organisation.

The researcher suggests that DF managers should create a matrix or combine the case management strategies and combine the workflows to determine the most feasible for the needs of the DF department or organisation. Additionally, the findings of both the second and third studies as synthesized suggest that there are likely other DF case management strategies and workflow implementation practices that further qualitative research may discover with a larger population sample.

6.5.3. Integration and Synthesis of Case Studies

In the discussion of the findings in Study Two (Interviews with DF managers), the researcher identified administrative interplay and investigative interplay. Both administrative and investigative interplay affect the Person-Hours of DF investigation. Of the two, administrative interplay is what integrates the three case studies because administrative interplay determines performance at the investigative interplay between people and process.

Administrative interplay deals with management methods DF managers apply in a DF department or organisation, including the allocation of human and technical resources. In administrative interplay, for example, the core of work in DF departments or organisations is similar but the DF case management strategies and workflow implementation practices vary. Different DF case management and implementation practices will approach control of Person-Hours differently from an administrative perspective. Therefore, administrative interplay will affect the Person-Hours in DF investigation. Aside from case management and workflow implementation, among the types of administrative interplay identified in Study Two (Interviews with DF managers) include such factors as policy, case generation, ISO certification and the use of a documented process, hiring, and promotion of examiners.

The length of a DF investigation in Person-Hours, however, is a phenomenon that occurs within the investigative interplay. Essentially, Person-Hours is the measure of time it takes to complete the DF investigation process, a core feature of investigative interplay.

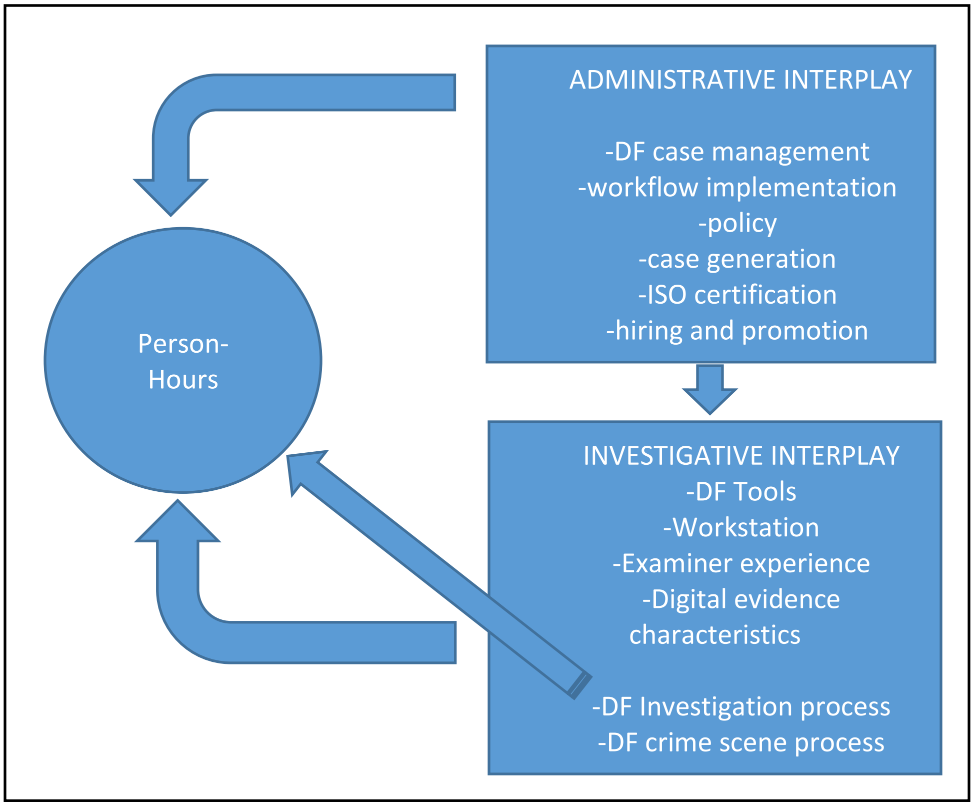


Figure 22. Interplays

Other factors that fall under investigative interplay also affect Person-Hours. These factors include the DF investigation process or model used in the DF department or organisation; the DF crime-scene process or framework; the DF tools; the workstation; the experience, skill, and knowledge of DF investigators or examiners; and the characteristics of the digital evidence. Study One (Investigation of the Dubai Police records) did not measure the impact of all these investigative interplays, but rather focused on the characteristics of digital evidence in terms of Total Evidence Volume per Case and Heterogeneity of Evidence Items per Case. What the three case studies suggest, however, is that it is also necessary to look at other investigative interplays. The observations carried out in Study One (Investigation of the Dubai Police records) identified how potential factors within investigative interplay like examiner experience may also affect Person-Hours in DF investigation. It would be interesting for future studies to examine the impact of other investigative interplay on Person-Hours, such as the type of DF investigation model.

While investigative interplay would not usually alter or affect the administrative interplay, administrative interplay will have a significant effect on investigative interplay. For example, case generation, as identified in Study Two (Interviews with DF managers), may affect the forensic tools used and the DF investigation model. Likewise, a DF workflow implementation practice, for example team workflow versus tiered workflow, will likely affect or alter the DF investigation process or model, as implemented in a DF department or organisation.

Study One (Investigation of the Dubai Police records) focused mainly on the investigative interplay, while the second and third case studies focused mainly on the administrative interplay, most specifically on the DF case management strategies and workflow implementation practices. The dual examination of both administrative and investigative interplay aimed at answering a primary research aim which was to determine the most common factors behind the delay of DF investigations or the Person-Hours in DF investigation.

What the research ultimately finds is that such factor as Heterogeneity of Evidence Items per Case, is not the only factors that affect Person-Hours in DF investigation, as illustrated by Study One (Investigation of the Dubai Police records). Instead, what affects Person-Hours of investigation is a combination of several factors that impact at the administrative and the investigative layer of DF practice, including the administrative interplay of DF case management strategies and workflow implementation practices, as discovered in the second and third case studies.

6.6. Case Management Strategies and Workflow Implementation Practices Decision Tables

To illustrate the usefulness of this research to DF practitioners the researcher proposes three Decision Tables to assist DF managers to decide on what DF case management strategy and workflow implementation practice could be applied to given conditions. In setting up the Decision Tables, the researcher will first introduce the conditions and actions followed by an analysis of how a DF manager may decide the case management strategy and workflow implementation practice.

Before proceeding, the researcher must make necessary assumptions about the conditions, the effects of which on Person-Hours this research has not fully examined. In all the tables, the researcher assumes equal quantity and quality of DF tools and workstations. Additionally, the researcher assumes that all the DF organisations use the DFRWS DF investigation model, and the MDEC DF crime scene process. Also, the researcher assumes that the received cases can be with varying Total Evidence Volume and Heterogeneity of Evidence Items per Case, that all the DF examiners in the organisation are receiving similar training and having similar knowledge, and that the hiring and promotion policies of the DF organisation are alike. The researcher notes that the suggested case management strategy actions and workflow implementation practice actions are not standard, and any of the actions could be followed by the examiners in any situation. However, the suggested actions are generated by the researcher from this research and outcomes of the interviews with people who are working in the field for many years.

Any changes to any of the assumed factors in investigative interplay could influence the Person-Hours of DF investigation. For example, not having the necessary DF tools would likely increase the Person-Hours. Likewise, using a DF investigation process like the EDIP, which has 13 activities, may require more Person-Hours than the DFRWS, which has 7 steps. The hiring and promotion policies of the DF organisation will likely affect the performance of the DF examiners. If the DF organisation hires examiners will less than three years of experience and possibly fresh graduates then that variety in the experiences, skills, and knowledge of the examiners requires the organisation to have a good training program alongside a robust and clear hiring and promotion policy.

The following Decision Tables apply to three different sized DF operations: (1) Decision Table 1 where there will be less than 10 examiners (Small Departments /sections). (2) Decision Table 2 with between 11 and 20 examiners (Medium Departments/Sections), and (3) Decision Table 3 with more than 21 examiners (Large departments/Sections). These categories were chosen following the interviews of DF managers and supervisors in Study 2 where the researcher found that the number of examiners working on different DF departments varied from 4 to 82 examiners. Thus, the researcher divided the Decision Tables depending mainly on the number of examiners working on that department.

6.6.1. Decision Table 1

This table can be used by any DF organisation with ten or less DF examiners.

Conditions	R1	R2	R3	R4	R3	R4	R5	R6	R7	R8	R9	R10
Senior	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N
Junior	Y	Y	Y	Y	N	N	N	N	Y	Y	Y	Y
Normal Flow of case generation	Y	Y	N	N	Y	Y	N	N	Y	Y	N	N
Urgent Cases	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N
Case Management Strategies - Actions												
Caseload		X	X	X	X	X	X	X	X	X	X	X
Ability	X	X	X	X	X	X	X	X	X	X	X	X
Parallel team												
Workflow Implementation Practices- Actions												
Traditional	X	X	X	X	X	X	X	X	X	X	X	X
Team	X	X	X	X	X	X	X	X	X	X	X	X
Parallel team												
Outsourced	X	X	X	X	X	X	X	X	X	X	X	X
Tiered		X		X								

Table 11. Decision Table 1

When deciding the DF case management strategy, the DF manager may choose among, or a combination of, the following strategies: caseload strategy, ability strategy, or parallel team strategy. The parallel team strategy will not likely apply because the size of the organisation limits it from creating parallel teams. The DF organisation will likely use either the caseload or the ability strategy. In most cases, the DF manager will apply the caseload strategy, especially where the DF manager views the DF examiners in the organisation as having similar skills, capabilities and knowledge. However, DF managers may also use the ability strategy and assign certain cases to those with more experience, and certain cases to those with less experience. It is likely, however, that the DF manager will only use the ability strategy on urgent cases. In this regard, the use of the ability strategy will depend largely on the DF manager's confidence in the abilities of its examiners. Those organisations with 10 or less DF examiners with similar experience, skill, and knowledge, will mainly rely on the caseload strategy.

When deciding the workflow implementation practices, the DF manager may choose among the following: traditional workflow, team workflow, parallel team workflow, outsourced workflow, and tiered workflow. For the same reasons stated above, the parallel team workflow will not likely apply. The DF manager would mainly rely on a traditional workflow but could also apply the team workflow where all the examiners can go to the crime scene and help in certain processes of the investigation and later the leader of that case will continue the investigation process. The DF manager could also use the outsourced workflow, the only obstacle being any policy or law prohibiting such a practice. In smaller organisations, outsourced workflow can be a helpful alternative or supplement to the existing workflow to enhance or fill any gaps in the organisation's skill, knowledge or experience in specialty areas of DF investigations. The DF manager may also apply a tiered workflow. The reason for the DF manager to apply the tiered strategy is the DF manager's confidence in the abilities of its junior examiners. Thus, it is suggested in the Decision Table to use the tiered strategy when a digital forensic department has both senior and junior examiners, normal flow of cases received and the case to be assigned is not urgent.

In summary, the administrative interplay analysis would lead the DF manager to use the *caseload strategy with a traditional workflow*. The choice of a caseload strategy and traditional workflow over the team-based strategy and workflow implementation affects the

Person-Hours because, as the Study One (Investigation of the Dubai Police records) shows, the number of examiners affects the Person-Hours. In team-based approaches, the organisation will likely lower the Person-Hours. In urgent cases, the DF manager may use the ability strategy. The DF manager would then analyse the investigative interplay, which the researcher has made assumptions around, as stated previously. Certainly, more research is needed to determine whether the impact on Person-Hours is statistically significant.

6.6.2. Decision Table 2

The second Decision Table applies to any DF organisation with between eleven and twenty DF examiners.

Conditions	R1	R2	R3	R4	R3	R4	R5	R6	R7	R8	R9	R10
Senior	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N
Junior	Y	Y	Y	Y	N	N	N	N	Y	Y	Y	Y
Normal Flow of case generation	Y	Y	N	N	Y	Y	N	N	Y	Y	N	N
Urgent Cases	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N
Case Management Strategies - Actions												
Caseload		X	X	X	X	X	X	X	X	X	X	X
Ability	X	X	X	X	X	X	X	X	X	X	X	X
Parallel team	X	X			X	X		X		X		
Workflow Implementation Practices - Actions												
Traditional	X	X	X	X	X	X	X	X	X	X	X	X
Team	X	X	X	X	X	X	X	X	X	X	X	X
Parallel team	X	X			X	X		X		X		
Outsourced		X	X	X	X	X	X	X	X	X	X	X
Tiered		X		X								

Table 12. Decision Table 2

When deciding the DF case management strategy, the DF manager may choose among, or a combination of, the following strategies: caseload strategy, ability strategy, or parallel team strategy. It is expected that a DF organisation with between eleven to twenty examiners will have examiners with a different range of experiences; thus, the organisation could apply the parallel team strategy. However, the DF organisation will not likely adopt this strategy due to inefficiencies as expressed by the overwhelming majority of DF managers in Study Three (Confirmation of the Interviews). Instead, the DF manager will be more likely to use a combination of the caseload and ability strategies. The primary driver in case management will probably be the Number of Evidence Items per Case. In cases with higher evidence items, the DF manager could form a team to lower the Person-Hours. In instances where the case is urgent, the DF manager could use the ability strategy, which the manager could also use to assign cases with special requirements to those with unique experience, skill, or knowledge. The DF manager could also use the caseload strategy to assign cases, aiming to give equal case allocation among all the examiners. Overall, the DF manager in this case will likely apply the ability strategy as the primary case management strategy, or a combination of the ability and caseload strategies.

When deciding the workflow implementation practices, the DF manager may choose among the following: traditional workflow, team workflow, parallel team workflow, outsourced workflow, and tiered workflow.

With the larger number of examiners, the DF manager is less likely to use outsourced workflow as a primary workflow implementation practice. If allowed under the organisational policy or law, the DF organisation may resort to the outsource workflow only when necessary and when no examiner in the organisation has the needed experiences, skills, or knowledge regarding a specialty or new DF field. Even though the organisation has enough examiners to create parallel teams, the DF manager will be unlikely to want to apply this workflow because of inefficiencies. Additionally, the varied flow of cases may require the DF manager to be more efficient in the workflow implementation.

The DF manager could apply the tiered workflow and separate the examiners into senior and junior positions and divide tasks as basic or critical. However, such an approach is best suited in organisations with a well-defined distinction between two groups of examiners. The tiered workflow is likely suitable when the organisation has good numbers of both senior and junior examiners with a normal flow of the cases and with a good number of non-urgent cases.

The DF manager would probably use the traditional or team workflow. However, since the size of the organisation allows it to form teams, the DF manager could best lower the Person-Hours by applying the team workflow, keeping in mind that a higher number of examiners means lower Person-Hours. The DF manager, therefore, would likely apply the team workflow, or a traditional workflow with teams.

In summary, the administrative interplay analysis would lead the DF manager to use the ability strategy as the primary case management strategy, or a combination of the ability and caseload strategies; and either a team workflow or a traditional workflow with teams. The use of the *ability strategy in a team setting* will likely allow the manager to control sufficiently the Person-Hours despite there being cases with varying Total Evidence Volume per Case and Heterogeneity of Evidence Items per Case.

6.6.3. Decision Table 3

This Decision Table applies to large DF organisations with more than twenty-one DF examiners.

Conditions	R1	R2	R3	R4	R3	R4	R5	R6	R7	R8	R9	R10
Senior	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N
Junior	Y	Y	Y	Y	N	N	N	N	Y	Y	Y	Y
Normal Flow of case generation	Y	Y	N	N	Y	Y	N	N	Y	Y	N	N
Urgent Cases	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N
Case Management Strategies- Actions												
Caseload		X	X	X	X	X	X	X	X	X	X	X
Ability	X	X	X	X	X	X	X	X	X	X	X	X
Parallel team	X	X			X	X		X		X		
Workflow Implementation Practices- Actions												
Traditional	X	X	X	X	X	X	X	X	X	X	X	X
Team	X	X	X	X	X	X	X	X	X	X	X	X
Parallel team	X	X			X	X		X		X		
Outsourced												
Tiered		X		X		X						

Table 13. Decision Table 3

In a larger organisation, when deciding the DF case management strategy, the DF manager may again choose among, or a combination of, the following strategies: caseload strategy, ability strategy, or parallel team strategy. While most DF organisation will not likely adopt the parallel team strategy, in a larger organisation the DF manager could use the parallel team strategy to enhance its existing training program, and to manage cases assigned to junior examiners more effectively. The DF manager could create two teams that could be assigned the same cases, and the teams could be tasked to identify areas of improvements and supplement each other's work. The team with the best performance could be given incentives like a bonus, given more challenging cases, and promoted to a higher position.

The DF manager could also apply either the caseload or the ability strategy for any received case. If junior members are working in teams, then the caseload strategy, where the DF manager assigns the cases based on the Number of Cases or the number of exhibits already assigned to the examiners, would be the most applicable alongside the parallel strategy.

When deciding the workflow implementation practices; with the varied experiences, skills, or knowledge of the examiners, the DF manager is not very likely to use outsourced workflow. If allowed under the organisational policy or law, the DF organisation may resort to outsource workflow only when necessary and when no examiner in the organisation has the needed experiences, skills, or knowledge regarding a specialty or new DF field. Given that the organisation may be considering team competition with junior members to enhance training, in that case a parallel team workflow might be chosen to match the parallel team strategy.

An alternative is for the DF manager to apply the tiered workflow and separate the examiners into senior and junior positions and divide tasks as basic or critical. This is best suited in organisations with a well-defined distinction between two groups of examiners. The tiered workflow could be suitable if the DF manager does not already use the parallel team workflow and the parallel team strategy.

It is most likely that the DF manager will use the traditional or team workflow if the DF manager employs the parallel team strategy and workflow. The DF manager may use the team workflow to lower the Person-Hours especially in instances where there is a sudden increase in cases with a higher number of exhibits. The DF manager, however, would likely apply the traditional workflow for examiners with more experienced examiners.

In summary, the administrative interplay analysis would lead the DF manager to use the *caseload strategy* for examiners with less experienced examiners, alongside the parallel strategy. For the workflow implementation practice, the DF manager will likely use the *traditional workflow* for examiners with more experienced examiners alongside the parallel workflow. The use of the parallel team strategy and workflow will allow the DF manager to enhance the DF organisation's training and performance of those with less than three years of experience, an option that becomes more viable in an organisation with a steady flow of cases.

CHAPTER 7: CONCLUSION

In this chapter, the researcher concludes the thesis by reviewing and discussing the research questions, summarising the main contributions of the research, highlighting the limitations of the research, and suggesting future work that may further enhance understanding of the phenomena discussed in this research.

7.1. Review and Discussion of Research Questions

At the outset, the research stated that the aim of this research was to identify different factors that create delay in DF investigation and affect DF investigation processes. The researcher proceeded to achieve the research aim by answering the following research questions:

Research Question 1:
What are the trends and challenges encountered by practitioners faced with large volume/heterogeneity DF investigations?

Research Question 2:
What is the effect of different factors on the delay of DF investigation process?

Research Question 3:
What are the different case management strategies and workflow implementation practices currently used?

It becomes necessary to review and discuss each of these research questions to provide closure to the research.

7.1.1. Research Question 1

The first research question asked the following question: "*What are the challenges and trends encountered by practitioners faced with large volume/heterogeneity DF investigations?*" The researcher has sufficiently answered the first research question. The researcher found in the literature several challenges practitioners faced when conducting DF investigations including; (1) heterogeneous sources of digital evidence, (2) data diversity, (3) the use of anti-forensics, (4) Total Evidence Volume per Case, (5) legal requirements, and (6) inefficiencies in DF departments.

In order to answer the research question further, the researcher conducted Study One (Investigation of the Dubai Police records), which asked three questions. First, the case study wanted to determine the trends in DF cases investigated over the past twelve years. Second, the case study wanted to determine the influence of the Total Evidence Volume per Case on the DF investigation process. Third, the study sought to determine the influence on Heterogeneity of Evidence Items per Case on the DF investigation process. Through these three questions posed in Study 1, the researcher answered the first research question. The researcher found that there *was an increase in the number and volume of cases*. Of the various sections in the Dubai Police DF Department, the Computer and Mobile Sections received the highest increase in the Number of Cases, while cases in the Network Section took the longest to investigate. The average Number of Evidence Items per Case and the average number of examiners working on a case remained between one and two.

It was found also that the Heterogeneity of Evidence Items per Case, as opposed to the Volume, affects the Person-Hours of investigation. There was also an effect of examiner experience and on the specificity of the case as detailed on the total number of Person-Hours.

7.1.2. Research Question 2

The second research question asked the following question: "*What are the effects of different factors on the delay of DF investigation process?"* The researcher has sufficiently answered the second research question. Study One (Investigation of the Dubai Police records) found that Heterogeneity of Evidence Items per Case affects moderately the time spent in investigation. From Study 2 and 3, the researcher found several common factors behind the delay of DF investigations that the researcher divided into administrative and investigative factors. The administrative factors include (1) lack of staff, (2) the number of examiners working on a case, (3) the experience of examiners, (4) delay in receiving the public prosecution report, (5) delay in shifting the exhibits from one department to another, and (6) unclear case details. Investigative factors include (1) the number of exhibits, (2) uses of anti-forensic techniques, (3) use of cloud computing, (4) use of password protected files/drive or mobiles, (5) use of social media applications, (6) use of network intrusions, and (7) the capability of the DF tools and software.

7.1.3. Research Question 3

The third research question asked the following question: "*What are the different case management strategies and workflow implementation practices currently used?"* The researcher has sufficiently answered the third research question. In the second and third case studies, the researcher identified and evaluated DF case management strategies and workflow implementation practices that DF managers use to manage and maintain factors affecting different DF case processes. The researcher identified three types of DF case management strategies: (1) caseload strategy, (2) ability strategy, and (3) parallel team strategy. The researcher further identified five workflow implementation practices: (1) traditional workflow, (2) team workflow, (3) parallel team workflow, (4) outsourced workflow, and (5) tiered workflow.

After that, the researcher posed a series of Decision Tables that demonstrate the systematic application of the identified DF case management strategies and workflow implementation practices. The systematic application of these strategies and practices can help DF managers manage cases. Additionally, the researcher identified the administrative and investigative interplays that affect the Person-Hours of investigations and can therefore help managers control the cases.

7.2. Research Contribution

The main contribution of this research is in the use of real cases records from the Dubai Police (DP) Databases and reports to indicate the trends, factors and challenges affecting the digital forensic investigation processes. A second contribution is the findings from the research of the experiences of the interviewed digital forensic managers and supervisors to identify challenges, case management strategies, and workflow implementation practices. Furthermore, this research suggests several Decision Tables that can assist DF managers and supervisors to consider best, and alternative, suggested case management procedures and workflow implementations.

The research can improve efficiencies and effectiveness in DF organisations, case management, and processes by identifying factors that contribute to delay in DF investigations, identifying existing gaps in the current research regarding these factors, and proposing a series of case management and allocation Decision Tables for addressing these factors. Further, the research identified factors that affect the time of investigation and categorised these factors as either administrative or investigative

Because minimal research exists that explores the techniques to optimize the complicated and timely process of case management prior to the start of the investigation process (James, 2014), the research contributes to a gap in the literature. While there are numerous papers proposing DF investigation models no research paper, that the researcher is aware of, explicitly talks about DF case management in DF departments or organisations. There has been a lack of studies concerning DF workflow implementation practices. The researcher's identification of the three DF case management strategies (caseload, ability, and parallel team) and five workflow implementation practices (traditional, team, parallel team, outsourced, and tiered) is, therefore, an important research contribution.

Further, the research reveals the further need to discover and document the various DF case management strategies and workflow implementation practices employed by DF managers. The research suggests that DF managers should pay attention to, and weigh the advantages and disadvantages of, a variety of DF case management strategies and workflow implementation practices.

7.3. Limitations of the Research

The research has several limitations, the biggest of which was the lack of enough time and resources within a Ph.D. program to do more. The researcher initially planned to conduct a grounded theory research with the aim of proposing a theory concerning methods and factors affecting DF case management, allocation, and completion but this was not possible in the time available. Researchers have recognised the time and resource challenges in a mixed methods research, and the limitations such challenges inherently pose.

There were also limitations relating to the secondary data used in Study One (Investigation of the Dubai Police records). The use of secondary data, while having the advantage of time and affordability, has an inherent limitation in that the data were not collected with the research questions in mind. Not being able to compare data from one DF department with data from another DF department is a further limitation.

Concerning the second and third case studies, there were limitations as to the number of interviewees. A higher number of participants may have revealed other DF case management strategies and workflow implementation practices. Finally, that a smaller number of the same participants participated in Study 3 (Confirmation of the Interviews) is another limitation in verifying and evaluating the findings from Study 2 (Interviews with DF managers). The researcher, therefore, hopes to complete future research to work on expanding the quantitative and qualitative findings in this research.

7.4. Further Work

Concerning Study One (Investigation of the Dubai Police records), analysis shows that there is no one factor that single-handedly affects the time of investigation. Instead, a combination of many factors correlates to the delay in investigation. Future work could be done with the aim of creating exact measures of time on the various factors that affect the time of DF investigation. Additionally, further observations that take additional factors and assumptions into account could be made to identify more factors behind the delay of cases.

Another line of enquiry would be to complete the study by deeply examining selected cases to check how much Total Evidence Volume per Case the examiners receive in real cases and measure the volume they examine out of the Total Evidence Volume per Case received. Of course, further work could be done with data from other DF departments or organisations so that the quantitative findings of this research may be tested.

While the research begins to identify administrative and investigative factors in the Person-Hours of DF investigation, future work may test these factors with further quantitative and qualitative studies that may also identify several other factors not found in this research. Additionally, future qualitative studies could be undertaken to identify other DF case management strategies. The researcher believes that there may be more case management strategies employed by various DF organisations. Further work may even be undertaken to consider smaller DF departments or organisations and comparing those strategies with lager counterparts. Future qualitative studies could be undertaken to identify other workflow implementation practices. Again, the researcher believes that there may be a few more workflow implementation practices employed by various DF organisations.

REFERENCES

ABIresearch. (2013). More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020. Retrieved 29/1, 2015, from https://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne

AccessData. (2013). Retrieved 18-December, 2013, from http://www.accessdata.com/products/digital-forensics/ftk

AccessData. (2013). Retrieved 14-April, from http://www.accessdata.com/products/digital-forensics/ftk

ACPO, P. u. (2007). Good Practice Guide for Computer-Based Electronic Evidence. 4. Retrieved 19-December, 2013, from http://www.7safe.com/electronic_evidence/#

ACPO Managers Guide (2011): Good Practice ad Advice Guide for Managers of eCrime Investigation. Version 1.4. http://www.acpo.police.uk/documents/crime/2011/201103CRIECI14.pdf.

Adedayo, O. (June 2016). Big Data and Digital Forensics: Rethinking Digital Forensics. Paper presented at the 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF). Vancouver, British Columbia.

Ademu, I. O., Imafidon, C. O., & Preston, D. S. (2011). A New Approach of Digital Forensic Model for Digital Forensic Investigation. IJACSA) International Journal of Advanced Computer Science and Applications, 2(12).

Allard, A. (2010). Examining the Relationship between Organizational Culture and Performance: Moderators of Culture Gap. Published thesis (Ph.D.) Northcentral University.

Almarzooqi, A. (2016). Digital Forensics Practices: A Road Map for Building Digital Forensics Capability. Published thesis (Ph.D.) DeMontfort University, Leicester, U.K.

Altiero, R. (2015). Digital Forensics Tool Interface Visualization. Published thesis (Ph.D.). Nova Southeastern University.

Anderson, W. L. (2004). Some challenges and issues in managing, and preserving access to, long-lived collections of digital scientific and technical data. Data Science Journal, 3(30), 191-202.

Andrews, L., Higgins, A., Andrews, M. W., & Lalor, J. G. (2012). Classic grounded theory to analyse secondary data: Reality and reflections. The Grounded Theory Review, 11(1), 12-26.

Antoniol G, Casazza G, DiLucca GA, DiPenta M, Rago F. A queue theory-based approach to staff software maintenance centers. In: Proceedings of the IEEE international conference on software maintenance, Florence, Italy, 2001.

Arpaci, I., Yardimci, Y., & Turetken, O. (2015). A Cross-Cultural Analysis of Smartphone Adoption by Canadian and Turkish Organizations. Journal of Global Information Technology Management, vol. 18, 2015, Issue 2, pp.214-238.

Athanasou, J. A., & Van Esbroeck, R. (2008). International handbook of career guidance: Springer.

Atlas. (2017). Digital Forensics Case Management, Improved. from http://sentineldata.com/atlas-digital-forensic-case-management/

Babbie, E. (1990). Survey Research Methods. Belmont, CA: Wadsworth Publishing.

Bakotić, D. (2016). Relationship between job satisfaction and organisational performance. Economic Research-Ekonomska Istraživanja Vol. 29 , Iss. 1.

Ballou, S. (2010). Electronic crime scene investigation: A guide for first responders: Diane Publishing.

Barbara, J. (2014). Streamlining the Digital Forensic Workflow: Part 2. Forensic Magazine. Available at https://www.forensicmag.com/article/2014/09/streamlining-digital-forensic-workflow-part-2 (last accessed Sept. 25, 2017).

Barrett, D. J. (Producer). (2012, 2/1/2015). Retrieved from http://tedxtalks.ted.com/video/The-Internet-of-Things-Dr-John

Barretoa, A., de O. Barrosb, M., Wernera.C. (2007). Staffing a software project: A constraint satisfaction and optimization-based approach. Computers & Operations Research 35 (2008) 3073 – 3089.

Baryamureeba, V., & Tushabe, F. (2004, August). The enhanced digital investigation process model. In Proceedings of the Fourth Digital Forensic Research Workshop.

Beebe, N., & Clark, J. (2005). Dealing with terabyte data sets in digital investigations Advances in Digital Forensics (pp. 3-16): Springer.

Beebe, N. L., & Clark, J. G. (2005). A hierarchical, objectives-based framework for the digital investigations process. Digital Investigation, 2(2), 147-167.

Beech, I. (1999). Bracketing in phenomenological research. Nurse Researcher, 6(3), 33-35

Bell, J. (2005) Doing your research project: a guide for first-time researchers in education, health and social science. Maidenhead: Open University Press

Bohm, G., & Zech, G. (2010). Introduction to statistics and data analysis for physicists: DESY.

Bouchard, R. F., & Franklin, J. D. (1980). Guidebook to the Freedom of Information and Privacy Acts [and] 1981 Supplement: ERIC.

Boyer, S. A. (2009). SCADA: supervisory control and data acquisition: International Society of Automation.

Bowcott, O. (2013). Big Data: police given access to British army's crime-fighting software., Technology, *theguardian*. Retrieved from http://www.theguardian.com/technology/2013/aug/07/big-data-police-army-software

Brewer, E. (2001) Mixed Method Research Designs in Farmer, E. & Rojewski, J. (2001). Research Pathways: Writing Professional Papers, Theses, and Dissertations in Workforce Education. University Press of America.

Brezinski, D., & Killalea, T. (2002). Guidelines for evidence collection and archiving. RFC3227.

Brezinski, D., & Killalea, T. (2002). Guidelines for evidence collection and archiving. Request For Comments, 3227.

Browne, K. (2006). Introducing sociology for AS level: Polity.

Bryman, A. (2008). Social Research Methods. Oxford University Press.

Caine, C. & Haque, S. (2008). Organizational Workflow and Its Impact on Work Quality in Hughes, R.G. (2008). Patient Safety and Quality: An Evidence-Based Handbook for Nurses.

CAINE. (2012). Computer Forensics Linux Live Distro. Retrieved 28-4, 2014

Campbell, D. T., & Fiske, D. W. (1959). Convergent and discriminant validation by the multitrait-multimethod matrix. Psychological bulletin, 56(2), 81.

Carrier, B. (2013). Digital Forensics Maximising Examiner Efficiency. Basis Technology. Retrieved from www.basistech.com/datasheets/Digital-Forensics-EN.pdf

Carrier, B., & Spafford, E. H. (2003). Getting physical with the digital investigation process. International Journal of Digital Evidence, 2(2), 1-20.

Carrier, B. D., & Spafford, E. H. (2006). Categories of digital investigation analysis techniques based on the computer history model. digital investigation, 3, 121-130

Casey, E. (2009). Handbook of Digital Forensics and investigation. Academic Press.

Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (3 ed. Vol. 1). Waltham, MA: Academic Press.

Casey, E., Katz, G., & Lewthwaite, J. (2013). Honing digital forensic processes. Digital Investigation, 10(2), 138-147.

Chen, W. and Hirschheim, R. (2004) A paradigmatic and methodological examination of information systems research from 1991 to 2001. Information Systems Journal, 14(3), pp.197–235

Choudrie, J. and Dwivedi, Y. (2005) Research design: Investigating the research approaches for examining technology adoption issues. Journal of Research Practice, 1(1), pp. 1-12.

Ciardhuáin, S. Ó. (2004). An extended model of cybercrime investigations. International Journal of Digital Evidence, 3(1), 1-22.

CISCO (2016). Cisco Global Cloud Index: Forecast and Methodology, 2015–2020. Available at https://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.pdf (last accessed Sept 17, 2017).

Cilesiz, S. (2011). A phenomenological approach to experiences with technology: Current state, promise, and future directions for research. Educational Technology Research and Development, 59(4), 487-510.

Clarke R. J (2005) Research Models and methodologies. HDR Seminar Series. http://iihsdphy.weebly.com/uploads/8/0/2/4/8024844/research_3.pdf. Last accessed 29 Aug 2017.

CMSA (2008). Case Management Caseload Concept Paper:
Proceedings of the Caseload Work Group. Available at http://www.cmsa.org/portals/0/pdf/CaseloadCalc.pdf (last accessed Sept. 25, 2017).

Cohen, L., Manion, L., & Morrison, K. (2011). Research methods in education. Routledge.

Collis, J. and Hussey, R. (2003) Business research: A practical guide for undergraduate and postgraduate students. Basingstoke: Palgrave Macmillan.

Cook, T. D, & Campbell, D. T. (1979). Quasiexperimentation: Design and analysis for field settings. Chicago: Rand McNally.

Creswell, J.W. (1994). Research design: Qualitative and quantitative approaches. Thousand Oaks, CA: Sage.

Creswell, J. W. (1995). Research design: Qualitative and quantitative approaches. Thousand Oaks, CA: Sage.

Creswell, J.W. (2003). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. (2nd ed.). SAGE Publication.

Creswell, J. W. (2013). Qualitative inquiry and research design: Choosing among five approaches. Sage.

Creswell, J. W. (2014). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. (4th ed.). SAGE Publication.

Creswell, J. W., & Plano, C. V. L. (2007). Designing and conducting mixed methods research. Thousand Oaks, Calif: SAGE Publications.

Creswell, J. W., Plano Clark, V. L., Gutmann, M. L. and Hanson, W. E. (2003). Advanced mixed methods research designs. In A. Tashakkori, C. Teddlie (Eds.), Handbook of mixed methods in social and behavioral research. Thousand Oaks, CA: Sage, 209–240

Crotty, M. (1998). The Foundations of Social Research: Meaning and Perspective in the Research Process. Australia: Allen and Unwin.

Daniels, A., & Salter, W. (1999). What is SCADA. Paper presented at the International Conference on Accelerator and Large Experimental Physics Control Systems.

Davison, T. (2014). Phenomenological Research Using a Staged Multi-Design Methodology. International Journal of Business, Humanities and Technology, vol. 4, no. 2.

DCI. Iowa Division of Criminal Investigation Retrieved 19-4, 2014, from http://www.dps.state.ia.us/DCI/

Dell. (2011). Dell™ Digital Forensics - Solution Guide.

de Braekt RI, Le-Khac NA, Farina J, Scanlon M, Kechadi T (2016) Increasing Digital Investigator Availability Through Efficient Workflow Management and Automation. In: 2016 4th International Symposium on DigitalForensic and Security (ISDFS), pp 68–73, DOI 10.1109/ISDFS.2016. 7473520

DeMers, J. (2014). 7 Guidelines for Delegating Tasks to Employees Retrieved 3/2, 2016, from http://www.inc.com/jayson-demers/7-guidelines-for-delegating-tasks-to-employees.html

Denscombe, M. (2007) The Good Research Guide: For Small-scale Social Research. (3rd ed.). Buckingham: Open University Press.

Dezfoli, F. N., Dehghantanha, A., Mahmoud, R., Sani, N. F. B. M., & Daryabar, F. (2013).

Digital Forensic Trends and Future. International Journal of Cyber-Security and Digital Forensics (IJCSDF), 2(2), 48-76.

Doherty & Perry. (2001). The cultural impact of workflow management systems in the financial services sector. Service Industries Journal, (August 2011), 37–41. doi:dx.doi.opg/10.1080/714005046.

Dowling, M. (2007). From Husserl to van Manen. A review of different phenomenological approaches. International journal of nursing studies, 44(1), 131-142.

DSC. (2013). Number of estimated population by sector and community.

Duggan J, Byrne J, Lyons G. A task allocation optimizer for software construction. IEEE Software 2004;21(3):76–82

El-Bialy, N. (2011). Measuring judicial performance: (The case of Egypt). [Working Paper n. 14]. German Working Papers in Law and Economics, Berkeley, CA.

Evans, D. (2013, 01/23/2014). Beyond Things: The Internet of Everything, Explained In Four Dimensions. Retrieved 1/29, 2015, from http://www.huffingtonpost.com/dave-evans/cisco-beyond-things-the-interne_b_3976104.html

Faily, S. & Fléchais, I. (2011). User-Centered Information Security Policy Development in a Post-Stuxnet World. 2011 Sixth International Conference on Availability, Reliability and Security (ARES).

Fernández, W. (2004) The grounded theory method and case study data in IS research: Issues and design. In Information Systems Foundations Workshop: Constructing and Criticising, Canberra, Australia.

Flick, U. (2011). Introducing research Methodology. Sage.

Forensics-Research. Computer Forensics History. Retrieved 16-June, 2014, from http://www.forensics-research.com/index.php/computer-forensics/computer-forensics-history/

Fraenkel, J. & Wallen, N. (1996). How to design and evaluate research in education. (3rd ed.). New York: McGraw-Hill.

Fraser, J. (2010). Forensic Science: A very short introduction: Oxford University Press.

Freiling, F. C., & Schwittay, B. (2007). A Common Process Model for Incident Response and Computer Forensics. Proceedings of Conference on IT Incident Management and IT Forensics. Germany.

Gable, G. (1994) Integrating case study and survey research methods: An example in information systems. European Journal of Information Systems, 3(2) pp.112-126.

Garfinkel, S. (2007). "Anti-Forensics: Techniques, Detection and Countermeasures", The 2nd International Conference on i-Warfare and Security (ICIW), Naval Postgraduate School, Monterey, CA, March 8-9, 2007.

Garfinkel, S. (2010). Digital forensics research: The next 10 years. Digital Investigation, 7, Supplement(0), S64-S73. doi: http://dx.doi.org/10.1016/j.diin.2010.05.009

Garfinkel, S. (2012). Lessons learned writing Digital Forensics tools and managing a 30TB digital evidence corpus. Digital Investigation, 9, Supplement(0), S80-S89. doi: http://dx.doi.org/10.1016/j.diin.2012.05.002

Garfinkel, S. L. (2012). Lessons learned writing Digital Forensics tools and managing a 30TB digital evidence corpus. Digital Investigation, 9, Supplement (0), S80-S89. doi: http://dx.doi.org/10.1016/j.diin.2012.05.002

Garfinkel, S. L., & Shelat, A. (2003). Remembrance of data passed: A study of disk sanitization practices. IEEE Security & Privacy, 1(1), 17-27.

Gay, L. & Airasian, P. (2000). Educational research: Competencies for analysis and application. (6th ed.). Upper Saddle River, NJ: Merrill.

Genius-Project. (2017). Genius Project. Retrieved 13/6, 2017, from https://www.geniusproject.com/

Ghasemi, A., & Zahediasl, S. (2012). Normality tests for statistical analysis: a guide for non-statisticians. International journal of endocrinology and metabolism, 10(2), 486.

Giorgi, A. (1986). The" Context of Discovery-Context of Verification" Distinction and Descriptive Human Science. Journal of phenomenological psychology, 17(2), 151.

Glaser, B. G., & Strauss, A. L. (1967). The discovery of grounded theory: Strategies for qualitative research. New Brunswick, NJ: Aldine.

Gogolin, G. (2010). The Digital Crime Tsunami. Digital Investigation, 7(1–2), 3-8. doi: http://dx.doi.org/10.1016/j.diin.2010.07.001

Goodwin, B (2003) Scotland Yard's Computer Crime Unit is cash-strapped but is still catching the crooks. Computerweekly.com, 12 March 2003. Retrieved from: http://www.computerweekly.com (Last Accessed 27-8-2017).

Greene, J. C., Caracelli, V. J., & Graham, W. F. (1989). Toward a conceptual framework for mixed-method evaluation designs. Educational Evaluation and Policy Analysis, 11, 255–274.

C Grobler and C Louwrens. 2007. Digital forensic readiness as a component of information security best practice. New approaches for security, privacy and trust in complex environments (2007), 13–24.

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. Handbook of qualitative research, 2, 163-194.

Guidance, S. (2013). Encase Forensic v7. from https://www.encase.com/products/Pages/encase-forensic/overview.aspx

Guidance, S. (2014). Encase Forensic v7. . from https://www.encase.com/products/Pages/encase-forensic/overview.aspx

Guo, Z., & Sheffield, J. (2008). A paradigmatic and methodological examination of knowledge management research: 2000 to 2004. Decision Support Systems, 44(3), 673–688. doi:10.1016/j.dss.2007.09.006

Hack, S. (1986). Electronic Communications Privacy Act of 1986.

Hadoop. (2014). Apache™ Hadoop®. from http://hadoop.apache.org/

Hanson, W. E., Creswell, J. W., Plano Clark, V. L., Petska, K. P., and Creswell, J. D. (2005). Mixed methods research designs in counseling psychology. Journal of Counseling Psychology 52 (2): 224–35.

Hardy, G. & Corrall, S. (2007). Revisiting the subject librarian: A study of English, Law and Chemistry. Journal of Librarianship and Information Science. 39 (2), 79-91.

Harrell, C. (2010). Overall DF Investigation Process. Retrieved from http://journeyintoir.blogspot.com/2010/10/overall-df-investigation-process.html

Harvey, J. (1987). Measuring Productivity in Professional Services. Public Productivity Review Vol. 11, No. 2 (Winter, 1987), pp. 29-38.

Hogan, D. E., & Burstein, J. L. (2007). General Concepts - Triage Disaster Medicine (secnd ed., pp. 13): Wolters Kluwer.

Hox, J. & Boeije, H. (2005). Data collection, Primary vs. Secondary. In Encyclopedia of Social Measurement, vol. 1, p. 593.

HTCIA. (2010). Report on Cyber Crime Investigation: Roseville, CA, High Technology Crime Investigation Association (HTCIA).

Husserl, E. (1970). The crisis of European sciences and transcendental phenomenology: An introduction to phenomenological philosophy: Northwestern University Press.

INFOSEC Institute (2016). Digital Forensics Models. http://resources.infosecinstitute.com/digital-forensics-models/#gref

Intella. (2013). https://www.vound-software.com/home.

Irons, A., & Lallie, H. S. (2014). Digital Forensics to Intelligent Forensics. Future Internet, 6(3), 584-596.

ISO. (2012). ISO/IEC 27037:2012. from https://www.iso.org/standard/44381.html

ISO-27037, o. (2012). Guidelines for identification, collection, acquisition and preservation of digital evidence. Retrieved 19-December, 2013, from http://www.iso.org/iso/catalogue_detail?csnumber=44381

Ivankova, N.V., Creswell, J.W. and Stick, S.L (2006). Using mixed-methods sequential explanatory design: from theory to practice. Field Methods, 18 (1), pp. 3-20.

Jain, A., & Chhabra, G. S. (2014, 7-9 Aug. 2014). Anti-forensics techniques: An analytical review. Paper presented at the Contemporary Computing (IC3), 2014 Seventh International Conference on.

James, J. I., & Gladyshev, P. (2013). A survey of digital forensic investigator decision processes and measurement of decisions based on enhanced preview. Digital Investigation, 10(2), 148-157.

James, Joshua, I., & Gladyshev, P. (2013). Challenges with Automation in Digital Forensic Investigations. arXiv preprint arXiv:1303.4498.

James, J. I. (2014). Multi-Stakeholder Case Prioritization in Digital Investigations. Journal of Digital Forensics, Security and Law, 9(2), 59-72.

Jawale, N. (2010). Locating and Extracting Digital Evidence from Hosted virtual desktop Infrastructures: Cloud Context. Published thesis (PhD) AUT University.

Jeffries, M. & Jewell, A. (2015). Webinar: How to Adopt a Collaborative Workflow for Faster Digital Forensic Investigations. NUIX. Available at https://www.nuix.com/videos/how-adopt-collaborative-workflow-faster-digital-forensic-investigations (last accessed Sept. 25, 2017).

Johannesson P., Perjons E. (2014) Research Strategies and Methods. In: An Introduction to Design Science. Springer, Cham

Johnson, L. (2013). Forenscs and Big Data Paper presented at the Information Security and Risk Management. http://www.isaca.org/Education/Conferences/Documents/NAISRM-2013-Presentations/222.pdf

Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. Computer, 31(2), 26-34. doi: 10.1109/MC.1998.4655281

Johnson, B., & Turner, L. A. (2003). Data collection strategies in mixed methods research. Handbook of mixed methods in social and behavioral research, 297-319.

Johnson, R.B., & Onwuegbuzie, A.J. (2004). Mixed methods research: A research paradigm whose time has come. Educational Researcher, 33(7), 14-26

Johnson, R., Onwuegbuzie, A. And Turner, L. (2007) Toward a Definition of Mixed Methods Research. Journal of Mixed Methods Research, 1(2) 112-133.

Johnston, M. (2014). Secondary Data Analysis: A Method of which the Time Has Come. Qualitative and Quantitative Methods in Libraries (QQML) 3:619 –626.

Jones, A., & Valli, C. (2009). Building a Digital Forensic Laboratory: Establishing and Managing a Successful Facility. Syngress Media Incorporated.

Jones, A., & Valli, C. (2011). Building a digital forensic laboratory: Establishing and managing a successful facility: Butterworth-Heinemann.

Jones, B., Pleno, S., & Wilkinson, M. (2012). The use of random sampling in investigations involving child abuse material. Digital Investigation, 9, S99-S107.

Jusas, V., Birvinskas, D., Gahramanov, E. (2017). Methods and Tools of Digital Triage in Forensic Context: Survey and Future Directions. Symmetry. MDPI. http://www.mdpi.com/2073-8994/9/4/49/pdf-vor.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to Integrating Forensic Techniques into Incident Response, NIST Special Publication 800-86. Gaithersburg: National Institute of Standards and Technology.

Keppel, G. (1991). Design and Analysis: A Researcher's Handbook (3rd ed.). Englewood Cliffs, NY: Prentice Hall.

Kessler, G. C. (2007). Anti-forensics and the digital investigator. Paper presented at the Australian Digital Forensics Conference.

Kim, Y. & Ployhart, R. (2014). The Effects of Staffing and Training on Firm Productivity and Profit Growth Before, During, and After the Great Recession. Journal of Applied Psychology. 2014, Vol. 99, No. 3, 361–389.

Kueng P. (2000) The Effects of Workflow Systems on Organizations: A Qualitative Study. In: van der Aalst W., Desel J., Oberweis A. (eds) Business Process Management. Lecture Notes in Computer Science, vol 1806. Springer, Berlin, Heidelberg

Kohn, M., Eloff, J., & Oliver, M. (2006). Framework for a Digital Forenisc Investigation. Proceedings of Information Security South Africa (ISSA) 2006 from Insight to Foresight Conference. South Africa.

Konkel, F. (2013). Boston probe's Big Data use hints at the future, *FCW The Business of Federal Technology*. Retrieved from http://fcw.com/articles/2013/04/26/big-data-boston-bomb-probe.aspx

Kumar, A., Van Der Aalst, W. M., & Verbeek, E. M. (2002). Dynamic work distribution in workflow management systems: How to balance quality and performance. Journal of Management Information Systems, 18(3), 157-193.

Lamersdorf, A., Munch, J., del Viso Torre, A., S’nchez, C. (2011). A Risk-Driven Model for Work Allocation in Global Software Development Projects. 2011 6th IEEE International Conference on Global Software Engineering (ICGSE).

Langdridge, D. (2007). Phenomenological psychology: Theory, research and method. Harlow: Pearson Education.

Lanka, S. (2011). Enhancing Forensic Investigation in Large Capacity Storage Devices using WEKA: A Data Mining Tool. Texas A&M University.

Laverty, S. M. (2003). Hermeneutic phenomenology and phenomenology: A comparison of historical and methodological considerations. International journal of qualitative methods, 2(3), 21-35.

LeCompte, M. D., & Schensul, J. J. (1999). Designing & conducting ethnographic research. Walnut Creek, Calif: AltaMira Press.

Leedy, P.D. & Ormrod, J.E. (2005). Practical research: planning and design. New Jersey: Pearson Merrill Prentice-Hall.

Leong, R. (2006). Challenges to Digital Forensics from cloud computing. Symposium conducted at the meeting of the DFRWS, Hong Kong. Retrieved from www.dfrws.org/2006/proceedings/4-Ieong.pdf

Leong, R. S. C. (2006). FORZA – Digital forensics investigation framework that incorporate legal issues. Digital Investigation, 3, Supplement(0), 29-36. doi: http://dx.doi.org/10.1016/j.diin.2006.06.004

Lima. (2017). Lima Forensic Case Management. from https://www.intaforensics.com/lima/?v=ea8a1a99f6c9

Lincoln, Y. S. and Guba, E. G. (2000). Paradigmatic controversies, contradictions, and emerging influences. In N. Denzin and Y. Lincoln (eds.), Handbook of Qualitative Research (2nd ed., pp. 163-188). Thousand Oaks, CA: Sage.

LoBiondo-Wood, G. & Haber, J. (1998). Nursing research: Methods, critical appraisal, and utilization (4th ed.). St. Liouis, MO: Mosby.

Maguire, C., Houck, M., Williams, R., & Speaker, P. (2012). Efficiency and the Cost-Effective Delivery of Forensic Science Services: Insourcing, Outsourcing, and Privatization. Forensic Science Policy & Management: An International Journal Vol. 3 , Iss. 2, 2012.

Marshall, C. and Rossman, G. (1999). Designing qualitative research. Sage Publications

Marshall, C. and Rossman, G. (2006) Designing qualitative research. 4th ed. Thousand Oaks: Sage.

Marturana, F., & Tacconi, S. (2013). A Machine Learning-based Triage methodology for automated categorization of digital media. Digital Investigation, 10(2), 193-204.

Mason, J. (2002) Qualitative Researching. London: Sage Publications.

Mason, J. (2006). Mixing methods in a qualitatively driven way. Qualitative Research, 6(1), 9-25.

MDEC. (2015). Digital Evidence Guide for First Responders. Massachusetts Digital Evidence Consortium.
Microsoft. (2017). Microsoft-Project-Management. from https://products.office.com/en/project/project-management

Mertens, D. M. (1998). Research methods in education and psychology: Integrating diversity with quantitative and qualitative approaches. London: Sage.

Mertens, D. M. (2003). Mixed methods and the politics of human research: The transformative-emancipatory perspective. In A.Tashakkori & C.Teddlie

(Eds.), Handbook of mixed methods in social and behavioral research (pp. 135–164). Thousand Oaks, CA: Sage.

Mohay, G. M. (2003). Computer and intrusion forensics: Artech House.

Mohay, G. (2005, 7-9 Nov. 2005). Technical challenges and directions for Digital Forensics. Paper presented at the Systematic Approaches to Digital Forensic Engineering, 2005. **First** International Workshop **on**.

Monica, D., Devi, S., Subashini, D., & Devi, R. (2014). Scheduling and Resource Allocation for Employees in Software Projects. International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Volume-2, Issue-5, May-2014.

Mora, R.-J., & Kloet, B. (2010). Digital forensic sampling. Hoffmann Investigations, Almere The Netherlands Digital forensics and incident response. Retrieved from http://computer-forensics.sans.org/blog/2010/03/29/digital-forensic-sampling/

Moser, A., & Cohen, M. I. (2013). Hunting in the enterprise: Forensic triage and incident response. Digital Investigation, 10(2), 89-98.

Moustakas, C. (1994). Phenomenological research methods. Sage Publications.

MPS-DEFS. (2015). London Metropolitan Police Service Digital Electronics and Forensics Service. from http://content.met.police.uk/Home

Mueller, L. (2013). A glimpse into the workflow of a digital investigator – David Cowen. Magnet Forensics. Available at https://www.magnetforensics.com/computer-forensics/a-glimpse-into-the-workflow-of-a-digital-investigator-david-cowen/ (last accessed Spet. 25, 2017).

Myers, M. (1997) Qualitative Research in Information Systems, MISQuarterly 21, pp. 241-242

Nelson, B., Phillips, A., & Steuart, C. (2014). Guide to computer forensics and investigations: Cengage Learning.

Neuman, L. (2000). Social research methods: qualitative and quantitative approaches. (4th ed.) Boston: Allyn & Bacon.

Neuman, W. (2004) Basic of social research qualitative and quantitative approaches. Boston, MA: Pearson/Allyn and Bacon.

Neuman, W. (2006) Social research methods: qualitative and quantitative approaches. 6th ed. Boston: Pearson.

Neuman, W. (2011) Social research methods: qualitative and quantitative approaches. 7th ed. Boston: Pearson.

Nirkhi, S. M., Dharaskar, R., & Thakre, V. (2012). DATA MINING: A PROSPECTIVE APPROACH FOR DIGITAL FORENSICS. International Journal of Data Mining & Knowledge Management Process, 2(6).

Nuix. The Investigative Lab: A Model for Efficient Collaborative Digital Investigations.

NUIX. (2013). Nuix Investigator Workstation. From http://www.nuix.com/

Oates, B.J. (2006). Researching Information Systems and Computing. Middlesborough UK: Sage Publications Ltd.

O'Brien, R. (2001). An Overview of the Methodological Approach of Action Research in Roberto, R. (Ed.), Theory and Practice of Action Research. Available at http://www.web.ca/~robrien/papers/arfinal.html (Last accessed 29 Aug 2017).

Onwuegbuzie, A. J., and C. Teddlie. 2003. A framework for analyzing data in mixed methods research. In Tashakkori, A. & Teddlie, C. (eds.) (2003). Handbook on mixed methods in the behavioural and social sciences. 351–84. Thousand Oaks, CA: Sage.

Oracle. (2017). Project Management Cloud from https://cloud.oracle.com/project-management-cloud

Orlikowski, W.J. & Baroudi, J.J. (1991). "Studying Information Technology in Organizations: Research Approaches and Assumptions", Information Systems Research (2), pp. 1-28.

Osborne, G., Turnbull, B., & Slay, J. (2010, 15-18 Feb. 2010). The "Explore, Investigate and Correlate' (EIC) Conceptual Framework for Digital Forensics Information Visualisation. Paper presented at the Availability, Reliability, and Security, 2010. ARES '10 International Conference on.

Overill, R. E., Silomon, J. A. M., & Roscoe, K. A. (2013). Triage template pipelines in digital forensic investigations. Digital Investigation, 10(2), 168-174. doi: http://dx.doi.org/10.1016/j.diin.2013.03.001

Palmer, G. (2001). A Road Map for Digital Forensic Research. Paper presented at the First Digital Forensic Research Workshop (DFRWS), Utica, New York.

Papadimitriou, S., & Jimeng, S. (2008, 15-19 Dec. 2008). DisCo: Distributed Co-clustering with Map-Reduce: A Case Study towards Petabyte-Scale End-to-End Mining. Paper presented at the Eighth IEEE International Conference on Data Mining, 2008. ICDM '08.

Paridis, E., O'Brien, B., Nimmon, L., Bandiera, G., & Martimianakis, M.A. (2016). Design: Selection of Data Collection Methods. Journal of Graduate Medical Education, May 1, 2016, p. 263.

Patten, M.L. (1997). Understanding research methods: An overview of the essentials. Los Angeles: Pyrczak.

Patton, M. Q. (1990). Qualitative evaluation and research methods . SAGE Publications, inc. Peisert, S., Bishop, M., & Marzullo, K. (2008,). Computer forensics in forensis. In Systematic Approaches to Digital Forensic Engineering, 2008. SADFE'08. Third International Workshop on (pp. 102-122). IEEE.

Patton, M. Q. (2002). Two decades of developments in qualitative inquiry a personal, experiential perspective. Qualitative social work, 1(3), 261-283.

Peng, G.C., & Annansingh, F. (2015). Experiences in Applying Mixed Methods Approach in Information Systems Research. In Research Methods: Concepts, Methodologies, Tools, and Applications. IGI Global. 2105.

Peng, G.C., Nunes, J.M.B. and Annansingh, F. (2011). Investigating information systems with mixed-methods research. In; Proceedings of the IADIS International Workshop on Information Systems Research Trends, Approaches and Methodologies (ISRTAM), 20 July 2011, Rome, Italy

Perumal, S. (2009) Digital forensic model based on Malaysian investigation process Vol. 9 (8) Available at: (http://paper.ijcsns.org/07_book/200908/20080805.pdf)

Petty, M. M., D. F. Chapman, C. M. Lowery and D. W. Connell (1995). Relationships Between Organizational Culture and Organizational Performance, Psychological Reports 76(2), 483–492.

Phillips, D. C., & Burbules, N. C. (2000). Postpositivism and educational research. New York: Rowman & Littlefield.

Pickard, A. (2013). Research Methods in Information. (2ns ed.). Facet.

Piriform. (2014). Recuva. from http://www.piriform.com/recuva

Pollitt, M. “Computer Forensics (1995): an Approach to Evidence in Cyberspace”, Proceedings (Vol. II, pp 487-491) of the National Information Systems Security Conference, Baltimore, MD. 1995 http://www.digitalevidencepro.com/Resources/Approach.pdf

Pollitt, M. M. (2001, October). Report on digital evidence. In 13th INTERPOL Forensic Science Symposium.

Pollitt, M. M. (2007, April). An ad hoc review of digital forensic models. In Systematic Approaches to Digital Forensic Engineering, 2007. SADFE 2007. Second International Workshop on (pp. 43-54). IEEE.

Pollitt, Mark. "A history of Digital Forensics." IFIP International Conference on Digital Forensics. Springer, Berlin, Heidelberg, 2010.

Pooe, A. & Labuschagne, L. (2013). Cognitive Approaches for Digital Forensics Readiness Planning in Peterson, G. & Shenoi, S. (Eds.) (2013). Advances in Digital Forensics. IX, IFIP AICT 410, pp. 53-56.

Powell, R. & Connaway, L. (2004). Basic research methods for librarians. Connecticut: Libraries Unlimited.

Prefuse. (2013). the prefuse visualization toolkit. from http://prefuse.org/

ProdicoverForensics. Computer Forensic Tool for Law Enforcement.

Punch, K. F. (1998). Introduction to social research: Quantitative and qualitative approaches. Thousand Oaks, CA: Sage.

Quick, D., & Choo, K.-K. R. (2014). Impacts of increasing volume of digital forensic data: A survey and future research challenges. Digital Investigation, 11(4), 273-294. doi: http://dx.doi.org/10.1016/j.diin.2014.09.002

Quinn, P. M. (2002). Qualitative research and evaluation methods. California EU: Sage Publications Inc.

Raasch, J., & Geary, M. (2010, 12, July). Child porn prosecutions delayed by backlog of cases. Retrieved 14-Apri, 2014, from http://www.easterniowanewsnow.com/2010/07/12/child-porn-prosecutions-del

Reinard, J. (1998). Introduction to communication research (2nd ed.). Boston: McGraw Hill.

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. International Journal of Digital Evidence, 1(3), 1-12.

Remenyi, D., Williams, B., Money, A. & Swartz, E. (1998). Doing Research in Business and Management. An Introduction to Process and Method. London: Sage.

Robson, C. (2002) Real World Research. Oxford: Blackwell

Rogers, M., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer Forensics Field Triage Process Model. Proceedings of Conference on Digital Forensics, Security and Law (pp. 27-40).

Rossman, G. B., & Wilson, B. L. (1985). Numbers and words: Combing quantitative and qualitative methods in a single large-scale evaluation study. Evaluation Review, 9, 627–643.

Roussev, V. (2011). Building Open and Scalable Digital Forensic Tools. Paper presented at the 2011 IEEE Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE).

Roussev, V., & Golden, R. (2004). Breaking the performance wall: The case for distributed Digital Forensics. Paper presented at the Proceedings of the 2004 Digital Forensics Research Workshop.

Roussev, V., Wang, L., Richard, G., & Marziale, L. (2009). A cloud computing platform for large-scale forensic computing Advances in Digital Forensics V (pp. 201-214): Springer.

Roy, M. B. (2014). An analysis of the applicability of federal law regarding hash-based searches of digital media. Monterey, California: Naval Postgraduate School.

Ruskova NA. Decision support system for human resources appraisal and selection. In: First international symposium intelligent systems, Varna, Bulgaria, September 2002. p. 354–7.

Saferstein, R. (2004). Criminalistics: An introduction to forensic science.

Sanya-Isijola, A. (2009). Models of Digital Forensic Investigation: University of East London.

SANS. (2013). The SANS Survey of Digital Forensics and Incident Response.

Saunders, M. Lewis, P. and Thornhill, A. (2003) Research methods for business students. London: Prentice Hall.

Schnaider LRC, Staffing planning in enterprise oriented software development environments, MSc thesis, COPPE/UFRJ, Brasil, 2003.

Schuster, A. (2008). The impact of Microsoft Windows pool allocation strategies on memory forensics. Digital Investigation, 5, Supplement(0), S58-S64. doi: http://dx.doi.org/10.1016/j.diin.2008.05.007

Sekaran, U. (2003). Research methods for business: A skill building approach. New York: Wiley.

Selamat, S., Yusof, R., & Sahib, S. (October 2008). Mapping Process of Digital Forensic Investigation Framework. International Journal of Computer Science and Network Security, vol. 8, no.10.

Shaw, A., & Browne, A. (2013). A practical and robust approach to coping with large volumes of data submitted for digital forensic examination. Digital Investigation, 10(2), 116-128.

Sleuthkit. (2013). from http://www.sleuthkit.org/

Smart-Sheet. (2017). Retrieved 13/6, 2017, from https://www.smartsheet.com/

Smith, E. (2008). Using secondary data in educational and social research. New York, NY: McGraw-Hill Education.

Smith, A. K., Ayanian, J. Z., Covinsky, K. E., Landon, B. E., McCarthy, E. P., Wee, C. C., & Steinman, M. A. (2011). Conducting high-value secondary dataset analysis: An introductory guide and resources. Journal of General Internal Medicine, 28(8), 920-929. doi:10.1007/s11606-010-1621-5

Sommer, P. (2011). Certification, registration and assessment of digital forensic experts: The UK experience. Digital investigation, 8(2), 98-105.

Sondhi, S., & Arora, R. (2014). Applying Lessons from e-Discovery to Process Big Data using HPC. Paper presented at the Proceedings of the 2014 Annual Conference on Extreme Science and Engineering Discovery Environment.

Spang, S. (2013). Regression Analysis Part I: Determining your Variables. Piston Agency. Available at http://www.pistonagency.com/blog/regression-analysis-part-i-determining-your-variables. (last accessed Sept. 25, 2017).

Spektor. Spektor Phone Intelligence Retrieved 15-4, 2014, from http://www.evidencetalks.com/index.php/en/?option=com_content&view=category&layout=blog&id=26&Itemid=133&lang=en

Spektor. (2013). SPEKTOR Forensic Intelligence Retrieved 19-4, 2014, from http://www.evidencetalks.com/index.php/en/spektor-fi

Stahl, B. (2008) Information Systems: Critical Perspectives. London: Rotledge.

Stake, R. E. (1995). The art of case study research. Thousand Oaks, CA: Sage Publications

Stange, K. C. (2006). Publishing multimethod research. Annals of Family Medicine, 4(4), 292-294.

Stephenson, P. (2003). A Comprehensive Approach to Digital Incident Investigation. Elsevier Information Security Technical Report. Elsevier Advanced Technology.

Straub, D., Boudreau, M. C., & Gefen, D. (2004). Validation Guidelines for IS Positivist Research. 13.

Strauss, A., & Corbin, J. (1990). Basics of qualitative research: Grounded theory procedures and techniques. Newbury Park, CA: Sage.

Streubert, H., & Carpenter, D. (1995). Qualitative research in nursing: Advancing the humanistic imperative. Philadelphia: J.B. Lippincott Company.

Taguchi, J. K. (2013). Optimal sector sampling for drive triage: DTIC Document.

Tashakkori, A. and Creswell, J.W. (2007). Editorial: the new era of mixed methods. Journal of Mixed Methods Research, 1, pp. 3−7

Tashakkori, A., & Teddlie, C. (Eds.). (2003). Handbook of mixed methods in social and behavioral research. Thousand Oaks, CA: Sage.

Taylor, G. R. and Trumbull, M. (2005). Developing a multi faced research design/ paradigm. In: G. R. Taylor (ed), Integrating quantitative and qualitative methods in research (2nd ed). University press of America.

Thomas, R. (2011). IBM Big Data Success Stories. IBM: IBM.

Tian, W., & Zhao, Y. (2015). 1 - An Introduction to Cloud Computing. In W. Tian & Y. Zhao (Eds.), Optimized Cloud Resource Management and Scheduling (pp. 1-15). Boston: Morgan Kaufmann.

Tjin-A-Tsoi, T. B. P. M. (2013). Trends, Challenges and Strategy in the Forensic Science Sector.

Trahan, A., & Stewart, D. (2013). Toward a Pragmatic Framework for Mixed Methods. Applied Psychology in Criminal Justice, 2013, 9(1)

Vaidya, C. (2013). Assessing the capability of e-discovery software tools. Auckland University of Technology.

Van de Vliert, E., & Smith, P. B. (2004). Leader reliance on subordinates across nations that differ in development and climate. The Leadership Quarterly, 15(3), 381-403.

Van Manen, M. (1990). Researching lived experiences. State University of New York Press, Albany.

Vanderfeesten, I & Reijers, H. (2005). The Impact of Workflow Systems on Organizations. Available in http://www.win.tue.nl/~hreijers/H.A.%20Reijers%20Bestanden/TRonline.pdf (last accessed Sept. 25, 2017).

Venter, C. (2010). International benchmarking of quality management In forensic science drug laboratories. Available at http://dspace.nwu.ac.za/bitstream/handle/10394/5063/venter_ch.pdf;sequence=1 (last accessed Sept. 25, 2017).

Vinton, D. (1987). Delegation for employee development. Training & Development Journal.

Volt, W. (1999). Dictionary of statistics and methodology: A nontechnical guide for the social sciences (2nd ed.). Thousand Oaks, CA: SAGE Publications.

Watson, D. L., & Jones, A. (2013). Digital forensics processing and procedures: Meeting the requirements of ISO 17020, ISO 17025, ISO 27001 and best practice requirements. Newnes.

Weber, R. (2004) The Rhetoric of Positivism Versus Interpretivism: A Personal View. [Editor's Comments]. MIS Quarterly, 28 (1) iii – xii.

Wheatley D. (2017) Autonomy in paid work and subjective well-being. Work and Occupations 44(3): 296–328.

Wigmore, I. (2013, June 2014). Definition - Internet of Things (IoT). Retrieved 1/29, 2015, from http://whatis.techtarget.com/definition/Internet-of-Things

Wohlin, C., Höst, M., & Henningsson, K. (2003). Empirical Research Methods in Software Engineering. In R. Conradi & A. Wang (Eds.), Empirical Methods and Studies in Software Engineering (Vol. 2765, pp. 7-23): Springer Berlin Heidelberg.

Wrike. (2017). Wrike. from https://www.wrike.com/project-management/

Wu, P.F. (2012). A Mixed Methods Approach to Technology Acceptance Research. Journal of the Association for Information Systems: Vol. 13 : Iss. 3 , Article 1. Available at: http://aisel.aisnet.org/jais/vol13/iss3/1

Xiao, Z., & Xiao, Y. (2014). Achieving Accountable MapReduce in cloud computing. Future Generation Computer Systems, 30(0), 1-13. doi: http://dx.doi.org/10.1016/j.future.2013.07.001

Yamane, T. (1967). Elementary sampling theory (L. e. o. 17:08:50 Ed.): Prentice-Hall (Englewood Cliffs, N.J).

Yates, S. J. 2004. Doing social science research. London, UK: Sage Publications/Open University.

Yüksel, P. & Yildirim, S. (2015). Theoretical Frameworks, Methods, and Procedures for Conducting Phenomenological Studies in Educational Settings. Turkish Online Journal of Qualitative Inquiry, January 2015, 6(1).

Yin, R. K. (1994). Case study research: Design and methods (2nd ed.). Newbury Park, CA: Sage Publications.

Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common phases of computer forensics investigation models. International Journal of Computer Science & Information Technology, 3(3), 17-31.

Appendices

Appendix 1 [Epoche]

For the Epoche process, I recall my own personal and professional experience in Dubai Digital Forensics Departments for the past 12 years. In this bracketing process, I leave my mind free from my experience in this department. Moustakas states that "Epoche requires the elimination of suppositions". The researcher main goal in this study is to understand the full meaning of participant's experience and eliminate any preconceived barriers.

I did not study forensics in my undergraduate programs. Neither did I study any management courses. I studied Software Engineering in my higher diploma studies with courses mainly targeting programming languages and object-oriented subjects. In my bachelor's degree I studied Business Information Technologies. Subjects like business managements, information technologies and basic networking studies were covered. Forensics was not known by me or any of my friends by then. In year 2004, when I started working in Digital Forensics Department, I gradually learnt about the field of forensics and self-learnt about different sections in this department. I worked as an examiner and my Digital Forensics experience improved after attending several courses and attending several internal development workshops. In year 2013, I started my master's degree in Zayed University and my study focused on Digital Forensics. Thus, I was exposed to this field earlier than most of the employees in Dubai department. Working in this field all these years allowed me to experience and be familiar with the workflow. Thus, I listed all my assumptions of different processes in Digital Forensics Department to make it clear that I did not apply those assumptions in my study and to ensure that I made my mind free of any pre-conceptions.

From my experience I had several believes of understanding the context of work in digital forensic departments such as:

- All digital forensic departments/ companies must have internal/external assessments to accredit examiners.
- Digital forensic manager always needs to understand the background/ experience and skills of experts.
- Every digital forensic leader rate complexity of cases, effort required to complete the cases and the enthusiasm of examiners to before assigning any case.

- The cases which find to be challenged are similar in all the digital forensic departments/companies.
- Very important/ high-profile cases affect the work flow of examiners.
- Private digital forensic departments are more open to share information such as capabilities, strengths, weaknesses, requirements and challenges compared to the government departments.

I also understood the cases assignment process as following:

- There is a clear strategy to follow when distributing cases among digital forensic practitioners.
- The cases which are assigned to a team are more efficient compared to the cases where only one examiner is working on.
- All the decision makers in the departments can freeze any case and ask the examiner to work on something else.
- The work pressure on decision makers influences the process of assigning cases.
- Every decision maker has a plan to maintain the future growth in Number of Cases.

I reflected the results from my previous study as factors and trends that affect the investigation process in others department:

- The yearly trend in the Number of Cases is increasing in all digital forensic departments/companies.
- The yearly trends of total volume of exhibits, Number of Evidence Items per Case and Heterogeneity of Evidence Items per Case are like what was found in Study One (where none of the factors was directly affecting the Person-Hours of working).
- The factors (total volume of digital forensic items, **Number of Evidence Items per Case** and Heterogeneity of Evidence Items per Case) are affecting the process of investigation.
- The type, complexity and effort required in each case affect the process of investigation.
- Every decision maker estimates the Person-Hours of work before allocating the case.

Moreover, I had several assumptions regarding the work context/ process in private and government Digital Forensics Departments:

- The work context is different between government and private sectors.

- The distribution process is identical in government and private sectors.
- The digital forensic examiners roles/ duties are similar in government and private sectors.
- The Person-Hours of investigation is more critical in private than in government.
- The Government departments have more budget supporting training, new software licenses and equipment's.

One might think that with this experience will make it difficult to reach to epoche process. However, during my experience I gradually developed as an examiner but did not work as a decision leader in any section of the Digital Forensics Department. I fully understand the process in the Dubai Police and the workflow in the Digital Forensics Department. I can offer subtle, believable encouragement to help the participants to describe their experience assigning cases in the Digital Forensics Department.

I believe that my experience in Digital Forensics Department allows me to clear my mind from any preconception thoughts and allow me to fully understand the decision leader's experiences. I am also very comfortable with clearing my consciousness of pre-conceptions to absorb all new ideas and comments shared by the participants to reach to the Epoche required.

Appendix 2 [Copy of Interview Information Sheet (participant procedure)]

University of Central Lancashire

School of Computing, Engineering and Physical Sciences
Methods and Factors Affecting Digital Forensic
Case Management, Allocation and Completion

By:
Ibtesam Mohammed Sharif Al-Awadhi
ID: G20614406

Information Sheet for MPhil/PHD dissertation research
Advisors:
Professor Janet Read
Dr. Andrew Marrington
Dr. Virginia Franqueira
February 2016

Information Sheet for MPhil/PHD dissertation research
You will be given a copy of this information sheet.
Dissertation title: Best Practices for Time Efficient Digital Forensic Investigations Involving High Volume, Heterogeneous Digital Evidence – A Case Study from Dubai Police

Dean of School

For any complaints/concerns this is dealt with via the Dean of School:
Name: Robert Wallace
Phone Number: +44 (0) 1772 89 3311
Email Address: rrwallace@uclan.ac.uk

Supervisor's contact details

Name: Professor. Janet C. Read
Position: Professor of Child Computer Interaction
Phone Number: 01772 893285
Email Address: jcread@uclan.ac.uk

Name: Dr. Virginia N. L. Franqueira
Position: Lecturer in Computing
Phone Number: +44 (0) 1332 592442
Email Address: V.Franqueira@derby.ac.uk

Name: Dr. Andrew Marrington
Position: Assistant Professor/ Graduate program director
Phone Number: +971-4-4021199
Email Address: andrew.marrington@zu.ac.ae

Student contact details

Name: Ibtesam Mohammed Alawadhi
Phone Number: +971-50-4211154
Email Address: ibtesam_alawadhi@hotmail.com , IAlawadhi@uclan.ac.uk

I would like to inform you that this research (Best Practices for Time Efficient Digital Forensic Investigations Involving High Volume, Heterogeneous Digital Evidence – A Case Study from Dubai Police) will be using the data collected from the interview.

Details of Study:

Project Background: There is no systematic approach tested by the researchers for the cases distribution process in digital forensic departments. Person-Hours is a critical aspect in digital forensic investigations. However, the effect of cases distribution process on Person-Hours is not been highlighted intensively in the literature.

Purpose of the study: The aim of this study is to understand the context of work in different Digital Forensics Departments around the world. Then, illustrate the current and future status of cases distribution process in those departments. After that, highlight the factors and trends that are likely to affect the process.

Contribution of the study: Mainly, the study will get reflections from professionals in the field and the key contribution of the work is to bring together people from different experiences and cultures to demonstrate their vision regarding the process of allocating cases. Thus, this study will help to make confident and rational decisions while distributing the cases among digital forensic examiners.

Your role in the Project:

Your participation will be highly valuable in this research since you have the experience working in a Digital Forensics Department. Your background of how the cases are distributed in your department will support the main target of this research. Your participation will be by undertaking an interview through phone/skype that will last for a maximum of an hour. The interview will be mainly to understand the current system of cases distribution in your Digital Forensics Department. The interview will be recorded. The recorded interview, plus all the collected data will be anonymized, encrypted and stored in accordance with the Data Protection Act 1998. No one will have access to the data other than myself and my supervisory team.

Things to know before starting

1.You can request having a copy of the recording - at the end of the interview - and it will be sent to you through secured line.

2.This study will come up with best practices used when distributing the digital forensic cases.

3. You will be informed for the interview date, as the ethical approval need to be obtained before the interview takes place.

4.Results from the study are mainly for my Doctoral thesis. It might also be published and disseminated internally at UCLan and externally in various academic venues and experts' events.

5.You will be informed once the study is finalized and ready to be published.

6.You can withdraw at any time within two weeks after taking the interview through contacting me via e-mail or phone. It will not be possible to withdraw your interview after this time as the collected data will be anonymized and analysed.

Confidentiality/ Anonymity

1. This study will use the data collected from the interview. The interview will be recorded, and the files will be encrypted and stored in the Dubai Police workstation. Encryption keys will be kept in a machine different than the one which will contain the encrypted data.

2. All the data will be stored in Dubai Police workstations and it will not be exported to any personal devices.

3. Dubai Police workstations are implementing the security legislations assigned by the UAE law and the information stored in those workstations will not be exposed to any unauthorized person.

4. All data will be collected and stored in accordance with the Data Protection Act 1998.

5. All the paper documents, electronic media or hardware or software used will be kept in a secure location until it has been appropriately destroyed and information it contains will no longer be accessible or recoverable.

6. Results from this research are expected to be published and disseminated internally at UCLan and externally in various forums such as in academic venues and experts' events.

7. The participant name, government/company name will be anonymized.

8. None of the personal details or government/company name will be declared. Anonymized references will be used for practitioners' name and government/company name. For

practitioner's names, random letters will be assigned to each practitioner. For government/company name will be designated with the continent name where this government/company is located. The representation of those references will be used in any education or publication report.

9.The data collected will not be used for any purpose other than the one specified in the research plan [You will be provided with a copy of the proposal and previous studied].

10. All the paper documents, electronic media, hardware or software used will be kept in a secure location until it has been appropriately destroyed.

11. Data extracted from the Database will be kept for 5 years after the PhD thesis is successfully defended, in accordance with UCLan regulations on data retention.

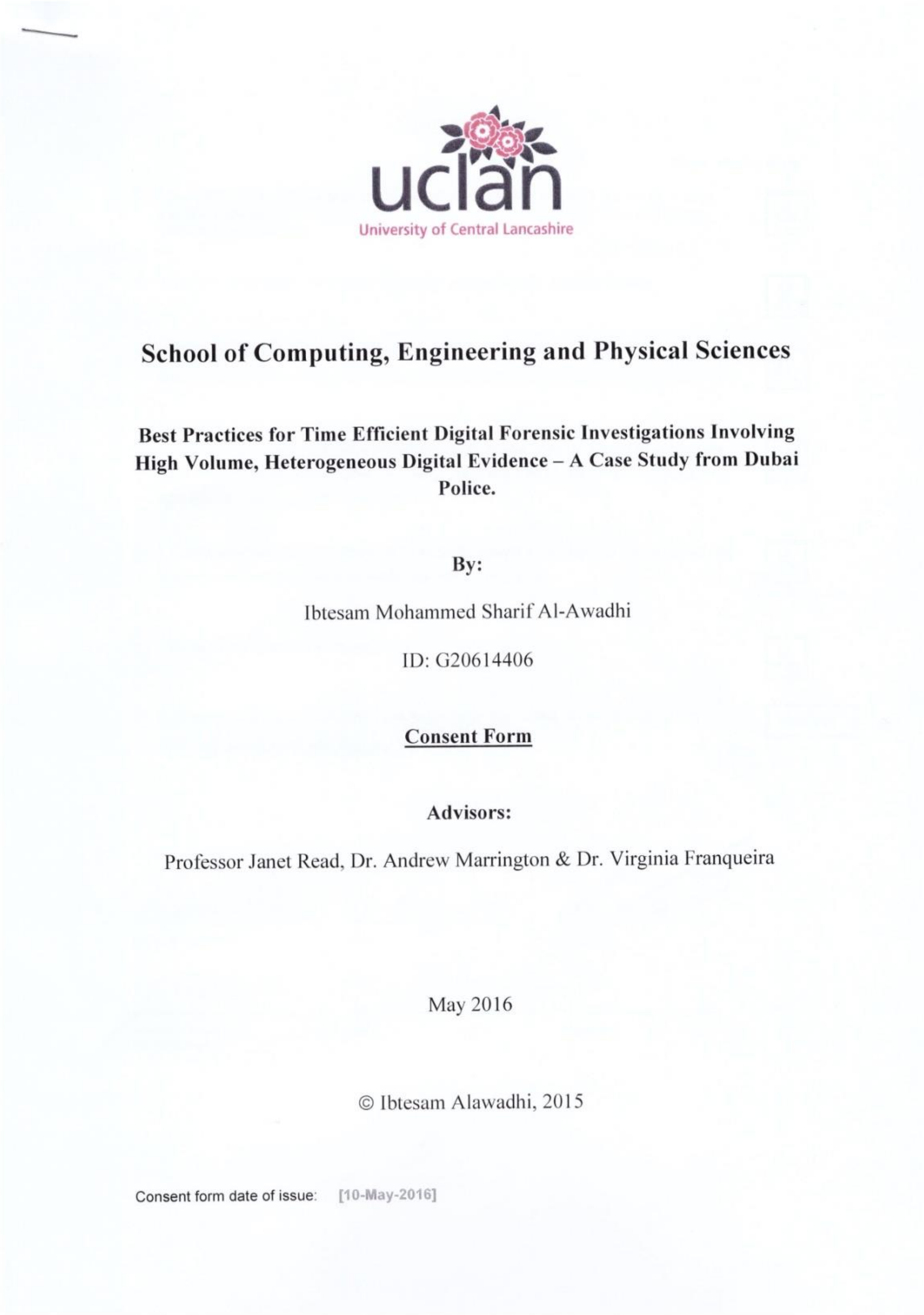
12. If you are withdrawing, all the data collected will be destroyed permanently from the workstation that is used to store the data in this research. Shift + Delete Button will be used to delete the files permanently and not replace them in the recycle Bin. Moreover, the researcher will send a confirmation email to the x-participant indicating that all the records were permanently destroyed.

Please read the following statement carefully:

Please discuss the information above with others, if you wish, or ask the researcher if there is anything that is not clear.

Contact UCLan Ethics Administration: Concerns should be addressed to the University Officer for Ethics at OfficerForEthics@uclan.ac.uk.

Appendix 3 [Template of Consent Form]



uclan

University of Central Lancashire

School of Computing, Engineering and Physical Sciences

Best Practices for Time Efficient Digital Forensic Investigations Involving High Volume, Heterogeneous Digital Evidence – A Case Study from Dubai Police.

By:

Ibtesam Mohammed Sharif Al-Awadhi

ID: G20614406

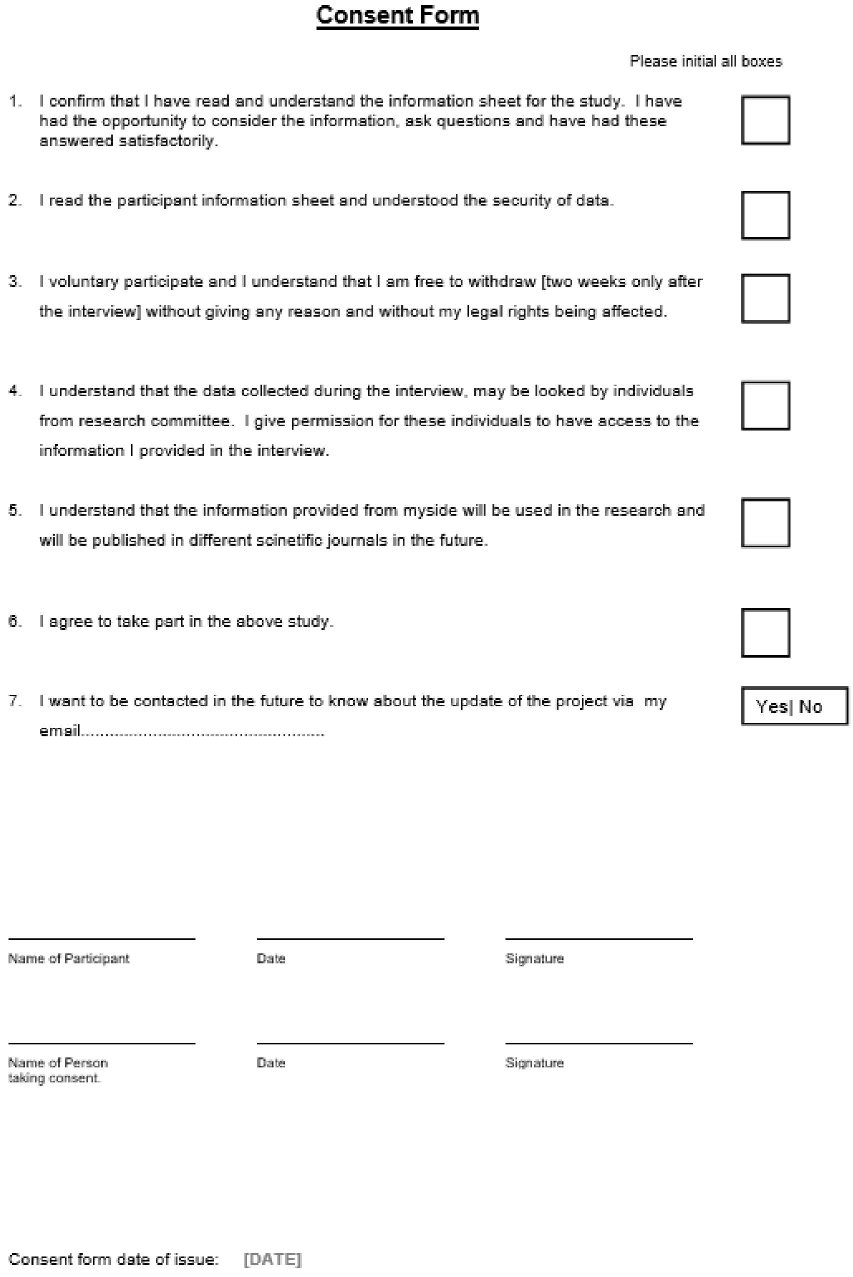
Consent Form

Advisors:

Professor Janet Read, Dr. Andrew Marrington & Dr. Virginia Franqueira

May 2016

Consent form date of issue: [10-May-2016]



Consent Form

Please initial all boxes

1. I confirm that I have read and understand the information sheet for the study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily. □

2. I read the participant information sheet and understood the security of data. □

3. I voluntary participate and I understand that I am free to withdraw [two weeks only after the interview] without giving any reason and without my legal rights being affected. □

4. I understand that the data collected during the interview, may be looked by individuals from research committee. I give permission for these individuals to have access to the information I provided in the interview. □

5. I understand that the information provided from myside will be used in the research and will be published in different scinetific journals in the future. □

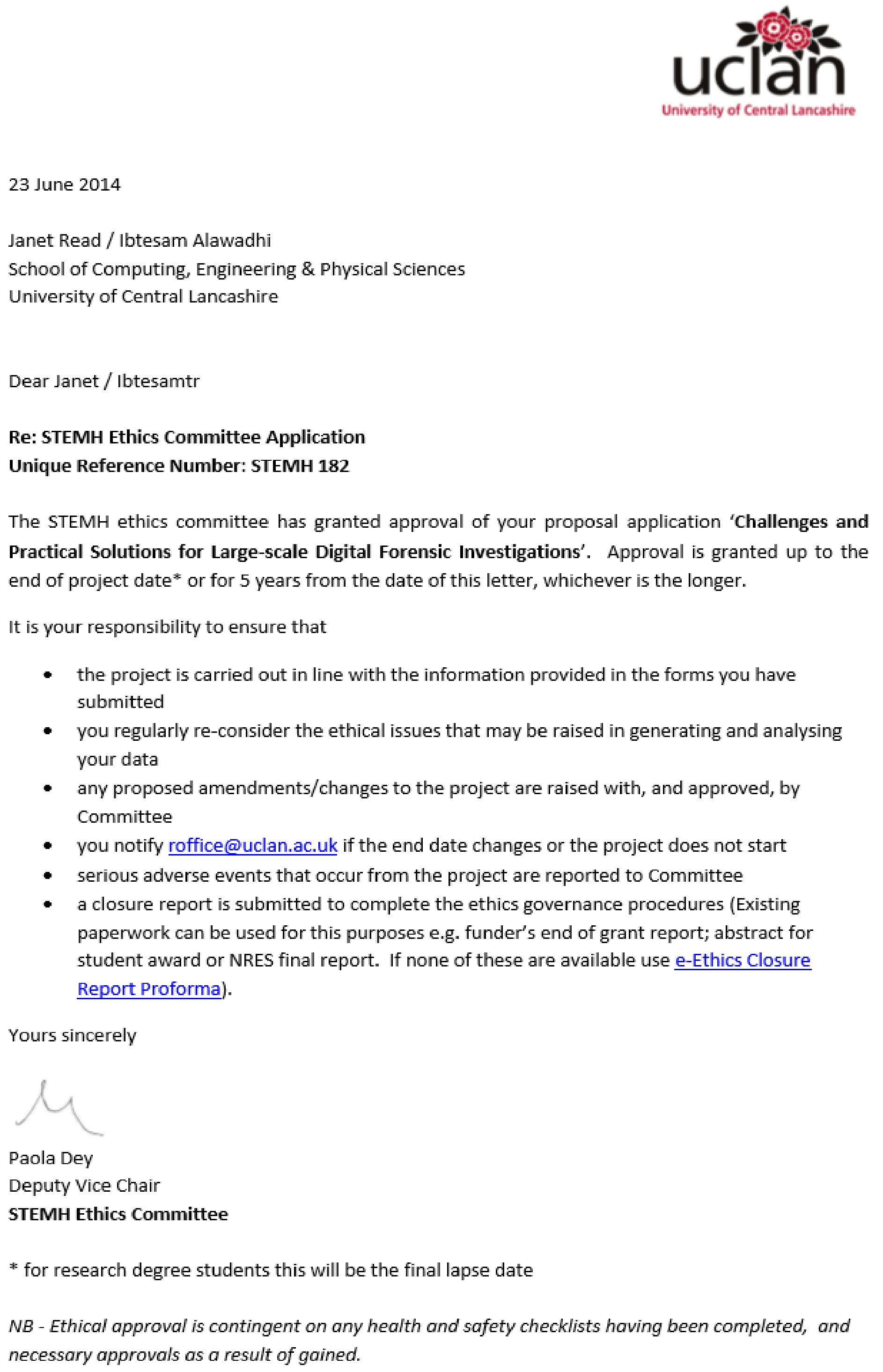
6. I agree to take part in the above study. □

7. I want to be contacted in the future to know about the update of the project via my email... Yes| No

____________________	____________________	____________________
Name of Participant	Date	Signature
____________________	____________________	____________________
Name of Person taking consent.	Date	Signature

Consent form date of issue: [DATE]

Appendix 4 [Copy of ethical approvals from the university to collect data for Study One (Investigation of the Dubai Police records), 2 and 3]



uclan
University of Central Lancashire

23 June 2014

Janet Read / Ibtesam Alawadhi
School of Computing, Engineering & Physical Sciences
University of Central Lancashire

Dear Janet / Ibtesamtr

Re: STEMH Ethics Committee Application
Unique Reference Number: STEMH 182

The STEMH ethics committee has granted approval of your proposal application **'Challenges and Practical Solutions for Large-scale Digital Forensic Investigations'**. Approval is granted up to the end of project date* or for 5 years from the date of this letter, whichever is the longer.

It is your responsibility to ensure that

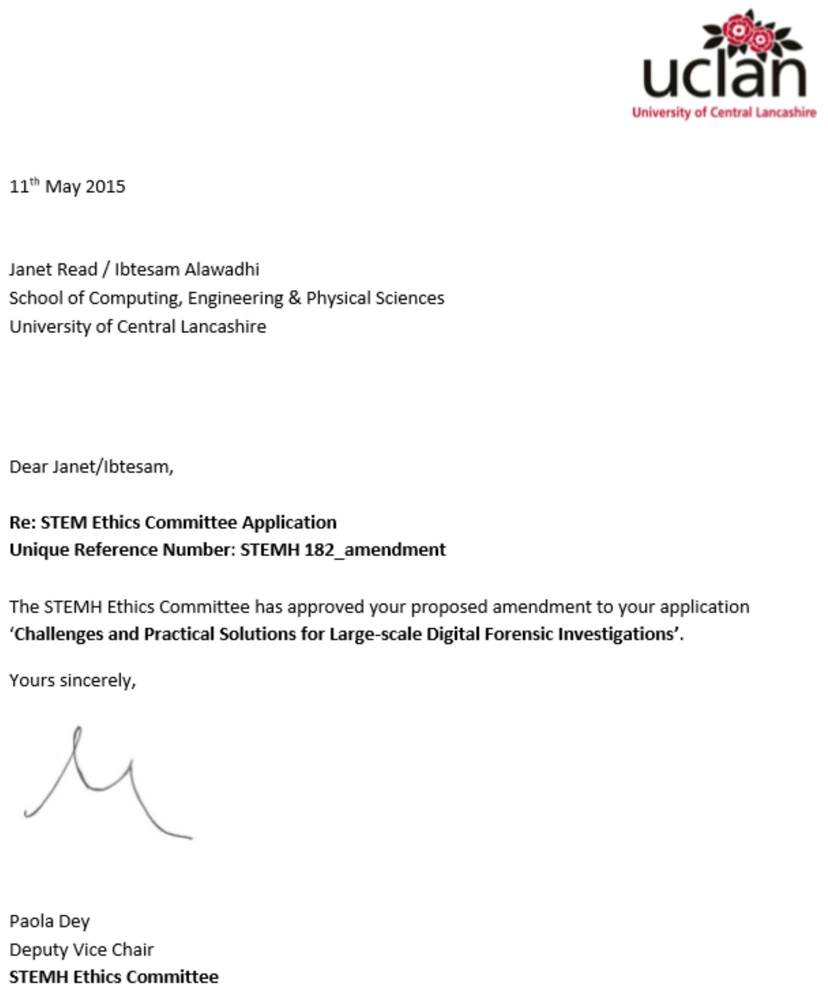
- the project is carried out in line with the information provided in the forms you have submitted
- you regularly re-consider the ethical issues that may be raised in generating and analysing your data
- any proposed amendments/changes to the project are raised with, and approved, by Committee
- you notify roffice@uclan.ac.uk if the end date changes or the project does not start
- serious adverse events that occur from the project are reported to Committee
- a closure report is submitted to complete the ethics governance procedures (Existing paperwork can be used for this purposes e.g. funder's end of grant report; abstract for student award or NRES final report. If none of these are available use e-Ethics Closure Report Proforma).

Yours sincerely

Paola Dey
Deputy Vice Chair
STEMH Ethics Committee

* for research degree students this will be the final lapse date

NB - Ethical approval is contingent on any health and safety checklists having been completed, and necessary approvals as a result of gained.



uclan
University of Central Lancashire

11th May 2015

Janet Read / Ibtesam Alawadhi
School of Computing, Engineering & Physical Sciences
University of Central Lancashire

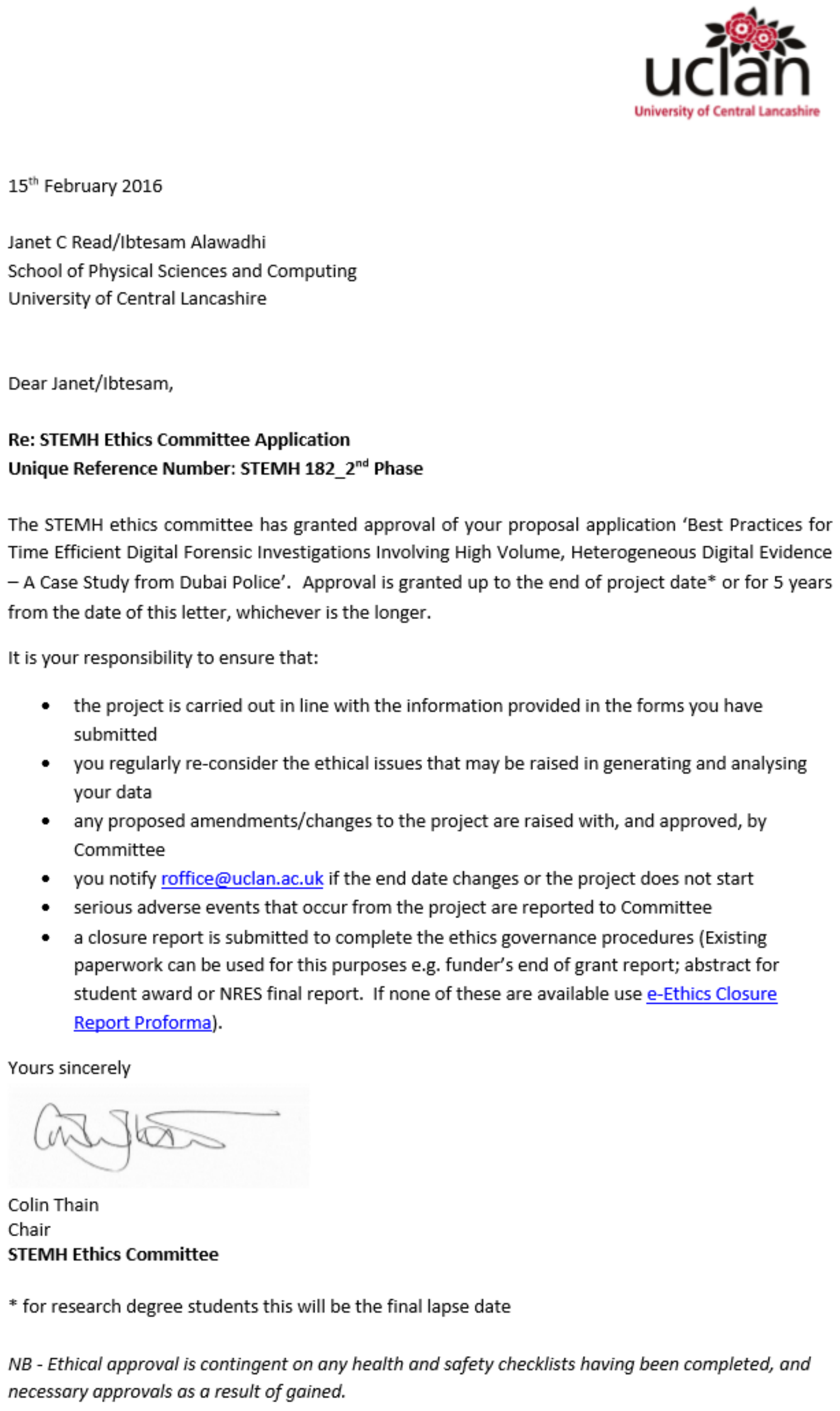
Dear Janet/Ibtesam,

Re: STEM Ethics Committee Application
Unique Reference Number: STEMH 182_amendment

The STEMH Ethics Committee has approved your proposed amendment to your application **'Challenges and Practical Solutions for Large-scale Digital Forensic Investigations'.**

Yours sincerely,

Paola Dey
Deputy Vice Chair
STEMH Ethics Committee



University of Central Lancashire

15th February 2016

Janet C Read/Ibtesam Alawadhi
School of Physical Sciences and Computing
University of Central Lancashire

Dear Janet/Ibtesam,

Re: STEMH Ethics Committee Application
Unique Reference Number: STEMH 182_2nd Phase

The STEMH ethics committee has granted approval of your proposal application 'Best Practices for Time Efficient Digital Forensic Investigations Involving High Volume, Heterogeneous Digital Evidence – A Case Study from Dubai Police'. Approval is granted up to the end of project date* or for 5 years from the date of this letter, whichever is the longer.

It is your responsibility to ensure that:

- the project is carried out in line with the information provided in the forms you have submitted
- you regularly re-consider the ethical issues that may be raised in generating and analysing your data
- any proposed amendments/changes to the project are raised with, and approved, by Committee
- you notify roffice@uclan.ac.uk if the end date changes or the project does not start
- serious adverse events that occur from the project are reported to Committee
- a closure report is submitted to complete the ethics governance procedures (Existing paperwork can be used for this purposes e.g. funder's end of grant report; abstract for student award or NRES final report. If none of these are available use e-Ethics Closure Report Proforma).

Yours sincerely

Colin Thain
Chair
STEMH Ethics Committee

* for research degree students this will be the final lapse date

NB - Ethical approval is contingent on any health and safety checklists having been completed, and necessary approvals as a result of gained.

Appendix 5 [Interview Transcript - Sample]

Interviewer: Ibtesam Alawadhi

Interviewee: From XXXX

Interview Setting: Interview conducted through SKYPE. The interview was conducted at 08:00 AM UK Time on Wednesday 18-6-2016. The interview was Recorded.

The interviewer will introduce herself. She will thank the interviewee for participation. Make sure that the interviewee received a copy of the information sheet, summarized version of previous study and he/she signed the consent form.

During the interview and when the interviewee talks about the factors found from previous study. The interviewee will list all the factors which were found previously and start asking the interviewer about the effects of those factors on their department/company.

Common definition (Those definitions are used in the Dubai Police)

1. Expert/Examiner/Practitioner: Digital forensic investigators who are experts in gathering, recovering, presenting data evidence from digital devices.
2. Analysts: analyse the data exported depending on the case factors and represent a complete report.
3. Technician:

a. Forensic technicians to complete certain tasks under the supervision of the experts. They might help in taking pictures of the digital forensic evidence, open the digital forensic evidence to extract the hard drive...etc.

b. IT technicians who are providing maintenance for Digital Forensics workstations, devices and servers. They make sure that everything is up to date, licensed and fully functional.

4. Administrative: complete administrative tasks in the department such as secretary, follow up with purchases, organize training programs...etc.

(Start of Interview)

Q1: What was your experience before working in this position in the Digital Forensics Department?
This is quite a long story to move to Digital Forensics. It started around about 1998 very early days of forensics in the XXXX. At that time my background was in information security. So, before that I was in information security, analysts. I used to accredit government department in connection to information security and do lots of other things. Carry out penetration testing, firewall installations, assessments against ISO 270001 standards. To grow a company, we looked at a different stand and what can we do and Digital Forensics which was very new at that time. If you think 1998 it was pretty much nothing. So, we looked around and we found a company called Guidance Software. And they had a product called Encase, and we spoke with the XXXX. My company was called XXXX was the first company that ever sold Encase. From there we grew the service and forensic services to the private sector. Generally, we were doing our police work. After that, after many years of doing that I left the company and moved to serious fraud office in XXXX. And I head it up their department for number of years. And develop their entire forensic infrastructure. after that, I moved to the financial content authority who didn't have forensic unit and set that up and procured all of the software the hardware put in the e-discovery platform for them and then after 6 years I left to do the same job where I am now in the XXXX I moved from private sector to central governments and to XXXX which is not government and then back into government. So now as director of the unit. I manage the strategy and develop our policies and procedures. I am also having the responsibility for direction of unit, the allocation of case work across the teams. Within the unit I manage, I have a bit like the terms that you referring to we have analyst, we have investigators, we have case work support, and administrators. But also, we have intelligent(s) as well. So, we have the intelligent(s) staff in my unit. In terms of the work that we do, we obviously have our own powers under the competition Act and under the enterprise Act. Generally, what we will do but because we are part of XXXX framework we have also concurrent regulates as such as Ofcom, Ofwat, Ofgem who works on in market so communications water, gas electricity. We also provide forensic service for those because they don’t have capability and sometimes other departments such as series fraud office and not so much of XXXX, so we work with those as well. So, we have capable

forensic unit with all the tools you will expect. We have Encase, Xways, IEF, XRY, Cellebrite, F-response all the tools and they all in the platform which called Nuix. And that is our processing and the platforms. I've given you all the answers.

Q2: Can you explain the main job of description of the intelligent(s)?

The intelligent(s) function they will develop our pipeline because we need to find the illegal activity somehow. it's not like police where a crime committed it quiets obvious the crime. With our intelligent functions they go to do logging for it. the work in the unit comes through few sources we have people who called leniency appliances. they are committing an offence with others and then come to us and says I am confessing and don't prosecute me, and I will help you to get the rest, so we offer that too. with the leniency appliances and the intelligence teams what we do we try to convert them into cheers we try to convert them into performance we use. but the intelligence team use various data mining products various open source tools and they use tool called I2 Which is an IBM tool. but we provided the intelligence team with number of tools which they can use called hackney these tools called RAID. These tools allow intelligence team to troll twitter and other thief's and look for trends and people discussing certain topic and then they will see that it seems that a lot of people are complaining about this topic. From that it will allow them to develop our pipeline the cases. The intelligence team will also collect data from XXXX in terms of their human activities like ministry of defines and the national health service we collect their data and we look who across that to look for trends in terms of the fair human activities and we will go and investigate that. so, the intelligence team number of open source and data sources and convert intelligence to us and i2. what they will also do, they will build a case until such a time as at least pass across to be investigated. Until they finish their work, we don't have a case. so, they develop all the background of the case and they handed a cross to investigate the investigators will see if there is a case obviously not. so, stop go there. We must pipe our development then new case will start on evidence type.

1. Roughly, how many staff member is there in each job description?

   Case work support (general admins): 15 / The intelligence: 8 /Digital Forensic Team: 10/ Investigators: 70 / the rest group admin management: 110

2. Describe the background/experience, skills, abilities and individual characteristics of experts in your department?

3. Do you get enough budget support for new equipment, software licenses and training programs?

a. Make sure to get information about the cases that they don't deal with because of lack of equipment, software licenses, skills and experience.

   We get plenty of support. We have IT department which is response of our equipment's and they have around 25 staff. In terms of hardware: we have commercial HP desktops, MAC, MAC books, we use i-Macs Intel machines, storage all HP supported by IT and we have numerous storages of terabytes above 100 terabits at least. We try to move the data into government client so instead of storing it internally we want a client to take over. Our hardware is supported by IT section. In terms of software are

4. What is the process followed to accredit an examiner?

   We have a confidence matrix. You might have heard of the standard ISO 17025. As a lab we must get accreditation to that as a lab. If we don't have that accreditation our evidences are not admissible. To be accredited and for that we developed confidence matrix, the accreditation process is that we need to be accredited on products that we use all staff have certificates, of encase, and they have Nuix certification and the employees will get through Xways and cellebrite certifications soon. They also looking the IASS qualification which some of them will have? During this career within two years we expect from them to progress through the confidence matrix. From basic to advance, for example basic confidence could be how to image a hard drive. So, they will be observed to see if they are capable to image a hard drive. A high level will be analysis of JTag which is high qualification in terms of confidence. We do a lot of internal training in terms of the accreditation plus we have some who needs to get product certification because they need to be accredited as a witness in court. then the rest are internally certified by our internal training.

5. Does your department deal with criminal cases only, civil cases only, or criminal and civil cases?

b. If both: Do considerations differ when dealing with criminal cases as compared to civil cases? If so, how?

   Both

6. What are the different types of case that your department deals with?

Because we XXXX, we have two powers under the competition act. Our role is really to identify people who are working in cartel. Not drugs cartel but cartel where the prices are officially increased and are officially mentioned. so, for example just a company sells pencils and there are manufactures of pencils so you will agree that you are going to charge 20 pence of a pencil. So, they are raising the price, which is illegal, but we are not looking to pencils we are looking to drugs pharmacy. The money there are much great we are talking about millions, so we have drugs companies so what we do is to defraud the increasing of the pricing. Another example is where we have like in copy right. If we use medication again a drug company will own a patent for the drug and earn a lot of money out of that. But that is expires after wile and then can everyone join so Boots, Super Drugs, Azda, tesco, they will all manufacture the drugs very cheaply so the profit of being in will goes. so what they do it calls pay for delay they will go to those companies and say that we will pay you to delay taking our patent so the owner of the patent will use it to make more profit so they will pay not to let their product go to the market. In that area we go and investigate where companies have too much of dominant position in the market so all what we work for are the consumers. So, the victims of our cases are consumers where they go and buy for example milk, they are paying more than what they should do.

7. For each type of case:

a. How do you rate the complexity of this type of case?

b. How do you rate the effort required to complete this type of case?

We do, part of our intelligent function is to try and find out more about the companies that we are going to raid. if we are dealing with an internal source, so we inform it then we can collect some information from there maybe do some Emil header analysis but if I give you an example which we carried last year this was an investigation in to a number of properties in street and we knew they were using cloud based storage. So, we had to concern whether they all are using same line, or whether they are all using same ISP, if they are using same service provider for the storage. That was quite complicated. we had to deploy different tools and we must speak with different people to find out where the data is. So, when we sat down before hand and discuss this, we came to conclusion that this was a complicated case and we need to deploy everything properly. IF you will go to our website which is cme.gov.uk and once you there you can click on our CM cases and you can have a look from there.

That was a complicated. a simple one is going to business and going to image laptops take some data from inside. When we attend with a warrant it makes it easy because they are obliging to gives us the data otherwise, we just take it if we have a warrant to take. We have our powers where we can attend the site and require copying the data for us, so we protect. Warrants are easy for us to take the data or devices, technically they are all simple. The only problems are coming across now is the blackberries heads where to get through encryption on global devices. And a problem is current cloud storage we don't know where it is. When do have powers to take it but we have problems of integrity of data and data being changed? So, they are some of complications we come across. Once it is in had you can know.

8. How do the complexity of cases and the effort required to complete a case affect the distribution process?

   It comes back to our confidence. We have two teams with team leaders. The cases will be assigned base on case capacity. It will not be on whether they have skills of the team or skill of individual it is always asking about the capacity to manage the case. They can manage 10 cases each and their role of the two leaders is with the case team investigators is to develop the forensic strategy and advise them on the best way to analyse the data. Which they are going to prepare how to best way to investigate internet history. So, the work is allocated to team leaders based on their capacity and underneath the leaders they have their own team. we use the process of matrix management if an investigator has a line manager who will use for reviews and post care. They also have work manager. what will happen is that we have a job in the manager will look what is required for example extraction for internet history and find in the confidence matrix and see who in the team has the appropriate confidences to carryout they dig into the internet history maybe one person who can carry out. So, he might split the job of a case or one person will carry it out. so, the confidence matrix is used to select best person for the job. Then after that he will look at capacity that this person has and current workload and the forth coming absences and holidays or coming tasks and determine the best person to deliver that task to the time required in to the case team. So, it is mainly capacity management. For example, it will go for another team because they don't have expertise to deal with.

9. How to develop in the confidence matrix? who fill it?

   The confidence matrix is updated as people develop their skills it is owned by the team. They will look at that and they will say that within two years we need to reach to confidence which is expected from us. So, for the principle investigator who is very technical will expect them to reach to top level of confidence within two years. Where one of our junior investigators that within two years we need you to be halfway through. so as the team work with different jobs and get experience they will go to their job and work go they will go to their managers and tell that you develop your skill in certain area then the leader will look into that and asses that and look to their notes maybe observe what they are doing to confirm what they reach to. In the same time, we need to make sure to give opportunity to reach the expected confidence level. If they are beyond that then we make sure to give procreate training for example somebody might be required to analyse P-list and the examiner couldn't develop his confidence in this area, then he will come and ask for a procreate trailing. In terms of training we have quite good budget which is enough to push all the team through Encase and using encase guidance passport plus the Nuix certification and if the staff want to do the MSA in forensics we also support that as training very important in our work and what we do.

10. Which cases does your department deal with most?
11. Which case does your department find to be challenged?
12. If the cases that you find to be challenged to your department are the most frequent cases, what would be your plan to overcome this challenge?

Questions which focus on the current and future process of distribution of digital forensic cases:

1. What are the easy/hard to allocate cases?
2. What strategy is followed when assigning a digital forensic case?
3. When, if ever, is this strategy bypassed?

a. Make sure that the interviewee talks about the effect of very important/high-profile cases on the distribution process and the work of examiners.

   No, not at all because of our ISO certification everything needs to follow the same rotes. everything that will come to the lab whether it is civil case or criminal case. Otherwise we will fail our certification. There is no way to bypassing what comes to the lab. However, there is a way of prioritization that so this is critical important we can deal with it as high priority but no bypassing.

4. How do different types of cases affect the distribution process?
5. How do you decide on the composition of a team of examiners if you want to assign a case to a team?

   All our cases are team based. working in teams are more efficient because different views across the data you have different experiences different backgrounds in a team the team is the best way to carry out, our investigations never individuals. We are not looking for a person duplicating music or stealing an IP we are working with large organizations so it is too much for one person anyway there are terabytes of data to put on it could be hundred exhibits in one case we can't assign it to one person. The work it goes across not only forensic team they also work in behalf of analytical tools that they will provide graphical representation of the data so they can look for connections. Everything is done in a team we are a team-based organization
6. What do you think, when a case is assigned to a team is more/less efficient than assigning it to one examiner?
7. What are the circumstances that allow decision maker and/or examiners to change case assignments?

a. Make sure that the interviewee talks about the examiners' ability to freeze or switch cases.

Questions which focus on the factors and trends that are likely to affect (or are already affecting) the distribution of digital forensic cases:

1. How do you describe the yearly trend (increase/decrease/steady) in the Number of Cases at your department?

   It is increasing; it is increasing by 300% each year. Only because we have an effective intelligence function that is generating this work if we don't' won't find it. It is out there.

These crimes are already taking place. The number small we talk about less than XXXX it is not compared to the police. But they are complex the law is complicated that we need to operate under but because of the investment we made recently in the enforcement division we are increasing the Number of Cases because we have more intelligent tools.

2. In Study One: We highlighted the factors affecting Person-Hours of work:

a. What is the effect of Study One factors on Person-Hours in your department?

i. What is the effect of total STORAGE CAPACITY of digital forensic items per case on Person-Hours in your department?

This is not of too much a problem for us and I will explain why this is. because I can see that this is going to be problems because the devices are increasing in storage capacity what we've done is to maintain this is to do this when we execute warrant, we will be spent days on site. We might go the sight for days. this allows us to put backend processing at front my forensic team on site carrying out forensic work on site and eliminating devices on site so we do a lot of work on triage on site we might take Nuix portable or other tools that allow us to do keyword searches if we need to image a type of hard drive we type to avoid that. so what we bring back is quite small in terms of volume because we do all the process in the front so once we have the data on our hand yes it takes space over network but it is not a problem as disc spaces are cheap we do not worry about the storage but what we are producing we do stream forensic reporting this XXXX and forensic regulator are really keen on we start analysing a hard drive and do all the work from that we put some key information names, profiles and what the machines use for in few of key points and then we present to the investigators and they may say that nothing on the machine that interests us so we eliminate that maybe they will not be attract to those profiles in the machines so we don't do full forensic analysis that comes in and we do a very quick snap shot on what is there and then we eliminate some more and eventually what will hit our review platform maybe couple of thousands file reduced from couple of millions. Instead of seizing everything for analysing we are analysing upfront and only we bring what we need to bring back and doing it. if we do the work as fraud office does and SCA in one day to take everything or image everything because they seize it, they need to review and analyse it. So, we reduce 300 to 400 exhibits. The investigators will take long time in scene to reduce the review later.

ii. What is the effect of Number of Evidence Items per Case per case on Person-Hours in your department?

iii. What is the effect of Heterogeneity of Evidence Items per Case on Person-Hours in your department?

b. In your opinion, what is the effect of Study One factors on the distribution process?

c. How do you describe the yearly trends of those factors (total volume, Number of Evidence Items per Case, Heterogeneity of Evidence Items per Case) in your department (increase/decrease/steady)?

d. Do you estimate the Person-Hours of work that any case might take?

i. What are the factors that you rely on to make your estimation?

ii. How effective is this estimation for the distribution process?

We don't, we have tasks associated with a case we will estimate the duration of that task. For example, we can say we will submit the internet history analysis by the 24 but then they have like a time to do this specific task but never to know the time it will take. it does not matter how long they spent on specific task, but the deliver outcome of that case is the important

e. The statistics showed an incremental increase in Number of Cases:

i. If the current Number of Cases doubled or tripled, how the department will be affected? And how do you think the distribution process will be impacted?

What we need is more staff. We need more software licensees and buy more hardware. The important thing is the staff. We can manage the double in load but not triple. We need to increase the staff in near future.

ii. With this increase in Number of Cases, do you think that you need to re-train or re-allocate the staff in your department (i.e. transfer employees from one section to another depending on the load of cases in that section)?

The types of cases we deal with are fixed. We are not like police. We know what the cases are. And we generate our own case from intelligent. The type of cases will not change at all. It will change maybe with the people we work with changed then we might change but I can't see that happening in near future. but we need training on windows 10 new environment or new types mobile devices, cloud we need to understand a lot of that because we need to understand how we get the data out of it and when we have a warrant nothing on site we executed a warrant last march and all what the only thing that we were able to seize for the entire company was blackberries. where all company using the business using blackberry, they didn't give us passwords in beginning but eventually they had to. Those kinds of problems might come across. So, the what we need to do with windows 10 we do small training for team and find training provider. Live forensics we need to think about too. More relevant to do.

3. How do background/ experience, skills, abilities and individual characteristics of experts affect the process of cases allocation?
1. From all the above-mentioned factors, what are the main factors that you consider while assigning a case?
4. From your perspective, what other factors affect the distribution process?
   All of it skill of individual. In our organization all skills similar level but in other the skills will be varied so the skills are the main target.
   Say you investigating hacking attempt you need skills in networking and sand routers firewalls type of skills to understand network infrastructures. In child abuse cases very difficult to allocate as you need to provide counselling facilities the nature of work is not nice. Other work like terrorism work need to have security plan, individuals. So, the skill of the person is important. In my team if we had particularly a sensitive case then will not allocate it to junior staff will assign it to senior staff, they will be more diplomatic about it. Mainly skill of individual and how much is the capacity to know the distribution and the load of work with the staff .so need case balance. We need also to give opportunity for trying new cases in order to improve their capabilities and confidence level. investigative capabilities are important it is not how to use encase for example you need to know how to investigate and dig in so investigative capabilities which is difficult to teach they develop by work. for example, if you are looking at internet history he was browsing internet but as investigative you need to say why he was on that website 5 minutes before committed the offence and what why what did he do after so things like this need to develop by time
5. From your perspective, how could you improve the process of allocating cases?
6. If you have pressure of work (administrative/managerial tasks to be completed), how would that effect your case allocation task?

Team leaders they will do all the allocation work and they are part of case team. Case team made of investigators, case supports, and case admin person the exhibits on a case. So, the structure of investigative team 10 individuals with different responsibility in different areas.

Appendix 6 [Textural Description - Sample]

1. I don't have any experience before joining the Digital Forensics field.
2. We have different job descriptions and they are: Expert, Examiner, Engineer, Trainee, Technician, and Administrative. We have around 2 Experts, 11 Examiners, 5 Engineers, 6 Trainees, 5 Technicians and 4 administrative.
3. The experts in our department have master's degrees in information security with work experience in IT, information security and Digital Forensics more than 20 years.
4. We are planning to prepare the others to be experts, where some of the examiner completes the Ph.D. and working only on specific cases only.
5. Actually, we have enough budgets every year for the new equipment, software licenses and training programs.
6. Before being an examiner, every employee has his own coaching manual where he should go throw this manual by starting with trainee and he must finish specific part to move to the next level. Then move to the next level to be an examiner.
7. The coaching manual contains the courses, devices, software and books required to be finished by the employee to be an examiner.
8. We deal with both criminal and civilian cases and same processes are used for both.
9. We deal with all cases if containing electronic devices. Examples are drugs, hacking, fraud, crime against person, child abuse and recovering data, etc
10. We rate the complexity of cases by the services requested, number of devices and the time.
11. Hacking is the case type that we find to be challenged in our department.
12. If the number of hacking cases increased, we will overcome this challenge by training the employees and buy the latest hardware and software tools.
13. There is queue for the cases and the then assigning depending on the level of the crime and the experience of the examiner.
14. This strategy is not allowed to bypass because we are accreted with is and we need to follow their procedures.
15. The composition of a team is chose depending on the experiences required for the case.
16. Assigning a case to a team is better than assigning it to one examiner because the team member together has more experience than the single member and ideas from group are more than single one.

17. We can switch or freeze a case in circumstances such as: After assigning a case to one examiner and he find something over his experience then in this case we need to freeze the case and assign it to another examiner who has experience to complete the case.
18. The experience of the examiner plays an important part in allocating the cases because some examiner have more experience in some types of cases than other types of cases for example some of them prefer working on hacking cases instead of drugs. Also, some examiner prefer working in certain type of cases instead of other for example working in hacking rather than child abuse where a lot of pornographic images.
19. We can improve the process of assigning cases by training the examiner and let them gain the experience on different type of cases that are familiar to them under supervision on an expert on this kind of cases. Provide more software and hardware in order to let more than examiner work. Also, we can train all the employees with basic, so they can be familiar with the requirements and working until allocating the cases to another examiner instead of waiting the examiner who has experiences in this types of cases finish his current job. Also, we could send some of case to other labs after getting the agreement from the sender but this step s needs to be organized depending the civil cases and criminal cases. Also, we could use case management system and benefit from the result at the end for each examiner and the cases he work on them (time he spent, procedure and resources he used including the hardware and software)

Appendix 7 [Structural Description for participants - Sample]

Sample 1

XXXX was an investigator doing white collar crimes (financial crimes) in 1999. Then he became a XXXX. He was patrolling the street for 9 years. He learnt about network intrusions independently. When XXXX police developed computer unit, XXXX were asked to join the unit. They sent him to couple of training courses. He got promoted, and in XXXX Police when somebody gets promotion, he needs to go back to XXXX. I worked there for a year and when an open came up in the computer department, I applied and get back to the department as supervisor of the department. Now I am working here for 13 years. About 5 to 6 years ago they started their internet crimes against children Unit (ICAC). Both unites high tech unit and ICAC unit fell under one person to manage. XXXX now is in charge for both units.

They are 12 employees, 7 forensic examiners and 4 investigators and one person who is designated to cell phone cases. Actually, all the forensic examiners can investigate cell phone cases but their specialist examiner is certified by Cellebrite and Jtag. They have the highest budget in the XXXX. Both ICAC and High-Tech units cannot hire a civilian with Bachelor/Master's degree in computer forensics. Our employees need to be from XXXX.

Investigators come from criminal detective background that is prerequisite to be in ICAC unit. It is also prerequisite to be in the lab. This is because, it is important for the examiner to go to the criminal mind and think of different strategies like why he would put specific file here, why he was using peer to peer software, why he was using LimeWire instead of bearshare and what type of keywords he is using and so on. Any examiner is promoted he will leave the unit XXXX and he will not be able to come back to unit unless there is an open for job vacancies. We have our own internal training centre that we take most of our examiners to.

Number of exhibits, types of exhibits and the volume capacity effects the person hours of investigation. Thus, they work hard to eliminate the number of evidence items we seize. They work hard in the crime scene on the previews to collect the related evidence items.

The XXXX in the ICAC unit are primarily investigators who are online and engaging the sexual predators. They develop the case and the search warrant then the High-Tech Crimes unit goes out with them to do the search warrant and collect the digital evidence and obviously examine it. ICAC unit and High-Tech Crimes unit accept digital forensic cases from the XXXX police and municipalities in the XXXX. They work on both criminal and civilian cases. Most of their cases are dealing with peer to peer. In the crime scene they try to limit the number of exhibits seized. They are also trying to limit like DVDs or CDs. If we have information that he saved information on those CDs or DVDs then we might take it otherwise they don't. They do previews and then identify which computers have contraband and which do not. Then they can segregate the computers which do not then focus on the computers that we found contraband so that's limit the amount of data we must examine and that helps us to in lab. Thus, they try to prioritize, triage the cases as they come to reduce the time of investigation. XXXX finds that network intrusion cases, Cases using Linux, cases using Cloud computing or Windows 10 are the complex cases. They never bypass their strategy, but they are able to priorities the cases. For ICAC cases, the entire lab goes to the crime scene with the search warrant and each person has different role. From the search warrant they know this case is assigned to a leader. The leader of the case can identify the targeted exhibits from the crime scene, and he will be responsible to exclude any evidence items. People who are assigned to that case will start previewing the evidence items in the crime scene. The rest will seize the required exhibits and go back to the lab. In the lab everyone will acquire the hard drive they seized from the crime scene and put it in one case so the leader of that case will go and examine it later. Thus, it is the total team effort in the crime scene and when they are back to lab each examiner will work on their own case that they were assigned as leader on. The case leader will be the one who will work on the case because he will be the one who will testify later in the court for his findings. If he required some help the rest of the examiners are there to share their knowledge and support. Thus, they start out in a team and then its kind starts to waddle down to one person. Cases can be freeze under certain circumstances like lack of skills or knowledge to deal with specific exhibit. XXXX can reject any case if they are under presser or they find their self not capable to handle the type of the case. However, most of the cases we receive are high profile cases involving kids involving aggravated physical harm assault, homicides, domestic abuse and so for the burglaries, and nonphysical cases. Some cases like shop lifting they can't take that even now they don’t accept that type of cases.

To allocate the ICAC cases which involve computers, they go around the room. If specific skill is required and it is not obtained by all the examiners, then that case will be assigned specifically to the experienced examiner. For cases other than ICAC, XXXX will triage the case depending on the case gravity. For any type of cases the unit leader will check the workload of the examiners and assign the case. He will also make sure that people who are planning to go to vacation or people who will go to trial (they will be there for a week) will not take new cases. For cases with cell phones, if it is an important case our cell phone person will handle the case and if it is normal case then our examiners will handle it. All examiners in the unit can handle all the types of cases. The only person that will not be assigned in routine is the cell phone expert because he will only work on cases with cell phone devices. There is an assistant for the unit leader who can complete the daily tasks of the leader.

Structural Description for participants – Sample

Sample 2

XXXX experience can be divided into parts: forensic investigations, forensic component development and security hardening. The component development is when a new technology is released; XXXX works with his team to create acquisition strategy and acquisition methodology.

They are 22 employees. They have different skill sets and thy come from vulnerability and exploit development background. They are mainly security people.

They have their own internal procedure to accredit examiners. They provide their employees with device specific trainings to learn about new technologies. They are also providing training support to their employees about products that are not yet released. They have internal knowledge Database that includes information about best way investigating all the devices Old, new or the upcoming.

They work on both civilian and criminal cases. All the cases come from the defence sector and law enforcement. Most of their cases are hacking and hardening cases. They are also mostly working on high profile cases. Most exhibits in the current cases are mobiles. They also work on security hardening for high end companies. They also work on proof of concepts (POC) when they are not running projects. POC is mainly to find vulnerabilities in the latest technology releases and then offering the solution to the companies. They keep an eye on the trends for example in the next one year what type of new devices are coming do they have public data or that type of community of view version available for example Microsoft alpha releases. They also support digital forensic departments to obtain ISO ISE 17020 17025 which is related to lab and its facilities and infrastructures looking into different aspects. XXXX provide varies training types. They can estimate the cost through the person hours required to solve the case. They can estimate the person hours of investigation by checking what are the skills required in the case for example does it need an analysis from phone wear, does it require IOS related skills or cryptanalysis. Then the cost can be decided depending also on the priority and level of urgency. For large data sets cases, they internally build up some customized system of automation of data handling and data processing.

In XXXX, they have internal motivation between the employees. They have two opposing teams with team leaders that compete each other in all the cases. Each team consists of 5 to 6 employees. The rest of employees are working on management and the analysis of the cases. When they receive a case a copy of the acquired images of the exhibits in that case will be assigned to both opposing teams. Both teams are adversarial, they fight against each other. Each team tries to beat the other. Each team will be having information regarding the estimation time to solve that case. Each team will try their best to solve it quickly because internally they would get a huge bonus to solve each case. XXXX charge differently for each case depending on the time spent to complete the case. The cases which are solved fast will be higher than the cases that will take longer time to be completed. There is also possibility for each team to solve half of the case or for example 20% is solved by this team and 40 % is conducted by the other team. The bonus in here will be divided between the two teams.

Volume capacity exhibits types and number are all affecting the person hours of investigation. Currently they are using a data mining solution which is kind of distributed parsing solution, so they are using cloud power to actually parse and increase the efficiency of our evidence processing capability. They are also using handle data using cloud power because we can do a lot of things with that. However, there are some limitation to that as it is still difficult to interpret with the data in the cloud.

First thing they do when they receive a case is by having discussion with the two team leaders. In this discussion they try to clarify the problem they are facing. These discussions might last for 3 days and in urgent cases it might last for one day maximum. XXXX have their procedures, manuals and technical details internally built to be followed when working on cases. They have certain written procedures and manuals to follow in terms of the technical details. They also have extensive documentation that they built internally. An example of manuals they have operation manual. This manual divided into technical and non-technical. In the technical, it covers all the technical steps required to complete certain tasks while examining specific exhibit. Non-technical are observations, findings, conclusions, things to avoid, things must see and management issues. For each case they have something called versioning. That versioning defines the nature of the case, complexity of the case, year and duration of that case. The two teams who work on cases are only focus on cases. However, other tasks are conducted by security or technical staff. They also have auditors. One is process auditors to follow up with the processes conducted by the teams and the other is security auditor to ensure minting the security limits. They work on similar case types. They prioritize their cases; however, the cases who will take higher priority will pay more. This is because they are commercial company and money is an important factor for them. In the case of the absence of the manager, one of the team leaders will take over the tasks.

Appendix 8 [Published Paper]

THE JOURNAL OF
DIGITAL FORENSICS,
SECURITY AND LAW

Journal of Digital Forensics,
Security and Law

Volume 10 | Number 4 Article 1

2015

Factors Influencing Digital Forensic Investigations: Empirical Evaluation of 12 Years of Dubai Police Cases

Ibtesam Alawadhi
University of Central Lancashire

Janet C. Read
University of Central Lancashire

Andrew Marrington
Zayed University

Virginia N. L. Franqueira
University of Derby

Recommended Citation

Alawadhi, Ibtesam; Read, Janet C.; Marrington, Andrew; and Franqueira, Virginia N. L. (2015) "Factors Influencing Digital Forensic Investigations: Empirical Evaluation of 12 Years of Dubai Police Cases," *Journal of Digital Forensics, Security and Law*: Vol. 10 : No. 4 , Article 1.
DOI: https://doi.org/10.15394/jdfsl.2015.1207
Available at: http://commons.erau.edu/jdfsl/vol10/iss4/1

FACTORS INFLUENCING DIGITAL FORENSIC INVESTIGATIONS: EMPIRICAL EVALUATION OF 12 YEARS OF DUBAI POLICE CASES

Ibtesam Al Awadhi, Janet C Read
University of Central Lancashire
School of Computing, Engineering and Physical Sciences. Preston, UK
{IAlawadhi, JCRead}@uclan.ac.uk

Andrew Marrington
Zayed University
College of Technological Innovation. Dubai, UAE
andrew.marrington@zu.ac.ae

Virginia N. L. Franqueira
University of Derby
College of Engineering and Technology. Derby, UK
v.franqueira@derby.ac.uk

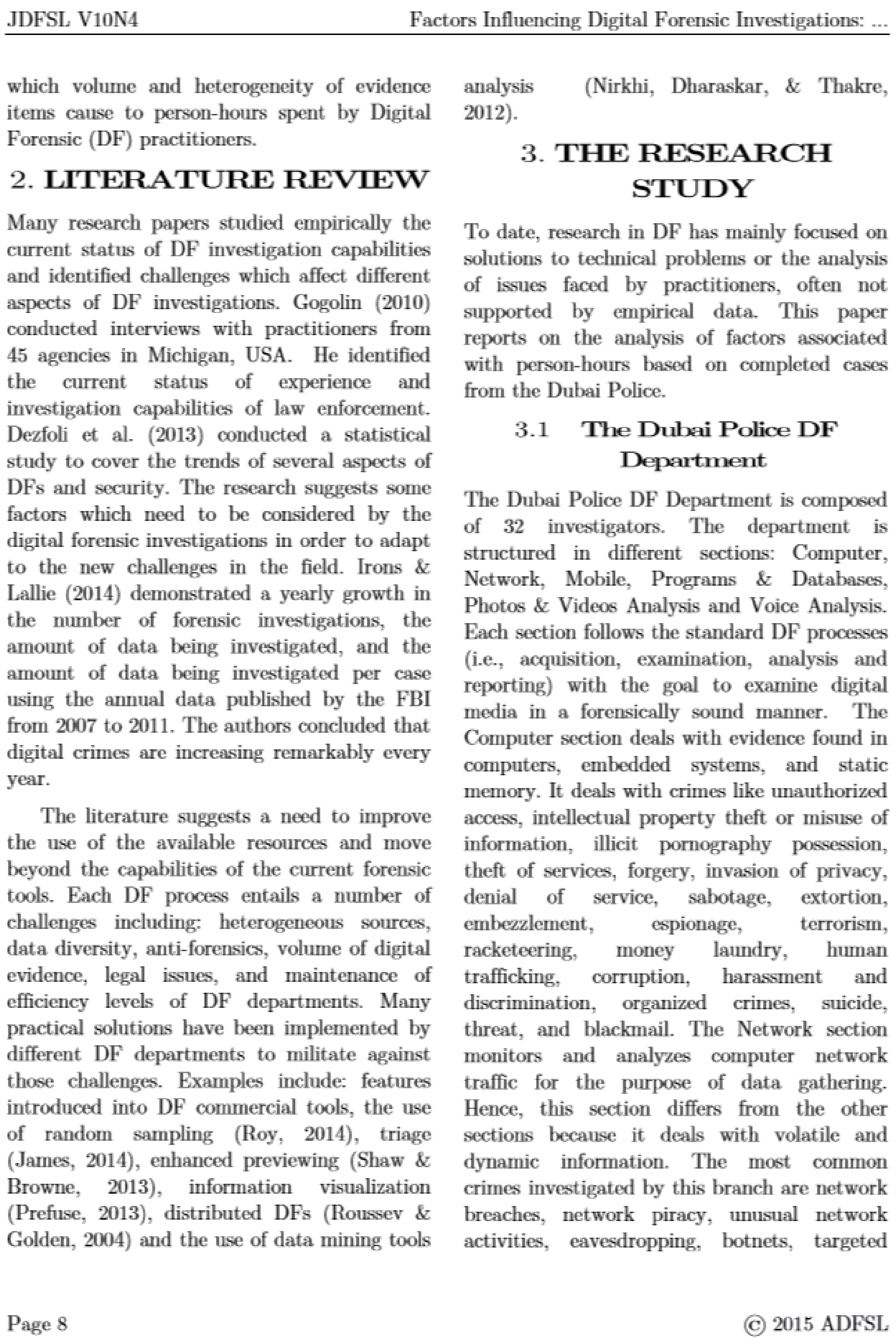
ABSTRACT

In Digital Forensics, the number of person-hours spent on investigation is a key factor which needs to be kept to a minimum whilst also paying close attention to the authenticity of the evidence. The literature describes challenges behind increasing person-hours and identifies several factors which contribute to this phenomenon. This paper reviews these factors and demonstrates that they do not wholly account for increases in investigation time. Using real case records from the Dubai Police, an extensive study explains the contribution of other factors to the increase in person-hours. We conclude this work by emphasizing on several factors affecting the person-hours in contrast to what most of the literature in this area proposes.

Keywords: cyber forensics, digital forensics, empirical data, forensic investigation, Dubai police

1. INTRODUCTION

Year on year, digital forensic teams face the mounting challenge of diversification of storage devices and distribution of data across many storage areas. In single investigations, practitioners are now expected to search more storage than they were five years ago (Irons & Lallie, 2014). This growth and spread of data raised considerations on how to best manage the analysis of material with finite human resource and time constraints. Forensic tools can take some of the work from the human element but still there is a need to better understand how to allocate and manage person-hours so that investigations can be concluded within reasonable time and reliable findings. This research adds to the understanding in this field by studying real case records from the Dubai Police for the past 12 years. The growth in cases is measured and the main factors behind time spent in their investigation are identified. This research contributes for the understanding of the effects



which volume and heterogeneity of evidence items cause to person-hours spent by Digital Forensic (DF) practitioners.

2. LITERATURE REVIEW

Many research papers studied empirically the current status of DF investigation capabilities and identified challenges which affect different aspects of DF investigations. Gogolin (2010) conducted interviews with practitioners from 45 agencies in Michigan, USA. He identified the current status of experience and investigation capabilities of law enforcement. Dezfoli et al. (2013) conducted a statistical study to cover the trends of several aspects of DFs and security. The research suggests some factors which need to be considered by the digital forensic investigations in order to adapt to the new challenges in the field. Irons & Lallie (2014) demonstrated a yearly growth in the number of forensic investigations, the amount of data being investigated, and the amount of data being investigated per case using the annual data published by the FBI from 2007 to 2011. The authors concluded that digital crimes are increasing remarkably every year.

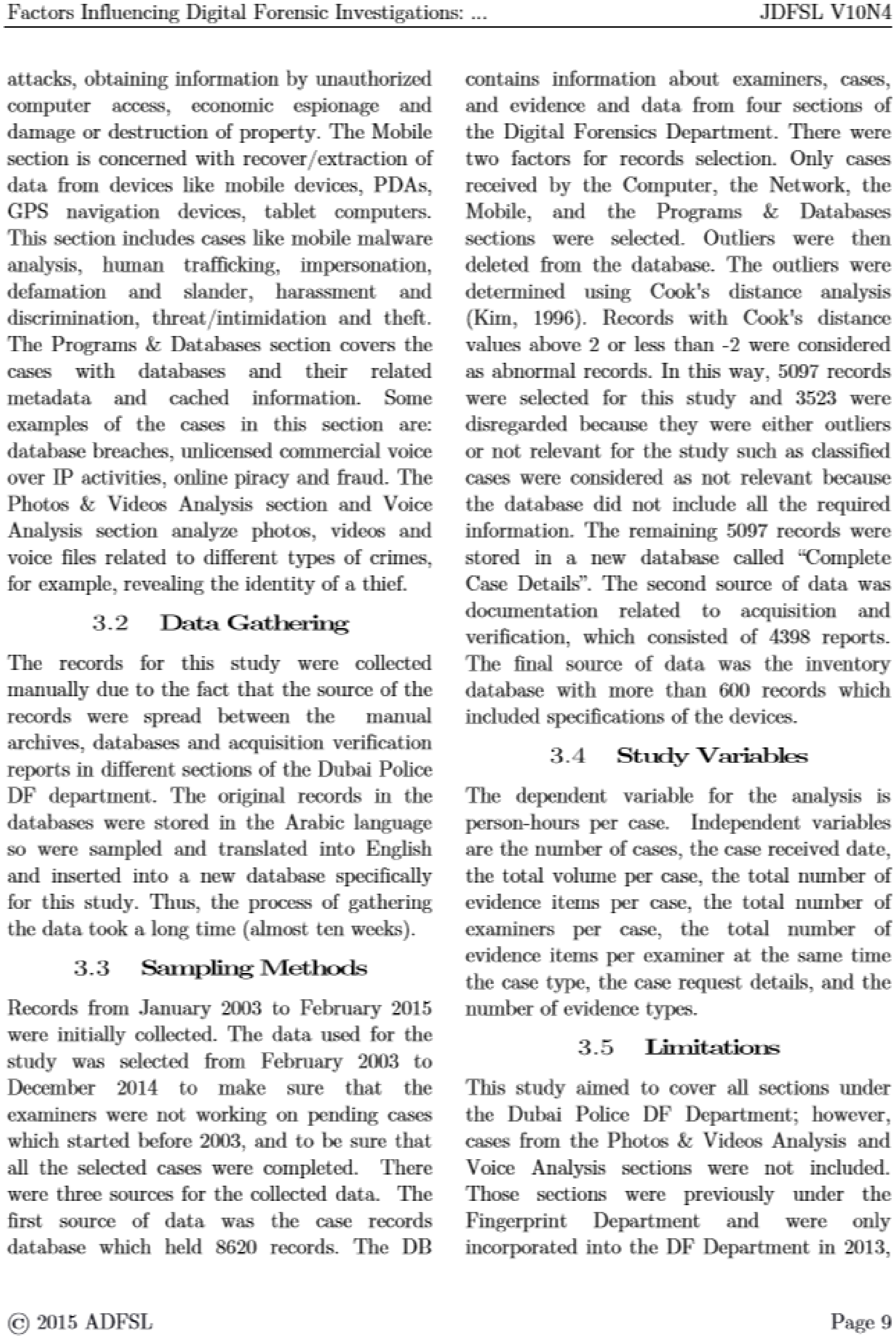
The literature suggests a need to improve the use of the available resources and move beyond the capabilities of the current forensic tools. Each DF process entails a number of challenges including: heterogeneous sources, data diversity, anti-forensics, volume of digital evidence, legal issues, and maintenance of efficiency levels of DF departments. Many practical solutions have been implemented by different DF departments to militate against those challenges. Examples include: features introduced into DF commercial tools, the use of random sampling (Roy, 2014), triage (James, 2014), enhanced previewing (Shaw & Browne, 2013), information visualization (Prefuse, 2013), distributed DFs (Roussev & Golden, 2004) and the use of data mining tools analysis (Nirkhi, Dharaskar, & Thakre, 2012).

3. THE RESEARCH STUDY

To date, research in DF has mainly focused on solutions to technical problems or the analysis of issues faced by practitioners, often not supported by empirical data. This paper reports on the analysis of factors associated with person-hours based on completed cases from the Dubai Police.

3.1 The Dubai Police DF Department

The Dubai Police DF Department is composed of 32 investigators. The department is structured in different sections: Computer, Network, Mobile, Programs & Databases, Photos & Videos Analysis and Voice Analysis. Each section follows the standard DF processes (i.e., acquisition, examination, analysis and reporting) with the goal to examine digital media in a forensically sound manner. The Computer section deals with evidence found in computers, embedded systems, and static memory. It deals with crimes like unauthorized access, intellectual property theft or misuse of information, illicit pornography possession, theft of services, forgery, invasion of privacy, denial of service, sabotage, extortion, embezzlement, espionage, terrorism, racketeering, money laundry, human trafficking, corruption, harassment and discrimination, organized crimes, suicide, threat, and blackmail. The Network section monitors and analyzes computer network traffic for the purpose of data gathering. Hence, this section differs from the other sections because it deals with volatile and dynamic information. The most common crimes investigated by this branch are network breaches, network piracy, unusual network activities, eavesdropping, botnets, targeted



attacks, obtaining information by unauthorized computer access, economic espionage and damage or destruction of property. The Mobile section is concerned with recover/extraction of data from devices like mobile devices, PDAs, GPS navigation devices, tablet computers. This section includes cases like mobile malware analysis, human trafficking, impersonation, defamation and slander, harassment and discrimination, threat/intimidation and theft. The Programs & Databases section covers the cases with databases and their related metadata and cached information. Some examples of the cases in this section are: database breaches, unlicensed commercial voice over IP activities, online piracy and fraud. The Photos & Videos Analysis section and Voice Analysis section analyze photos, videos and voice files related to different types of crimes, for example, revealing the identity of a thief.

3.2 Data Gathering

The records for this study were collected manually due to the fact that the source of the records were spread between the manual archives, databases and acquisition verification reports in different sections of the Dubai Police DF department. The original records in the databases were stored in the Arabic language so were sampled and translated into English and inserted into a new database specifically for this study. Thus, the process of gathering the data took a long time (almost ten weeks).

3.3 Sampling Methods

Records from January 2003 to February 2015 were initially collected. The data used for the study was selected from February 2003 to December 2014 to make sure that the examiners were not working on pending cases which started before 2003, and to be sure that all the selected cases were completed. There were three sources for the collected data. The first source of data was the case records database which held 8620 records. The DB contains information about examiners, cases, and evidence and data from four sections of the Digital Forensics Department. There were two factors for records selection. Only cases received by the Computer, the Network, the Mobile, and the Programs & Databases sections were selected. Outliers were then deleted from the database. The outliers were determined using Cook's distance analysis (Kim, 1996). Records with Cook's distance values above 2 or less than -2 were considered as abnormal records. In this way, 5097 records were selected for this study and 3523 were disregarded because they were either outliers or not relevant for the study such as classified cases were considered as not relevant because the database did not include all the required information. The remaining 5097 records were stored in a new database called "Complete Case Details". The second source of data was documentation related to acquisition and verification, which consisted of 4398 reports. The final source of data was the inventory database with more than 600 records which included specifications of the devices.

3.4 Study Variables

The dependent variable for the analysis is person-hours per case. Independent variables are the number of cases, the case received date, the total volume per case, the total number of evidence items per case, the total number of examiners per case, the total number of evidence items per examiner at the same time the case type, the case request details, and the number of evidence types.

3.5 Limitations

This study aimed to cover all sections under the Dubai Police DF Department; however, cases from the Photos & Videos Analysis and Voice Analysis sections were not included. Those sections were previously under the Fingerprint Department and were only incorporated into the DF Department in 2013, and their records prior to 2013 were not available.

This paper focuses on factors such as the increase in the number of cases and hard disk volume vs. person-hours, independent of the complexity of the cases concerned.

4. GENERAL DESCRIPTION OF DATA

Descriptive statistics show that the number of cases increased each year as illustrated in Figure 1. There were 51 cases in 2003 and more than 900 cases in 2013. In 2010 there was an extraordinary increase in the number of cases due to several high profile crimes in that year which led to the need to initiate more cases. Generally, the number of cases kept increasing throughout the past twelve years. The Computer and Mobile sections received the highest number of cases in across the years.

Across the years, the average time spent in investigation per case was between 100 to 200 hours. There was an exception in 2007, 2008 and 2009 where the average time was less than 100 hours. The average person-hours per case reached a peak of 198 hours in 2014. The averages of the total number of person-hours across the different DF sections show that the cases in the Network section took longer to investigate than other sections in most of the years except for the years 2003, 2006 and 2008. The cases in the Computer section required the second highest amount of time for investigation in all the years from 2004 to 2010. In 2003, the Computer section cases required the highest amount of time for investigation. Since 2011, the cases in the Computer section need less time to investigate than the cases in the Mobile section and Databases & Programs section. It is also noticeable that the time to investigate the cases in the Mobile section has been steadily increasing since 2012.

The volume average of evidence items per case also increased over the years. In years 2011 and 2014 there was a 20% increase For example, the average jumped from 171GB per case in 2010 to 900GB in 2011 and 1186GB in 2014. The Network section received the highest volume average of DF items compared to other sections in the years between 2003-2010 and 2013. In 2011, the Databases section received the highest volume of DF items. In years 2012 and 2014, the Computer section received the highest volume of DF items.

The average of the total number of evidence items per case was between 1 and 2 items among all the years (1.67 in 2003 and 2.09 in 2014) except 2011 where it reached a peak of 3.77. The Databases & Programs section received the highest average of the total number of evidence items in years 2003 - 2006. After that, the Network section remained in a peak from 2004 to 2014.

The average number of examiners working in a case remained between 1 and 2 over the years for all sections (2003-2014). However, the load of evidence items each examiner had at a particular time has fluctuated. The number of evidence items each examiner had at once was around (1.9, 2.92, 2.18, 1.69, 2.01, 2.58, 2.28, 4, 3, 3, 5.21, and 5.89) respectively for years 2003 to 2014. As we can see, the number of evidence items has kept increasing over the years reaching almost 6 items at once in 2014.

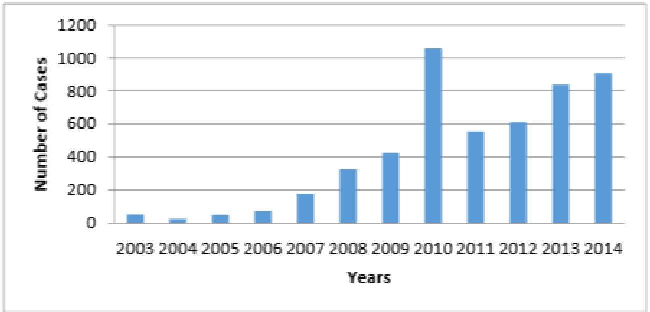


Figure 1. Number of cases from 2003 to 2014 investigated by the Dubai Police DF department

5. ANALYSIS

Data analysis for this study was carried out using a variety of statistical techniques. Data were analyzed using the computerized statistical analysis program SPSS (Version 20). Pearson's Correlation was used to measure the linear correlation between the variables.

5.1 Person-Hours vs. Years

As shown in Figure 1, the number of cases steadily increased over the years. Every year there was a 48% increase in the number of cases compared to the previous year. The Pearson Correlation analysis of the number of cases vs. year equals .884. This means that the total number of cases and the year are strongly correlated. Thus, the number of cases increases progressively every year.

It is important to determine if the total number of person-hours per case has also increased through the years. Simple linear regression was utilized as a key method of regression analysis to study the relationship between this bivariate data, as shown in Figure 2. The Pearson Correlation coefficient .117 reveals a weak relationship between year and person-hours per case. This suggests that person-hours per case did not significantly increase over the years. The majority of cases over the years required less than 200 hours of investigation process for all the evidence items in the case. The number of cases that took more than 200 hours increased slightly over the years and reached a peak by 2011 when it took 4368 hours (nearly 2 years) to investigate 64 evidence items in one case with a size of 28 Terabytes. Despite outlying cases like these, the majority of cases still take less than 200 person-hours to complete.

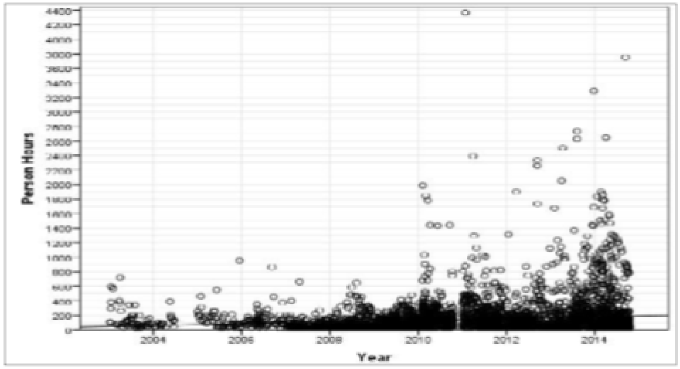


Figure 2. Relationship between person-hours and the year in the Dubai Police DF department

5.2 Person-Hours vs. Volume

The total volume per case also did not affect positively the time of investigation. The Pearson Correlation shows a weak relationship between volume and time spent on each case with a correlation coefficient of 0.388.

5.3 Person-Hours vs. Evidence Items

The Pearson Correlation coefficient between the number of evidence items involved in a case and person-hours spent investigating the case was 0.266. This represents a weak relationship between these bivariate data.

The total number of evidence types per case does not affect the time needed for investigation. The Pearson Correlation of 0.278 indicates a weak relationship between these variables.

Our analysis also showed no significant impact of the category of case on the time taken to conclude the investigation, although on the whole, fraud cases seemed to take more time than other case types.

Although the Pearson Correlation shows that the relationship between the total number of evidence items and year is weak, as discussed in section 5.1, an increase was observed in the number of evidence items over the years.

6. DISCUSSION OF FACTORS INFLUENCING PERSON-HOURS

This section highlights several factors that might influence the increase in person-hours with the caveat that the increase might be a result of the combination of those factors. Environmental factors that might influence the amount of person-hours include hardware specification of workstations used by investigators, availability of investigative software (e.g., specialist DF tools/versions), examiners' experience, complexity of the case and availability of case details. Sections 6.1-6.4 discuss experiments representing some of those assumptions.

6.1 Person-Hours vs. Volume Experiment

There are cases where the total volume of evidence items varied while person-hours were similar. Several filters were applied on the database to select the desired collection of records. First of all, cases with a total storage volume equal to 4 GB and 1024 GB were selected. 1092 records are selected out from 5097 records in the database. The records were then grouped by the total number of person-hours; this resulted in 85 distinct groups. It was found that the majority of the cases with a total of 4 GB volume in a case were received between 2003 and 2011 and most of the cases with 1024 GB volume were received between 2012 and 2014. Thus, the circumstance of spending similar total numbers of person-hours in cases could be explained by factors that must have changed over time; for example, workstation specifications, DF tools and DF practitioners' experience. These tools were more primitive between 2003 and 2011 compared to 2012 to 2014. The cases received in recent years were investigated with better capabilities and sophisticated workstations, tools and experience.

6.2 Number of DF Practitioners vs. Volume Experiment

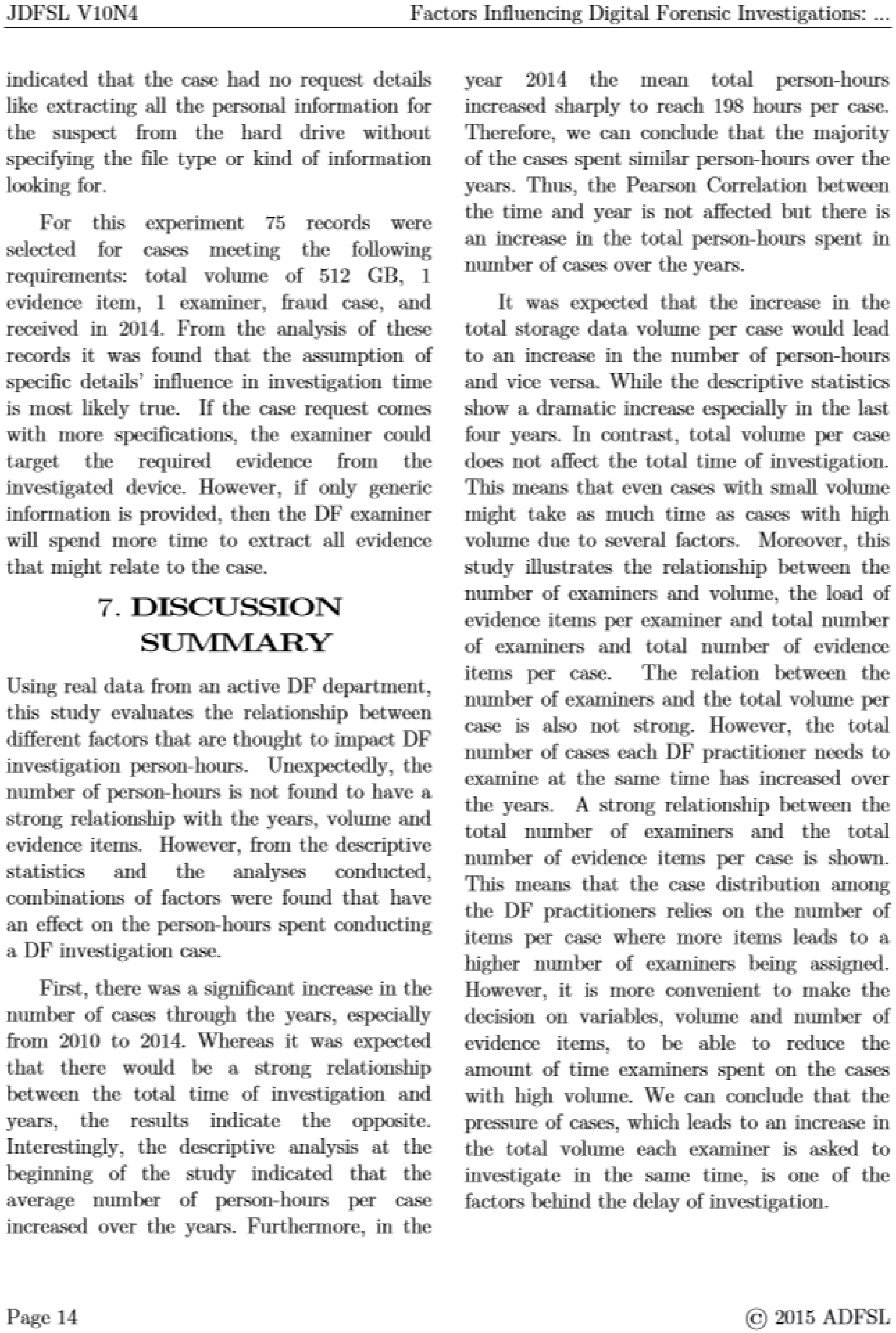
There are many cases where the number of DF practitioners varied but the total volume of evidence items per case did not. To understand this, cases with volume of 2048 GB were selected from the year 2013 and separately cases with a total volume of 20480 GB were selected from the year 2014. There were 47 such cases found in 2013 and 7 such cases found in 2014. By analyzing the records, it was identified that the cases with identical volume took less total hours with higher numbers of forensic practitioners than fewer forensic practitioners. The selected records were analyzed in terms of case priority where the total volume is fixed and the priority of the cases varied. This experiment shows that the cases with high priority are more often assigned to more practitioners than the cases with normal priority. Hence, it is likely that if two cases are received with the same specifications but different priorities, a higher number of forensic examiners will be assigned to the high priority cases compared to the normal priority cases.

6.3 Practitioners' Experience Experiment

In this experiment the examiners were divided in three groups depending on their experience: (novice) less than 3 years of experience, (proficient) 3-7 years of experience, and (expert) more 7 years of experience. Cases with similar volume (512 GB) with one examiner working per case were selected from one specific year (2013) resulting in the selection of 256 records. The Pearson Correlation equals -.233. This shows that the strength of association is small. However, the analysis of these records also showed that there was evidence that novice examiners spent more time than the other levels of examiners, and that expert examiners spent the least time in investigations.

6.4 Person-Hours vs. Case Details Experiment

It is well known among digital forensic practitioners that the amount of details that comes in the case request to describe what is required from the examiner to search for affects the person-hours. It is assumed that the cases with more details and specifications could be investigated faster than cases with generic or little information. This experiment sought to understand the effect of case details variable on person-hours. A case details value was incorporated into the dataset, which could be either 'specific' or 'general'. *Specific* indicated that the case had provided search keywords and/or details like asking for the existence of a specific type of file in the hard drive or the case request provided the forensic examiner with personal details of the suspects. *General*



indicated that the case had no request details like extracting all the personal information for the suspect from the hard drive without specifying the file type or kind of information looking for.

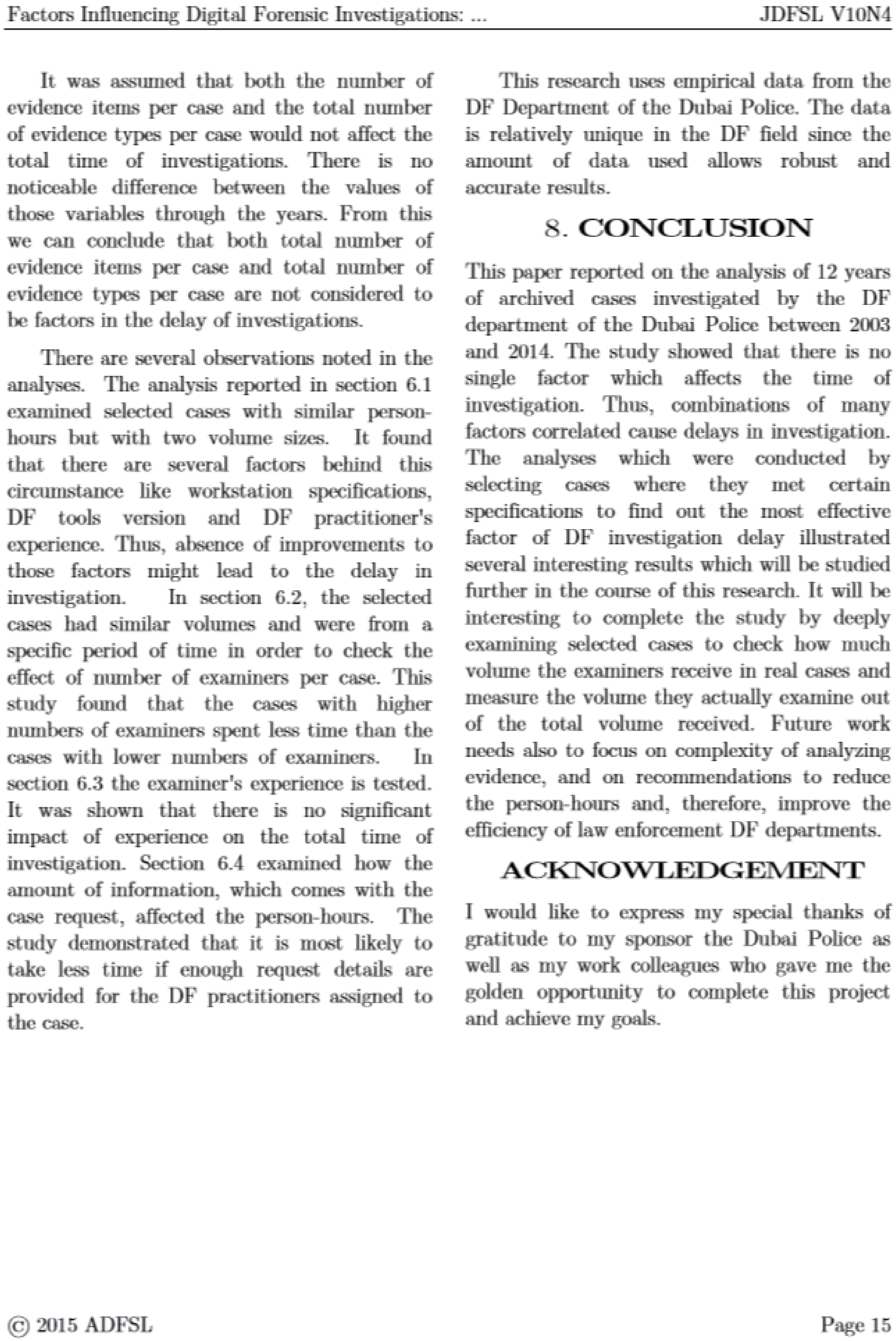
For this experiment 75 records were selected for cases meeting the following requirements: total volume of 512 GB, 1 evidence item, 1 examiner, fraud case, and received in 2014. From the analysis of these records it was found that the assumption of specific details' influence in investigation time is most likely true. If the case request comes with more specifications, the examiner could target the required evidence from the investigated device. However, if only generic information is provided, then the DF examiner will spend more time to extract all evidence that might relate to the case.

7. DISCUSSION SUMMARY

Using real data from an active DF department, this study evaluates the relationship between different factors that are thought to impact DF investigation person-hours. Unexpectedly, the number of person-hours is not found to have a strong relationship with the years, volume and evidence items. However, from the descriptive statistics and the analyses conducted, combinations of factors were found that have an effect on the person-hours spent conducting a DF investigation case.

First, there was a significant increase in the number of cases through the years, especially from 2010 to 2014. Whereas it was expected that there would be a strong relationship between the total time of investigation and years, the results indicate the opposite. Interestingly, the descriptive analysis at the beginning of the study indicated that the average number of person-hours per case increased over the years. Furthermore, in the year 2014 the mean total person-hours increased sharply to reach 198 hours per case. Therefore, we can conclude that the majority of the cases spent similar person-hours over the years. Thus, the Pearson Correlation between the time and year is not affected but there is an increase in the total person-hours spent in number of cases over the years.

It was expected that the increase in the total storage data volume per case would lead to an increase in the number of person-hours and vice versa. While the descriptive statistics show a dramatic increase especially in the last four years. In contrast, total volume per case does not affect the total time of investigation. This means that even cases with small volume might take as much time as cases with high volume due to several factors. Moreover, this study illustrates the relationship between the number of examiners and volume, the load of evidence items per examiner and total number of examiners and total number of evidence items per case. The relation between the number of examiners and the total volume per case is also not strong. However, the total number of cases each DF practitioner needs to examine at the same time has increased over the years. A strong relationship between the total number of examiners and the total number of evidence items per case is shown. This means that the case distribution among the DF practitioners relies on the number of items per case where more items leads to a higher number of examiners being assigned. However, it is more convenient to make the decision on variables, volume and number of evidence items, to be able to reduce the amount of time examiners spent on the cases with high volume. We can conclude that the pressure of cases, which leads to an increase in the total volume each examiner is asked to investigate in the same time, is one of the factors behind the delay of investigation.



It was assumed that both the number of evidence items per case and the total number of evidence types per case would not affect the total time of investigations. There is no noticeable difference between the values of those variables through the years. From this we can conclude that both total number of evidence items per case and total number of evidence types per case are not considered to be factors in the delay of investigations.

There are several observations noted in the analyses. The analysis reported in section 6.1 examined selected cases with similar person-hours but with two volume sizes. It found that there are several factors behind this circumstance like workstation specifications, DF tools version and DF practitioner's experience. Thus, absence of improvements to those factors might lead to the delay in investigation. In section 6.2, the selected cases had similar volumes and were from a specific period of time in order to check the effect of number of examiners per case. This study found that the cases with higher numbers of examiners spent less time than the cases with lower numbers of examiners. In section 6.3 the examiner's experience is tested. It was shown that there is no significant impact of experience on the total time of investigation. Section 6.4 examined how the amount of information, which comes with the case request, affected the person-hours. The study demonstrated that it is most likely to take less time if enough request details are provided for the DF practitioners assigned to the case.

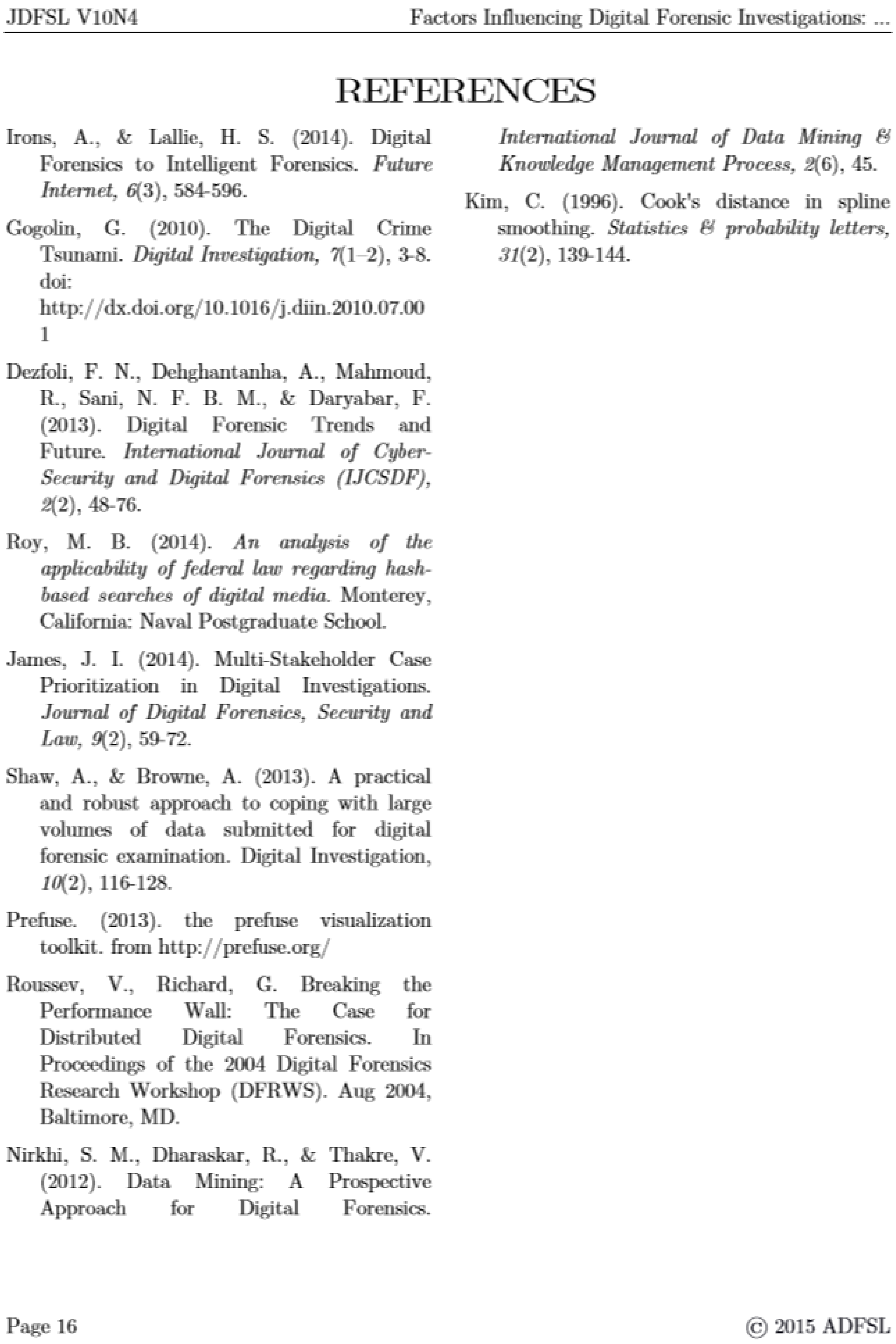
This research uses empirical data from the DF Department of the Dubai Police. The data is relatively unique in the DF field since the amount of data used allows robust and accurate results.

8. CONCLUSION

This paper reported on the analysis of 12 years of archived cases investigated by the DF department of the Dubai Police between 2003 and 2014. The study showed that there is no single factor which affects the time of investigation. Thus, combinations of many factors correlated cause delays in investigation. The analyses which were conducted by selecting cases where they met certain specifications to find out the most effective factor of DF investigation delay illustrated several interesting results which will be studied further in the course of this research. It will be interesting to complete the study by deeply examining selected cases to check how much volume the examiners receive in real cases and measure the volume they actually examine out of the total volume received. Future work needs also to focus on complexity of analyzing evidence, and on recommendations to reduce the person-hours and, therefore, improve the efficiency of law enforcement DF departments.

ACKNOWLEDGEMENT

I would like to express my special thanks of gratitude to my sponsor the Dubai Police as well as my work colleagues who gave me the golden opportunity to complete this project and achieve my goals.



REFERENCES

Irons, A., & Lallie, H. S. (2014). Digital Forensics to Intelligent Forensics. *Future Internet, 6*(3), 584-596.

Gogolin, G. (2010). The Digital Crime Tsunami. *Digital Investigation, 7*(1–2), 3-8. doi: http://dx.doi.org/10.1016/j.diin.2010.07.001

Dezfoli, F. N., Dehghantanha, A., Mahmoud, R., Sani, N. F. B. M., & Daryabar, F. (2013). Digital Forensic Trends and Future. *International Journal of Cyber-Security and Digital Forensics (IJCSDF), 2*(2), 48-76.

Roy, M. B. (2014). *An analysis of the applicability of federal law regarding hash-based searches of digital media*. Monterey, California: Naval Postgraduate School.

James, J. I. (2014). Multi-Stakeholder Case Prioritization in Digital Investigations. *Journal of Digital Forensics, Security and Law, 9*(2), 59-72.

Shaw, A., & Browne, A. (2013). A practical and robust approach to coping with large volumes of data submitted for digital forensic examination. Digital Investigation, *10*(2), 116-128.

Prefuse. (2013). the prefuse visualization toolkit. from http://prefuse.org/

Roussev, V., Richard, G. Breaking the Performance Wall: The Case for Distributed Digital Forensics. In Proceedings of the 2004 Digital Forensics Research Workshop (DFRWS). Aug 2004, Baltimore, MD.

Nirkhi, S. M., Dharaskar, R., & Thakre, V. (2012). Data Mining: A Prospective Approach for Digital Forensics. *International Journal of Data Mining & Knowledge Management Process, 2*(6), 45.

Kim, C. (1996). Cook's distance in spline smoothing. *Statistics & probability letters, 31*(2), 139-144.