
**A Method to Enhance the Accuracy of
Digital Forensics in the Absence of Complete
Evidence in Saudi Arabia**

PhD Thesis

Fahad Mosalm Alanazi

*A Doctoral Thesis Submitted in Partial Fulfilment of the
Award of Doctor of Philosophy*

Cyber Security Center

De Montfort University

United Kingdom

27th April 2017

Abstract

The tremendous increase in the use of digital devices has led to their involvement in the vast majority of current criminal investigations. As a result, digital forensics has increasingly become one of the most important aspects of criminal investigations. The digital forensics process involves consideration of a number of important phases in order to achieve the required level of accuracy and to reach a successful conclusion of the investigation into the digital aspects of crimes; through obtaining acceptable evidence for use in a court of law. There have been a number of models developed and produced since 1984 to support the digital investigation processes. In this submission, I introduce a proposed model for the digital investigation processes which is based on the scope of the Saudi Arabia investigation process, which has been integrated with existing models of digital investigation processes and has produced a new phase to deal with a situation where there is insufficient evidence.

In this research, grounded theory has been adopted as a research method to investigate and explore the participant's perspectives and their opinions regarding the adoption of a method of a digital forensics investigation process in the absence of complete evidence in the Saudi Arabian context. The interaction of investigators with digital forensics processes involves the social aspect of digital investigation which is why it was suitable to adopt a grounded theory approach. A semi-structured data collection approach has been adopted, to enable the participants to express their visions, concerns, opinions and feelings related to factors that impact the adoption of the DF model for use in cases where there is an absence of sufficient evidence in Saudi Arabia.

The proposed model emerged after conducting a number of interviews and analysing the data of this research. The researcher developed the proposed model based on the answers of the participant which helped the researcher to find a solution for dealing with cases where there is insufficient evidence, through adding a unique step in the investigation process, the “TraceBack” Phase.

This study is the first in Saudi Arabia to be developed to enhance the accuracy of digital forensics in the absence of sufficient evidence, which opens a new method of research. It is also the first time has been employed a grounded theory in a digital forensics study in the Saudi context, where it was used in a digital forensics study, which indicates the possibility of applying this methodology to this field.

Dedication

To my Parents

For all their love, help and patience; without their endless support

I would not have finished my PhD!

To my Brothers and Sisters

For their endless support and encouragement, from the beginning of my study until the
very end

To my Wife

For her endless love, support, and patience

Without her patience, most of this work would not have been done

To my sons

Naïf, Rayan and Sultan who are sacrificed to that time during my study which I should
be with them

Thank you very much indeed for everything you have done for me, I am forever
indebted.

Declaration

I declare that the work described in this thesis is original work undertaken by me for the degree of Doctor of Philosophy, at Cyber Security Center at De Montfort University, United Kingdom.

No part of the material described in this thesis has been submitted for any award of any other degree or qualification in this or any other university or college of advanced education.

Fahad Alanazi

Publications

Professional Conference papers (published)

- Alanazi, F., & Jones, A. (2015, September). The Value of Metadata in Digital Forensics. In *Intelligence and Security Informatics Conference (EISIC), 2015 European* (pp. 182-182). IEEE.
- Alanazi, F., & Jones, A. (2017). A Method to Enhance the Accuracy of Digital Forensic in the Absence of Sufficient Evidence in Saudi Arabia. *World Academy of Science, Engineering and Technology, International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering, 11(3)*, 464-468.
- **Professional Journal papers (Under review)**
- Alanazi, F., & Jones, A. (2017). Sharia Law and Digital Forensics.

List of Figures

Figure 1 Computer forensic Investigation Process	16
Figure 2 Scientific Crime Scene Investigation Model	17
Figure 3 Digital Forensic Research Workshop Model (DFRWS).....	18
Figure 4 Abstract Digital Forensic Model (ADFM).....	19
Figure 5 Integrated Digital Investigation Process (IDIP).....	20
Figure 6 Enhanced Digital Investigation Process Model (EDIP).....	22
Figure 7 Extended Model of Cybercrime Investigation	24
Figure 8 Computer Forensic Field Triage Process Model (CFFTPM)	26
Figure 9 Framework for a Digital Forensic Investigation.....	27
Figure 10 Common Process Model for Incident and Computer Forensics	28
Figure 11 Digital Forensic Model based on Malaysian Investigation Process (DFMMIP)	29
Figure 12 Network Forensic Generic Process Model.....	30
Figure 13 Generic Computer Forensic Investigation Model.....	31
Figure 14 A new Triage Model Conforming to the Needs of Selective search and seizure of electronic Evidence	32
Figure 15 Paradigm Model in Axial Coding.....	105
Figure 16: Conduction Investigation category.....	162
Figure 17 Investigators experiences with insufficient evidence.....	168
Figure 18: Core category	172
Figure 19 Traceback Process	179
Figure 20 - Collaboration process between investigator and digital investigator	180
Figure 21 Proposed Framework.....	194

List of Tables

Table 1 comparison of digital investigation phases.....	34
Table 2 Comparison between Quantitative and Qualitative Methods	75
Table 3 Comparisons of the two schools of Grounded Theory	101
Table 4 Advantages and disadvantages of the Pilot Study	118
Table 5 Pilot Study interview Questions	123
Table 6 Empirical study cycle	125
Table 7 Pilot Study interview Questions	126
Table 8 Full Study interview Questions	127
Table 9: Comparison of digital investigation phases in the proposed research model with existing mode	193

Acknowledgements

First and foremost, I owe my sincerest gratitude to the most merciful ALLAH for all the things he blessed me with throughout my whole life, without those blessings, I would not be able to accomplish any of this work.

I would also like to offer my genuine gratefulness to my supervisor and the one behind this project, Prof. Andrew Jones, for his endless support, encouragement, and guidance. This thesis would have been unachievable without him and I am so fortunate and happy to have completed my PhD under his supervision.

I would like to express my deepest thanks to Dr. Helge Janicke, my advisor and the head of the Cyber Security for his guidance and care for everyone in Cyber Security. Of course, I cannot forget to thank all the researchers, colleagues and staff of the Cyber Security, Faculty of Technology, De Montfort University for the friendly and convenient working atmosphere as well as all the constructive discussions that we have had over the years!

Last but not least, I would like to express my deepest thanks to my parents for their prayers, support and encouragement, whose prayers and blessings were no doubt the true reason behind any success I have! I especially would like to show my love and appreciation for my late father who encouraged me to pursue this PhD in the first place. Special gratitude is due to my Mother, brothers and lovely sisters for their loving, support, genuine concern and encouragement throughout all these years, and I would like to special gratitude my wife for being patient while I was doing my thesis, without her patience most of this work would not have been accomplished.

Table of Contents

1. Chapter 1:.....	1
Introduction.....	1
1.1 Problem Statement and Motivation.....	2
1.2 Objective.....	3
1.3 Research Question.....	4
1.4 Contribution.....	4
1.5 Thesis Structure.....	6
2 . Chapter 2:.....	8
Literature Review.....	8
2.1 Introduction.....	9
2.2 Review of Current Research Methods in the Investigation Process.....	15
2.2.1 Computer Forensic Investigation Process.....	16
2.2.2 Scientific Crime Scene Investigation Model.....	16
2.2.3 Digital Forensic Research Workshop Model (DFRWS).....	17
2.2.4 Abstract Digital Forensic Model (ADFM).....	18
2.2.5 Integrated Digital Investigation Process (IDIP).....	20
2.2.6 Enhanced Digital Investigation Process Model (EDIP).....	21
2.2.7 Extended Model of Cybercrime Investigation.....	24
2.2.8 Computer Forensic Field Triage Process Model (CFFTP).....	25
2.2.9 Framework for a Digital Forensic Investigation.....	27
2.2.10 Common Process Model for Incident and Computer Forensics (CPMICF).....	28
2.2.11 Digital Forensic Model Based on Malaysian Investigation Process (DFMMIP).....	28
2.2.12 Network Forensic Generic Process Model (NFGP).....	30
2.2.13 Generic Computer Forensic Investigation Model (GCFIM).....	31
2.2.14 A new triage model conforming to the needs of selective search and seizure of electronic evidence.....	32
2.3 Discussion.....	33
2.4 Legislation in Saudi Arabia.....	40
2.5 Sharia Law.....	41
2.6 Digital Forensics in Saudi Arabia.....	45
2.6.1 Saudi legislation with regards to criminal investigations.....	48

2.6.2	Experts' scope of work under Saudi Legislation	49
2.6.3	Summary of the role of the investigation within the Saudi courts	51
2.7	Digital Forensics Procedure	51
2.8	Size of digital crimes in Saudi Arabia	59
2.9	Drug crime.....	62
2.9.1	Why Drugs?	63
2.9.2	Why Saudi?	64
2.10	Conclusion.....	66
3	Chapter 3:.....	68
	Research Methodology	68
3.1	Introduction.....	69
3.2	Paradigm level	69
3.3	Methodological Levels.....	70
3.4	Quantitative Versus Qualitative Methodologies	71
3.5	Method Adopted for Current Research.....	78
3.6	Data Collection	79
3.7	General Discussion of Interview and Chosen Interview	80
3.7.1	Method used in semi-structured interviews	85
3.7.2	Rationale for the use of semi-structured interviews.....	87
3.8	Research Method.....	87
3.8.1	Introduction.....	87
3.8.2	Grounded theory	91
3.8.3	The Value of Using Grounded Theory in IS Research	93
3.8.4	Criticisms of Grounded Theory	94
3.8.5	Constant comparison.....	96
3.8.6	Theoretical sampling.....	97
3.8.7	Glaserian vs. Straussian approaches	98
3.8.8	Straussian approach procedures	103
3.8.9	Grounded Theory Techniques.....	107
3.8.10	Justification for the selected research methods and methodology with regards to the research questions	109
3.9	Conclusion.....	110
4	Chapter 4:.....	112

Research Design.....	112
4.1 Introduction.....	113
4.2 Definition of pilot study.....	113
4.3 Value and Goal of the Pilot Study	115
4.4 Advantages and disadvantages of the pilot study	118
4.5 Interview Protocol.....	119
4.6 Interview Procedure	120
4.7 Sample size of the pilot study and its justification	122
4.8 Empirical Study	124
4.9 Full study interview questions	125
4.10 Justification for the selected sample of interviewees	128
4.10.1 What is a Stakeholder?	129
4.10.2 Who are the Stakeholders?.....	130
4.11 Conclusion.....	131
5 Chapter 5:.....	132
Research analysis finding and discussion.....	132
5.1 Introduction.....	133
5.2 Open coding	134
5.3 Axial Coding.....	155
5.3.1 Investigation Procedure in drug's cases	155
5.3.2 Investigators' experience with insufficient evidence	163
5.4 Selective coding	170
5.4.1 Story line	170
5.4.2 The relationship between the core and other categories (emerged from axial coding)	171
5.4.3 Advantages of cooperation.....	181
5.4.4 Importance of cooperation	182
5.4.5 Proposed research model for solving the issue of insufficient evidence	183
5.4.6 Example of a case with insufficient evidence	185
5.4.7 Application of Traceback.....	187
5.4.8 The difference between the Traceback process and other digital investigation processes.....	191
5.4.9 Proposed Framework.....	193

5.4.10	Justification for proposed framework	202
5.4.11	Conclusion	204
6	Chapter 6:.....	206
	Conclusion.....	206
6.1	Introduction.....	207
6.2	Research contribution	207
6.3	Recommendations for Further work	211
6.4	Research limitation	211
6.5	Conclusion	212
7	References	213
8	Appendix	233

Chapter 1:

Introduction

Objectives

- Provide a problem statement along with the motivation and objectives for this research.
 - Highlight the research question and sub questions
 - Outline the main research contribution
 - Present thesis structure
-

1.1 Problem Statement and Motivation

Criminals today use computers not only to carry out illegal and immoral activities but also to help them hide such activities (Al qahtani, 2014).

Digital crimes are not always a new form of crime: they are the result of the use of computer systems for nefarious purposes. Such crimes have led to the creation of a form of investigation called digital forensics (Čisar* and Čisar, 2011). Digital forensics calls for investigators with a very specific set of skills and qualifications and the use of specified tools with integrity in order to guarantee that the evidence collected is admissible as evidence in a court of law.

It is becoming increasingly difficult for digital forensic investigators to carry out thorough and reliable investigations given the increasing complexity of the environment in which such crimes are committed due to ever more sophisticated applications, the increasing number of networks systems, the volume of storage available, cloud computing and the exponential increase in the number of interactions. Thus, digital forensic investigations are susceptible to mistakes, which can lead to digital evidence not being recovered or not being admissible in a court of law because, for example, failure to follow the correct processes, of a lack of accuracy, incomplete evidence or invasion of privacy.

The digital world has expanded exponentially in recent years. Alongside increased internet use there has been an increase in the number and diversity of tools used by criminals. Therefore, digital forensics needs to be able to counter challenges arising from the growing complexity of criminal scenarios and make it possible to properly handle evidence. This is a major concern for the implementation of the investigation process when seeking to achieve a comprehensive and reliable conviction.

In the last three decades (specifically from 1984 to 2013), researchers have proposed a number of investigation models in an attempt to create a model which is applicable to any scenario (Yusoff et al, 2011), (Hong et al, 2013). The models proposed, however, do not cover all aspects of digital crime investigation. One of the main aspects, which have not been covered in these models, is how to deal with cases where there is insufficient evidence. In addition, a report issued by the Saudi Ministry of Justice revealed that cybercrime increased during the past two years by more than 437 %. The report shows a lot of crimes since applying cybercrime in Saudi Arabia, reach a number of 775 crimes were registered in Saudi courts. These 775 crimes exceeded the number of crimes that were registered in Saudi courts that were 573 in 2015 and 164 in 2014 (Alaraby, 2016). Therefore, there were many reasons motivating the decision to undertake this research; see below:

1. The field of digital forensics in Saudi Arabia needs a mechanism for helping improve the accuracy of the digital evidence to be acceptable in the court of law.
2. There is a lack of studies concerning digital investigation process in Saudi Arabia.
3. There are an absence of studies regarding digital investigation process in case where there is insufficient evidence in Saudi Arabia.
4. There is not officially procedure to carry out digital investigation written yet.
5. The digital investigation processes identified in other researcher since 1984 did not identified any investigation process that address the issue of sufficient evidence.

1.2 Objective

The main objective of this research is to identify the factors that influence the digital investigation process and address the challenges which arise with regard to ensuring that

the evidence gathered is as complete as possible and is also admissible in a court of law in Saudi Arabia. The objectives of the research are:

- To establish a novel mechanism to improve the accuracy of the analysis in the case of incomplete and/ or imprecise evidence.
- To compare the results with existing approaches.

1.3 Research Question

How can the accuracy of the digital forensic procedure in cases where there is insufficient evidence be improved in Saudi Arabia?

Sub Questions

- What is the definition of Digital Forensics?
- What are the research models of digital investigation processes available?
- Are there any specific issues that arise as a result of the use of Sharia Law in Saudi Arabia?
- What is the process of investigation for digital crimes in Saudi Arabia?
- How does the Saudi Arabia investigation procedure handle cases with insufficient evidence?

1.4 Contribution

The field of digital forensics needs a mechanism which will help improve the accuracy and completeness of the digital evidence gathered. The way in which this concept will function is such that the evidence gathered by the digital forensic investigator will be permissible to use interrogatively alongside statements collected from suspect individuals in Saudi Arabian court of law.

Therefore, this research proposes to enhance the accuracy of digital forensics process in cases of where there is insufficient evidence in Saudi Arabia, by extending the existing the digital forensic investigation processes. This extension includes adding a phase (traceback) to the existing framework for the investigative process. For example, in cases where there is insufficient evidence, the theoretical framework ensures that the investigator has taken all necessary actions to collect evidence and later, the traceback phase aims to guide further investigation to discover leads that may be relevant to the case and help it to reach a point where there is sufficient evidence. In doing so this research benefits from existing models of the digital investigation process by integrating existing high-efficiency mechanisms with the new process which will improve the accuracy of digital investigation process in cases where there is an initially insufficient evidence.

The review of the digital investigation processes identified in other research since 1984 did not identify any investigation process that addresses the issue of insufficient evidence; (a lack of sufficient evidence or fact to prove for a jury to reach a verdict) (The Law Dictionary).

In addition, there is a lack of research in Saudi Arabia addressing the digital investigation process and enhancing the accuracy of digital forensics in cases where there is insufficient evidence. Thus, there is a need to undertake this research, which will enable organisations to deal with incomplete evidence and reduce the number of cases rejected by the courts. In the process of developing and enhancing digital forensics procedures which is, in turn, developing a new method to deal with incomplete evidence, this research provides a new mechanism to deal with incomplete evidence through a new phase which is called Traceback which is explained in Chapter 5, section 5.6. This study implements grounded

theory as a research methodology to make a theoretical contribution to the academic understanding of the chosen topic.

1.5 Thesis Structure

This thesis consists of six chapters. This introductory chapter has addressed the scope of this research by mentioning the lack of prior research conducted in Saudi Arabia regarding methods to enhance the accuracy of digital forensics in evidence. It has also addressed the motivations for studying this subject and has outlined the objectives of this study and research question. The chapter concludes by establishing the research novelty that will be investigated in the study.

The second chapter is the literature review. This chapter provides an overview of the current research methods in the digital forensics investigation process. It also gives an overview of digital forensics and the scale of crimes involving digital devices in Saudi Arabia. It provides the reason for choosing the context of Saudi Arabia, drug crimes and cases where there is insufficient evidence in Saudi Arabia.

Chapter three discusses the research methodologies that have been applied in this research. It provides an overview of qualitative and quantitative research methods and the data collection method and justifies the research methodology. In addition, it refers to the analysis method and discusses in depth grounded theory through adapting the Strauss approach. Moreover, this chapter also reviews the differences and similarities between the versions of grounded theory presented by its two originators, Glaser and Strauss (Strauss and Corbin, 1990). Justification is provided for choosing the Strauss approach as a data analysis process.

Chapter four denotes the research design, this chapter discusses the pilot study; definitions, the value and goal of pilot study, advantages and disadvantages of the pilot study, size of the sample, and the justification for choosing these samples and interview protocol. It also provides an overview of the empirical study and the implementation of the empirical study and data collection, full study questions and justification for the selected sample of interviewees.

Chapter five discussed the finding that emerged from the Saudi context in more details. The first section discusses the categories that emerged and the interrelationships between concepts and categories. This section finishes by determining the core category from the Saudi context.

Chapter six presents the research conclusions. This chapter including answers to the research questions, addresses the contributions of this research to knowledge, recommendations, evaluation, limitations of the research and suggestions for future studies.

Chapter 2:

Literature Review

Objectives

-
- To review the available digital investigation processes
 - To review legislation in Saudi
 - To review Digital Forensics in Saudi
-

2.1 Introduction

The current digital era is characterised by the wide range of digital applications and rapid changes in technology. Today's technological world has seen a tremendous rise in the use of digital device(s) in people's private lives and also in commercial, educational and governmental organisations. Unfortunately, the use of computers and digital devices to commit crimes has also increased as technological advances can also help criminals to carry out and hide their illegal activities. Cybercrime consists of two elements – old crimes making use of the new technologies and new crimes that could not exist before, such as those identified by Gillespie “cyberspace has allowed the crimes to commit in new ways - phishing or hacking into a bank account the publishing of illicit material to the webpage. Computers focused crimes, however, are different and are those crimes that came into existence because the computer is an intrinsic part of the conduct of such crimes. A classic example here would be hacking. There was no crime of hacking before a computer because hacking requires a computer - something has to be hacked” (Gillespie, 2015: pp 4); which exploits computer technology and the easy access of information. Cybercrimes are the result of the availability of computer technology and a malicious user's proficiency. During an investigation, digital forensics investigators must follow legally defined and dependable forensic procedures to identify and prosecute criminals who have committed crimes using digital technology (Wit, 2013).

In the past few years, computer forensics has become a significant method of identifying and prosecuting criminals who have committed crimes using computers or on which data related to the crime is stored (Čisar, 2011).

Although Computer Forensics is a relatively new science its definition has been extended to include all types of forensics which involve digital devices (de Wit, 2013).

The process of identification, collection, analysis, preservation and presentation of digital evidence from a computer by using tools and techniques to determine potential evidence for legal purposes is referred to as Computer Forensics (Zareen et al, 2013), (de Wit, 2013).

Digital forensics is defined as *“the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorised actions shown to be disruptive to planned operations”* (DFRWS 2001).

Digital forensics is a combination of computer science concepts such as *“computer architecture, operating systems, file systems, software engineering and computer networking with legal procedures and rules of evidence”*, which can be used in criminal and civil litigation (Elsheik, 2016). It is the process of identifying and determining important relevant information from digital sources. This includes the collection and preservation of information without the loss of its integrity and its analysis and presentation (Casey, 2011; Holt et al, 2012; Magnus, 2014). The result of the forensic investigation process (es) carried out is referred to as digital evidence (Chow et al, 2014, Cohen, 2015; Adams, 2012).

Some authors clearly distinguish between computer forensics and digital forensics. However, de Wit, (2013), consider the two to be the same in their work. “Thus, computer forensics implies a connection between computers, the scientific method, and crime detection. Digital forensics is largely used interchangeably with computer forensics, but

implies the inclusion of devices other than general-purpose computer systems, such as network devices, cell phones, and other devices with embedded systems” (Mohammed and Nwachukwu, 2015).

In general terms digital forensics can be defined as the application of computer techniques and analysis procedures to digital forensics investigations or the collection of evidence from digital devices (Čisar* and Čisar, 2011).

Many computer or digital device related cases remained unsolved before the development of digital forensics investigation procedures and techniques (de Wit, 2013).

Digital forensics is increasingly important in the investigation of crimes. The evidence, which is collected by investigator through the use of accepted tools, techniques and procedures, will be admissible in the courts (Stephenson and Gilbert, 2013). Digital investigation involves creating and testing hypotheses to assess the state of a digital device and its data; when one cannot directly examine digital device and its data, because the digital investigator in this case will investigate within the context these hypotheses to establishment of perception on the case to access to the evidence or presumptions that may lead to prove or disprove the case. For example, when FBI believed that the iPhone of one of the suspects, who committed an armed attack in San Bernardino County may provide evidence for the investigation. Thus, the FBI requested the Apple Company to override the password of the suspect iPhone; however Apple rejected the request because of the protection of the privacy of its customers. The FBI, based on their belief that the iPhone might contain data related to the case eventually contacted a third party to break the password without prejudice to any existing information (The New Arab, 2016). To give a parallel example, when one learns of something through someone else instead of

through direct experience, the extent to which one believes what one has heard depends on the level of trust one has in the other person. In digital forensics, trustworthiness is based on the hardware/software, the processes used and the skills and experience of the investigators used to collect and analyse the evidence during the investigation. The tools, techniques and methods used to create and test the hypotheses make the investigation a scientific process (Kohn et al, 2013).

There are many reasons why the prosecution of a digital criminal might stop at the investigation level, the most important being lack of preparation (for example the scope of the warrant must not be breached at any circumstances. If different evidence is found that does not relate to the case then a new warrant must be applied to investigate that evidence (procedure). Other examples include preparation for the lab and report), and the lack of skill in choosing tools to collect digital evidence in a successful way or failure to maintain the chain of custody which is “documentation of all the steps (collection, transportation, analysis, and storage processes) that evidence has taken from the time it is located at the crime scene to the time it’s introduced in the courtroom” (Solomon et al, 2011), because they are the main keys to ensure integrity, accuracy and reliability, additionally professional acceptance that may be subject to question by opposing. Digital evidence is digitally stored or transmitted information, which can be used to prove or disprove a crime in a court of law during the trial process (Čisar* and Čisar, 2011).

Digital evidence can be found in diverse sources such as computing devices (for instance, laptop and desktop, satellite and navigation systems, digital cameras, iPads, iPods, personal digital assistants [PDAs] and mobile phones) and network devices (servers, routers, hub, modem and network hardware) (Brown, 2010; Lang, 2014; Holt et al, 2012). In some cases the information which has evidentiary value may also be found on other

digital media like main computer memory, Compact Disk (CDrom), digital versatile discs (DVDrom), external drives like USB, Harddisk and memory cards (from digital cameras and mobile phones) (Hirwani et al , 2012; Achille and Roger, 2014; Bem et al , 2008; Gayed et al , 2013).

As stated by Casey, (2010) and Frowen, (2009), judges and other judicial panels must have some knowledge of the various types of Information and Communication Technology (ICT) devices to make the right decision about the admissibility of digital evidence and to understand expert witness testimony (Casey, 2011; Frowen, 2009). Makutsoane and Leonard, (2014); Olajide, (2011) and Baca et al, (2013) claim that such knowledge should be gained from personal experience that involve of using of computers and the internet, not necessarily from formal education and training (Makutsoane and Leonard, 2014; Leslie, 2014; Olajide, 2011 and Baca et al, 2013).

In the USA, judges must have a clear understanding of the “*application of the Fourth Amendment and State Constitution rules to digital devices*” before they consider admitting digital evidence (Kessler, 2010). In addition, it is the responsibility of the judges to balance the need for a thorough examination of the evidence with the need for a speedy trial (Kessler, 2010). “*The Fourth Amendment to the U.S. Constitution requires law enforcement personnel to have a legitimate search warrant to seize property for examination and analysis purposes. Exceptions to these requirements to obtain a search warrant are described later*” (Kessler, 2010). Sharia Law (Shria Law is the common Law within the Islamic religion to guide the Muslim people in their daily lives. Sharia Law is described as the way to follow God’s (Allah’s) Law (Wiechman et al., 1994).) is compatible with most of the recognised western basic principles of ethics (Editorial International Journal of Surgery, 2006), and the establishment of rules which take into

account social development within the ethical standards that are based on the Qur'an (Islam's Holy Book) and Sunna (the Prophet Mohammad's saying).

Many people are not aware of the potential impact of the value of the data stored on their digital devices and in digital repositories used in their daily lives (Dijk, 2012). Such repositories include computer labs, facilities within utility companies and communication systems and networks that have the capability of operating automatically based on technical functions. Furthermore, surveillance cameras, closed-circuit television, security systems, automobiles and online activities like e-mail, ecommerce payment systems and social network sites also collect data, which may prove useful in forensic investigations (Dijk, 2012). However, ICT users generally only have a basic, and sometimes incorrect, understanding of how these ICTs work (Kessler, 2010). Hence, applying critical analysis techniques to reports based on digital evidence may be a difficult task when the statement is submitted in a courtroom (Placid and Wynekoop, 2011, 2004; Mason, 2008; Baca et al, 2014).

Digital forensics has recently become common in the investigation of a wide range of crimes as law enforcement agencies recognise that the vast majority of people not only use computer systems but also have access to a variety of digital devices and these can be used as a medium in criminal activities. Computer forensics investigators are likely to focus on specific methods for specific platforms to collect evidence. For this reason, digital forensics must be designed to cover all types of present and future digital devices/technologies. According to (Čisar* and Čisar, 2011), there exist a chain of tools and procedures, which are based mainly on law enforcement requirements, system administrator's requirements and hacker experiences, but there is no standardised procedure to perform a digital forensic investigation, because after the review the digital

forensics guidelines , the researcher notes that there are ACPO guidelines for UK and NIJ guidelines for US. (Even though ACPO is used not in the UK, but only in England, Wales and N.Ireland. It's not a Standard. It's a good practice guideline for digital forensic investigation in the UK.) ISO only has a standard for testing and calibrating labs (ISO 17025), it does not have a standard procedure for digital forensic investigation This makes the investigation process challenging before and during the trial process because evidence should be collected using proven methods to maintain evidence integrity (Čisar* and Čisar, 2011).

2.2 Review of Current Research Methods in the Investigation Process

This chapter examines existing models of digital investigation, which have been used over the last few years. These models are not comprehensive in that they cannot deal with cases where there is an absence of evidence.

Between 1984 and 2013, academics and law enforcement agencies including the FBI developed models to preserve, collect, examine/observe and present computer evidence (Yusoff et al, 2011). Therefore, the procedure adopted in investigations would be applicable to any scenarios, and also applicable in a digital investigation which does not have sufficient evidence. Therefore, digital investigations should follow an accepted investigative procedure to generate conclusive results.

This chapter will present the main digital investigation models developed and used from 1984 to 2013. The proposed model, which can also deal with incomplete evidence, will also be discussed in the research evaluation and contribution chapter.

2.2.1 Computer Forensic Investigation Process

Pollitt (1984) proposed an approach/model to deal with digital evidence in investigations, which comprises four phases:

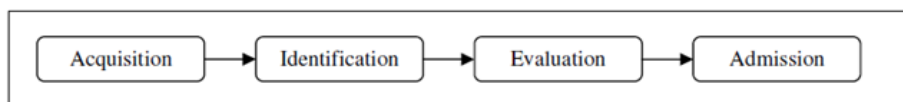


Figure 1 Computer forensic Investigation Process

The Acquisition phase ensures that the evidence is acquired by the authorities in an admissible manner. The Identification phase identifies the digital components and converts them to a format understood by human, which makes the information recognisable. The Evaluation phase determines which components are pertinent to the case and can be reflected as authentic evidence. In the Admission phase, the evidence that was acquired is presented in court (Yusoff et al, 2011), (Solinas, 2014), (Lutui, 2015).

2.2.2 Scientific Crime Scene Investigation Model

A model proposed by Lee et al. (2001) consisted of four (4) stages: recognition, identification, individualisation and reconstruction (Yusoff et al, 2011). This model does not deal with the full investigation process, but deals only with the crime scene investigation (Cosic et al, 2011). These steps fall within the investigation process as described on other methods; however there is no a 'preparation' nor a 'presentation' phase (Perumal, 2009).

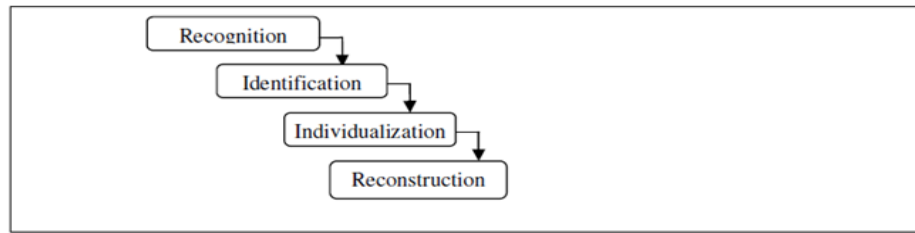


Figure 2 Scientific Crime Scene Investigation Model

Figure 2 shows the Lee Scientific Crime Scene Investigation Model that focuses on a systematic and methodological approach to investigating a digital crime case. “The major limitation of this model is that it refers only to the forensic part of an investigation and issues such as the exchange of information with other investigators are not addressed” (Ciardhuái, 2004: pp 2).

The first phase of the Scientific Crime Scene Investigation Model is Recognition, where patterns or items are seen to be potential evidence. This leads to documentation, collection and preservation. This phase is immediately followed by the Identification phase, which includes the task of classification of the evidence and comparison. The next phase is the Individualisation phase involving the determination of unique evidence that might be relevant to the case, which must be evaluated and interpreted. The final phase is the Reconstruction phase, which leads to presentation and reporting. This involves collecting the outputs of the process and the relevant data, which the investigator has obtained to provide details about the case at the crime scene (Ciardhuái, 2004).

2.2.3 Digital Forensic Research Workshop Model (DFRWS)

The Digital Forensic Research Workshop model (2001) comprises six phases which can be widely employed to the investigations (Kilungu, 2015). This model wasn’t proposed

as a final inclusive version, but to serves as a base for future work toward the creation if a full digital investigation process model (Kilungu, 2015).

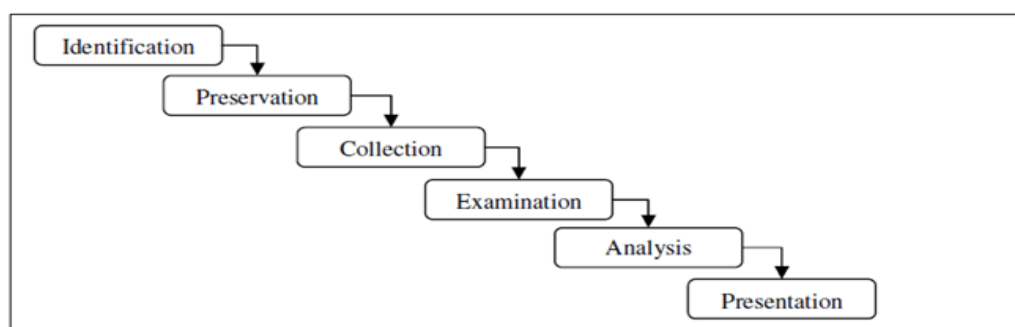


Figure 3 Digital Forensic Research Workshop Model (DFRWS)

The DFRWS investigation model starts with the Identification phase, which comprises system monitoring, profile detection, audit analysis, etc. The next phase is the Preservation phase, which ensures an acceptable chain of custody, as well as the data being free from contamination. This phase/stage is immediately followed by the Collection phase/stage, which incorporates the task of collecting relevant data, based on various recovery techniques and approved methods. The next phases are the Examination phase and the Analysis phase, which include evidence validation, evidence tracing, recovery of data mining, hidden/encrypted data, etc. The last phase is the Presentation phase, which involves documentation, expert testimony, etc (Yusoff et al, 2011).

2.2.4 Abstract Digital Forensic Model (ADFM)

Reith, Carr and Gunsch (2002) proposed a standardised Abstract Digital Forensic Model (ADFM) inspired by the DFRWS, which is applicable to any type of cybercrime. The authors introduced three additional phases to the DFRWS, which are Preparation, Approach Strategy and Returning Evidence (Yusoff et al, 2011), (Kim, 2015). This model has nine phases.

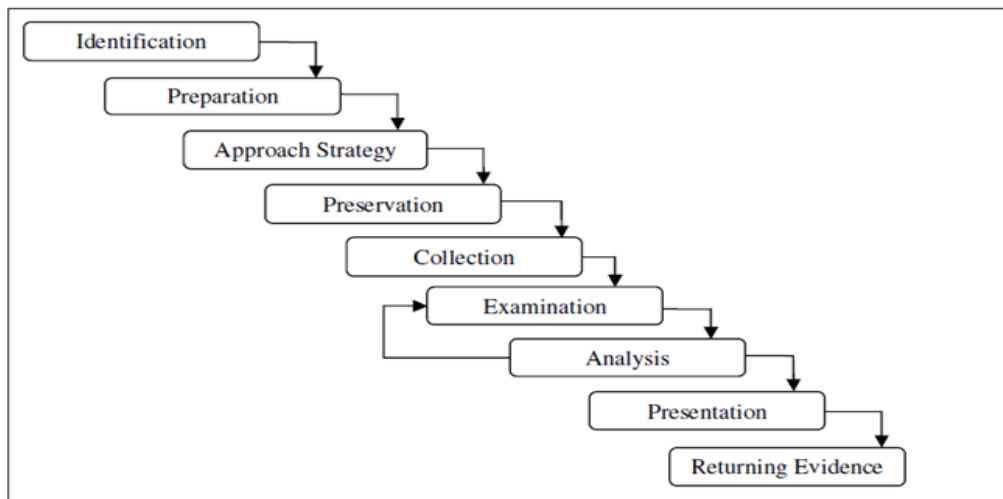


Figure 4 Abstract Digital Forensic Model (ADFM)

The first phase in the ADFM is the Identification phase, which determines and identifies which type of incident has taken place. The next phase is the Preparation phase, which includes the preparation of tools and identifies and determines techniques, monitoring authorisations, obtaining search warrants and gaining management support. This phase is followed by the Approach Strategy phase, which ensures the collection of untainted evidence to minimise or avoid any negative impact. There is a need to secure and preserve physical and digital data, which should be properly isolated. The Preservation phase performs all of these tasks. Next is the Collection phase where data is extracted and duplicated. This phase is followed by the Examination phase to determine and identify the potential evidence relating to the case from the collected data. The next phase, Analysis, determines evidence and draws conclusions according to the evidence found. The findings are summarised and an explanation of the conclusions is given in the Presentation phase. In the Returning Evidence phase the physical and digital possessions is given back to its owner. This phase completes the investigation process (Yusoff et al, 2011), (Agarwal and Kothari, 2015), (Kim, 2015).

2.2.5 Integrated Digital Investigation Process (IDIP)

Carrier and Spafford (2003) proposed a model which combines and integrates the various available investigative processes into one model. This model is called the Integrated Digital Investigation Process Model (IDIP) and has seventeen phases organised into five groups: Readiness, Deployment, Physical Crime Scene Investigation, Digital Crime Scene Investigation and Review, in which hardware and software is used to create the notion of digital crime scene as mentioned in the virtual environment (Agarwal et al, 2011), (Yusoff et al, 2011), (Kim, 2015), (Lutui, 2016).

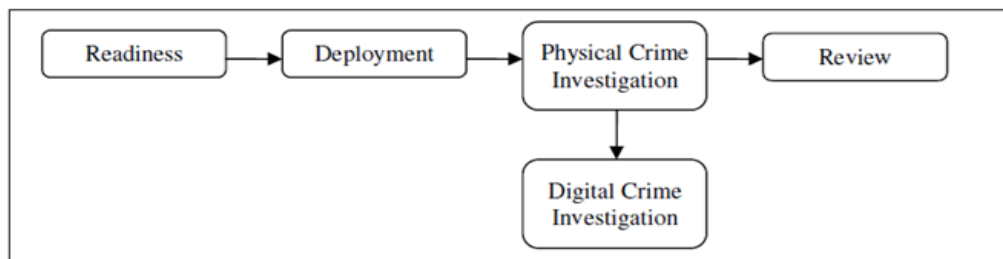


Figure 5 Integrated Digital Investigation Process (IDIP)

In IDIP, the first phase is the Readiness phase, which involves ensuring that the physical and operational infrastructure, the equipment and the personnel are prepared to support any future investigation. This phase comprises two sub-phases: Operation Readiness, which involves providing the required personnel training, and equipment; and Infrastructure Readiness, which involve that data should be existed for carrying out a full investigation. The next phase, the Deployment phase, seeks to provide a technique for detecting and confirming an incident. This phase comprises two sub-phases: Detection and Notification where the appropriate people are informed that an incident has been detected and Confirmation and Authorisation where the incident is confirmed in order to get legal authorisation to obtain a search warrant. This phase is immediately followed by

the Physical Crime Scene Investigation phase, involves the collecting and analysing of physical evidence. This phase comprises two sub-phases: Preservation, which involves the crime scene preservation to enable the collection and identification of digital evidence by trained personnel and Survey, which involves the identification of physical evidence by an investigator, who walks through the physical crime scene. The Documentation phase involves the capturing of as much relevant information as possible to record and preserve important details. The Search and Collection phase, involves search of the scene deeply and collection of data so that additional physical evidence is identified. The Reconstruction phase involves the organisation of the analysis results for developing a theory for the incident and the Presentation phase presents digital and physical evidence in court. The Digital Crime Scene Investigation phase focuses on the digital evidence in a digital environment similar to a Physical Crime Scene Investigation. This phase has two sub-phases, namely the Preservation phase, which involves the preservation of the digital crime scene for future evidence and the Survey phase where the relevant data is transferred by the investigator from a physical place to a controlled location. The Documentation phase includes documenting the digital evidence and the Search and Collection phase involves an in-depth analysis of the digital evidence. The final phase is the Review phase, which involves reviewing the whole investigation process (Yusoff et al, 2011), (Agarwal et al, 2011), (Chandrakumar et al, 2014), (Joshi, Pilli, 2016).

2.2.6 Enhanced Digital Investigation Process Model (EDIP)

Baryamueeba and Tushabe (2004) proposed The Enhanced Digital Investigation Process Model (EDIP) that modifies the Integrated Digital Investigation Model, which was proposed by Carrier and Spafford (2003). This model seeks to separate the digital crime scene and the physical crime scene into two phases, namely Traceback and Dynamite, to

avoid inconsistencies (Agarwal and Kothari, 2015). This model comprises five phases which are; Readiness, Deployment, Traceback, Dynamite and Review as shown in the below.

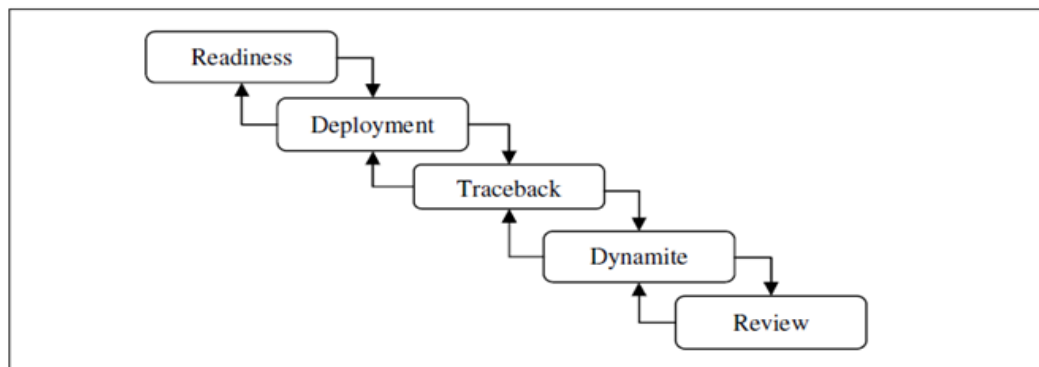


Figure 6 Enhanced Digital Investigation Process Model (EDIP)

In the Readiness phase the series of tasks performed here are the same as those described in the same phase in the IDIP. The Next phase is the Deployment phase, which involves providing technique(s) to detect and confirm an incident. This phase comprises five sub-phases, unlike the IDIP Model. It includes both physical crime scene investigations and digital crime scene investigations and the presentation of findings to legal enforcement entities as in the Detection and Notification phase, which involve detecting the incident and informing the appropriate people. The Physical Crime Scene Investigation phase involves carrying out a physical examination of the scene and identifying probable digital evidence. The Digital Crime Scene Investigation phase involves an examination of the digital scene to obtain digital evidence with probably an evaluation of the extent of the impact or damage. The Confirmation and Authorisation phase involves obtaining authorisation to obtain a search warrant if necessary and carry out investigations. The Submission phase includes presentation of the physical and digital evidence to corporate management or legal entities. This phase is followed by the

Traceback phase, which involves tracking down the crime scene, which contains the devices that were used to carry out the act. This phase comprises two sub-phases, namely the Digital Crime Scene Investigation phase, in which tasks are performed and traced back to the primary crime scene in accordance with presumptions obtained from the preceding phase and the authorisation phase, which involves tasks allowing for further investigation and access to information when permission is received from relevant legal bodies. Following the Traceback phase is the Dynamite phase. In this phase, the primary crime scene is investigated with the aims to identify the potential culprits and to obtain further evidence through the items found at the primary crime scene. This phase consists of four sub-phases, namely the Physical Crime Scene Investigation phase, which involves tasks to recognise potential digital evidence at the physical examination of the scene; the Digital Crime Scene Investigation Phase “*when an electronic examination of the scene is performed to obtain digital evidence of the incident and possibly an estimation of the time and dates when the incident was launched*” (Baryamureeba, V & Tushabe, 2004) ; the Reconstruction phase, which involves identifying the most likely investigative hypotheses by putting the pieces of the digital puzzle together (Hanaei and Rashid, 2014) and the Communication phase where the conclusions and interpretations about the physical and digital evidence are presented to corporate management or to the court. The final phase of the EDIP is the Review phase where the investigative processes are reviewed and areas for possible improvement are identified (Baryamureeba, V & Tushabe, 2004), (Yusoff et al, 2011), (Chandrakumar et al, 2014), (Hanaei and Rashid, 2014).

2.2.7 Extended Model of Cybercrime Investigation

Ciardhuáin (2004) proposed the Extended Model of Cyber Crime Investigation, which can support digital investigation processes to develop the techniques and tools of digital forensics by providing a common reference framework. It also supports investigator training and conformance testing and provides learned materials and best practice data for investigations (Cosic et al, 2011).

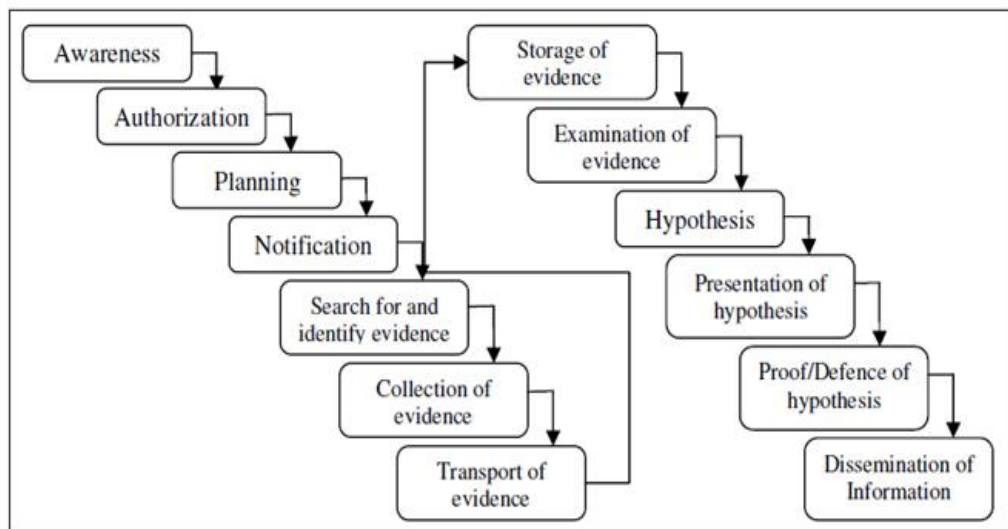


Figure 7 Extended Model of Cybercrime Investigation

The first phase of the Extended Model of Cyber Crime Investigation model is the Awareness phase, which involves creating an awareness regarding the type of investigation needed. This clarifies awareness of those incidents needing investigation (Malik et al, 2014). The Authorisation phase involves authorising the investigation after identifying the need for one. The next phase is the Planning phase, which is impacted by the information that is provided from both inside the investigation organisation (through its polices, strategies and information about previous investigations) and the outside (information collected from external sources by the investigator and the general context of the investigation). The notification phase involves notifying the topic of an

investigation or other involved organisations about the undergoing investigation. The next phase is the Search and Identification of Evidence phase where the exact location of the evidence is determined. This is followed by the Collection phase, which involves the data that can be preserved and analysed as evidence. This phase is followed by the Transport phase, which involves transporting the relevant items to a secure location. In the Storage phase the evidence is stored under appropriate conditions. The Examination phase uses a set of techniques for finding and interpreting significant data. The Hypothesis phase involves constructing a hypothesis of what occurred. In the Presentation phase, the assumptions essentially need to be shown to persons other than the investigators. For a proper police investigation; these assumption will be placed before adjudicators, while an internal company investigation will make a decision on the procedures to be taken. This is followed by the Proof/Defence phase, which involves constructing a contrary hypothesis to face any criticism and challenge to the evidence. The final phase/stage of this model is the Dissemination phase, which involves presenting the information from the investigation (Ciardhuáin, 2004), (Perumal, 2009), (Yusoff et al, 2011).

2.2.8 Computer Forensic Field Triage Process Model (CFFTPM)

Rogers et al. (2006) proposed a Computer Forensics Field Triage Process Model to Identify, examine and interpret digital evidence within a limited time frame without further need to take devices back to the lab. This model has six phases, which are then separated further into another six sub-phases (Roger et al, 2006).

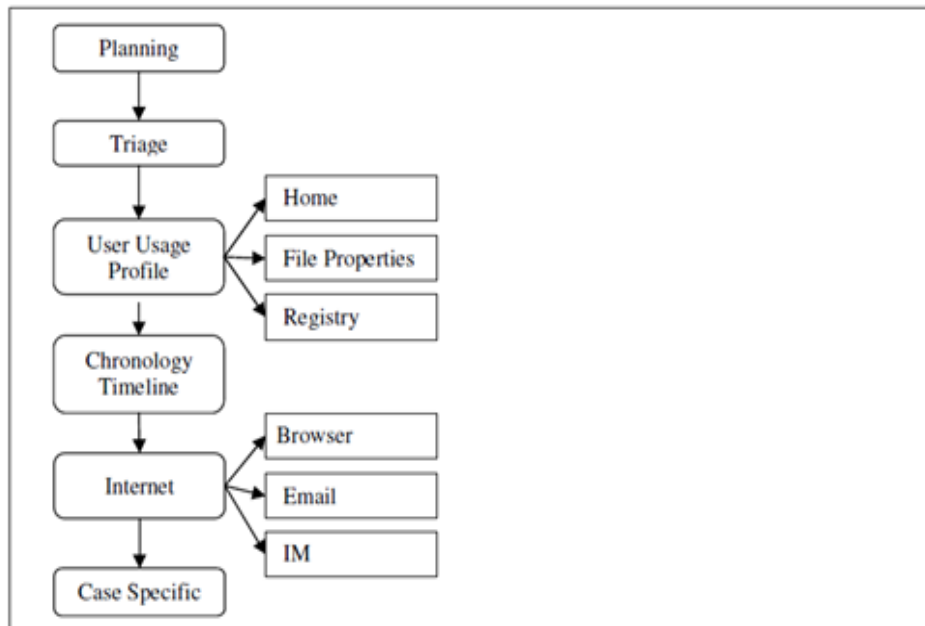


Figure 8 Computer Forensic Field Triage Process Model (CFFTPM)

The first phase of the CFFTPM model is the Planning phase, which involves identifying what needs to be known about the case to improve the rate of an investigation success. The next phase is the Triage phase, which involves ranking and classifying the evidence. The Usage Profile phase focuses on analysing suspect activity and profiling the user. Arrangement of the potential crime actions is the main aim of Chronology Timeline phase. The Internet Phase involves examining internet activity. This also comprises sub-phases, namely Browser Artefacts, E-mail Artefacts and Instant Messaging Artefacts (Quick and Choo, 2014). Lastly, in the Case Specific Evidence phase, focus on the examination of the case is adjusted by the investigator. The investigator should be capable of assessing time resources, determining and highlighting search aims (Roger et al, 2006), (Lutui, 2015), (Kim, 2015), (Rogers et al, 2016).

2.2.9 Framework for a Digital Forensic Investigation

Kohn, Eloff and Olivier (2006) proposed this model to obtain a complete framework as a result of merging existing frameworks. This model has three phases: “*Preparation, Investigation and Presentation*”, which group of gather the phases of previously proposed frameworks (Kim, 2015).

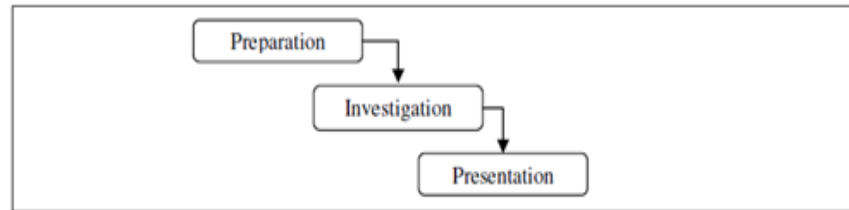


Figure 9 Framework for a Digital Forensic Investigation

The Preparation phase involves defining the criteria used in the organisation, rules and techniques to help in the investigation, training, legal consultation, notifying the correct specialists, documenting of previous cases and scheduling; also known as an ‘approach scheme (Kohn et al, 2006).

This is followed by the Investigation Phase, which involves searching for and identifying evidence on a device, gathering evidence from the device, and transporting it to a secured place. The evidence collected at the scene should be stored and examined using the proper tools (finding evidence which is related) and performing analysis to identify the value and importance of the evidence found. The final phase of this model is the Presentation phase, which involves presenting and proving the analysis (Kohn et al, 2006), (Yusoff et al, 2011), (Agarwal and Kothari, 2015).

2.2.10 Common Process Model for Incident and Computer Forensics (CPMICF)

Freiling (2007) proposed the CPMICF model to investigate computer security incidents. This model aimed to improve the process of investigation by linking the concepts of Incident Response and Computer Forensics (Freiling, 2007).

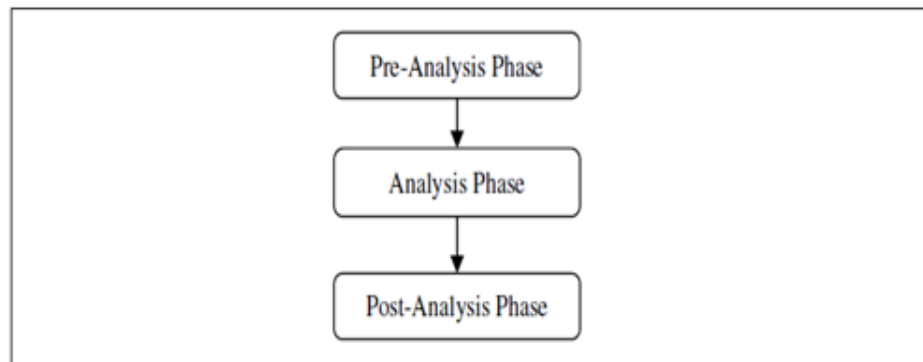


Figure 10 Common Process Model for Incident and Computer Forensics

The first phase of this model is the Pre-Analysis phase, which comprises all phases that have to occur before the actual analysis starts. This is followed by the Analysis phase and the Post-Analysis phase, which involves documenting all the activities which occurred during the investigation reporting stage (Freiling, 2007), (Yusoff et al, 2011), (Kim, 2015).

2.2.11 Digital Forensic Model Based on Malaysian Investigation Process (DFMMIP)

Perumal (2009) proposed the DFMMIP Model, which is based on Malaysian investigation processes. This model involve seven phases, which are “*Planning, Identification, Reconnaissance, Transport and Storage, Analysis, Proof and defence and Archive Storage*” (Kim, 2015).

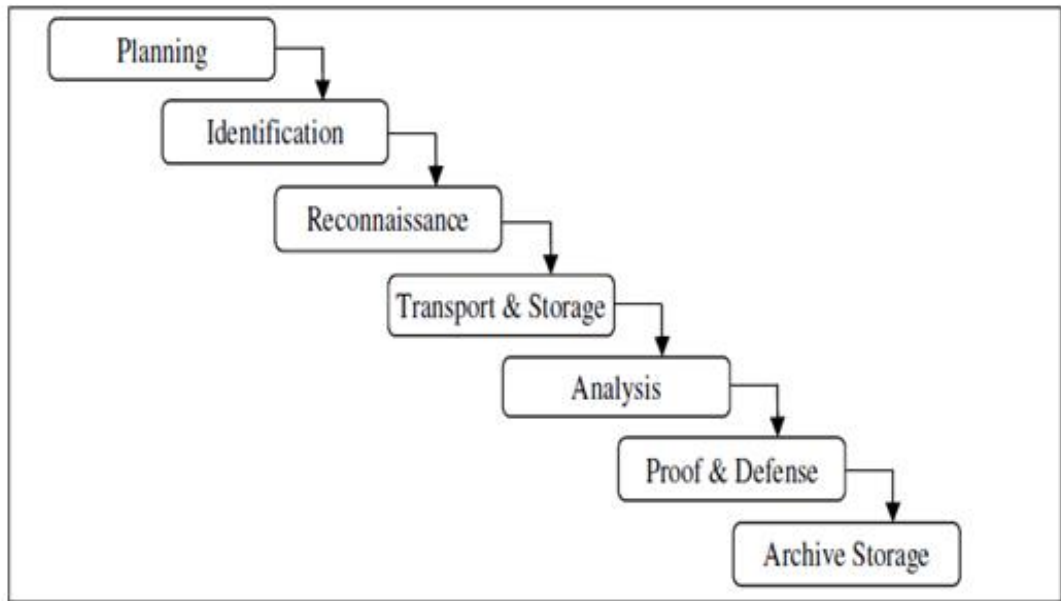


Figure 11 Digital Forensic Model based on Malaysian Investigation Process (DFMMIP)

The Planning phase consists of two sub-phases, which are Authorization and Obtaining Search Warrant. This is followed by the Identification phase, which involves identifying all of the suspect's electronic equipment which is of interest to the investigator.

This phase has two sub-phases, which are Identify Seized Items and Identify Fragile Evidence. The next phase is the Reconnaissance phase, which means performing live forensics, where the investigation is conducted when the devices are still running (Kerrigan, 2013). The following phase is the Transport and Storage phase, which involves securely transporting the evidence to the investigation site and storing it properly (Elers, 2014). The Analysis phase involves analysing and examining the data to obtain proof to support the case by using the appropriate techniques and tools. The Proof and Defence phase involves proof finding, gathering more evidence and creating the report. The final phase of this model is the Archive Storage phase where all evidence is stored for future reference (Perumal, 2009), (Agarwal and Kothari, 2015).

2.2.12 Network Forensic Generic Process Model (NFGP)

Pilli, Joshi and Niyogi (2010) proposed the NFGP model for network forensic analysis, which consists of nine phases, namely Preparation, Detection, Incident Response, Collection, Preservation, Examination, Analysis, Investigation and Presentation (Yusoff et al, 2011).

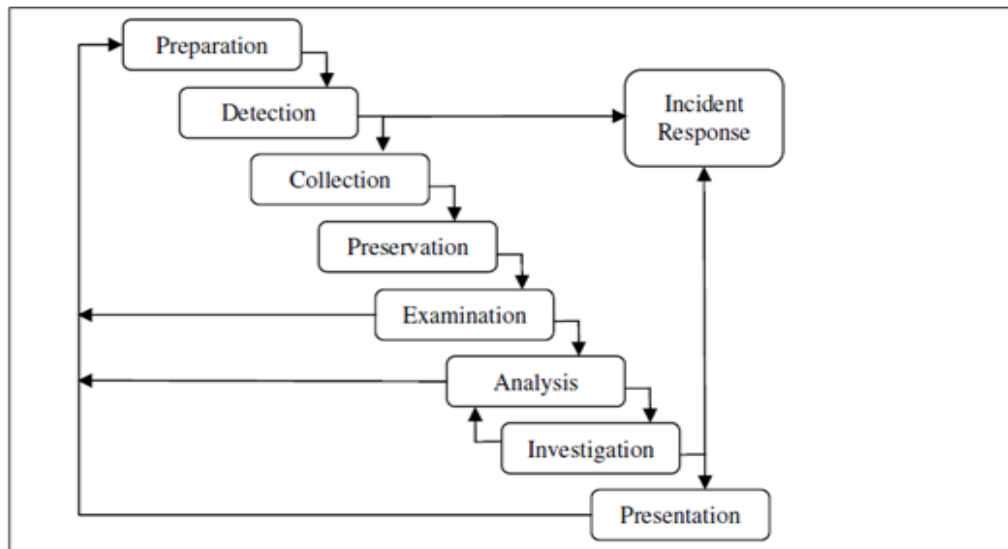


Figure 12 Network Forensic Generic Process Model

The Preparation phase involves gathering the authorisations and legal warrants to avoid any incidents of violating privacy. This is followed by the Detection phase where the nature of the attack is ascertained.

The Incident Response phase involves planning how to respond to certain types of attack and explaining how to defend from future attacks while taking decisions about whether to continue the investigation to collect more data. In the Collection phase the data is obtained from sensors used to gather traffic data. The Preservation phase ensures that the data is stored on a backup device to preserve the original data. The Examination phase examines the data methodically to search for evidence and extract specific indicators

related to the case. The Analysis phase involves linking and classifying indicators to inference important clarifications via existing attack patterns. The Investigation phase identifies the route from a victim system or network through any communication pathways and middle systems and provides information about incident response and attackers prosecution. The final phase is the Presentation phase, which involves presenting the conclusions of the network analysis (Pilli et al, 2010).

2.2.13 Generic Computer Forensic Investigation Model (GCFIM)

Yusoff, Ismail and Hassan (2011) proposed the GCFIM Model, comprising five phases namely “*Pre-Process, Acquisition and Preservation, Analysis, Presentation and Post-Process*”.

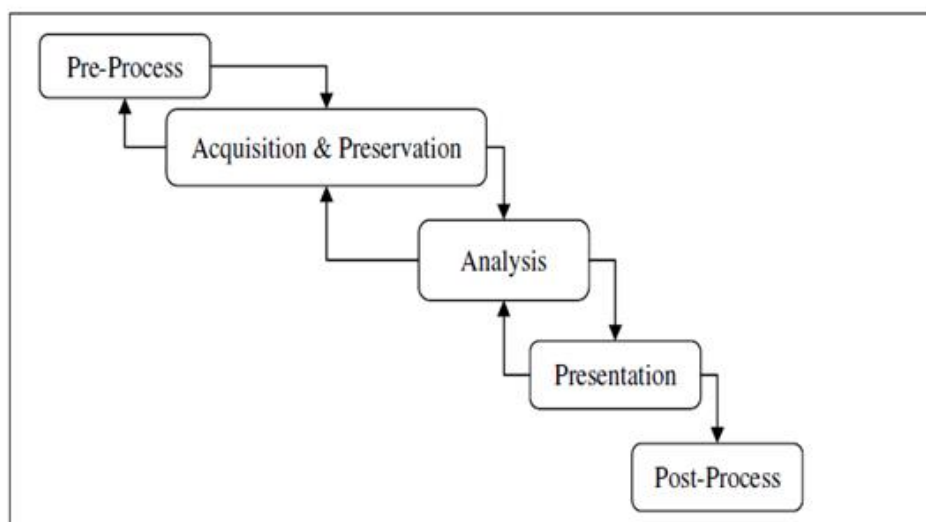


Figure 13 Generic Computer Forensic Investigation Model

The Pre-Process phase comprises all tasks that need to be done before the investigation and start of the collecting a data. The following phase is the Acquisition and Preservation phase where data is collected, stored and made available for the following phase. This phase also comprises tasks related to the “*the identifying, acquiring, collecting, transporting, storing and preserving of data*”. The Analysis phase, analyses

the data for identifying the source and the person responsible for the crime. The next phase is the Presentation phase, which involves documenting and presenting the resulting from the Analysis phase to the authorities. Finally, the Post-Process phase involves appropriate closure of the investigation. Physical and digital evidence should be give back to the owner, or if necessary kept in safe place (Yusoff et al, 2011), (Lutui, 2015).

2.2.14 A new triage model conforming to the needs of selective search and seizure of electronic evidence

The triage model proposed by Hong, Yu, Lee and Lee (2013) may be able to meet the demands of different legal systems for protection of privacy and supports decision making by field officers, who provide information on the level of resources of law enforcement agents; such as the available laboratory or equipment supply, time constraints and technical limitations.

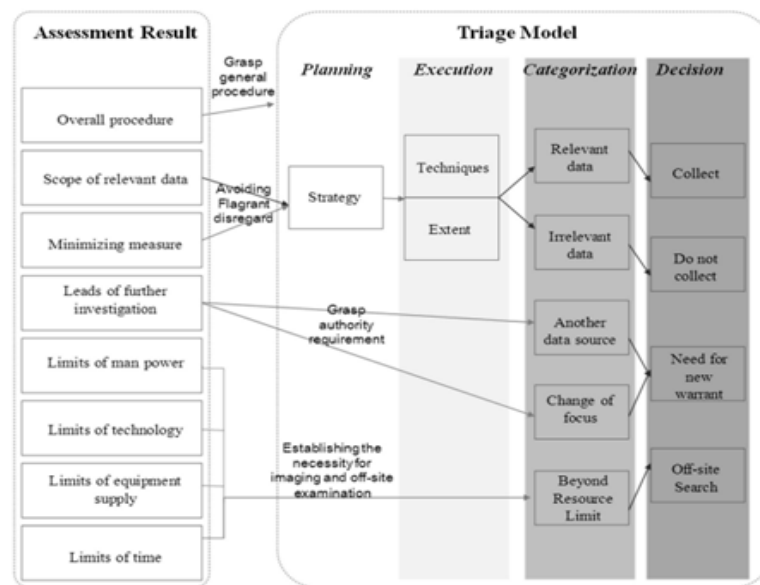


Figure 14 A new Triage Model Conforming to the Needs of Selective search and seizure of electronic Evidence

2.3 Discussion

In this review, the researcher has arranged the digital investigation models in chronological order to identify phases shared throughout all of the models. Afterwards, all the phases were extracted and arranged so that similar tasks were grouped together with unique identifiers according to each of the digital investigation processes as shown in the table 1 (Yusoff et al, 2011). It was found that in many cases, the phases overlap each other, and in some cases are even duplicated. Certainly, the multitude of digital forensics models proposed by the authors reveals the complexity of the digital forensics processes and did not identify any investigation process that addresses the issue of insufficient evidence.

Table 1 comparison of digital investigation phases

Name of phase	Found in														
	CFIP	SCSIM	DFRWS	ADFM	IDIP	EEDI	EDIP	EMCI	CFFTPM	FDPI	CPMICF	DFMMIP	NFGP	GCFIM	NTM
Acquisition	✓													✓	
Admission	✓														
Analysis			✓	✓		✓					✓	✓	✓	✓	
Approach Strategy				✓											
Archive Storage												✓			
Authorization								✓							
Awareness								✓							
Case Specific Analysis									✓						
Chronology Timeline Analysis									✓						
Collection			✓	✓		✓		✓					✓		
Deployment					✓		✓								
Detection													✓		
Digital Crime Investigation					✓										
Dissemination of Information								✓							
Dynamite							✓								
Evaluation	✓														
Examination			✓	✓		✓		✓					✓		
Hypothesis creation								✓							
Identification	✓	✓	✓	✓		✓						✓			
Incident Response													✓		
Individualization		✓													

Internet Investigation									✓						
Investigation										✓			✓		
Notification								✓							
Physical Crime Investigation					✓										
Planning								✓	✓				✓		
Post-Analysis												✓			
Post-Process														✓	
Pre-Analysis												✓			
Pre-Process														✓	
Preparation					✓						✓			✓	
Presentation			✓	✓		✓		✓		✓			✓	✓	
Preservation			✓	✓		✓							✓	✓	
Proof & Defense								✓					✓		
Readiness					✓		✓								
Recognition		✓													
Reconnaissance													✓		
Reconstruction		✓													
Returning Evidence					✓										
Review					✓		✓								
Search & Identify								✓							
Traceback							✓								
Transport & Storage								✓							
Triage									✓						
User Usage Profile Investigation									✓						

As there have been various models which already identified by other researchers in digital forensics investigation, however they largely did not cover all the aspects of digital investigation. One of the main aspects, which have not been covered in these models, is how to deal with cases where there is insufficient evidence as shown below:

The original computer forensics investigation process model was proposed by Pollitt, and consisted of four phases: acquisition, identification, evaluation, and admission. The author stated that the processes used should conform to both science and the law. Thus, the computer forensic process in this methodology was mapped to guarantee the admissibility of evidence in a court of law.

Whereas, Lee proposed the scientific crime scene investigation model encompassed in four phases: recognition, identification, individualisation, and reconstruction. These phases fall within the investigation process phases; however, there is no 'preparation' or 'presentation' phase.

Furthermore, the framework development has been based on the following phases: identification, preservation, collection, examination, analysis, and presentation, as specified by DFRWS, as of value to the majority of digital investigations. Their model highlighted two important phases: investigation and presentation.

The abstract digital forensic model was proposed by Reith, Carr and Gunsch, and consists of a number of phases: identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation, and returning evidence, which are not referred to in the above models. This methodological process can provide a framework that can be applied to categorise specified incidents. However, the third phase of this framework is likely to be the same as the second phase.

On one hand, Carrier and Spafford (2003) proposed IDIP, which depends on the source and effects of the events. Hence, it eventually builds a mechanism for faster investigations.

On the other hand, Baryamereeba and Tushube (2004) proposed EDLP essentially to recreate two crime scenes at the same time to form a primary crime scene (devices), and a secondary crime scene (the physical crime scene) to deflect conflicts arising.

Also, the framework proposed by Ciardhuáin (2004) supported investigators' work by providing a foundation for the development of tools and techniques.

Moreover, the framework proposed by Beeb and Clark (2004) was multi-tiered. This framework conquered the problems which arose in Carrier and Spafford's framework by emphasising specificity and practicality. Hence, the framework was rendered more usable and flexible, in the form of a hierarchical structure, which enabled the framework to impact on investigation phases.

In 2007, Freiling proposed the common process model for incident and computer forensics. The aim of this model was to improve the investigation process by combining the two concepts: computer forensics and incident response. This model focused on the analysis phase, consisting of a pre-analysis, analysis and post-analysis. Moreover, it offered a method to perform analytical incident response, while applying principles known as computer forensics, merged with forensic analysis in the incident response framework

. Perumal proposed the DFMMIP. This model did not focus on all aspects of an investigation; hence, it is not adequate for use in a cybercrime investigation.

Still, The Generic Computer Forensic Investigation Model was proposed in 2011. The authors established the model after studying other investigative models. Hence, this model is characterised by its ability to return to any previous phase of an investigation to seek out fresh information or review evidence.

Finally, the triage model proposed by Hong, Yu, Lee and Lee (2013) may be able to meet the demands of different legal systems for protection of privacy and supports decision making by field officers.

The previous section presented the most commonly published digital investigation models, however there is still a requirement for a model to handle cases where there is insufficient forms of non-digital evidence.

In conclusion, the models presented aim to address a range of the issues related to digital investigations and have been developed over a considerable period. What is clear is that in the current environment of mobile computing, cloud computing and an increasing range of digital devices (the Internet of Things), there is a requirement for the continued development of models to meet the developing needs.

In summary, the researcher reviewed a number of models and frameworks which have been developed since 1984 to support the digital investigation processes. Digital forensics seeks to achieve the successful investigation of digital crimes through obtaining acceptable evidence from digital devices that can be presented in a court of law. Thus, digital forensics investigation is normally performed through a number of phases, in order to achieve the required level of accuracy in the investigation process.

Therefore, the researcher has investigated the models above. For instance, the abstract digital forensic model and the original computer forensics investigation process model

have common activities and processes in their models. The Computer Forensics Field Triage Process Model and Integrated Digital Investigation Process emphasised constructing a mechanism for reaching to quicker forensics examinations, a Hierarchical, Objective-Based Framework for the Digital Investigation has an emphasis on the process of analysis in order to get the evidence and improve the investigation process. Consequently, these models have their own strengths; nevertheless until now there is no single model could be used for investigating in all cases as a general guideline.

From the existing models mentioned in section 2, each of proposed models was built on the experience of the previous; some of them have similar approaches and in some of them the emphasis is on different areas. Consequently, the researcher has found that there is a need to design a framework to handle the case where there is insufficient evidence, which is not currently addressed.

Therefore, this section answered some sub questions of the research question, which are:

- What is the definition of Digital Forensics?
- What are the research models of digital investigation processes available?

However, during the developing the literature review, the researcher found that the investigation processes with insufficient evidence were not addressed by previous authors in this field, as far as the researcher knows.

In the next section the researcher will present the investigation of digital crimes from an Islamic view; with evidence from the Qur'an and Hadith (Sunna) that has shown the principles which are followed by Muslims. It will also outline the application of digital

forensics in Saudi Arabia that have been applied based on Sharia Law and highlight some of the issues regarding the collection of evidence.

2.4 Legislation in Saudi Arabia

These days, digital crime is one of main challenges for law enforcement. Many of the laws which are used to protect the users of current technologies in countries that adopt Sharia law were derived from legislation and laws that are utilized in the control of crimes that are based in the physical realm. There is a need to establish specific legislation to deal with digital crimes that is compatible with Sharia Law, which affects more than one billion Muslims. This section presents a view of digital crime in Islam by providing the principles from the Qur'an and the Hadith, which is the sayings and deeds of the Prophet Mohammad, which are the foundation of Sharia Law and respected by all Muslims. Sharia Law is the basic of Saudi law, therefore, in Criminal offenses, Saudi Arabia applies its laws to all Muslim groups and also non-Muslims who commit crime in Saudi Arabia. Saudi law does not look at the doctrine of the person, but rather looks at an offense based on the law that is followed by the government to achieving justice and equality between individuals. However, Saudi Arabia takes into account the different religious sects, and there are many courts available to accommodate the different groups of Muslims that follow their differing beliefs. These courts address religious differences and are for solving the issues that are faced by them, for examples there is a court in al Qatif city for the Shia sect to solve personal issues and everything related to doctrinal beliefs such as fasting issues, social issues or praying issues. In addition, Sharia law guarantees to non-Muslims their human rights, as long as they live under the umbrella of Islamic rule, as the Prophet Muhammed said: "Beware! Whoever is cruel and hard on a non-Muslim

minority, curtails their rights, burdens them with more than they can bear, or takes anything from them against their free will; I (Prophet Muhammad) will complain against the person on the Day of Judgment." (Al Hwaimel, 2009).

Forensic science emerged in response to a need to uncover the facts behind inappropriate, illegal and criminal activities. The role of forensics can be represented using forensics models, techniques and methodologies and by following the commonly accepted stages of an investigation; i.e. preservation, collection, analysis and presentation of evidence to the courts. The digital forensics process follows the same stages of investigation as traditional forensics. Sharia Law is compatible with most of the recognised western basic principles of ethics (Editorial International Journal of Surgery, 2006). This section looks at the inclusion of Sharia Law in all people's activities through the establishment of rules which take into account social development within the ethical standards that are based on the Qur'an (Islam's Holy Book) and Hadith (the Prophet Mohammad's saying and deeds).

2.5 Sharia Law

Sharia Law arose with the coming of the Prophet Mohammad in the seventh century, which gave rise to the birth of Islam. Sharia Law is the common Law within the Islamic religion to guide the Muslim people in their daily lives. Sharia Law is described as the way to follow God's (Allah's) Law (Wiechman et al., 1994). As a result, Islam is considered to be not just a religion, but a path to life, because it provides guidance and instructions for Muslims' daily activities (Editorial, International Journal of Surgery, 2006); where the Prophet Mohammed said, "I was sent to complete the epitomes of Ethics" (AbdelBaky, 1951).

Sharia Law can deal with serious crimes because the punishments have been fixed for those crimes. In Sharia Law there are a number of crimes which are against God (Allah) such as murder, robbery, apostasy (the abandonment or renunciation of a religious or political belief or principle) and the consumption of intoxicants. There are three major crime groups under Sharia Law: 'Had' Crimes that are serious crimes such as Murder; Apostasy from Islam, making war upon Allah and his messengers; Fornication; Theft; Defamation, False accusation of adultery. The punishment of these crimes are pre-established in the Qur'an, which does not allow the judge to reduce or change the punishment of these crimes because they were set by God and found in the Qur'an. Sharia Law considers the higher level of proof and the reasons which led the person to commit the crime; this can be through confessing to the crime or through sufficient witnesses to the crime. When there is no confession, not enough witnesses or doubt about the guiltiness; Sharia Law will punish these crimes as a 'Tazir' crime. 'Tazir' Crimes are less serious than 'Had' crimes. 'Tazir' crimes are the acts that are considered to cause harm to the societal interest and it's punishment of these crimes are not pre-established in the Qur'an as are 'Had' crimes. Sharia Law seeks to work in the societal interest and prevent such crimes from being committed. 'Tazir' punishments vary according to the seriousness of the crime. In this area, Sharia Law is flexible, where the judge, through Sharia Law in a 'Tazir' crime, is free to set the punishment based on many factors such as customs and local norms, in order to deter and rehabilitate the offenders. The common punishments for 'Tazir' crimes are: fines, seizure of property, flogging and imprisonment (Madkoar, 1980). In 'Qisas' Crimes, which are typically revenge crimes, the penalty may include restitution. The punishments for these crimes are set in the Qur'an, where 'Qisas' punishments have many forms including 'Diya', which is the monetary payment of

damages to the victim. For example, if somebody is killed; his family has the right to ask for 'Qisas' punishment for the offender or to ask for 'Diya'. Any victim of a crime has the right to seek retribution, as Allah said in Qur'an "We prescribed to them in it that life is for life, and an eye for eye, and a nose for nose, and an ear for ear, and a tooth for tooth, and for wounds, retaliation" (Al-Maeda Verse No:45) (Madkoar, 1980) (Abbas, 2009).

However, Muslims are encouraged to give forgiveness and to seek reward from Allah; as the Prophet Mohammed said "whoever suffers an injury and forgives (the person responsible), God will raise his status to a higher degree and remove one of his sins" (Hadith Tirmidhi) (Ariane, 2013). Sharia Law provides punishment that is both of this world and in the hereafter to protect the five absolute necessities in Islam, which are: Religion, Life, Intellect, Offspring and Property; through moral education that seeks to awaken religious consciousness and human awareness; moreover through inflicting a deterrent punishment according to the type of crime that is committed (Madkoar, 1980). The digital world has created new methods of committing crime, where the crimes related to the digital world are continuing to grow significantly with the development of technology and this is seen in the growing concerns over the threat of digital crime. To date, there has been a lack of understanding of offenders' behaviour and some of the issues that are related to both religious and social upbringing. There are experts in a number of fields in law in western nations that have participated in assessments and contributed to the modification of the existing laws in their respective countries to ensure that they are suited to, and updated with digital crimes, for example in 1990, the UK government introduced the Computer Misuse Act. From the Islamic point of view, digital crimes are not a new type of crime but a new method of committing existing crimes (Alfaifi, 2001). There are many examples from both the Qur'an and Hadith to show that

no crime is acceptable in Islam whether it is a traditional crime or a digital crime. For example, the Qur'an even gives the proper etiquette for visiting one another. According to the Qur'an, Allah Said "O you who have believed! Do not enter houses other than your own houses until you ascertain welcome and greet their inhabitants. That is best for you; perhaps you will be reminded [i.e., advised]." [Qur'an, 24:27] (Islamweb, 2009). Therefore, the Islamic principles ask Muslims to gain permission before they access the properties of another, which is the Islamic approach to protecting the rights of privacy. Based on this principle, a person must not gain access to digital devices (physically or logically) which are not his own or have a look at their contents without permission.

In another example from the Qur'an, Allah said: "O believers! Avoid immoderate suspicion, for in some cases suspicion is a sin, do not spy on one another" (Al-Hujurat, 12) (Malik, 2001). This Islamic principle urges individuals not to spy on the secrets of others, which can logically be extended to include those contained in digital devices.

Furthermore, in another quote from the Qur'an, Allah said: "Male or female, whoever is guilty of theft, cut off the hand (that was used in theft) of either of them as a punishment for their crime. This is an exemplary punishment ordained by Allah. Allah is Mighty, Wise." (Al-Maaeda, 38). This is evidence of the prohibition of theft. Therefore, any access to other persons properties without permission or illegally is considered as theft. In the digital world, one of the problems that is faced is that the technology has created the problem of facilitating crimes that have none of the conventional boundaries. As a result, Muslims lean towards following the Islamic teachings which have instilled the fear of God (Allah) in all Muslim's daily transactions.

2.6 Digital Forensics in Saudi Arabia

Legislators in Saudi Arabia have realised that traditional procedural rules are not applicable to cybercrimes, and have introduced new procedural rules that are better adapted to electronic communications (Atalla, 2010).

There are policies and procedures in Saudi Arabia related to computer incident response, but these do not include preparation procedures for computer forensics. Moreover, these principles do not consider the prerequisite of Islamic law for acceptable proof at an authoritative level in Saudi Arabia. However, this may in turn result in digital forensic investigations breaking the Saudi law which is derived from the Islamic sharia law when they follow global digital forensics principles. This fact is not one unique to Saudi Arabian law and one such example is the response to the UK Computer misuse act; when the evidence is compelling, some defence lawyers have been known to try to attack the credibility of the examiner who carried out this act. In addition, another issue “as identified by section 7 of a report by House of Commons Science and Technology Committee is that 'section 8 of the Contempt of Court Act 1981 and the related common law assures the confidentiality of a jury's deliberations and precludes research into these deliberations” (BCS, 2006). In Saudi Arabia, this may cause problems if a representative of one of the parties sues an Islamic court on the grounds that the law of Saudi Arabia follows Islamic (Al Sharia) law. Because Legislation must be in conformity with the Shari’ah and in harmony with the general principles and spirit of Islam. While, the English law based on the Liberal democracy with a sovereign Parliament that may pass any laws it pleases. And the ways of demonstrating proof in an Islamic court are not limited, but are subject to adjustment in order to show the truth and prove the case. Therefore, ways in which proof is provided are not limited and any way of showing the

truth and revealing reality will be accepted as reliable in the court. If specified, the general rules on the ways in which proof is provided means that there is the opportunity to plug loopholes in the regulations and limits the authorization of the Islamic religion to the judge, who conducts the trial, as is deemed appropriate in the public interest. Sharia Law shows caution with regard to the freedom of the judge in tracking legitimate non-Islamic methods in order to avoid confusion, manipulation, fraud, loss of the judiciary times, and ongoing arguments between the parties. However, it may also provide an opportunity for the judges to prove the claim on the basis of imagination, doubts and flimsy arguments. Hence, there is a need for the identification of the methods for providing proof to make the responsible parties aware of what they must do, and the methods, procedures and practices that they must adhere to, in order to guarantee avoiding disbelief and denial, and the basics of these methods are: Witnesses, Confession, Oath, documents and also arguments, presumptions and preview by the judges of the testimony of experts who help to provide the required knowledge of sciences, such as the testimony of a doctor and the scientific experts (Studies and Research Department. (2013).

These legal prerequisites in Sharia Law need to be integrated into the information technology processes and procedures in order to carry out digital forensic investigations. In the Islamic legal system, the process of digital forensics comprises looking for evidence, gathering evidence, preserving evidence and presenting the digital evidence and all of phases of an investigation are compatible with those used in the West. However, in the case of an investigation involving networks, this means that there is a potential conflict between the specialised procedure used to gather digital evidence by digital forensic investigators and the forensics procedure principle in Saudi Arabia, because the criminal justice faces challenges that should be overcome, some instance of those

challenges are: digital crime targeting intangible property, the evaluation and adoption of the legality for data which is provided by digital evidence laboratories, the diversity and multiplicity of digital devices and the lack of a stable law or rules for digital evidence (Al Beshri, 2008). Hence, the investigator must be conscious of the Sharia law requirements during the investigation in order to ensure that the evidence is admissible in an Islamic court. There is no specialized technical investigative standard for dealing with digital evidence under Sharia Law (Al-Murjan and Xynos, 2008).

Therefore, The Council of Ministers in Saudi Arabia approved regulations regarding Combating Cybercrime and Electronic Transactions on the 26 March 2007 which were aimed at reducing digital crimes; identifying the target system, estimating penalties for each crime and infraction and determining the jurisdiction and application of the sanctions (Atalla, 2010).

The interest, which such laws seek to protect is undoubtedly the public interest. Members of the public need to know that their use of digital devices and the international information network (Internet) is safe (Atalla, 2010).

Saudi regulations define the computer in the first article of the regulation regarding electronic transactions as any digital device, fixed or movable, or wired or wireless, that contain systems for data processing, storage, sending, receiving or browsing and carrying out functions determined according to the programmes and commands that is given (Article 1 of the Electronic Transaction Regulation of Cybercrime Regulation, 2007) (Atalla, 2010).

In addition, the Saudi regulation on electronic transactions defines electronic transactions as any exchange or correspondence or contact or other procedure concluded or

implemented by electronic methods (Article 1.10). Electronic data is defined as data that has a number of characteristics including text, symbols, images, sounds, drawings or other electronic data (Article 1.11) (Atalla, 2010). Before the issuance of this regulation, substantive rules guided by traditional texts in Islamic law and the penal regulation of the criminalisation of theft, fraud, breach of trust and forgery were used for protecting data by the law (Atalla, 2010).

2.6.1 Saudi legislation with regards to criminal investigations

Article No. 24 of the Saudi Law of Criminal Procedure states that investigators must, “Search for and arrest criminal offenders and collect the information and evidence necessary for the investigation,” and, “Indictment shall be undertaken by a criminal investigation officer”. The investigator has a right to seek the assistance of experts during the collection of information relating to the crime or crimes, and the criminal investigation investigator has full freedom to select an expert, determine the task that should be done by the digital investigator, how it is to be undertaken, and how to present the findings. Thus, the expert opinion about a case is one of the inferred reports that is submitted to the court (Al-sahimi, 2007).

Article No. 76 of the Saudi Law of Criminal Procedure states that, “The Investigator may seek the assistance of a specialised expert with respect to any matter relating to the investigation”. Further, Article No. 77 states that:

“The expert shall submit his report in writing within the time prescribed by the Investigator. If the expert fails to submit his report by the deadline, or if he finds justification therefor, the investigator may replace him with another expert. Each of the

litigants may submit a report prepared by another expert retained by him in an advisory capacity”.

2.6.2 Experts' scope of work under Saudi Legislation

It is clear from the previous sections that the expert (the digital investigator) is not allowed to undertake the digital investigation for the case before obtaining permission from the investigator, who is in charge of the case.

The expert report and opinion is not binding for the investigator, because the assistance of a specialised expert is dependent on the investigator, who may choose to use or reject it without having to give a reason (Al-sahimi, 2007).

Furthermore, according to Article No. 77, the expert should provide a written report within the timeframe stipulated by the investigator, and should provide in the report all findings, a signature, the date, and a summary of the precise topic that the investigator requested be discussed.

In addition, the investigator should ensure that the report provided by the expert is related to the correct case, and then attach it to the case file.

Therefore, the expert's tasks can be summarised as follows:

- The expert should present all steps undertaken, and all information that emerged during the task.
- The expert should present a summary of their findings, and their opinion about that case.
- The expert report must include the date and the expert's signature.

The expert report should be limited to any task that is assigned by the investigator ; the expert should not exceed the scope defined by them, and should not take decisions about the case, such as stating whether the suspect is related to the case or not (Al-sahimi, 2007).

In addition, the expert's report cannot be solely relied upon as evidence for proving guilt; this can only be determined after the opponents have discussed and commented on the expert's report. Opponents can defend and provide their own evidence that might contradict what is provided in the expert's report, and highlight any shortcomings or mistakes, or even disagreements on opinion. As a result, the court does not rely on the expert's report, according to Article No. 78 of Saudi Law of Criminal Procedure, which states that:

“The litigants may, on sufficient cause, object to the appointment of the expert. Such objection shall specify the reasons thereof and be submitted to the Investigator for decision. The Investigator shall issue his decision within three days from the date of submission of that objection. When an objection has been filed, the expert shall not continue in his assignment except in case of urgency, in which case the Investigator shall order the expert to continue”.

Therefore, the expert's report is not admissible as evidence in court until the investigator has discussed it with the opponents, after they have examined it, submitted their comments and provided evidence.

2.6.3 Summary of the role of the investigation within the Saudi courts

As discussed above, the expert report is not considered evidence until the investigator or judge takes it or some part of it, or may reject it, citing their the reasons for rejecting it. From the court's perspective, the expert's report is just the opinion of the expert, which may help to prove the case or provide probative value to the case. In addition, in applying the principle of judicial conviction, the judge has the right to estimate the value of this report. Therefore, the court in Saudi Arabia is dependent on its conviction about what the report that is provided by the expert contains. Therefore, the expert report must be accurate, with certain steps having been followed (as mentioned in Chapter 2, Section 2.5.2), or the report will not be accepted by the court (Al-sahimi, 2007).

Currently, digital investigations in Saudi Arabia are conducted according to Saudi Anti-Cyber Law by the Bureau of Investigation and Public Prosecution.

Therefore, the disadvantages of the current process in Saudi Arabia are:

- There is not direct contact between the digital investigator and the investigator who is charged for the case
- There is no sharing information between digital investigator and the investigator during investigation

2.7 Digital Forensics Procedure

With an increase the number of internet users, the internet may provide criminals in charge of organised crime protection, through some social networking or websites. The legal regulations of each country reflect the reality of trends and tendencies in society.

The Kingdom of Saudi Arabia issued the regulation related to digital crime with the aim of reducing digital crimes by identifying such crimes and prescribing punishments related to such crimes (CARJJ, 2012).

This section describes the conventional forensic procedures used in Saudi Arabia and applies them to information systems. It will also highlight the aspects of Islamic law which forensic investigators need to be aware of in order to be able to handle and produce digital evidence, which is acceptable to the authorities in Saudi Arabia. The forensic procedures to be followed for gathering data as evidence and exploring and securing a decision to punish the guilty in Al Sharia law were drawn up by the Saudi Arabia Government (Dafiri 2003). When a crime occurs in a Muslim society, evidence is needed to back the claims on the grounds that the Qur'an states "Bring forth your proofs, if you are truthful" (The noble Qur'an 27:64). The point of the investigation in Sharia Law is to find out what actually happened and ensure equity between individuals. This strategy incorporates the following steps:

The first step after a crime has been reported is to ascertain that the crime has been committed, because the Messenger of Allah (peace upon him) stated that "Were people to be given everything that they claimed, men would [unjustly] claim the wealth and lives of [other] people. But, the onus of proof is upon the claimant, and the taking of an oath is upon him who denies" (Islam Hadiths, Hadiths 32-34, Nawawi). Derivation is defined by Al Sharia law as data provided as evidence. It is characterised as giving personal private evidence in light of the fact that it is not referred in the Qur'an and the (Hadith) (Dafiri 2003). There is no procedure and technique which provides the best way to gather evidence relating to some crimes. These days, derivation is known as a methodology for gathering evidence in forensic procedures to verify that a crime has been committed in

light of the fact that it is mentioned in the Qur'an that, "If an evil-doer comes to you with a report, look carefully into it, lest you harm people in ignorance ..." (The Noble Qur'an 49:6).

The objective of this stage is attained by gathering as much data as possible around a particular crime to inform the decision on whether to close the case due to inadequate evidence or to take forward the investigation.

In Islamic law, it is necessary to give evidence when the victim reports the crime. Ways of demonstrating crime in Al Sharia law are disputable (Alkarmi 2005; Al-Zohaili 1994). There are two perspectives: The primary perspective accepts that these strategies are restricted to particular routines, for example, witnesses, confessions and oaths. This perspective is focused around the Qur'an and the Hadith (Al-Zohaili 1994). The second perspective accepts that these techniques are boundless and can incorporate any system that prompts reality, for example, confessions, evidence that is available against the offenders, witnesses, bearing affirmation (Al Qarinah which means presumption) and investigative techniques.

Evidence in AL Sharia law is interpreted as being a sign, which could help find the answer to a riddle (Al-Zohaili, 1994). There are various rules for gathering data as evidence in AL Sharia law as shown below (Al-Zohaili, 1994):

- The evidence must be the result of an investigation: the evidence ought not to be speculated or anticipated, the evidence ought to be extracted by scientific methodology;
- The evidence must connect a crime with its victim or the crime and its culprit. In the event that there is a solid connection between them this evidence is called

strong evidence, otherwise it is powerless evidence. Strong evidence is adequate in Al-Sharia as a primary strategy for evidence; powerless evidence is inadmissible in light of the fact that it is based on prediction.

Therefore, at the outset, the specialist investigator must keep these principles in mind when gathering and collecting data about the crime, for example when listening to witnesses and meeting the victim (Dafiri 2003).

Nowadays, computer abuses/crimes necessitate exceptional processes to be used to identify the guilty party. Seeking, gathering and examining data helps to find the evidence to accomplish equity.

An investigation in Saudi Arabia is described as demonstrating a crime with acceptable evidence (Dafiri 2003). A forensic investigation is a set of procedures and lawful strategies that are followed by investigators before a trial to find out the facts and identify the guilty party by assessing and investigating the evidence of crime (Dafiri, 2003). Various forensic investigation procedures could be used, for example, searching for specific evidence of a crime against private property (Dafiri, 2003). It is a technical process to discover a connection between a crime and a suspect, keeping in mind the end goal, which is to demonstrate or that there has been or has not been a crime.

As per article 46 of Saudi Cybercrime Law which says “the inspection is allowed only for searching the devices that relate to the crime, which provide information about it, however, if during inspection of the device(s), there is evidence which may relate to the crime or to be helpful to discover another crime, it must be seized or documented in the inspection record by the criminal investigation officer ” of the forensic process in Saudi Arabia, a specialised investigator has authority to look for data and items that can be

identified as being related to a specific crime (Dafiri, 2003). Consequently, a definitive objective of this stage is to look for data that relates to a particular crime and to ensure the privacy of suspects. Carrying out searches breaches Al-Sharia law in light of the fact that it abuses the protection of individuals; the Qur'an states "spy not" (The noble Qur'an 49:12). This procedure is only permitted if it is deemed vital, and only in an extremely limited manner within the scope of the crime which is investigated (Al-Sannd, 2004). The search must be halted when evidence has been discovered (Dafiri, 2003).

Al-Murjan and Xynos proposed in 2008 the search procedure also applies to computer abuse/crime. The following steps must be taken after applying for a search permit:

- It is important to ascertain whether a computer is on or off as some data may not be recovered if the computer is off, for example, unstable information (e.g. ARP cache and routing table). The ACPO guidelines are a valuable source of information in such cases and recommend what to do in either of the circumstances.
- The computer system ought to be inspected physically. Documentation ought to report on any distortion (The International Association of Computer Investigative Specialists, 2007).
- When the machine is switched on a picture of the screen should be taken to document the change of evidence during collection.
- It is not permitted to violate of the privacy of suspect by the person who gathers the forensic data to examine the evidence, because the Islamic principles ask Muslims to gain permission before they access the properties of another, which is the Islamic approach to protecting the rights of privacy. Based on this principle, a

person must not gain access to digital devices (physically or logically) which are not his own or have a look at their contents without permission.

- Investigation ought to begin where the information of evidentiary worth is most likely to be discovered (The International Association of Computer Investigative Specialists, 2007).
- A full index posting ought to be made to incorporate filenames, time stamp and so forth.
- Files made by users ought to be analysed by using file viewers, for example, email and database.
- Operating system files ought to be analysed, for example, registry, temporary, cache and history files.
- Only an authorised individual is to analyse the data, which is evidence;
- It is helpful to analyse unused and unallocated space volume in advance of deleted information and slack space information, because “the files may be automatically carved out of the unallocated portion of the unused space based upon known file headers” (Dempsey, 2010. Pp 300-301).
- All findings ought to be recorded.
- All procedures ought to be recorded.

The first step of the search in an investigation is to seize the evidence for a particular crime. Seizing is holding evidence with lawful power, keeping in mind the end goal is to secure the integrity and accessibility to evidence (Dafiri, 2003). Seizure is done to demonstrate a claim as well as to disprove a claim. Article 56 of Saudi Criminal Procedure System states “the messages, telegraphic, telephone conversations and other of communications networks are not be allowed to accessed or observing them except for

reasoned and for a definite period, as provided for by this regulation”, Article 57 states “The head of Investigation and Prosecution Bureau has the right to seized parcels, documents, and can authorise the monitoring and recording of telephone conversations, when this is useful to reach to the crime which has occurred, with permission reasoned and duration of no more than 10 days which are extendable accordance to investigation requirement.”, Article 58 states “The investigator has the right to access the documents, parcels and all items seized, and can listen to recordings, in accordance with the requirements of the investigation, in addition, the investigator can copy and annexe material to the case file or he can return them of the owner.” and Article 60 said “ The owner of the device seized has the right to ask the investigator to return his device to him, in cases where the request is rejected; he can appeal to the head of department” relating to forensic procedures in Saudi Arabian law which could be applied in forensic investigations to seize evidence relating to computer crime (Dafiri, 2003):

- It is permitted to seize the device without getting to the information and the date and time of seizing the machine should be recorded.
- It is permitted to keep the seized content of a device, CDs, flash memory, floppy disks and papers in a safe store (The International Association of Computer Investigative Specialists, 2007).
- It is permitted to seize any printouts and pictures identified with a crime.
- It is permitted for device owners to have the seized papers returned.
- The investigator is in charge of the security of the seized items.

The next stage is the Inspection phase, which seeks to give the entire picture of the crime by demonstrating the connection between a crime scene and a suspect or between a

suspect and a victim. This stage is imperative in light of the fact that it will demonstrate or negate the connection between a suspect, a crime and the seized items.

To apply this process to computer abuse/crime, the following processes should be followed:

- The original information ought not to be inspected to ensure the integrity of evidence.
- The name of the suspect ought to be kept from the inspector to pre-empt lying and cronyism.
- In inspection process there should be undertaken a logical order to develop a working model for the entire inspection.
- When the content of a seized device is submitted to an analyst, the inspector ought to check and sign for them; authorizing the examination pertaining to the evidence to be examined.
- A duplicate of the data is used for the examination.
- Log files, which exist in IDS, router, firewall, DHCP, and so on should be examined.
- The evidence should to be extracted.
- All the procedures should to be recorded.

The following phase involves engaging an expert witness; someone with a high level of expertise in investigative procedures and connecting a suspect with a crime scene. In Islam it is permitted to have an expert witness (Dafiri, 2003) as stated in the Qur'an, "So ask of those who know the Scripture if you know not" (The noble Qur'an 16:43). There are various conditions to be met when using an expert witness, including (Dafiri 2003):

- An expert is obliged to give the process of connecting a suspect and a crime scene.
- An expert is obliged to give a report at the requisite time.
- An expert can provide a plan of action to an alternative expert.
- It is permissible for both the victim and the suspect to engage a private advisor to examine the processes of the expert.
- Both the victim and the suspect can disagree the report drawn up by the expert.

The last phase in the digital forensic investigation is obliged to provide answers to questions regarding what kind of crime was committed, the type of evidence gathered, how it was gathered, what happened, when and by whom (Al-Murjan and Xynos, 2008).

2.8 Size of digital crimes in Saudi Arabia

As we know that digital crimes are committed using digital devices, as well as the behaviour of criminals being multi-dimensional and diversified (Gabe, 2010). Therefore, the researcher looked at the most common crimes in Saudi society carried out through computers and the internet to bring them to the attention of the relevant officials and organisations, social associations, educational, media and mosque preachers and scientific institutions charged with the control and reduction of such crimes. The researcher reviewed the information gathered for 1055 users on 15 websites by (Kaisi, 2011) concerning crimes committed using technology in Saudi Arabia. The main points that resulted from this research are as follows:

1. The sexual crimes rate (53.6%) relates to people accessing obscene sites on the Internet. A proportion (49.8%) of users were sent invitations via email from sexually obscene sites. 2% of the crimes related to defamation of individuals on the Internet. 5.2% related to maligning individuals over the Internet, and 6.8 %

to using email to distribute sexually material. Whereas, 32.4% had pornography from some source dumped to their email addresses.

2. Crimes attacking websites (hacking/ denial of service) are the most common, with 7.7% of websites having experienced electronic penetration. While a rate of 2.4% were subject to destruction. A rate of 33.8% of the research sample, had their personal devices subjected to attacks online. 29.3% of the sample had been subjected to attack via the Internet. In addition, 26.8% of email addresses were targeted. 16.6% of the samples' email addresses were subjected to access to information or destroy it. 63.8% received emails which contained viruses or Trojans.
3. The most widely recognised crimes related to money: the field study information demonstrated that 3.5% of crimes were related to credit card fraud on the Internet. 29.3% were subjected to calls for betting on the Internet. 8.2% had their online data tampered with by third parties. 2.9% were subjected the promotion of and trade in drugs. 13.7% were subjected to calls for access to sites related to money-laundering.
4. The size of the more basic legal violations of privateering or robbery: 24.6% related to theft of a personal computer. 8.4% were subjected to calls from one of the sites relating to the spread of stolen material. 10.3% suffered harm to their individual information due to pirated materials and 10.7% had pirated materials sent through their e-mail. Furthermore, 40.9% accessed product containing pirated material through the Internet. 19.3% were subjected to attack due to the planting of malicious materials in mail advertising.

5. The level of the most well-known crime, digital terrorism: 23.9% were subjected to materials related to digital terrorism. 0.9% used their email to convey thoughts of terrorism. 1.2% was contacted by mystery associations to undertake certain demonstrations. 50.5% were subjected to demands for donation by anonymous persons on the Internet.

6. The range of the issues of digital crime: 64% accept that the Internet may encourage the spread of sexual materials. 53.3% are aware of the inability of systems to provide absolute security of information. 51.3% accept that some unacceptable material will slip through the filters on the Internet. Furthermore, 45% accept that social assaults over the Internet may undermine public opinions. 36% of the sample group find that unlawful acts over the Internet are bringing about a loss of trust in innovation advancement and are undermining the human personality. 32% of the research samples addressed said that it is difficult to deal with network information because of the easy leakage of personal information. 28.3% of the research community feel that there is a risk that undermines individual opportunity. 28.2% of the research samples did not prefer to visit different web sites because of fear of piracy. 25.2% find support to be available on the web. Meanwhile 23.5% of the research sample, compared the disadvantages of the internet with its advantages, and found limited learning and utilisation of the internet. 22.1% think that they have lost trust in the material distributed over the Internet. 22% accept that using the Internet means accepting that there is lack of protection. 17.8% of the research sample had some issues dealing with websites to perform transactions. 16.5% viewed the Internet was

one avenue for drug smuggling. 10% experience issues in using the Internet because of badgering and provocation over the Internet.

2.9 Drug crime

Nowadays, cybercrimes have become the source of a real threat for many countries, because such crimes are no longer limited to the theft of bank funds or those of individuals, but have now reached new sectors such as port security, which may be exposed to serious attacks from organized crime gangs or terrorists or even hostile states (Al ittihad, 2016). In addition, there is a global market which provides illegal goods from anywhere in the world which is called “The Dark Web”. This provides to its users the ability to buy and sale various illegal goods anonymously. The most prevalent items on the dark web are drugs, because they are dealt in large quantities and are very difficult to intercept. Therefore, dealers and drug users resort to these sites in order to buy the drugs without leaving any traces (Hosni, 2016). As mentioned by (Gehl, 2014) web browsers and Dark Web Social Network are accessed through tools such as the TOR proxy (“Tor is actually an open network and free software, aiming at camouflaging your IP and providing you with a secure pathway to the Internet” (Ali, 2014)) for illegal activities such as watching pornography, dealing with illicit drugs among others. Therefore, the Director of the Drug Enforcement Administration in Saudi Arabia affirmed that social networking sites in Saudi Arabia are thought to be a suitable environment for the promotion and sale of drugs. In addition, the drugs trade through the internet is becoming a global issue, and social networks are one of modern methods for promoting drugs (Al-Ghamdi, 2016).

According to Laithi, 2015 Saudi Arabia have been exposed 4400 cyber-attack during 2014, which led Saudi Arabia to be the 36th place globally in its exposure to cyber threats of 55 countries which were exposed cyber-attack in 2014. This necessitated urgent consideration of the issue of special legislation to combat cybercrime in the Kingdom of Saudi Arabia. Regulation No. M/17 was issued in 26/03/2007 based on the decision of Council of Ministers Resolution No. 79 taken on 25/03/2007. It includes a definition of cybercrime in the first article (any act committed, including the use of computers or network to violation of the provisions of this regulation) (Gabe, 2010).

The Saudi regime seeks to punish those who use computers and the Internet in particular, to breach public morality. The act stated in Article 6, that this is "punishable by imprisonment for a term not exceeding five years and a fine of not more than three million Riyals" (Gabe, 2010).

2.9.1 Why Drugs?

This research adopts drugs crimes as the topic of study for a number of reasons:

1. The researcher found that there is increase in the rate of drug crimes in Saudi Arabia, based on the statistics provided by the Saudi Ministry of Interior; up to 147 suspects were arrested within a single day, which equates to six people every hour. Also, nearly 230,000 Captagon pills and 82 kg hashish per a day. For example, according to the security spokesman for the Interior Ministry in Saudi Arabia in 2016, he said that identified a number of drugs promoters' who were marketing their drugs through social networks such as snapchat (Al Shaya, 2016).

2. The researcher could gain access to the drugs crimes files in the narcotic department and the Prosecution Authority Department in terms of finding contacts and meeting investigators whom were related to this study.
3. The researcher also found the investigators in drugs crimes department more cooperative and responsive, as well as giving details of drugs crimes that are often characterized by ambiguity because drug dealers intend to maintain anonymity in their activities (for example, selling drugs within social networks and they delivering them anonymously and taking payment in bitcoin (encrypted online anonymity point of sale) make it harder to trace who paid the money and collected the money (encrypted online anonymity point of sale). The researcher did not find any response from of investigators in other departments. For example, homicide department did not share any information about their cases they handle, which was acceptable because such cases are very sensitive and needs more privacy due to the conservative Saudi society and culture.
4. The procedure of the digital investigation process is used with all types of crimes in the department to gather the data.

2.9.2 Why Saudi?

In Saudi Arabia there is a lack of studies concerning digital forensics. More precisely, there is an absence of studies regarding digital forensics processes where there is insufficient evidence. Cybercrime in Saudi Arabia has been shown to be on the increase, with 437% increase over the past two years. Furthermore, 775 cyber crimes have been registered in Saudi courts, however, due to the inability to solve these digital offences

using specific digital forensic methods, these crimes cannot be dealt with adequately. (Alaraby, 2016).

Moreover, there is an absence in the cooperation between investigating bodies and digital investigator. There are also limitations in both the processes used by digital investigators and the current permissibility in Saudi Arabian laws when it comes to incorporating cyber crime suspect statements with digitally extracted evidence.

Currently in Saudi Arabia, there is no digital investigation procedure in cases where there is insufficient evidence. Therefore, it is becoming increasingly more difficult for digital forensic investigators to carry out thorough and reliable investigations.

Consequently, this research is aimed at identifying the factors that influence the digital investigation process which arise with regards to ensuring that the evidence gathered is as complete as possible and is also admissible in a court of law in Saudi Arabia. In addition, this work proposes a development framework to improve the accuracy and completeness of the analysis in the case of incomplete and/ or imprecise evidence.

The research reviewed previous studies in digital forensics investigation which have been developed around the world during the past three decades and the differences between them in table NO 10 and 11, for example Pollitt (1984), Kohn, Eloff & Olivier (2006), Al-Murjan and Xynos (2008), Yusoff, Ismail & Hassan (2011), Hong, Yu & Lee, (2013).

There are several reasons for choosing Saudi Arabia context for the purpose of this research:

- According to American studies, Saudi Arabia was ranked as the first country in the use of the Internet within Arab countries, where the young people constitute the largest percentage of the total Internet users in the Arab world (Alarabiya, 2013).
- A report issued by the Saudi Ministry of Justice revealed that cybercrime increased during the past two years by more than 437 %. The report shows a lot of crimes since applying cybercrime in Saudi Arabia, reach a number of 775 crimes were registered in Saudi courts. These 775 crimes exceeded the number of crimes that were registered in Saudi courts that were 573 in 2015 and 164 in 2014 (Alaraby, 2016).
- There is a lack of studies concerning digital forensics process in Saudi Arabia. More precisely, there is an absence of studies regarding digital forensics process where there is insufficient evidence.

In sum, the researcher has presented the investigation of digital crimes from an Islamic view; with evidence from the Qur'an and Sunna Hadith that provide Muslims with principles to follow. It has also outlined the application of digital forensics in Saudi Arabia that has been applied based on Sharia Law. However the researcher did not identify any points that address the issue of insufficient evidence with the investigation processes in Saudi Arabia.

2.10 Conclusion

Digital forensics seeks to achieve the successful investigation of digital crimes through obtaining acceptable evidence from digital devices that can be presented in a court of law. Thus, the digital forensics investigation is normally performed through a number of phases in order to achieve the required level of accuracy in the investigation processes.

In this chapter, the researcher reviewed a number of models and frameworks which have been developed since 1984 to support the digital investigation processes.

In addition, this chapter has presented the investigation of digital crimes from an Islamic view; with evidence from the Qur'an and Sunna that provide Muslims with principles to follow. It has also outlined the application of digital forensics in Saudi Arabia that has been applied based on Sharia Law.

Therefore, this chapter answered some questions of research question. The questions below are discussed in chapter 2.

- Are there any specific issues that arise from the use of Sharia Law in Saudi Arabia?

In this chapter was identified the question below was answered partially by (Al-Murjan, 2008) because it only presented an abstract of the investigation process without providing the investigation mechanism.

- What is the process of investigation with digital crimes in Saudi Arabia?

This chapter does not cover the answer of some sub question as shown below to solve the research problem regarding dealing with the incomplete evidence.

- How does the Saudi Arabia investigation procedure handle insufficient evidence?

Regarding to the lack of studies about Saudi Arabia in the digital forensics, the researcher found that the literature review did not address issues related to insufficient evidence, as far as the researcher knows.

The next chapter will be the methodology for data collection and research method that will be adopted in solving the research questions.

Chapter 3:

Research Methodology

Objectives

-
- Presents the research methods that are employed and research methodology
 - Presents the data collection method
 - Present the research method
-

3.1 Introduction

The varied and dichotomous nature of research methodology and the associated literature is regarded as contentious not only because of the varied nature of research approaches, but also due to concerns about the major philosophical arguments advanced in the literature (Fitzgerald and Howcroft, 1998). This argument has been advanced by several authors in discussions of the epistemology of research (Guba and Lincoln, 1994), (Lee, 1991), (Morey and Luthans, 1984). The basis of some discussions is outlined in the method and methodology chapter. Some of the dichotomies that exist within the research literature include the positivist vs. interpretivist, quantitative vs. qualitative, exploratory vs. confirmatory, and induction vs. deduction. Discussions of these dichotomies play a role in the decision as to how to structure the research as well as the identification and adoption of the most suitable methods and methodology.

It should be noted that the above list of dichotomies is indicative rather than definitive (Fitzgerald and Howcroft, 1998). It should also be noted that the listed level of abstraction of the dichotomies differs; while some are overarching, some may be identical (Fitzgerald and Howcroft, 1998). The comparison below provides some indications of the nature of these terminologies and how they relate to the development of the research method and methodological arguments.

3.2 Paradigm level

The two dichotomies at the paradigmatic level are the positivist and the interpretivist. Some strong arguments have been made about the dichotomy between the positivist and interpretivist paradigms. The crux of the argument is that a positivist maintains that the world adapts to fix the laws with complexity resolved by reductionism. The benefit of the positivist argument is on objectivity, repeatability and measurement. For the

interpretivist, knowledge is dependent on the researcher's interpretations and the existence of neutrality. In seeking to develop an understanding of the divide between the positivist and interpretivist paradigms, the use of Sandberg's metatheoretical assumptions of positivism and interpretivist, which indicate that the ontology, epistemology, research object, method validity and reliability are all different, is a fallacy (Weber, 2004). For example, Weber (2004) argues that some form of reality exists 'beyond our perceptions' (p.5). It is therefore important that the method or methodology chosen for research is appropriate and not based on the vacuous idea of paradigmatic dichotomies.

3.3 Methodological Levels

Various differences between the methodological levels have been explored over the years, particularly in terms of the quantitative versus the qualitative. Fitzgerald and Howcroft (1998) argue that the quantitative entails the use of mathematical and statistical methods in the identification of facts as well as the causal relationship between variables. This usually entails the use of a larger sample size, with the result generalised to a larger population. On the other hand, the qualitative argument indicates that it is more important to determine what exists rather than the quantity. Various other differences have been identified by Johnson and Christensen (2008) and Lichtman (2006), arguing, for example, that the qualitative usually uses smaller sample sizes than the quantitative. Qualitative data analysis could involve the identification of patterns, features and themes. Conversely, the quantitative uses statistical processes. However, Johnson and Christensen, (2008) notes that while there may be some differences, the qualitative may use numbers and descriptive statistics in the process of analysis, making the dichotomy a fallacy in this case.

Additionally, the methodological level is also concerned with exploratory and confirmatory methods. Confirmatory methods are concerned with the testing of the hypothesis as well as the verification of theory. This is related to the positivist and the quantitative. In contrast, the exploratory focuses on patterns in research data by providing an explanation and understanding through the laying of a basic descriptive foundation that leads to the generation of a hypothesis (Fitzgerald and Howcroft, 1998). This corresponds to Hurley et al. (1997), who argue that confirmatory analysis requires a strong theoretical understanding and measurements.

A further dichotomy concerns induction and deduction. It is argued that deduction uses the overall results in ascribing properties to specific instances. It is also associated with the verification of theory. On the other hand, the inductive begins with the specifics that are then used for generalisation. As new evidence emerges, conclusions can be revised. Whilst the inductive is often criticised by researchers, it is important in the conception of hypotheses and theories (Fitzgerald and Howcroft, 1998). This is in agreement with the argument (Decoo, 1996) about both induction and deduction and their starting point with regard to the specific and general and vice versa. The various arguments outlined above show that what is important in the choice of research methodology is its suitability to the planned research. Given the fact that at the methodological level, the qualitative and quantitative are fundamental, the two should be explored further before confirming the adopted method for the research as well as the rationale for the adoption of this choice.

3.4 Quantitative Versus Qualitative Methodologies

A number of different perspectives underpin the development of knowledge from quantitative and qualitative methodologies. Quantitative research is based on the use of experimental and scientific methods that can be applied to various areas, such as

behavioural psychology, while qualitative methodology on the other hand is hermeneutical or explanatory with applications in sociology and anthropology. The methodologies used in qualitative processes lead to data collection and analysis that in turn lead to the description and testing of theories (Maanen, 1979) Qualitative research provides a means of understanding complex phenomena with an emphasis on details, experiential and process orientation (Miles and Huberman, 1994). In its own right as a field of inquiry, the qualitative methodology transcends subject matter, field of study and discipline. One claim made by researchers is that the research aims to study a phenomenon in its natural setting by attempting to make sense of it and interpreting the situation based on the meanings that people bring to the situation in question (Denzin and Lincoln, 1994: 2). Some categories of qualitative data include characters (non-numeric) like images, words, and sounds, which may be found in a researcher's diary, company documents, websites or developers' models. Ethnographic action and case study research would usually generate data and information as listed above.

A wide range of research paradigms can be observed in the area of information systems (Weber, 1987). A summary of the debate by Bryman (2001) indicates that there are three ways in the relationship between quantitative and qualitative methodologies. Wesley (2009) indicates that the first perspective argues in favour of the clear distinction between the ontological traditions of quantitative and qualitative methodology. For researchers who favour this perspective, there is a hard-and-fast connection between the quantitative methods as related to positivism on the one hand, and on the other the connection between qualitative methods and relativism. This perspective is related to the discussion in the previous paragraph that indicated that quantitative positivists believe in the principle of

verifiability, which does not necessarily correspond to the qualitative relativist belief that reality is socially constructed.

The second way is outlined in (King et al, 1994), (Laudon and Traver, 2007) and argues that quantitative and qualitative methods are measurable within the positivist way to social life. This perspective does not necessarily recognise the marked distinctness propounded by the first perspective, but rather that the differences are stylistic, making this methodologically and substantively unimportant. While the first two perspectives take extreme views, the third takes the middle ground. This middle ground was developed by (Wesley, 2009), (Brady and Collier, 2010) and indicates that quantitative and qualitative methodological traditions co-exist within a broad accommodating scientific environment. Wesley, (2009) argues that while some scholars may sit solely in one camp, many others clearly believe that the two traditions support each other. Bryman, (2004) argues that the connection between research strategy, epistemology and ontology is not deterministic. Both quantitative and qualitative researchers have been accompanied with both the positivist and interpretivist communities respectively.

As discussed above, the underlying assumption regarding quantitative methodology is that the design were mostly expressed based on the objective view that the world seems to present, which is connected to the positivist paradigm of controlling variables while testing for pre-specified hypotheses. Quantitative data involves numerical variables or evidence. Whilst these may be generated by other research strategies, they are mostly generated by experiments and surveys (Oates, 2006). Such types of data are mostly analysed by positivist researchers. Examples of numerical data include the following:

- The number of visitors expressing satisfaction with the IT helpdesk of an organisation;
- The turnover of a company in each of the last five years;
- The amount of time in seconds taken to process a data file;
- The number of characters featured in a computer animation;
- The number of hot links located on a website;
- The number of people who accessed the Internet for more than 20 hours per week.

A researcher's choice of research methods as well as that of analysis depends mostly on the investigation being carried out. A researcher concerned with generalisation across a whole population would choose to administer survey questionnaires to a representative sample of the relevant population. In contrast, a researcher concerned with seeking a contextual understanding of an individual's social actions would be more inclined to use an ethnographic participant observation or an open-ended interview. In order to ensure triangulation, researchers would usually use a combination of both qualitative and quantitative methodology as part of a multi-strategy or mixed-mode method.

Further criteria that determine whether quantitative or qualitative techniques are suitable for use in a particular research study are the underlying assumptions of the researcher as well as the nature of the phenomenon under investigation (Moore and Benbasat, 1991). Table 2 below indicates some of the differences that exist between quantitative and qualitative methodologies with regard to the four following parameters: assumptions,

purpose, approach and the role of the researcher. It can be seen from the table that several interlinked concepts are seen as differences. For example, purpose, generalisability and contextualisation have some connections given the fact that generalising involves indicating how the findings from the sample population would fit the general population. In contextualisation, the researcher's aim is to look at the inductive process. While the differences cannot be juxtaposed, they can be explained to have a similar magnitude in both quantitative and qualitative methods.

Table 2 Comparison between Quantitative and Qualitative Methods

Quantitative	Qualitative
Assumptions	
<ul style="list-style-type: none"> • Objective reality • Method has primacy • Identifiable variables 	<ul style="list-style-type: none"> • Socially constructed reality • Subject has primacy • Complex variables
Purpose	
<ul style="list-style-type: none"> • Generalisability of results • Predictable results from hypothesis 	<ul style="list-style-type: none"> • Contextualisation of results • Interpretation
Approach	
<ul style="list-style-type: none"> • Use hypothesis as starting point • Formal instrument • Deductive process • Data reduction to numerical indices 	<ul style="list-style-type: none"> • Work towards hypothesis and theory • Naturalistic • Inductive • Search for patterns

Researcher's Role	
<ul style="list-style-type: none"> • Impartiality and detachment • Objective portrayal 	<ul style="list-style-type: none"> • Personal involvement • Empathetic understanding

Source: Author's construction from (Wesley, 2009), (Morgan and Smircich, 1980)

Wesley (2009) argues that research at the quantitative analytical level deals with numbers, whilst this is unlikely with qualitative analysis. However, it must be noted that descriptive statistics such as percentages and modes can be used in qualitative data analysis, making the process quantitative in some form. Miles and Huberman (1994) argues that as part of the existing process of qualitative data analysis, the process and involving abstraction of data provide a means of using both qualitative and quantitative analyses. In quantitative analysis, phenomena, behaviours and ideas need to be 'quantified'. Whatever the observation, it must be 'quantified' through the process of counting or scoring. Analysts using qualitative methods approach social life by treating phenomena in other ways, such as by using symbols, images, words and other non-numerical ways.

In quantitative data analysis, data reduction is performed through the grouping of observations in a pre-defined way. Attributes of phenomena that have been observed are counted or ranked using variables. Observations are filtered using a set of criteria defined before to the start of the analysis. On the other hand, qualitative analysis uses the identification of themes. Different techniques, such as Miles and Huberman's 13 qualitative analysis methods, can be employed. These include 'soaking', 'chucking', 'puzzle-solving' and 'concept mapping' (Wesley, 2009).

Researchers from the quantitative school of thought conceptualise and refine their variables or pre-defined criteria, while qualitative analysts or researchers develop new concepts or reform concepts that existed before they had a grounded purpose in data (Neuman and Robson, 2012). Because the criteria in the analysis of qualitative data are not all pre-defined, the process is flexible in the recording of the data. There is variation in meanings from qualitative observations, as these may change from observer to observer. To ensure that an inclusive data collection process can accord for the variations; qualitative analysts use open-ended questionnaires, interviews and data coding to develop the patterns (Babbie and Benaquisto, 2002), (Neuman and Robson, 2012).

Researchers dealing with Quantitative apply proven statistical processes, correlation coefficients, regression analysis, and significance tests to check for regularities within the data. On the other hand, qualitative analysts use 'softer' approaches that include some of the approaches described above as well as 'soaking and poking' and 'extracting' various themes and patterns that appear within the data (King et al, 1994), (Putnam, 1993), (Shively, 1998). Quantitative analysis may be used to illustrate numerical data in the form of graphs, tables and charts. Where necessary, qualitative analysis uses some of the illustrations from quantitative analysis, but the process may also involve the use of verbal communication.

In seeking to review standards of evidence grounded in mathematics and numbers, researchers in the quantitative method area, including (Manhein et al, 2002), Neuman and Robson, 2012), rely on statistical significance and other means involving probability in the establishment of the boundaries that lead to some conclusions. Qualitative

researchers, on the other hand, report their findings by looking at plausibility based on the odds (expression of relative probabilities) of statistics as well as the credibility of their results based on real world observations. Reasons and strength of character must be utilised to establish the trustworthiness of the findings of qualitative analysis (Meyers et al, 2006), (Neuman and Robson, 2012).

3.5 Method Adopted for Current Research

The previous section examined the philosophical underpinnings of research paradigms as well as some of the methodology theories. Various attributes of both the quantitative and qualitative approaches were discussed and reviewed. The process laid the groundwork to identify what would be the most appropriate paradigm for this research, purpose and methodologies for this study. The above narrative provides a sense of purpose in the designation of the research approach for the current study.

The researcher can determine the type of research approach through research paradigms.

This researcher follows:

1. The interpretivist school of philosophy. Research philosophy is a faith concerning the route in which data should be gathered about a phenomenon, analysed and used. Therefore, this study identifies the interpretivist model as suitable to achieve this target rather than positivism, because the researcher is not going to prove or disprove a hypothesis but he is looking to present explanations of how people see their world. This requires a deep understanding of this relationship rather than changing the status quo; which justifies why interpretivist rather than critical research is appropriate for this study.
2. This research uses qualitative methodology, based on the research question, which requires exploring the meaning and experience of people.

3. This research is exploratory, which provides an explanation and understanding through the laying of a basic descriptive foundation that leads to the generation of a hypothesis, providing that the research follows the interpretivist paradigm and qualitative methodology.

4. The research, in terms of causality, uses an inductive approach as qualitative research which tends to generate theory.

This research adopted the Qualitative approaches to reveal issues, answer research questions in and understand phenomena. In addition this approach does not allow the researcher any trying to manipulate the phenomenon, because the answering of the research question should be in a context-specific setting, as pointed out by Patton, “real world setting where the researcher does not attempt to manipulate the phenomenon of interest” (Patton, 2002, p. 39, as cited in Aguirre et al., 2014). Moreover, the qualitative approach does not seek out to how of the subject while to seeks to why, because the qualitative approach relies upon pictures and videos, interview texts, recordings, notes and feedback forms to reach conclusions, unlike quantitative research that depend on statistics or numbers (Hoepfl, 1997).

3.6 Data Collection

Various methods have been used in information system research. Data collection involves the process of obtaining opinions as well as other useful information relevant to the research from sample respondents. The process can involve the collection, classification and categorisation in accordance with the socio-economic variables (Churchill, 1987).

This section will outline a number of data collection methods which support qualitative research methods, such as observations, documents and interviews.

The observation method is a method that depends on observe rather than to ask, where Nicholas Walliman (2006) pointed out that through the actions of people may disclose their experience of the phenomena rather than speech. This method could be used to collect both qualitative and quantitative data (Walliman 2006). This method is unsuitable for this research because the aim of this research is to explore and investigate the factors and barriers which may influence the adoption of DF in Saudi Arabia, rather than observing the actions of participants.

The documents method is recognised as "available or existing data" which may be personal, official, physical or archived (Johnson and Turner 2003). This method is unsuitable for this research because it might have given an imprecise perspective on the situation under investigation (Oates 2006).

In this research, the interview was used as the main method of data collection, to explore the experiences, views, motivations and beliefs of participants.

3.7 General Discussion of Interview and Chosen Interview

Fox (2009) argues that the interview is an essential data collecting technique in research. It involves verbal communication between the researcher and the participants. Interviews are used in the design of surveys as well as in exploratory and descriptive studies. The quality of the collected data in interview depends on the design of the interview as well as the skill of the interviewer. If the interview is performed by a person with a poor interviewing technique, the quality of the data collected is likely to be poor (Fox, 2009). It is therefore argued that the initial interview questions should be piloted on a sample with similar characteristics to the real sample. The development of technology means that an interview is no longer solely a face-to-face activity, but rather one that can also be

implemented using the telephone, social networking sites such as MSN or email (Opdenakker, 2006).

Opdenakker (2006) argues that each interview technique has advantages and disadvantages, which are briefly discussed here. The face-to-face interview is described as synchronous communication in time and place. Because of its double synchronous nature, face-to-face has the advantage of providing social cues that can help the interviewer in the collection of data as well as offering the opportunity to check attitudinal issues. The spontaneous nature of the interviewee's answers is important in ensuring that the possibility of self-deception is reduced. Another advantage is that in face-to-face interviews the synchronous place and time provides a means for the interviewer to create the right environment that allows the interviewee to relax and provide truthful answers. The disadvantage is that if the location of the person to be interviewed is some distance from interviewer, it would cost a substantial amount to perform a face-to-face interview (Fox, 2009).

The other way in which an interview could be conducted involves the use of telephone calls, skype, FaceTime or other communications app. Fox (2009) argues that such an interview would be synchronous in time but asynchronous in place. Some of the advantages of telephone interviews include geographical access to people not close to the interviewer and the ability to contact a hard-to-reach population. Other advantages include the possibility of including sensitive accounts that the interviewee would not like to disclose face-to-face. However, there are a number of disadvantages, including the lack of social cues. Another disadvantage is that the interviewer has no idea of the situation in which the interviewee is in. Despite this, telephone interviews are conducted where necessary (Opdenakker, 2006).

As with the telephone interview, the social network interview is synchronous in time but asynchronous in place. When MSN is utilised, various emotions can be seen from the typing of the interview. The advantage of this form of social network interview is that it could reduce costs. However, a good awareness of the technology is required in order to avoid serious misunderstandings. Email interviews are asynchronous in both time and place but have the advantage of low cost. A disadvantage is the lack of social cues. Face-to-face interviews there remain the most advantageous technique and were employed in this research. Moreover, using Skype and similar tools such as FaceTime can be useful in research interview. Those tools have several of advantages which are low-cost; flexible to communicate for any distance; easy to install and use; providing sharing, collecting and managing data between participants through messaging function; and ease of audio and video recording (Sivula, 2011).

A number of different processes may be used in interviews. There are three main kinds of interview: structured, semi-structured and unstructured. In a structured interview, the interviewer asks each respondent the same questions. This is often useful for quantitative data analysis and data are usually pre-coded. The advantage is that it reduces the burden in regards to data analysis and other interview techniques. It may also be referred to as formalised or standardised interviews. This type of interview is conducted to obtain unambiguous information from each job applicant. To make objective conclusions on the results of this interview, each applicant must be formally comparable with the responses of other applicants (Fox, 2009).

The second form of interview is the semi-structured interview, which is similar to the structured interview but involves the use of open-ended questions (some proposed by the

researcher (“Tell me about...”) and some of them are arising during the interview (“You said a moment ago...can you tell me more?”) and the closed question are contrasted with open ended questions, where the closed ended question can be answered by a simple "yes" or "no". Semi-structured interviews are an important means of obtaining attitudinal information on a large scale. They provide a means of developing a rapport with the interviewee as well as asking different questions depending on the answers given by each interviewee (Khdhir, 2015). Some of the strengths of the semi-structured interview include the development of a positive rapport, high validity, the discussion of complex matters, pre-judgement of problems and the ease of recording. Weaknesses include the high level of interview skills required, the time-consuming nature of such interviews and challenges in analysis and personalisation (Pathak and Inratat, 2012).

In addition to structured and semi-structured interviews, unstructured interviews in which the interviewer asks various questions without any structure may also be used. This has the advantage of enabling the collection of a vast amount of data and allows him or her to discuss issues that arise during the interview freely. However, disadvantages include the cost and time to the interviewer and participants as well as the possibility of inefficiencies. Additionally, the information generated is difficult to contextualise and may involve biases (Samoylova, 2014).

Given the three interview types discussed above, this research used semi-structured interviews as these provide both the structure and flexibility to enable the in-depth collection of data from various respondents. This involved the creation of an interview schedule of initial questions followed by other questions based on the answers provided.

The interview is one of the most commonly used methods for data collection in qualitative research. The types of interview, particularly semi-structured interviews, are discussed below. The semi-structured interview was chosen as it let the researcher to ask sub-questions in the interview and involves a rather open dialogue. An interview was performed with a drugs investigator in order to view the procedure used to deal with digital evidence and the procedure used in drugs investigations.

The interview is the most common method for obtaining information in survey designs. In practice, an interview is a method of interpersonal communication. It is also a common and widespread phenomenon in social life and a huge diversity of interview types exists. Interviews may be conducted in the workplace as well as for employment, research or evaluation purposes. Tools for the interviewer may contain themes and an ordered list of approximate wording of the questions, which may be reworded for each respondent.

The main area of research in this study concerned drugs investigations. Some researchers use '*funnelling questions*' when working towards difficult or sensitive questions by exploring wider areas of choice or interest. Before having to answer more difficult, personal or sensitive questions, the respondents are permitted to become accustomed to the situation. It is important to ask the right questions are asked in order to obtain the necessary information. Considerable attention should be paid to this when taking into consideration any interview guide that may be used. The main role of an interviewer is to listen. It is a necessity to show respect. In order to achieve a connection in the interview process, some practically important interviewing skills are very beneficial. Mason, 1996; based on Myers 2005) argues that interviewers need to consider the following during the interview:

- *Listening: this should be active as previously described;*
- *Remembering what people have said and what has already been asked and discussed;*
- *Observing: picking up non-verbal cues.*

Semi-structured interviews are the fastest way of obtaining information from individuals or small groups. The guidance of the semi-structured interview is flexible enough to use recommendations on how to constantly check questions with the available tools at hand, while providing an opportunity for participants to influence the issues that they consider most relevant. A prearranged guide may be supplemented and corrected through joint efforts by the research team, the project team and client representatives in order to meet two parallel goals, namely flexibility and focus on the research topic. The strategy of the semi-structured interview is to use a minimum amount of advance preparation questions. Such a small number of questions helps to not avoid certain topics and allows the conversation to be carried flexibly, thus allowing the interviewer to become familiar with the subject or area of study. Interviewees can be familiarised those leading the interview. Knowledge of the local language and culture in the form of an informal conversation is a direct prerequisite for the interview.

3.7.1 Method used in semi-structured interviews

As mentioned in the previous sections, the semi-structure method is very flexible; the researcher shows below the steps which should be considered when use semi-structures method.

1. Determine the direction of interview (subject of conversation);
2. Interviewer prepare questions in advance;

3. At the beginning of the interview, interviewers ask general questions to establish contact with each other. Following this, target and clarifying questions are asked to start the interview. The end of interview includes the control (final) questions.
4. The interviewer should create an emotionally friendly atmosphere;
5. Any type of question may be asked during the interview;
6. The interview is conducted in the framework of the applicants' free time;
7. Any necessary records and notes may be made discretely during the interview (Pathak, and Intratat, 2012).

Semi-structured interviews consider individual lists of mandatory cluster aspects used to obtain information. It usually refers to the context in which the interviewer has a set of issues that are involved in the general scheme of the interview, although the series of questions may differ. Issues are often in a somewhat more generalised form than is often the case in a structured interview. Additionally, the interviewer generally has a freedom for asking additional questions in reply to what the interviewer regards as and meaningful and important answers. Semi-structured interviews can be used to gather qualitative information and to explore problems perceived by key informants. Semi-structured interviews provide the opportunity to change the words but not the meaning of questions. Semi-structured interviews are less standardised, and allows deviations from procedures to be made. Clarifying questions that increase the validity of responses may be used. Since semi-structured interviews do not consist of closed questions, it may be hard to end them. The semi-structured interview is an intermediary between structured and unstructured interviews. The researcher needs to provide the list of general questions, usually referred to as interview a guide. Questions may not be exactly as outlined on the schedule. The interviewers may pick upon things that are not included in the guide. The interviewer is

free to add some questions or areas based on the condition and the flow of the respective conversation (Neville 2007).

Semi-structured interviews should be used to explore problems perceived by key informants during diagnoses (Laforest 2009).

Qualitative research is the data source for semi-structured interviews and usually proceeds according to a chosen time and location out of everyday events. Semi-structured interviews should last between one hour and one hour and 30 minutes to let the participants express their opinions by taking their time and leave them to feel free. One-hour interviews are ideal and should ensure that neither the interviewer nor the interviewee experiences a lapse in concentration (Cicco-Bloom and Crabtree 2006).

3.7.2 Rationale for the use of semi-structured interviews

1. Semi-structured interviews are most suited to educational research and case studies;
2. Semi-structured interviews permit an in-depth exploration of experiences;
3. The respondent has the opportunity to answer freely whilst the interviewer retains control;
4. Semi structured approaches enable information relevant to the research question to be accessed and answered (Drever 1995).

3.8 Research Method

3.8.1 Introduction

Deciding on the appropriate research method enables most of the critical improvements to be presented to the researcher (Phillips 1976). The method of research needs to be clearly defined to enable the research to be reliable and credible. This is particularly

important for early career researchers as it does not require decades of refinement and practice.

There are a number of qualitative analysis methods used by researchers to analyse their data, which might be case study, survey, experimental, ethnography, action research or grounded theory.

Case study is one of common social sciences research methodologies. The case study research method aims to explore causation through deep investigation within the real-life context over a period of time for a single individual, group or event. It may involve both the qualitative and quantitative research method for data collection (Alkout & Khalfan, 2004; Yin, 2009). This method is unsuitable to this research, because it leads to generalisation with poor credibility, due to its lack of rigour and reliability (Denscombe 2003; Oates 2006; Khairul, 2008). The researcher in the case study does not know if he is naturally good at it, because there are not rules in using case study. (Oates 2006).

Survey can be used in diverse aims by the researchers, which contain a number of methods such as interview and questionnaires. The survey uses the structured interview in the large scale and focuses on using statistical methods for the data collected in quantitative analysis (David & Sutton, 2004). Moreover, this method can produce a general statement about the phenomena through the relationship shared between the participants that were established and determined. There are a number of researches based on quantitative surveys (Chen & Hirschheim 2004; Wareham et al., 2005; Avison et al., 2008). This method is not appropriate for the purposes of this research because will not adopt a qualitative method.

The experimental method is handled in the laboratory, which critics point out that the laboratory environments do not equate to a reliable environment (Collis & Hussey, 2003). This means that method is not suitable for the aim of this research.

The ethnography method is used to collect empirical data on human cultures as studied through writing, to describe the nature of people (Phillip, 2005, pp. 2-3, 16-17, and 34-44). Therefore, this method is not appropriate for the purpose of this research as this method needs a considerable time for gathering data and carrying out interpretive analyses that considers and interprets the observations and understanding and developing relationships with participants for reaching to the depth scrutiny and investigation.

Action research “it is used by researchers who want to investigate and improve their own working practices” (Oates 2006, p.254). Action research seeks to obtain a personal understanding of action and to use that understanding to solve or develop a problem. It also seeks to add knowledge to social sciences (Myers, 1997, pp.1-2). When considering the goals of this research with regard to the collaboration between the researcher and participants in the research which may be influence on the investigation inquiry. This method might be considered as method used by journalists or a research consultancy (Gummesson, 1991).

Grounded Theory is a qualitative research method developed by Glaser and Strauss (1967) for use in the health sciences. However, since the beginning of the 1990s grounded theory has been used by many IS researchers, such as Orlikowski (1993, pp. 309–340), Allan (2003, pp. 1–10) and Coleman and O’Connor (2007, pp. 654–667). In this research grounded theory is adopted for exploring and investigating participants “views, opinions and perspectives” concerning the adoption of a method of a digital forensics investigation

process in the absence of complete evidence is Saudi Arabia context as the research method for a number of reasons:

1. The use of grounded theory is possible for this form of research as it is of an interpretive nature.
2. It is helpful for the researcher to build a theoretical framework which explains that data was collected; this is because grounded theory includes systematic inductive methods for collecting and analysing data (Glaser and Strauss 1967) to provide rigorous perception into an unknown area relative to the researcher.
3. It is a useful method for assisting the researcher to create a model with which to identify the factors effects on the DF in the Saudi context.
4. It allows for the researcher to develop theory through generation of concepts and categories.
5. It is flexible and allows the researcher to update interview questions for identifying emergent and new issues.
6. Grounded theory differs from other research approaches through a constant interaction between the stages of data collection and analysis of data (Myers and Avison, 2002).

The grounded theory has been selected as a research method, which systematically provides the researcher with a strict and detailed method of analysing data. The advantage of applying this it helps the researcher in understanding the preliminary conditions. In this regard, the researcher has more freedom to investigate the scientific direction and to allow questions to appear (Glaser 1978, 1992, 1998, 2001; Bryant 2002).

This results in the grounded theory method being useful in achieving a better understanding of areas previously unknown to the researcher.

Grounded theory is the qualitative method used in social sciences for the purpose of the acquisition of the theory from data. Data processing of textual information, notes of supervision and the production of a shorthand report on the interview usually occur.

The chapter is organised into two parts, the first of which concerns the discrepancy that has arisen in accordance with the founders of the grounded theory (Glaserian and Straussian). The second part presents the concepts and categories arising from the investigators' contexts as a consequence of the implementation of Strauss's approach.

3.8.2 Grounded theory

Grounded theory consists of a grounded method, the origin of which lies in the symbolical interactionism of its approach, which in itself follows from the pragmatist ideas of James, Dewey, Sacks (Heath and Cowley 2004). The term "symbolical interactionism" was coined by Blumer in 1937 (Manning and Smith 2010) and, together with "naturalistic to investigation", played a critical role in the development of grounded theory (Heath and Cowley 2004).

The grounded theory method was first introduced by Strauss and Glaser (1967) and arose from a successful cooperation during training on hospital deaths in the early 1960s (Charmaz 2006). Strauss and Glaser suggested that the theory could be created through the application of systematic qualitative analysis (Charmaz 2006). However, subsequent work led to a divergence of opinion between these authors.

A number of forms of grounded theory were presented from the moment of its initial development (Heath and Cowley 2004), such as those from Chenitz, Swanson (1986),

Schatzman (1991) and Charmaz (2003). However, the most noticeable variation occurred in the case of the two initiators of the creation of the grounded theory, namely Glaser and Strauss (Heath and Cowley 2004). A difference between these two versions is described later in section 3.9.7, with the subsequent explanation of the reason for the choice of a particular version in this research. The procedures of the chosen version are then reviewed.

According to the founders of grounded theory, their objective was to learn the theory through the systematic analysis of data. Glaser and Strauss (1967, item 3) argue that this theory is able to do the following: (1) provide an explanation of behaviour, (2) predict theoretical achievements in the field of sociology, (3) to allow a greater understanding of situations and to take them under control, (4) to provide a perspective on behaviour, and (5) to provide a style for scientific research in the concrete area of behaviour.

The theory that meets all these requirements is suitable for use in the subsequent relations: theoretical categories have to fit in with data in such a way that is actual and clear. The key idea must be given the opportunity to appear and must explain current and future occurrences and interpret events. It must also be modified in such a way that enables the theory to be changed at any time that new data is collected (Backman and Kyngäs 1999; Corbin and Strauss 1990; Glaser 1978).

In order to fulfil the above-mentioned requirements, a “systematic opening of the theory from these sociological researches” was clarified by Glaser and Strauss (1967, item 3). The authors claim that the main features of such a theory are that it is difficult disprove in the presence of a large amount of data or its replacement with another theory.

3.8.3 The Value of Using Grounded Theory in IS Research

The advantages of using a grounded theory include: its position on social problems (Glaser & Strauss 1967), its applicability to society's experiences (Charmaz 2003; Goulding 1998), its emergent properties (Glaser 1978; Glaser & Strauss 1967), absence from restrictions imposed by prior information (Glaser & Strauss 1967; Glaser 1978), and the ability of the method to build on the work of other researchers (Martin & Turner 1986).

It is of value to those who attach particular importance to the stage of formation (Fernández 2004; Charmaz 2006; Charmaz 2008). The grounded theory research method closely follows the main principles given by Glaser and Strauss (1967), and will transcend providing a dense description from which to render substantive theory (Gulding 2001; Fernández, Martin Gregor, Stern, & Vitale 2006). This notion is backed by Ellis and Levi (2009) who argue that grounded theory can be more beneficial when the literature does not support the notional evolution of the phenomena.

The grounded theory method is a necessary means of investigating the subject of social character. Environmental researchers may be concerned with questions of a public and technical nature. Fernández and Lehnmanm (2005) argue that researchers should accept new techniques in public and technical areas: where they suggested an alternate methodology: the grounded theory building research, where arising theory could assist explain, in conceptual terms and what is occurring in the broader area of research. Alternative methods may lead to the introduction of prejudice due to the transmission of inexact theoretical assumptions when developing the phenomena. The grounded theory method can counterac these problems by preventing the emergence of bias from

assumptions in order to avert a choice of prejudiced theories by which the researcher is required to explain to the record the social and technical phenomena.

Walsham (2006) noted the importance of the method chosen by the researcher. Walsham (2006) argued that having chosen according to the researcher's preference, his or her interactions and beliefs in others' justification of a method will facilitate the work. This was borne in mind when selecting the grounded theory method in this research. In the case of this research, the grounded theory method does not demand the use of previously prepared concepts of knowledge or reality. It is accepted that ontology and the theory of knowledge mean that knowledge does not stand still, but rather undergoes constant transformations and also, is interpreted by the participants and the observer. The meaning moves by dialogue and an act. Dialogue and acts introduce understanding of the experience. It is through the means of interaction and discourse that an understanding can be unblocked and transferred to the observer. Thus, from this perspective, the grounded theory method allows the researcher to achieve an in-depth understanding of the subject.

3.8.4 Criticisms of Grounded Theory

The most widespread criticism in the field of Information System (IS) is based on the argument that whereas it uses interpretivist and constructionist tools, it follows from positivism or objectivism. In this regard an internal mismatch is apparent (Bryant 2002). The section below discusses the detailed criticism. Criticisms include that it is naive an inductive (Bryant 2002; Gulding 2001), restrictions on aprioristic knowledge (Gulding 2001; Bryant 2002; Charmaz 2006), phenomenalism (Gulding 2001), paradox of "theory" (Bryant 2002; Charmaz 2006), and constricted generalisation of theoretical ideologies

(Burava 1991; Nasirin, Birks, and Jones 2003; Charmaz 2006). The resolution of such criticism is beyond the scope of this study.

Grounded theory is qualitative in nature. Data are usually acquired by means of textual information, supervision notes and shorthand reports on conversations. Various ideas about the philosophical arrangements of grounded theory have been proposed. It is considered by some as a positivistic/objectivistic method as can be seen in the language used by Glaser and Strauss (1967). Terms such as “emergence” and “opening” suggest that to make objective representation realistic, only one “real” reality can be accepted (Locke 2001). This assumption may be as a result of the strong argument posed by Glaser and Strauss for the structured method of qualitative analysis (Charmaz 1990, p. 253).

Gulding (1998) and Locke (2001) assumed that grounded theory is more in line with interpreting the paradigm and referred to the American pragmatism and the symbolic interactionist school of sociology. Glaser confirmed this point of view with reference to Strauss's influence and in-depth experience in the Chicago school of a symbolical interactionism. He stated, “Through Anselm [Strauss], I started learning the social construction of realities by symbolic interaction making meanings through self-indications to self and others. I learned that man was a meaning making animal” (Glaser 1998, p.32).

Glaser (2005) inclined towards an inconsistent opinion of the provision of the grounded theory and referred to it as a substitute to all paradigms: “Grounded Theory is not an either/or method. It is simply an alternative to positivistic, social constructionist and

interpretive qualitative data methods” (Glaser 2001, p.6). Glaser (2001) emphasises that the selection of a method determines the requirements of such research, as opposed to by any paradigm bias: “My bias is clear, but this does not mean I rubber stamp ‘ok’ or indict any method. The difference in perspectives will just help any one researcher decide what method to use that suits his/her needs within the research context and its goals for research” (Glaser, 2001, p. 2). The grounded theory method is based on the constant comparative analysis, a process that looks for regularities in data and their conceptualisations prior to further coding and analysis (Glaser and Strauss 1967). It is possible to reach a theoretical method of selection defined as “a process of data collection for generation of the theory” (Glaser and Strauss 1967, p.45). These subjects are discussed in the following subsection.

3.8.5 Constant comparison

The constant comparative method aims to make the theory systematic by beginning the analysis and coding of data at the same time (Glaser and Strauss 1967). It is used in conjunction with theoretical selection and provides flexibility and uncertainty to help formulate the theory (Glaser and Strauss 1967).

Constant comparison aims to compare cases in each of the categories, integrate properties of each of the categories, differentiate the theory, and to write down the theory (Glaser and Strauss 1967, p.105). The use of a method of continuous comparison aims to research critical points in the performance of respondents who are connected to research questions that remain uncertain. It also aims to elicit further details from the interviewees.

Strauss and Corbin (1998, p.78) claim that theoretical comparison “is for the stimulation of thinking of properties and the dimensions and to direct theoretical selections”, and possesses the potential to offer additional interview questions based on the evolving

theory. The comparative analysis can create two versions of theories, the formal and substantive. “*Substantive theory is developed for a substantive area of sociological inquiry, while formal theory is developed for a formal on sociological inquiry*” (Glaser and Strauss 1967, p.32).

This research will develop into a theory due to the focus of the researcher on the main area of research, namely enhancing the accuracy of digital forensics in the absence of complete evidence. The main focus of this research is the comparative approach to the examination of a situation in a digital investigation process with incomplete evidence. Generation of the theory on the basis of comparative analysis is possible (Glaser and Strauss 1967). Moreover, Glaser and Strauss claim that the probability of successful comparison increases considerably when widely opposing procedures are selected.

3.8.6 Theoretical sampling

Theoretical sampling refers to the accumulation of data from which to generate a theory (Glaser and Strauss 1967). Strauss and Corbin (1990) define it as a sampling “of concepts that have proven theoretical relevance to the evolving theory” (p.177). They note that the process can help the researcher to define the type of data they need to collect and how to locate it. It will also assist the researcher by enabling the identification of gaps in existing theory, prompting scientific research questions (Glaser and Strauss 1967). This links to the argument that theoretical selection is a deductive activity based on inductive categories or hypotheses (Beckman and Kyngas 1999; Fernández 2004).

The theoretical method of data selection is developed for application in the course of collecting and analysing data (Glaser and Strauss 1967). Strauss and Corbin (1990) claim

that it helps to further communication between concepts raised, and introduce categories based on certain properties and dimensions.

To meet the objectives of this research, the researcher chose interviews as the main procedure of collecting data. The researcher is seeking to provide a rich source of data by interviewing people who have are experienced and have knowledge of the investigation process. Strauss and Corbin (1990) emphasise that theoretical selection of information is a form of deliberate selection. Moreover, it is useful when the analysis of data is being carried out in conjunction with other data collection methods (Strauss and Corbin 1990, p.183) that provide an opportunity to study a representative population during data collection. In summary, the theoretical process of theory selection can stop when the categories reported on reach the point of saturation. Theoretical saturation is therefore, the criterion determining at what stage the researcher can stop theory selection and data collection (Glaser and Strauss 1967).

However, following of their work on the “detection of the grounded theory”, there was a divergence in views between Glaser and Strauss about the best method for the generation of theory from data. This issue will be discussed in the following subsection.

3.8.7 Glaserian vs. Straussian approaches

Grounded theory was initially proposed by Glaser and Strauss (1967). Yet, they later separated leading to two branches of the theory (Strauss & Corbin 1990; Glaser 1992): the Glaserian school and the Straussian school (Stern 1994). They each have many distinctions of varying significance. The main distinctions are associated with history, and can have considerable impact on researchers employing them. For example, Glaser takes a natural approach and expects that researchers begin their studies with no preconceptions, whereas, Strauss expresses general ideas about the territory being

studied. Glaser conducts the research with the principles that the theory has to arise while Strauss uses structured questions for emergence of the theory.

Locke (1996) investigated grounded theory schools, emphasising Glaserian and Straussian approaches. She noted a lack of considerable distinctions between Glaser and Strauss concerning analytical procedures; for example, related to continuous comparison and theoretical selection. However she noted that they fail to agree on the interaction between the researcher and area of research. Glaser claims that Strauss and Corbin do not learn from a theory, but provide a full the conceptual description of it (Glaser 1992). Robrecht (1995) also indicates a divergence between the Glaserian and Straussians approaches, seeing it as methodological, rather than ontological and epistemological in character; stating that the Straussians' developed their own analytical methods (Heath and Cowley 2004). The general distinction between the two founders is summarised here.

While, according to Strauss and Corbin, the researcher should actively participate in the process of research, he or she has no such role according to Glaser (Onions 2006). Moreover, one of the main differences between Glaserian and the Straussians' approaches concerns the conceptualisation process (Smit and Bryant 2000). When following the Straussian approach the researcher has to give each observation a sentence and name representing the phenomenon. Meanwhile, Glaser testifies that instead of this, the researcher must compare each case to other incidents or concepts (Smit and Bryant 2000). The third distinction established by Strauss concerns the offer to raise questions concerning for instance what, who when and which; Glaser declares this can alter the data and lead to biased analysis (Charmaz 2006). She adds that Glaser offers some alternative neutral questions, how *“what is the data a study of?”* *“What property of category does*

this incident indicate?” A further difference between the Glaserian and Straussian approaches is explained by the role of literature from the perspectives of the two schools of research. They agree that a researcher does not leave the field unchanged, but they do not agree on the role of literature (Heath and Cowley 2004). Strauss and Corbin (1990) emphasise a need for the researcher to become acquainted with existing knowledge about a studied phenomenon when conducting a study. Thus, they emphasise that the application of literature to scientific research is a sound basis for professional knowledge (Allan 2003).

Moreover, Heath and Cowley (2004, p.142) claim that literature provides a data management tool for the novice researcher, although Glaser (1978) criticises this as encompassing potential for bias in the interpretation of data. It is therefore the case that knowledge of a language cannot direct the attention of the researcher; thus, the researcher will need to suspend knowledge of specific phenomena as they relate to consequences (Beckman and Kyngas 1999).

Thus, Glaser notes that when employing grounded theory it is necessary to study reality and to analyse data which does not have a prejudiced hypothesis (Allan, 2003). Research into literature arises only after theories re developed (Heath and Cowley 2004). Carpenter (2011) provided a useful summary of the distinctions between these two approaches as displayed in the table below.

Table 3 Comparisons of the two schools of Grounded Theory

Glaser & Strauss/ Glaser	Strauss and Corbin/Corbin and Strauss
Epistemology	
The researcher has to begin with no preconceived ideas and no literary review about area of study. While the researcher has to begin according to learn from experts.	The researcher can gain an impression about data by means of a literary review. Theories consider a lens through which the researcher comes closer to the data, and which can be verified if used.
Research question/ research problem	
The research question is not essential; while, the researcher studies areas of interest	A research question is essential.
Ethical considerations	
Grounded theory affects concepts not people. The transcription of polls is not obligatory; however, data about particular persons has to remain confidential.	The copying of interviews is recommended to beginners. Storage of Data should be considered reliable. Assurance of confidentiality should be guaranteed..
Data gathering	
An interview guide is not necessary as it is based on prejudiced opinions. Participants and experts are considered and show their primary concerns. Field notes can be used, as can photos, news	Interviews are recommended. Remarks are also part of data, however, can be interpreted and be specified with participants.

articles, historical documents and other information that specifies concepts.	
Data analysis	
Researchers carry out repeated sorting of notes to insure main concepts are clear. Theoretical connections between concepts should be specified.	Computer programs can be used for help in the data analysis.
Results	
Studying can lead to a main theory, which establishes occurrences in an interesting area. Numerous theories can be open from one studying.	Analysis of results leads to subjects and concepts. Theories can also develop from data; however, it is not obligatory to have a result.
Evaluation	
Fitness, work, importance and changeability.	Fitness, applicability, concepts, conceptualisation of concepts, logic, depth, change, creativity, sensitivity, and certification of notes.

In this circumstance, the researcher prefers the Straussian approach for a data collection, and as an analytical technique. Strauss offers a beneficial approach for novice researchers, by suggesting the study of literature to acquire background knowledge before commencing field work. This is opposite to the Glaserian approach, when the researcher begins field work immediately, and then subsequently reviews literature.

Although there are no ontological and epistemological distinctions between the two approaches, there is a methodological distinction in terms of the analytical procedures applied. Those in Strauss's approach are more systematic than Glaser's, giving the researcher a more active role in determining analytical procedures, which will benefit this research. Therefore, in the following section, procedures applied as part of Strauss's approach will be discussed.

3.8.8 Straussian approach procedures

In this section we will discuss the procedures for coding in accordance with Strauss' approach. Coding in grounded theory is a fundamental component of the analytical process employed by the researcher (Corbin and Strauss 1990, p.12). Strauss and Corbin defined coding as processes associated with data analysis. Strauss and Corbin advised coding as "micro analysis which consists of the analysis of data and codings of sense in words or groups of words" (Strauss and Corbin 1990, p.65). Crawford et al. (2000) criticised procedures for installing codes as time consuming, and leading to excessive conceptualisation; this concurs with Glaser (1992). Three types of coding, opened, axial, and selective which will be discussed below.

3.8.8.1 Open coding

This is "*the process of breaking down, examining, comparing, conceptualising, and categorizing data*" (Strauss and Corbin 1990, p.61). The first step in coding the data is the "*conceptualisation process*". Textual analysis begins by unpicking underlying key phrases that make rudimentary sense (Sandelowski 1995). In this stage of coding, the researcher should compare one case to other similar incidents, or instances in other parts of the data, then decide on a name which represents the phenomenon (Corbin and Strauss

1990; Strauss and Corbin 1990). It is possible to concentrate attention to the text of an interview on the line behind the line, or behind the key point (Strauss and Corbin 1998). Concept labelling can be arrived at by both parties through communication and asking such questions as: what is it? Is it that? Thus, means of the analysis in grounded theory depends on the frequency of “*solutions of comparisons*” and “*asking questions*”. For this reason, grounded theory is termed a “*constant comparative method of the analysis*” (Glaser and Strauss 1967). At this stage, the researcher can use notes to record the researcher’s analysis, thoughts, interpretation, ideas and future directions for data collection (Strauss and Corbin 1998).

The second stage is categorising. At this stage, concepts found will be compared among themselves, and with concepts that seem integrated and concern the same phenomenon and are united across more groups (Corbin and Strauss 1990; Strauss and Corbin 1990). For this purpose, a question should be raised: What does the concept seem to be about? This will make it easier to categorise concepts. An easy way to remember categories, involves naming each category to distinguish it from other categories. The name selected can come from the researcher, from literature, or informants, or from “*natural conditions*” codes. It is not important where the name comes from, but that the first analysis is a name (Strauss and Corbin 1990, 1998).

Categorisations of concepts are very important because they provide a number of units that can be reduced (Strauss and Corbin 1998). Together with these categories, there are subcategories, which are connected with and linked to the main category. Establishing a connection between categories and subcategories is an important aspect of an open code. This can be done by means of property and dimensions. ‘The characteristics or identifying properties relating to a section’s properties, and ‘dimensions along a continuum’ (Strauss

and Corbin 1990). To detect properties in each category, the researcher can ask similar questions; e.g. how, *where*, and *when*. Properties can also have sub-properties.

3.8.8.2 Axial coding

Strauss and Corbin defined this as “a set of procedures whereby data are put back together in new ways after open coding, by making connection between categories” (Strauss and Corbin 1990, p.96). It functions to communicate between categories and subcategories. The researcher can then develop categories.

In axial coding, the subcategories are connected with other categories by means of a paradigm model; which allows the researcher to consider concerning data systematically. Using this model will provide the researcher with power, density and accuracy (Corbin and Strauss 1990; Strauss and Corbin 1990). To carry out axial coding effectively, the following variables must be considered:

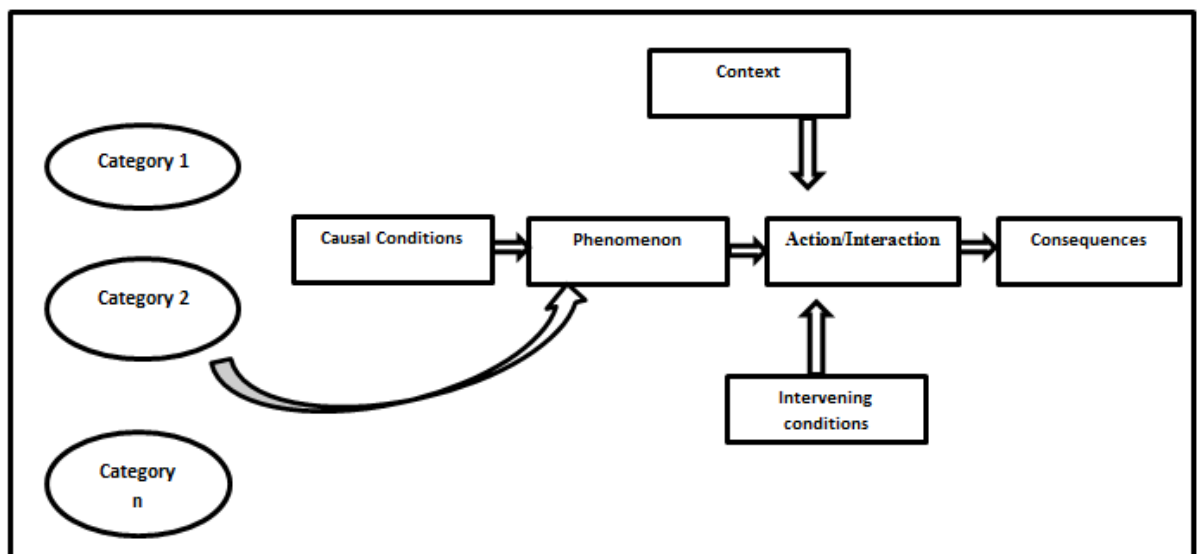


Figure 15 Paradigm Model in Axial Coding.

- **Causal conditions:** incidents, events leading to the emergence or development of a phenomenon.
- **Phenomenon:** The main concept, event, or incident in which a series actions or interactions is directed toward management, processing, or whereby a set of the actions are connected by a page.
- **Context:** represents a set of conditions, during which action / interactional strategy is accepted.
- **Intervening conditions:** structural settings bearing on actions / interactional strategies, which belong to a phenomenon.
- **Action/Interaction:** strategies are developed for management, processing, to carry out and answer phenomena at a certain stage regarding perceived conditions.
- **Consequences:** results or results of activity / interactional

3.8.8.3 Selective coding

In axial coding, the researcher should develop a basis for selective coding, which is the final stage of coding. Selective coding is defined as *“the process of selecting the core category, systematically relating it to other categories, validating those relationships, and filling in categories that need further refinement and development”* (Corbin and Strauss 1990, p.116). This means examining categories, which have already been revealed to see if any are abstract or capture something described previously (Strauss and Corbin 1990). To this category will be added an additional category detailing the main spectacle around which all other categories are integrated. To ensure integration, it is

important to create a subject line to judge the story created by the data (Strauss and Corbin 1990).

Grounded theory needs to be employed to qualify the coding procedure (Strauss and Corbin 1998). Grounded theorists can assist with the application of manual techniques, improving assistance in the analysis process. The importance of such management will be discussed in the sub section below.

3.8.9 Grounded Theory Techniques

A huge body of raw data (Miles & Guberman 1994) can create high-quality scientific research informing the development of productivity indicators (Robson 2002). Organisation, maintenance, coding, and data control are not trivial tasks and novice researchers should not underestimate the effort involved. Two methodologies are employed to process activities and data control at the data analysis stage. The first methodology is the *manual process*, which needs to be employed every now and again, in order to avoid the admission of important data and to add reliability to the process (Malterud 2001). Meanwhile, the second technique indicates the application of technology for data control and to avoid being overwhelmed by primary data (Lee & Esterhuizen 2000). Authors have reported that manual processing can be combined with the computer analysis software, CAQDAS (Computer Assisted Qualitative Data Analysis Software). It can be used to draw credible and verifiable conclusions. Moreover, a *mixed approach*, merging manual and automatic data analysis tools is considered suitable. The main approach for the application of traditional qualitative research methodologies is to establish the ability of CAQDAS to support the compression of data using use “temporary start” (Miles & Guberman 1994, p.58) codes, which emerge from manual development of a research question.

Johny Saladana wrote in 2009, that he was one of those teachers who demand that their pupils at first to execute ‘manual’ coding of the qualitative analysis of data with use of paper and a pencil on paper of the data entered and formatted only with the basic software of a text editor. “*The reason consists in that each class purpose of data collection is rather small-scale*” and, thereby “The project operated for the analysis in this manner. However, if a student has a thesis such as my own independent scientific research, interviews with participants and expanded fieldwork and field notes will be required. CAQDAS will be an important and irreplaceable tool to handle this data. When comparing personal experience between manual and electronic coding. We concluded that the choice will depend on the enormity of the project, means and time, and, a predisposition and experience of the researcher (Johny Saladana, 2009).

Trying to learn the basis of coding and analysing qualitative data at the same time as learning about the difficult instructions and plural functions of the CAQDAS program can be a huge and challenging task. Years of mental energy would be concentrated on understanding the software, at the expense of the data. The author recommends that beginners or small-scale researchers code manually and not use a computer (cf Bazeley 2007). There is something about manipulation of qualitative data on paper with a pencil and in written form codes with a pencil that allows me better control over the work. There is also benefit to laying out information in a table in the form of a big puzzle; something that would be impossible on a computer screen. Establish codes in printed form, then transfer them to an electronic file.

When abstract information is turned into concrete data it becomes clearer (Grau & Wai 1998, p.145). Even supporters of CAQDAS recommend using listings in printed form.

Coded data can be created first with traditional writing-materials to learn new things about the data.

3.8.10 Justification for the selected research methods and methodology with regards to the research questions

This research follows the recommendations of the Straussian school. Strauss has a basic concept of where to begin querying theory, i.e. inclusion of structured queries, conceptual descriptions, and improving theoretical sensitivity using defined research methods. An observer interprets theory, and the trustworthiness of the theory comes from the flexibility of the method. This research grounded theory is adopted for exploring and investigating participants' "views, opinions and perspectives" concerning the adoption of a method of a digital forensics investigation process in the absence of complete evidence in Saudi Arabia context. Furthermore, grounded theory is helpful for the researcher to build/develop a theoretical framework which explains that data was collected; this is because grounded theory includes systematic inductive methods for collecting and analysing data (Glaser and Strauss 1967) to provide rigorous perception into an unknown area relative to the researcher, it is a useful method for assisting the researcher to create a model with which to identify the factors effects on the DF in the Saudi context, it allows for the researcher to develop theory through generation of concepts and categories, it is flexible and allows the researcher to update interview questions for identifying emergent and new issues and grounded theory differs from other research approaches through a constant interaction between the stages of data collection and analysis of data (Myers and Avison, 2002).

3.9 Conclusion

This research adopted the Qualitative approaches to reveal issues, answer research questions in and understand phenomena. It may be concluded that semi-structured interviews are flexible and allow the interviewer to conduct the research according to a plan and to prepare the main points. However, the interviewer is still able to react to the respondents' replies, to correct points or add some extra questions in accordance with gain a fuller picture of the subject. This helps avoid duplication of the questions and allows the interviewer to show consideration to respondents' answers.

In addition, in this chapter we discussed the grounded theory approaches in more detail, presenting the distinctions between Glaserian and Straussian approaches. The chapter explained why Strauss was preferred to Glaser as a guide for data collection and method of analysis in this research. The results of grounded theory will be useful in rendering a clear understanding of key areas of research. Moreover, we know that grounded theory is best employed in the social sciences with qualitative methods. Grounded theory was originally derived from symbolic interactionism. Anselm Strauss and Barney Glaser were the first sociologists to introduce grounded theory. Therefore, in this chapter we discussed the value of using grounded theory, and criticisms of grounded theory, constant comparison and theoretical sampling methods. Moreover, we discussed the Glaserian and Straussian approaches in greater detail. The chapter also included a table to compare the approaches of Glaser and Strauss/ Glaser and Strauss and Corbin/Corbin and Strauss, as regards epistemology, research question/ research problem, ethical considerations, data gathering, data analysis, results and evaluation. The three types of coding that are applied in Straussian approaches (open coding, axial coding and selective coding) were also discussed. To conclude, a summary of grounded theory techniques and justifications for

selecting specific research methods the methodology was given, with regard to the research questions.

Moreover, a computer system conference held in 2009 presented nine papers that applied grounded theory to information technology topics, which clearly shows the importance of grounded theory in the field and allow the examination of how people respond to various phenomena. Since the field of digital forensics is relatively new and involving interaction between the people and technology, grounded theory appears most suitable in developing a framework, because this research deals with the interactions of digital investigators with digital evidence, others involved in the digital forensics environment and with technology that has been used in the digital forensics investigation.

Chapter 4:

Research Design

Objectives

- Present Research design
 - Present Pilot Study
 - Present Empirical Study
-

4.1 Introduction

This chapter describes and defines the pilot study used and empirical study. The importance of the pilot study and the logistical issues that may be detected by a pilot study are described. This research also examines how the resulting data and information may be used and the reasons for conducting a pilot study. The three phases of a pilot study and their advantages and disadvantages are also discussed. The interview protocol is then described. The last part of this chapter describes empirical study methods, the assessment of objectives and the reasons for and advantages of using such methods. The stages of the empirical cycle and the role of the empirical study are described and relevant research questions presented in tables.

4.2 Definition of pilot study

A pilot study is one that is conducted in a simplified form prior to the main study. It is used to determine the necessary sample size and to clarify the content of questionnaires and tests. A pilot study is the most important aspect in planning any experimental studies; it defines the main directions and principles of organisation and methods of basic research in accordance with the most important hypotheses (Edwin et al, 2001).

Arain et al. (2010) state that a pilot study may be conducted following the statement of a problem and before any attempt is made to use a new method. Such scientific work is intended to provide fundamentally new results in a little-explored area. A pilot study involves the search for ideas and hypotheses, understanding the market situation and the specification of ambiguously defined problems. This study may involve the use of printed materials, group interviews or focus groups run by qualified professionals or surveillance of the market and customers (Leon et al. 2011).

Arain et al, (2010) note that a pilot study aims to develop methods and possible ways of achieving scientific decisions in order to undertake further research. Such studies also aim to summarise decisions and tasks, organise previously known approaches and research methods in order to use theories and concepts in practice and to present results to discuss with the scientific community in the form of publications and presentations at conferences, symposia and congresses.

A pilot study may involve a reliability trial – a smaller version of the full study carried out in preparation. It can also involve pre-testing research tools, questionnaires and interview schedules (Simon, 2011), (Calitz, 2009).

A vivid and direct vision of the research topic and question are required before conducting the pilot study, the techniques and methods to be used and to have an idea of how the research study going to look like? It has been described as “*reassessment without tears*” (Calitz, 2009) that allows the researcher to determine whether all research techniques and methods are likely to work and practice effectively. If needed, these can be changed to consequently conform (Calitz, 2009). In this research, a pilot study was used to assess the methods and research techniques as well as the interviews.

The pilot study was conducted with two interviewees on the grounds that in the pilot flexibility is required rather than accuracy, since their aim is to identify possible solutions to the problem rather than to check hypothetical assumptions. Exploratory studies are primarily designed to precisely formulate the problem, determine the possible causes of its appearance, and verify the hypothesis and to identify most likely solutions. Such studies are important and remarkable, to identify new directions for solving various problems and for the verification of the research methodology.

The value of initial piloting is discussed in the next paragraph; time, energy and money can be wasted if a pilot study is of diminutive value.

4.3 Value and Goal of the Pilot Study

The value of a pilot study, as widely described in the literature, was first discussed and its applicability to the current study assessed. After stating the value and the objective of the pilot study, this particular project was also considered.

Blaxter *et al.* (1996:122) state that, “*You may think that you know well enough what you are doing, but the value of pilot research cannot be overestimated. Things never work quite the way you envisage, even if you have done them many times before, and they have a nasty habit of turning out very differently than you expected.*” Yet, clearly a pilot study is important in this research in order to avoid the waste of time, money and energy (Blaxter, 2010).

The main objective of a pilot study is purposely connected to the research project which it is an extension. The pilot study aims to provide important information relating to the research project as a whole. These quotes concern the value and goal of pilot studies: “*to see if the beast will fly*” (De Vos, 2002:410), “*reassessment without tears*” (Blaxter *et al.*, 1996:121) and “*Do not take the risk. Pilot test first*” (Van Teijlingen & Hundley, 2001:2) cited by (Calitz, 2009). In this case, the general objective was to save time, effort and money. Unforeseen attributes could result in the failure of a major research study. A small scale study was conducted as an objective in order to understand the issues that could lead to failure in the research procedure and to reduce the risk of these occurring.

The pilot study in this research comprised two parts. The first aimed to identify or explore the practical elements that could have a consequential impact on the development and subsequent success of the processes in the research. The second aimed to understand all of the respective practical's connected to measuring instruments and the applicability of these instruments are the probably result of the studies.

Two aspects of the pilot study are important. The first involves preparation for the main feasibility study or the carrying out of small-scale versions of full studies, whilst the second involves pre-testing of a particular research tool. Good pilot studies could also lead to an increase in the probability of success in the basic study (Claxton et al. 2005).

Pilot studies should suggest potential research failures, deviating or problems with tools or proposed models, and it is expected detecting the issues that may influence the research (Edwin et al, 2001).

A number of logistical issues may affect a pilot study. The following factors should be decided as part of the research strategy subsequent to commencing the main study: ensuring that the given instructions are followed by the investigators; ensuring comprehensive skills and procedures and the tools are operated correctly. The reliability and validity of results are checked. If a task is so difficult or so easy that it is likely to produce skewed results, a floor or ceiling effect may be detected. The pilot study may also specify early humane endpoints; intervention may be capped by measuring the level (*for example the dose of a drug*) and adverse effects (*pain, suffering, distress or lasting harm*) likely to be caused by the procedure and the efficiency of processes that could be used to reduce them (*for example analgesia dose rates and schedules*) to be investigated (NC3RS, 2006).

Logistical issues, information and data will most likely be incorporated with the main design of the study. The main aim of a pilot study is to assess the feasibility of an experiment. It rarely makes sense to display more than an outline of the statistics of the data. If problems with the methods are discovered the data might, in fact, be digressive (NC3R^S, 2006).

The pilot study should not result in the modification of tools or proceedings, with the result that the data collected may be adequate for the incorporation into the main study. The sampling strategy will be applied to choose the important topics and the changes that could occur over time; this must be considered carefully before incorporating pilot data into the study. However, if the pilot data was not utilized in this path or the final design varies markedly from the pilot, it is beneficial to contain all the information related to the pilot study in any reports or publications emerging from the main experiment as this should be stated in the design of future experiments (NC3R^S, 2006).

Pilot studies may be used to test the adequacy of research tools. Other reasons for their use are as follows: to evaluate the feasibility or quality of a (full-scale) study/survey; designing a research procedure; evaluating the research procedure whether it is realistic and practicable; or to determine if the sampling frame and technique are effective and adequate; or to evaluate the potential success of proposed methods; or to identify the difficulties of logistical that may arise via using the proposed methods; to determine sample size through estimating the variability in outcomes; or for collecting initial data and determining the resources (such as finance or staff) that would be required for a planned study; or to evaluate the proposed data analysis techniques to discover likely problems; or to formulate research questions and research plans; or to train a researcher as possible in as many components of the research process twelfth, or to show funding

bodies that the research team are experienced and educated; and lastly to demonstrate to the funding bodies or stakeholders the main study is feasible and merits funding and support (Edwin et al, 2001).

4.4 Advantages and disadvantages of the pilot study

This section covers the advantages and disadvantages of the pilot study. Advantages and disadvantages involve weighing the options to reach a conclusion. This section illustrates the main steps of a pilot study and further describes the advantages and disadvantages of pilot studies. Advantages and disadvantages were listed according to (MILES, 2013)

Table 4 Advantages and disadvantages of the Pilot Study

Advantages
<ul style="list-style-type: none"> • Brief trial study • Obtains the information required • May add to the results of the final survey • Improves the design • Provides sufficient data to decide whether to proceed with the main study • Resolve unanticipated problems • Allows any necessary alterations to data collection methods to be made • Allows the data in the main study to be efficiently analysed • Offers an opportunity to evaluate usefulness of the data • Allows primary testing of all hypotheses, which makes testing more accurate in the main study. Also, it might lead to some changes to the hypothesis or to some hypotheses being omitted or to the development of new hypotheses.

- Supplies the researcher with ideas and approaches that were not predicted. It develops the possibility of obtaining clear findings from the main study.
- Allows the overall the analytical procedures and planned statistical to be checked, giving a chance to evaluate their quality of the data.
- It minimizes the number of anticipated difficulties given the possibility to redesign parts of the study to deal with issues in the pilot study.
- May save a lot of time and money. It may help to reduce losses from ineffective and inefficient actions. It may be a feasibility study for the project.
- In the pilot study, the investigator may carry out a list of actions and afterwards choose the clearest results use in the main study.

Disadvantages

- The research design for the study is a structured study
- Success in the main study is not guaranteed
- Time-consuming

4.5 Interview Protocol

To guarantee the success of the research process, another procedure that is used is producing the interview protocol. Explanations of its aims, processes, and some of the structured data discussed with interviewees which are given below.

- Obtaining ethical approval.
- Agreeing a suitable time, date and location with interviewees.
- Providing an official letter from the university to the host organisation to describe the academic aims of the research.

- Explaining the aims of research for interviewees.
- Viewing a brief explanation about the research.
- Gaining the official acceptance to record the interview.
- Interview questions should be prepared.
- Translating the answers to interview questions from Arabic to English.
- Providing two people to validate the translation from Arabic to English.

4.6 Interview Procedure

One procedure that can be carried out to ensure the success of the research process is the interview protocol. Descriptions of its targets, procedure and some of the information discussed with interviewees are presented in the next paragraph.

This guide suggests a plan for the outline, layout and audience for the study. Prior to conducting the interview, participants were contacted by the researcher in order to agree a date and time for the interview. Data were gathered using semi-structured interviews as described in chapter 3 in section 3.7.1. Interviewees were notified of the purpose of the research and required to give their consent to participate in the interview. In addition, a consent letter was sent to the interviewees when explaining their rights regarding confidentiality and privacy and pseudonyms were used when reporting the results of the research.

Moreover, interviewees were asked by the researcher to give their permission to record the interview on a digital voice recorder and any decision taken by them was respected. If the interviewee did not consent to having their answers digitally recorded, answers were recorded by the researcher from memory after the conclusion of the interview.

The interviews were conducted in Saudi Arabia in one cycle from 2014 to 2015. The researcher contacted the interviewees and reminded them of the date and time agreed for the interview. Prior to each interview, the interviewees were given a summary of the research objectives and provided with a consent form to confirm that they had given their authorisation to be interviewed. They read and signed the form to demonstrate that they agreed with its substance.

The interviews conducted in Saudi Arabia were conducted in person in the interviewees' first language, Arabic, and were recorded using an MP3 recorder.

The content of the recording was subsequently transcribed into text form.

The participants that were included in the study were chosen through theoretical sampling in data collection from Glaser and Strauss method to reach to the aim of this research was to enhance the accuracy of digital forensics in cases where there was insufficient evidence.

Glaser states that purposeful and selective sampling differs from theoretical sampling. With purposeful or selective methods, the respondents are selected by the researcher at the start of the research. Research questions may be used to identify who is of interest for the research. However, in the theoretical sampling method in 3.8.6, respondents are selected during the research process (Glaser, 1967).

This research was based on the grounded theory method, which aims to show the understanding and explanation for the phenomenon rather than the generalisation produced as a result of quantitative studies that have comparatively large sample sizes. The use of a theoretical saturation technique (which is defined as a point in which

interview was performed several times but unlikely to reveal new information that hasn't emerged in the result of the past interview) led to the use of a small sample size.

4.7 Sample size of the pilot study and its justification

Strauss and Corbin (1990, 1998, p.292 (20) state that, "*Sometimes the researcher has no choice and must settle for a theoretical scheme that is less developed than desired*". Due to the sensitivity of the subject, the researcher selected two police officers in Saudi Arabia who were willing to participate in the interview. The two interviewees were selected on the basis of their knowledge of the research area.

Regarding to the data collection method that has been adopted and justified in chapter 3, the researcher build the interview questions based on the sub research questions which are: What is the process of investigation for digital crimes in Saudi Arabia? And "How does the Saudi Arabia investigation procedure handle cases with insufficient evidence?" that have not been answered yet. The number of interview questions that have been created depends on how the rich data the researcher wants to collect, and also based on the research questions to learn entire process of this study. In addition, the main aim of the pilot study is determine the necessary sample size and clarify the content of the questions.

Table 5 Pilot Study interview Questions

Questions	Purpose	Expected answer	Research question
1. What kinds of cases are investigated by Police Officers?	To determine the types of the cases.	Represent many kinds of cases such as drugs and theft.	What is the process of investigation for digital crimes in Saudi Arabia?
2. What types of drugs' criminal do you mostly faced?	To determine the type of drugs' criminal, drug abuse or Promotion.	There is varying of drugs' criminal known as drug abuse or drug promotion or both.	
3. How do you investigate drugs' abuse?	To determine the procedure which are used for investigation with both or severally.	The procedure which are used for investigation with both or severally.	
4. How can you deal with drugs' cases in which evidence is incomplete?	To see how the investigators deal with incomplete evidence.	The procedure which are used for investigation with incomplete evidence.	
5. How can digital devices be used to gain access to any available evidence which against suspects?	To determine the procedure in which used in drugs cases with availability of digital evidence.	The procedure in which used in drugs cases with availability of digital evidence.	How does the Saudi Arabia investigation procedure handle cases with insufficient evidence?
6. How did you decide that the investigations of such cases with incomplete evidence should be terminated? Please explain?	The researcher can find out the new technique for dealing with incomplete of digital evidence.	The mechanism that used it to terminate the cases which include incomplete digital evidence.	

The table above shows the pilot study interview questions that will help the researcher to reach the answer of sub research questions which mentioned above. Where the researcher aimed from questions 1, 2, 3 and 4 in the table above to get the full picture of the process of investigation for digital crimes in Saudi Arabia. Questions 5 and 6 will shows the researcher how the Saudi Arabia investigation procedure handles cases with insufficient evidence.

4.8 Empirical Study

Information gained by observation, experience, or experiment is caused empirical evidence. The main objective of a scientific method is that evidence found must be empirical and should be based on arguments. Scientifically, the word “*empirical*” refers to the use of a working state of a hypothesis that could be proven using observation or experiment.

The main objectives of the empirical study are to make observations in reporting and to combine large-scale research with case study details. Working in a real world environment can demonstrate the relevancy of theory and contribute to understanding and improving the environment.

There are three main reasons for using empirical study methods. Firstly, it avoids reliance on traditional knowledge. Secondly, empirical study methods help to integrate research and practice. Thirdly, educational processes need to move forward for example, developed training courses.

The advantages of using empirical methods include increasing understanding, to react more suitably to the dynamics of situations and to ensure respect for contextual

differences. By helping to build on what is already known the researcher may ensure that professional research can meet higher standards (Hani, 2009).

The two types of empirical study are experimental and non-experimental. Experimental interference can lead hypotheses to be changed to a series of variables of interest. Non-experimental study is when all subjects are noticed without experimental interference (Robergs, 2010).

The empirical cycle comprises of the following stages: observation, induction, deduction, testing and evaluation. Hani (2009) defines the empirical cycle as shown in the table below.

Table 6 Empirical study cycle

<ol style="list-style-type: none">1. Observation: includes gathering and organising the facts of empirical for forming a hypothesis.2. Induction: The process of bringing a hypothesis together.3. Deduction: Deduct outcome with newly gained empirical data.4. Testing: New empirical data test the hypothesis.5. Evaluation: Evaluating the outcome of testing
--

The main role of empirical study is to involve other arguments based on empirical research in order to refocus the argument. (Wallace, 2004).

4.9 Full study interview questions

After reviewing the pilot study results, it was found that some interview questions needed to be changed in order to strengthen the research and to better achieve its objectives. In addition, the pilot study provided a fuller picture of how to resolve the research problem.

The interview questions were changed from those used in the pilot study (shown in Table 7) to the full study questions shown in Table 8 in order to better meet the requirements of the research.

Table 7 Pilot Study interview Questions

Question	Purpose	Expected answer
1. What kinds of cases are investigated by Police Officers?	To determine the types of the cases.	Represent many kinds of cases such as drugs and theft.
2. What types of drugs' criminal do you mostly faced?	To determine the type of drugs' criminal, drug abuse or Promotion.	There is varying of drugs' criminal known as drug abuse or drug promotion or both.
3. How do you investigate drugs' abuse?	To determine the procedure which are used for investigation with both or severally.	The procedure which are used for investigation with both or severally
4. How can you deal with drugs' cases in which evidence is incomplete?	To see how the investigators deal with incomplete evidence.	The procedure which are used for investigation with incomplete evidence.
5. How can digital devices be used to gain access to any available evidence which against suspects?	To determine the procedure in which used in drugs cases with availability of digital evidence.	The procedure in which used in drugs cases with availability of digital evidence.
6. How did you decide that the investigations of such cases with incomplete evidence should be terminated? Please explain?	The researcher can find out the new technique for dealing with incomplete of digital evidence.	The mechanism that used it to terminate the cases which include incomplete digital evidence.

For example, the first question in the pilot study was changed in order to obtain a specific answer from the drugs investigators and to determine the different types of drugs cases. Moreover, the third question was changed to that shown in Table 8 in order to better determine the procedures used for investigation. Furthermore, Question 7 was added (see

Table 7): “What steps help you to find additional intelligence or digital evidence?” in order to obtain a better and more understanding of the linked reasons.

Question	Purpose	Expected answer
1. What categories of drug’s cases are currently being investigated?	To determine the different types of drugs cases.	Representation of many types of drugs’ cases.
2. What are the most common crimes that you encounter?	To determine the different types of drug related criminals, drug abuse and/or promotion.	There are different types of drug criminals, drug abuse and/or drug promotion etc.
3. What procedure do you follow to investigate these crimes?	To determine the procedures that is used for investigation.	The procedure that is used for investigation.
4. Are you able to deal with those cases which have incomplete evidence? If so ... how?	To see how the investigators deal with incomplete evidence.	The procedure which is used for the investigation of cases with incomplete evidence.
5. Do you use digital evidence in these investigations? If so ... how?	To determine the procedure which is used in drugs cases regarding the use of digital evidence.	The procedure which is involved in drug cases through the use of digital evidence.
6. How do you decide whether to continue or stop an investigation if there is insufficient or incomplete evidence?	The researcher can determine the new technique for dealing with incomplete digital evidence.	The mechanism that is used for terminating the cases involving incomplete digital evidence.
7. What steps help you to find additional intelligence / digital evidence?	To gain an understanding of the associated reasons.	

Table 8 Full Study interview Questions

4.10 Justification for the selected sample of interviewees

It was not assumed that six interviews would necessarily be sufficient to meet the research objectives or to use the above findings above to justify “quick and dirty” research. Morse’s (1994) recommendation for phenomenological studies is consistent with the six interviews. For qualitative studies in technology usability, analogical evidence-based recommendations may be used. Six interviews may be enough to include the development of significant themes and to provide useful explanations. Guest et al. (2005) argued that over 73% of codes can be obtained from the first six out of a total of 30 interviews. The small number of participants is necessary to ensure an understanding of the phenomenon of interest. The question arises of whether six interviews, for example, would provide as much useful information as could be gained from 12, 18, 24 or 30 interviews (Guest et al. 2005). The rate of code application after each set of six interviews was also added. From one site, one code in the first round of analysis was used for all six of the transcripts, leading to high prevalence across participants. In the other 24 transcripts, the same code was never repeated. Another code appeared for the first time in the seventh transcript by applying it to the other 24 transcripts (Guest et al. 2005).

Six interviewees therefore provided more than 73% of codes; if the number of interviewees increased, the number of the codes must be reduced in order to avoid saturation. One of the advantages of grounded theory is that the data can be tested for saturation at the time of data collection, as data saturation means that no new data has been produced.

In addition, Strauss and Corbin (1990), Mores (1994) and (Guest et al. 2005) state that six interviewees may be enough to include development of significant themes and to provide useful explanations.

Postgraduate students may encounter difficulties in this area. Strauss and Corbin (1990-1998) described the 20 most commonly posed questions in their seminars and classes. An example question is “*How many interviews or observations are enough?*” and “*When do I stop gathering data?*” Strauss and Corbin (1990 p.292 state that, “*Sometimes the researcher has no choice and must settle for a theoretical scheme that is less developed than desired.*” This answer outlines the concept of saturation, including the availability of participants, time and energy.

The reasons and categories of individuals selected for interview are as follows:

1. Due to the sensitive nature of the topic, only drugs investigators were deemed to have adequate information related to drug cases.
2. The study aimed to gain an in-depth understanding of the mechanism associated with the investigation of drug issues.
3. The study aimed to explore the depth and richness of the subject in order to address the complexities of the research question.
4. The data were further enriched by undertaking a number of interviews before analysing the data.

4.10.1 What is a Stakeholder?

This study examines the meaning of the term stakeholder by reviewing some of the existing institution and scholars’ definitions. Stakeholders are defined by the Standard Research Institute (SRI) as “Those groups without whose support the organization would

cease to exist”. Stakeholders are also defined by Freeman in 1984 as “Any group or an individual who can affect or is affected by the achievement of the organisation’s objectives”, and Friedman in 2006 supported this definition of a shareholders. Therefore, in the following section the researcher will identify the stakeholders that were chosen for this study.

4.10.2 Who are the Stakeholders?

The stakeholders for this search were identified by the researcher are drugs investigators from the Bureau of Investigation and public Prosecution in Saudi Arabia, which established in 1989 for providing security and justice in all parts of Saudi Arabia. The participants were allocated individual codes to make it easier for data analysis and more understandable for the reader, as shown below:

INV1: Drugs investigator and Public Prosecutor

INV2: Drugs investigator and Drugs Enforcement Detective

INV3: Drugs investigator and Head of Personal Attacks Circuit

INV4: Drugs investigator and Head of General Criminal Circuit

INV5: Drugs investigator

INV6: Drugs investigator

INV7: Drugs investigator

INV8: Drugs investigator

4.11 Conclusion

This chapter discussed the process of data collection. It began discussing with overview of pilot study. And was discussed the sample size of the pilot study and its justification. The chapter discussed the empirical study question, interview questions and justification for the selected sample of interviewees for empirical study. This chapter designed to be the basis for data collection, which is covered in the next chapter.

Chapter 5:

Research analysis finding and discussion

Objectives

-
- To present the research analysis finding and discussion
 - To highlight research contribution
 - To present the proposed framework
-

5.1 Introduction

This chapter addresses the findings and discussions from the analysis of the data from drugs investigators. The methodology defined by Strauss and Corbin (1990) has been used, as detailed in chapter 3. The analysis process includes three stages: open coding, axial coding and selective coding. These processes are discussed below. In open coding, the interviewer using the constant comparison method, using theoretical sampling and memos to categorise the similar codes that emerged from one category by comparing the codes with each other until the point was reached where no new concepts emerged and saturation had been reached. When the axial and selective coding stages were applied, categories were re-categorised through the use of the paradigm model to show the themes which represent the core categories.

The categories and concepts that emerged during the application of the open coding procedure, which are based on the properties and dimensions of the codes, will be discussed in the following sub sections.

In addition, this research revealed the attitude of investigators in drugs investigations towards the procedure which led to a reduction in the concerns about not reaching the required levels of accuracy in the investigation process. This became clear when the findings showed that the attitude of the investigators have an effect on the investigation. Moreover, many researchers seek out to enhance the digital investigation process for reaching to the accuracy of digital investigation, amongst them are (Al-Murjan and Xynos, 2008; Yusoff, Ismail and Hassan, 2011 and Hong, Yu, Lee and Lee, 2013);

whereas, they do not refer in their investigation processes to any phase to deal with the cases that have incomplete evidence.

5.2 Open coding

Five categories were identified in the open coding stage of the drug investigators' replies. Each category will be discussed in detail in the following subsection. The categories are grouped under a heading according to their properties and dimensions. The categories that emerged are: drug cases, drugs investigation procedure, drug's investigation procedure in cases where there is insufficient evidence, digital evidence and the final category called decision, which will be discussed in the following sub-sections.

1. Drug cases

An analysis of relevant studies carried out in Saudi Arabia to enhance the accuracy of digital forensics in the absence of complete evidence yielded the following categories relating to drug cases: Smuggling, Promotion (drug's Transport, Drug Sale, Drug Buying and drugs given freely as a gift), Drug Use, Possession (Possession for supply, Possession for Use and Possession in the abstract (without any intent)) and Facilitating Trafficking and Dealing.

When the researcher asked the participants about the current cases being investigated the cases that they mentioned all fell within the categories mentioned above. The categories are interrelated, that is, drugs which enter the country through smuggling are then received by the person who will sell or supply the drugs to drug users, who will then therefore be the persons in possession of the drugs. The Saudi Head of the Investigation Department, within the Investigation

and Prosecution Authority, who participated in the study, stated that the above categories capture the most common drugs related cases:

“The categories of drug cases being investigated currently are: smuggling cases; drug promotion cases and using and possession cases.” INV1

The smuggling cases referred to by INV1 refer to the fact that drugs enter the country illegally through state land borders, ports, or airports. INV2 agreed with INV1 on the common types of drug cases and provided more detail about the methods used for smuggling:

“Smuggling cases involve two methods: either smuggling through a land border or smuggling through Saudi airports. Cases involving smuggling through Saudi airports are very simple cases involving 20 to 30 pills, usually for personal use. Saudi Customs look for drugs in places where they are commonly hid, either in cars or in a suspect’s personal belongings. These are the most common incidents we face in drug smuggling through Saudi ports.” INV2.

Participant INV4 spoke about the question of intent in smuggling cases:

“Smuggling is intended. It means transporting drugs across the borders of Saudi Arabia through any port, e.g. land port, airport or seaport. This crime is most commonly referred to as import smuggling.”

The smuggling of drugs occurs across a border where there is a recipient. The recipient and the smuggler are both classified as smugglers. There is smuggling through reception and smuggling through entering and, of course, smuggling for using and smuggling for the purpose of trading. Of these, smuggling for trading is the most common. The intent of smuggling can be identified by quantity. When suspects are in possession of 2 or 3 pills it is clear that they are smuggling for the purpose of using and the suspect is always released in this case. However, if a suspect is caught with a 1000 or 500 pills or half a kilo of hashish or opium, i.e. a quantity that can be measured in kilograms, the purpose for smuggling.” INV4.

The mere entry of drugs into any country means that there is a receiver for the drugs, who in turn would be selling or supplying the drugs, therefore implying that the drugs are distributed by the receiver to customers.

INV2, who is an investigator with the Investigation and Prosecution Authority Department in a border region city of Saudi Arabia, pointed out that the promotion of drugs cases can be further split up into promotion of drugs through Transport, Sale, Buying and through the Gift categories:

“Drugs cases being investigated now are simple possession cases, promotion cases and drug smuggling cases of all kinds, whether through promotion, transportation, sale or purchase or by gifting.” INV2.

Participant INV4 agreed with Participant INV2 on the categorisation of drug cases and added that the Sale of drugs is the most common category:

Promotion has many forms. Promotion through sales is the most common; there is also promotion through transport, i.e. transporting the drugs from one place to another place, for example, from city to city. Drugs can also be promoted by gifting. INV4.

Finally, possession of drugs cases were referred to by Participants INV1, INV2, INV3, INV4 and INV6 as being one of the most prevalent types of cases facing drugs investigators. INV2 stated that possession of drugs cases in his region included possession of Marijuana and Amphetamine pills:

Simple possession cases are now popular and widespread throughout the region. Often possession involves weed or Amphetamine pills. INV2

Participant INV3 elaborated upon the categories of possession of drugs cases, which are Possession, Intent to Use and Possession with Intent to supply:

“Drug cases are currently being investigated, and include all kinds of smuggling, promotion, use and possession, intent to use, possession and intent to promote all categories. There is also possession and unintentional promotion, transfer or dealing, but there are only rare impacts from such these cases” INV3

Participant INV4 added Possession in the Abstract (without any identified motive) to the categories listed by INV3 in possession cases:

“Drug cases fall into three categories: possession, (2) promotion, and (3) smuggling. Possession can be of more than one type: (i) possession for promoting, (ii) possession for use, and (iii) possession in the abstract. Some suspects, when asked by an investigator, admit possession. When asked about the reason for this, the suspect does not give a reason. This situation is called possession in the abstract and is often applied when someone has drugs in their keeping, either for use by a friend or an abuser who has asked the suspect to keep the drugs.” INV4.

Participant INV5, who is a drug investigator, added Trafficking or Dealing and Facilitating to the list given by the other participants:

“Trafficking or dealing and facilitating – both.” INV5.

In summary, the participants agreed on the categories of drug cases identified through the literature (CARJJ, 2012), and added further detail to some types of cases such as smuggling and possession. They also added the factor Trafficking or Dealing and Facilitating (INV5). The categories of drug cases are interrelated and this affects the investigation process as the investigators must understand and deal with all relevant factors in a case. This research agreed with (Gabe, 2010) that consideration of the issue of special legislation to combat cybercrime in the Kingdom of Saudi Arabia needs to be addressed as a matter of some urgency. The global drug trade is linked to gangs and organisations through the internet which can now provide a communications network via instant messaging, forums and

encrypted rooms etc. that can avoid detection (Alshehri, 2010). As a consequence, there is some concern regarding the issue of not being able to obtain sufficient evidence.

2. Drug investigation Procedure

The participants revealed that there are a number of factors which have to be considered when dealing with drug cases. These factors support the proposed model which will deal with cases where there is insufficient evidence. When the participants were asked by the researcher about the investigation procedure which is currently used in drug cases they mentioned that there were several stages involved in the procedure, namely: arresting the suspect, studying the case, studying the accompanying paperwork, preserving relevant devices, ensuring the security for equipment's which were seized, evidence collection, investigation, interrogating the suspect, confronting the suspect's evidence, having the suspect face the charges against him, seeking to contribute by asking questions, presumptions, processing the chemical report, researching whether the suspect has a history with drugs, looking at any relationships with other cases, looking for evidence, confession, gathering information, previewing any items which has been seized, tracking emails, tracking phone messages. The Head of the Investigation Department, Participant INV1 referred to the drug investigation procedure based on the investigation process:

“Of course, the procedures followed include studying the case proceeding from the drugs officer or arrest team that has taken control of the investigation and

evidence collection and the arrest. We then start studying the documents that come with the suspect, questioning the suspect and confronting the suspect's evidence, as presented by the arresting team. After questioning and confronted him/ her with the evidence, we decide to arrest or release him/her, depending on the law, and then to deal with the case, either by transference of the case to the court or preservation of evidence. These procedures are typical with all drug cases” INV1

Participant INV1 gave details of the investigation process used in drug cases, from arresting the suspect to taking a decision on how to deal with the case. The participant, who is himself an investigator, referred to specific reasons why some case proceedings are preserved:

“Case proceedings are preserved for specific reasons. For example, insufficient evidence, or specific circumstances associated with the person who committed the crime. These are only for drug use crimes. The circumstances include, for example, the fact that the suspect is of a young age; the fact that it is the first time that the suspect has used; small quantity of drugs seized and avoiding charging the suspect in order to preserve the person.” INV1.

Participant INV2 added to the points made by INV1. He said that the investigation process in their department relies on the information which is provided by the arresting department:

“The arresting department listens to the suspect before coming to the point of the investigation; when the suspect comes to the investigator, the suspect faces the

charge against him. Therefore, we contribute by asking questions that will help us to find the method used for smuggling drugs based on existing evidence and presumptions and recordings related to the case. In cases where the suspect denies the charges, we present existing evidence to them.” INV2.

Participant INV2 referred to another method of investigation if there is no information provided:

“We wait for a chemical report on the suspect’s sample to be returned as positive or negative. We might get some information about the suspect’s involvement in previous actions – i.e. has the suspect been arrested in a drugs case previously, or does she/ he have a history with drugs. Seek out the suspect’s relationship with other cases ...” INV2.

Participant INV3 agreed with INV1 and INV2’s information on how to investigate drugs cases. However, INV3 pointed out that 98% of drug cases are where the suspect is caught in flagrante delicto:

“Usually, drugs cases are in flagrante delicto cases, where the suspect is arrested 98% in flagrante delicto. The procedure used is to investigate the suspect and face him while making a police recording. You can also investigate ways of looking for evidence with the suspect. The evidence in drug cases is mainly in the police record, often a confession because the suspect was arrested in flagrante delicto. However, in some cases there is incomplete evidence. It starts with the interrogation of the suspect by asking him questions: why was he arrested? If the suspect has confessed the case will end. But if the suspect does not confess, the

suspect will be faced with the recording registered by the police, or asked questions, for example, where were you? Then we take down this information.”

INV3

Participant INV4 referred to strategies used in the investigation of drug cases which were not mentioned by INV1, INV2 and INV3 and described the kind of evidence gathered in such of drug cases:

“The suspect faces an arrest record. As is well known in customs rules, every person is responsible for what they have in their possession. The arrest record shows possession, whether the item is in his pocket, his clothes, his bag, or his car. Promotion cases are often arranged by prior sale; that means the criminal investigation focuses on the management of anti-drug strategies. Information is gathered from private detectives and counter-narcotics in the search for promoters. This involves pushing a confidential source to name the promoters. These confidential sources may be citizens, collaborators, or anti-drug personnel.... This is the most common case of promotion that we might face. I check a suspect in the arrest record; the arrest record should be fully completed and include evidence such as communication evidence or evidence which proves that this is his house ... certified evidence, that is the strongest evidence in Islamic law. There are other forms of evidence, such as mobile evidence, money numbered by the government and a car...” INV4.

When participants INV1, INV2, INV3 and INV4’s responses were compared with INV5’s, it was found that the responses differed according to their experiences.

INV1's response regarding the procedures used focused on "studying the documents that came with the suspect, questioning the suspect and confronting the suspect's evidence"; INV2 mentioned "seeking to contribute by asking questions"; INV3 highlighted that people involved in drug cases are often caught in flagrante delicto and INV4 based his responses on his investigation of the suspect's arrest record. INV5 gave details about the procedure which has a number of sequential steps and is comprehensive. His responses are not inconsistent with the other participants' responses, as can be seen by this response:

"Drug cases come to us as investigators usually from the General Directorate for Drug Control and then we follow the procedure described, that is, study the case, study the accompanying paperwork and preview anything seized with the case and ensure the safety of seizures and the suspect's situation and health examination documents, question the suspect, confront the suspect with evidence presented against him by the arresting Department and then detain or release the suspect based on the law. The case is then referred to public prosecution, which in turn transmits details of the suspects and the case to the Court." INV5.

INV6's responses did not differ from the previous participants' responses with regard to the investigation process. INV6 stated that the investigator's task is to confront the suspect with the evidence which is found by the Anti-Drugs Department or gather more information when this is lacking:

"The anti-drugs department is responsible for drugs cases initially and they arrest the suspect. There are arrest records that show all circumstances of the case and show the evidence in detail. After this, the arrest record provides information

about the investigation and the suspects; the investigator confronts the suspect with the evidence that was found and was recorded in in the arrest record. After which, the investigator decides to re-file the case, show it to the police to gather additional evidence in cases of insufficient evidence to convict the suspect; close the case or send it the court to convict the suspect if the evidence is sufficient. The investigator closes the cases in instances where the amount of drugs is small. There may also be other circumstances to consider, such as if the officer who arrested the suspect made a mistake, or it is not possible to complete evidence... and there are other things, such as approval by investigators.” INV6.

Participant INV2 also spoke about digital means of investigation such as tracking emails and phone messages:

“Tracking emails and phone messages.” INV2

These emergent codes are categorised under the Investigation Procedures in Drug Cases which agree with the drugs’ investigation procedures that are proposed by researchers, such as (Pollitt, 1984) (Al-Murjan and Xynos, 2008 and Yusoff, Ismail and Hassan, 2011) because of the relationship between the codes, their properties and dimensions.

3. Drug’s investigation procedure in cases where there is insufficient evidence

In the open coding phase and the breaking down of data phase it was found that the concerns regarding cases with incomplete evidence are influenced by shortcomings in the investigation procedure used for investigate drug cases. The

participants spoke about their experiences in cases where there was a lack of sufficient evidence. Participant INV1 stated that in cases where the evidence is not complete there is a requirement for greater effort:

“Of course, there are cases that have incomplete evidence; therefore, the investigator should make a greater effort in these cases, more so than in the cases that have complete evidence. If there is incomplete evidence, we often seek to build new evidence. That means extracting evidence of acts committed, or examining a person’s circumstances or the reality of the situation, so that the evidence might be weak, but it will be strengthened by new presumptions or new evidence that will back the weak evidence. No, the investigator should search for evidence to complete the other evidence, or end the investigation if there is not sufficient new evidence.” INV1.

INV1 pointed out that the cases which do not have sufficient evidence need more effort than cases that have sufficient evidence. In his response INV1 relayed his experience and reflected his personal opinion that the investigation should not end if there is not sufficient new evidence; rather the weak evidence should be strengthened via new presumptions or the gathering of new evidence.

Participant INV2 agreed with INV1 on the point of looking for new evidence in cases that have insufficient evidence. In addition, INV2 suggests basing the investigation on the suspect’s previous record to find more information about the case:

“Some cases come to us with incomplete evidence; we try to look for new evidence. As I mentioned previously we try to research the suspect’s previous history Modern digital devices can now help us acquire information.” INV2.

In agreement with Participant INV2’s response, INV3 mentioned using the police records about the suspect in the police database to find additional evidence. INV3 also agreed with the INV1 statement that cases which have insufficient evidence require time and patience:

“Cases that contain incomplete evidence require time and patience. Even where the evidence is incomplete you start questioning, how and why, especially in promoting cases. Consider why this person is being observed. Did the police target him and are there written reports about him? Have the police recorded some issues in the past? Start looking for information about the suspect. Sometimes you find previous reports and previous records about the suspect from other police teams and find he was an observer and there is a report about him ...” INV3.

In addition, INV3 gave more details about strengthening the charges against the suspect that were not stated by INV1 and INV2:

“We collect a large number of presumptions. For example, if there is a suspect, we will collect information about his mobile phone communications and take a

certificate of 9 or 10 people who sign the arrest record and purchase thus gathering several presumptions to strengthen the charges against the suspect..."

INV3.

Moreover, INV3 based on his experience and understanding added a point based on his understanding which was not stated by either INV1 or INV2, that is that more than the majority of drug cases are where the suspect is caught in flagrante delicto:

"the majority of drug cases are in flagrante delicto cases. Very few drug cases have ambiguity or incomplete evidence..." INV3.

Participant INV4 did not totally agree with INV1, INV2 and INV3's responses about such cases. He is of the view that cases in which there is insufficient evidence are rare:

"Incomplete evidence is a rare occurrence in drug cases. Yes, I can deal with cases that contain digital evidence but this is rare because drug cases are 98% or 99% in flagrante delicto cases..." INV4.

Participant INV5's response does not differ greatly from INV1, INV2, INV3 and INV4's responses. INV5 highlighted the technique which is used in this kind of case which is to gather preliminary inferences about the case and link the events and facts with the words of the suspect and his health condition:

“We gather preliminary inferences about the case, and in the absence of complete evidence we link the events and facts with the words of the suspect and his health condition” INV5.

INV6 did not add anything new to the previous participants’ responses but did point out that there is a Department that specialises in gathering evidence in cooperation with the arrest team:

“There are parties and sections that specialise in gathering incomplete evidence in cooperation with the arrest team” INV6.

The codes which emerged are categorized under the drugs investigation in cases where there is insufficient evidence because of the relationship between codes and their properties and dimension which are not covered in the previous research such as (Al-Murjan and Xynos, 2008), (Hong, Yu and, Lee, 2013) and (Pilli, Joshi and Niyogi, 2010). The investigators’ responses regarding their concern about providing information in cases which have insufficient evidence indicates that the investigation process which is followed by the investigators because there are no procedures for dealing with such cases, as the investigators’ responses are based on their experience in dealing with such these cases. Hence, all factors interrelate to contribute to complete evidence in such cases.

4. Digital evidence

Most members of a community use technology in their daily communications; thus this technology is used in some cases to commit crimes. When the researcher

asked the participants to talk about digital evidence in drug cases which are being investigated they identified many types of digital evidence. A digital device serves to facilitate many drug related acts; some people even resort to promoting drugs through websites, social networking programs and chat rooms. Participant INV1 stated that digital evidence in drug cases is commonly gathered from messaging applications which are used in smart phones or the data which is provided by cameras for monitoring traffic and those monitoring banks or shops:

“Of course, digital evidence in the form of a voice or image, etc. The problem with digital evidence is that most of the community members who handle digital crimes have not reached the stage of using technology to commit crimes, but they do now use handheld devices, such as smart devices. Smart devices can be used for messaging through messaging programs. And we can get evidence from them and possibly use techniques that exist, such as the Saher system, which is a camera for monitoring traffic violations. However, there may be a drug related incident committed at a site near to or in front of the cameras that are for monitoring or controlling cameras for tracking banks or shops. Where these cameras are used as evidence it is also necessary to preview the site and make sure it is possible to determine if the crime took place...” INV1.

INV1 spoke about the promotion of drugs through websites or social networking programs or chat rooms:

“There are some people who are resorting to the promotion of drugs through websites or social networking programs or chat rooms (chatting) but these people are rare”. INV1.

INV2 spoke about emails as a form of digital evidence mentioned by INV1:

“The consignment office stated the consignment was sent by a person named John Doe and that the person was unknown to the office. We checked that all the emails had arrived at the office; many emails were sent from a specific email to the office’s email and there was just one person who answered the emails from the office. This gave us an indication that a consignment would arrive at this office.”

INV2.

Adding to INV1’s response, participant INV3 spoke about video clips, messages and photos as digital evidence:

“In a drugs case, the Anti-Drugs Department was able to access the drugs through a video clip. The suspect was arrested using this video clip, although there was no charge against him, but this video clip condemned all the people in the group who were with him...” INV3.

INV4 did not add anything new to INV1, INV2 and INV3’s responses about digital evidence but agreed that the suspect’s phone communications and photos form part of the digital evidence gathered:

“When searching one of the suspect’s phones a picture was found of him with the seized quantity, holding it as a kind of prize. Thus, digital evidence proved the suspect’s ownership, because he had implicated himself with the image...” INV4

In agreement with INV1, INV2, INV3 and INV4’s responses INV5 highlighted the fact that all that is included in digital devices such as telephones and tablet computers contribute to digital evidence:

“Yes, the using of digital evidence in most cases is inevitable, because the reality in which we live is not free from digital devices such as telephones and tablet computers and geographical locations and many other systems. Therefore, and from this standpoint, when any operation or raid takes place, we preserve such devices for use in the case, as they may be a key point in the investigation.” INV5.

INV6 spoke about the communication between the suspects, and he agreed with previous participants’ responses:

“Yes, because in light of the evolution of modern technology, computers and smart phones can do everything. Meanwhile, criminals exploit technology to commit their crimes, such as trafficking drugs and promotion. The criminals use these devices to communicate with each other” INV6.

Based on the participants' responses, digital evidence comprises video clips, photos, phone records and text messages. Because digital devices are so prevalent, drug cases often rely on digital evidence which is especially useful in investigations there is a lack of sufficient evidence.

5. Decision types

A number of factors which could be grouped under this category are related to the decisions taken by the participants emerged from their responses. The differences between the types of decisions made are based on the participants' view of the cases which they are investigating. The decision to be made centres on whether to continue or end the investigation depending on the evidence:

“Continue or end the investigation depending on the same evidence. There might be available evidence in the initial phase. This either suggests the conviction that a suspect is the perpetrator of a crime, but if evidence surrounding an incident is weak, the investigator will require more effort and collaboration from people surrounding the investigator, using a procedure of search, investigation and adjustment of certain sites and inspections, including digital devices including mobile phones. If an investigative path is closed from the beginning, or evidence is locked away, or no evidence is produced, I will end the investigation.” INV1.

Participant INV2 agreed with INV1's statement that the investigator is responsible for the full case and bases his decision to continue or stop the investigation on strong signals or evidence about the suspect:

“I am as an investigator responsible for the full case. Sometimes the case requires evidence that is not attainable. Sometimes, there was strong evidence about a suspect who had some drugs, but it is discovered during the investigation that this person is not the right person; or the case against him or charge is wrong. In this case, I decide as an investigator based on strong signals or strong evidence that is evident to me during the investigation, to stop the investigation or review the search and look for another suspect, if I have realised that the suspect is not related to the case.” INV2.

On the other hand, Participant INV3 reported that his decision on whether to continue or stop the investigation was dependent upon the police record of the suspect:

“If the police record is strong about a suspect, I continue the investigation...”
INV3.

Participant INV4, in line with INV1, INV2 and INV3’s responses, bases the decision on whether to continue or stop the investigation on the circumstances of the case:

“In drug cases, I can stop the investigation if there are no drugs seized. If there are drugs the case continues...” INV4.

Furthermore, the participant mentioned that the investigator cannot take any decision before the case has been completed and is clear. INV5's response on how an investigator decides on whether to continue an investigation did not differ from the responses of participants INV1, INV2, INV3 and INV4 but he makes a new point regarding the way the decision is made:

“We will not open any formal communication before the investigation conditions are completed; that is prescribed by the legislature. The police will not collect inferences except in the form of a complete communique or a complete and clear case.” INV 5.

Participant INV6 disagreed with the other participants with regard to the closing of investigations. In his experience all unresolved cases remain open:

“It does not stop the investigation, but the case remains open and the reason for this is that most of the drug cases are related with each other.” INV6.

The participants' responses indicate that the decision on whether to pursue an investigation is taken by the investigator as the investigator is fully responsible for the case which is being investigated by him. Hence, the investigator's knowledge and experience are the main factors which will impact the decision. Therefore, an appropriate decision could be reached by following a comprehensive procedure that will deal with all kind of cases proposed by the researcher in order to achieve the accuracy of the investigation.

5.3 Axial Coding

In this phase of the analysis process connections are made among the categories which emerged from the open coding stage (Strauss and Corbin, 1990). In the axial coding phase, the number of categories reduced by comparing and re-categorising similar categories under one category using the paradigm given in Figure 15 which encompasses the causal conditions and different action/interactional strategies and consequences for the same phenomenon. The paradigm presents the relationship among the categories identified in open coding. Two categories were produced from the axial coding which have been named:

1. Investigation Procedure in Drug Cases.
2. Investigators' experience with insufficient evidence.

This was done after applying axial coding procedure, below is an example of using paradigm model in axial coding and show how the two mentioned categorise were produced.

5.3.1 Investigation Procedure in drug's cases

Conducting the investigation in drug cases is the central idea of the first category which comprises three causal conditions: drug case, Investigation and Presumptions. The causal condition is identified by dimensions and properties and can be found by looking through the data for events that seem to precede the phenomenon.

A. Causal Conditions

- Drug case
- Investigation
- Presumptions

The factor drug case leads to an occurrence of the phenomenon and this factor is considered to be significant in the emerged data. . One participant INV1 confirmed a casual condition by saying:

“The categories of drug cases being investigated currently are: smuggling cases; drug promotion cases and using and possession cases.” INV1.

In addition to that another participant also stated that “drug case” is a casual condition confirmed by INV2 for conducting investigation in drugs case by saying:

“Drugs cases being investigated now are simple possession cases, promotion cases and drug smuggling cases of all kinds, whether through promotion, transportation, sale or purchase or by gifting.” INV2.

Therefore, all participants agreed in their answers that factor “drugs case” is a cause or reason for the phenomenon. Some of them added some details in their answer, for example, INV4 added more details about the type of possession cases as he said:

Drug cases fall into three categories: possession, (2) promotion, and (3) smuggling. Possession can be of more than one type: (i) possession for promoting, (ii) possessing for use, and (iii) possession in the abstract.

Another participant INV2 confirmed “Investigation” to be another casual condition to conduction the investigation in drug case. This factor is one of the events that lead to the occurrence and development of the phenomenon by seeking to contribute to find the method used for the cases as INV2 said:

“We are seeking to contribute by asking questions that will help us to find the method used for smuggling drugs, based on existing evidence and presumptions, and recordings of the case.” INV2.

Presumption (unusual behaviour) was identified as another causal condition which leads to the occurrence of the phenomenon. For example, INV1 alluded to the impact of presumption to conducting the investigation as follows:

“So that the evidence might be weak, but it will be strengthened by new presumptions or new evidence that will back the weak evidence.” INV1.

B. Phenomenon

Secondly, phenomenon defines “the central idea which a set of actions/interactions is directed at handling” (Chisnall, 1998). The phenomenon in this category is:

- Conducting the investigation in drug cases

C. Context

- Email.
- Phone messages
- Pictures
- Communications
- Whatsapp messages.
- Twiter messages
- Social network
- Video
- GPS for phones.
- Chat rooms (Chatting).
- Voice

Thirdly, context is “the particular set of conditions within which the action/interactional strategies are”. Eleven factors emerged from the participants’ responses based on their properties and

dimensions which are; email, phone messages, pictures, communications, WhatsApp messages, Twitter messages, social networks, videos, GPS for phones, chat rooms and voice. Hence, it is possible to say that Investigation Procedure in Drug Cases is essential when this set of conditions (factors) arises. Some examples taken from the participants' replies take into account the impact on a phenomenon in terms of voice, message and picture on the phenomenon; as INV1 said:

“Digital evidence in the form of a voice or image, etc. The problem with digital evidence is that most of the community members who handle digital crimes have not reached the stage of using technology to commit crimes, but they do now use handheld devices, such as smart devices. Smart devices can be used for messaging through messaging programs. As we can get evidence from them, and possibly use techniques that exist, such as the Saher system, which is a camera for monitoring traffic violations. However, there may be a drug related incident committed at a site near to or in front of the cameras that are for monitoring or controlling cameras for tracking banks or shops. Where these cameras are used as evidence” INV1.

INV3 claimed that the phenomenon “Investigation Procedure in Drug Cases” is influenced by the video as the evidence of the crime, as said:

“In a drugs case, the Anti-Drugs Department was able to access the drugs through a video clip. The suspect was arrested using this video clip, although there was no charge against him ... There is a lot of evidence, i.e. messages and photos” INV3.

In addition, INV1 argued that chat rooms and communication through social networks may affect the phenomenon of the investigation procedure in drug cases, as he said:

“Let me say as the best context: there are some people who are resorting to the promotion of drugs through websites or social networking programs or chat rooms (Chatting) but these people are rare.” INV1.

D. Intervening Conditions

- Have a history with drugs.
- Electronic purchase and sale.
- Health report of the suspect.

Next, intervening conditions which is “the structural conditions that affect the action/interactional strategies that are relevant to the phenomenon” (Chisnall, 1998).

These intervening conditions may affect the investigation procedure in drug cases, because such conditions can contain technology, economics, time, culture, space and history and individuals. INV2’s response refers to the suspect’s history with drugs. A participant, INV2, affirmed that the suspects history with drugs is one of the conditions that may also affect the phenomenon, as said:

“Wait for a chemical report on the suspect’s sample to be returned as positive or negative. We might get some information about the suspect’s involvement in previous action – i.e. has the suspect been arrested in a drugs case previously, or have a history with drugs. Seek out the suspect’s relationship with other cases ...” INV2.

Based on the participant’s response that online purchases and sales impact on investigation procedure in drug cases, because it encouraged the criminals to adopt the online transactions to do their activities, as INV1 said:

“There is a process of online purchase and sale that means receiving banned pharmaceuticals including drugs or medications that are psychotropic, where these drugs are available in other countries so the suspect is able to communicate with a supplier to receive the goods from a courier company (shipping).” INV1.

INV5 supported all the previous participants’ views, as related to influence of the investigation procedure in drug cases, when he pointed out the health report of the suspect, as he said:

“Drug cases are given to us as investigators usually from the General Directorate for Drug Control and then we follow the procedure described, study the case, study the accompanying paperwork and preview anything seized with the case, and ensure the safety of seizures, and the suspect’s situation and health examination documents, question the suspect...” INV5.

E. Strategies

- Judiciary

Fifthly, “Action/Interaction: strategies devised to handle and respond to a phenomenon under a specific set of perceived conditions” (Chisnall, 1998).

The strategies can be identified through cues in the data. The strategies to handle the phenomenon under a certain set of conditions and the strategies which manage the phenomenon will have consequences (Strauss and Corbin, 1990). Hence, the strategy is represented in the judiciary, where it is an action in response to the information to reach the results of the investigation in drug cases. For example, this strategy which is taken under a set of conditions to handle and to respond to a phenomenon, as the participant INV4 saying:

“The judiciary judges any suspicion. INV4.

F. Consequences

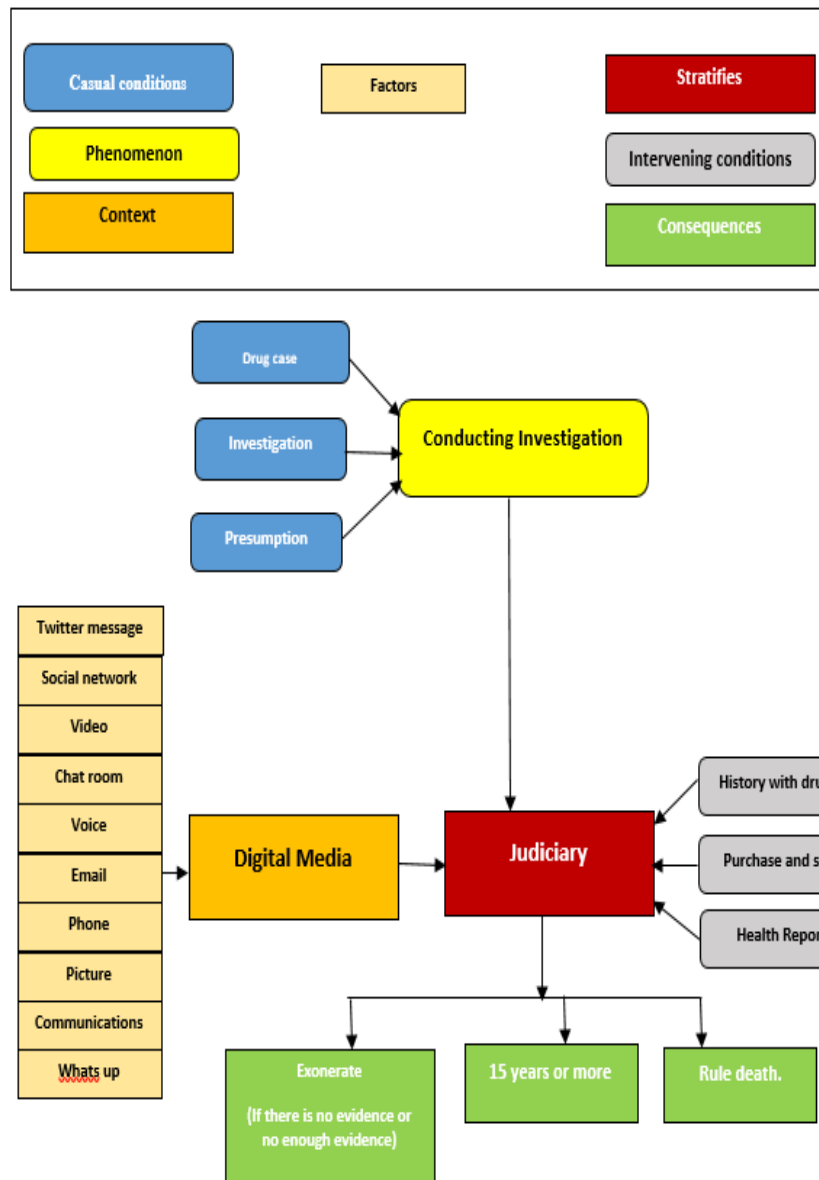
- Innocence
- The judging will be at least 15 years for smuggling discretionary.
- The judge can rule death.

Finally, the consequences are the outcome of these actions and interactions which are mentioned from the participants’ responses; which are represented in the judge’s decision, for example innocence , the judging will be at least 15 years for smuggling case, the judgement could lead to the death sentence. INV4 participant confirmed the Judge decision by saying:

the Islamic law or statutory rules, the judging will be at least 15 years for smuggling discretionary”.

The figure 16 below summerise the relationship between the factors of the category above

Figure 16: Conduction Investigation category



The phenomenon is developed by the paradigm model based on the set of conditions which are mentioned above. For example, the first category phenomenon is (Investigation procedure) that affected by a set of conditions and events, such as, Drug case, Investigation and Presumptions, which mean that the cause to conducting the investigation procedure. It has been found that different digital evidence plays a role

within taken action of strategies to a phenomenon. There are also conditions which facilitate actions/interactions or strategies are taken, that is named intervening conditions. For example, Have a history with drugs, Electronic purchase and sale and Health report of the suspect, all these conditions facilitate actions/interactions or strategies taken to manage a phenomenon with respect to Judiciary. The consequences of the “investigation procedure category” can result in either; innocence years imprisonment or the judge can rule death.

5.3.2 Investigators' experience with insufficient evidence

The second category which emerged from the axial coding is Drug's Investigation Procedure where there is not sufficient Evidence. As mentioned above, the data for events which precede the phenomenon can be provided by the causal conditions which are identified by properties and dimensions. There are a number of causal conditions: incomplete evidence, no evidence and ambiguity (Reasonable doubt). These conditions are the events which lead to the occurrence of a phenomenon. Hence, the central idea of this category is 'Investigators' experience with 'insufficient evidence'. This category was identified because it can make connections between categories and gathers the data together after open coding.

A. Causal Conditions

- Incomplete evidence.
- No evidence.
- Ambiguity.

Participant INV1 asserted that the phenomenon “conducting the investigation in drug cases which have incomplete evidence” occurred when there is not sufficient evidence to seek to build the evidence case, as INV1 said:

There are cases that have incomplete evidence; therefore, the investigator should make a greater effort in these cases, more so than in the cases that have complete evidence. If there is incomplete evidence, we often seek to build new evidence. That means extracting evidence of acts committed, or examining a person’s circumstances or the reality of the situation, so that the evidence might be weak, but it will be strengthened by new presumptions or new evidence that will back the weak evidence. INV1.

In addition that another participant INV2 also confirmed that “incomplete evidence” is a causal condition for conduction investigation by saying:

Some cases come to us with incomplete evidence; we try to look for new evidence. INV2.

Participant INV2 affirmed that no evidence is one of causal condition that may also lead to the occurrence of the phenomenon, as said:

When there is no evidence but there is a presumption of guilt we will try to take further action. INV2.

Another causal condition is Ambiguity. INV3 asserted that is factor impact on the investigation and lead to occur the phenomenon, as he said:

More than 95% of drugs cases are flagrante delicto cases. Very few drug cases have ambiguity or incomplete evidence.

B. Phenomenon

Investigators' experience with insufficient evidence

C. Context

- Link the events.
- Suspect is related to drug smuggling.
- Facts.
- Indication

Thirdly, the context which is defined as “the particular set of conditions within which the action/interactional strategies are” (Chisnall, 1998) occurred in this research on many occasions. For example, in this research a number of contexts emerged from the participants’ responses, for example “link the events”. This factor impacts the phenomenon, where INV5 claimed that the phenomenon is impacted by linking the events and facts to reach to the evidence, as said:

“We gather preliminary inferences about the case, and in the absence of complete evidence we link the events and facts with the words of the suspect and his health condition” INV5.

In addition, through the constant comparison and theoretical sampling methods, the indication was given as another factor that affects this phenomenon. INV2 reveals the impact of indication:

“Many emails were sent from a specific email to the office’s email and there was just one person who answered the emails from the office, this gave us an indication that a consignment would arrive at this office.” INV2.

D. Intervening Conditions

- Medical condition.
- Relationship with another case and person.

Fourthly, another intervening condition is “the structural conditions that affect the action/interactional strategies that are relevant to the phenomenon” (Chisnall, 1998). Intervening conditions such as the health condition for the suspect, the relationship with other cases and persons related to drugs cases may affect the investigation procedure in drug cases in the presence of insufficient evidence.

The health condition of the suspect was a related intervening condition that affects the strategies that are relevant to the phenomenon, where INV 5 asserted by saying:

“We link the events and facts with the words of the suspect and his health condition.”

INV5.

Another participant INV2 affirmed that a relationship with another case and person who is related to drugs is a condition which may also have an effect on the phenomenon, as said:

“The suspect in prison was arrested on 14/05 and the drugs were seized on 15/05. When the suspect’s phone was searched on 14/05, it turned out there were messages which showed that there was a relationship with another case and person.” INV2.

E. Strategics

- Interrogation.
- Strengthening presumptions.
- Looking for information.

The next, strategy which is “Action/Interaction: strategies devised to handle and respond to a phenomenon under a specific set of perceived conditions” (Chisnall, 1998). Strauss and Corbin (1990) claim that strategies are used to respond to a phenomenon under certain conditions. In this research the strategies that were taken tend to support the investigation process in the absence of sufficient evidence. The strategies used to reach the target are Interrogation, Strengthening Presumptions and Looking for Information, as INV3 claimed:

“It starts with the interrogation of the suspect by asking him questions.” INV3

Moreover, the participant INV2 points out the another strategy which is strengthening presumptions, that is taken to carry out or develop the phenomenon, as said:

“Strengthening presumptions, because sometimes these are the best thing for an accusation. But in this case there was no evidence or suspect.” INV2

Furthermore, looking for information is one of the strategies, which was stated by INV3 as:

“Start looking for information about the suspect.” INV3.

F. Consequences

- No evidence is produced.
- I decided to stop the investigation and wait for further instruction from head of department,
- Evidence that is not attainable.
- Transfer the case to head of the department.
- We terminated the case and it ended inconclusively.

- There was another case in which I decided to discontinue the investigation.
- Proving the case.

Ultimately, the outcome of these actions and interactions based on the participants statements may lead to the investigators reaching the following conclusions: the lack of evidence may lead to the termination of the case, the evidence provided is unattainable, the case is transferred to the head of the department or the case is terminated completely as it is rendered inconclusive.

INV1 participant confirmed the investigator decision by saying:

If an investigative path is closed from the beginning, or evidence is locked away, or no evidence is produced, I will end the investigation INV1.

Another participant INV2 confirmed “Evidence that is not attainable” is one of outcome of these actions, as he said:

“I am as an investigator responsible for the full case. Sometimes the case requires evidence that is not attainable. Sometimes, there was strong evidence about a suspect who had some drugs, but it is discovered during the investigation that this person is not the right person; or the case against him or charge is wrong. In this case, I decide as an investigator based on strong signals or strong evidence that is evident to me during the investigation, to stop the investigation or review the search and look for another suspect, if I have 168btain168h that the suspect is not related to the case.”INV2.

The figure 17 below summerise the relationship between the factors of the category above

Figure 17 Investigators experiences with insufficient evidence



The investigators' experiences category as shown in figure 17, indicates what happens in the cases of incomplete evidence, no evidence and ambiguity (reasonable doubt), these were taken as casual conditions to use their experiences in such these cases. This occurs based on a set of conditions and properties, including Link the events, Suspect is related to drug smuggling, Facts and Indications. In addition, the researcher must consider Medical conditions and Relationships with another case and person as an intervening condition to perform the facilitation of the adoption of DF with insufficient evidence in Saudi. Furthermore, Interrogation, Strengthening presumptions and Looking for

information can be taken as Action/Interaction strategies. The availability of strategies within an investigation processes will affect investigators attitudes towards the adoption of a method to enhance the accuracy of digital forensics in the absence of sufficient evidence. The outcome of the decision will be affected by all previous factors. As a consequence of the investigator may decide to stop the investigation, transfer the case to a more senior member of staff, complete termination due to the inconclusiveness of the case or prove the case based on the paradigm model shown in figure 17.

5.4 Selective coding

Selective coding is the final stage for integrating the theory; it is not considerably different from the previous stage which was axial coding. It also yielded a core category which helps describe what the research is about and organises the other categories in an explanatory whole (Strauss 1987). There are several techniques which are used in the integration process, including writing the storyline, using computer programmes and using diagrams. Finally, the researcher will validate the theory by applying it to the participants' responses and comparing it to the raw data.

To identify the integrated relationship between the core category and other categories we created a story line that conceptualises the narrative, as follows

5.4.1 Story line

The main story of this research is to identify the factors that influence the digital investigation process and address the challenges which arise with regard to ensuring that the evidence gathered is as complete as possible and admissible in a court of law.

The digital world has expanded exponentially in recent years. Alongside increased internet use there has been an increase in the diversity of criminal tools. Therefore, digital

forensics needs to be able to counter challenges arising from the growing complexity of criminal scenarios and make it possible to properly handle evidence. This is a major concern for the implementation of the investigation process when seeking to achieve a comprehensive and reliable conviction.

In the last three decades (specifically from 1984 to 2013), researchers have proposed a number of investigation models in an attempt to create a model which is applicable to any scenario (Yusoff et al, 2011) (Hong et al, 2013). The models proposed, however, do not cover all aspects of digital crime investigation. One of the main aspects, which has not been covered in these models, is how to deal with incomplete evidence.

In particular, this research proposes to improve the accuracy of digital forensics in the case of incomplete evidence. It seems from the participants' responses that there is no procedure to deal with cases which have absence of complete evidence. The participants deal with such cases as they deem fit on the basis of their experience.

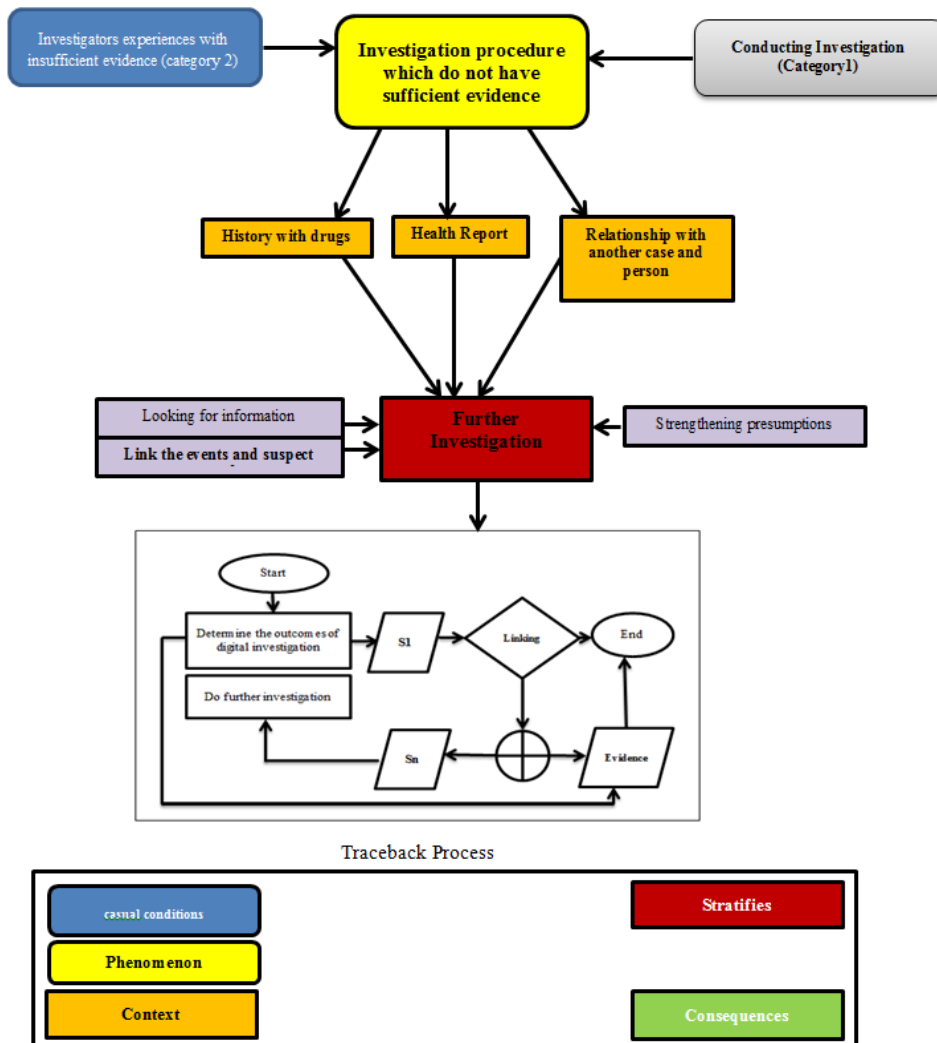
5.4.2 The relationship between the core and other categories (emerged from axial coding)

In this research, two categories emerged as a result of the axial coding process, as explained in Figure 18. These two categories were 'Investigation procedure in drug cases' and 'Investigators' experience with insufficient evidence' and were related to the core category, 'Investigation procedure where there is insufficient evidence'. This relation was identified using the paradigm model.

Following the axial coding process, the selective code serves to provide an overall understanding of the research and conceptualise the overriding idea in this phase, which in the case of this research is the role of digital forensics in investigation where there is insufficient evidence and investigators require additional information in order to solve

the case. As a result of the research the researcher identified the need for a new phase. Which is the researcher have called 'traceback' and that figure 18 shows the elements of an investigation that are affected by the new phase.

Figure 18: Core category



The category of investigator experience and related subcategories were taken as causal conditions, due to investigators' experiences in these cases (Drug cases), which underpins the core category. The identified factors found to influence the core category were: incomplete evidence, ambiguity, and unobtainable evidence that caused conducting this phenomenon ('Investigation procedure where there is insufficient evidence'), as stated by INV1:

"There are cases that have incomplete evidence; therefore, the investigator should make a greater effort in these cases, more so than in the cases that have complete evidence"
INV1.

Furthermore, INV3 explained that the ambiguity factor affected an investigation, leading to the occurrence of the phenomenon ('Investigation procedure where there is insufficient evidence'), further stating that:

"Very few drug cases have ambiguity or incomplete evidence" INV3.

Finally, 'unobtainable evidence' is one of the outcomes of the 'Investigators' experience with insufficient evidence' category, which is represented in investigator's decision which is one of the causes to conducting this phenomenon ('Investigation procedure where there is insufficient evidence'), as explained by INV2:

"I am as an investigator responsible for the full case. Sometimes the case requires evidence that is not attainable," INV2.

The data shows that there are several conditions that must be fulfilled before reaching a phenomenon ('Investigation procedure where there is insufficient evidence') strategy. These conditions are the following:

1) The suspect's history with drugs. This condition was confirmed by one participant to be one of the main conditions that can affect the phenomenon; they further elaborated on the significance of the suspect's history of drug crimes, and their previous relationships, which could serve to obtain more interlinked information in efficient procedure. The participant stated that

“We might get some information about the suspect's involvement in previous actions – i.e. has the suspect been arrested in a drugs case previously? Or does she he have a history with drugs? Seek out the suspect's relationship with other cases,” INV2.

2) The suspect health report, which can possibly indicate that they were involved in the crime. From the suspect's medical reports and tests, the investigator can tell whether the suspect is a drug addict, or used to be. In such cases, the suspect may have a link to at least one drug dealer. Participant INV5 argued that it is typical procedure in these case investigations to acquire the necessary information of the suspect's health history, due to the substantial influence on investigation flow. INV5 explained that:

“Drug cases are given to us as investigators usually by the General Directorate for Drug Control, and then we follow the procedure described, study the case, study the accompanying paperwork, preview anything seized in relation to the case, ensure the safety of seizures, the suspect's situation and health examination documents, and question the suspect...” INV5.

3) The final condition is the potential relationship between the suspect and other persons responsible for other crimes. In fact, in many previous investigations into a specific case, the investigator has undertaken detailed checking and analysis of the suspect's network of contacts and connections, via their mobile device and social media accounts.

Consequently, this process identifies further links to other different cases and other additional suspects. Participant INV2 confirmed the usefulness of this strategy by describing an incident that took place during an investigation of a suspect. They explained that:

“The suspect in prison was arrested on 14/05, and the drugs were seized on 15/05. When the suspect’s phone was searched on 14/05, it turned out that there were messages that showed that there was a relationship with another case and person.” INV2.

While gathering and analysing the context of a case, there are other influential factors that cannot be ignored when collecting evidence; these factors formulate the ‘intervening conditions’. The intervening conditions can be defined as “the structural conditions that affect the action/interactional strategies that are relevant to the phenomenon.” The intervening conditions fall under the ‘conducting the investigation’ category which emerged in axial coding. One of the main such conditions is digital media, or specifically social media, which tends to be the main vehicle of communication, due to its ease of use, effectiveness and speed. Accordingly, it is a vital medium for facilitating the committing of a crime. This is confirmed by INV1, who stated that:

“Digital evidence is in the form of a voice, image, and so on. The problem with digital evidence is that most of the community members who handle digital crimes have not reached the stage of using technology to commit crimes, but they do now use handheld devices, such as smart devices. Smart devices can be used for messaging through messaging programmes. We can get evidence from them, and possibly use certain techniques that exist.” INV1.

As a result of the above situations and factors, the investigation process reaches the level of the 'Further Investigation' strategy, which is defined as, "action/interaction strategies devised to handle and respond to a phenomenon under a specific set of perceived conditions".

At this stage, the investigators could utilize many methods to enhance the process, beginning with looking for information, as confirmed by INV3:

"Cases that contain incomplete evidence require time and patience. Even where the evidence is incomplete, you start looking for information about the suspect. Sometimes you find previous reports and previous records about the suspect from other police teams, and find that they were observed and there is a report about them ..." INV3.

The second step is to link the events and the suspect, as explained by INV5:

"We gather preliminary inferences about the case, and in the absence of complete evidence we link the events and facts with the words of the suspect and their health condition" INV5.

The third step is strengthening presumptions, which is described as:

"Strengthening presumptions, because sometimes these are the best thing for an accusation, where the case had no evidence or suspect previously," INV2.

Most of the participants considered the above to be steps that, in their experience of the investigation process, assist them in deciding upon a procedure that will enhance their evidence to make it more accurate and acceptable in the Saudi Court. Moreover, this procedure contributes from their perspective in obtaining better results in the investigation process.

Alternatively, in cases where there is cooperation between the investigator and the digital investigator, together they will agree on a procedure to be used to enhance the investigation process, where the digital evidence, which is considered in the Saudi context as a presumption.

In the case of core category, the current investigation procedures in Saudi Arabia will be affected positively because of the collaboration between the investigators. The role and responsibility of the investigator is defined according to article 14 of the Law of criminal procedure in Saudi Arabia and article 15 of Saudi Anti-Cyber; as who someone is entrusted to carry out the investigation for finding out the truth in criminal incidents and digital crimes. According to the article 76 of Law of criminal procedure in Saudi Arabia, this role is define as someone who has the technical knowledge in regards to any matter relating to the investigation, including the gathering of existing links that are to be analysed in support of current evidence.

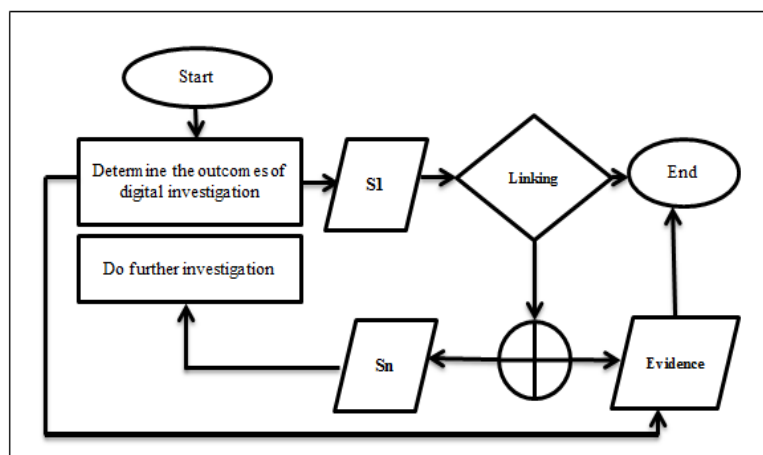
Therefore, the outcome of these actions and interactions based on the participant's statements led the researcher to the following conclusion: a 'Traceback' phase to solve the issue of insufficient evidence in the Saudi context, which is a new step intended to improve the investigation process and help solve cases where initially there is insufficient evidence. The investigator can use the Traceback phase to address any shortfall in the collected evidence relating to the case, and thus to proceed further with the investigation process, through linking the data that emerged from initial analyses, and collaboration between the digital investigators and the investigator to identify elements of criminal offences. Any crime has physical elements and incorporeal elements, which easily conceive in the understanding, such as action or rights. Digital crimes will have physical elements that reflect the will of the actors, and which are provable; incorporeal elements

also reflect the will of the digital criminal, to achieve acceptance in the Saudi Arabian court of law.

The importance of this collaboration was clear from the participants' responses in this research; for instance, INV4 stated that, "digital evidence in Saudi courts may not be acceptable because it is intangible and they look at it as presumption, because it is possible that is forgery". In addition, the Saudi court has difficulty with digital evidence of discovering proven evidence; there is no clear violence or blood, just data and figures, which can be changed or erased from the records, stored in the memory of digital devices, and may not have an external physical impact (Faiza, 2012). INV1 confirmed the statement of INV4. In addition, INV2 mentioned that digital evidence is used to support an interrogation by proving the suspect's relationship to the case.

Therefore, it is clear that cooperation between the digital investigator and the investigator is essential to support the use of digital evidence, which is viewed by the court in Saudi Arabia as presumption, for achieving criminal offences elements to obtain evidence that will be acceptable to the court. This phase was developed following the identification of four factors (incomplete evidence; other suspects; drugs linked to other suspects; links between cases), which arose from the analysis in Chapter 5, Section 5.5, and which are not discussed in the existing studies reviewed in Chapter 2 (Pollitt, 1984; Lee et al., 2001; DFRWS, 2001; Reith, Carr & Gunsch, 2002; Carrier & Spafford, 2003; Stephenson, 2003; Baryamueeba & Tushabe, 2004; Ciardhuáin, 2004; Beebe & Clark, 2004; Rogers, Goldman, Mislán, Wedge & Debrotá, 2006; Kohn, Eloff & Olivier, 2006; Freiling, 2007; Perumal, 2009; Pilli, Joshi & Niyogi, 2010; Yusoff, Ismail & Hassan, 2011; Hong, Yu & Lee, 2013).

In the Traceback phase, the digital investigator will follow the steps outlined in Figure 19 below, which emerged from the analysis of participants' responses. The researcher collected these experiences within Traceback to develop a comprehensive framework within the Saudi context to reduce the number of cases on hold because of insufficient evidence. For example, a case "will be strengthened by new presumptions or new evidence that will back up the weak evidence" (INV1), and thus "gathering several presumptions to strengthen the charges against the suspect" (INV3). Furthermore, "the investigator should search for evidence to complete the other evidence," (INV1), and so, "we try to look for new evidence" (INV2) First, investigators, "start looking for information about the suspect" (INV3), they then, "link the events and facts with the words of the suspect and their health condition" (INV5), and potentially, "look for another suspect, if I have realised that the suspect is not related to the case" INV2.



S= Suspect's device

Figure 19 Traceback Process

Figure 19 shows how the Traceback phase is undertaken. After the investigation process the investigator can review the available evidence and then take a decision on whether to

use Traceback, or move on to the evaluation phase and presentation phase. If the investigation results are not sufficient, the digital investigator can use Traceback to seek out further evidence, and improve existing evidence by identifying areas of the case where there is insufficient evidence. The digital investigator can link insufficient data (and metadata) with other data obtained from or relating to the same suspect to determine whether there is a relationship between this data, and seek out additional evidence.

The digital investigator will use all data on the suspect’s devices in order to go through all possibilities of search results,

The Traceback process should be fed with information that is gained from the investigation process, which should be conducted by an investigator, according to the Saudi Law of Criminal Procedure and Saudi Anti-Cyber Law, in order to arrive at a comprehensive and integrated conclusion. This will lead to the discovery of more evidence, or more information related to the case, such as the identification of another suspect or case (which will again require further investigation through Traceback), both of which will help determine the facts, as shown in Figure 20 below:

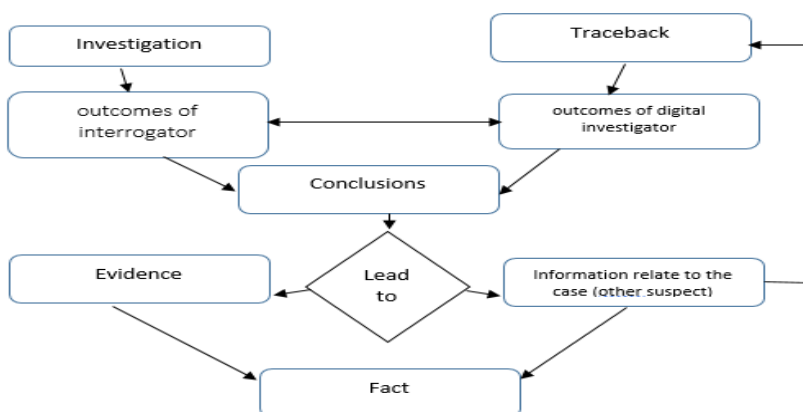


Figure 20 - Collaboration process between investigator and digital investigator

Having linked the data, the digital investigator will reach one of three possible outcomes:

- Completing the investigation, if there is no additional linkage between the data relating to the suspect.
- Obtaining additional evidence based on data that is linked between the investigator's outcomes and digital investigator's outcomes.
- Doing further investigation of another suspect, with whom a relationship with Suspect 1 has been established. Each case may involve N suspects, therefore the investigation loop continues until the case is closed.

5.4.3 Advantages of cooperation

The relationship between the interrogation process and digital investigation process is symbiotic, and this thesis strongly argues that this cooperation between the digital forensics investigator and the investigators in charge of an investigation plays an important role in exploring new outcomes, phenomena, or suspected activity related to the case. At present, this is not the situation in Saudi Arabia, as confirmed by INV2, who said, "I am the only investigator responsible for the entire case".

The outcomes of a cooperative process will enhance the digital investigation in cases where there is insufficient evidence, and the outcomes of interrogation will likewise support the digital investigator in uncovering facts. This can be achieved through linking what has been found on the suspect's digital device with the results of interrogation, such as suspect's activities, and times and dates. Furthermore, the outcomes of interrogation may provide valuable information in the digital device to be evidence against the suspect.

Hence, the cooperation between the investigator and digital investigator will reveal and identify the suspect's personality and intentions through his/ her digital activities, which will help the investigator who charge the case to reach a valid and sound conclusion.

In addition, the cooperation will be helpful in the Saudi investigation processes in several points:

- Identify the suspect's relationships and connection with others
- The quick access to facts and to other parties before losing their impact and thwarting their plans
- Find out explanation for any indications about the case
- Save time

5.4.4 Importanced of cooperation

According to Al-onzi (2009), a digital investigator is helpful to the current investigation process for any criminal investigation. However, from the judge's perspective, all findings that have been provided by digital investigators help only to support the case (Al-onzi, 2009). The data that is provided by the investigator will be more valuable, in addition to the incident report given to the digital investigator during the investigation, because the investigator will provide more information about the case. Therefore, cooperation will be especially helpful in:

1. Extracting more entries for a keyword list that is used in the data analysis.
2. Reducing the search time for both the digital investigators and investigators, and obtaining more information through cooperation, leading to the establishment of facts.

5.4.5 Proposed research model for solving the issue of insufficient evidence

The Traceback phase aims to enhance the digital investigation process so that it can more easily solve cases where there is insufficient evidence.

This is a starting point to encourage digital investigators to obtain sufficient evidence from digital investigation processes, and to reduce the number of cases that are on hold because of insufficient evidence, by allowing for further investigation and supporting digital evidence, so that it can be used in Saudi courts.

The Traceback phase emerged from data collected in this research via the grounded theory method, which included a literature review of the emergent field of digital forensics. The literature review also clarified the digital investigation process, which has been developed by authors over a number of years; this is presented in Chapter 2, Section 2.2.

Previous studies have contributed to digital forensics processes by addressing certain research problems. For example, Hong (2013) proposed a “new triage model that is designed to meet the recent requirements of the Korean legal system for privacy protection from, specifically, a Korean perspective”. However, following the literature review, these studies were found to have not determined how to address cases where there is insufficient evidence, as the present study does. The findings of the participant interviews and the literature review confirm that there is no procedure for cases with insufficient evidence.

The researcher designed questions to ask the participants about insufficient evidence, and the participants' responses revealed that there is no specific procedure to deal with case in which there is a lack of evidence in Saudi Arabia, and that this depends upon the

discretion of the investigator and their experience in the field of investigation. According to the investigation procedure that is followed in Saudi Arabia, the investigator in a case where there is insufficient evidence must make their decision based on the incomplete findings of the investigation (INV1, INV2, INV3 and INV4).

As a result, this study has developed a research model to enhance the digital investigation process in the Saudi context following an analysis of the data collected in this research (literature review and participant interviews, which led to the development of the Traceback phase of investigations. The interview questions in this research were designed to explore the participants' experiences, knowledge and opinions about the investigation processes.

For example, interview question 4 (mentioned in Chapter 4, Section 4.8) encouraged the participants to describe their experiences with regards to dealing with cases where there is insufficient evidence. In Chapter 5 the researcher reviewed the participants' responses to this question; all of the participants stated that the cases with insufficient evidence require more effort to find additional evidence. For instance, INV1 explained that, "there are cases that have incomplete evidence; therefore, the investigator should make a greater effort in these cases".

Moreover, interview question 6 (mentioned in Chapter 4, Section 4.8) also helped the researcher to understand how decisions are made by investigators in cases where there is insufficient evidence, as INV1 explained that they would:

"Continue or end the investigation depending on the same evidence. There might be evidence available in the initial phase. This either suggests that a suspect is the perpetrator of a crime, or not, but if evidence surrounding an incident is weak, the

investigator will require more effort and collaboration from people surrounding the investigation.”

From the participants’ responses, it was learned that the responsibility for taking the decision to stop or continue the investigation lies with the investigator. Therefore, the knowledge and experience of the investigator is one of the main factors influencing the decision to terminate or continue the investigation, as described by INV2: I am, as an investigator, responsible for the entire case”. These answers enabled and supported the proposition, in this research, of a mechanism to help the investigator make a decision about a case in which evidence is insufficient, and also to reach a point in the investigation process where a final decision can be made on whether there is sufficient admissible evidence to take the case to the court of law.

Based on the analysis of the results of this research, the researcher added the Traceback phase to the proposed model to produce a comprehensive model of the digital investigation process, one that can be used in cases where there is insufficient evidence, to carry out further investigation.

5.4.6 Example of a case with insufficient evidence

Below is an example of a case in Saudi Arabia that was cited by one of the participants (INV2) in this research. On the 10th September 2016 the drugs enforcement department received information from one of their informants about someone driving a car, whereby the occupant was in possession of an amount of illegal pills (Captagon); accordingly, a team of anti-narcotics investigators was sent to arrest the driver. The team found the suspect’s car and asked him to stop; however, he refused to stop, and drove away. The

team continued to chase the driver and attempted to force him to stop on a number of occasions, but the driver managed to escape. After some time, the suspect decided to stop the vehicle and run away on foot, and disappeared. Later, when inspecting the car, the team found 135,000 illegal pills.

5.4.6.1 Team Action

The car information details were then retrieved from the traffic department. The anti-narcotics team decided to bring the owner of the car in to question him about the incident. The owner of the vehicle denied any knowledge of what had taken place. The team decided to gather all available information to link the owner of the car to the incident, by using his telephone records, text messages, and any information that could be retrieved from any digital device at his location, but could not find anything to prove that he was linked to the incident. As a result, the charges against the owner of the vehicle were dropped, and the search for the driver began again.

According to Article No. 76 of the Saudi Law of Criminal Procedure, the investigator is permitted to seek expert assistance. In this case, the investigator in charge would ask a digital investigator to search the digital devices belonging to the owner of the vehicle for any information that could lead to the person who committed the crime.

Unfortunately, the digital investigator's chief responsibility is to follow the digital investigation procedure described in Chapter 2, Section 2.5.2 to analyse the suspect's devices and look for evidence related to the case. In other words, the digital forensics team receives a request from the investigation department to extract all data in any digital device linked to the suspect. The digital investigator's responsibilities end when the report is written presenting what data has been found on the suspect's device, according to the investigative procedures. The findings of the digital investigator are then sent to

the investigator, whose responsibility it is to take a decision about the case and any information found, which will be to either drop the charges against the suspect, prove the charges, or hold the case until further information arises. The criminal laws of Saudi Arabia state that, “The accused is innocent until proven guilty”, and so this principle must be adhered to by the investigator throughout their investigation process, as confirmed by INV4. In the case described in the previous section, the decision was to put the case on hold (no further action), due to insufficient evidence.

Through the interviews with the participants, it was found that the crime scene team and investigator provide the digital investigator with the suspect’s devices (mobile phone and laptop,) without a briefing of the incident (Al-sahimi, 2007). After analysing the suspect’s device, a report is generated and submitted to the investigator, who will then present the suspect with any evidence or information that has been recovered from their devices. In the case that no evidence is found, the investigator will attempt to elicit a confession from the suspect, and then take a final decision accordingly. INV3 explained that:

“We collect a large number of presumptions. For example, if there is a suspect, we will collect information about his mobile phone communications and take a testimony of 9 or 10 people who sign the arrest record thus gathering several presumptions to strengthen the charges against the suspect.”

5.4.7 Application of Traceback

In cases like the one described above, the researcher recommends the use of ‘Traceback’, a phase that is intended to enhance the digital investigation process in cases where there is insufficient evidence; The Traceback phase involves increasing the degree of

collaboration between the investigator and the digital investigator in analysing the suspect's devices, rather than relying solely on the incident report, as is currently the case. This phase aims to obtain more details about the suspect's activities, and about the events before and after the incident, which may not be discovered through a regular investigation.

The collaboration process between the investigator and the digital investigator was explained in Figure 20. The research participants confirmed that the investigation would "be strengthened by new presumptions or new evidence that would back up weak evidence" (INV1), "thus gathering several presumptions to strengthen the charges against the suspect" (INV3). Furthermore, they explained that, "the investigator should search for evidence to complete the other evidence" (INV1) and "try to look for new evidence" (INV2) or "start looking for information about the suspect" (INV3) In addition, they would try to "link the events and facts with the words of the suspect and his health condition," (INV5) and "look for another suspect, if ... the suspect is not related to the case" (INV2).

The aim of this process is to create a network of connections amongst the contents of the suspect's devices and their statements in the report of questioning, and establish a complete picture of the incident and arrive at fact (Evidence or another suspect or case) by using all the information that has been retrieved from different media devices, and through interrogation by the investigator.

Due to the sensitivity of the information related to the case described earlier in this section, the participant who provided the example case was not able to give specific information, as the case is still pending.

The researcher would strongly recommend that digital investigators use the proposed research model, particularly the Traceback phase, especially in cases where there is insufficient evidence. The Traceback phase enhances the investigation process and can lead to the discovery of further evidence, thus reducing the number of hold cases.

The application of the Traceback phase in digital investigations in cases where there is insufficient evidence will give the digital investigator the opportunity to carry out further investigation and look for new evidence, or discover other information that relates to the case, and again reduce the number of 'on hold' cases.

Digital investigators follow the digital investigation process outlined in Chapter 5, Section 5.6.2 to collect evidence. If the result of investigation is not conclusive, then Traceback should be applied to the results of the analysis phase.

The Traceback phase is intended to determine the relationship between information collected by the initial investigation and the interrogation process that caused the investigation to be put on hold pending further investigation.

This situation requires greater effort and further analysis in order to discover any related information about the case that could enable the case to be revisited. If the digital investigator is successful in identifying further information related to the case, then they can suggest possible scenarios of what might have happened in regards to the incident. At this point, this research suggests that the presence of the interrogation outcomes with a digital investigator during the data analysis (which is not currently the case, according to participants' responses) is essential, because it establishes a strong collaboration when seeking further information about the case.

For example, the investigator can assist the digital investigator by providing a number of facts regarding the incident. The facts that can assist the digital investigator include a list of keywords that could be searched for on the suspect's devices, pictures of the crime scene, or detailed information about the crime scene itself, which could also be helpful to the investigation process. This research strongly argues that this collaboration between the digital forensics investigator and the investigator enables the exploration of new ideas and phenomena about the case. The next section will explain the linking mechanism used in this phase systematically:

- The digital investigators should link all of the information that has been extracted from the suspect's device(s) together, and with the information provided by the investigator.
- If the contents of the suspect's device(s) and the investigator's findings lead to an explanation, this could also add value to the investigation process and progress the case from hold to live status. This process will also include analytical thinking; for example, in the case mentioned earlier, this collaboration between the digital investigator and the investigator could lead to evidence of another suspect, because the owner of the car did not use the car, and was proven to be not guilty, meaning that there must have been another person, or group of people, involved. This might also lead to information suggesting that this crime was a cover for another, larger crime, and many other scenarios. The possibility of such scenarios could again open up the investigation by suggesting either a new suspect, or group of suspects, and, once the information indicating the involvement of an additional party to the crime is confirmed, the same procedure can be followed as with the first suspect.

Traceback can be added to existing frameworks and investigative processes to ensure that the investigator has taken all possible and necessary actions to collect evidence. Later, the Traceback phase aims to guide further investigation to discover leads that may be relevant to the case, and to help it reach a point where there is sufficient evidence for prosecution. In suggesting this additional phase, this research draws on existing models for the digital investigation process by integrating existing high-efficiency mechanisms with the new process, in order to improve the accuracy of the digital investigation process in cases where there is initially insufficient evidence, defined as a lack of sufficient evidence or fact to enable a jury to reach a verdict (The Law Dictionary).

5.4.8 The difference between the Traceback process and other digital investigation processes

Below is a summary and review of the various digital investigation models in chronological order, enabling the identification of phases that are common to all models. Following this, all of the phases were extracted and arranged so that similar tasks were grouped together with unique identifiers according to each of the digital investigation processes, as shown in the table below. It can be seen that, in many cases, the phases overlap each other, and in some cases are duplicated. Certainly, the multitude of digital forensics models proposed by different authors reveals the complexity of digital forensics processes. The table below combines a number of investigation models in order to establish grounds for comparison and discussion.

Phase in the proposed model	Found in:
Preservation	DFRWS Investigative Model; Abstract Digital Forensic Model; End to End Digital Investigation; Network Forensic Generic Process Model; Generic Computer Forensic Investigation Model.
Identification	Computer Forensic Investigative Process; DFRWS Investigative Model; Abstract Digital Forensic Model; Digital Forensic Model based on Malaysian Investigation Process. (DFMMIP); Scientific Crime Scene Investigation Model; End to End Digital Investigation.
Preparation	Abstract Digital Forensic Model; a Hierarchical, Objective-Based Framework for the Digital Investigation; Framework for a Digital Forensic Investigation; Network Forensic Generic Process Model.
Collection	DFRWS Investigative Model; Abstract Digital Forensic Model; End to End Digital Investigation; Extended Model of Cybercrime Investigation; a Hierarchical, Objective-Based Framework for the Digital Investigation; Network Forensic Generic Process Model.
Acquisition	Computer Forensic Investigative Process; Generic Computer Forensic Investigation Model.
Examination	DFRWS Investigative Model; Abstract Digital Forensic Model; End to End Digital Investigation; Extended Model of Cybercrime Investigation; Network Forensic Generic Process Model.
Analysis	DFRWS Investigative Model; Abstract Digital Forensic Model; Common Process Model for Incident and Computer Forensics; Digital Forensic Model based on Malaysian Investigation Process (DFMMIP); End to End Digital Investigation; A Hierarchical, Objective-Based Framework for the Digital Investigation; Network Forensic Generic Process Model; Generic Computer Forensic.
Evaluation	Computer Forensic Investigative Process.
Traceback	None.
Presentation	DFRWS Investigative Model; Abstract Digital Forensic Model; End to End Digital Investigation; Extended Model of Cybercrime Investigation; a Hierarchical, Objective-Based Framework for the Digital Investigation; Framework for a Digital Forensic Investigation;

	Network Forensic Generic Process Model; Generic Computer Forensic Investigation Model.
Returning evidence	Abstract Digital Forensic Model

Table 9: Comparison of digital investigation phases in the proposed research model with existing mode

From the above, the absence of a critical phase for further investigation can be observed, which has not been addressed by other authors.

5.4.9 Proposed Framework

5.4.9.1 Introduction

In this section, the researcher sought to propose a model to take advantage of all the models existing in digital investigations and the application of GT and data collected in this research. This conformity with sharia law for reaching to a comprehensive model in digital investigation in the absence of sufficient evidence in Saudi Arabia to reduce number of cases rejected in the courts.

Interview questions encouraged the participants to explain the procedure of investigation from which the researcher was able to develop the investigation process including search in an investigation, Inspection, expert witness and investigation presentation that works in accordance with process of investigation that is mentioned in chapter2 section 2.4.2.

In addition to that the respondents helped the researcher to think of a solution for insufficient evidence. Therefore, the researcher developed a framework to enhance the digital investigation process in the presence of insufficient information by introducing the below framework by adding a unique step in the investigation process “TraceBack Phase”.

In the description phases of the proposed framework, the researcher has to reveal the relationship between each phase in an acceptable way and this framework can be help to the investigators to find out the relationship between the phases.

Therefore, the proposed model is designed to achieve the level of accuracy in an investigation and gain sufficient evidence to be admissible in the Saudi court. The phases implemented in the proposed model are as follows:

5.4.9.2 Framework Design

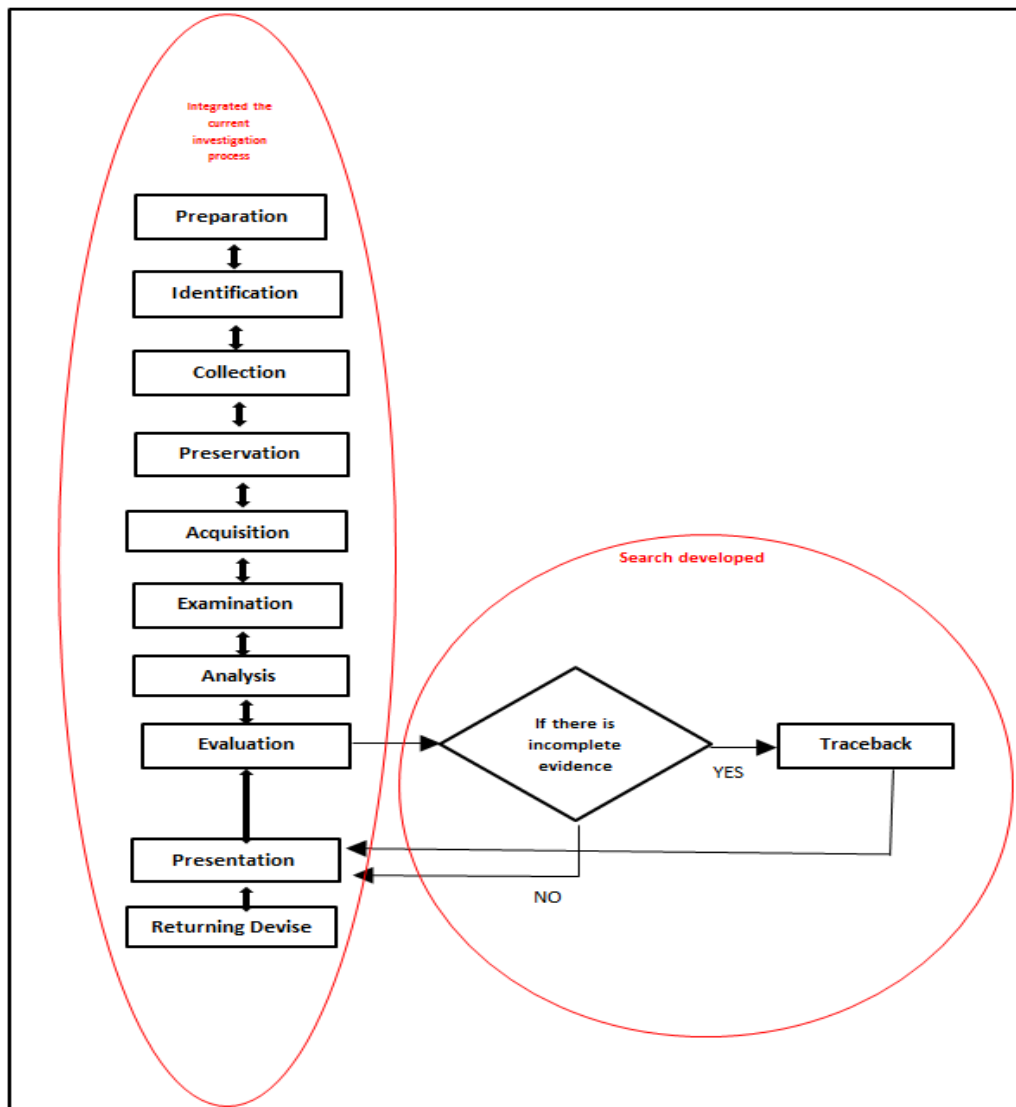


Figure 21 Proposed Framework

Then the **preparation** phase is to prepare the investigation environment and consists of the selection of tools, techniques, search warrants, authorisation and management support. Next is the **identification** phase, this phase will help the investigator to identify the suspect digital equipment and the type of incident. The **Preservation** phase is used to preserve the evidence from the crime scene without any contamination. The **Collection** phase involves the task of seizing the suspect's device and is the source of evidence. The **Acquisition** phase is to collect data, including items such as deleted, swapped, hidden and corrupted files from the suspect device by using forensic tools and techniques. The **Examination** phase involves the identification, verification and validation of potential evidence. Next is the **analysis** phase, which involved analysis of data to prove or disprove the case. The **Evaluation** phase is to determine what evidence is relevant to the case. If there is not sufficient evidence found during the evaluation phase, the investigator will proceed to the **Traceback** phase which leads the investigation to go further with the suspect's devices and the collected data and its metadata of the suspect's devices, then link this data to obtain evidence or leads for further investigation with suspect's devices. The **Presentation** phase is to present the end result (relevant data) of the investigation. **Returning evidence** is the final phase; once the investigation process is completed the investigator has to return the physical devices to its original owner.

I. Preparation

This phase represents the preparation of the digital investigation environment which involves planning and selection of suitable

investigation tools and techniques, obtaining search warrants and authorisation and management support.

Therefore, there are several tasks in this phase which represent a need to prepare the Forensics Lab to conduct a digital investigation to handle any type of digital crime. Digital forensic investigations should be performed by a digital investigator who has the knowledge and experience in dealing with this type of digital forensics cases.

The forensic investigators should use media imaging software and maintain the evidence integrity by using Write Blockers. These techniques will aid the investigator in protecting the evidence from any contamination.

The chain of custody should always be maintained by the investigator to demonstrate when, where and by whom the evidence was handled and how it has been stored and, in case of any accidental damage, who is responsible for the evidence that is seized by the police.

The final task in this phase is that the investigator should prepare the investigation process report by following ACPO (as such this guide is assists in investigating cyber security incidents which is consistent with Sharia Law) guidelines and recommendations.

II. Identification

This phase determines what which kind of process will be followed during the next stages of a digital investigation. There are two factors involved in this phase, determining the type of incident and the type of suspect digital

device. These two factors help the investigator to determine the steps to be taken in the preparation phase, because the investigator cannot proceed further to the preservation phase without knowing these two factors.

Prior to starting the investigation, the police officer provides a statement containing information about the type of incident and the description of the suspect's digital equipment to the forensics investigator. Using this statement of information the investigator can proceed further to the preservation phase.

III. Collection

After the successful identification and preparation of the case, then the investigator needs to seize the identified device from the crime scene.

Further, this phase involves collecting the suspect's devices and information about the place and source of evidence. These files and information can be used later by the investigator to analyse and verify the relationship with the case.

IV. Preservation

This phase involves preservation of suspect's device seized by police from any contamination by ensuring that an acceptable chain of custody has been initiated and maintained throughout the investigation process. This will help the evidence to be admitted in the court.

Guidelines for preserving the evidence are explained in the Association of Chief Police Officers (ACPO) guidelines. The suspect's device (Laptop,

PC, USB etc.) should be seized and preserved in a secure place to avoid any accidental deletion or changes. All further investigation is undertaken by taking image of suspect's device which is used for the investigation in order to maintain the integrity of data during the investigation.

V. Acquisition

The acquisition phase is to collect data by using forensic tools to unveil all the evidence, including deleted, swapped, hidden or corrupted files.

This phase will determine the process carried out, time of process, result of process and the steps taken during the investigation process.

After the development of the case structure, the investigator assigns a name to the case and records where the case was created and stored.

Next, collect evidence, verify and establish the chain of custody to determine the location of the evidence, from where it is obtained and create an audit trail.

The investigator should ensure that the device under investigation is write protected by using a write blocker.

The investigators' next task is to determine the tools required to acquire evidence and the information about the evidence.

The tools used to acquire the evidence should support and verify the evidence through the use of file hashes such as the MD5 Hash, because the investigator has to prove that the collected evidence and copy is not changed from the time it was acquired. This can be done using MD5

hashes to match the evidence and its copies. Guidelines on this aspect are provided in principle 1 of the ACPO guidelines.

Finally, the investigator returns the device to the Evidence Officer and confirms that the documentation of the chain of custody is complete.

Here the researcher clearly states that there is no further investigation, if any of the phases fails to fulfil its condition. As the examination is to enhance the investigator ability to identify, determine and validate the potential evidence from the collected data.

VI. Examination

After the evidence collection, the investigator examines all the data which is collected from the suspect's devices to identify, determine and validate the potential evidence related to the case.

The relationship between the examination phase and the analysis phase is to help the investigator to determine the further course of action while dealing with the available evidence.

VII. Analysis

The analysis stage involves the analysis of data which is identified and collected by using tools and techniques to determine facts. The analysis processes that can be performed comprise timeframe, data hiding analysis, Application and file analysis, and Ownership and possession analysis. Timeframe analysis can be useful to identify the time of events occurred on the system. Moreover, it's useful to find the relationship between

individual(s) and the usage of digital device at the time when the events occurred.

Next, data hiding analysis can be useful for detecting and recovering the data which may concealed on the system which may indicate intent, ownership etc. Application and file analysis helpful to identify the programs and files that may have data relevant to the investigation. Ownership and possession that is helpful to determine who created, accessed or modified the file, and also including information specific to a user. After the analysis process there are some results which need to be analysed by the investigator who interprets the analysis of evidence described and provides suggestion for further analysis and interpretation of the results and give opinion.

VIII. Evaluation

This phase helps to determine the relations between the collected evidence and other available evidence. This phase can help the investigators to identify whether there is any relevant information related to the case. Also, this phase helps the investigator to proceed to the next phase i.e. Traceback or move to the presentation phase if the information is completed.

The relationship between the evaluation phase and the Traceback phase is to assist the investigator in the decision-making process.

IX. Traceback

This phase is a new step that is proposed for helping the investigation process to deal with any cases where there is not sufficient evidence. The investigator should use this phase to find any shortfall in evidence related to the case and to proceed further with the investigation process with greater accuracy.

X. Presentation

This phase comprises the presentation of the investigation results (relevant data). This stage is a standard way of explaining how and why the data was reviewed, and what conclusions were reached. There are some rules and procedures which should be followed by investigators while presenting the results. These rules/procedures include the details of the incident. The report should be understandable and reasonable for the decision-makers, be capable to withstand challenges at the court proceedings, not be opened to misinterpretation (unambiguous), be easily referenced, should include all of the information needed to explain the investigators conclusions, presenting unbiased and valid conclusions, opinions, recommendations (if asked for) all these should be done in an timely manner.

XI. Return evidence

This phase involves the return of physical and digital devices to their original owner.

5.4.10 Justification for proposed framework

We found that the current literature regarding digital forensic investigation did not address issues related to insufficient evidence and thus we have sought to investigate means in which sufficient data can be gathered in Saudi Arabia. We used the grounded theory method for solving the research problem and for data collection. This method is good means for gathering information that is not currently covered in the literature. The advantage of the research methodology used is that it allows for the development of a framework. Therefore, based on the ideas from the extensive literature review, we proposed that the digital investigation process and data analysis is the most accurate and comprehensive when it comes to the suitability of insufficient evidence in Saudi Arabia.

The proposed framework will be advantageous for Saudi law of criminal procedure in numerous ways. Firstly, it will help to reform the Saudi legislation for the digital crimes by allowing the sharing of information between the expert and the investigator in the investigation process to obtain sufficient information and admissible and strong evidence in the Saudi Court. This will be achieved by upgrading the 76 article of Saudi Arabian criminal law procedure by abolishing the mere seeking of help when it comes to the investigator and instead allowing for the incorporation of teamwork between investigator and digital investigator when it comes to all cybercrime cases. This will allow for quicker verdicts to be made and will hopefully lessen the burden on the judicial system and would be a direct result from the use of a digital investigator as they are specialists in the field. Furthermore, the incorporation of this procedure of Traceback will allow for the reforming of administrating process of the investigation. Thus, it is of utmost importance to involve the digital investigator, not by choice but as a consequence of law amendments

when it comes to cybercrime cases, as this will enable the linking of crime elements and further strengthen conviction of these crimes. Moreover, the direct link between investigator and digital investigator will enhance accuracy and completeness compared to current cybercrime processes utilised in Saudi Arabia. The reforming of the legislation will upgrade the digital evidence in Saudi Arabia from presumption to evidence of demonstrable value. These amendments will improve the creativity of digital investigation including factors such as suspect character, manners and potential suspect targets.

Secondly, it will help in reforming the existing Saudi digital investigation procedure (see chapter 2, section 2.5.2); by integrating all phases that were proposed by other authors throughout the years and adding the Traceback phase to the existing procedure that emerged from the data analysis. The current process in Saudi Arabia was established in 2007 by the Saudi government and looked at the digital evidence as a presumption. Therefore, the proposed framework is a much more modern and contemporary method to use in the constantly evolving world of technology. As such data presented in a court of law must be obtained through methods which are up to date and reliable; which we believe can be achieved using our suggested framework in cases where there is insufficient digital crime data. This will in turn reduce the number of cases rejected by the Saudi Arabian court of law.

It will also speed up the trial process through the cooperation between the investigator and digital investigation, where the court will not look at the digital investigator's outcome as just presumption because it is supported by the interrogation outcome which brings the information directly from suspect. This incorporation will unify the investigation process in the court should the opposing bodies disagree with the findings,

the collaboration between investigator and digital investigator will be more likely to result in conviction, as the conclusions made would be the same. Should the litigant decide to change digital investigators based on article 78 of Saudi Arabian law of criminal procedures, we propose that the both prior and newly appointed digital investigators follow the exact same procedures to gather digital evidence, thus ensuring that the investigation process is accurate, consistent, and precise and will lead to sufficient evidence for Saudi Arabian court of law.

Finally, the proposed framework can be used as a standard for future work in digital forensics science in Saudi Arabia. This methodology, will not only contribute to the way in which digital crime evidence is handled in the Saudi arabian court of law but it will also contribute to the development of digital forensic science as a whole by bringing it into the 21st century, with modern procedures that will be specific to all digital investigators. This will generate a level of consistency, reliability, and completeness in all future investigations of digital forensic evidence that is obtained and presented in a court of law. It will hopefully reduce and perhaps abolish the current inconsistencies and insufficiencies found in digital crime evidence brought to Saudi Arabian courts. In addition, it will prove very helpful to other countries that follow the same culture by using the factors that emerged in this research to add new contribution to their own digital forensics processes.

5.4.11 Conclusion

In this chapter dicussed and explained in more details the research findings, implementation of grounded theory, associated to the Straussian approach; which is suitable research method for analysing, investigating and exploring the

participants' opinions and views, and perspective about digital investigation process in Saudi Arabia. In addition, the answer to the research questions make the researcher able to obtain the understanding of the relating issues affecting digital investigation process in Saudi.

The chapter also described how the interpretivist approach employed, which aimed to produce a framework to build a theory that detects the reality obvious in interactions among individuals. Moreover, this enables the research to identify individual's experience, people's attitudes and deep understanding of data context. In addition, were underpinning findings of this research in literature review, and by empirical evidence. These reasons support the motives for the decisions taken throughout this research, and ensure that it contributes to knowledge.

Chapter 6:

Conclusion

Objectives

-
- Provide a summary of answering the research questions
 - Present the research contribution
 - Provide recommendation for further work
 - Research evaluation
 - Limitations of this research
-

6.1 Introduction

This chapter concludes this research, which sought a means to achieve a comprehensive and reliable conclusion to a case by identifying the factors that influence the digital investigation process and to address the challenges that arise when ensuring that evidence gathered is as complete as possible and admissible in a court of law. In particular, this research aimed to improve the accuracy of digital forensics in cases where the evidence is incomplete. This chapter also summarises the study contribution, research questions and the answers found, the research limitations, and recommendations from the author to overcome the barriers to the adoption of digital forensics in the absence of complete evidence in the context of Saudi Arabia.

6.2 Research contribution

The main objective of this research was to extend the existing the digital investigation processes and present a theoretical framework to facilitate the adoption of digital investigation procedures in cases where there is insufficient evidence, by identifying those factors, which impact on the digital investigation process. A secondary intention was to answer the research question: “How can the accuracy of the digital forensic procedure in the absence of complete evidence be improved in Saudi Arabia?” This encouraged the researcher to investigate those factors that influence digital investigation processes, and to examine why these factors constitute an impediment to the digital investigation process in Saudi Arabia. Determination of the relationship between these factors and their effect

on one another was achieved. This was apparent in the data collected from the participants and when analysing the data (see chapter 5).

In addition, the researcher covered additional issues by posing the following sub-questions:

- *What is Digital Forensics?*

This thesis provides the definitions of digital forensics in chapter 2, and relies on these definitions of digital forensics throughout the research.

- *What is digital forensics in Saudi Arabia?*

The status of digital forensics in Saudi Arabia is described in chapter 2, specifically in section 2.4. This section also introduces Legislation in Saudi Arabia and Sharia Law. In section 2.5 was introduced digital forensics in Saudi Arabia, digital forensics procedures, digital evidence, the extent of digital crime in Saudi Arabia and drug crimes in Saudi Arabia.

- *What is the nature of the relationship between each factor and how does that relationship affect the overall process of digital investigation in cases where there is insufficient evidence in the Saudi Arabia context?*

This question was part of a full empirical study, as discussed in chapter 5, where grounded theory was applied to participants' perspectives in reference to cases involving drugs issues that influence the adoption of digital investigation processes in cases of insufficient evidence. Moreover, additional Investigation Procedures in Drug Cases, and in cases where the

Absence of Complete Evidence is a factor, had an essential impact on the adoption of digital investigation process.

In addition, the research questions answered afforded an understanding of how digital investigation process factors impact digital investigation processes in the absence of complete evidence of adoption in Saudi Arabia. Moreover, each factor was discussed and explained in relation to the participants' answers, as detailed in chapter 5.

The findings are supported by the empirical evidence and literature review.

1. This study has implemented grounded theory for the research analysis to analyse the impact of those factors on the adoption of a digital investigation process in the absence of sufficient evidence to be the first kind of study that has used this research methodology.
2. The contribution of this study to the field of the digital investigation processes in the absence of sufficient evidence by investigating novel factors (insufficient evidence, drugs linked to other suspects, link between cases, collection of incomplete information and linking of incomplete information and linking of suspect's responses during interrogation) influencing the digital investigation processes in the absence of sufficient evidence in the Saudi context. Where the previous research concentrated on improving the digital investigation processes to make it more comprehensive (Yusoff, Ismail and Hassan, 2011) and meet the demands of different legal systems for the protection of privacy and to support decision making by field officers (Hong, Yu, Lee and Lee, 2013). Thus, this research makes a novel contribution, in particular in Saudi Arabia, to the field of enhancing the accuracy of digital investigation processes in the absence of sufficient evidence.

3. There are factors of relevance to Saudi Arabia which are new and significant that was revealed by this research, including the absence of complete evidence, drugs linked to other suspects, link between cases, collection of incomplete information and linking of incomplete information and linking of suspect's responses during interrogation. This factors a unique contribution to the digital investigation process of Saudi Arabia.
4. The core component has been to extend the investigation phases to achieve the level of completeness in the digital forensics investigation processes in the absence of sufficient evidence in Saudi Arabia. The grounded theory was validated through empirical work generated with the data which presented the different attitudes of investigators. The proposed model is novel, where the integration of all the different stages of the investigation processes that have been proposed by researchers to gain a comprehensive and integrated model for reaching the accuracy of investigation, in addition to the finding that helped in the production of the Traceback stage which deals with insufficient evidence.
5. This study differs from previous studies which are mentioned in chapter 2, section 2.2 on the adoption of a digital investigation process in the absence of sufficient evidence, where they concentrated on the admissibility of evidence in the court of law (Pollitt, 1984), building the mechanism for faster investigation (Carrier and Spafford ,2003), providing a foundation for the development of tools and techniques (Ciardhuain, 2004), improve the understanding for the issues of integrity, privacy and accessibility of the evidence (Al-Murjan and Xynos, 2008), developing a generic computer investigation model (Yusoff, Ismail and Hassan ,2011) and meeting the demands of different legal systems for the protection of privacy and supporting decision making by field officers (Hong, Yu, Lee and Lee,2013).

6.3 Recommendations for Further work

To overcome the barriers to the digital investigation process in the absence of sufficient evidence, further research is recommended. The following actions are recommended:

- The researcher recommends validating this model in different contexts to extend the generalisability and contribution of this model.
- A further recommendation is to retest factors identified in different contexts to determine if they have the same impact or less significant.

6.4 Research limitation

This research is the first of its kind in the field of digital investigation in the absence of complete evidence in Saudi Arabia; it has limitations, as follows:

- The semi-structured method was used to collect data face to face from participants who were selected from the Investigation and Prosecution Authority. The data collection was limited to Tabouk city in Saudi Arabia, because it is a border city, in which drug cases abound. Moreover, it would have been difficult to conduct empirical studies including other Saudi cities because of the time involved in travelling between them.
- The limitation in this research relates to the effect of the absence of complete evidence regarding the digital investigation processes in Saudi Arabia.
- The theoretical framework of this research is limited to the Saudi Arabian context, the findings may be generalised with further complementary

research confirming its conclusions. In future the findings will be build based on the context of researchers shared factors and local culture.

6.5 Conclusion

This study focused on digital investigation processes and the factors which impact them., This research also applies the grounded theory as a qualitative research method for developing the current digital investigation process where there is insufficient evidence, ,from the perspectives of investigators in Saudi Arabia. The data was analysed by Straussian approach and revealed the relationship between the core category and its sub-categories; as explained in chapter 5.

Furthermore, this research contributes to the body of knowledge by addressing issues and factors previously found in the literature. This research has a theoretical framework of practical and methodological implications (as mentioned in more detail in chapter 5), and this should assist researchers including stakeholders, government, decision-makers to do more to understand the factors affecting the adoption of digital investigation processes in absence of complete evidence in the Saudi context.

References

- Abbas, N. H. (2009). Qur'an's search for a concept tool and website (Doctoral dissertation, University of Leeds (School of Computing)).
- Abdel-Baky, M.F. (1951). Al-Mowatae of Imam El-Aema wa Alem El Madina, Malek Ibn Anas, El-Shaeb Book. Husn El Kholok, Hadith # 8, p. 564.
- Achille, M. M., & Roger, A. E. (2014). Obtaining Digital Evidence from Intrusion Detection Systems. *International Journal of Computer Applications*, 95(12), 34-41.
- Adams, R. (2012). *The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice* (Doctoral dissertation, Murdoch University).
- Adobe Systems Incorporated, *PDF Reference- Adobe Portable Document Format*, 5th ed, Version 1.6, 14 November 2004. Retrieved 12 March 2014 from <http://partners.adobe.com/public/developer/en/pdf/PDFReference16.pdf>.
- Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. C. (2011). Systematic digital forensic investigation model. *International Journal of Computer Science and Security (IJCSS)*, 5(1), 118-131.
- Agarwal, R., & Kothari, S. (2015). Review of digital forensic investigation frameworks. In *Information Science and Applications* (pp. 561-571). Springer Berlin Heidelberg.
- Aguirre, R. T., and Bolton, K. W. (2014) Qualitative interpretive meta-synthesis in social work research: Uncharted territory. *Journal of Social Work*, Vol. [14], No. 3, pp. 279-294.
- Ahmed Laithi. (2015). «Cyber attacks» penetrate the Saudis privacy. Available: <http://www.al-madina.com/node/588705>. Last accessed 11th OCT 2016.
- Alanazi, F., & Jones, A. (2015). The Value of Metadata in Digital Forensics. In *Intelligence and Security Informatics Conference (EISIC), 2015 European* (pp. 182-182). IEEE.
- Al Beshri Mohammed. (2008). Habilitation investigators for computer crimes and Internet networks. Naif Arab University for Security Science. 1 (1), 33-34.
- Alfaifi, M.A. (2001). The Economic Crimes Adjudgments in the Computer. Al-Hakeem, Mohammad Bin Abdullah (1990). Almustadrak, Dar Alkutob Publish, 1990. (In Arabic)
- Al Hwaimel, A. (2009). The application of the Sharia and its impact on the Nations . Riyadh: Dar Ibn Al Atheer. 1-48.

Ali Qamar. (2014). *What is Tor Proxy and Whether You Should Use It or Not*. Available: https://securitygladiators.com/2014/10/12/tor-proxy-and-its-uses/?nabe=5494145976369152:1&utm_referrer=https%3A%2F%2Fwww.google.com.sa%2F. Last accessed 20th Mar 2017.

Al ittihad. (2016). *Cybercrime.. gained profits more than what gained by drug trade* . Available: <http://www.alittihad.ae/details.php?id=5035&y=2016>. Last accessed 21th Sep 2016.

Alkout, A. and Khalfan, A. (2004) The use of case study methodology on IT/IS research: a framework of issues, In EMCIS 2004 (Ed.), European & Mediterranean Conference on Information Systems, Tunis.

Allan, G. 2003. A critique of using grounded theory as a research method. *Electronic Journal of Business Research Methods*, 2 (1), pp.1-10.

Al-Murjan, A., & Xynos, K. (2008, April). Network Forensic Investigation of Internal Misuse/Crime in Saudi Arabia: A Hacking Case. In *Proceedings of the Conference on Digital Forensics, Security and Law* (pp. 15-32).

Al-onzi. A. (2009). Discretionary authority of investigator in Saudi penal procedural law: a root-oriented comparative-applied study. Available: <http://repository.nauss.edu.sa/bitstream/handle/123456789/56923/%D8%A7%D9%84%D8%B3%D9%84%D8%B7%D8%A9%20%D8%A7%D9%84%D8%AA%D9%82%D8%AF%D9%8A%D8%B1%D9%8A%D8%A9%20%D9%84%D9%84%D9%85%D8%AD%D9%82%D9%82%20>. Last accessed 12th OCT 2016.

Al qahtani. A. (2014). *Improving interrogation skills to confront information crimes from Bureau of Investigation and Prosecution investigators in Riyadh city point of view*. Available: <http://repository.nauss.edu.sa/handle/123456789/54573>. Last accessed 15 OCT 2016.

Al-sahimi. H. (2007). The role of experts in penal trial in consonance to Saudi penal procedural law: an original analytical study . Available: <http://repository.nauss.edu.sa/bitstream/handle/123456789/51631/%D8%AF%D9%88%D8%B1%20%D8%A7%D9%84%D8%AE%D8%A8%D9%8A%D8%B1%20%D9%81%D9%8A%20%D8%A7%D9%84%D8%AF%D8%B9%D9%88%D9%89%20%D8%A7%D9%84%D8%AC%D8%>. Last accessed 08 11th 2016.

Ariane. (2013). How to forgive those who have hurt you, even when it's difficult. Available at <http://decodingeden.com/how-to-forgive-others-fault-even-when-its-difficult/>. Last accessed 28/05/2016.

Arain, M., Campbell, M. J., Cooper, C. L., & Lancaster, G. A. (2010). What is a pilot or feasibility study? A review of current practice and editorial policy. *BMC medical research methodology*, 10(1), 67.

Atalla, S. (2010). *The fight against cybercrime in Saudi Arabia*. Retrieved 01 15, 2015, from King Saud University: <http://faculty.ksu.edu.sa/shaimaaatalla/Pages/crifor.aspx>.

Avison, D., Dwivedi, Y.K., Fitzgerald, G. and Powell, P., (2008) The beginnings of a new Era: Time to reflect on 17 years of the ISJ, *Information Systems Journal*, Vol. [18], No. 1, pp.5-21.

BABBIE, E.R. and BENAQUISTO, L. (2002) *Fundamentals of Social Research*. Scarborough: Nelson Thomson Learning

Baca, M., Cosic, J., & Cosic, Z. (2013, June). Forensic analysis of social networks (case study). In *Information Technology Interfaces (ITI), Proceedings of the ITI 2013 35th International Conference on* (pp. 219-223). IEEE.

Backman, K., and Kyngas, H. 1999. Challenges of the grounded theory approach to a novice researcher. *Nursing and Health Sciences*, 1, pp. 147-153.

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

BCS. (2006), Presenting digital evidence to court. Available at <http://www.bcs.org/content/ConWebDoc/7372>. Last accessed 14/06/2016.

Bell, J., & Waters, S. (2014). *Doing Your Research Project: A guide for first-time researchers*. McGraw-Hill Education (UK).

Bem, D., Feld, F., Huebner, E., & Bem, O. (2008). Computer Forensics-Past, Present and Future. *Journal of Information Science and Technology*, 5(3), 43-59.

Ben-Assuli et al (2014). Using electronic health record systems to optimize admission decisions: The Creatinine case study. *Health informatics journal*, 1460458213503646.

Blaxter, L., Hughes, C., and Tight, M. (1996) *How to research*, Buckingham: Open University Press.

Brady, H. E., & Collier, D. (Eds.). (2010). *Rethinking social inquiry: Diverse tools, shared standards*. Rowman & Littlefield Publishers.

Brown, C. L. (2010). *Computer evidence: Collection and preservation*. Nelson Education.

BRYMAN, A. (2001) *Social Research Methods*. Oxford: Oxford University Press.

Bryant, A. (2002). Re-grounding grounded theory. *JITTA: Journal of Information Technology Theory and Application*, 4(1), 25.

Bryman, A. (2004) *Understanding Research for Social Policy and Practice: Themes, Methods and Approaches*. The Policy Press.

Burawoy, M. (1991). Reconstructing social theories. In M. Burawoy (Ed). *Ethnography unbound. Power and resistance in the modern metropolis* (pp. 8-27). Berkeley: University of California Press.

Calitz, M. G. (2009). A cultural sensitive therapeutic approach to enhance emotional intelligence in primary school children (Doctoral dissertation). Retrieved from <http://uir.unisa.ac.za/handle/10500/1648> on 16 October, 2014.

camel, T. M. (2012, 02 26). *Digital evidence in criminal prosecution*. Retrieved 01 20, 2015, from Star Times Forums: <http://www.startimes.com/f.aspx?t=30245909>

Carpenter, D. 2011. Grounded theory as method. In: Surrena, H (ed). *Qualitative research in nursing*. Philadelphia: Lippincott williams & wilkins, pp.123-139.

Casey, E. (2010). Digital investigations, security and privacy. *Digital Investigation*, 7(1), 1-2.

Centre Arabe de Recherches Juridiques et Judiciaires (CARJJ), (2012, 12 17). Claims of digital crimes and their proving evidences, in Arab legislations between reality and expectations. Retrieved 01 2015, 20, from Centre Arabe de Recherches Juridiques et Judiciaires (CARJJ):

<https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCEQFjAA&url=http%3A%2F%2Fwww.carjj.org%2Fsites%2Fdefault%2Ffiles%2F%25D8%25AF%25D8%25B9%25D8%25A7%25D9%2588%25D9%2589%2520%25D8%25A7%25D9%2584%25D8%25AC%25D8%25B1%25D8%>

Chabot, Y., Bertaux, A., Nicolle, C., & Kechadi, M. T. (2014). A complete formalized knowledge representation model for advanced digital forensics timeline analysis. *Digital Investigation*, 11, S95-S105.

Chandrakumar, F. J., Bridge, A. A. D., Card, S. D., Unit, G. G. P., & Memory, R. R. A. (2014). An evidence-based Android cache forensics model.

Charmaz, C. 2006. *Constructing grounded theory: A practical guide through qualitative analysis (introducing qualitative methods series)*. Newbury Park: SAGE Publication Ltd.

- Charmaz, C. 2003. Grounded theory: Objectivist and constructivist methods. In: Denzin, N and Lincoln, Y (eds). *Strategies of qualitative inquiry*. CA: Sage Publications, pp. 249-292.
- Charmaz, K. (1990). 'Discovering' chronic illness: Using grounded theory. *Social Science and Medicine*, 30(11), 1161-1172.
- Charmaz, K. (1983). The grounded theory method: An explication and interpretation. In R. Emerson (Ed.), *Contemporary field research: A collection of readings* (pp. 109-126). Boston, MA: Little Brown Com-pany.
- Charmaz, K. (2008). Grounded theory. In J. A. Smith (Ed.), *Qualitative psychology: A practical guide to research methods* (pp. 81-110). Los Angeles: SAGE.
- Chen, W.S., and Hirschheim, R., A., (2004) paradigmatic and methodological examination of information systems research from 1991 to 2001, *Information Systems Journal*, Vol. [14], No. 3, pp.197–235.
- Chenitz, C., and Swanson, J. 1986. Qualitative research using grounded theory. In: Chenitz, C and Swanson, J (eds). *From practice to grounded theory: Qualitative research in nursing*. California: Addison Wesley, Menlo Park, pp. 3-15.
- Chiovitti, R., and Piran, N. (2003) Rigour and grounded theory research. *Journal of Advanced Nursing*, Vol. [44], No. 4, pp. 427-435.
- Chisnall, A. C. (1998). Grounded theory for knowledge acquisition.
- Chow, K. P., Law, F., & Mai, Y. H. (2014). Understanding Computer Forensics Requirements in China Via The “Panda Burning Incense” Virus Case. *Journal of Digital Forensics, Security and Law*, 9(2), 51-58.
- CHURCHILL, G.A. (1987) *Marketing Research: Methodological Foundations*. 5th ed. New York: The Dryden Press.
- Čisar, P., & Čisar, S. M. (2011). Methodological frameworks of digital forensics. In *2011 IEEE 9th International Symposium on Intelligent Systems and Informatics* (pp. 343-347). IEEE.
- Blaxter, L. (2010). *How to research*. McGraw-Hill Education (UK).
- Cosic, J., Cosic, Z., & Baca, M. (2011). " Chain of Digital Evidence" Based Model of Digital Forensic Investigation Process. *International Journal of Computer Science and Information Security*, 9(8), 18.

Cohen, F. B. (2015). Digital diplomatics and forensics: Going forward on a global basis. *Records Management Journal*, 25(1).

Coleman, G., & O'Connor, R., (2007) Using grounded theory to understand software process improvement: A study of Irish software product companies. *Information and Software Technology*, Vol. [49], pp. 654-667.

Collis, J., and Hussey, R., (2003) *Business Research: A practical guide for undergraduate and postgraduate students*. 2nd edition, Palgrave Macmillan: New York. Competence on Championing IT, *Information Systems Research*, Vol. [14], No. 4, pp.317-336.

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

Corbin, J., & Strauss, A. (2014). *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage publications.

Corbin, J., and Strauss, A. 1990. Grounded theory research: procedures, canons, and evaluative criteria. *Qualitative Sociology*, 13 (1), pp. 3-22.

Council of Europe. (2001). *Details of Treaty No.185*. Available: <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>. Last accessed 07 NOV 2016

Crawford, K., Leybourne, M., and Arnott, A. 2000. How we ensured rigour in a multi-site, multi-discipline, multi-researcher study. *Forum Qualitative Research*. [Online Journal], 1 (1), Article 12, Available at: <http://www.qualitative-research.net/fqs-texte/1-00/1-00crawfordetal-e.htm>.

Dang, T., Feng, W. C., & Bulusu, N. (2011, April). Zoom: A multi-resolution tasking framework for crowdsourced geo-spatial sensing. In *INFOCOM, 2011 Proceedings IEEE* (pp. 501-505). IEEE.

Decoo, W. (1996) 'The Induction-Deduction Opposition: Ambiguities and Complexities of the Didactic Reality', *International Review of Applied Linguistics*, Vol. 34, No. 2, pp. 95-118

Dempsey, J. S. (2010). *Introduction to private security*. Cengage Learning.

Denscombe, M. (2003). *The social research guide*. second edition Edition. 2nd ed. Philadelphia, USA: Open University Press.

Denzin, N. K., & Lincoln, Y. S. (2000). Introduction. In N. K. Denzin & Y. S. Lincoln, *The discipline and practice of qualitative research. Handbook of qualitative research* (pp. 1-29). London: Sage.

Denzin, N and Lincoln, Y (Eds) (1994) *Handbook of Qualitative Research*, Thousand Oaks (Calif), Sage

De Vos, A.S. 2002b. Intervention research. (In De Vos, A.S., ed., Strydom, H., Fouchè, C.B., & Delpont, C.S.L. *Research at grass roots: for the social sciences and human service professions*. 2nd ed. Pretoria: Van Schaik. p. 394-418).

De Wit, J. (2013). *Continuous Forensic Readiness*.

Demirchyan, A., Goenjian, A. K., & Khachadourian, V. (2014). Factor Structure and Psychometric Properties of the Posttraumatic Stress Disorder (PTSD) Checklist and DSM-5 PTSD Symptom Set in a Long-Term Postearthquake Cohort in Armenia. *Assessment*, 1073191114555523.

Dr. Hani. (2009). *Empirical Research*. Available: <http://researcheshealthcenter.webs.com/>. Last accessed 10/10/2014.

Dr. Robergs . (2010). *Introduction to Empirical Research*. Available: <http://www.unm.edu/~rrobergs/604Lecture3.pdf>. Last accessed 01/11/2014.

E. S. Pilli, R. C. Joshi, & R. Niyogi, (2010) “Network Forensic frameworks: Survey and research challenges,” *Digital Investigation*, Vol. 7, pp. 14-27.

Editorial. (2006). Biomedical research ethics: An Islamic view, part I. *International Journal of Surgery*.

.Edwin R. van Teijlingen and Vanora Hundley. (2001). The importance of pilot studies. Available: <http://sru.soc.surrey.ac.uk/SRU35.html>. Last accessed 10 Oct 2014.

Elers, S. (2014). Online investigation: Using the internet for investigative policing practice.

EM Ahmed Elsheik, M. (2016). A Survey in Modern Techniques in Digital Forensic Evidence in Graphics Design Applications. *International Multilingual Academic Journal*, 1(1).

Fernández, W. 2004. Using the glaserian approach in grounded studies of emerging business practices. *Electronic Journal of Business Research Methods*, 2(2), pp. pp.83-94.

Fernández, W. D. (2004). The Glaserian approach and emerging business practices in information systems management: Achieving relevance through conceptualisation. *3rd*

European Conference on Research Methodology for Business and Management Studies. A. Brown and D. Remenyi. Reading UK, University of Reading.

Fernández, W. D., Martin, M. A., Gregor, S. D., Stern, S. E., & Vitale, M. R. (2006). A multi-paradigm approach to grounded theory. *Information Systems Foundations Workshop: Constructing and Criticising*, School of Accounting and Business Information Systems, College of Business and Economics, The Australian National University, Canberra, Australia, 2006.

Fernández, W. D., & Lehmann, H. (2005). Achieving rigour and relevance in information systems studies: Using grounded theory to investigate organizational cases. *The Grounded Theory Review*, 5(1), 79-107.

Figueiras, J., & Frattasi, S. (2011). *Mobile positioning and tracking: from conventional to cooperative techniques*. John Wiley & Sons.

Fitzgerald, B., & Howcroft, D. (1998, December). Competing dichotomies in IS research and possible strategies for resolution. In Proceedings of the international conference on Information systems (pp. 155-164). Association for Information Systems.

Floyd, K., & Yerby, J. (2014). DEVELOPMENT OF A DIGITAL FORENSICS LAB TO SUPPORT ACTIVE LEARNING. *DEVELOPMENT*, 4, 14-2014.

Fox, N. (2009) Using Interviews in a Research Project, Yorkshire and Humber: NIHR

Freiling, F. C., & Schwittay, B. (2007). A common process model for incident response and computer forensics. Paper presented at the Conference on IT Incident Management and IT Forensics, Germany.

Frowen, A. (2009). *Computer forensics in the courtroom: Is an IT literate judge and jury necessary for a fair trial?* Retrieved April 20, 2010, from <http://www.articlesnatch.com/Article/Computer-Forensics-In-The-Courtroom--Is-An-It-Literate-Judge-And-Jury-Necessary-For-A-Fair-Trial-/568057>.

Frühwirt, P., Kieseberg, P., Schrittwieser, S., Huber, M., & Weippl, E. (2013). InnoDB database forensics: Enhanced reconstruction of data manipulation queries from redo logs. *Information Security Technical Report*, 17(4), 227-238.

Gabe, M. N. (2010, 05 12). *INFORMATIONAL CRIME* . Retrieved 01 2015, 21, from <http://www.iasj.net/iasj?func=fulltext&aId=28397>
iraqi academic scientific journals:

Garfinkel, S. (2012). Digital forensics XML and the DFXML toolset. *Digital Investigation*, 8(3), 161-174.

Gayed, T. F., Lounis, H., Bari, M., & Nicolas, R. (2013, May). Cyber Forensics: Representing and Managing Tangible Chain of Custody Using the Linked Data

Principles. In *COGNITIVE 2013, The Fifth International Conference on Advanced Cognitive Technologies and Applications* (pp. 87-96).

Geertz, C. (1973). *The interpretation of cultures: Selected essays*. New York: Basic Books.

Gehl, R. W. (2014). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *new media & society*, 1461444814554900

George J. Wallace . (2004). *The Role of Empirical Research*. Available: <https://www.afsaonline.org/CMS/fileREPOSITORY/The%20Role%20of%20Empirical%20Research.pdf> . Last accessed 20/10/2014.

Geri, N., & Geri, Y. (2011). The information age measurement paradox: Collecting too much data, *Inform-ing Science: the International Journal of an Emerging Transdiscipline*, 14, 47-59. Retrieved from <http://www.inform.nu/Articles/Vol14/ISJv14p047-059Geri587.pdf>

Gillespie, A. A. (2015). *Cybercrime: key issues and debates*. Routledge.

Glaser, B., and Strauss, A. 1967. *The discovery of grounded theory*. Chicago: Aldine.

Glaser, B. 1978. *Theoretical sensitivity: Advances in the methodology of grounded theory*. Mill valley, California: Sociology Press.

Glaser, B. 1992. *Emergence vs forcing: basics of grounded theory*. Mill Valley, California: Sociology Press.

Glaser, B. G. (1998). *Doing grounded theory. Issues and discussions*. Mill Valley, CA: Sociology Press.

Glaser, B. G. (2001). *The grounded theory perspective: Conceptualization contrasted with description*. Mill Valley, CA: Sociology Press.

Goulding, C. (1998). Grounded theory: The missing methodology on the interpretivist agenda. *Qualitative Market Research: An International Journal*, 1(1), 50-57.

Goulding, C. (2001). Grounded theory: A magical formula or a potential nightmare. *The Marketing Review*, 2(1), 21-33.

Grispos, G., Glisson, W. B., & Storer, T. (2014). Rethinking Security Incident Response: The Integration of Agile Principles. *arXiv preprint arXiv:1408.2431*.

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. *Handbook of qualitative research*, 2(163-194), 105.

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field methods*, 18(1), 59-82.

Gummesson, E. (1991) Marketing-orientation Revisited: The Crucial Role of the Part-time Marketer, *European Journal of Marketing*, Vol. [25], No. 2, pp. 60-75.

Halboob, W., Mahmood, R., Abulaish, M., Abbas, H., & Saleem, K. (2015, April). Data Warehousing Based Computer Forensics Investigation Framework. In *Information Technology-New Generations (ITNG), 2015 12th International Conference on* (pp. 163-168). IEEE.

Hanaei, E. H. A., & Rashid, A. (2014, May). DF-C2M2: A Capability Maturity Model for Digital Forensics Organisations. In *Security and Privacy Workshops (SPW), 2014 IEEE* (pp. 57-60). IEEE.

Heath, H., and Cowley, S. 2004. Developing a grounded theory approach: A comparison of glaser and strauss. *International Journal of Nursing Studies*, 41 (2), pp. 141-150.

Hirwani, M., Pan, Y., Stackpole, B., & Johnson, D. (2012). Forensic acquisition and analysis of vmware virtual hard disks. The 2012 International Conference on Security and Management.

Hlady-Rispal, M., & Jouison-Laffitte, E. (2014). Qualitative research methods and epistemological frameworks: a review of publication trends in entrepreneurship. *Journal of Small Business Management*, 52(4), 594-614.

Hoepfl, M. C., (1997) Choosing qualitative research: A primer for technology education researchers. *Journal of Technology Education*, Vol. [9], No.1, pp. 47-63.

Holt, T. J., Blevins, K. R., & Burruss, G. W. (2012). Examining the stress, satisfaction, and experiences of computer crime examiners. *Journal of Crime and Justice*, 35(1), 35-52.

Hong, I., Yu, H., Lee, S., & Lee, K. (2013). A new triage model conforming to the needs of selective search and seizure of electronic evidence. *Digital Investigation*, 10(2), 175-192.

Human Rights Council. (2016). *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development*. Available:
http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session31/Documents/A%20HRC%2031%2055_A.docx. Last accessed 07 NOV 2016.

Hurley, A.E., Scandura, T.A, Schriesheim, C.A., Brannick, M.T., Seers, A., Vandenberg, R.J. and Williams, L.J. (1997) 'Exploratory and Confirmatory Factor Analysis Guidelines, Issues and Alternatives', *Journal of Organisational Behaviour*, Vol. 18, pp. 667-683

Hutchinson, S. A. (1988). Education and grounded theory. In R. R. Sherman & R. B. Webb (Eds.), *Qualitative research in education: Focus and methods*. Lewes, UK: The Falmer Press.

Imam Nawawi's Forty Hadith: Hadith 32, 33, and 34: Do not harm, Burden of proof, Resisting evil. Available at <http://bible-Qur'an.com/islam-hadiths-hadiths-32-34-nawawi/>. Last accessed 07/06/2016.

Ishihara, N., & Cohen, A. D. (2014). *Teaching and learning pragmatics: Where language and culture meet*. Routledge.

Islamweb. (2009). Morality in Islam. Available at <http://www.islamweb.net/en/article/134385/morality-inislam>. Last accessed 28/05/2016.

Isra Hosni. (2016). The Dark Web. Available: <http://www.youm7.com/story/2016/1/21/-%D8%A7%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%A7%D9%84%D9%85%D8%B8%D9%84%D9%85-%D8%A7%D9%84%D8%B3%D9%88%D9%82-%D8%A7%D9%84%D8%A3%D9%88%D9%84-%D9%84%D8%AA%D>. Last accessed 11th OCT 2016.

Johnson, B. and Christensen, L (2008) *Educational Research: Quantitative, Qualitative, and Mixed Approaches*, Thousand Oaks: Sage Publication

Johnson, B., and Turner, L.(2003). Data collection strategies in mixed methods research. In: Tashakkori, A and Teddye, C (eds). *Handbook of mixed methods in social and behavioural research*. Thousands Oaks, California: Sage Publications, pp. 297-320.

Kahlke, R. (2014). Generic qualitative approaches: pitfalls and benefits of methodological mixology. *International Journal of Qualitative Methods*, 13, 37-52.

Kaisi, N. A. (2011, 12 14). *Some Internet crimes against Internet users in Saudi Arabia*. Retrieved 01 11, 2015, from Umm Al-Qura Univesity: https://uqu.edu.sa/lib/digital_library/saudi_msgs_view/ar/4/141

Karie, N. M., & Venter, H. S. (2014, March). A Generic Framework for Enhancing the Quality of Digital Evidence Reports. In *13th European Conference on Cyber Warfare and Security ECCWS-2014 The University of Piraeus Piraeus, Greece* (p. 251).

Karl Claxton, Simon Eggington, Laura Ginnelly, Susan Griffin, Christopher McCabe, Zoe Philips, Paul Tappenden and Alan Wailoo. (2005). *A Pilot Study of Value of Information Analysis to Support Research Recommendations for the National Institute for Health and Clinical Excellence*. Available: http://www.york.ac.uk/media/che/documents/papers/researchpapers/rp4_Pilot_study_of_value_of_information_analysis.pdf. Last accessed 01/11/2014.

Kalla, D. (2014). Prison Education: an interdisciplinary examination of prisons, punishment, schools, and education.

Kerrigan, M. (2013). A capability maturity model for digital investigations. *Digital Investigation*, 10(1), 19-33.

Kessler, G. C. (2010). *Judges' awareness, understanding, and application of digital evidence* (Doctoral dissertation, Nova Southeastern University).

Khairul, N. (2008). Case study: A strategic research methodology. *American Journal of Applied Sciences*, 5 (11), pp.1602-1604.

Khalid Al Shaya. (2016). Saudi Arabia: arrest promoter drugs via the "snapchat". Available:

<https://www.alaraby.co.uk/society/2016/3/30/%D8%A7%D9%84%D8%B3%D8%B9%D9%88%D8%AF%D9%8A%D8%A9-%D8%B6%D8%A8%D8%B7-%D9%85%D8%B1%D9%88%D8%AC%D9%8A-%D9%85%D8%AE%D8%AF%D8%B1%D8%A7%D8%AA-%D8%B9%D8%A8%D8%B1-%>. Last accessed 12th OCT 2016.

Khdhir, C. H. (2015). Change in the Perceptions of Pre-Service Teachers as a Result of the Difficulties They Faced During Elt Practicum: Insights from a Four-Week Teaching Practice Period. AuthorHouse.

Khusro, S., Latif, A., & Ullah, I. (2014). On methods and tools of table detection, extraction and annotation in PDF documents. *Journal of Information Science*, 0165551514551903.

Kilungu, M. K. (2015). *An Investigation of Digital Forensic Models Applicable in the Public Sector (A case of Kenya National Audit Office)* (Doctoral dissertation).

Kim, K. J. (Ed.). (2015). *Information Science and Applications* (Vol. 339). Springer.

King, G., Keohane, R. O., & Verba, S. (1994). Designing social inquiry: Scientific inference in qualitative research. Princeton university press.

Kohn, M. D., Eloff, M. M., & Eloff, J. H. (2013). Integrated digital forensic process model. *Computers & Security*, 38, 103-115.

- Joshi, R. C., & Pilli, E. S. (2016). *Fundamentals of Network Forensics: A Research Perspective*. Springer.
- Ilieva, S. (2014). COMPONENTS OF THE DELPHI PROCESS THEORETICAL AND RESEARCH STUDIES. *ASSOCIATION SCIENTIFIC AND APPLIED RESEARCH*, 2, 128.
- Lang, A. (2014). A new portable digital forensics curriculum.
- Laudon, K. C., & Traver, C. G. (2007). *E-commerce*. Pearson/Addison Wesley.
- Lee, A. S. (1991). Integrating positivist and interpretive approaches to organizational research. *Organization science*, 2(4), 342-365.
- Lee, K., & Boddington, M. R. (2012). A Workflow to Support Forensic Database Analysis.
- Leon, A. C., Davis, L. L., & Kraemer, H. C. (2011). The role and interpretation of pilot studies in clinical research. *Journal of psychiatric research*, 45(5), 626-629.
- Leslie, D. A. (2014). Introduction, Money Laundering and Cyber crime. In *Legal Principles for Combatting Cyberlaundering* (pp. 1-54). Springer International Publishing.
- Leslie, D. A. (2014). Cyberlaundering: Concept & Practice. In *Legal Principles for Combatting Cyberlaundering* (pp. 55-117). Springer International Publishing.
- Leslie, D. A. (2014). The Present International and National Legal Framework Against Cyberlaundering. In *Legal Principles for Combatting Cyberlaundering*(pp. 119-200). Springer International Publishing.
- Li, J. T., Tang, Z. Y., & Li, X. (2011). Computer intrusion forensic based on temporal logic of actions. *Application Research of Computers*, 7, 098.
- Li, S., Rickert, R., & Sliva, A. (2013). Risk-Based models of attacker behavior in cybersecurity. In *Social Computing, Behavioral-Cultural Modeling and Prediction* (pp. 523-532). Springer Berlin Heidelberg.
- Lichtman, M. (2006) *Qualitative Research in Education: A Users' Guide*, Thousand Oaks: Sage Publication
- LoBiondo-Wood, G., & Haber, J. (2006) *Nursing research: Methods and critical appraisal for evidence-based practice* (6th edition). St. Louis, MO: Mosby
- Locke, K. 1996. Rewriting the discovery of grounded theory after 25 years. *Journal of Management Inquiry*, 5 (3), pp. 239-246.
- Locke, K. (2001). *Grounded theory in management research*. London: Sage.

- Lutui, P. R. (2015). *Digital forensic process model for mobile business devices: smart technologies* (Doctoral dissertation, Auckland University of Technology).
- Lutui, R. (2016). A multidisciplinary digital forensic investigation process model. *Business Horizons*, 59(6), 593-604.
- Madkoar, M.S. (1980). The Effect of Islamic Legislation on Crime Prevention in Saudi Arabia. Ministry of Interior, Kingdom of Saudi Arabia, (In Arabic)
- Magnus, J. (2014). Evidentiary data collection from Global Positioning Systems: A qualitative study from a Queensland Police Search Coordinator's perspective. *www.journalofsar.org*, 20.
- Mahmoud El-Deeb. (2015). Drug smuggling through the (Internet) , worries the world. Available: <https://www.hitsnet.net/main/?p=9158>. Last accessed 12th OCT 2016.
- Makutsoane, M. P., & Leonard, A. (2014, July). A conceptual framework to determine the digital forensic readiness of a Cloud Service Provider. In *Management of Engineering & Technology (PICMET), 2014 Portland International Conference on* (pp. 3313-3321). IEEE.
- Malik, N. M. N. A., Yahya, S., & Abdullah, M. T. (2014). Critical Phases in Network Forensics-A Review. In *The International Conference on Digital Security and Forensics (DigitalSec2014)* (pp. 68-75). The Society of Digital Information and Wireless Communication.
- MANHEIM, J.B., RICH, R.C., and WILLNAT, L. (2002) *Empirical Political Analysis: Research Methods in Political Science*. New York: Longman.
- Manning, P., and Smith, G. 2010. Symbolic interactionism. In: Elliott, A (ed). *The routledge companion to social theory*. Oxon: Routledge, pp. 37-56.
- Mason, S. (2008). Judges and technical evidence. Keynote address at CFET 2008: The 2nd International Conference on Cyberforensics Education and Training, Canterbury Christ Church University, Canterbury, UK, September.
- Mertens, D. M. (2014). *Research and evaluation in education and psychology: Integrating diversity with quantitative, qualitative, and mixed methods*. Sage Publications.
- MEYERS, L.S., GAMST, G., and GUARINO, A.J. (2006) *Applied Multivariate Research: Design and Interpretation*. Sage Publications Inc.

- MILES D. WOKEN . (2013). *Advantages of a Pilot Study*. Available: <http://www.uis.edu/ctl/wp-content/uploads/sites/76/2013/03/ctlths7.pdf>. Last accessed 23/10/2014.
- Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. Sage.
- Mohammed Al-Ghamdi. (2016). The drug trade over the Internet. Available: <http://www.alriyadh.com/1142921>. Last accessed 12th OCT 2016.
- Mohammed, A., & Nwachukwu, E. O. (2015). Computer Forensic: A Reactive Strategy for Fighting Computer Crime. *International Journal of Computer Science and Security (IJCSS)*, 9(3), 157.
- Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information systems research*, 2(3), 192-222.
- Morey, N. C., & Luthans, F. (1984). An emic perspective and ethnoscience methods for organizational research. *Academy of Management Review*, 9(1), 27-36.
- Morgan, G., & Smircich, L. (1980). The case for qualitative research. *Academy of management review*, 5(4), 491-500.
- Morse, J. M. (1994). Designing funded qualitative research.
- Muhammad Farooq-i-Azam Malik (2001). *Al-Qur'an, the Guidance for Mankind - English Translation of the Meanings of Al-Qur'an with Arabic*. U.S: The Institute of Islamic Knowledge. 691-692.
- Myers, M. D., (1997) *Qualitative Research in Information Systems*. *MIS Quarterly*, Vol. [21], No.2, pp. 241-242. *MISQ Discovery*, archival version. http://www.misq.org/discovery/MISQD_isworld/. *MISQ Discovery*, updated version, last modified: May 13, 2010 www.qual.auckland.
- Myers, M., and Avison, D., (2002) *Qualitative Research Information System*. SAGA Publication Ltd, London.
- Nasirin, S., Birks, D. F., & Jones, B. (2003). Re-examining fundamental GIS implementation constructs through the grounded theory approach. *Telematics and Informatics*, 20(4), 331-347.
- Nations, G. M., Gourley, C. R., Gonsalves, M. F., & Neidermire, T. (2014). *U.S. Patent No. D715,818*. Washington, DC: U.S. Patent and Trademark Office.

- NC3RS. (2006). *Conducting a pilot study*. Available: <https://www.nc3rs.org.uk/conducting-pilot-study>. Last accessed 20/07/2014.
- Neuman, W. L., & Robson, K. (2012). *Basics of social research: Qualitative and quantitative approaches*.
- Niemi, T., & Niinimäki, M. (2013, September). Data integration for phone users' mobility analysis. In *Computer Science and Engineering Conference (ICSEC), 2013 International* (pp. 120-125). IEEE.
- Nolan, D., & Lang, D. T. (2014). *XML and Web Technologies for Data Sciences with R*. Springer.
- Oates, B. (2006). *Researching information systems and computing*. London: SAGE Publications.
- OATES, B.J. (2006) *Researching Information Systems and Computing*. Middlesborough UK: Sage Publications Ltd.
- Olajide, F. (2011). *A study of application level information from the volatile memory of Windows computer systems* (Doctoral dissertation, University of Portsmouth).
- Onions, P. 2006. Grounded theory application in reviewing knowledge management literature. In: *Proceedings of the Postgraduate Research Conference on Methodological Issues and Ethical Considerations*. Leeds, UK, May 24 2006: UK: Leeds University, pp.1-20.
- Opendakker, R. (2006) 'Advantages and Disadvantages of Four Interview Techniques in Qualitative Research', *Forum Qualitative Social Research*, Vol. 7, No. 4, pp. 1-9
- Orlikowski, W. J., (1993) Case tools as organisational change: Investigating Incremental and Radical Changes in Systems Development. *MIS Quarterly*, Vol. [17], No. 3, pp. 309-340.
- Pathak, A. and Intrat, C. (2012) 'Use of Semi-Structured Interviews to Investigate Teacher Perception of Student Collaboration', *Malaysian Journal of ELT Research*, Vol. 8, No. 1, pp. 2-1-10.
- Patton, M. Q., (2002) *Qualitative evaluation and research methods* (3rd Edition). Thousand Oaks, CA: Sage Publications, Inc. Research methods.
- Perumal, S. (2009). Digital forensic model based on Malaysian investigation process. *International Journal of Computer Science and Network Security*, 9(8), 38-44.

- Phillip, C., (2005) *Window on Humanity: A Concise Introduction to General Anthropology*. New York, McGraw Hill (pp. 2-3, 16-17, 34-44).
- Placid, R., & Wynekoop, J. (2011). Tracking the Footprints of Anonymous Defamation in Cyberspace: A Review of the Law and Technology. *Journal of Information Privacy and Security*, 7(1), 3-24.
- PUTNAM, R.D. (1993) *Making Democracy Work: Civic Traditions in Modern Italy*. Princeton, NJ: Princeton University Press.
- 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.
- Robrecht, L. 1995. Grounded theory: Evolving methods. *Qualitative Health Research*, 5 (2), pp. 169-178.
- Rogers, M. K., Goldman, J., Mislán, R., Wedge, T., & Debrotá, S. (2006). Computer forensics field triage process model. In *Proceedings of the conference on Digital Forensics, Security and Law* (p. 27). Association of Digital Forensics, Security and Law.
- Rogers, M. K., Goldman, J., Mislán, R., Wedge, T., & Debrotá, S. (2016). Paper Session II: Computer Forensics Field Triage Process Model.
- Saleem, S., Popov, O., & Bagilli, I. (2014). Extended abstract digital forensics model with preservation and protection as umbrella principles. *Procedia Computer Science*, 35, 812-821.
- Samoylova, A. (2014). *A High Tech Start-up's Journey Towards Funding*.
- Sandelowski, M. 1995. Qualitative analysis: What it is and how to begin. *Research in Nursing and Health*, 18 (4), pp. 371-375.
- 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.
- SHIVELY, W.P. (1998) *The Craft of Political Research*. 4th ed. New Jersey: Prentice Hall.
- Simon, M. K. (2011). *Conducting Pilot Studies* (Doctoral dissertation, Dissertation and Scholarly Research: Recipes for Success).
- Sivula, M. (2011). Using Skype as an Academic Tool: Lessons Learned. *Elearn*, 2011(7), 7. doi:10.1145/2001333.2011843.
- Skyrius, R., & Bujauskas, V. (2010). A study on complex information needs in business activities. *Inform-ing Science: the International Journal of an Emerging Transdiscipline*,

13, 1-13. Retrieved from <http://www.inform.nu/Articles/Vol13/ISJv13p001-013Skyrius550.pdf>

Smit, J., and Bryant, A. 2000. *Grounded theory method in IS research: Glaser vs. Strauss*. Working paper, School of information management, Leeds Metropolitan University. Available from: www.lmu.ac.uk/ies/im/documents/2000. [Accessed 23-09-2014].

Solinas, F. (2014). Technical and legal perspectives on forensics scenario.

Solomon, M. G., Rudolph, K., Tittel, E., Broom, N., & Barrett, D. (2011). *Computer forensics jumpstart*. John Wiley & Sons.

Spulber, D. F. (2014). *The Innovative Entrepreneur*. Cambridge University Press.

Stern, P. N. (1994). Eroding grounded theory. In J. M. Morse (Ed.), *Critical issues in qualitative research methods* (pp. 212 -223). London: Sage.

Strauss, A., and J Corbin. 1998. *Basics of qualitative research*. London: SAGE Publications.

Strauss, A., & Corbin, J. (1998). *Basics of qualitative research: Procedures and techniques for developing grounded theory*. ed: Thousand Oaks, CA: Sage.

Strauss, A., and Corbin, J. 1990. *Basics of qualitative research: Techniques and procedures for developing grounded theory*. London: SAGE Publications.

Strauss, A., & Corbin, J. M. (1990). *Basics of qualitative research: Grounded theory procedures and techniques*. Sage Publications, Inc.

Strauss, A., and J Corbin. 1998. *Basics of qualitative research*. London: SAGE Publications.

Studies and Research Department. (2013), Claims of cybercrimes and evidence proof in the Arab legislations between reality and expectations. Available at <http://www.carjj.org/sites/default/files/%D8%AF%D8%B9%D8%A7%D9%88%D9%89%20%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85%20%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9%20%20%D8%A7%D9%>

84%D8%B3%D8%B9%D9%88%D8%AF%D9%8A%D8%A9.docx. Last accessed 12/06/2016.

Suddaby, R. (2006). From the editors: What grounded theory is not. *Academy of Management Journal*, 49(4), 633-642.

The New Arab. (2016). FBI attack the "iPhone" and end the case against the "Apple" .. Apple: We will protect users. Available:

<https://www.alaraby.co.uk/medianews/2016/3/29/fbi-%D9%8A%D8%AE%D8%AA%D8%B1%D9%82-%D8%A3%D9%8A%D9%81%D9%88%D9%86-%D9%88%D9%8A%D9%86%D9%87%D9%8A-%D8%A7%D9%84%D8%AF%D8%B9%D9%88%D9%89-%D8%B6%D8%AF-%D8%A2%>. Last accessed 26/07/2016.

Van Dijk, J. (2012). *The network society*. Sage Publications Ltd.

Van Maanen, J. (1979). Reclaiming qualitative methods for organizational research: A preface. *Administrative science quarterly*, 24(4), 520-526.

Walsham, G. (1995). Interpretive case studies in IS research: Nature and method. *European Journal of In-formation Systems*, 4(2), 74-81.

Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems*, 15(3), 320-330.

Walliman, N. 2006. *Social research methods*. London: Sage Publications.

Wareham, J., Zheng, J.G., and Straub, D., (2005) Critical themes in electronic commerce research: a meta-analysis, *Journal of Information Technology*, Vol. [20], pp.1-19.

Weber, R. (1987). Toward a theory of artifacts: A paradigmatic base for information systems research. *Journal of Information Systems*, 1(2), 3-19.

Weber, R (2004) 'The Rhetoric of Positivism Versus Interpretivism: A Personal View', *MIS Quarterly*, Vol. 28, No. 1, pp. iii-ix

Wesley, J. J. (2009, May). Building bridges in content analysis: quantitative and qualitative traditions. In Annual meeting of the Canadian Political Science Association. Carleton University, Ottawa, May (Vol. 29).

Wiechman, D.J., Kendall, J.D., & Azarian, M.K. (1994). *Islamic Law Myths and Realities*. University of Illinois

Wit, J. (2013). *Continuous forensic readiness*.

Yam, C. S., Kruskal, J., & Larson, M. (2012). Creating Animated GIF Files for Electronic Presentations Using Photoshop. *American Journal of Roentgenology*.

Yin, R. K. (2009) Case study research: Design and methods(4th edition). Thousand Oaks, CA: Sage.


Zaaiman, J., & Leenan, L. (Eds.). (2015, February). Iccws 2015-The Proceedings of the 10th International Conference on Cyber Warfare and Security: ICCWS2015. Academic Conferences Limited.

Zareen, M. S., Waqar, A., & Aslam, B. (2013, December). National University of Sciences and Technology, Islamabad, Pakistan. In *Information Assurance (NCIA), 2013 2nd National Conference on* (pp. 21-29). IEEE.

Zareen, M. S., Waqar, A., & Aslam, B. (2013, December). Digital forensics: Latest challenges and response. In *Information Assurance (NCIA), 2013 2nd National Conference on* (pp. 21-29). IEEE.

Appendix

7/23/2015 De Montfort University Mail - RE: Ethical application - Fahad ALANAZI 1415/268

 Fahad Alanazi <p0800238x@myemail.dmu.ac.uk>

RE: Ethical application - Fahad ALANAZI 1415/268

Ethics - Technology <ethics.tech@dmu.ac.uk> 6 July 2015 at 16:19
To: Fahad Alanazi <p0800238x@myemail.dmu.ac.uk>
Cc: Richard Howley <rgh@dmu.ac.uk>, Andrew Jones <andrew.jones@dmu.ac.uk>, "research.students@dmu.ac.uk" <research.students@dmu.ac.uk>, Ethics - Technology <ethics.tech@dmu.ac.uk>

Dear Fahad

Research Ethics Application Approval: 1415/268 Enhance the accuracy of digital forensic in the presence of incomplete evidence

Your application to gain ethical approval for research degree activities has been considered and APPROVED by the Faculty Human Research Ethics Committee (FHREC) on 18 June 2015.

Please be aware that changes to the project plan or unforeseen circumstances may raise ethical issues. If this is the case it is the researcher's duty to repeat the ethics approval process.

Kind regards

Anne

Anne Smith
Research & Innovation Coordinator
Research & Innovation Office (4.64)
Faculty of Technology

DE MONTFORT UNIVERSITY
Gateway Building
The Gateway
Leicester LE1 9BH
UK
T: +44 (0) 116 250 8519
E: ansmith@dmu.ac.uk
W: dmu.ac.uk

<https://mail.google.com/mail/u/0/?ui=2&ik=167530726&view=pt5&ref=ical%20application&as=true&search=query&tag=146693dced2609ba&siml=1466932...> 1/3

Project: Enhance the accuracy of digital forensic in the presence of incomplete evidence.

Date _____

Time _____

Location _____

Interviewer Name _____

Interviewer signed _____

Interviewee _____

Interviewee signed _____

Introduction

Welcome and thank you for your participation today. My name is Fahad Alanazi and I am a PhD student at De Montfort University conducting my Special Study in partial fulfilment of the requirements for the degree of PhD of Digital Forensics. This follow-up interview will take about 60 minutes and will include 7 questions regarding your experiences. I would like your permission to tape record this interview, so I may accurately document the information you convey. If at any time during the interview you wish to discontinue the use of the recorder or the interview itself, please feel free to let me know. All of your responses are confidential. Your responses will remain confidential and will be used to develop a better understanding of how you and your peers view your life satisfaction and what might influence it. The purpose of this study is to increase our understanding of social work students and to promote their well-being.

At this time I would like to remind you of your written consent to participate in this study. You and I have both signed and dated each copy, certifying that we agree to continue this interview.

Your participation in this interview is completely voluntary. If at any time you need to stop, take a break, or return a page, please let me know. You may also withdraw your participation at any time without consequence. Do you have any questions or concerns before we begin? Then with your permission we will begin the interview.

The interview will be conducted in Arabic language, the voice recorder will then change it to transcript and the transcript will be translated to English language.

There will be two people who will make the validation for translation.

Purpose of Interview

1. Due to the sensitive nature of the topic, police officers and drugs investigators only are judged to have adequate information related to drug cases.
2. The researcher wishes to gain an in-depth understanding of the mechanism associated with the investigation of drug issues.
3. The researcher seeks to explore the depth and richness of the subject to address the complexities of the research question.
4. The data will be further enriched by undertaking a number of interviews, and then performing a preliminary analysis.

Questions

1. What categories cases are currently being investigated?
2. What are the most common crimes that you encounter?

7. What steps to you help to find additional intelligence / evidence to digital evidence?

Thank you to interviewee to reassure confidentiality.