PRIORITISATION IN DIGITAL FORENSICS: A CASE STUDY OF ABU DHABI POLICE

AHMED MOHAMMED ALRUMITHI

A thesis submitted in partial fulfilment of the requirements of Liverpool John Moores University for the degree of Doctor of Philosophy

July 2018

Abstract

The main goal of this research is to investigate prioritization process in digital forensics departments in law enforcement organizations. This research is motivated by the fact that case prioritisation plays crucial role to achieve efficient operations in digital forensics departments. Recent years have witnessed the widespread use of digital devices in every aspect of human life, around the globe. One of these aspects is crime. These devices have became an essential part of every investigation in almost all cases handled by police. The reason behind their importance lies in their ability to store huge amounts of data that can be utilized by investigators to solve cases under consideration. Thus, involving Digital Forensics departments, though often over-burdened and under-resourced, is becoming a compulsory to achieve successful investigations. Increasing the effectiveness of these departments requires improving their processes including case prioritisation.

Existing literature focuses on prioritisation process within the context of crime scene triage. The main research problem in literature is prioritising existing digital devices found in crime scene in a way that leads to successful digital forensics. On the other hand, the research problem in this thesis focuses on prioritisation of cases rather than digital devices belonging to a specific case. Normally, Digital Forensics cases are prioritised based on several factors where influence of officers handling the case play one of the most important roles. Therefore, this research investigates how perception of different individuals in law enforcement organization may affect case prioritisation for the Digital Forensics department. To address this prioritisation problem, the research proposes the use of maturity models and machine learning. A questionnaire was developed and distributed among officers in Abu Dhabi Police. The main goal of this questionnaire is to measure perception regarding digital forensics among employees in

Abu Dhabi police. Response of the subjects were divided into two sets. The first set represents responses of subjects who are experts in DF; while the other set includes the remaining subjects. Responses in the first set were averaged to produce a benchmark of the optimal questionnaire answers. Then, a reliability measure is proposed to summarize each subject's perception. Data obtained from the reliability measurement were used in machine learning models, so that the process is automated. Results of data analysis confirmed the severity of problem where the proposed prioritisation process can be a very effective solution as seen in the results provided in this thesis.

Acknowledgments

First and foremost, praise to Allah Almighty for his blessings and guidance in giving me the strength, courage, patience and perseverance to endure this long and challenging study journey.

I am grateful for the wise council of my former supervisor, Profess Madjid Merabiti. I have been fortunate, privileged and honoured to know and work under the supervision of such an academic. I am also thankful to my supervisor; Mr. Andy Laws (Programme Leader for MComp/BSc Multimedia Computing & BSc IT & Multimedia Computing, Liverpool John Moores University) for his guidance, useful suggestions, insightful comments and constructive feedback during my PhD journey. Indeed, I am really grateful for their supervision, expertise and knowledge from which I have benefited enormously.

Finally yet important, a great expression of thanks goes to my father and my mother, who have given me exceptional love, constant care, emotional support and encouragement throughout my life, and who continue to do so, and to my beloved wife and my children for their unconditional love and endless support. Thank you for your loving support, sacrifices, prayers, and endless encouragement.

Declaration

This is to declare that this thesis is my original work and written by me. I am solely responsible for the whole work. I also declare that this thesis has not been submitted to any other institution within a degree programme and any mistakes in this thesis are of my sole responsibility

Table of Contents

List of Figures

List of Tables

Chapter 1: Introduction

1.1 Overview

With the development of various forms of technology and computers, there have been increasing levels of sophistication to modern crimes and, consequently, their detection has become very difficult. The field of digital forensics has become very important in enhancing corporate security, through providing an understanding of previous breaches that can lead to more resilient systems, and to the gathering of intelligence for agencies of law enforcement, and so data collected from digital sources and computers has become very important in the detection of modern crime. For the corporate sector, investigations tend to have a focus upon control of damage, the upholding of the standards of evidence, and rapid response; the result being that, rather than always expediting the process of investigation, digital forensics offers a support function (Garfinkel, 2010). There is often a sizeable backlog within many organisations, and so digital forensics frequently delays an investigation from reaching a conclusion, despite digital evidence often not being essential to a case, with it usually being corroborative in nature. It could be claimed that the distinct advantages of new technologies offers the upper hand to a cybercriminal, with them being able to outwit the activities of security and law enforcement agencies (SANS Institute, 2002). The menace from computer-based crime has grown hugely across the world in recent years, with everyone at risk of identity theft, hacking, terrorism, invasion of privacy or identity theft. Dr. Eva Vincze, Director of the High Tech Crime Investigations Programme at George Washington University has claimed that no agency of law enforcement nor national government is able to fully deal with these threats (Aziz, 2007).

Given the changing nature of many modern crimes, there has been a request for the latest technologies to be employed for the detection of them by Abu Dhabi-based agencies of criminal investigation (Gulfnews, 2011). There has been a continual rise in high-tech crimes in Middle East and North African (MENA) countries in recent years that have led to a call for enhanced digital forensic tools to investigate cybercrime (Iman, 2011; Malik, 2014). For example, Table 1 below shows the increase in the number of cybercrime cases in Dubai in the last three years, As the figure was doubled from 2012 to 2013 (Moukhallati, 2014).

Table 1.1: Number of cybercrime cases in Dubai from 2011-2013 (Moukhallati, 2014).

Year	**Number of cybercrime cases**
2011	588
2012	792
2013	1419

Even with enhanced tools, the data acquired through digital forensics can be problematic when compared to other forms of data and evidence (Allen, 2005). A degree of sophistication is needed to collect computer forensics evidence, both in terms of expertise and technology. There may be difficulties in seizing the hardware to use as evidence and, once a crime has been committed, it is sometimes impossible to ensure that data has not been altered (Allen, 2005). Also, as there is a lack of research within the digital forensics field, the results for law enforcement agencies can be unreliable, and methods can actually become obsolete rather quickly. Abu Dhabi is not an exception amongst the MENA countries in being very limited in regards to research into the application of digital forensics (Iman, 2011). This research study, then, has the primary aim of providing a critical analysis of the role that digital forensics plays in Abu Dhabi in the solving of crimes. The study aims to provide an analysis of how digital forensics are employed within the Abu Dhabi criminal justice system, make a comparison with their use in solving crimes by the agencies of law enforcement of other countries, and also identify whether digital forensics have been used to their full potential. The study will also undertake a critical analysis of education and training and the technology used, to ascertain whether they are adequate. In addition, the effectiveness and limitations of digital forensics for helping in investigations and the detection of cybercrimes within Abu Dhabi will be assessed, prior to the suggestion of measures that could enhance the role played by the Abu Dhabi Police Digital Forensics Department in the solving of crimes.

1.2 Challenges of Digital Forensics

Digital forensics presents a number of challenges to investigators. Due to the nature and variety of these challenges, the workload of investigators can be difficult to manage. Most of the software, applications and programs utilized by the organizations and individuals to guard themselves against the cyber-crimes have proven to be an inadequate protective measure as they are faced with constantly developing technologies with the capabilities to easily go undetected by these applications. Constant development and discovery of more modern techniques would turn the current technologies obsolete in no time. Therefore it has become absolutely essential to develop techniques that would be able to withstand the test of time and be robust enough to counter any new or developing threat. Such robust applications are necessary to meet the ever-changing demands of the modern cybercrime scene.

1.2.1Time Inefficiencies

There are several different elements that contribute to the ineffectiveness of the modern digital forensics, but nearly all of them can be linked or traced to the inefficiency of the modern techniques with regards to the time. The following three elements contribute to the fact that modern forensic methodologies take too much time.

- Substantial increase in the general workload of a digital examiner
- Ineffectiveness or limitations related to the software
- Varying size of the data and its related evidence

Software Limitations

For a long period of time the single Workstation computers have been the prime source of resource utilized by the general public, professionals and individuals to meet their daily computing needs. This scenario only changed when the solution of grid computing was introduced. Due to this discovery the general users and professionals were able to utilize a far more efficient and effective resource of computers through Storage and computational management systems.

This technology further evolved to take the modern form of cloud computing that has enabled the users to access very powerful computational capabilities due to the emergence of stronger bandwidth capabilities. However, despite the emergence of cloud computing the fact still remains that this technology needs to evolve further to become completely effective especially in the avenue of digital forensics. But despite its immaturity it is being held as a revolutionary system by developers, researchers and consumers. It provides a level of flexibility that was unimaginable in the past.

Since the users usually operate on single workstation computers, for such an extended period of time, the related software and its development has also been limited to the single workstation computers; the same holds true for forensic applications and software. In modern investigations the amount of data and evidence required to be examined is simply too large to be handled by a single computer, which creates the issue of time and inability to process the data in a timely manner.

Forensic analysis software tends to revolve around the sources where the data was originally present or manipulated, therefore the popular or modern forensic tools are limited to analyzing the data in these standard platforms and do not have the same capabilities across different platforms. But the forensic investigations can range across different platforms depending on the need the investigators have to develop or purchase tools that can be used to carry out effective investigations across such platforms as well. The issue extends to the systems that were designed to operate across different platforms as they require some compatibility mechanism or adjustment to comply with different sources. This issue can be resolved by utilizing tools that have the capability of operating across different platforms but such open source programs often quickly become obsolete or lack the proper evidence collection and documentation mechanisms.

Size of Evidence Data

In the modern world the data storage has become very cheap which has enabled even the smallest consumer to have huge sizes of data at their disposal. Due to this fact, the examiners have to deal with huge sets of data during their examinations. The problem further escalates when the examiners have to deal with network based or shared storage systems such as NAS (Network Attached Storage), RAID or large data mechanisms.

Increased Workload

On top of ineffective tools and huge sets of data, the increasing popularity of technology has caused a significant increase in the level of cybercrimes creating the need for more examinations. Several state-sponsored programs and privately funded projects also work on development of new and improved software that escalate the threat of new and developing threats for the examiners. It is extremely difficult and tricky for the examiners to remain in touch with all the developing threats and technologies. As the workload becomes too large to handle for the examiners, they have to ditch certain investigations in favor of more urgent ones to conduct effective investigations. This backlogging enables the cyber criminals to conduct more attacks and affect a large population.

The things are further complicated when the private investigators and the dedicated security teams in organizations conduct their own investigations on the issue and use inefficient or ineffective methodologies that could damage the evidence or even if these teams find any meaningful information they tend to keep it private in order to protect the sanctity and reputation of the organization. There is lack of sharing of data or information primarily due to the fact that there is no platform available that can be used to share the information in a meaningful or efficient manner. Sharing such information on public domains can expose the infrastructure or security of the organizations to the malicious entities and hackers as well who can use this information to their own advantage and cause significant damage. These issues give rise to the every man for himself mentality, which significantly compromises the effectiveness of the investigations.

1.2.2Heterogeneity of the Evidence

On top of the inefficiencies and issues found in the contemporary investigation systems, a far more serious issue is the range of devices available in the market that can store and manipulate data and the different types of data and ranges that these devices can store and manipulate. The modern investigation labs and systems need to become flexible in order to deal with these wide ranges of data and applications. Equipping such diverse systems can be extremely difficult due to the significant development and training costs involved. In addition to such a large scale of data that needs to be investigated, very little automation can corroborate evidence across different platforms.

There is a significant need to develop methodologies and procedures that can create abstraction of data. However, the biggest hurdle in its development is the difficult of the available resources and its implementation. The forensic tools should be capable of handling a wide range of platforms and different varieties of data available on these platforms. Efficient tools need to be developed to deal with the authentication and credibility of the data and evidence.

1.2.3Application Domains

The forensic examination sector and different significant portions of the industry would great benefit from an all-encompassing and secure collaborative system that would allow the forensic examiners to share their knowledge, experience and methodologies. But presently there is no such platform that could operate across all avenues and still maintain the health of the evidence. Therefore, the forensic teams have to share information and collaborate through channels that are very complex or inefficient. A clear example of this issue is observed when the forensic investigators have to share information and only avenues available to them is either set-up a dedicated servers with limited access to other agency or provide the exact replica of the evidence to the agency. The security issues associated with such sharing of information are very critical and can harm the health of the evidence.

The need for a collaborative system mostly exists in the law enforcement system who constantly need to share information in order to carry out effective investigations. There are several instances where the reach of a cybercrime may also extend to the jurisdiction of other agencies or geographical locations.

Almost all companies and organizations need a forensic investigation at one time or another. In some cases it becomes more beneficial for such organizations to hire an external team or completely outsource their forensic function while in other cases it become beneficial to maintain a dedicated department at the organization with all the required tools and resources to handle the security and forensic investigation of the company. In either case, the professionals who would be conducting the investigations would have varied methodology, tools and documentation system. Because there are no common forensic tools that can deal with all the possible instances that arise in the real world.

1.3 Problem Statement

Several practical problems within digital forensics fields can be recognized. One of the most important problems is prioritisation of cases and resources. As discussed before, limited resources and increased number of cases in recent years leads to a situation where law enforcement organizations are not able to efficiently address and handle all cases effectively. Their lack of efficiency can be recognized on different levels. One example of such levels is the identification of relevance of data and devices to the cases under consideration. There is no efficient mechanism for investigators to decide whether a piece of equipment or data is necessary for investigation process. In addition, a filtering approach to filter evidence and exhibits, which are mostly relevant to the cases is needed.

Another level of low efficiency is due to the lack of mechanisms and techniques to resolve conflict among stakeholders in investigation process. Each one of police officers, technical staff and government representatives would like to influence the investigation process based on their beliefs and understanding. At the same time, digital forensics labs handle different cases from different departments. Each one of these department would prefer their cases to be prioritised. The lack of prioritisation mechanism which is standard and agreeable among all stakeholders would let these conflicts reduce the efficiency and utilization of forensics lab resources.

In addition, cases importance should be reflected on how they are prioritised. Any law enforcement organization has different aspect of their mission prioritized. Most of these organizations are concerned about protecting the public from national security threats in first place. Then, violent crimes and threats come in second place. Other missions are less important than the previous two such as financial crimes and protecting vulnerable individuals. This prioritisation of organization missions should be reflected in how cases and resources are prioritised within digital forensic departments. However, the lack of prioritisation mechanism prevents from embedding organization missions in the department operations. It is expected that some cases would be prioritized regardless of organization mission due to some other factors such as the support of officers with higher ranking. Such behaviours in digital forensics departments (or any other department within law enforcement organization) reduce effectiveness and efficiency.

Keep in mind that the lack of standard prioritisation would lead to having chaotic investment behaviour. Priority would be shifted from time to time based on external factors such as social pressure. This behaviour would lead to short-term investments on the issue under consideration. Such investments will not produce valuable experience for individuals in the organization. Also, any knowledge acquired will be lost shortly. In addition, frequent shifting of priority will lead the public to have a negative perception of the organization. In addition, it will exhaust organization resources without any valuable return.

It is clear that addressing prioritisation in digital forensics departments is very critical for the success of law enforcement operations. Standard mechanisms for prioritisation are highly needed to resolve conflicts among stakeholders and to design long term policy for investments in digital forensics departments.

1.4 Research Questions

In general, digital forensics is a new field. There are more questions than answers. As mentioned before, this research will focus on one aspect of digital forensics, which is the prioritisation process. Specifically speaking, this research addresses the following questions:

- What are the main stages and phases described in the literature to assist in addressing the digital forensics issues of classical operations of police?
- Are these models suitable for addressing modern cases faced by investigators?
- What are the negative consequences of poor case prioritisation processes within digital forensics departments?
- What is the general perception among stakeholders about the maturity of Abu Dhabi police with regard to digital forensics department operations?

- What is the best approach to address the negative aspects of existing perception about digital forensics maturity in police organization?
- Can advanced automation techniques, such as machine learning approaches, be used to improve prioritisation in digital forensics?

1.5 Research Aim and Objectives

The main aim of this thesis is to investigate inefficiency problem of prioritisation process in digital forensics departments. To achieve this aim, this research has these objectives:

- To critically review literature on digital forensics investigation models for understanding capability maturity aspects.
- To develop and analyse the results of a questionnaire to measure the perception of stakeholders regarding the digital forensic maturity of Abu Dhabi Police Department, based on an appropriate capability maturity model.
- To investigate and develop machine learning techniques, such as Support Vector Machines, Decision Trees and Neural Networks, for reliability estimation in prioritisation process in digital forensics departments.
- To develop and critically evaluate an enhanced prioritisation process for digital forensic investigation and develop an implementation strategy.

1.6 Research Contributions

There are several main contributions of this research. These contributions establish the proposed framework. Contributions are:

- Utilization of maturity model concepts in measuring perception regarding digital forensics operations within the organization. Usually, these models are developed and used to indicate an organization's position in an industry sector. In this research, we contribute to the literature by providing a tool to measure perception regarding digital forensics based on maturity models. This tool comes in the form of questionnaire and can be used by other law enforcement organizations to conduct studies about the perception of employees regarding digital forensics.

- This research also contributes a reliability measurement. Investigations have shown that the perception of case handlers plays a crucial role in the severity of prioritisation problem. There are no ways to know a priori how the case handler will perceive the maturity of digital forensic in the organization. Thus, this research contributes to the literature a measurement technique to measure how reliable the case handler judgment is regarding digital forensics maturity in the organization.
- The utilization of machine learning in improving the proposed reliability measurement. To the best knowledge of the author, this work is the first to utilize machine learning in the context of case prioritisation in digital forensics. By introducing machine learning, measurements of reliability can be automated in a way that increases efficiency of digital forensics department.
- A mechanism to integrate the proposed reliability measurement into the existing prioritisation process is a further contribution of this research. Integration is one of the most important aspects of any implementation process. There is need to not disturb the existing operations when new improvements are adopted. Otherwise, any proposed solution will have difficulty in adoption since digital forensics operation are very critical to the overall law enforcement organization

objective. The proposed integration leads to smooth integration with any negative impact on the existing operations.

In addition, the research study was conducted in Abu Dhabi Police which led to insightful findings which can used by similar law enforcement organizations in the region and around the globe. An important finding of this study is that the proposed approach can be easily adopted without a lot of effort. Any data collected based on the adoption of proposed framework can be used by other stakeholders in the organization; especially decision makers. Such valuable data can be essential to improve digital forensics in any law enforcement organization.

1.7 Thesis Organization

This thesis starts with providing the necessary background and literature review regarding digital forensics operations in second chapter. Then, Chapter 3 discusses the research context and the environment in which the research was conducted and develops measurement tool based on maturity model to measure the general perception about digital forensics operations in the organization. Based on this proposed measurement, Chapter 4 introduces a prioritisation model by utilizing the new emerging techniques of machine learning. Data collection and analysis is discussed in Chapter 5, before the thesis is concluded in Chapter 6 where the main findings of this research are highlighted.

Chapter 2: Background

This chapter performs extensive literature review regarding digital forensics. It was written to align with this research scope and its main problem, namely case prioritisation in digital forensics. The main goal in this chapter is to deliver a detailed description of digital forensics processes so that a good understanding of prioritisation problem can lead to solutions in following chapters.

2.1 Overview

In past few decades, a new phenomenon has begun to shape around the world, which is those crimes that are committed by digital or electronic means (Simon and Choo, 2014). Law enforcement and investigation agencies are increasingly faced with the challenge to investigate crimes, which occur in these domains (Floyd and Yerby, 2014). There is a need for extensive research in order to develop techniques and technologies that are capable of collecting, preserving and analyzing such evidences (Floyd and Yerby, 2014). The electronic evidence can take many forms from questionable photographs, videos to encrypted files used in different kinds of frauds and internet crimes (Thorpe et al, 2014).

Today nearly all crimes have some digital aspects attached to them (Taylor et al, 2014). White collar crimes and even violent crimes are conducted with the help of digital media, which helps the criminals in disguising their activities and avoiding apprehension by the law enforcement agencies (Mercuri et. al., 2005). This new dimension to crimes creates a lot of complications for attorney, judges and investigation agencies (Alkaabi et. al., 2010). Law enforcement agencies have begun to view every computer connected to the internet as a port of entry for the criminals (James and Breitinger, 2015). Digital media has become a favorite source for organized criminals groups to communicate, disperse and initiate different criminal activities (Amann et. al., 2015). Researchers have even found evidence of groups using the digital media for keeping records of different criminal activities (Cole et al, 2015). Some of the largest thefts and robberies of current era are happening through computer networks (Flory et. al., 2014). Even terrorist organizations are using internet to communicate their agenda, distribute training material, recruit for their organizations and launder money (James et. al., 2014). Internet has become means through which propagandas by different illicit groups are being broadcasted to the entire world (Cole et al, 2015).

Due to the heavy reliance of governmental agencies on network-based systems, they have become more vulnerable to cyber-attacks (Ben-Asher and Gonzalez, 2015). Different governmental facilities such as health, energy, emergency services and financial service rely on network based systems to provide their services (Hajek et. al., 2015). In past few years, several instances have been identified where large corporate and government organizations have suffered the instances of information theft (Hargreaves et. al., 2012). The hackers can use this information to disrupt the infrastructure of the government (Simon et. al., 2014).

In addition to the all, the negative aspects of technology there are some positives well (Floyd et. al., 2014). Criminals leave strong trails and evidences of their activities due to the excessive use of information technology that can lead to the discovery and apprehension of the criminals (James and Breitinger, 2015). Digital evidence is recognized as a viable and strong piece of information in different civil and criminal cases around the world (Assuncao et. al., 2015). It has become common for the law enforcement agencies to use digital means in order to discover culprits behind the crime or help in enforcing the rights of a citizen in civil disputes (Moser et. al., 2013). Digital records can reveal several key factors about the crime (Glasser et. al., 2014). They can identify the location of the culprit at the time of crime, the conversation that they had and even intention of crime can be identified through digital records (Gupta et. al., 2016).

Digital data is around us in different forms and must be collected on regular basis to assist in different types of criminal investigations (Helbing, 2015). It is highly likely that an individual involved in a crime would use mobile phone, computer or the Internet to fulfill their purpose (James and Breitinger, 2015). Corporate investigations can also benefit from different data collected from the computer of the employee (Ben et. al., 2015). In addition to revealing the identity of the criminal digital data can also reveal how a crime was committed, and can help the organization understand how the security breach occurred so that they can take measures to ensure that such breaches can be prevented in future (Reith et. al., 2002).

Digital Evidence and Computer Systems

Digital evidence refers to all form of data dispersed or saved using computer and other digital devices that provides support in favor or against a certain offence or that can provide evidence about a critical part of the crime (Hegarty et al, 2014). This evidence can take many forms ranging from text, photos, videos and even audio recordings (Kohn et. al., 2006). Computer systems are broadly categorized in three categories based on the type of digital evidence that they carry (Karie et. al., 2015). First, open computer systems, which are common computers that are easily recognizable as computers and carry a recognizable hard drive, keyboard and other peripherals (Hassitt, 2014). These kinds of system are rapidly growing and have the ability to store a large amount of data that can be used as digital evidence (Damshenas et. al., 2012). Any file on the open computer can provide key evidence that incriminates the criminal (Choo et. al., 2012). Details about the creation and modification of a file or content can help the investigators track the source of the information (Digital et. al., 11).

A second category of computer systems is communication systems (Hassitt, 2014). All kinds of communication systems and programs can be used to collect digital evidence (Thorpe et. al., 2014) including telephones, Internet-enabled computers and other wireless communication devices (Cohen et. al., 2011). Telecommunication devices especially phones have become very advanced and can contain information about when a call was made, to whom the call was made and the content of messages can all help in investigations (Digital et. al., 11). In order to get accurate information about the messaging and call records of a phone, investigators need to contact the service that handles these facilities for the users (Thorpe et. al., 2014). Some communication devices and systems can be configured to collect all the data that goes through the phone enabling the investigation agencies to obtain a lot of digital evidence (James et. al., 2014).

A third category of computer systems is that of embedded computer systems (Hassitt, 2014). Devices and tools that have embedded computer chips can be used to collect digital evidence (Wang et. al., 2015). Credit cards, mobile phones and smart cards are a common example of such systems (Mercuri et. al., 2005). Mobile devices can also provide access to a lot of personal information to the users (Quick et. al., 2014). Navigations systems in cars are also an example of embedded computer systems that can shed light upon different location that the car owner has travelled to and can also provide the time of visit at certain location (Ben et. al., 2015). Module systems in the car are widely used for analyzing different accidents, these module systems collect a lot of information about the position of throttle, brake, position of the car and vehicle speed (Noblett et. al., 2000). Cooking apparatus and televisions also contain programmable and wireless connectivity features, using these features the users can carry different types of communications (Shah et. al., 2014).

Since digital technology has become so common in the modern world, most crimes contain some form of digital communication and digital evidence (Flory, 2014). Specially trained individuals can analyze these digital evidences to learn about different dimensions of the crime (Alkaabi et. al., 2010). Most of the time, computer history and phone records contain more information about an individual than any other source that makes digital evidence very important for any case (Bennett et. al., 2012). Some social marketing and commerce sites collect this information to make predictions about the possible behavior of the user and advertise specific products to them (Assuncao et al, 2015).

2.2 Digital Forensic Terminology

Law enforcement and governmental organizations have formed new terms like cybercrime and digital forensic to identify different new criminal activities that have risen due to the heavy involvement of the digital world (Nelson et al, 2015). The legal agencies have also developed newer security systems that have the potential to deal with such digital threats (Simon et. al., 2014). Cybercrime and digital forensic are very digital terms and can carry different meanings depending on the circumstances, understanding and localities, therefore it is essential to understand the clear meaning of these terms (Reith et. al., 2002). It is important to understand that nearly all types of crimes involve some form of computer and digital use (Floyd et. al., 2014). Only because a crime contains a facet of technology does not make it a digital crime (Anderson et. al., 2013). Although there is no universal definition of cybercrime but through time its meanings have filtered and have more specific meaning attached to them.

(Cohen et. al., 2011). Although there is no universal definition of cybercrime but through time its meanings have filtered and have more specific meaning attached to them.

Cybercrime refers to a limited set of activities that are recognized as cybercrimes under the law (Leukfeldt and Yar, 2015). The list of these crimes includes unauthorized access to personal information, harassing using videos or photos, financial fraud through computers, stealing personal information, piracy and plagiarism, distribution of racist or violent material, credit card information theft and distribution of viruses (Leukfeldt and Yar, 2015). The most basic difficulty faced in defining cybercrime arises when a crime has different sides and some of those sides relate to internet, computer or some form of electronic communication (Garfinkel et. al., 2010). For such crimes usually a loose term called computer related crimes is used (Anderson et al, 2013). Computer related refers to those crimes that are not directly related to computers or digital world but to some extent use digital means in order to fulfill their intentions (Kerrigan et. al., 2013).

In the past, nearly all forms of cybercrimes were conducted through computers and therefore the investigating field for such crimes was dubbed as computer forensics or computer analysis (Glasser and Taneja, 2014). But as the technology became more advanced and other form of digital communications also became common in the world these terminologies lost their significance because the researchers were now able to extract the information from several different devices and digital media (Karie et. al., 2015). These days the computer forensic is a more specialized terms that refers to the analysis and extraction of information from computer related equipment such as hard drives, Compact disks, magnetic tapes and printers (Casey et. al., 2011). While in the past the term computer forensic was thought to incorporate all fields of cybercrime investigations (Wang and Alexander, 2015).

2.3 Digital Forensic Personnel

Personnel in digital forensics are the most important asset (Elyas et al, 2014). Prioritisation problem is hugely affected by the competency of personnel (Wang, 2014). Digital forensic is a detailed study about the computer hardware, software, science, relevant forensic laws nationally as well as internationally and ability to logically analyze all forms of digital evidence (Hegarty et. al., 2014). Digital Forensic scientists rely on a combination of these skills to solve different cybercrime cases (Hajek et. al., 2015).

Government and corporate organizations are becoming more exposed to digital crimes that require specialized personnel such as digital forensic scientists to deal with them (Karie and Venter, 2015). Digital forensic is a science that deals with the knowledge of all computer related matters such as storage, recovery and transportation of data (Nelson et al, 2015). Compared to other forms of sciences, digital forensic science is still in very developing stages (Cantrell et. al., 2012). It has become increasingly important as the technology has advanced, several law enforcement agencies and courts rely on digital evidences in order to apprehend criminals or absolve individuals of criminal charges (Agarwal et. al., 2011). Therefore, it is extremely important for forensic scientists to have proper training, knowledge and experience to deal with different kinds of digital evidences. (Sainath et. al., 2014).

There are two broad complications in the development of digital forensic specialists (Raghavan et. al., 2013). First is that the technology does not remain static and keeps changing with time and advancement, new forms of technology are introduced every single day (Agarwal et al, 2011). These developing technologies make it extremely difficult for the forensic scientists to remain properly aware of the current developments in the digital world (Amann et. al., 2015). It is like aiming at a rapidly moving target in a dark room (Ruan et. al., 2012). The second issue deals with the current methods of education and training of digital forensics personnel (Hargreaves et. al., 2012). These individuals are supposed to possess the specialized set of skills to deal with the collection, analysis and storage of information stored through electronic or binary means (Agarwal and Kothari, 2015). Their duties may differ from country to country, but generally it refers to an individual that possess the ability to collect digital evidence and carry out the investigation on it (Jiang et. al., 2015). Digital Forensic examiners are more likely to be hired by government or law enforcement agencies, but they can also be found in the private sectors where large corporations employ their services to improve the security of their systems or to investigate breaches of information that cannot be publically revealed (Kohn et. al., 2013).

Forensic examiners need to possess extensive knowledge and specialized skill sets (Kohn et. al., 2006). A good forensic examiner should be able to demonstrate technical knowledge about different kinds of computer hardware, networks, system software and various types of programs and applications (Amann et. al., 2015). They may also be required to have the knowledge about relevant laws that can be narrated in the court when testifying about certain crimes (Jang et. al., 2014). They also need to have very good communication skills in order to relay their findings to technical and non-technical individuals (Mohamed et. al., 2014). But in reality there are very few programs that provide the individuals with an opportunity to acquire such extensive knowledge of these subjects, which leads to the limited number of individuals in the industry with such extensive ability to analyze different forms of data (Wang et. al., 2015). As a result, managing available competent examiners becomes very important to have successful investigation (Glasser et. al., 2014). Such good management requires excellent prioritisation mechanisms to maximally utilize available skills. (Agarwal et. al., 2015).

2.4 Digital Forensic Process

Most of the early texts on the investigative general forensic process adopt an instructive procedure, where different stepwise instructions are provided to solve, investigate or acquire data for digital evidence (Shah and Malik, 2014). Therefore the early texts on the topic deal with a stepwise approach about the process of investigating certain crimes in the network systems (Reith et al, 2002). The problem with such stepwise instructions is that they tend to be very rigid in their approach and do not provide techniques through which other similar cases can be resolved (James et. al., 2013). This shortcoming led to the development of more generalized instructions for the investigators that help them form opinions and results based on the different results of the investigative procedure (Kohn et al, 2006). This generalization led to the development of varied models that are currently in use for investigating digital crimes (Agarwal and Kothari, 2015).

Such models are extensively used for training, referencing, creating educational material in the field, benchmarking and research work (Quick et. al., 2014). The examiners have to be completely thorough in investigation to ensure that none of the details in the project are missed (Choo et. al., 2012). A formalized methodology creates a defined process through which the forensic examiners can analyze all the sides of the case without missing any kinds of details (Pollitt et. al., 2007). This form of methodological approach also decreases the chance of omission and human error that could compromise the sanctity of the investigation (Hegarty et. al., 2014). Methodological approach also encourages the safe means to handle different kinds of evidence leading to more accurate results (Floyd et. al., 2014). It also reduces the time required for the investigation (Taylor et. al., 2014). Another reason for development of these models is to create a method of investigation that is free of all kinds of bias and has the potential of rendering accurate results (Cohen et. al., 2011). A good model is flexible and provides a stepwise approach regarding the extraction, analysis and collection of digital evidence and can be applied to investigate any new and old technology (Hannan et. al., 2004). These models also prove to be great tools for investigative reports and provide a great insight of the entire procedures to assist in law making process. (Damshenas et. al., 2012).

At the end of the day these models are designed to assist the forensic examiners in their investigations and should not be treated rigidly rather the models are open to the interpretation of the investigators (Casey et. al., 2011). The models serve as foundation upon which the forensic examiners can base their studies (Wang et. al., 2014). Like any other tool, forensic investigation models also have some limitations (Agarwal and Kothari, 2015). Therefore the investigators must be aware about the extent of the applicability of these models (Cantrell et. al., 2012). Most of the modern models in digital forensic are based upon the older approach of linear process but have embedded more flexibility as compared to the older models (Pollitt, 2007).

A complete and competent forensic digital investigation involves five broad steps (Agarwal and Kothari, 2015). In the first step the investigative team formulates the action plan that defines how the timeline should be handled and they also determine how the supporting information regarding the project would be collected (Ben et. al., 2015). In the second step the forensic examiners carry out surveys and identify the sources of digital evidence, these digital evidence can be found at an organization, within a network, at the location of the crime or over the internet (Sainath et. al., 2014). The word "Identify" has a very precise meaning in digital forensic field (Reith et. al., 2002). The word "Identify" has a very precise meaning in digital forensic field (Reith et. al., 2002). The word "Identify" has a very precise meaning in digital forensic field (Reith et. al., 2002). It refers to the survey of evidence and formulating a list about the possible leads that can general digital evidence (Ruan et. al., 2012). The third step ensures that all the potential sources of digital evidences are isolated so they cannot be tempered with (Flory et. al., 2014). The steps carried out by investigation team for isolation of these sources include isolating the network, collecting log files, preventing access and collecting data that can be lost if the system is turned off or given a reset (Noblett et. al., 2000). After the collection of all the data the analysis phase is conducted (Challenges et. al., 48). Although some models consider examination and analysis are similar terms; in the world of digital forensic they have clear distinction (Nelson et al, 2015). Examination means collecting the information is extracted from the data and sources of evidence and then sent for analysis, while at analysis the investigation team attempts to formulate answers about different questions concerning the case (Karie et. al., 2015). The Forensic examiners use various models and critical thinking to discover hidden connections between different variables (Garfinkel et. al., 2010). And as a last step the investigation teams conveys their find through a satisfactory mean (Raghavan et. al., 2013).

2.5 Prioritisation

There are certain challenges (see section 1.2) faced by the investigators during the cases that can lead them to the pursuit of less important sources and add to the increased consumption of resources in terms of time (Choo et. al., 2012). Such delays can also have grave threats to the organization (Hargreaves et. al., 2012). Sometimes it is difficult to think about the facts of a case without some level of bias leading to the case being investigated in the way an organization wants rather than upholding the wishes of the victims or justice department (James, 2014).

Inability to formulate a prioritisation model can cause a more reactive behavior rather than proactive and can lead to the wastage of resources (Moser and Cohen, 2013). Most of the blame for the delays is levied upon the digital forensic laboratories (Jones and Valli, 2011). Due to the complexity of the task the laboratory services may be a bit slow leading to over consumption of resources and delays in the case (Hegarty et. al., 2014).

Some cases may be given more priority than the other because factors beyond control of organization such as public opinion or media attention, but in most circumstances the cases are ineffectively prioritized due to the bias on part of the ranking officers (Cantrell et al, 2012). And in such cases rather than forcing the blame on ranking officer, it usually falls upon the forensic laboratory to explain the cause of delay and face the brunt of the blame even if the prioritisation powers were held by ranking officers rather than the laboratory (James, 2014).

A well-designed prioritisation method can easily resolve these issues (Strom and Hickman, 2014). Ranking officers should take the opinions and suggestions from all the departments and laboratories involved in the investigation (Ben et. al., 2015). Many investigation organizations fail to have a solid prioritisation model, which can make an organization look weak and incompetent (Strom et al, 2009). A clear understanding of the priorities of the organization and the assurance that these priorities would not be changed in the short term can ease the mindset of the investigator and enable them to perform better in the long run (James et. al., 2015). Unbiased prioritisation would ensure that the cases are thoroughly investigated by the digital examiners (Jiang et al, 2015).

There is a lack of prioritisation models which specifically developed for digital forensics operations in the literature. Most of existing prioritisation methods in literature were developed specifically for digital forensics triage which is the process of ranking various aspects and elements in the digital forensics investigation according to their importance. One of the most recent prioritisation models for digital triage is called Dual-Triage Digital Forensic Process Model (DTDFPM) (Yang et. al., 2016). The model is based on using Artificial Neural Networks to perform the most appropriate sorting for digital evidence under investigation. Another recent model is proposed in (Gupta et. al., 2016) which utilizes mixed integer linear programming. This model is developed to schedule available human resources and to choose the most important digital devices from the crime scene.

Montasari (2016) proposed Formal Two Stage Triage Process Model (FTSTPM) for triage process. The proposed model divides the triage process into two main stages. Each one of these stages is composed of several steps. The main focus of this model is appropriate legality of collected evidence. Conversely, this thesis is focused on the efficiency. On other hand, Scanlon (2016) focused on a specific technical issue which is the necessary duplicated analysis effort. He proposed a model of distributing the load in a way that improves efficiency of digital forensics operations.

An early important model which can be compared these recent ones is proposed by Rogers et. al. (2006). This model is called CFFTPM (Computer Forensic Field Triage Process model) and it contains six phases. The phases include Planning, User Usage, Timeline production, Usage of resources such as internet, case specific resources, and Triage. This model is designed to help the investigators to analyze and discover leads on site rather than go through lengthy processes that could take week or months in certain cases. Roger argues that the investigation carried on site is as reliable as any other and also maintains the chain of custody that enhances its reliability even further. In reality the model does not provide any graphical representations nor does it identify any processes or guidelines to maintain the overall chain of custody. The model is highly effective in scenarios where the investigation calls for a quick collection of evidence but it less suitable for investigation where a detailed analysis is required. Therefore, the investigators should only use this model where it is applicable while keeping the technical and legal considerations in mind. The CFFTPM proved that an investigation can be conducted without going through the lengthy process of collecting the evidence then transferring to lab and then carrying out the investigation. It rather proposes a quick and easy solution by conducting onsite investigation.

2.6 Evidence vs. Case Prioritisation

Each case handled by digital forensics department has its own nature which reflects on its evidences importance. It is evident that there will be a ranking of evidence based on their importance to the case (Garfinkel, 2010). Similarly, digital forensics cases are not created equal. Some cases are more important to the police organization than others (James, 2014) depending on the nature of the organization (i.e. FBI vs. local police). However, the same prioritisation techniques used for one can be used for the other. In other words, a specific prioritisation technique can be used to rank cases. Then, the same technique can be used to rank evidences within each case. One can consider case prioritisation as prioritisation on global level while evidence prioritisation is local. Following this arrangement, one can rank all evidences handled by digital forensics department by taking the case prioritisation as a weighting factor and integrating it with local prioritisation. This integration will lead to a measure of importance that can be used for ranking all evidence under investigation.

Keep in mind that evidence ranking is highly influenced by the complexity of required digital forensics analysis. For example, analyzing unencrypted hard drive should not take a lot of time compared to encrypted one. Hence, it is reasonable to finish the simpler task first so that digital forensics department throughput is increased. Throughput here represents number of analyzed evidence items per time unit. Therefore, if the throughput is the main concern for digital forensics department, then case prioritization will be dependent on evidence prioritization. This is a direct result of the fact that each case priority will depend on the raking of its evidence items in digital forensics department queue. Cases which requires a lot of analysis will be at the end of the queue which means that they have lower priority with respect to digital forensics department throughput. However, this is not the case in general. It is clear that some cases will have more importance regardless of their evidence ranking. This importance will advance their associated evidence items in digital forensics department queue. Keep in mind that case importance is affected by factors outside digital forensics department scope. Nevertheless, it can be concluded that both of case prioritization and evidence prioritization are linked and each one of them impact the other based on the case importance.

2.7 Chapter Summary

This chapter provided the necessary background on digital forensics to understand the complexities faced by personnel in digital forensics departments (Agarwal et. al., 2011). The main takeaways for this chapter are:

Today nearly all crimes have some digital aspects attached to them (Taylor et. al., 2014). Crimes are conducted with the help of digital media, which helps the criminals in disguising their activities and avoiding apprehension by the law enforcement agencies (Wang et. al., 2014). This new dimension to crimes creates a lot of complications for investigation agencies (Damshenas et. al., 2012). Law enforcement agencies have begun to view every computer connected to the internet as a port of entry for the criminals (Glasser et. al., 2014). Digital media has become a favorite source for organized criminals groups to communicate, disperse and initiate different criminal activities (Thorpe et. al., 2014). Some of the largest thefts and robberies of current era are happening through computer networks (Cole et. al., 2015). Even terrorist organizations are using internet to communicate their agenda, distribute training material, recruit for their organizations and launder money (Casey et. al., 2011). Internet has become means through which propagandas by different illicit groups are being broadcasted to the entire world (Hannan et. al., 2004).

Trained individuals can analyze digital evidences to learn about different dimensions of the crime (Ruan et. al., 2012). Most of the times, computer history and phone records contain more information about an individual than any other source that makes digital evidence very important for any case (Simon et. al., 2014).

Prioritisation problem is hugely affected by the competency of personnel (Floyd et. al., 2014). Digital forensic is a detailed study about the computer hardware, software, science, relevant forensic laws nationally as well as internationally and ability to logically analyze all forms of digital evidence (Garfinkel et. al., 2010). Digital Forensic scientists rely on a combination of these skills to solve different cybercrime cases (Moser et. al., 2013).

A complete and competent forensic digital investigation involves five broad steps (Sainath et. al., 2014). In the first step the investigative team formulates the action plan (Kohn et. al., 2006). In the second step the forensic examiners carry out surveys and identify the sources of digital evidence (Assuncao et. al., 2015). The third step ensures that all the potential sources of digital evidences are isolated so they cannot be tempered with (Bennett et. al., 2012). The fourth step is data analysis (James et. al., 2014). The fifth step is developing analysis conclusion (Mercuri et. al., 2005).

Even though there is a high level of appreciation for problems which face digital forensics operations, nevertheless we can point out the following shortcomings in the literatures:

There is an extreme lack of investigation in digital forensics literature with regards to prioritisation problem (Wang et. al., 2015). The closest attempts to this topic is studying crime scene triage where the digital forensics specialist tries to prioritize existing digital devices found in the scene (Hegarty et. al., 2014). Literature does not have any work that address prioritisation issue specifically (Reith et. al., 2002).

At the same time, most works in literature deals with digital forensics issues with generalization mentality (Mercuri et. al., 2005). They only try to address macro issues such as general policies adopted by law enforcement organization with regards to digital forensics operations (James et. al., 2015). There are very few works which are concerned with micro issues such as crime scene triage and analysis techniques used in digital forensics (Cantrell et. al., 2012).

In addition, there are limited works which approaches human aspects of digital forensics (Agarwal et. al., 2011). The implicit assumption that digital forensics operation are very mechanical and human factors do not play any role is widely spread in literature (Kohn et. al., 2006). Digital forensics have high level of technicality which give the impression that the negative impact of human factors will be minimized in its operations (Bennett et. al., 2012).

Lastly, most researchers in digital forensics literature use only traditional methodologies to address their issues under investigation (Glasser et. al., 2014). There are no attempts worth mentioning where the researcher borrowed or utilized investigation techniques from other field of sciences. (Karie et. al., 2015).

The primary aim of this research to address these shortcomings in a way that contributes to literature valuable work that can be used by other researchers as starting point of investigation in digital forensics.

Chapter 3: Reliability Measurement through Maturity Model

This research adopts mixed methods of qualitative and quantitative methodologies to conduct its investigation. The qualitative methodology is the basis for this chapter while the quantitative methodology is the basis for the next chapter.

3.1 Research Context

Given the changed nature of many modern crimes, there has been a request for the latest technologies to be employed for the detection of them by Abu Dhabi-based agencies of criminal investigation (Gulfnews, 2011). There has been a continual rise in high-tech crimes in Middle East and North African (MENA) countries in recent years that have led to a call for enhanced digital forensic tools to investigate cybercrime (Iman, 2011; Malik, 2014). For example, Figure 3.1 below shows the increase in the number of cybercrime cases in Dubai in three years from 2011-2013. Figures were doubled from 2012 to 2013 (Moukhallati, 2014).

Year	Number of cybercrime cases
2011	588
2012	792
2013	1419

Figure 3.1: Number of cybercrime cases in Dubai from 2011-2013 (Moukhallati, 2014).

Even with enhanced tools, the data acquired through digital forensics can be problematic when compared to other forms of data and evidence (Allen, 2005). A degree of sophistication is needed to collect computer forensics evidence, both in terms of expertise and technology. There may be difficulties in seizing the hardware to use as evidence and, once a crime has been committed, it is sometimes impossible to ensure that data has not been altered (Allen, 2005). Also, as there is a lack of research within the digital forensics field, the results for law enforcement agencies can be unreliable, and methods can actually become obsolete rather quickly. Abu Dhabi is not an exception amongst the MENA countries in being very limited in regards to research into the application of digital forensics (Iman, 2011).

The Digital forensic laboratory in Abu Dhabi, has a dedicated, all-female team that has played a key role in helping to solve around 95 cases (Absal, 2010). Such a development is recent, with the Director of the Advanced Cyber Forensics research having stated that: "Digital Forensics and Cyber Crime Investigation are relatively new fields in the Middle East region and especially in Arab Countries some of which haven't focused on these two vital fields and enhanced their applications in them except recently” (Zayed University, 2010, Para:7). The Head of the branch of the Abu Dhabi police force dedicated to cybercrime has pointed out, however, that "H.H Lieutenant General Sheikh Saif bin Zayed Al Nahyan, Deputy Prime Minister, UAE Minister of Interior has always been committed to making sure that the Ministry keeps up with the pace of various technological developments in the fight against cyber-crimes, and our knowledge of digital forensics" (Zayed University, 2010:5). Despite such a proclamation, around $54milliom (Dhs. 95 million) was lost due to credit card fraud in the UAE in just the year 2009 alone, an increase of about 20% from its extent in 2008. Moreover, due to breaches of security, firms have lost up to $2 million a year - a figure for 2009 which represents a rise of 75% from 2008. It is clear, therefore, that digital forensics have grown in importance for solving both civil and criminal cases (Ameinfo, 2011).

As noted by Absal (2010), the UAE has become a target for sophisticated financial cybercrimes and child pornography, as well as there being a rise in high tech crime and crime generally. According to the Cybercrimes Branch Manager at Abu Dhabi Police, nearly 1000 different cases were received from various security departments in Abu Dhabi. Those cases were mainly related to pornography, cyber-attack, financial fraud and digital forensic. Therefore, the role played by the Abu Dhabi Police Digital Forensics Lab has become increasingly pivotal in the solving of such crimes in the country.

Several practical problems within digital forensics fields can be recognized. One of the most important problems is prioritisation of cases and resources. As discussed before, limited resources and increased number of cases in recent years leads to a situation where law enforcement organizations are not able to efficiently address and handle all cases effectively. Their lack of efficiency can be recognized on different levels. One example of such levels is the identification of relevance of data and devices to the cases under consideration. There is no efficient mechanism for investigators to decide whether a piece of equipment or data is necessary for investigation process. Also, a filtering approach to filter evidence and exhibits which are mostly relevant to the cases is needed.

Another level of low efficiency is due to the lack of mechanisms and techniques to resolve conflict among stakeholders in investigation process. Each one of police officers, technical staff and government representatives would like to influence the investigation process based on their beliefs and understanding. At the same time, digital forensics labs handle different cases from different departments. Each one of these department would prefer their cases to be prioritized. The lack of prioritisation mechanism which is standard and agreeable among all stakeholders would let these conflicts reduce the efficiency and utilization of forensics lab resources.

In addition, cases importance should be reflected on how they are prioritized. Generally speaking, any law enforcement organization has different aspect of their mission prioritized. Most of these organizations are concerned about protecting the public from national security threats in first place. Then, violent crimes and threats come in second place. Other missions are less important than the previous two such as financial crimes and protecting vulnerable individuals. This prioritisation of organization missions should be reflected in how cases and resources are prioritized within digital forensic departments. However, the lack of prioritisation mechanism prevents from embedding organization missions in the department operations. It is expected that some cases would be prioritized regardless of organization mission due to some other factors such as the support of officers with higher ranking. Such behaviours in digital forensics departments (or any other department within law enforcement organization) reduce effectiveness and efficiency.

Keep in mind that the lack of standard prioritisation would lead to having chaotic investment behaviour. Priority would be shifted from time to time based on external factors such as social pressure. This behaviour would lead to short-term investments on the issue under consideration. Such investments will not produce valuable experience for individuals in the organization. Also, any knowledge acquired will be lost shortly. In addition, frequent shifting of priority will lead the public to have a negative perception of the organization. Also, it will exhaust organization resources without any valuable return.

It is clear that addressing prioritisation in digital forensics departments is very critical for the success of law enforcement operations. Standard mechanisms for prioritisation are highly needed to resolve conflicts among stakeholders and to design long term policy for investments in digital forensics departments.

3.2 Digital Forensics Models

Qualitatively speaking, one of the main goals of this research is to find out how different individuals in law enforcement organization perceive their organization maturity in term of digital forensics. Defining maturity model of digital forensics and investigation can be tricky subject (Gupta et. al., 2016; Amann and James, 2015; James et. al., 2014).

Digital forensics one of the technical field that can be easily divided into different stages. This fact motivated many researchers to develop framework and models to describe digital forensics operations. One of the earliest models is proposed by (Kruse & Heiser, 2001) which divided digital forensics operations into three main components. The first component is all about acquiring the digital evidence that includes operations such as collection, storage, custody and documentation. a second component is mainly about authentication so that the collected data is kept similar to the original. The last component in digital forensics operations according to (Kruse & Heiser, 2001) is analyzing the collected data while keeping a high level of integrity.

Another popular model of digital forensics operations was suggested by (Casey, 2011). In this model, Casey divided digital forensics operations into five main components instead of three. The first two components are about planning and recognition. After those two comes preservation, classification and reconstruction. The main criticism that last two model faces is their focus on procedural aspects of digital forensics operations which limit their scope. Qualitatively speaking, one of the main goals of this research is to find out how different individuals in law enforcement organization perceive their organization maturity in term of digital forensics. An early maturity model is proposed by (Humphrey, 1988) for software processes which can be applied to digital forensics. This model is composed of five components which are evaluation, vision, prioritisation, planning and execution. The first important extension of this model was SEI-CMM

(Paulk et. al., 1993) which is later extended further by one of authors in P-CMM (Curtis et. al., 2009). P-CMM was focused on the maturity with regard to the workforce in the organization especially in knowledge management and human resource development.

Capability maturity model proposed by (Al Hanaei & Rashid, 2014) has a wide scope with regard to digital forensics. It tackles all aspects related to the main three components in digital forensics operations which are processes, individuals and equipment. It is based on modularity concepts where all aspects of digital forensics operation are divided into modules which perform its own quality and maturity evaluations and improvements. This feature of this proposed model is very appealing from practical perspective.

A similar description of the model in (Al Hanaei & Rashid, 2014) with regard to this thesis can be directed to a recent model published in (Almarzooqi & Jones, 2016) as well. The later model was developed based on grounded theory where formal and mathematical relations were modelled among distinct digital forensics capabilities.

As mentioned is section 2.6, CFFTPM (Computer Forensic Field Triage Process Model) by Rogers et. al. (2006) is one of the earliest good important models. The model has been applied multiple time in several practical scenarios. There are multiple publications on the CFFTPM model and it has been reviewed extensively by the peers as well. Due to practical application, the error rate of the CFFTPM is also readily available. The evidence collected from the CFFTPM is permissible in the court of law as there have been several instances where the court has accepted the evidence collected through the CFFTPM model. Furthermore, the CFFTPM model has been developed in accordance of U.S. Federal Law.

The Extended Model for Cybercrime Investigation (EMCI) developed by Ciardhuain (2004) is arguably very detailed digital forensic investigation method. Ciardhuain tweaked previous models by incorporating activities that were left unanswered in the previous models. EMCI is presented in a linear manner. It also follows the waterfall approach that allows the investigator to move back and forth between the processes to conduct an effective investigation depending on the current scenario.

Ciardhuain points out several weaknesses in the previous models. He argues that some of them lacks a proper chain of custody required to ensure perfect flow of information during the investigation. He further argues that the chain of custody should only be assigned to experienced personnel who have previously dealt with such tasks. He further exclaims that the chain of custody should be responsible for transferring the evidence from one step to another. EMCI model makes a huge contribution to the world of digital forensic investigation by providing a model that deals with the information flow during an investigation. It proposes a systematic manner for handling information from its collection to its conclusion. Contrary to other models that only deal with the processing of the information. Although the model proposes a good approach for dealing with the flow of information it fails to address the issue of destruction of the digital evidence when the investigation has concluded. EMCI model does not explicitly identify the goals of the investigation on each step therefore it is highly open to interpretation of the investigators which can lead to a lot of inconsistencies making the overall comparison difficult.

Kent et. al. (2006) proposed a model that assists organizations in becoming self-reliant when it comes to digital forensic investigation by equipping their IT professionals with required skills, training, and guidelines. Four Step Forensic Process (FSFP) model states that every organization should adopt a model that suits their needs perfectly based on their current requirements rather than going for a standardized model that may or may not produce effective results. Despite suggesting a unique model for each scenario, the FSFP model does propose a high level abstract model that is based on 4 distinct forensic stages. The stages are collection of information, examination of the information and evidence, Reporting and Analysis of the information. Kent proposes that these stages are common to every investigation and are supported by the previous models that have been proposed by different researchers. Kent argues that the FSFP model provides greater detail for each of the four stages identified previously compared to the previous models.

Comparatively, FSFP model is far simpler than the other existing models. It provides the basic framework for the organization that they can use to develop their own skills and abilities in the field of forensic investigation. It identifies different guiding principles relating to resources, training, and procedures relating to digital forensic investigation. The model also provides ample detail regarding the basic forensic processes that the organization can utilize to develop their response capability to the digital investigations. Like other models, FSFP model also has some shortcomings. The first and foremost is that it does not provide detailed guidelines relating to the event reconstruction, presentation, interpretation, and finalization of the investigation. It is important to understand that these phases are extremely important in order to carry out a comprehensive investigation. The lack of a proper framework, detailed guidelines, and lack of phases relating to pre and post data make this model highly impractical when it comes to real life application.

Kohn et. al. (2013) proposed Integrated Digital Forensic Process Model (IDFPM) that presents the model of conducting forensic investigation in the manner of a process flow diagram that has 36 sub processes clumped in 5 overall processes. The phases include planning, preparation, presentation, digital forensic investigation, and incident responses. Majority of the components of this model have been extracted from the previous models. IDFPM does not contain detailed guidelines for the lower level activities that are actually performed during an investigation. Although the model seeks to provide a detailed approach to the forensic investigation it still lacks proper details relating to the sub phase processes. The IDFPM model makes a clear distinction between the investigation principle and a process. For example, the model treats documentation as a principle that needs to be adhered to the entire process of investigation rather than treat it as an activity that is only relevant to certain phases. On the hand, IDFPM model does not include some of the critical investigative principles that are central to conducting an effective investigation. These critical processes include the information flow, preservation, chain of custody, safety issues, and proper management of the case. The initial perception regarding the Kohn's model suggest that it focuses more towards the incidental responses rather than the investigation. The model lacks processes relating to law enforcement that otherwise would have been necessary if it was an investigative model.

A Common Process Model for Incident Response and Computer Forensics (CPMIRCF) was introduced by Freiling and Schwittay (2007). This model has been designed to quickly formulate responses when a forensic breach or security threat arises. In CPMIRCF model, the researchers have made a clear distinction between digital forensic investigation and the incidental responses. The CPMIRCF model argues that the incidental responses should deal with the actual activities of the organization that is should undertake in case a breach of security occurs. It further states the activities should have the aim to detect the breach as soon as possible, contain it in a timely manner to it does not escalate further, and rectify it so the similar instances can be avoided in the future. The CPMIRCF model has 3 distinct phases. The phases include Pre-Analysis of the data, Analysis, and Final or post-analysis. The previous models failed to deal with the issue of live response but the CPMIRCF model does so by explicitly mentioning live responses that are based on the proven forensic techniques.

The main weakness of this model lies in the terminology used by authors. The terms used by the authors are dubious and fail to completely encompass the breadth of the phase and activities. In the previous models the term Analysis was associated with the activity of analyzing the digital evidence collected. In case of CPMIRCF model, the term analysis encompass all the activities stemming from collecting data, its analysis, and the final reporting. This lack of terminology can make it difficult to differentiate between the main and sub phases of the model resulting in the reduction of its reliability when it comes to application.

Carrier and Spafford (2003) proposed Integrated Digital Investigative Process (IDIP) model. It has 17 levels that are divided in 5 groups. This model bases itself on the guidelines set in the physical crime scene investigation. In IDIP, the computer is treated as the door to the room that needs to be investigated. The Spafford and Carrier identify the physical crime scene as a real-world environment where the evidence and incident exist in a physical form. The place where the crime initially happened it treated as the primary crime scene while all other environments are considered as secondary instances. The Digital crime scene on the other hand is defined by an environment that is created by the software and is virtual in nature and where the evidence of the crime occurred. The IDIP argues that the deployment phase is completely independent of the physical or digital forensic investigation. In practice however, the digital investigation cannot proceed without conduction the physical investigation initially. The primary investigation scene is where the crime actually occurred while secondary location is where the victim is located or based. The IDIP model does not contain any distinction between these two locations. Due to the lack of this distinction the model fails to account for the possibility of a malicious activity which compromises the structure and reliability of the entire sequence of investigation. This can further lead of incomplete evidence collection or findings in the final report.

Also, IDIP is ineffective for time sensitive scenarios. It requires that the entire list of processes need to be concluded before a conclusion can be drawn or any lead can be investigated that can become highly impractical in the real life scenarios such as child abduction. However, the court and legal authorities require the investigation to be conducted in a systematic manner so that the evidence can be reliable and unquestionable. Therefore, models concentrate on quick data examination can face serious challenges in the court of law. It has been suggested that although IDIP has certain weaknesses that have been highlighted by the researchers there are several methodologies that have been introduced in the model that are widely adopted. The digital crime scene is one such concept that has been highly lauded by the forensic investigators. The biggest contribution of the IDIP model is the introduction of the concept of physical investigation's interaction. The IDIP model also introduces a comprehensive model for the collection, interrogation, analysis and final reporting of the data. Despite having some serious flaws, the IDIP model has been credited with highlighting the physical crime scene as part of the digital forensic investigation. Making distinction between the physical and digital crime scenes is an important but a trivial matter. In the execution phase it is extremely important to distinguish between physical and digital crime scene so that investigation can be properly conducted.

Beebe and Clark (2005) proposed Hierarchical Objectives Based Framework for the Digital Investigation Process (HOBFDIP) as an entirely new model as they believed that the prior models lacked any practical details required to apply these models in real life scenarios. The Beebe and Clark's model therefore focuses on the detailed activities that the forensic investigators have to perform in order to conduct an investigation rather than focus on abstract principles that only serve as guidelines but fail to provide practical application. The Beebe and Clark's model has 6 distinct phases. The initial impressions of the Beebe and Clark model suggest that it does not base itself on any of the previous models but rather provides a complete set of instructions and principles for the base level activities of an investigation. The Clark and Beebe's model is divided between phases, objectives, and principles. Phases are arranged in a sequential manner, have time limits specified to them and are explicitly defined in unique processes. The principles on the hand have much wider scope and can apply to multiple phases simultaneously while the objectives are the goals that each phase or principle is expected to accomplish.

Despite having such a detailed model, the Beebe and Clark model still contains some weaknesses. One of them is the fact that the list of objectives is incomplete. Another weakness is that the model requires further expansion and interpretation before it can be applied to different scenarios and cases. Other arguments against the HOBFDIP model include that it only specifies detail processes for the initial phase of the data analysis process. The other processes in the model have very little details and the modeled is centered more towards the network forensic as compared to having wider frame of application. In conclusion, each digital investigation model has its own pros and cons. Therefore, no single model has been found to be the absolute standard for all situations (Amann and James, 2015).

By taking the detailed assessment of some of the most popular digital forensic investigation model it can be concluded that only Rogers and Ciardhuain have taken a complete scientific approach towards the development of their models. Therefore, it can be concluded that majority of the models discussed above have no single agreed upon scientific approach or methodology. Most of the authors have presented their respective models in a unique way, other than the instances where the model has been developed or based on the previous model or collection of models. It was further observed that the majority of the models have not been tested in the real-life scenarios except a few to actually determine whether the models actually work or not. Majority of the existing models are incomplete as they do not provide a comprehensive guidelines for the investigation. The models rather focus on the middle portion of the digital investigation rather than providing a full review. In addition, there is no single methodology or agreed upon principle. All the models have been presented in different lights bases on the perception of the author and the issue that the model was supposed to respond to. The majority of the authors have adopted their own mode of investigation based on their personal findings and experiences. Besides EMCI and CFFTPM, all the models have not been subjected to real life testing or application in real life scenarios. Although the models have been reviews and widely published. The existing models do not provide a detailed step by step approach for conducting an investigation they rather provide abstract guiding principles that can be used to conduct an investigation. Furthermore, no model reviewed above adhered to a particular principle or set of laws that can be used to determine the potential failure rate or wide acceptance of the model in question.

Despite the authors claim that their models were comprehensive and could be applied to a wide variety of situations in reality all the models did not have wider application as the peer reviews identified several shortcomings and weaknesses within the model. For a model to be considered truly universal it needs to be able to be applied to different scenarios and fields of digital forensic investigation. Furthermore, it can also be argued that majority of the models do not provide a detailed, low level guiding principles regarding the forensic investigation they rather provide abstract views in view of which the investigation should be conducted. These models fail to provide proper guidelines to investigators so that they can be applied to real life scenarios.

At current stage, it is important to employ models that define processes of investigation on the five general processes (Agarwal and Kothari, 2015). These processes involve Pre-process, Analysis, Acquisition and Preservation, post process and presentation. The investigation capability of an organization can be examined by referring to the numerous activities that are engaged during the investigation. This referral creates a more affective model that enhances the investigation. Furthermore, Digital Investigation or Forensics processes do not operate in isolation and need to be considered in combination of other factors such as Technology and People. These factors combine together to create a comprehensive model that can be used to evaluate different capabilities of the organization regarding digital investigation.

Evaluating organization maturity based on any model can be very subjective. This thesis proposes to utilize this subjectivity to understand how individuals behave in digital forensics department. Research approach in this thesis is based on asking individuals in law enforcement organization regarding maturity of digital investigation and forensics based on a specified model. Subjective answers of these individuals contain information which can explain their perception regarding digital forensics and their behaviour motivations. The following section provides brief background about the adopted maturity model. Then, discussions regarding data collection and analysis processes will be delivered.

3.3 Kerrigan Maturity Model

The basic idea of adopted maturity model is based on categorizing law enforcement maturity with regards to digital investigation and forensics according to specified levels (Kerrigan, 2013). The first reason to choose this model is the fact that it is a maturity model instead of being operational and process model. At the same time, it is not a general capability maturity model. It rather focuses on digital forensics specifically. In addition, this model is not very detailed to the point that it is only understandable by specialists, nor it is very abstract. These facts make this model the most appropriate to construct an instrumentation tool to measure maturity perception about digital forensics in law enforcement organizations.

There are five levels of maturity with the fifth level representing the highest maturity. The adopted model considers all three aspects of digital investigation and forensics which are technology, processes and people. The following explains properties that would be present at each level in terms of these aspects.

3.3.1Level 1

Organizations with level 1 rating tend to lack any formal procedure of digital investigation. All actions toward digital investigation would be unregulated and general in nature rather than a planned approach. Officers conducting investigation would function without assistance and coordination. This approach and lack of planning can lead to destruction of evidence and wrong conclusions for investigation.

When it comes to resources, they would be extremely short or non-existent. At this level, the organization would have no expertise in order to carry out investigation properly. Technologies and tools necessary for investigation would also be absent and the organization usually turn to IT or general departments in order to carry out digital investigation or seek advice. At this level, processes are not properly performed or they are incomplete.

With regards to people, level 1 organization does not possess any kind of internal expertise in investigations. The organization may even carry some misbelieves that IT or general support department can carry out the investigations. The organization would be completely reliant upon external or 3rd party investigators, but it would lack the expertise and knowledge to utilize the investigation to its benefit.

With regards to technology, level 1organizations do not possess any kind of special tools necessary to carry out a successful investigation. The only form of technology present would be in form of administrative or general IT tools. In severe needs, the organization may develop copies of tools to analyze and experiment with.

3.3.2Level 2

At this level, the organization would have some experience in handling digital investigation. It would also have developed some processes that are essential for a successful investigation. It would also possess limited capability of carrying out investigations, but all the organization’s understanding regarding digital investigation would be focused to the technical or technological aspects. The organization would have firm belief that the scope of digital investigation only exceeds to technical or IT related matters. There would not be a dedicated department for digital investigations and forensics, but the approach and response would differ from case to case. Compared to level 1, handling of information would be much more effective, but the risk of poorly analyzing the evidence and drawing wrong conclusions would still exist.

At level 2, the organization would have developed several basic processes such as:

- Awareness

Law enforcement organization would have the basic knowledge about different events and causes that may require digital investigation. The organization would have also established systematic actions regarding the purpose and nature of digital investigation. However, processes at this level would be inconsistence and each investigator would have a unique and different approach.

- Authorization

  The organization would have placed an authorization process in place which would ensure that appropriate level of consent is obtained before an investigation can begin. Organizations or regions that are operating under some legal or regulatory mandate can have implied authorization due to their position or legal framework. But when questions of complex and inter-jurisdictional matter arise, the organization may not have the proper controls and procedures in place. At level 2, the internal policies and procedures regarding digital investigation would not be clear and well defined.

- Planning

  Planning at level 2 would depend on the case and the investigator handling the case. Therefore, each scenario would be different and each investigation would use different tools and techniques to draw conclusions.

- Notification

  Notification refers to the process through which the concerned individual or authorities are notified about the impending or current digital investigation. However, where it is critical for the organization to conceal the investigation so evidence is not eradicated, such notifications would not be distributed. In certain circumstances it might be part of the legal requirements to send notifications to the concerned parties when the investigation is started. At level 2, law enforcement organization would have proper understanding about notification.

- Search and Identification

  At level 2, there would be lack of consistency in the search and identification process. There may be some understanding about the retrieval and handling of the general evidence. But in more complex cases, there would be a lot of inconsistency due to the lack of predefined processes.

- Collection

  At level 2, law enforcement organization has a process of collecting evidence from different sources, but these capabilities are only restricted to a few devices and sources. Principles of collecting, retrieving and analyzing information are also defined.

- Transfer

  Law enforcement organization does not have any standard process for the transfer of evidence which significantly increases risk of contamination. The transfer process would be done according to the discretion of investigators and each investigator would have different approach to the task.

- Storage

  The important aspects of storage of critical evidences would not be well-defined in the organization and would have a lot of inconsistencies. This could lead to the contamination of evidences while they are being compiled for analysis for investigation.

- Examination

  At level 2, investigators would have general understanding about the processes and techniques used to examine evidences in the laboratory. Despite having a good understanding of the techniques, knowledge of investigators may be limited to few devices and manual methods rather than using automated techniques.

- Hypothesis

  At level 2, investigators would be working around the expected hypothesis. They would be collecting evidences in order to prove or disprove the proposed hypothesis. Such limitation of scope would lead investigators to ignore broader context of the investigation.

- Presentation

  At level 2, findings would be communicated in form of a written report by the investigators.

With regards to people, most of investigations at level 2 law enforcement organization would revolve around only a few processes. With passage of time the acquired forensic skills would become obsolete and investigators would have very little exposure in order to update or renew those skills. Therefore, investigators would not be utilized inside the court as witnesses or experts. The organization would have an encouraging environment for digital investigations, but the digital investigation team would not be taken on board in case of a non-digital investigation.

With regards to technology, the organization would be faced with the constraint of resources and would only be capable of collecting evidence in few types of investigations. This issue would also extend to the types of technologies available at their disposal.

3.3.3Level 3

At level 3, the organization would have a reputation of carrying out several successful digital investigations. At this level, the organization would have developed standard processes in order to carry out different types of investigations, present findings and handle evidence from different sources. At level 3, the organization would have also achieved some sort of certifications regarding digital investigation in terms of quality. Digital investigators within the organization become equipped with the ability to offer a range of investigation services in a defined period of time. However, investigators may draw wrong conclusions or analyze the evidence in wrong manner leading to misinterpretation. This inability to properly analyze data arises because the organization fails to incorporate investigators in planning phase of the investigation.

Level 3 means that the organization would have developed standard procedures regarding the collection, storage, Retention, identification, authorization, analysis and examination of digital evidence. These well-defined protocols would instill consistency across all the investigations.

- Planning

  At level 3, planning stage would involve communication of investigation goals and objectives to the concerned investigation officers. Composition of investigation teams would also be decided at this stage. The organization would not be listing tasks or outlining directions of the investigation, but it would rather outline the purpose of the investigation. The planning stage would also outline the time frame of the investigation based on some priorities. The investigation team would also be made aware of any kind of limitation that they would have to bear during the investigation. These limitation can take several forms like restriction on the time during which the evidence can be handled, costs or resources.

- Hypothesis

  At level 3, the investigation team may be required to formulate a hypothesis about what events occurred. The tone and formality of the hypothesis would be based upon the investigation type. Criminal cases tend to have a more detailed hypothesis with extensive list of supporting documents.

- Presentation

  At this level, digital investigators in the organization would be expected to have good skills in presenting the evidence and findings in whatever form they are necessary. They would also be able to act as expert witness in the court.

- Proof/Defense

  Investigators at level 3 law enforcement organization would have the ability to defend their investigation against any kinds of criticism and doubts.

- Dissemination

The dissemination at this level would concentrate on the internal policies and reviews. These reviews would further strengthen the effectiveness of the procedures and policies regarding investigations.

With regards to people in level 3 law enforcement organization, investigators would be constantly in touch with their skills as they would be getting more project consistently leading to a greater skill retention. Individuals would also be required to hone, polish and maintain their skills as well as remain in sync with the latest technological and procedural advances. The non-digital team would also have detailed knowledge about the different aspects of digital investigation. Other departments in the organization would also approach digital investigation team to assist in any kind of investigation.

With regards to technology, the organization would have required skills and toolsets at their disposals in order to carry out digital investigations effectively. The constant flow of different investigation projects would also help the organization in maintaining a wide array of tools and skillsets. But the investment in new and advanced technologies would be limited to a few sources and devices.

3.3.4Level 4

At this level, roles of the investigators change from merely employees to business partners, who are actually involved in the planning and strategizing phases. Investigators would be able to express their opinion and contribute to the strategy by regarding the extent of the evidence required, importance and priority of the evidence and outline special circumstances where the evidence may not be recoverable. This participation leads to more efficient and effective digital investigations while keeping cost and time requirements low.

Compared to level 3, processes at level 4 would have more qualitative approach. They would seek to encompass not only current circumstances but would also attempt to figure out circumstances that might arise in the future.

- Planning

  The planning stage would become more comprehensive and would attempt to concentrate on factors such as the extent of the evidence required, methodologies and sources that should be tapped into to gather the evidence and the importance of the evidence. The investigators would have complete details regarding the background of cases, locations and technologies involved.

- Dissemination

  Findings and information related to different cases may be shared across different organizations and may even appear in professional and educational journals.

In term of people, law enforcement organization at level 4 would have a very strong technical and professional capability. This provides the organization with the ability to handle any kind of digital investigation. Investigators at this level would be encouraged and assisted in remaining well-informed about the latest advancement in their field. They would be considered to be complete experts who would direct the outlook of the industry.

In term of technology, investigators would have the latest technology at their disposal and their access would extend to all the latest advancements in the industry. The investigative teams would also have access to the previous works that have been performed in relation to the current scenario in question.

3.3.5Level 5

At this level, digital investigation capabilities of the organization become central to its survival. Digital investigation becomes a part of core values and competencies of the organization. At this level, the organization would be leading the digital investigation industry and developing new tools, strategies and investigative techniques.

Processes at this level would be highly refined and would be more automated in nature, creating a more effective body of work. Investigators would be highly skilled and may even be considered the leading figures and experts in their respective field. They would be participating in the development of new technologies and patents. They would also be involved in the legislative process regarding digital investigation industry. In addition, the organization would be actively involved in developing much more advanced and effective tools that would assist them in any future or current investigation.

3.4 Rating Approach

To operate at any of the levels described above, the organization would have to proof that all the specified activities are operating at the recommended levels. For example, those organizations that exceed in some aspects or have level 4 ratings while fall short in other activities and have level 2 activities would not be rated at level 3 (Averaged). The organization would need to work on those weakened activities before moving on to develop other activities to much more advanced level in order to be rated at level 3.

It is important to note that despite identifying 5 levels above, it would not be feasible to all organization to develop their digital investigation abilities to such a level. The arguments holds very true for the public sector organization who have to operate under very limited resources and developing such high investigative capabilities may not be justified or feasible unless the organization has to face special circumstances where the case load is very high. Therefore, in most circumstances it would be more appropriate to maintain a level 3 investigative capabilities. Based on this analysis the organizations should not compromise on level 1 if the digital investigation capabilities are important to them.

3.5 Maturity and Reliability

3.5.1Reliability Model

The reliability model used in this thesis is based on utilizing stakeholder’s subjectivity with regard to organization maturity. Stakeholders of criminal cases pass them to digital forensics team when there is a need to perform digital investigation. For example, the chief investigator of the case may want to decrypt a mobile phone found in the crime scene. Each coming case would have a description specifying general information about the case such as severity of crime and number of victims. Due to the increased number of coming cases, digital forensics team has to prioritize cases. Importance specified by the case provider will play an important role in prioritisation. Here, the main problem is the reliability of importance evaluation.

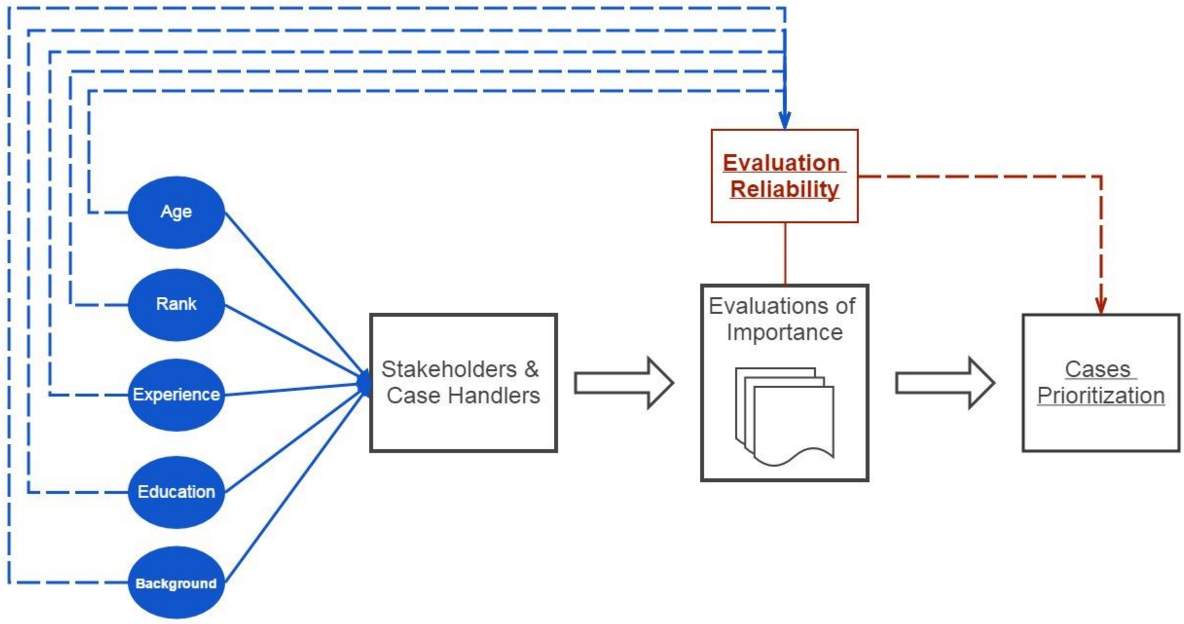


Figure 3.2: Reliability of importance evaluation and cases prioritisation.

If importance evaluation is not reliable, cases prioritisation process will be affected negatively. There is indirect relationship between cases prioritisation and evaluation reliability. In addition, several aspects of case provider can shed a light on her/his ability to provide accurate importance evaluation. This research proposes to use the following elements:

- Age
- Rank
- Experience in Digital Forensics
- Overall Experience in Police Work
- Technical Background
- Level of Education

These elements are directly related to the stakeholder reliability. Age and rank are highly correlated. As the officer advances with higher ranks, she or he gets older and more experienced. Leadership positions are usually given to high rank officers in all law enforcement organizations. Hence, the probability of leading an investigation case increases with age, rank and experience. This doesn’t mean that selecting case lead investigator is purely objective based on these three characteristics. Other factors such as office politics may play huge impact on choosing the case leader. The last two chosen elements which are technical background and education are directly linked to the ability of understanding the technical aspects of digital forensics.

Digital forensics requires having a good background in information technology. Most of highly educated people will certainly have a good experience with Information Technology solutions due to their education experience. It is almost impossible to acquire a high education degree without utilising advanced technology equipment and techniques. As a result, highly educated persons will be initially equipped with the necessary background to understand the entry level of technological aspects in digital forensics. At the same time, having a good background in Information Technology due to the previous experience will certainly help forming a better understanding of digital forensics operations. For example, network technician will be much able to understand different aspects of difficulty in digital forensics operations than a financial specialist. Nevertheless, the financial specialist would be able to grasp the necessary initial understanding due to his experience with utilising financial software and solutions.

Keep in mind, there is no clear approach to measure reliability in this context. This research proposes to utilize maturity concept to propose a measure of reliability. The main idea behind the proposed measure is to use a questionnaire instrument which measures how stakeholders perceive organization maturity in term of digital forensics.

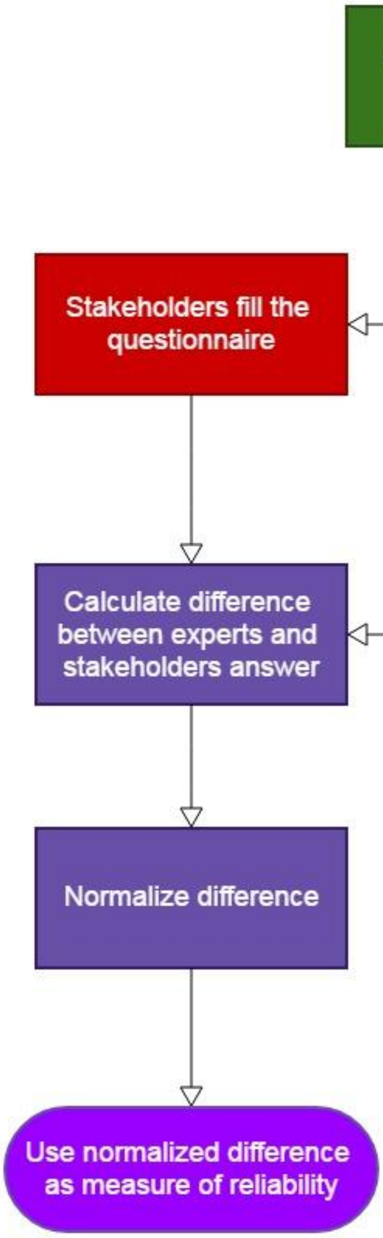

Construct maturity questionnaire
Stakeholders fill the questionnaire
Experts fill the questionnaire
Calculate difference between experts and stakeholders answer
Standardize experts answers
Normalize difference
Use normalized difference as measure of reliability

Figure 3.3: Process of calculating reliability.

First, group of experts within the organization who are very familiar with digital forensics operations will be asked to fill the questionnaire. There answers will be a good measure of organization maturity in term of digital forensics. Then, a group of stakeholders will be asked to answer the same questionnaire. Their answers will be compared with the standardized version of experts' answers. The difference of each stakeholder answers with standardized version of experts' answers will be a measure of reliability. As difference decreases, reliability increases. This reliability measure can be easily incorporated in calculation of prioritisation metric which used to rank cases.

3.5.2Questionnaire Instrument

This research uses a questionnaires instrument to study the overall perception of stakeholders in law enforcement organization regarding digital forensics operations. The main goal of questions is to find out how each stakeholder evaluate the maturity of digital forensics. These questions are designed based on the maturity model mentioned above. The goal of questionnaire was not to estimate level of maturity of law enforcement organization in term of digital forensics. Instead, it was understanding how subject perception may lead to the adoption of unrealistic believe about maturity of digital forensics operations. Such unrealistic believe will lead the stakeholder to overestimate digital forensics departments capabilities. Or, it may lead him to underestimate the complexity of digital forensics operation. In both cases, such stakeholders will overwhelm digital forensics department with cases that are prioritize based on shallow understanding of digital forensics operation or the organization capabilities.

Table 3.1: Proposed Qestionnaire.

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Do Not Apply
1	Digital forensics is mainly concerned about cybercrimes.	□	□	□	□	□	□
2	The organization has clear procedures to handle all aspects of digital investigation.	□	□	□	□	□	□
3	IT department is controlling digital forensics operations.	□	□	□	□	□	□
4	Delivering and acquiring information regarding digital	□	□	□	□	□	□

	investigation are very organized.						
5	Each digital forensics case has its own plan of operations and processes.	□	□	□	□	□	□
6	The organization has the ability to examine any digital device regardless of its complexity.	□	□	□	□	□	□
7	The organization has clear guidelines about storing and transferring digital evidences.	□	□	□	□	□	□
8	Digital investigators in the organization are well trained and they have all necessary skills to perform any operation in digital forensics.	□	□	□	□	□	□
9	The organization needs to increase number of digital investigators.	□	□	□	□	□	□
10	Most types of criminal investigations in the organization use digital forensics.	□	□	□	□	□	□
11	Achievements of digital forensics team are well-known throughout the organization.	□	□	□	□	□	□
12	The organization needs to acquire more technologies and tools for digital forensics.	□	□	□	□	□	□
13	The organization has the ability to develop new digital forensics tools that can be used by other organizations.	□	□	□	□	□	□
14	The organization depends on digital forensics teams of third parties to help with digital investigations.	□	□	□	□	□	□
15	Digital forensics team has influence on drawing the general policy and strategy of the organization.	□	□	□	□	□	□
16	The organization helps other organizations in term of digital forensics.	□	□	□	□	□	□
17	Digital forensics team has full access to all information in any assigned case.	□	□	□	□	□	□
18	There are established programs to train and develop human resources for digital forensics positions.	□	□	□	□	□	□
19	Employees of digital forensics can easily work IT department without additional training and vice versa.	□	□	□	□	□	□
20	The organization conducts seminars to familiarize stakeholders with operations of digital forensics in the organization.	□	□	□	□	□	□

Table 4.1 presents the proposed questionnaire. Here, questions are qualitative in nature asking about subjects' perception. Then, a quantitative analysis will be performed in Chapter 6 to provide a broader generalization of perception regarding digital forensics. The combination of both of these techniques would add more relevance and efficiency to the results of this study as discussed in Chapter 6.

3.5.3Reliability Measurement

Questionnaire is distributed among all stakeholders of the organization. Each one of these subjects will answer the questionnaire based on his understanding of organization maturity in term of digital forensics. A subset of these subjects are experts in digital forensics. Their answers will be very similar and they will be used as a benchmark. The likert scale will be converted into numerical values as follows:

Strongly Disagree	→	1
Disagree	→	2
Neutral	→	3
Agree	→	4
Strongly Agree	→	5

Then, average of experts answers for each question will be used as optimal answer. For every other subject, the difference between his answer and expert average will be calculated.

$$\varepsilon = |\gamma - \mu|$$

Where μ is expert average, γ is subject answer and ε is the absolute difference. Then, reliability will be measured as follows:

$$R = 1 - \frac{\sum_i^N \varepsilon_i}{Z}$$

Where N is the number of questions and Z is the largest possible difference. This reliability measure has values between zero and one; where one is the most reliable while zero is the least reliable.

3.6 Chapter Summary

The main goal of this chapter is to present concept of maturity for digital forensics capabilities in law enforcement organization. Then, questionnaire instrument was developed based on the adopted maturity model. In addition, a reliability measurement approach was proposed. This approach measures the accuracy of stockholder estimation with regard to case importance in term of digital forensic operations.

Chapter 4: Automated Prioritisation Model

This thesis proposes to automate prioritisation process of digital forensics through combining collected data from survey and utilizing machine learning techniques. These techniques are designed to extract its functionality seed from data which make them very adaptive. Hence, the proposed prioritisation model will custom to each law enforcement organization by taking into consideration only data that was collected locally. Such adaptability and customization should greatly improve prioritisation process rather than using general solutions of prioritisation.

Machine learning is considered to be the sub-category of the computer sciences. It is also called predictive modeling or predictive analysis. The purpose of this modeling is to formulate models or artificial intelligence protocols that have the capability of learning different patterns and analyzing the data in a meaningful manner with a constant accuracy. It also encompasses the ability of the model or software to find meaningful patterns and make connections between unseen or unrelated data.

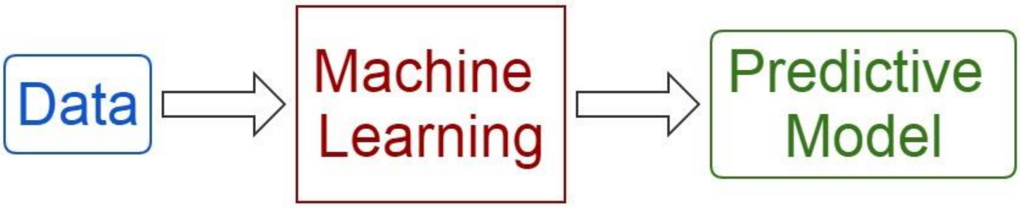


Figure 4.1: Machine learning process.

As an example imagine the dataset in form of a table that contains rows and columns. The rows represent the observations and the columns represent the features of these observations and their related values. At the conclusion of a machine learning exercise the dataset is divided in two or three different sets. The sets are then categorized as training data set and validation data set. Once this data set is formulated the predictive capabilities of a system can be analyzed and its accuracy can be determined as well.

The predictive and learning capabilities of a machine based system can prove to be very beneficial as they possess the capability of finding patterns and connection at a much higher speed and with better accuracy as compared to the manual systems. These predictive systems rely heavily on mathematical equations and statistical optimization. The process of optimization identifies the smallest or largest number or value in an equation commonly referred to as minima or maxima. Gradient descent and normal equation are two of the widely used machine learning algorithm. In short machine learning can be summarized as an accurate method of discovering meaningful patterns out of new or unseen data.

4.1 Machine Learning Techniques

There are several machine learning techniques that can be used in many situations. This thesis focuses on the most reliable techniques.

4.1.1Decision Trees

It is the most popular method of inductive interference learning (Rokach & Maimon, 2014). It is a very practical method of discovering impactful solutions with regards to the machine learning. An illustration of a tree is used to represent the known functions and different branches on the tree represent the different learned outcomes and results (Rokach & Maimon, 2014). Decision tree uses the popular outcome mapping system to identify a classifier. Every node in the tree represents an outcome, variable, feature or query that is attributed to the main scenario. While each branch attached to the node represents a possible value that can be attached to that instance. A condition or scenario start at the root of the tree then moves down to attach with a corresponding value (Oliver et. al., 2016). This process is continuously repeated down the tree until a corresponding value is discovered. There are several prevalent algorithms that are widely used by the investigators, examiners, statisticians and professionals to construct decision trees using a predefined data set. ID3 is the popular example of such practice (Rutkowski et. al., 2016). This is a very conservative approach of decision tree that uses specific attributes so that the data separation can reach the optimal level. This approach outlines all the possible outcomes and hypothesis so that no possible solution is left out and also avoids the risk of creating bias within the hypothesis. It tends to favor smaller trees against the larger trees (Rokach & Maimon, 2014).

4.1.2Artificial Neural Network

ANNs or Artificial Neural Network is a popular and practical method of learning and formulating different target functions from examples (Daniel, 2013). It is widely applied to real valued, vector valued and discrete valued functions (Akerkar & Sajja, 2016). The Back propagation algorithm is a prime example of ANNs that employs gradient descent principles to alter the network parameters so they can fit perfectly the training set with input-output pair. ANN has wide applications and it has been successfully used with speech recognition and visual scene analysis tasks (Nahar, 2012).

4.1.3Instance-based learning

Contrary to the other learning methods that rely on the construction of an abstract scenario of the target function through training examples this method simply employs the examples themselves to achieve the learning outcomes. An example is used as the primary driver for the equation where every possible outcome or instance is analyzed against the conditions that are prevalent in the example to identify any possible relation or association with the target value function. Instance based methods are also referred to as lazy learning methods that carry a stark difference as compared to the other learning methods. Locally weighted regression is a prime example of this type of lazy learning.

Nearest Neighbor is most used Instance-Based learning algorithm. The basic principle behind this method of learning is to identify the nearest points with regards to the numbers in the training sample in order to assign a target value to a new point. The number of samples that the algorithm would use can be outline or predefined by the users (Constant) or can depend upon the density of the local points (Radius based or variable). The algorithm can employ any popular metric for measuring distance but it uses Euclidean most commonly. These are non-generalizing learning method that remember all instances of training data.

4.1.4Support Vector Machine

With regards to the machine learning protocols a support vector machine learning system is a supervised model used for leaning that has attached algorithms which analyze and evaluate the data for categorization and regression analysis. It uses a set of training examples that are then categorized into two different categories by employing an SVM learning algorithm. Due to its application of such method it is categorized as a non-probabilistic binary linear function. SVM model attempts to create a representation of different points in space that uses a clear and wide gap. New examples or instances are then filled into these gaps by analyzing the common characteristic they have in relation to the gaps (Gonzalez & Dutt, 2011; Lejarraga et. al., 2012; Gonzalez, 2013).

4.1.5Bagging

Bagging is a type of ensemble algorithm that constructs several different scenarios and instances based on the original training set and then accumulates these separate predictions to construct a single, decisive and final algorithm (Witten et. al., 2016). The bagging methods are primarily used to ensure that the variance in base estimators is reduced as far as possible (Domingos, 2012). The reduction in variance is achieved by applying randomization scenarios into the procedure and then aggregating them to form a perfect ensemble. Bagging is a very simple method to effectively improve the algorithm using a single model without requiring it to adhere to any other based algorithm. Bagging methods tend to work well with complex and strong models contrary to the boosting models (Shallow trees) that work far effectively with the weaker models (Harrington, 2012).

4.1.6Clustering

Cluster analysis is the application of a grouping of observations into subsets called clusters (Witten et. al., 2016). Each cluster holds all the instances that hold or carry the similar characteristics as the rest of the population. Each cluster contains similar instances and values but each cluster is different from the other cluster in the model. Different clustering methods use different criteria to assemble the data in separate clusters (Harrington, 2012). It is common to install a differentiation mechanism in the algorithm that groups the similar instances in a single cluster while the differentiating instances are grouped in separate clusters (Witten et. al., 2016). Clustering is a great model for achieving unsupervised learning outcomes and considered to be a very good method for conducting statistical analysis.

4.2 Case Prioritisation and Machine Learning

The biggest advantage embedded in machine learning is its ability to adapt to different and diverse scenarios (Witten et. al., 2016). In this thesis, machine learning is used to automate reliability measurement. In other words, the output of machine learning model will be proxy to the reliability of case leader. Using this proxy will eliminate the need to perform extensive evaluation of all digital forensics stakeholders in the law enforcement organization. Keep in mind that it is a fact that the modern computing capabilities have not achieved the advancement that makes them as efficient as human observation or learning (Witten et. al., 2016). Yet there have been scenarios where machine learning has been effectively and successfully applied (Witten et. al., 2016). In the 90s era a detailed theoretical learning foundation was identified and subsequent programs have been developed to confirm or comply with that guiding principle (Witten et. al., 2016). Machine learning is considered to be effective in the following scenarios.

- Data mining tasks where a large number of data needs to be sorted and the database contains differentiating characteristics that can be discovered through machine learning mechanisms.
- Domains that have not been completely understood by the humans and the computers can generate models to replicate different scenarios such as facial recognition and playing different games.
- Scenarios where the programs have to quickly adapt to the changing circumstances and scenarios.

In short, machine learning is heavily data oriented (Witten et. al., 2016). They try to mimic the relationship in the training sets to extrapolate it to the rest of the data available. In this thesis, the training set is the collected data from questionnaire. But if the training set does not truly represent the problem or identifying pattern in the data, then the resulting model may have several contingencies and differentiations from the actual problem or desired outcome (Witten et. al., 2016). The biggest limitation in machine learning scenarios is their inability to account for the prior information available. To overcome this limitation, cross validation can be used.

4.3 Training and Testing Datasets

Identifying the relations in a function and then employing that very function on the same data is considered to be a very common methodological error and tends to construct a self-repeating model that fails to predict any new scenarios or identify any meaningful relationship or pattern in the available data (Domingos, 2012). Such a scenario is referred to as over-fitting. To avoid such a situation it is recommended in supervised machine learning scenarios to abstain a part of the data from making into the actual algorithm and use it as an experimenting sample. It is critical to note that every learning model starts as an experiment even in the most commercial settings.

When assessing numerous settings (Hyper parameters) the models run a risk of overfitting due to the fact that the parameters can be edited and tweaked until a perfect or optimal estimator is identified (Domingos, 2012). The knowledge regarding the estimator can combine into the model resulting in compromised evaluation that fails to report on the general performance. So resolve this issue a separate part of the dataset can held exclusive called “validation set” so that the training continues without any interruptions and the final test can be run on data set. However, when three different samples are held out of the model its ability to learn through samples is drastically compromised. And the outcome can be devised through a completely random pairs of choices.

A solution to this issue can be achieved through cross-validation (Domingos, 2012). A test set or example still needs to be retained from final evaluation, but the validation set can be ignored in a CV. The set is then further divided into smaller parts that are denoted with k-folds. The following methodology is employed for each k-fold

- A model is devised or trained using k – 1 of folds as data for training.
- The resulting model is then applied to the remaining data (that can be used to create performance measure such as accuracy)

The resultant performance measure through k-fold validation is the average of the values present in the loop. This solution can be very expensive with regards to the computational resources, but it avoids the wastage of a large amount of data; which can prove to be a very big advantage in scenarios where the sample is small (Domingos, 2012).

4.4 Combining Reliability and Prioritisation Model

Usually, prioritisation is done based on priority metric. This metric can be calculated using wide range of formulas. These formulas take into consideration several aspects of the digital forensics case such as:

- Number of victims.
- Amount of losses.
- Severity.
- Relation to national security.
- Public pressure.
- Complexity of investigated devices.

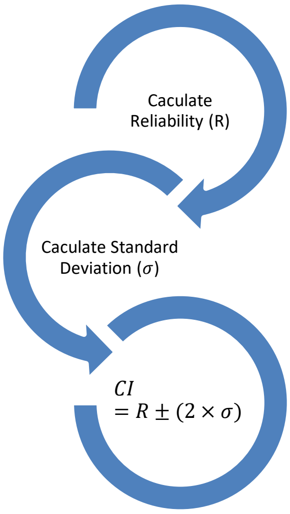
These aspects are among the most used ones to evaluate case importance (Chawki et. al. 2015). There are many factors that can be used to calculate the priority metric. These factors depend on the law enforcement organization nature. Some organizations are focusing national security; while others are dealing with only financial crimes. Hence, how the actual priority metric is calculated is out of the scope of this research to insure generalizability of the proposed solution. Focusing on specific subset of metrics will reduce the applicability of proposed model. However, this thesis is proposing a linear integration approach to provide high degree of controllability. This linear approach works by adding reliability estimation to already existing priority metric.

$$\beta = \alpha R + (1 - \alpha) P$$

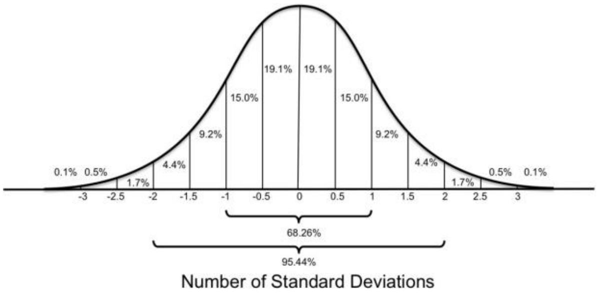
Where β is the new priority metric after integration, R is the estimated reliability measure, P is the old priority metric and α is weighting factor to balance between reliability estimation and existing priority measure. Keep in mind that variables in the previous formula are normalized which means that their values lie between zero and one. In this linear integration, α controls the degree of which reliability estimation influence existing priority. For example, if α is set to zero, the integrated priority will be exactly the existing priority metric.

Another way to look to this integration approach is as a correction parameter. It assumes that the existing prioritisation metric has embedded error due to the low reliability of case handler. To remove this error, estimated reliability estimation is added. This addition introduces the necessary shift in the existing prioritisation metric so that it becomes more accurate.

One may introduce a confidence interval as well by calculating the standard deviation of reliability estimation and assuming the normal distribution of estimation error. Adding and subtracting values of two standard deviations will be considered as an interval of 95% confidence around the new prioritisation metric.


Caculate Reliability (R)
Caculate Standard Deviation (σ)
$CI = R \pm (2 \times \sigma)$

A necessary assumption for confidence interval calculation is normality of data distribution. If calculated reliability measurement of all stakeholders in the organization follow normal distribution, then the following graph describes the confidence interval.



After calculating the integrated priority (β) for each case, then case with the highest β will be given higher priority. It is evident that have higher reliability estimation for any case will increase its priority.

4.5 Chapter Summary

This chapter discusses machine learning techniques as the base methodologies to automate prioritisation process of digital forensic cases. Several machine learning techniques were discussed. In addition, two integration approaches were proposed. The first approach is linear while the second is non-linear. Both of them can be used to improve prioritisation process without extreme modifications to the existing prioritisation process used in the digital forensics department.

Chapter 5: Results and Discussions

As mentioned in previous chapter, the main goal of this research is to improve prioritisation process of cases in digital forensics departments. This chapter provides empirical data, their quantitative analysis, and interpretation of received results. The data were collected by the questionnaire. For analysis of the data, the statistical methods have been used. The choice of the method was conditioned by purposes and objectives of the given study. The investigation of the dependence the perception of digital forensics operation in the organization from demographic aspects of subjects has been performed by the two-sided Chi-Square test. Such demographic aspects as Gender, Education, Age, Rank, Career Experience, Years in the Organization, Years in Current Position and Years in Digital Forensics were investigated.

Seven hypotheses have been investigated. The null hypotheses are: “There are no differences in perception of the digital forensic between groups of the respondents with different social-demographic characteristics such as Gender ($H1_0$), Age ($H2_0$), Education ($H3_0$), Rank ($H4_0$), Years in current position ($H5_0$), Number of the years in organization ($H6_0$), Experience in digital forensic ($H7_0$)”. The alternative hypotheses accordingly are: “There are differences in perception of the digital forensic between groups of the respondents with different social-demographic characteristics such as Gender ($H1_{alt}$), Age ($H2_{alt}$), Education ($H3_{alt}$), Rank ($H4_{alt}$), Years in current position ($H5_{alt}$), Number of the years in organization ($H6_{alt}$), Experience in digital forensic ($H7_{alt}$)”. Each hypothesis consists of twenty items (sub-hypotheses). The null hypothesis is rejected if at least one null sub-hypothesis is rejected. For testing of the hypothesis, the standard level of the significance 0.05 was used in this research. The analysis has been conducted by using the SPSS software (version 23).

5.1 Demographic Characteristics of Respondents

The frequencies and distribution of the respondents by gender are presented in Table 5.1 and Figure 5.1.

Table 5.1: Frequencies and percentage distribution of respondents by gender.

Gender	Frequency	Percentage
Female	58	28
Male	151	72
Total	209	100

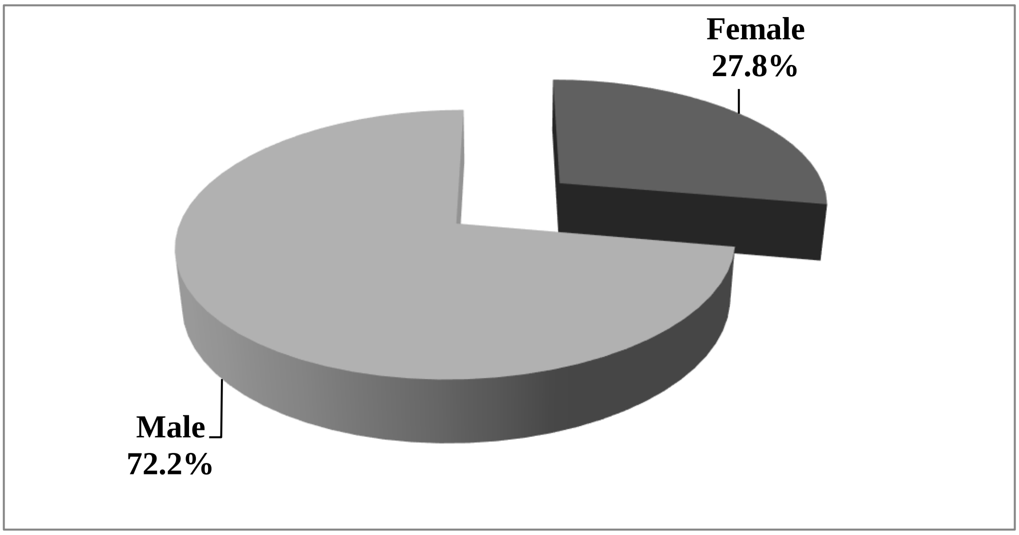


Figure 5.1: Percentage distribution of respondents by gender.

Table 5.1 and Chart 5.1 present frequencies and distribution of respondents by gender. Around 72% of the respondents were males (72.2%) whereas 27.8% were females. So this data indicate the majority of the respondents were males. It can be explained by the specificity of the law enforcement organizations. Frequencies and respondents percentage distribution of by level education are displayed in Table 5.2 and Figure 5.2.

Table 5.2: Frequencies and respondents distribution by education.

Educational Level	Frequency	Percentage
Bachelor	114	55
Master	53	25
PhD	10	5
Secondary	32	15
Total	209	100

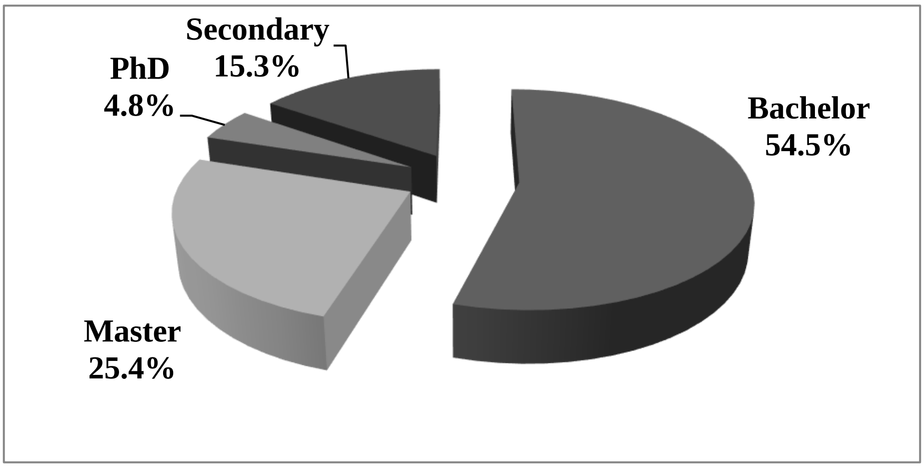


Figure 5.2: Percentage distribution of respondents by education.

In the above Figure and table, the percentage distribution of respondents by education level are shown. More than 54% of the respondents have a Bachelor degree and above 25% have a Master degree. About 15.3% of respondents have a secondary education. Only 4.8% of respondents have Ph.D. degree. These data show that majority of respondents have Bachelor degree.

Frequencies and percentage distribution of respondents by rank are demarcated in Table 5.3 and Figure 5.3.

Table 5.3: Frequencies and respondents distribution by rank.

Rank	Frequency	Percentage
1st. Lieutenant	43	21
1st. Warrant Officer	8	4
Captain	36	17
Lieutenant	18	9
Lt. Colonel	10	5
Major	94	45
Total	209	100

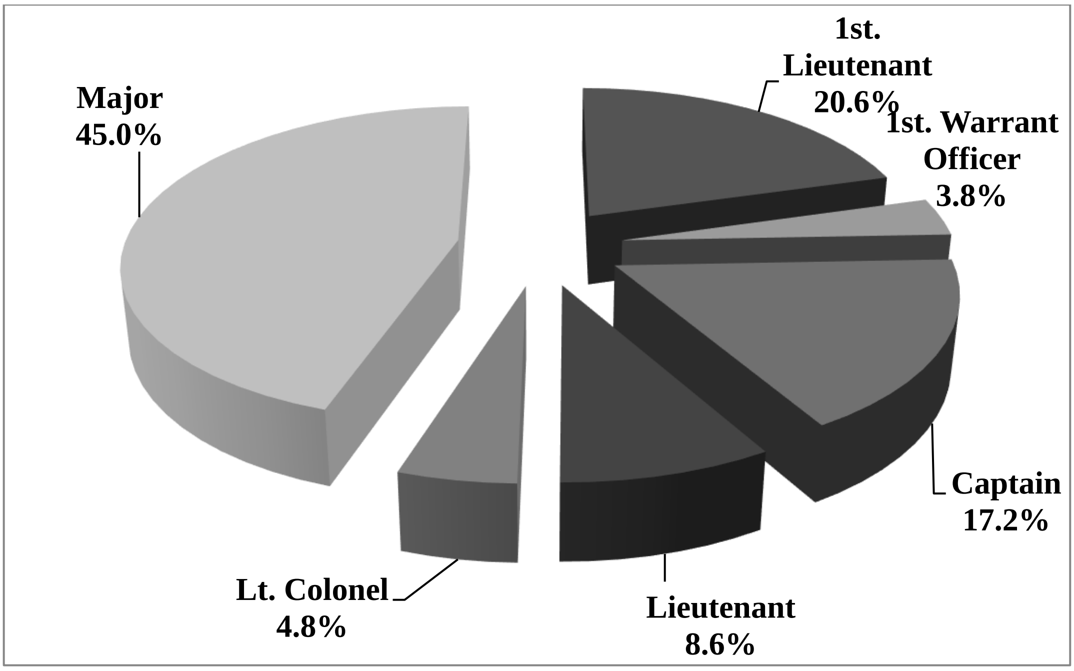


Figure 5.3: percentage distribution of respondents by rank.

Table and Figure above show 45% respondents have Major rank, 20.6% respondents have 1st Lieutenant Rank, 17.2% respondents have Captain Rank, 8.6 % respondents have Lieutenant Rank, 4.8% respondents have Lt. Colonel Rank and 3.8% respondents have 1st. Warrant officer Rank. So the majority of the respondents have Major, 1st. Lieutenant, and captain Ranks.

Table 5.4 and Figure 5.4 indicate the frequency and percentage distribution of the respondents by number years in current position.

Table 5.4: Frequencies and respondents distribution by number years in current position.

Number years	Frequency	Percentage
1	55	26.3
2	50	23.9
3	55	26.3
4	49	23.4
Total	209	100

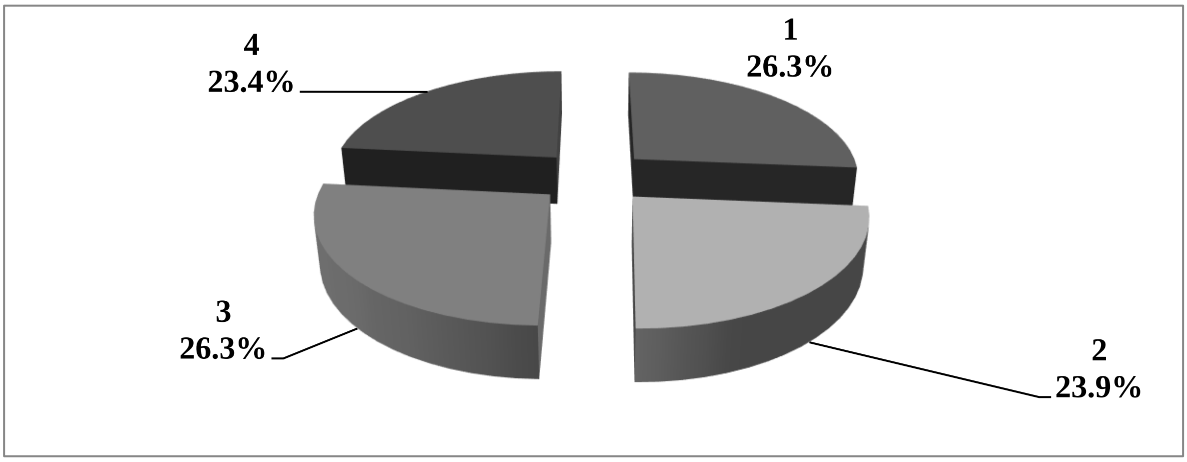


Figure 5.4: Percentage distribution of respondents by number years in current position.

The above Figure and Table display the frequencies and percentage distribution of respondent by number years in current position. The equal shares of the respondents (26.3%) work one and three years in the current position in the organization, 23.9%

respondents work two years in current position and 23.4% respondents work 4 years in current position. So data indicate the approximately equal shares of the respondents work during 1, 2, 3, and 4 years in current position.

Table 5.5 and Figure 5.5 present percentage distribution of respondent and frequencies by number years in digital forensics.

Table 5.5: Percentage distribution of the respondents and frequencies by number years in digital forensics.

Years in Digital Forensics	Frequency	Percentage
0	185	88.5
1	4	1.9
2	3	1.4
3	3	1.4
4	2	1.0
5	1	.5
8	1	.5
9	1	.5
10	3	1.4
11	2	1.0
12	1	.5
15	1	.5
17	1	.5
26	1	.5
Total	209	100.0

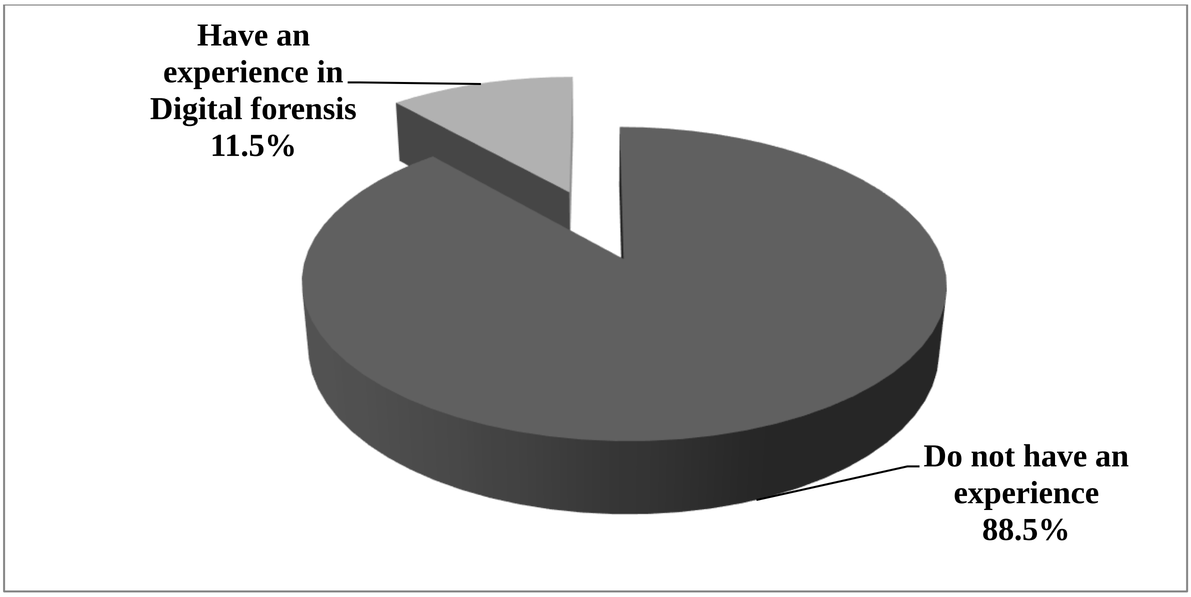


Figure 5.5: Percentage distribution of the respondents by number years in digital forensics.

Table 5.5 indicates the majority of the respondents (88.5%) not have experience in digital forensic (such respondents marked “null” years). Only four respondents have 1 year experience in digital forensic. Experience 2, 3 and 10 years have three respondents. Two respondents have 11 years in digital forensic. Other numbers of years in digital forensic noted in Table 5.5 have by one respondent. As a little number of respondents has one or another number years in digital forensic, in further all respondents will be divided into two groups those who worked in digital forensic and respondents without experience in digital forensic. Figure 5.5 shows only 11.5% of respondents worked in digital forensic. So, above data indicate the majority of the respondents do not have an experience in digital forensic.

The respondents’ frequencies and distribution by years in the organization are presented in Table 5.6.

Table 5.6: The respondents’ frequencies and distribution by years in organization.

Years in the Organization	Frequency	Percentage
1	1	0.5
2	6	2.9
3	3	1.4
4	10	4.8
5	11	5.3
6	11	5.3
7	14	6.7
8	12	5.7
9	6	2.9
10	15	7.2
11	6	2.9
12	11	5.3
13	8	3.8
14	7	3.3
15	5	2.4
16	8	3.8
17	10	4.8
18	4	1.9
19	6	2.9
20	9	4.3
21	8	3.8
22	8	3.8
23	5	2.4

24	3	1.4
25	5	2.4
26	1	0.5
27	7	3.3
28	2	1
29	1	0.5
30	3	1.4
31	3	1.4
Total	209	100

As Table 5.6 indicates, the range of years in the organization is from 1 up to 31. This is enough large diapason. Therefore, for further analysis, we will create three age groups (See Table 5.7).

Table 5.7: The respondents’ frequencies and distribution by years in organization (tree groups).

Years in the Organization	**Frequency**	**Percentage**
1-10 years	89	42.58
11-20 years	74	35.41
21-31 years	46	22.01
Total	209	100

Table 5.7 and Figure 6.6 indicate that 42.6% of the respondents work in the organization from 1 to 10 years. 35.4% of respondents are in the organization from 11 to 20 years. The rest of respondents (22%) work in the organization for 21 years up to 31 years. So

the majority of respondents work in the organization from 1 up to 10 and from 11 up to 20 years.

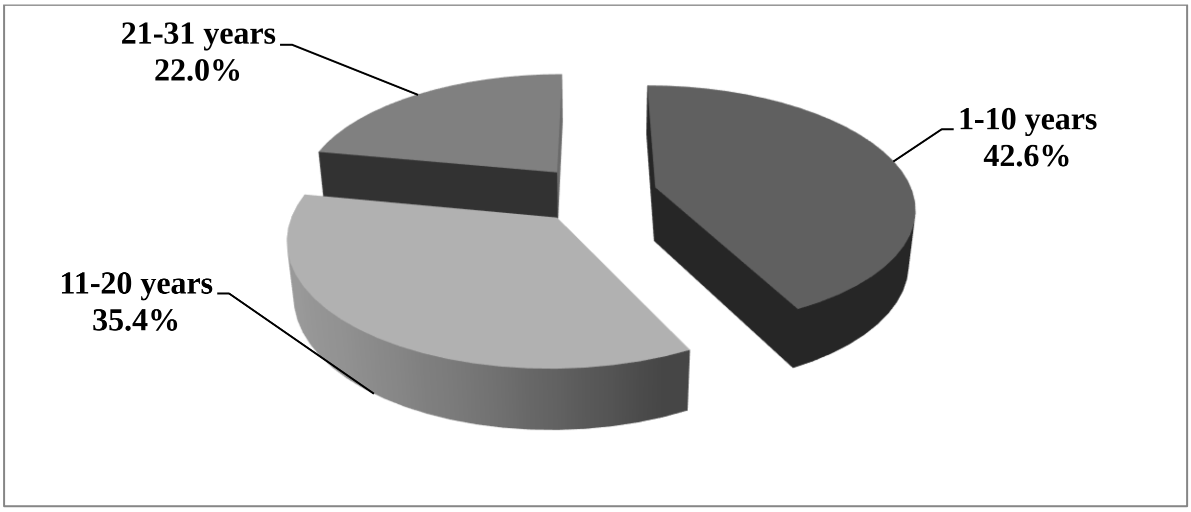


Figure 5.6: Respondents’ distribution by years in organization.

For career experience, the frequencies and respondents’ distribution were received identical results as for years in the organization (See Table 5.8 and Table 5.6).

Table 5.8: The respondents’ frequencies and distribution by career experience.

Career Experience, years	Frequency	Percentage
1	1	.5
2	6	2.9
3	3	1.4
4	10	4.8
5	11	5.3
6	11	5.3
7	14	6.7

8	12	5.7
9	6	2.9
10	15	7.2
11	6	2.9
12	11	5.3
13	8	3.8
14	7	3.3
15	5	2.4
16	8	3.8
17	10	4.8
18	4	1.9
19	6	2.9
20	9	4.3
21	8	3.8
22	8	3.8
23	5	2.4
24	3	1.4
25	5	2.4
26	1	.5
27	7	3.3
28	2	1.0
29	1	.5
30	3	1.4
31	3	1.4
Total	209	100.0

Thus, this variable was excluded from further analysis as fully identical variable “Years in organization”.

The range of the age of respondents also is large (from 26 up to 52 years). Therefore, for the further analysis the three age groups have been created: (1) 26-34 years, (2) 35-43 years, and (3) 44-52. The respondents’ frequencies and distribution by age groups are presented in Table 5.9 and Figure 5.7.

Table 5.9: The respondents’ frequencies and distribution by age groups.

Age Group, years	Frequency	Percentage
26-34	98	46.9
35-43	63	30.1
44-52	48	23.0
Total	209	100

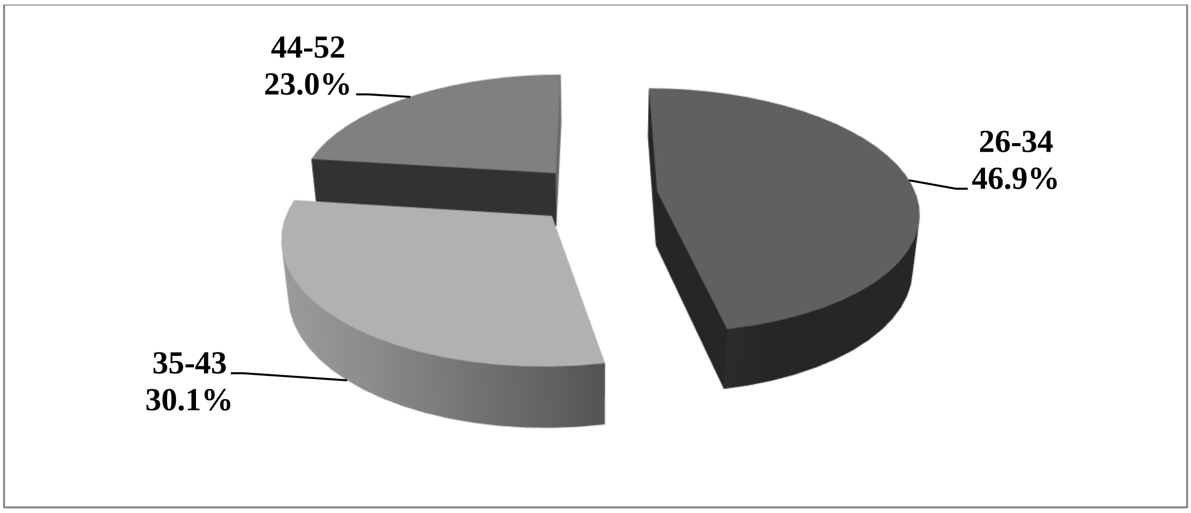


Figure 5.7: Respondents’ distribution by ace groups.

As Table 6.9 and Figure 6.7 display, 46.9% of respondents have an age from 26 up to 34 years. Around 30% of respondents are from age group 35-43 years and 23% of respondents are from age group 44-52 years. Hence, the majority respondents are from age groups 26-34 and 35-43 years.

5.2 Perception of Digital Forensics - sample of the respondents in general

For the study of the respondents' perception of Digital Forensics in law enforcement organization, the answers of respondents on the correspondent question were investigated. Table 5.10 presents frequencies and Percentage distribution of the respondents' estimations the statement “Digital forensics is mainly concerned about cybercrimes”.

Table 5.10: Frequencies and percentage distribution by respondents' estimations the statement “Digital forensics is mainly concerned about cybercrimes”.

Estimation	Frequency	Percentage
Agree	14	6.7
Disagree	7	3.3
Neutral	75	35.9
Strongly Agree	6	2.9
Strongly Disagree	107	51.2
Total	209	100.0

As Table 5.10 displays 51.2% of respondents are strongly disagree that digital forensics is mainly concerned about cybercrimes, 35.9% of respondents are neutral, 6.7% agree, 3.3% of respondents disagree, and 2.9% strongly agree. This data indicate the majority of the respondents strongly disagree that digital forensics is mainly concerned about cybercrimes.

The frequencies and distribution of the respondents’ estimations the statement “The organization has clear procedures to handle all aspects of digital investigation” are demarcated in Table 5.11.

Table 5.11: Frequencies and percentage distribution by respondents' estimations the statement “The organization has clear procedures to handle all aspects of digital investigation”.

Estimation	Frequency	Percentage
Agree	5	2.4
Disagree	117	56.0
Neutral	44	21.1
Strongly Agree	11	5.3
Strongly Disagree	32	15.3
Total	209	100

The results presented in Table 5.11 show 56% of respondents disagree that their organization has clear procedures to handle all aspects of digital investigation and 15.3% strongly disagree with this statement. Only 5.3% of respondents strongly agree and 2.4% agree. The rest of the respondents (21.1%) are neutral. These data indicate the majority of the respondents disagree that their organization has clear procedures to handle all aspects of the digital investigation. Table 5.12 shows frequencies and distribution of the respondents’ estimation the statement “IT department is controlling digital forensics operations

Table 5.12: Frequencies and percentage distribution by respondents' estimations the statements “IT department is controlling digital forensics operations”.

Estimation	Frequency	Percentage
Agree	10	4.8
Disagree	11	5.3
Neutral	88	42.1

Strongly Agree	6	2.9
Strongly Disagree	94	45.0
Total	209	100

As Table 5.12 presents the 45% of respondents strongly disagree that IT department is controlling digital forensics operations in their organization and 5.3% disagree. The 4.8% of respondents agree with this statement and 2.9% strongly agree. The rest 42.1% of respondents are neutral. Hence, about half of the respondents strongly disagree that IT department is controlling digital forensics operations in their organization.

Frequencies and Percentage distribution of the respondents’ estimations about the statement “Delivering and acquiring information regarding digital investigation are very organized” are displayed in Table 5.13.

Table 5.13:Frequencies and percentage distribution by respondents' estimations the statements “Delivering and acquiring information regarding digital investigation are very organized”.

Estimation	**Frequency**	**Percentage**
Agree	18	8.6
Disagree	115	55.0
Neutral	27	12.9
Strongly Agree	8	3.8
Strongly Disagree	41	19.6
Total	209	100.0

Table 5.13 shows that 55% of respondents disagree that delivering and acquiring information regarding digital investigation are very organized in their organization and 19.6% of respondents strongly disagree with this statement. The 8.6% of respondents agree with this thesis and 3.8% of respondents strongly agree. The remaining of the respondents (12.9%) is neutral. Hence, this data indicate the majority respondents

disagree and strongly disagree that delivering and acquiring information regarding digital investigation are very organized in their organization

Table 5.14 shows the frequencies and Percentage distribution of the respondents by estimations the statement “Each digital forensics case has its own plan of operations and processes.

Table 5.14: Frequencies and percentage distribution of the respondents by estimations the statement “Each digital forensics case has its own plan of operations and processes”.

Estimation	**Frequency**	**Percentage**
Agree	107	51.2
Disagree	8	3.8
Neutral	70	33.5
Strongly Agree	10	4.8
Strongly Disagree	14	6.7
Total	209	100.0

As displayed in Table 5.14, 51.2% of respondents agree that each digital forensics case has its own plan of operations and processes and 4.8% of respondents strongly agree with that. Around 7% of respondents strongly disagree and 3.8% disagree with this sentence. The rest 33.5% of respondents are neutral. Hence, the majority of the respondents agrees and strongly agrees that each digital forensics case has its own plan of operations and processes.

In table 5.15 the frequencies and Percentage distribution of the respondents by estimations the statement “The organization has the ability to examine any digital device regardless of its complexity” are demarcated.

Table 5.15: Frequencies and percentage distribution of the respondents by estimations the statement "The organization has the ability to examine any digital device regardless of its complexity".

Estimation	Frequency	Percentage
Agree	22	10.5
Disagree	112	53.6
Neutral	30	14.4
Strongly Agree	14	6.7
Strongly Disagree	31	14.8
Total	209	100

According to Table 5.15, above 53% of respondents disagree and 14.8% strongly disagree that the organization has the ability to examine any digital device regardless of its complexity whereas 10.5% of the respondents agree and 5.7 strongly agree with this statement. The rest 14.4% of respondents are neutral. The majority of the respondents disagree and strongly disagree the organization has the ability to examine any digital device regardless of its complexity. Table 5.16 presents frequencies and Percentage distribution of the respondents by estimations the statement "The organization has clear guidelines about storing and transferring digital evidence".

Table 5.16: Frequencies and percentage distribution of the respondents by estimations the statement "The organization has clear guidelines about storing and transferring digital evidences".

Estimation	Frequency	Percentage
Agree	11	5.3
Disagree	110	52.6
Neutral	36	17.2
Strongly Agree	9	4.3
Strongly Disagree	43	20.6
Total	209	100

Table 5.16 indicates the 52.6% of the respondents disagree and 20.6% of respondents strongly disagree that the organization has clear guidelines about storing and transferring digital evidence. A minority of the respondents agree and strongly agree with this statement (5.3% and 4.3% correspondently) and 17.2% of respondent are neutral. Hence, the majority of the respondents disagrees and strongly disagrees that the organization has clear guidelines about storing and transferring digital evidence.

The frequencies and Percentage distribution of the respondents by estimations the statement “Digital investigators in the organization are well trained and they have all necessary skills to perform any operation in digital forensics” are displayed in Table 5.17.

Table 5.17: frequencies and percentage distribution of the respondents by estimations the statement “Digital investigators in the organization are well trained and they have all necessary skills to perform any operation in digital forensics”.

Estimation	Frequency	Percentage
Agree	11	5.3
Disagree	123	58.9
Neutral	32	15.3
Strongly Agree	11	5.3
Strongly Disagree	32	15.3
Total	209	100

Taking into account Table 5.17, 58.9% of respondents disagree that digital investigators in the organization are well trained and they have all necessary skills to perform any operation in digital forensics and 15.3% of respondents strongly disagree with this statement. A small part of respondents agree (5.3%) and strongly agree with that whereas the rest 15.3% of the respondents are neutral. These data indicates the majority of the respondents disagree and strongly disagree that digital investigators in the organization are well trained and they have all necessary skills to perform any operation in digital forensics.

Table 5.18 shows the frequencies and Percentage distribution of the respondents by estimations the statement “The organization needs to increase the number of digital investigators**”.**

Table 5.18: Frequencies and percentage distribution of the respondents by estimations the statement “The organization needs to increase number of digital investigators”.

Estimation	Frequency	Percentage
Agree	8	3.8
Disagree	16	7.7
Neutral	70	33.5
Strongly Agree	98	46.9
Strongly Disagree	17	8.1
Total	209	100

As Table 5.18 displays 46.9% of the respondents strongly agree and 3.8% agree that the organization needs to increase the number of digital investigators. Around 8% of respondents strongly disagree and 7.7% disagree with that. The remaining 33.5% of the respondents are neutral. Hence, the majority of the respondents agrees and strongly agrees that the organization needs to increase the number of digital investigators.

The frequencies and Percentage distribution of the respondents by estimations the statement “Most types of criminal investigations in the organization use digital forensics” are demarcated in Table 5.19.

Table 5.19: Frequencies and percentage distribution of the respondents by estimations the statement "Most types of criminal investigations in the organization use digital forensics".

Estimation	Frequency	Percentage
Agree	105	50.2
Disagree	18	8.6
Neutral	64	30.6
Strongly Agree	3	1.4
Strongly Disagree	19	9.1
Total	209	100

Table 5.19 indicates around half of the respondents (50.2%) agree and 1.4% strongly agree that most types of criminal investigations in the organization use digital forensics. The 30.6% of respondents are neutral whereas the remaining of the respondents disagree (8.6%) and strongly disagree with that. These data show the majority of the respondents agree and strongly agree that most types of criminal investigations in the organization use digital forensics.

Table 5.20 presents the frequencies and Percentage distribution of the respondents by estimations for the statement "Achievements of digital forensics team are well-known throughout the organization".

Table 5.20: Frequencies and percentage distribution of the respondents by estimations the statement "achievements of digital forensics team are well-known throughout the organization".

Estimation	Frequency	Percentage
Agree	12	5.7
Disagree	116	55.5
Neutral	35	16.7
Strongly Agree	11	5.3
Strongly Disagree	35	16.7
Total	209	100

Considering table 20 more 55% of the respondents disagree and 5.3% strongly disagree that achievements of digital forensics team are well-known throughout the organization. A minority of the respondents agree (5.7%) and strongly agree (5.3%) with that. The rest 16.7% of the respondents are neutral. These data indicates the majority of respondents disagree and strongly disagree that achievements of digital forensics team are well-known throughout the organization. In Table 5.21, the frequencies and Percentage distribution of the respondents by estimations the statement “The organization needs to acquire more technologies and tools for digital forensics” are shown.

Table 5.21: Frequencies and percentage distribution of the respondents by estimations the statement “The organization needs to acquire more technologies and tools for digital forensics”.

Estimation	**Frequency**	**Percentage**
Agree	10	4.8
Disagree	14	6.7
Neutral	79	37.8
Strongly Agree	95	45.5
Strongly Disagree	11	5.3
Total	209	100

As Table 5.21, 45.5% of the respondents strongly agree and 4.8% agree with the statement that organization needs to acquire more technologies and tools for digital forensics whereas 37.8% of respondents are neutral. The rest of the respondents disagree (6.7%) and strongly disagree (5.3%) with this statement. Hence, the majority of respondents agrees and strongly agrees that organization needs to acquire more technologies and tools for digital forensics.

The frequencies and Percentage distribution of the respondents by estimations the statement “The organization has the ability to develop new digital forensics tools that can be used by other organizations” are reported in Table 5.22.

Table 5.22: Frequencies and percentage distribution of the respondents by estimations the statement “The organization has the ability to develop new digital forensics tools that can be used by other organizations”.

Estimation	Frequency	Percentage
Agree	10	4.8
Disagree	14	6.7
Neutral	77	36.8
Strongly Agree	95	45.5
Strongly Disagree	13	6.2
Total	209	100

According to Table 5.22 around 45% of the respondents strongly agree and 4.8% agree that organization has the ability to develop new digital forensics tools that can be used by other organizations. 12.9% of the respondents have an opposite view: 6.2% strongly disagree and 6.7% disagree with that. The rest 36.8% of respondents are neutral. Therefore, the majority of the respondents agrees and strongly agrees that organization has the ability to develop new digital forensics tools that can be used by other organizations.

Table 5.23 presents the frequencies and Percentage distribution of the respondents by estimations the statement “The organization depends on digital forensics teams of third parties to help with digital investigations”.

Table 5.23: Frequencies and percentage distribution of the respondents by estimations the statement "The organization depends on digital forensics teams of third parties to help with digital investigations".

Estimation	Frequency	Percentage
Agree	107	51.2
Disagree	9	4.3
Neutral	67	32.1
Strongly Agree	8	3.8
Strongly Disagree	18	8.6
Total	209	100

As table 5.23, more that 51% of respondents agree and 3.8% strongly agree that organization depends on digital forensics teams of third parties to help with digital investigations whereas 4.3% disagree and 8.6% of respondents strongly disagree with this statement. The remaining 32.1% of the respondents are neutral. These data indicate the majority of the respondents agree and strongly agree that organization depends on digital forensics teams of third parties to help with digital investigations.

Table 5.24 shows the frequencies and Percentage distribution of the respondents by estimations the statement "Digital forensics team has an influence on drawing the general policy and strategy of the organization".

Table 5.24: Frequencies and percentage distribution of the respondents by estimations the statement "Digital forensics team has influence on drawing the general policy and strategy of the organization".

Estimation	Frequency	Percentage
Agree	6	2.9
Disagree	8	3.8
Neutral	77	36.8
Strongly Agree	10	4.8
Strongly Disagree	108	51.7
Total	209	100

Table 5.24 shows 51.7% of the respondents strongly disagree and 3.8% disagree that digital forensics team has an influence on drawing the general policy and strategy of the organization. A small part of the respondents has opposite view: 2.9% agree and 4.8% strongly agree with this statement. The rest 36.8% of the respondents are neutral. It indicates the majority of the respondents disagree and strongly disagree that digital forensics team has an influence on drawing the general policy and strategy of the organization.

The frequencies and Percentage distribution of the respondents by estimations the statement "The organization helps other organizations in term of digital forensics" are reported in Table 5.25.

Table 5.25: Frequencies and percentage distribution of the respondents by estimations the statement "The organization helps other organizations in term of digital forensics".

Estimation	Frequency	Percentage
Agree	8	3.8
Disagree	123	58.9
Neutral	34	16.3
Strongly Agree	9	4.3
Strongly Disagree	35	16.7
Total	209	100

Considering Table 5.25 around 59% of respondents disagree and 16.7% disagree that their organization helps other organizations in term of digital forensics whereas 3.8% and 4.3% of respondent agree and strongly agree with that. The rest 16.3% of the respondents are neutral. Hence, the majority respondents disagree and strongly disagree that their organization helps other organizations in term of digital forensics.

Table 5.26 presents the frequencies and Percentage distribution of the respondents by estimations the statement “Digital forensics team has full access to all information in any assigned case”.

Table 5.26: Frequencies and percentage distribution of the respondents by estimations the statement “Digital forensics team has full access to all information in any assigned case”.

Estimation	**Frequency**	**Percentage**
Agree	17	8.1
Disagree	103	49.3
Neutral	41	19.6
Strongly Agree	16	7.7
Strongly Disagree	32	15.3
Total	209	100

As table 5.26, more than 49% of respondents disagree and 15.3% strongly disagree that digital forensics team has full access to all information in any assigned case. The minority of the respondents has an opposite position: 8.1% of respondents agree and 7.7% strongly agree with this statement. The remaining of the respondents (19.6%) are neutral. Therefore, the majority of the respondents disagree and strongly disagree that digital forensics team has full access to all information in any assigned case.

Table 5.27 shows the frequencies and Percentage distribution of the respondents by estimations the statement “There are established programs to train and develop human resources for digital forensics positions”.

Table 5.27: Frequencies and percentage distribution of the respondents by estimations the statement “There are established programs to train and develop human resources for digital forensics positions”.

Estimation	Frequency	Percentage
Agree	16	7.7
Disagree	111	53.1
Neutral	39	18.7
Strongly Agree	5	2.4
Strongly Disagree	38	18.2
Total	209	100

Table 5.27 indicates 53.1% of the respondents disagree that there are established programs to train and develop human resources for digital forensics positions and 18.2% strongly disagree with that. Around 10% of respondents have an opposite opinion. 7.7% of respondents agree and 2.4% strongly agree with this statement. 18.7% of respondents are neutral. Hence, the majority of respondents disagrees and strongly disagrees that there are established programs to train and develop human resources for digital forensics positions in their organization.

In Table 5.28 the frequencies and Percentage distribution of the respondents by estimations the statement “Employees of digital forensics can easily work IT department without additional training and vice versa” are reported.

Table 5.28: Frequencies and percentage distribution of the respondents by estimations the statement "Employees of digital forensics can easily work it department without additional training and vice versa".

Estimation	Frequency	Percentage
Agree	8	3.8
Disagree	118	56.5
Neutral	46	22.0
Strongly Agree	11	5.3
Strongly Disagree	26	12.4
Total	209	100

As table 5.28, 56.5% of respondents disagree and 12.4% strongly disagree that employees of digital forensics can easily work IT department without additional training and vice versa whereas 22% of respondents are neutral. Only 3.8% of the respondents agree and 5.3% strongly agree with that. It indicates the majority of the respondents disagree and strongly disagree that employees of digital forensics can easily work IT department without additional training and vice versa.

The frequencies and Percentage distribution of the respondents by estimations the statement "The organization conducts seminars to familiarize stakeholders with operations of digital forensics in the organization" are displayed in Table 5.29.

Table 5.29: Frequencies and percentage distribution of the respondents by estimations the statement “The organization conducts seminars to familiarize stakeholders with operations of digital forensics in the organization”.

Estimation	Frequency	Percentage
Agree	103	49.3
Disagree	15	7.2
Neutral	73	34.9
Strongly Agree	3	1.4
Strongly Disagree	15	7.2
Total	209	100

Considering Table 5.29, 49.3% of the respondents agree and 1.4% strongly agree that the organization conducts seminars to familiarize stakeholders with operations of digital forensics in the organization. Around 7% of respondents disagree and 7.2% of respondents strongly with that. Hence, the majority of the respondents agrees and strongly agrees that the organization conducts seminars to familiarize stakeholders with operations of digital forensics in the organization.

5.3 Differences in Perception of the digital forensic: Hypotheses testing

5.3.1Gender

The results of the Chi-square test for differences in Perception of the digital forensic by gender are reported in Table 5.30.

Table 5.30: Chi-square test results for differences in perception of the digital forensic by gender.

Sub-hypotheses	Statements	Pearson Chi-Square Value	df	Asymptotic Significance (2-sided)
$H1_1$	Digital forensics is mainly concerned about cybercrimes	1.56	4	0.816
$H1_2$	The organization has clear procedures to handle all aspects of digital investigation	0.233	4	0.994
$H1_3$	IT department is controlling digital forensics operations	4.302	4	0.367
$H1_4$	Delivering and acquiring information regarding digital investigation are very organized	1.176	4	0.882
$H1_5$	Each digital forensics case has its own plan of operations and processes	6.198	4	0.185
$H1_6$	The organization has the ability to examine any digital device regardless of its complexity	3.567	4	0.468
$H1_7$	The organization has clear guidelines about storing and transferring digital evidences	0.726	4	0.948
$H1_8$	Digital investigators in the organization are well trained and they have all necessary skills to perform any operation in digital forensics	3.304	4	0.508
$H1_9$	The organization needs to increase the number of digital investigators	7.237	4	0.124
$H1_{10}$	Most types of criminal investigations in the organization use digital forensics	2.07	4	0.723
$H1_{11}$	Achievements of digital forensics team are well-known throughout the organization	8.855	4	0.065
$H1_{12}$	The organization needs to acquire more technologies and tools for digital forensics	2.932	4	0.569

$H1_{13}$	The organization has the ability to develop new digital forensics tools that can be used by other organizations	1.037	4	0.904
$H1_{14}$	The organization depends on digital forensics teams of third parties to help with digital investigations	3.714	4	0.446
$H1_{15}$	Digital forensics team has influence on drawing the general policy and strategy of the organization	2.435	4	0.656
$H1_{16}$	The organization helps other organizations in term of digital forensics	6.17	4	0.187
$H1_{17}$	Digital forensics team has full access to all information in any assigned case	4.236	4	0.37
$H1_{18}$	There are established programs to train and develop human resources for digital forensics positions	8.338	4	0.08
$H1_{19}$	Employees of digital forensics can easily work IT department without additional training and vice versa	1.037	4	0.904
$H1_{20}$	The organization conducts seminars to familiarize stakeholders with operations of digital forensics in the organization	1.898	4	0.755

Hypothesis $H1_0$: There are no differences in the perceptions of the digital forensic by gender.

Hypothesis $H1_{alt}$: There are differences in the perceptions of the digital forensic by gender.

Table 5.30 indicates that there aren’t statistically significant differences in perception of the digital forensic between gender groups as the p-value for all items is more than 0.05. Hence, the hypothesis H1 is accepted.

But for two items “Achievements of digital forensics team are well-known throughout the organization” and “There are established programs to train and develop human resources for digital forensics positions” p-values are less than 0.1. It gives a possibility to suggest that in this items the differences in perception of digital forensic between gender groups can be statistically significant if sample size will be increased. But for this, the future investigations are needed.

5.3.2Age

The results of the Chi-square test for differences in Perception of the digital forensic by age groups are displayed in Table 5.31.

Table 5.31: Chi-square test results for differences in perception of the digital forensic by age.

Sub-hypotheses	Statements	Pearson Chi-Square Value	df	Asymptotic Significance (2-sided)
$H2_1$	Digital forensics is mainly concerned about cybercrimes	10.351	8	0.241
$H2_2$	The organization has clear procedures to handle all aspects of digital investigation	6.087	8	0.637
$H2_3$	**IT department is controlling digital forensics operations**	**20.176**	**8**	**0.01**
$H2_4$	Delivering and acquiring information regarding digital investigation are very organized	12.195	8	0.143
$H2_5$	Each digital forensics case has its own plan of operations and processes	9.152	8	0.33
$H2_6$	**The organization has the ability to examine any digital device regardless of its complexity**	**22.483**	**8**	**0.004**
$H2_7$	The organization has clear guidelines about storing and transferring digital evidences	9.146	8	0.33
$H2_8$	**Digital investigators in the organization are well trained and they have all necessary skills to perform any operation in digital forensics**	**15.964**	**8**	**0.043**
$H2_9$	**The organization needs to increase the number of digital investigators**	**21.95**	**8**	**0.005**

$H2_{10}$	Most types of criminal investigations in the organization use digital forensics	13.89	8	0.085
$H2_{11}$	Achievements of digital forensics team are well-known throughout the organization	14.289	8	0.075
$H2_{12}$	The organization needs to acquire more technologies and tools for digital forensics	12.451	8	0.132
$H2_{13}$	The organization has the ability to develop new digital forensics tools that can be used by other organizations	7.158	8	0.52
$H2_{14}$	The organization depends on digital forensics teams of third parties to help with digital investigations	12.167	8	0.144
$H2_{15}$	Digital forensics team has influence on drawing the general policy and strategy of the organization	13.574	8	0.094
$H2_{16}$	The organization helps other organizations in term of digital forensics	9.256	8	0.321
$H2_{17}$	Digital forensics team has full access to all information in any assigned case	11.712	8	165
$H2_{18}$	There are established programs to train and develop human resources for digital forensics positions	6.163	8	0.629
$H2_{19}$	Employees of digital forensics can easily work IT department without additional training and vice versa	15.021	8	0.059
$H2_{20}$	The organization conducts seminars to familiarize stakeholders with operations of digital forensics in the organization	11.739	8	0.163

Hypothesis $H1_0$: There are no differences in the perceptions of the digital forensic by age.

Hypothesis $H1_{alt}$: There are differences in the perceptions of the digital forensic by age.

Table 5.31 indicates that there are differences between age groups for some items (they are marked in the table) as correspondent p-values are less than 0.05. Hence,, investigate these items more detailed.

Table 5.32: Contingency table for Hypothesis 2.

Age group	$H2_3$: IT department is controlling digital forensics operations					Total
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	
26-34	2.0%	0%	46.9%	1.0%	50.0%	100.0%
35-43	6.3%	12.7%	38.1%	3.2%	39.7%	100.0%
44-52	8.3%	6.3%	37.5%	6.3%	41.7%	100.0%
Total	4.8%	5.3%	42.1%	2.9%	45.0%	100.0%
Age group	$H2_6$:The organization has the ability to examine any digital device regardless of its complexity					Total
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	
26-34	11.2%	62.2%	14.3%	4.1%	8.2%	100.0%
35-43	7.9%	57.1%	14.3%	3.2%	17.5%	100.0%
44-52	12.5%	31.3%	14.6%	16.7%	25.0%	100.0%
Total	10.5%	53.6%	14.4%	6.7%	14.8%	100.0%
Age group	$H2_8$: Digital investigators in the organization are well trained and they have all necessary skills to perform any operation in digital forensics					Total
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	
26-34	6.1%	69.4%	11.2%	4.1%	9.2%	100.0%
35-43	3.2%	47.6%	15.9%	6.3%	27.0%	100.0%
44-52	6.3%	52.1%	22.9%	6.3%	12.5%	100.0%
Total	5.3%	58.9%	15.3%	5.3%	15.3%	100.0%
Age group	$H2_9$: The organization needs to increase the number of digital investigators					Total
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	

26-34	1.0%	3.1%	36.7%	54.1%	5.1%	100.0%
35-43	3.2%	11.1%	39.7%	34.9%	11.1%	100.0%
44-52	10.4%	12.5%	18.8%	47.9%	10.4%	100.0%
Total	3.8%	7.7%	33.5%	46.9%	8.1%	100.0%

Table 5.32 indicates that respondents from the younger group more often strongly disagree and less agree that IT department is controlling digital forensics operation in comparison to other two age groups. This difference is significant as Chi-Square statistic has p-value 0.01 <0.05 (See Table 6.31). Thus, the Hypothesis $H2_{3\mathit{0}}$ is rejected and Hypothesis $H2_{3alt}$ is accepted.

The respondents from an older group less often disagree that organization has the ability to examine any digital device regardless of its complexity in comparison to other two age groups. This difference is significant as correspondent Chi-Square statistic has p-value 0.004 <0.05 (See Table 6.31). Thus, the Hypothesis $H2_{60}$ is rejected and Hypothesis $H2_{6alt}$ is accepted.

The group 24-36 years more disagrees that digital investigators in the organization are well trained and they have all necessary skills to perform any operation in digital forensics in comparison to other two age groups. This difference is significant as correspondent Chi-Square statistic has p-value 0.043 <0.05 (See Table 5.31). Thus, the Hypothesis $H2_{80}$ is rejected and Hypothesis $H2_{8alt}$ is accepted.

The group of the respondents 24-36 years more often strongly agree and less disagree and strongly disagree that organization needs to increase the number of digital investigators in comparison to other two age groups. This difference is significant as correspondent Chi-Square statistic has p-value $0.005 < 0.05$ (See Table 5.31). Thus, the Hypothesis $H2_{90}$ is rejected and Hypothesis $H2_{9alt}$ is accepted.

Other null sub-hypotheses from hypothesis H2 are accepted. In general, the Hypothesis $H2_0$ is rejected and Hypothesis $H2_{alt}$ is accepted. There is an association between perception of the digital forensic and age. The younger respondents are more not satisfied with the current usage of the digital forensic in the organization and give more importance of the usage of the digital forensic in future activity of the organization.

5.3.3Education

The results of the Chi-square test for differences in Perception of the digital forensic by education are described in Table 5.33.

Table 5.33: Chi-square test results for differences in perception of the digital forensic by education.

Sub-hypo-theses	Statements	Pearson Chi-Square Value	df	Asymptotic Significance (2-sided)
H3$_1$	**Digital forensics is mainly concerned about cybercrimes**	**30.957**	**12**	**0.002**
H3$_2$	**The organization has clear procedures to handle all aspects of digital investigation**	**36.012**	**12**	**0.000**
H3$_3$	IT department is controlling digital forensics operations	15.435	12	0.219
H3$_4$	Delivering and acquiring information regarding digital investigation are very organized	**21.356**	12	**0.045**
H3$_5$	**Each digital forensics case has its own plan of operations and processes**	**22.506**	**12**	**0.032**
H3$_6$	**The organization has the ability to examine any digital device regardless of its complexity**	**23.277**	**12**	**0.025**
H3$_7$	**The organization has clear guidelines about storing and transferring digital evidence**	**23.836**	**12**	**0.021**
H3$_8$	**Digital investigators in the organization are well trained and they have all necessary skills to perform any operation in digital forensics**	**32.828**	**12**	**0.001**
H3$_9$	**The organization needs to increase the number of digital investigators**	**31.063**	**12**	**0.002**
H3$_{10}$	**Most types of criminal investigations in the organization use digital forensics**	**27.281**	**12**	**0.007**
H3$_{11}$	**Achievements of digital forensics team are well-known throughout the organization**	**39.874**	**12**	**0.000**
H3$_{12}$	**The organization needs to acquire more technologies and tools for digital forensics**	**24.06**	**12**	**0.020**
H3$_{13}$	**The organization has the ability to develop new digital forensics tools that can be used by other organizations**	**21.893**	**12**	**0.039**

H3$_{14}$	**The organization depends on digital forensics teams of third parties to help with digital investigations**	**30.044**	**12**	**0.003**
H3$_{15}$	Digital forensics team has influence on drawing the general policy and strategy of the organization	20.856	12	0.053
H3$_{16}$	The organization helps other organizations in term of digital forensics	20.922	12	0.052
H3$_{17}$	**Digital forensics team has full access to all information in any assigned case**	**25.083**	**12**	**0.014**
H3$_{18}$	**There are established programs to train and develop human resources for digital forensics positions**	**23.548**	**12**	**0.023**
H3$_{19}$	**Employees of digital forensics can easily work IT department without additional training and vice versa**	**29.042**	**12**	**0.004**
H3$_{20}$	**The organization conducts seminars to familiarize stakeholders with operations of digital forensics in the organization**	**23.751**	**12**	**0.022**

Hypothesis H3$_0$: There are no differences in the perceptions of the digital forensic by education level.

Hypothesis H3$_{alt}$: There are differences in the perceptions of the digital forensic by education level.

As Table 5.33 indicates there are statistically significant differences in perception of the digital forensic by education for 16 items with 20. The null sub-hypotheses H3$_3$, H3$_4$, H3$_{15}$, and H3$_{16}$ are accepted. In other cases, the null sub-hypotheses are rejected and the alternative hypotheses are accepted.

Table 5.34 shows the contingency tables for statistically significant cases of Hypothesis 3.

Table 5.34: Contingency tables for statistically significant cases of Hypothesis 3.

	H3$_1$: Digital forensics is mainly concerned about cybercrimes					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
Bachelor	7.0%	2.6%	38.6%	5.3%	46.5%	100.0%
Master			34.0%		66.0%	100.0%
PhD			40.0%		60.0%	100.0%
Secondary	18.8%	12.5%	28.1%		40.6%	100.0%
Total	6.7%	3.3%	35.9%	2.9%	51.2%	100.0%
	H3$_2$: The organization has clear procedures to handle all aspects of digital investigation					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
Bachelor	4.4%	46.5%	28.9%	7.0%	13.2%	100.0%
Master		75.5%	1.9%		22.6%	100.0%
PhD		90.0%			10.0%	100.0%
Secondary		46.9%	31.3%	9.4%	12.5%	100.0%
Total	2.4%	56.0%	21.1%	5.3%	15.3%	100.0%
	H3$_5$: Each digital forensics case has its own plan of operations and processes					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
Bachelor	46.5%	4.4%	32.5%	6.1%	10.5%	100.0%
Master	64.2%		35.8%			100.0%
PhD	80.0%		20.0%			100.0%
Secondary	37.5%	9.4%	37.5%	9.4%	6.3%	100.0%
Total	51.2%	3.8%	33.5%	4.8%	6.7%	100.0%
	H3$_6$: The organization has the ability to examine any digital device regardless of its complexity					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
Bachelor	12.3%	50.0%	17.5%	8.8%	11.4%	100.0%
Master	3.8%	60.4%	11.3%		24.5%	100.0%
PhD		90.0%			10.0%	100.0%

Secondary	18.8%	43.8%	12.5%	12.5%	12.5%	100.0%
Total	10.5%	53.6%	14.4%	6.7%	14.8%	100.0%
	H3$_{7}$: The organization has clear guidelines about storing and transferring digital evidence					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
Bachelor	5.3%	47.4%	24.6%	6.1%	16.7%	100.0%
Master	1.9%	66.0%	5.7%		26.4%	100.0%
PhD		70.0%			30.0%	100.0%
Secondary	12.5%	43.8%	15.6%	6.3%	21.9%	100.0%
Total	5.3%	52.6%	17.2%	4.3%	20.6%	100.0%
	H3$_{8}$: Digital investigators in the organization are well trained and they have all necessary skills to perform any operation in digital forensics					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
Bachelor	8.8%	53.5%	19.3%	7.0%	11.4%	100.0%
Master		73.6%		1.9%	24.5%	100.0%
PhD		90.0%	10.0%			100.0%
Secondary	3.1%	43.8%	28.1%	6.3%	18.8%	100.0%
Total	5.3%	58.9%	15.3%	5.3%	15.3%	100.0%
	H3$_{9}$: The organization needs to increase the number of digital investigators					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
Bachelor	6.1%	7.9%	30.7%	43.0%	12.3%	100.0%
Master			39.6%	60.4%		100.0%
PhD			30.0%	70.0%		100.0%
Secondary	3.1%	21.9%	34.4%	31.3%	9.4%	100.0%
Total	3.8%	7.7%	33.5%	46.9%	8.1%	100.0%
	H3$_{10}$: Most types of criminal investigations in the organization use digital forensics					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
Bachelor	45.6%	12.3%	26.3%	1.8%	14.0%	100.0%
Master	69.8%		30.2%			100.0%

PhD	50.0%		50.0%			100.0%
Secondary	34.4%	12.5%	40.6%	3.1%	9.4%	100.0%
Total	50.2%	8.6%	30.6%	1.4%	9.1%	100.0%
	H3$_{11}$: Achievements of digital forensics team are well-known throughout the organization					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
Bachelor	6.1%	53.5%	25.4%	5.3%	9.6%	100.0%
Master	1.9%	69.8%	3.8%		24.5%	100.0%
PhD		60.0%			40.0%	100.0%
Secondary	12.5%	37.5%	12.5%	15.6%	21.9%	100.0%
Total	5.7%	55.5%	16.7%	5.3%	16.7%	100.0%
	H3$_{12}$: The organization needs to acquire more technologies and tools for digital forensics					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
Bachelor	7.9%	8.8%	35.1%	40.4%	7.9%	100.0%
Master			39.6%	60.4%		100.0%
PhD			30.0%	70.0%		100.0%
Secondary	3.1%	12.5%	46.9%	31.3%	6.3%	100.0%
Total	4.8%	6.7%	37.8%	45.5%	5.3%	100.0%
	H3$_{13}$: The organization has the ability to develop new digital forensics tools that can be used by other organizations					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
Bachelor	6.1%	9.6%	35.1%	40.4%	8.8%	100.0%
Master			41.5%	58.5%		100.0%
PhD			30.0%	70.0%		100.0%
Secondary	9.4%	9.4%	37.5%	34.4%	9.4%	100.0%
Total	4.8%	6.7%	36.8%	45.5%	6.2%	100.0%
	H3$_{14}$: The organization depends on digital forensics teams of third parties to help with digital investigations					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
Bachelor	39.5%	7.0%	37.7%	5.3%	10.5%	100.0%

Master	67.9%		32.1%			100.0%
PhD	70.0%		30.0%			100.0%
Secondary	59.4%	3.1%	12.5%	6.3%	18.8%	100.0%
Total	51.2%	4.3%	32.1%	3.8%	8.6%	100.0%
	H3$_{17}$: Digital forensics team has full access to all information in any assigned case					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
Bachelor	7.9%	49.1%	21.9%	11.4%	9.6%	100.0%
Master	9.4%	58.5%	9.4%		22.6%	100.0%
PhD		60.0%		10.0%	30.0%	100.0%
Secondary	9.4%	31.3%	34.4%	6.3%	18.8%	100.0%
Total	8.1%	49.3%	19.6%	7.7%	15.3%	100.0%
	H3$_{18}$: There are established programs to train and develop human resources for digital forensics positions					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
Bachelor	13.2%	48.2%	21.9%	3.5%	13.2%	100.0%
Master	1.9%	62.3%	7.5%	1.9%	26.4%	100.0%
PhD		60.0%	10.0%		30.0%	100.0%
Secondary		53.1%	28.1%		18.8%	100.0%
Total	7.7%	53.1%	18.7%	2.4%	18.2%	100.0%
	H3$_{19}$: Employees of digital forensics can easily work IT department without additional training and vice versa					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
Bachelor	3.5%	52.6%	27.2%	7.0%	9.6%	100.0%
Master	3.8%	79.2%	3.8%		13.2%	100.0%
PhD		50.0%	20.0%		30.0%	100.0%
Secondary	6.3%	34.4%	34.4%	9.4%	15.6%	100.0%
Total	3.8%	56.5%	22.0%	5.3%	12.4%	100.0%
	H3$_{20}$: The organization conducts seminars to familiarize stakeholders with operations of digital forensics in the organization					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total

Bachelor	42.1%	11.4%	35.1%	1.8%	9.6%	100.0%
Master	66.0%		34.0%			100.0%
PhD	80.0%		20.0%			100.0%
Secondary	37.5%	6.3%	40.6%	3.1%	12.5%	100.0%
Total	49.3%	7.2%	34.9%	1.4%	7.2%	100.0%

Table 5.34 displays statistically significant differences in perception of the digital forensic are in differences between respondents with Master and Ph.D. degrees and other groups. Thus, respondents with Master and Ph.D. degrees in comparison with other groups:

- Disagree that organization has clear procedures to handle all aspects of digital investigation ($H3_{2alt}$ is accepted).
- Agree that each digital forensics case has its own plan of operations and processes ($H3_{5alt}$ is accepted).
- Disagree that organization has the ability to examine any digital device regardless of its complexity ($H3_{6alt}$ is accepted).
- Disagree that organization has clear guidelines about storing and transferring digital evidence and that digital investigators in the organization are well trained and they have all necessary skills to perform any operation in digital forensics ($H3_{7alt}$ and $H3_{8alt}$ are accepted).
- Agree that the organization needs to increase the number of digital investigators ($H3_{9alt}$ is accepted).
- Mildly disagree that most types of criminal investigations in the organization use digital forensics ($H3_{10alt}$ is accepted).
- Agree that achievements of digital forensics team are well-known throughout the organization ($H3_{11alt}$ is accepted).

- Agree that organization needs to acquire more technologies and tools for digital forensics ($H3_{12alt}$ is accepted).
- Agree that organization has the ability to develop new digital forensics tools that can be used by other organizations ($H3_{13alt}$ is accepted).
- Agree that organization depends on digital forensics teams of third parties to help with digital investigations ($H3_{14alt}$ is accepted).
- Disagree that digital forensics team has full access to all information in any assigned case ($H3_{17alt}$ is accepted).
- Disagree that there are established programs to train and develop human resources for digital forensics positions and that employees of digital forensics can easily work IT department without additional training and vice versa ($H3_{18alt}$ is accepted).
- Agree that organization conducts seminars to familiarize stakeholders with operations of digital forensics in the organization ($H3_{19alt}$ is accepted).

Consider above, in general, the hypothesis $H3_0$ is rejected and hypothesis $H3_{3alt}$ is accepted. There is an association between perception of the digital forensic and age. The respondents with higher education level understand the digital forensic more widely than others; these respondents are not satisfied with the current usage of the digital forensic in the organization and give more importance of the usage of the digital forensic in future.

5.3.4 Rank

The results of the Chi-square test for differences in perception of the digital forensic by rank are presented in Table 6.35.

Table 5.35: Chi-square test results for differences in perception of the digital forensic by rank.

Sub-hypo-theses	**Statements**	**Pearson Chi-Square Value**	**df**	**Asymptotic Significance (2-sided)**
$H4_1$	**Digital forensics is mainly concerned about cybercrimes**	**45.805**	**20**	**0.002**
$H4_2$	**The organization has clear procedures to handle all aspects of digital investigation**	**31.841**	**20**	**0.045**
$H4_3$	**IT department is controlling digital forensics operations**	**36.268**	**20**	**0.014**
$H4_4$	**Delivering and acquiring information regarding digital investigation are very organized**	**44.837**	**20**	**0.001**
$H4_5$	**Each digital forensics case has its own plan of operations and processes**	**42.564**	**20**	**0.002**
$H4_6$	**The organization has the ability to examine any digital device regardless of its complexity**	**45.724**	**20**	**0.001**
$H4_7$	**The organization has clear guidelines about storing and transferring digital evidence**	**40.127**	**20**	**0.005**
$H4_8$	**Digital investigators in the organization are well trained and they have all necessary skills to perform any operation in digital forensics**	**47.358**	**20**	**0.001**
$H4_9$	**The organization needs to increase the number of digital investigators**	**42.193**	**20**	**0.003**
$H4_{10}$	**Most types of criminal investigations in the organization use digital forensics**	**53.697**	**20**	**0.000**
$H4_{11}$	**Achievements of digital forensics team are well-known throughout the organization**	**32.997**	**20**	**0.034**
$H4_{12}$	**The organization needs to acquire more technologies and tools for digital forensics**	**44.681**	**20**	**0.001**
$H4_{13}$	**The organization has the ability to develop new digital forensics tools that can be used by other organizations**	**47.955**	**20**	**0.000**
$H4_{14}$	**The organization depends on digital forensics teams of third parties to help with digital investigations**	**38.297**	**20**	**0.008**
$H4_{15}$	**Digital forensics team has influence on drawing the general policy and strategy of the organization**	**42.483**	**20**	**0.002**

$H4_{16}$	The organization helps other organizations in term of digital forensics	26.141	20	0.161
$H4_{17}$	**Digital forensics team has full access to all information in any assigned case**	**42.203**	**20**	**0.003**
$H4_{18}$	**There are established programs to train and develop human resources for digital forensics positions**	**31.542**	**20**	**0.048**
$H4_{19}$	**Employees of digital forensics can easily work IT department without additional training and vice versa**	**32.241**	**20**	**0.041**
$H4_{20}$	**The organization conducts seminars to familiarize stakeholders with operations of digital forensics in the organization**	**48.437**	**20**	**0.000**

Hypothesis $H4_0$: There are no differences in the perceptions of the digital forensic by Rank.

Hypothesis $H4_{alt}$: There are differences in perceptions of the digital forensic by Rank.

As Table 5.35 shows there are statistically significant differences in perception of the digital forensic by education for 19 items with 20. Hence, the null sub-hypothesis $H4_{16}$ is accepted and other null sub-hypotheses are rejected and accordingly alternative sub-hypotheses are accepted. Table 5.36 displays the contingency tables for statistically significant items of Hypothesis 4.

Table 5.36: Contingency tables for statistically significant cases of hypothesis 4.

Rank	$H4_1$: Digital forensics is mainly concerned about cybercrimes					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
1st. Lieutenant			41.9%		58.1%	100.0%
1st. Warrant Officer	37.5%	12.5%	25.0%		25.0%	100.0%
Captain			47.2%		52.8%	100.0%
Lieutenant	16.7%	11.1%	27.8%	5.6%	38.9%	100.0%
Lt. Colonel	20.0%	10.0%	10.0%		60.0%	100.0%
Major	6.4%	3.2%	34.0%	5.3%	51.1%	100.0%
Total	6.7%	3.3%	35.9%	2.9%	51.2%	100.0%
	$H4_2$: The organization has clear procedures to handle all aspects of digital investigation					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
1st. Lieutenant	2.3%	74.4%	14.0%	2.3%	7.0%	100.0%
1st. Warrant Officer		37.5%	25.0%	12.5%	25.0%	100.0%
Captain		66.7%	11.1%		22.2%	100.0%
Lieutenant		27.8%	44.4%	16.7%	11.1%	100.0%
Lt. Colonel		50.0%	40.0%		10.0%	100.0%
Major	4.3%	51.1%	21.3%	6.4%	17.0%	100.0%
Total	2.4%	56.0%	21.1%	5.3%	15.3%	100.0%
	$H4_3$: IT department is controlling digital forensics operations					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
1st. Lieutenant			46.5%		53.5%	100.0%

1st. Warrant Officer			75.0%		25.0%	100.0%
Captain			33.3%		66.7%	100.0%
Lieutenant	11.1%	11.1%	33.3%	5.6%	38.9%	100.0%
Lt. Colonel	20.0%		50.0%		30.0%	100.0%
Major	6.4%	9.6%	41.5%	5.3%	37.2%	100.0%
Total	4.8%	5.3%	42.1%	2.9%	45.0%	100.0%

	H4$_4$: Delivering and acquiring information regarding digital investigation are very organized					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
1st. Lieutenant	9.3%	74.4%	7.0%	4.7%	4.7%	100.0%
1st. Warrant Officer	12.5%	12.5%	50.0%		25.0%	100.0%
Captain	5.6%	80.6%		2.8%	11.1%	100.0%
Lieutenant	5.6%	33.3%	22.2%	11.1%	27.8%	100.0%
Lt. Colonel		50.0%	20.0%		30.0%	100.0%
Major	10.6%	44.7%	14.9%	3.2%	26.6%	100.0%
Total	8.6%	55.0%	12.9%	3.8%	19.6%	100.0%

	H4$_5$: Each digital forensics case has its own plan of operations and processes					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
1st. Lieutenant	60.5%		39.5%			100.0%
1st. Warrant Officer	50.0%	25.0%	12.5%		12.5%	100.0%
Captain	72.2%		27.8%			100.0%
Lieutenant	22.2%	5.6%	50.0%	11.1%	11.1%	100.0%
Lt. Colonel	50.0%		20.0%	10.0%	20.0%	100.0%
Major	44.7%	5.3%	33.0%	7.4%	9.6%	100.0%

Total	51.2%	3.8%	33.5%	4.8%	6.7%	100.0%
	$H4_6$: The organization has the ability to examine any digital device regardless of its complexity					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
1st. Lieutenant	9.3%	76.7%	11.6%		2.3%	100.0%
1st. Warrant Officer	50.0%	25.0%	25.0%			100.0%
Captain	8.3%	72.2%	8.3%	5.6%	5.6%	100.0%
Lieutenant	5.6%	50.0%	11.1%	11.1%	22.2%	100.0%
Lt. Colonel	10.0%	40.0%	10.0%	10.0%	30.0%	100.0%
Major	9.6%	40.4%	18.1%	9.6%	22.3%	100.0%
Total	10.5%	53.6%	14.4%	6.7%	14.8%	100.0%
	$H4_7$: The organization has clear guidelines about storing and transferring digital evidence					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
1st. Lieutenant	2.3%	74.4%	14.0%		9.3%	100.0%
1st. Warrant Officer	25.0%	37.5%	25.0%	12.5%		100.0%
Captain	8.3%	61.1%	8.3%	2.8%	19.4%	100.0%
Lieutenant	5.6%	27.8%	33.3%	5.6%	27.8%	100.0%
Lt. Colonel	20.0%	30.0%		10.0%	40.0%	100.0%
Major	2.1%	47.9%	20.2%	5.3%	24.5%	100.0%
Total	5.3%	52.6%	17.2%	4.3%	20.6%	100.0%
	$H4_8$: Digital investigators in the organization are well trained and they have all necessary skills to perform any operation in digital forensics					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
1st. Lieutenant	2.3%	86.0%	2.3%	2.3%	7.0%	100.0%

1st. Warrant Officer		12.5%	50.0%		37.5%	100.0%
Captain	5.6%	75.0%	5.6%	2.8%	11.1%	100.0%
Lieutenant	11.1%	55.6%	22.2%	11.1%		100.0%
Lt. Colonel		60.0%	30.0%		10.0%	100.0%
Major	6.4%	44.7%	19.1%	7.4%	22.3%	100.0%
Total	5.3%	58.9%	15.3%	5.3%	15.3%	100.0%
	$H4_{9}$: The organization needs to increase the number of digital investigators					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
1st. Lieutenant			34.9%	65.1%		100.0%
1st. Warrant Officer		12.5%	37.5%	37.5%	12.5%	100.0%
Captain			50.0%	50.0%		100.0%
Lieutenant	5.6%	16.7%	27.8%	33.3%	16.7%	100.0%
Lt. Colonel	20.0%	20.0%	20.0%	30.0%	10.0%	100.0%
Major	5.3%	10.6%	28.7%	42.6%	12.8%	100.0%
Total	3.8%	7.7%	33.5%	46.9%	8.1%	100.0%
	$H4_{10}$: Most types of criminal investigations in the organization use digital forensics					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
1st. Lieutenant	67.4%		32.6%			100.0%
1st. Warrant Officer	25.0%	12.5%	50.0%	12.5%		100.0%
Captain	77.8%		22.2%			100.0%
Lieutenant	33.3%	22.2%	27.8%		16.7%	100.0%
Lt. Colonel	30.0%	20.0%	20.0%		30.0%	100.0%
Major	39.4%	11.7%	33.0%	2.1%	13.8%	100.0%

Total	50.2%	8.6%	30.6%	1.4%	9.1%	100.0%
	H4$_{11}$: Achievements of digital forensics team are well-known throughout the organization					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
1st. Lieutenant	4.7%	79.1%	4.7%	2.3%	9.3%	100.0%
1st. Warrant Officer		25.0%	25.0%	12.5%	37.5%	100.0%
Captain	8.3%	69.4%	11.1%	2.8%	8.3%	100.0%
Lieutenant		44.4%	22.2%	5.6%	27.8%	100.0%
Lt. Colonel	20.0%	30.0%	20.0%		30.0%	100.0%
Major	5.3%	46.8%	22.3%	7.4%	18.1%	100.0%
Total	5.7%	55.5%	16.7%	5.3%	16.7%	100.0%
	H4$_{12}$: The organization needs to acquire more technologies and tools for digital forensics					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
1st. Lieutenant			44.2%	55.8%		100.0%
1st. Warrant Officer			62.5%	12.5%	25.0%	100.0%
Captain			44.4%	55.6%		100.0%
Lieutenant	5.6%	11.1%	33.3%	50.0%		100.0%
Lt. Colonel		10.0%	20.0%	70.0%		100.0%
Major	9.6%	11.7%	33.0%	36.2%	9.6%	100.0%
Total	4.8%	6.7%	37.8%	45.5%	5.3%	100.0%
	H4$_{13}$: The organization has the ability to develop new digital forensics tools that can be used by other organizations					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
1st. Lieutenant			46.5%	53.5%		100.0%

1st. Warrant Officer	25.0%	12.5%	25.0%	25.0%	12.5%	100.0%
Captain			33.3%	66.7%		100.0%
Lieutenant	11.1%	5.6%	38.9%	27.8%	16.7%	100.0%
Lt. Colonel		30.0%	40.0%	30.0%		100.0%
Major	6.4%	9.6%	34.0%	40.4%	9.6%	100.0%
Total	4.8%	6.7%	36.8%	45.5%	6.2%	100.0%
	$H4_{14}$: The organization depends on digital forensics teams of third parties to help with digital investigations					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
1st. Lieutenant	58.1%		41.9%			100.0%
1st. Warrant Officer	62.5%		12.5%		25.0%	100.0%
Captain	63.9%		36.1%			100.0%
Lieutenant	44.4%	5.6%	27.8%		22.2%	100.0%
Lt. Colonel	30.0%		50.0%	10.0%	10.0%	100.0%
Major	45.7%	8.5%	26.6%	7.4%	11.7%	100.0%
Total	51.2%	4.3%	32.1%	3.8%	8.6%	100.0%
	$H4_{15}$: Digital forensics team has influence on drawing the general policy and strategy of the organization					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
1st. Lieutenant			25.6%		74.4%	100.0%
1st. Warrant Officer		25.0%	25.0%	12.5%	37.5%	100.0%
Captain			47.2%		52.8%	100.0%
Lieutenant			38.9%	16.7%	44.4%	100.0%
Lt. Colonel	10.0%		30.0%		60.0%	100.0%
Major	5.3%	6.4%	39.4%	6.4%	42.6%	100.0%

Total	2.9%	3.8%	36.8%	4.8%	51.7%	100.0%
	H4$_{17}$: Digital forensics team has full access to all information in any assigned case					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
1st. Lieutenant	14.0%	62.8%	9.3%	4.7%	9.3%	100.0%
1st. Warrant Officer		25.0%	25.0%		50.0%	100.0%
Captain	8.3%	75.0%	2.8%	8.3%	5.6%	100.0%
Lieutenant	5.6%	33.3%	44.4%	5.6%	11.1%	100.0%
Lt. Colonel		40.0%	20.0%	10.0%	30.0%	100.0%
Major	7.4%	39.4%	25.5%	9.6%	18.1%	100.0%
Total	8.1%	49.3%	19.6%	7.7%	15.3%	100.0%
	H4$_{18}$: resources for digital forensics positions					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
1st. Lieutenant	4.7%	72.1%	14.0%	2.3%	7.0%	100.0%
1st. Warrant Officer		87.5%			12.5%	100.0%
Captain	11.1%	63.9%	11.1%	2.8%	11.1%	100.0%
Lieutenant	5.6%	22.2%	33.3%		38.9%	100.0%
Lt. Colonel	20.0%	40.0%	10.0%		30.0%	100.0%
Major	7.4%	44.7%	23.4%	3.2%	21.3%	100.0%
	7.7%	53.1%	18.7%	2.4%	18.2%	100.0%
	H4$_{19}$: Employees of digital forensics can easily work IT department without additional training and vice versa					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
1st. Lieutenant	4.7%	74.4%	11.6%	2.3%	7.0%	100.0%

1st. Warrant Officer		25.0%	50.0%	12.5%	12.5%	100.0%
Captain	5.6%	69.4%	11.1%	8.3%	5.6%	100.0%
Lieutenant		38.9%	44.4%		16.7%	100.0%
Lt. Colonel		80.0%			20.0%	100.0%
Major	4.3%	46.8%	26.6%	6.4%	16.0%	100.0%
Total	3.8%	56.5%	22.0%	5.3%	12.4%	100.0%

	H4$_{20}$: The organization conducts seminars to familiarize stakeholders with operations of digital forensics in the organization					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
1st. Lieutenant	65.1%		34.9%			100.0%
1st. Warrant Officer	12.5%		62.5%	12.5%	12.5%	100.0%
Captain	58.3%		41.7%			100.0%
Lieutenant	27.8%	22.2%	22.2%	5.6%	22.2%	100.0%
Lt. Colonel	50.0%		40.0%		10.0%	100.0%
Major	45.7%	11.7%	31.9%	1.1%	9.6%	100.0%
Total	49.3%	7.2%	34.9%	1.4%	7.2%	100.0%

We will consider each item because the single pattern in differences is absent in this case.

1. Digital forensics is mainly concerned about cybercrimes.

The main differences are that groups with ranks 1st. Lieutenant and Captain are divided only “neutral” and “strongly disagree” whereas other groups noted other estimation. Also, a group with rank “1st. Warrant Officer” less strongly disagree than other groups (H4$_{1alt}$ accepted).

2. The organization has clear procedures to handle all aspects of the digital investigation.

Groups with ranks 1st. Lieutenant and Captain more disagree than other groups and groups with ranks 1st. Warrant Officer and Captain are more strongly disagree than other ($H4_{2alt}$ accepted).

3. IT department is controlling digital forensics operations

The group with rank 1st. Warrant Officer is more neutral than other groups. The group with rank Lt. Colonel agree more than other groups whereas groups with ranks Captain and 1st. Lieutenant strongly disagree more than groups with other ranks ($H4_{3alt}$ accepted).

4. Delivering and acquiring information regarding digital investigation are very organized.

The groups with ranks Captain and 1st. Lieutenant are in more disagree and group with rank 1st. Warrant Officer is neutral more than other ($H4_{4alt}$ accepted).

5. Each digital forensics case has its own plan of operations and processes

The respondents with rank Captain agree more than other ($H4_{5alt}$ accepted).

6. The organization has the ability to examine any digital device regardless of its complexity.

The respondents with rank St. Warrant Officer agree while the respondents with rank Captain and 1st. Lieutenant disagree more than respondents with other ranks ($H4_{6alt}$ accepted).

7. The organization has clear guidelines about storing and transferring digital evidence.

The respondents with rank Captain and 1st. Lieutenant more often disagree and respondents with rank Lt. Colonels more often strongly disagree than respondents with other ranks ($H4_{7alt}$ accepted).

8. Digital investigators in the organization are well trained and they have all necessary skills to perform any operation in digital forensics.

The respondents with rank 1st. Warrant Officer less disagree that respondents with other ranks ($H4_{8alt}$ accepted).

9. The organization needs to increase the number of digital investigators

The respondents with rank Captain and 1st. Lieutenant more strongly agree with that than other ($H4_{9alt}$ accepted).

10. Most types of criminal investigations in the organization use digital forensics

The respondents with rank Captain and 1st. Lieutenant more agree with this statement and respondents with rank 1st. Warrant Officer are more neutral that respondents with other ranks ($H4_{10alt}$ accepted).

11. Achievements of digital forensics team are well-known throughout the organization.

The respondents with rank Captain and 1st. Lieutenant more disagree with that than respondents with other ranks ($H4_{11alt}$ accepted).

12. The organization needs to acquire more technologies and tools for digital forensics.

The respondents with rank 1st. Warrant Officer less strongly agree with this statement whereas the respondents with rank Lt. Colonel are more strongly agree than other ($H4_{12alt}$ accepted).

13. The organization has the ability to develop new digital forensics tools that can be used by other organizations

The respondents with rank Captain and 1st. Lieutenant more strongly agree while respondents with rank Lt. Colonel are more disagree with this statement than other respondents ($H4_{13alt}$ accepted).

14**.** The organization depends on digital forensics teams of third parties to help with digital investigations

The groups with ranks 1st. Lieutenant, 1st. Warrant Officer and Captain more agree than other respondents ($H4_{14alt}$ accepted).

15. Digital forensics team has influence on drawing the general policy and strategy of the organization

The respondents with ranks 1st. Lieutenant and Lt. Colonel more often strongly disagree with this statements than respondents from other groups ($H4_{15alt}$ accepted).

17. Digital forensics team has full access to all information in any assigned case.

The groups with ranks 1st. Lieutenant and Captain more disagree with this statement and respondents which have a rank 1st. Warrant Officer are more strongly disagree than other respondents ($H4_{17alt}$ accepted).

18. There are established programs to train and develop human resources for digital forensics positions

The groups with ranks 1st. Lieutenant, 1st. Warrant Officer and Captain more disagree than other respondents ($H4_{18alt}$ accepted).

19. Employees of digital forensics can easily work IT department without additional training and vice versa

The respondents with ranks 1st. Lieutenant, Captain, and Lt. Colonel more often disagree than respondents with other ranks ($H4_{19alt}$ accepted).

20. The organization conducts seminars to familiarize stakeholders with operations of digital forensics in the organization

The respondents which have the ranks 1st. Lieutenant, Captain, and Lt. Colonel more often agree with this statement than respondents with other ranks ($H4_{20alt}$ accepted).

Hence, considering above, the hypothesis $H4_0$ is rejected and hypothesis H_{4alt} is accepted. But in this case, we cannot distinguish a common pattern of the association between digital forensics perception and Ranks. Perhaps such relationship can be found if sample size will be increased. But for this, the future investigations are needed.

5.3.5 Years in current position

The results of the Chi-square test for differences in perception of the digital forensic by a number of years in current position are presented in Table 5.37.

Table 5.37: Chi-square test results for differences in perception of the digital forensic by number of years in current position.

Sub-hypo-theses	Statements	Pearson Chi-Square Value	df	Asymptotic Significance (2-sided)
$H5_1$	Digital forensics is mainly concerned about cybercrimes	13.507	12	0.333
$H5_2$	The organization has clear procedures to handle all aspects of digital investigation	9.565	12	0.654
$H5_3$	IT department is controlling digital forensics operations	8.148	12	0.773
$H5_4$	Delivering and acquiring information regarding digital investigation are very organized	10.939	12	0.534
$H5_5$	Each digital forensics case has its own plan of operations and processes	10.431	12	0.578

$H5_6$	The organization has the ability to examine any digital device regardless of its complexity	10.631	12	0.561
$H5_7$	The organization has clear guidelines about storing and transferring digital evidence	10691	12	0.556
$H5_8$	Digital investigators in the organization are well trained and they have all necessary skills to perform any operation in digital forensics	8.44	12	0.750
$H5_9$	The organization needs to increase the number of digital investigators	9.555	12	0.655
$H5_{10}$	Most types of criminal investigations in the organization use digital forensics	7.835	12	0.798
$H5_{11}$	Achievements of digital forensics team are well-known throughout the organization	4.59	12	0.970
$H5_{12}$	The organization needs to acquire more technologies and tools for digital forensics	11.941	12	0.450
$H5_{13}$	**The organization has the ability to develop new digital forensics tools that can be used by other organizations**	**22.435**	**12**	**0.033**
$H5_{14}$	The organization depends on digital forensics teams of third parties to help with digital investigations	13.739	12	0.318
$H5_{15}$	Digital forensics team has influence on drawing the general policy and strategy of the organization	7.492	12	0.823
$H5_{16}$	The organization helps other organizations in term of digital forensics	11.89	12	0.455
$H5_{17}$	Digital forensics team has full access to all information in any assigned case	12.918	12	0.375
$H5_{18}$	There are established programs to train and develop human resources for digital forensics positions	12.666	12	0.394
$H5_{19}$	Employees of digital forensics can easily work IT department without additional training and vice versa	15.996	12	0.191
$H5_{20}$	The organization conducts seminars to familiarize stakeholders with operations of digital forensics in the organization	10.715	12	0.553

Table 5.37 displays only one case of the difference in perception of the digital forensics by a number of years in the current position in the organization. Hence, all null sub-hypotheses exclude $H5_{13}$ are accepted. The null sub-hypothesis $H5_{13}$ is rejected and alternative hypothesis $H5_{13alt}$ is accepted. For this case, the contingency table is reported in Table 6.38.

Table 5.38: Contingency tables for statistically significant cases of hypothesis 4.

Years in Current position	$H5_{13}$: The organization has the ability to develop new digital forensics tools that can be used by other organizations					Total
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	
1	1.8%	12.7%	29.1%	52.7%	3.6%	100.0%
2	4.0%	4.0%	44.0%	40.0%	8.0%	100.0%
3		3.6%	38.2%	49.1%	9.1%	100.0%
4	14.3%	6.1%	36.7%	38.8%	4.1%	100.0%
Total	4.8%	6.7%	36.8%	45.5%	6.2%	100.0%

In Table 5.38, the respondents which are four years in a current position more rarely consider that their organization has the ability to develop new digital forensics tools that can be used by other organizations. Hence, the Hypothesis $H5_0$ is rejected and Hypothesis $H5_1$ is accepted. The respondents which are 4 years in current position are more pessimistic about ability of the organization to develop new digital forensics tools that can be used by other organizations.

5.3.6 Number of the years in organization

The results of the Chi-square test for differences in perception of the digital forensic by a number of years in the organization are presented in Table 5.39.

Table 5.39: Chi-square test results for differences in perception of the digital forensic by number of years in organization.

Sub-hypo-theses	Statements	Pearson Chi-Square Value	df	Asymptotic Significance (2-sided)
$H6_1$	Digital forensics is mainly concerned about cybercrimes	4.937	8	0.764
$H6_2$	The organization has clear procedures to handle all aspects of digital investigation	5.225	8	0.733
$H6_3$	**IT department is controlling digital forensics operations**	**15.933**	**8**	**0.043**
$H6_4$	Delivering and acquiring information regarding digital investigation are very organized	8.894	8	0.351
$H6_5$	Each digital forensics case has its own plan of operations and processes	9.288	8	0.319
$H6_6$	**The organization has the ability to examine any digital device regardless of its complexity**	**17.92**	**8**	**0.022**
$H6_7$	The organization has clear guidelines about storing and transferring digital evidence	11.561	8	0.172
$H6_8$	Digital investigators in the organization are well trained and they have all necessary skills to perform any operation in digital forensics	8.484	8	0.388
$H6_9$	**The organization needs to increase the number of digital investigators**	**19.344**	**8**	**0.013**
$H6_{10}$	**Most types of criminal investigations in the organization use digital forensics**	**18.089**	**8**	**0.021**

$H6_{11}$	Achievements of digital forensics team are well-known throughout the organization	11.473	8	0.176
$H6_{12}$	**The organization needs to acquire more technologies and tools for digital forensics**	**15.993**	**8**	**0.042**
$H6_{13}$	The organization has the ability to develop new digital forensics tools that can be used by other organizations	10.189	8	0.252
$H6_{14}$	**The organization depends on digital forensics teams of third parties to help with digital investigations**	**18.84**	**8**	**0.016**
$H6_{15}$	Digital forensics team has influence on drawing the general policy and strategy of the organization	14.408	8	0.072
$H6_{16}$	The organization helps other organizations in term of digital forensics	5.311	8	0.724
$H6_{17}$	Digital forensics team has full access to all information in any assigned case	9.095	8	0.334
$H6_{18}$	There are established programs to train and develop human resources for digital forensics positions	6.162	8	0.629
$H6_{19}$	**Employees of digital forensics can easily work IT department without additional training and vice versa**	**16.149**	**8**	**0.040**
$H6_{20}$	The organization conducts seminars to familiarize stakeholders with operations of digital forensics in the organization	11.243	8	0.188

Table 5.39 indicates seven cases of differences in perception of the digital forensics by a number of years in the organization. Hence, the null hypothesis $H6_1$, $H6_2$, $H6_4$, $H6_5$, $H6_7$, $H6_8$, $H6_{11}$, $H6_{13}$, $H6_{15}$-$H6_{18}$, and $H6_{20}$ are accepted. Other null sub-hypotheses are rejected and accordingly alternative hypotheses are accepted. The contingency tables for these items are described in Table 5.40.

Table 5.40: The contingency tables for hypothesis 6.

Years inorganization	H6$_{3}$: IT department is controlling digital forensics operations					Total
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	
1-10 years	2.2%		43.8%	1.1%	52.8%	100.0%
11-20 years	6.8%	9.5%	43.2%	2.7%	37.8%	100.0%
21-31 years	6.5%	8.7%	37.0%	6.5%	41.3%	100.0%
Total	4.8%	5.3%	42.1%	2.9%	45.0%	100.0%
	H6$_{6}$: The organization has the ability to examine any digital device regardless of its complexity					Total
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	
1-10 years	11.2%	65.2%	13.5%	3.4%	6.7%	100.0%
11-20 years	9.5%	48.6%	17.6%	6.8%	17.6%	100.0%
21-31 years	10.9%	39.1%	10.9%	13.0%	26.1%	100.0%
Total	10.5%	53.6%	14.4%	6.7%	14.8%	100.0%
	H6$_{9}$: The organization needs to increase the number of digital investigators					Total
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	
1-10 years	1.1%	2.2%	38.2%	53.9%	4.5%	100.0%
11-20 years	5.4%	9.5%	36.5%	36.5%	12.2%	100.0%
21-31 years	6.5%	15.2%	19.6%	50.0%	8.7%	100.0%
Total	3.8%	7.7%	33.5%	46.9%	8.1%	100.0%
	H6$_{10}$: Most types of criminal investigations in the organization use digital forensics					Total
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	
1-10 years	64.0%	5.6%	27.0%	1.1%	2.2%	100.0%
11-20 years	43.2%	9.5%	33.8%	1.4%	12.2%	100.0%

21-31 years	34.8%	13.0%	32.6%	2.2%	17.4%	100.0%
Total	50.2%	8.6%	30.6%	1.4%	9.1%	100.0%
	H6$_{12}$: The organization needs to acquire more technologies and tools for digital forensics					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
1-10 years	1.1%	2.2%	43.8%	50.6%	2.2%	100.0%
11-20 years	8.1%	9.5%	35.1%	41.9%	5.4%	100.0%
21-31 years	6.5%	10.9%	30.4%	41.3%	10.9%	100.0%
	4.8%	6.7%	37.8%	45.5%	5.3%	100.0%
	H6$_{14}$: The organization depends on digital forensics teams of third parties to help with digital investigations					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
1-10 years	56.2%	1.1%	38.2%		4.5%	100.0%
11-20 years	51.4%	8.1%	21.6%	6.8%	12.2%	100.0%
21-31 years	41.3%	4.3%	37.0%	6.5%	10.9%	100.0%
Total	51.2%	4.3%	32.1%	3.8%	8.6%	100.0%
	H6$_{19}$: Employees of digital forensics can easily work IT department without additional training and vice versa					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
1-10 years	4.5%	64.0%	20.2%	3.4%	7.9%	100.0%
11-20 years	1.4%	52.7%	23.0%	10.8%	12.2%	100.0%
21-31 years	6.5%	47.8%	23.9%		21.7%	100.0%
Total	3.8%	56.5%	22.0%	5.3%	12.4%	100.0%

In table 5.40, the main pattern is in differences respondents which are 1-10 years in the organization from other groups of the respondents. Thus, the respondents which are 1-10 years in organization in comparing to respondents from other groups:

- More often strongly disagree and more rarely agree that IT department is controlling digital forensics operations ($H6_{3alt}$ is accepted);
- More often disagree and more seldom strongly agree that their organization has the ability to examine any digital device regardless of its complexity ($H6_{6alt}$ is accepted);
- More often agree and more rarely disagree and strongly disagree that their organization needs to increase the number of digital investigators and that most types of criminal investigations in the organization use digital forensics ($H6_{9alt}$ and H610alt are accepted);
- More often strongly agree and more rarely strongly that their organization needs to acquire more technologies and tools for digital forensics ($H6_{12alt}$ is accepted);
- More rarely disagree and strongly disagree that organization depends on digital forensics teams of third parties to help with digital investigations ($H6_{14alt}$ is accepted);
- More often disagree and strongly disagree that employees of digital forensics can easily work IT department without additional training and vice versa ($H6_{19alt}$ is accepted).

As all above differences are statistically significant the null hypothesis H6 is rejected and alternative Hypothesis $H6_{alt}$ is accepted. There is an association between perception of digital forensic and number years in the organization. Received results indicate that respondents who work in organization 1-10 years are more skeptical about the current usage of the digital forensic in the organization than respondents who have been working in the organization for longer time. Also, the respondents which work 1-10 years understand the importance of the use of the digital forensic in future more than respondents who work in the organization more than 10 years.

5.3.7Experience in digital forensic

The results of the Chi-square test for differences in perception of the digital forensic by experience are presented in Table 5.41.

Table 5.41: Chi-square test results for differences in perception of the digital forensic by experience in forensic.

Sub-hypo-theses	Statements	Pearson Chi-Square Value	df	Asymptotic Significance (2-sided)
$H7_1$	**Digital forensics is mainly concerned about cybercrimes**	**17.912**	**4**	**0.001**
$H7_2$	**The organization has clear procedures to handle all aspects of digital investigation**	**14.814**	**4**	**0.005**
$H7_3$	**IT department is controlling digital forensics operations**	**16.539**	**4**	**0.002**
$H7_4$	**Delivering and acquiring information regarding digital investigation are very organized**	**22.162**	**4**	**0.000**
$H7_5$	**Each digital forensics case has its own plan of operations and processes**	**17.95**	**4**	**0.001**
$H7_6$	**The organization has the ability to examine any digital device regardless of its complexity**	**17.19**	**4**	**0.002**
$H7_7$	**The organization has clear guidelines about storing and transferring digital evidence**	**20.427**	**4**	**0.000**
$H7_8$	**Digital investigators in the organization are well trained and they have all necessary skills to perform any operation in digital forensics**	**18.957**	**4**	**0.001**
$H7_9$	**The organization needs to increase the number of digital investigators**	**26.132**	**4**	**0.000**
$H7_{10}$	**Most types of criminal investigations in the organization use digital forensics**	**15.59**	**4**	**0.004**
$H7_{11}$	**Achievements of digital forensics team are well-known throughout the organization**	**15.059**	**4**	**0.005**
$H7_{12}$	**The organization needs to acquire more technologies and tools for digital forensics**	**23.507**	**4**	**0.000**

$H7_{13}$	**The organization has the ability to develop new digital forensics tools that can be used by other organizations**	**27.797**	**4**	**0.000**
$H7_{14}$	**The organization depends on digital forensics teams of third parties to help with digital investigations**	**17.975**	**4**	**0.001**
$H7_{15}$	**Digital forensics team has influence on drawing the general policy and strategy of the organization**	**21.203**	**4**	**0.000**
$H7_{16}$	**The organization helps other organizations in term of digital forensics**	**12.723**	**4**	**0.013**
$H7_{17}$	**Digital forensics team has full access to all information in any assigned case**	**23.993**	**4**	**0.000**
$H7_{18}$	**There are established programs to train and develop human resources for digital forensics positions**	**16.295**	**4**	**0.003**
$H7_{19}$	**Employees of digital forensics can easily work IT department without additional training and vice versa**	**20.91**	**4**	**0.000**
$H7_{20}$	**The organization conducts seminars to familiarize stakeholders with operations of digital forensics in the organization**	**16.222**	**4**	**0.003**

Table 5.41 indicates that there are statistically significant differences for all items as all p-value are less than 0.05. Therefore, all null sub-hypotheses H7 are rejected and all alternative sub-hypotheses are accepted.

Quantifying employee knowledge is a very complex process (Gourova et. al., 2016). At the same time, the number of individuals in the digital forensics department in Abu Dhabi police is not very big. Hence, five years of experience was chosen as the threshold. Any employee who has five years' experience or more is considered an expert (indicated by YES in the following table). The contingency tables for Hypothesis 7 are present in Table 5.42.

Table 5.42: The contingency tables for hypothesis 7.

Experience in digital forensic	$H7_1$:Digital forensics is mainly concerned about cybercrimes					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
No	7.6%	3.8%	39.5%	3.2%	45.9%	100.0%
Yes			8.3%		91.7%	100.0%
Total	6.7%	3.3%	35.9%	2.9%	51.2%	100.0%
	$H7_2$: The organization has clear procedures to handle all aspects of digital investigation					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
No	2.7%	51.4%	23.8%	5.9%	16.2%	100.0%
Yes		91.7%			8.3%	100.0%
Total	2.4%	56.0%	21.1%	5.3%	15.3%	100.0%
	$H7_3$: IT department is controlling digital forensics operations					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
No	5.4%	5.9%	45.4%	3.2%	40.0%	100.0%
Yes			16.7%		83.3%	100.0%
Total	4.8%	5.3%	42.1%	2.9%	45.0%	100.0%
	$H7_4$: Delivering and acquiring information regarding digital investigation are very organized					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
No	9.7%	49.2%	14.6%	4.3%	22.2%	100.0%
Yes		100.0%				100.0%
Total	8.6%	55.0%	12.9%	3.8%	19.6%	100.0%
	$H7_5$: Each digital forensics case has its own plan of operations and processes					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
No	45.9%	4.3%	36.8%	5.4%	7.6%	100.0%
Yes	91.7%		8.3%			100.0%
Total	51.2%	3.8%	33.5%	4.8%	6.7%	100.0%

	$H7_6$: The organization has the ability to examine any digital device regardless of its complexity					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
No	10.8%	48.6%	16.2%	7.6%	16.8%	100.0%
Yes	8.3%	91.7%				100.0%
Total	10.5%	53.6%	14.4%	6.7%	14.8%	100.0%

	$H7_7$: The organization has clear guidelines about storing and transferring digital evidence					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
No	5.9%	47.0%	19.5%	4.9%	22.7%	100.0%
Yes		95.8%			4.2%	100.0%
Total	5.3%	52.6%	17.2%	4.3%	20.6%	100.0%

	$H7_8$: Digital investigators in the organization are well trained and they have all necessary skills to perform any operation in digital forensics					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
No	5.9%	53.5%	17.3%	5.9%	17.3%	100.0%
Yes		100.0%				100.0%
Total	5.3%	58.9%	15.3%	5.3%	15.3%	100.0%

	$H7_9$: The organization needs to increase the number of digital investigators					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
No	4.3%	8.6%	37.3%	40.5%	9.2%	100.0%
Yes			4.2%	95.8%		100.0%
Total	3.8%	7.7%	33.5%	46.9%	8.1%	100.0%

	$H7_{10}$: Most types of criminal investigations in the organization use digital forensics					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
No	45.4%	9.7%	33.0%	1.6%	10.3%	100.0%
Yes	87.5%		12.5%			100.0%
Total	50.2%	8.6%	30.6%	1.4%	9.1%	100.0%

	H7$_{11}$: Achievements of digital forensics team are well-known throughout the organization					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
No	6.5%	50.8%	18.9%	5.9%	17.8%	100.0%
Yes		91.7%			8.3%	100.0%
Total	5.7%	55.5%	16.7%	5.3%	16.7%	100.0%

	H7$_{12}$: The organization needs to acquire more technologies and tools for digital forensics					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
No	5.4%	7.6%	41.6%	39.5%	5.9%	100.0%
Yes			8.3%	91.7%		100.0%
Total	4.8%	6.7%	37.8%	45.5%	5.3%	100.0%

	H7$_{13}$: The organization has the ability to develop new digital forensics tools that can be used by other organizations					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
No	5.4%	7.6%	41.1%	38.9%	7.0%	100.0%
Yes			4.2%	95.8%		100.0%
Total	4.8%	6.7%	36.8%	45.5%	6.2%	100.0%

	H7$_{14}$: The organization depends on digital forensics teams of third parties to help with digital investigations					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
No	45.9%	4.9%	35.1%	4.3%	9.7%	100.0%
Yes	91.7%		8.3%			100.0%
Total	51.2%	4.3%	32.1%	3.8%	8.6%	100.0%

	H7$_{15}$: Digital forensics team has influence on drawing the general policy and strategy of the organization					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
No	3.2%	4.3%	41.1%	5.4%	45.9%	100.0%
Yes			4.2%		95.8%	100.0%
Total	2.9%	3.8%	36.8%	4.8%	51.7%	100.0%

	$H7_{16}$: The organization helps other organizations in term of digital forensics					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
No	4.3%	54.6%	18.4%	4.9%	17.8%	100.0%
Yes		91.7%			8.3%	100.0%
Total	3.8%	58.9%	16.3%	4.3%	16.7%	100.0%

	$H7_{17}$: Digital forensics team has full access to all information in any assigned case					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
No	8.6%	43.2%	22.2%	8.6%	17.3%	100.0%
Yes	4.2%	95.8%				100.0%
Total	8.1%	49.3%	19.6%	7.7%	15.3%	100.0%

	$H7_{18}$: There are established programs to train and develop human resources for digital forensics positions					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
No	8.6%	48.1%	20.5%	2.7%	20.0%	100.0%
Yes		91.7%	4.2%		4.2%	100.0%
Total	7.7%	53.1%	18.7%	2.4%	18.2%	100.0%

	$H7_{19}$: Employees of digital forensics can easily work IT department without additional training and vice versa					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
No	4.3%	50.8%	24.9%	5.9%	14.1%	100.0%
Yes		100.0%				100.0%
Total	3.8%	56.5%	22.0%	5.3%	12.4%	100.0%

	$H7_{20}$: The organization conducts seminars to familiarize stakeholders with operations of digital forensics in the organization					
	Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Total
No	44.3%	8.1%	37.8%	1.6%	8.1%	100.0%
Yes	87.5%		12.5%			100.0%

Total	49.3%	7.2%	34.9%	1.4%	7.2%	100.0%

In table 5.42, respondents which have experience in digital forensic in comparison with another group:

- More often strongly disagree that digital forensics is mainly concerned about cybercrimes ($H7_{1alt}$ is accepted);
- More often disagree that their organization has clear procedures to handle all aspects of digital investigation ($H7_{2alt}$ is accepted);
- More often disagree that IT department is controlling digital forensics operations in their organization ($H7_{3alt}$ is accepted);
- All disagree that delivering and acquiring information regarding digital investigation are very organized ($H7_{4alt}$ is accepted);
- More often agree that each digital forensics case has its own plan of operations and processes ($H7_{5alt}$ is accepted);
- More often disagree that their organization has the ability to examine any digital device regardless of its complexity and that their organization has clear guidelines about storing and transferring digital evidence ($H7_{6alt}$ and $H7_{7alt}$ are accepted).
- All disagree that digital investigators in the organization are well trained and they have all necessary skills to perform any operation in digital forensics ($H7_{8alt}$ is accepted);
- More often strongly agree that the organization needs to increase the number of digital investigators and more often agree that most types of criminal investigations in the organization use digital forensics ($H7_{9alt}$ and $P7_{10alt}$ are accepted);

- All disagree and strongly disagree that achievements of digital forensics team are well-known throughout the organization ($H7_{11alt}$ is accepted);
- More often strongly agree that their organization needs to acquire more technologies and tools for digital forensics ($H7_{12alt}$ is accepted);
- All strongly agree and neutral that organization has the ability to develop new digital forensics tools that can be used by other organizations ($H7_{13alt}$ is accepted);
- More often agree that organization depends on digital forensics teams of third parties to help with digital investigations ($H7_{14alt}$ is accepted);
- All disagree and neutral that digital forensics team has influence on drawing the general policy and strategy of the organization ($H7_{15alt}$ is accepted);
- All disagree and strongly disagree that their organization helps other organizations in term of digital forensics ($H7_{16alt}$ is accepted);
- More often disagree that digital forensics team has full access to all information in any assigned case ($H7_{17alt}$ is accepted);
- More often disagree that there are established programs to train and develop human resources for digital forensics positions in organization ($H7_{18alt}$ is accepted);
- All disagree that employees of digital forensics can easily work IT department without additional training and vice versa ($H7_{19alt}$ is accepted);
- More often agree that their organization conducts seminars to familiarize stakeholders with operations of digital forensics in the organization ($H7_{20alt}$ is accepted).
- As all above difference is statistically significant the Hypothesis $H7_0$ is rejected and $H7_{alt}$ is accepted.

Hence, the respondents which have experience in digital forensic have a better understanding of the digital forensic than those who do not have experience. The respondents which have experience in digital forensic are more unsatisfied the current usage of the digital forensic in the organization. Such respondents give the digital forensic more importance in future activities of the organization.

Another thing to note here is strong alignment among experts in digital forensics regarding their answers to the questions in the questionnaire. There are three questions out of the 20 questions which have 100% agreement among experts in their answers. Moreover, there are 14 questions out of 20 with 90% agreement. The remaining three questions have more than 80% agreement. In other words, 80% of experts have identical answers to the questionnaire questions which indicates a high level of alignment among them.

More statistical analysis can be performed by converting Likert scale into numerical values and perfuming mean and standard deviation calculations. One way is to use scale from -2 to 2 where -2 represents Strongly Disagree and 2 represents Strongly Agree. The second scale that can be used is from 1 to 5 where 1 represents Strongly Disagree and 5 represents Strongly Agree.

H71 has 31.35 as an average value with respect to the first scale with 81.59 as standard deviation for non-experts. With respect to the second scale, it has 158.0 as a mean and 184.57 as standard deviation. The mean of experts is 76.91 based on the first scale and 202.31 based on the second scale where the standard deviation values are 153.82 and 380.04.

H72 has -7.94 as an average value with respect to the first scale with 56.27 as standard deviation for non-experts. With respect to the second scale, it has 117.46 as a mean and

76.97 as standard deviation. The mean of experts is -31.77 based on the first scale and 93.63 based on the second scale where the standard deviation values are 81.29 and 149.02.

H73 has 28.01 as an average value with respect to the first scale with 70.24 as standard deviation for non-experts. With respect to the second scale, it has 152.15 as a mean and 167.3 as standard deviation. The mean of experts is 69.39 based on the first scale and 194.79 based on the second scale where the standard deviation values are 138.78 and 338.81.

H74 has -8.78 as an average value with respect to the first scale with 63.84 as standard deviation for non-experts. With respect to the second scale, it has 116.62 as a mean and 86.26 as standard deviation. The mean of experts is -41.8 based on the first scale and 83.6 based on the second scale where the standard deviation values are 83.6 and 167.2.

H75 has -31.35 as an average value with respect to the first scale with 81.68 as standard deviation for non-experts. With respect to the second scale, it has 94.05 as a mean and 74.63 as standard deviation. The mean of experts is -76.91 based on the first scale and 48.49 based on the second scale where the standard deviation values are 153.82 and 74.47.

H76 has -12.12 as an average value with respect to the first scale with 58.65 as standard deviation for non-experts. With respect to the second scale, it has 114.53 as a mean and 67.81 as standard deviation. The mean of experts is -45.14 based on the first scale and 80.26 based on the second scale where the standard deviation values are 74.7 and 152.29.

H77 has -3.34 as an average value with respect to the first scale with 62.57 as standard deviation for non-experts. With respect to the second scale, it has 123.31 as a mean and

87.14 as standard deviation. The mean of experts is -36.78 based on the first scale and 88.62 based on the second scale where the standard deviation values are 82.18 and 157.17.

H78 has -10.87 as an average value with respect to the first scale with 59.97 as standard deviation for non-experts. With respect to the second scale, it has 114.53 as a mean and 78.68 as standard deviation. The mean of experts is -41.8 based on the first scale and 83.6 based on the second scale where the standard deviation values are 83.6 and 167.2.

H79 has 17.56 as an average value with respect to the first scale with 39.62 as standard deviation for non-experts. With respect to the second scale, it has 142.96 as a mean and 126.06 as standard deviation. The mean of experts is 40.13 based on the first scale and 165.53 based on the second scale where the standard deviation values are 80.26 and 318.66.

H710 has -32.6 as an average value with respect to the first scale with 80.33 as standard deviation for non-experts. With respect to the second scale, it has 92.8 as a mean and 65.65 as standard deviation. The mean of experts is -73.57 based on the first scale and 53.09 based on the second scale where the standard deviation values are 147.14 and 72.64.

H711 has -9.61 as an average value with respect to the first scale with 59.29 as standard deviation for non-experts. With respect to the second scale, it has 117.04 as a mean and 76.5 as standard deviation. The mean of experts is -31.77 based on the first scale and 93.63 based on the second scale where the standard deviation values are 81.29 and 149.02.

H712 has 14.21 as an average value with respect to the first scale with 38.27 as standard deviation for non-experts. With respect to the second scale, it has 140.87 as a mean and

132.0 as standard deviation. The mean of experts is 38.46 based on the first scale and 163.86 based on the second scale where the standard deviation values are 76.91 and 303.25.

H713 has 14.63 as an average value with respect to the first scale with 37.81 as standard deviation for non-experts. With respect to the second scale, it has 140.03 as a mean and 127.22 as standard deviation. The mean of experts is 40.13 based on the first scale and 165.53 based on the second scale where the standard deviation values are 80.26 and 318.66.

H714 has -30.51 as an average value with respect to the first scale with 82.76 as standard deviation for non-experts. With respect to the second scale, it has 94.89 as a mean and 70.51 as standard deviation. The mean of experts is -76.91 based on the first scale and 48.49 based on the second scale where the standard deviation values are 153.82 and 74.47.

H715 has 36.37 as an average value with respect to the first scale with 78.35 as standard deviation for non-experts. With respect to the second scale, it has 160.51 as a mean and 184.61 as standard deviation. The mean of experts is 80.26 based on the first scale and 205.66 based on the second scale where the standard deviation values are 160.51 and 398.89.

H716 has -9.2 as an average value with respect to the first scale with 61.38 as standard deviation for non-experts. With respect to the second scale, it has 116.2 as a mean and 83.99 as standard deviation. The mean of experts is -31.77 based on the first scale and 93.63 based on the second scale where the standard deviation values are 81.29 and 149.02.

H717 has -7.52 as an average value with respect to the first scale with 54.06 as standard deviation for non-experts. With respect to the second scale, it has 117.88 as a mean and 62.35 as standard deviation. The mean of experts is -43.47 based on the first scale and 81.93 based on the second scale where the standard deviation values are 78.85 and 159.71.

H718 has -9.61 as an average value with respect to the first scale with 60.08 as standard deviation for non-experts. With respect to the second scale, it has 117.04 as a mean and 82.18 as standard deviation. The mean of experts is -35.11 based on the first scale and 90.29 based on the second scale where the standard deviation values are 78.85 and 147.99.

H719 has -10.45 as an average value with respect to the first scale with 54.18 as standard deviation for non-experts. With respect to the second scale, it has 114.95 as a mean and 74.75 as standard deviation. The mean of experts is -41.8 based on the first scale and 83.6 based on the second scale where the standard deviation values are 83.6 and 167.2.

H720 has -32.6 as an average value with respect to the first scale with 77.37 as standard deviation for non-experts. With respect to the second scale, it has 92.8 as a mean and 78.17 as standard deviation. The mean of experts is -73.57 based on the first scale and 53.09 based on the second scale where the standard deviation values are 147.14 and 72.64.

5.4 Survey Summary

Based on received results, we can conclude that there are associations between social and demographic aspects of the subjects and their perception of the digital forensic. The most association with perception of the digital forensic were found for experience in digital forensic (20 items), next followed by education level (16 items), years in the organization (7 items), age (4 items), and years in current position (1 item).

Considering above reported results, the main patterns of association between perception of the digital forensic and social-demographics characteristics of the personnel are summarized in Table 5.43.

Table 5.43: Main pattern between perception of the digital forensic and social-demographics aspects of the personnel.

Aspects	**Main patterns of associations with perception of the digital forensic**
Age	The respondents from younger age-group are not satisfied with the current status of the digital forensic in the organization and give more importance of the usage of the digital forensic in future activity of the organization.
Educational	The respondents with higher education level understand the digital forensic more widely than other, these respondents are not satisfied with the current status of the digital forensic in the organization and give more importance of the usage of the digital forensic in future.
Rank	The respondents with lower ranks usually understand the digital forensic more widely than other, these respondents are not satisfied with the current status of the digital forensic.

Years in current position	The respondents which are 4 years in current position are more pessimistic about the ability of the organization to develop new digital forensics tools that can be used by other organizations.
Years in organization	The respondents who work in the organization up to 10 years have more skeptical responses regarding the current status of the digital forensic in the organization than respondents who are working in the organization for longer time. Also, the respondents which work 1-10 years more understand the importance of the use of the digital forensic in future than respondents who work in the organization more than 10 years.
Digital forensic experience	The respondents which have experience in digital forensic understand of the digital forensic more widely than those who do not have the same experience. The respondents which have experience in digital forensic are more unsatisfied with the current status of the digital forensic in the organization. Such respondents give the digital forensic more importance in future activities of the organization.

Hence, demographic aspects of personnel such as Education, Age, Years in the Organization, Years in Current Position and Years in Digital Forensics can be a good indication of how subjects perceive maturity of digital forensics operation in the organization.

The statistically significant differences in perception of the digital forensic by gender weren’t found. But for some items, the differences by Gender are significant at significance level 0.1. We can suggest that differences in perception of digital forensic by gender can be statistically significant if sample size will be increased. Many differences in perception of the digital forensic by Rank were found. But common patterns of association between perception of the digital forensic and Rank weren't found. We also can suggest that such patterns of association can be found if sample size will be increased in future research.

5.5 Predictive Model

Based on survey findings, one can use stakeholder information to predict their reliability through the use of predictive model. Stakeholder information is:

- Age
- Rank
- Experience in Digital Forensics
- Overall Experience in Police Work
- Technical Background
- Level of Education

The predictive model is generated by using machine learning techniques mentioned in the previous chapter. Data set used to generate the predictive model is composed subjects information and the reliability values as calculated in section 4.3.3. Then cross validation is used to measure the error rate for each machine learning technique. It worth mentioning that the used dataset was divided into two sets; where the first set was used as training set and the second set was used as testing set. The analysis presented in the following table is conducted on testing set only so that the testing will be reliable.

Table 5.44: Performance of machine learning techniques.

	Average Error	Standard Deviation
Nearest Neighbors	0.0698	0.0196
Decision Tree	0.0555	0.0118
Support Victor Machine	0.0695	0.0133
Neural Networks	0.0489	0.0108

Table 5.44 shows that using machine learning to predict reliability of stakeholders is very effective due to the low average error rate of prediction. This agrees with findings of survey analysis. Hence, one can generate a predictive model to estimate reliability and use this estimation to calculate priority metric as mentioned in section 5.4.

5.6 Proposed Prioritisation Process

This research tries to develop a framework for practitioners in digital forensics department so that they can measure reliability of handlers judgments regarding the importance of DF examination in their investigations. If the handler judgment is reliable, then their suggestions and evaluations will be considered in prioritisation process. Otherwise, prioritisation process will be based on other factors regardless of handler judgment.

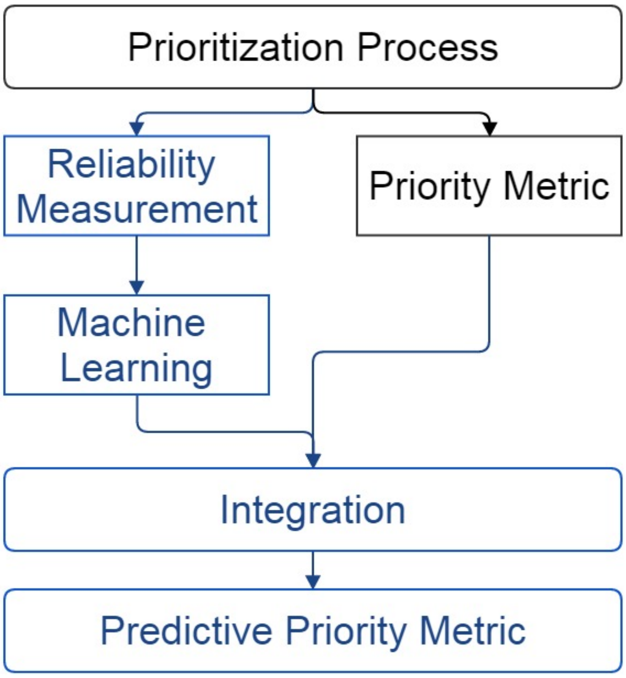


Figure 5.8: Proposed improvements.

Figure 5.8 shows the proposed improvements in this thesis to the prioritisation process in digital forensics departments. The first improvement is the proposed reliability measurement of stakeholders with regards to their believe and knowledge about digital forensics operations. Section 4.3 discusses how reliability measurement is constructed. Then, data generated by reliability measurement will used to generate machine learning models so that an automated estimation is reliability can be performed as discussed in Chapter 5. Finally, generated predictive models will be integrated with existing priority metric calculation to produce an improved metric so that prioritisation process takes in consideration reliability of stakeholders.

5.7 Applicability and Justifications

The most important feature of the proposed solution is the ease of integration with the existing prioritisation mechanism. This feature allows any digital forensics department to apply the proposed solution in their prioritisation process. Case importance which is set by the case leader plays an important role in prioritisation of the case within digital forensics department. Increasing the accuracy of case importance will certainly improves the prioritisation.

Another justification to use the proposed solution is to introduce evaluation feedback within the digital forensics department and associated departments. Such feedback will help to find a common ground for distributing workloads and scheduling cases for digital investigation. In addition, utilising the proposed prioritisation framework will allow digital forensics departments to find out weaknesses with regard to the importance evaluation of digital forensic cases. Calculating reliability estimation for all possible case handlers in the organisation will lead to having a dataset that describe the ability of each one of the case handlers to accurately evaluate case importance. Such dataset is very valuable for studies and investigations that can improve prioritisation process and general efficiency in digital forensics department. As mentioned before, one may use this dataset to introduce uncertainty in the prioritisation process in a way that improve the process overall outcome. Such dataset can be easily converted into the solution that can describe the probability distribution of having an accurate importance evaluation for digital forensics cases. At the same time, this dataset would be a dynamic one where its content would be evolving over time by continuous calculation of reliability measurement for all possible case handlers in the organisation. Furthermore, updating machine learning models with this continuous updating dataset will certainly improve predictability of these models. Lastly but not least, adopting the proposed linear integration process to the existing prioritisation process will reduce any possible negative disruption to the existing operations. From digital forensics department perspective, adopting the proposed prioritisation process based on reliability estimation can only have a positive impact on the operations with little to no existing overhead.

5.8 Chapter Summary

The main purpose of this chapter was to discuss analysis of data collected in this research. Statistical analysis was performed to validate that biographical aspects of stakeholders can be used to predict reliability. The main findings of statistical analysis can be summarized as follow:

- Younger respondents are not pleased with the status of the digital forensic in Abu Dhabi police. They gave more importance of the usage of the digital forensic in future activities of the organization.
- Education is an important aspect in understanding digital forensics operations. The respondents with higher education level understand the digital forensic more widely than other, these respondents are not satisfied with the status of the digital forensic in the organization and give more importance of the usage of the digital forensic in future.
- Individual seniority in the organization is significant as well. In general, the respondents which are four years in current position are more pessimistic about the ability of the organization to develop new digital forensics tools that can be used by other organizations. Similarly, the respondents who work in the organization up to 10 years have more sceptical responses regarding the status of the digital forensic in the organization than respondents who are working in the organization for longer time. Also, the respondents which work 1-10 years more understand the importance of the use of the digital forensic in future than respondents who work in the organization more than 10 years.
- Finally, the most important aspect is digital forensics experience. The respondents which have experience in digital forensic understand its operations

more widely than those who do not have the same experience. The respondents which have experience in digital forensic are more unsatisfied with the status of the digital forensic in the organization. Such respondents give the digital forensic more importance in future activities of the organization.

Then, predictive model based machine learning was evaluated with regards to reliability estimation. All results confirm that the proposed framework can be very effective to improve prioritisation process in digital forensics department.

Chapter 6: Conclusions

6.1 Overview

Digital forensics departments in law enforcement organizations are not able to handle all investigation cases due to increased adoption of digital devices in all types of crimes and the limited available resources in these departments. Hence, DF department has to prioritize cases to insure effectiveness and highest possible utilization. Prioritisation process of case depends on many factors such as number of victims, value of damages, and relation to organization goal. One of the most important factors is the necessity of performing digital forensics in case context. For example, some cases may already have the necessary evidence to solve the case. Any extra evidence after performing digital forensics will not change the situation. It will not be efficient to waste valuable and limited DF resources on such investigation. At the same time, investigators in DF department do not have full access to all aspects of criminal investigation. They have to rely on the judgment of case handlers. Usually, those handlers are not aware of DF operation and what DF can offer depending on the available resources. Therefore, handlers' judgment and awareness of DF operations play an important role in prioritisation process. The research problem lies on the fact that there is no clear way to measure reliability of handler judgment in literature. Having such measurement will provide DF investigators with the ability to prioritize cases based on how valuable DF operations in successful investigation.

The main practical problem in this research is prioritisation of digital forensics cases. This research argues that addressing this problem is essential to improve digital forensics operations. Hence, the starting point in the adopted approach is to find out what is the most important aspect of prioritisation process that needs addressing. This research suggests that the overall understanding of stakeholder about digital forensics is very important; especially when considering their reliability of estimating case importance and priority. A questionnaire instrument is proposed which asks questions based on qualitative nature. Nevertheless, the quantitative aspects of subjects' answers were mainly considered such as the general statistics. Then, a prioritisation model based on machine learning was proposed by utilizing survey data in a way that automates and improves prioritisation process in digital forensics department. Finally, a general framework was suggested to be used by managers of digital forensics department.

Limited resources and increased number of cases in recent years leads to a situation where law enforcement organizations are not able to efficiently address and handle all cases effectively. Each one of police officers, technical staff and government representatives would like to influence the investigation process based on their beliefs and understanding. At the same time, digital forensics labs handle different cases from different departments. Each one of these department would prefer their cases to be prioritized. The lack of prioritisation mechanism which is standard and agreeable among all stakeholders would let these conflicts reduce the efficiency and utilization of forensics lab resources. It is clear that addressing prioritisation in digital forensics departments is very critical for the success of law enforcement operations. Standard mechanisms for prioritisation are highly needed to resolve conflicts among stakeholders and to design long term policy for investments in digital forensics departments.

6.2 Thesis Summary

An extensive literature review was conducted which showed that there is an extreme lack of investigation in digital forensics literature with regards to prioritisation problem. The closest attempts to this topic is studying crime scene triage where the digital forensics specialist tries to prioritize existing digital devices found in the scene. Literature does not have any work that address prioritisation issue specifically. At the same time, most works in literature deals with digital forensics issues with generalization mentality. They only try to address macro issues such as general policies adopted by law enforcement organization with regards to digital forensics operations. There are very few works which are concerned with micro issues such as crime scene triage and analysis techniques used in digital forensics.

In addition, there are limited works which approaches human aspects of digital forensics. The implicit assumption that digital forensics operation are very mechanical and human factors do not play any role is widely spread in literature. Digital forensics have high level of technicality which give the impression that the negative impact of human factors will be minimized in its operations. Similarly, most researchers in digital forensics literature use only traditional methodologies to address their issues under investigation. There are no attempts worth mentioning where the researcher borrowed or utilized investigation techniques from other field of sciences.

6.3 Research Contribution

The first contribution of this thesis manifested in providing the necessary background on digital forensics to understand the complexities faced by personnel in digital forensics departments. The provided background can be summarized in these main points:

- Law enforcement agencies have begun to view every computer connected to the internet as a port of entry for the criminals.

- Computer history and phone records contain more information about an individual than any other source that makes digital evidence very important for any case.
- Prioritisation problem is hugely affected by the competency of personnel.
- A complete and competent forensic digital investigation involves several complex steps.
- There is an extreme lack of investigation in digital forensics literature with regards to prioritisation problem.
- Most researchers in digital forensics literature use only traditional methodologies to address their issues under investigation.

After highlighting the most important lessons from literature, this thesis highlighted the salient features and policies of the Abu Dhabi and UAE police force to establish the necessary understanding of research context. This contribution led to these takeaways:

- UAE is a developing country with a very rapid development rate in economic, political and social aspects. Hence, security challenges are expected to increase in the future where digital devices and technical solution are going to be used in criminal acts.
- There are few nationals who have acquired the necessary skills to perform digital forensics.
- Based on Abu Dhabi police structure, digital forensics still not considered as one of the major functionalities of police operations.

Having that in mind, this research tried to develop a framework to improve prioritisation process in digital forensics department. This research effort led to these important outcomes:

- In this research, we contribute to the literature by providing a tool to measure perception regarding digital forensics based on maturity models.
- Another contribution of this research to literature is a measurement technique to measure how reliable is case handler judgment regarding digital forensics maturity in the organization.
- In addition, another main contribution of this research is the utilization of machine learning in improving the proposed reliability measurement.
- An integration mechanism of the proposed reliability measurement into the existing prioritisation process is another contribution of this research.

Lastly, the study is the first one in the country and region. There is no available publication that add in case prioritisation in police force to compare our results against. The response from the stakeholders has been very positive and the Abu Dhabi police is looking at implementing our findings in the future.

6.4 Future Work

This research focused on prioritisation of cases in digital forensics department. It proposes a framework based on measuring perception of stakeholders regarding digital forensics maturity to evaluate their reliability. Then, collected data is used to build predictive models through machine learning to estimate reliability. Similar, approach can be utilized to investigate other aspects of digital forensics operations. For example:

- A straightforward future work is to conduct a comparative study of different law enforcement organizations. Techniques developed in this thesis can be applied directly without any modifications. Preferably, data should be collected form several organizations from different geographical regions and economy size. Also, the organization size should play role in the selection process so that different maturity levels of digital forensics can be investigated.

- Machine learning techniques can be used to tackle other aspect of digital forensics operation. For instance, it will be interesting future work to investigate if machine learning can be used to predict how long a digital forensics task will last. Such capability can greatly improve scheduling process of available resources and personnel in digital forensics department.
- Other maturity models can be used to develop the data collection tool which will be used to study perception regarding digital forensics. Furthermore, one may even develop a custom maturity model which is focused on specific process in digital forensics department. The model can be very detailed and technically oriented which cannot be said about the existing maturity models.

There are many more ideas for future works that can be considered. As said before, there is an extreme lack of studies in literature which are focused on efficiency aspects of digital forensics operations. Any research effort in this direction is very welcome.

References

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.

Akerkar, R., & Sajja, P. S. (2016). Artificial neural network. In Intelligent Techniques for Data Science (pp. 125-155). Springer International Publishing.

Al Hanaei, E. H., & Rashid, A. (2014). DF-C2M2: A Capability Maturity Model for Digital Forensics Organisations. In Security and Privacy Workshops (SPW), 2014 IEEE (pp. 57-60). IEEE.

Al Sharif, S., Al Ali, M., Salem, N., Iqbal, F., El Barachi, M., & Alfandi, O. (2014, March). An Approach for the Validation of File Recovery Functions in Digital Forensics' Software Tools. In New Technologies, Mobility and Security (NTMS), 2014 6th International Conference on (pp. 1-6). IEEE.

Al-Ali, J., (2008), “Emiratisation: drawing UAE nationals into their surging economy”, International Journal of Sociology and Social Policy, Vol. 28, No. 10, pp.365 - 379

Alanezi, A., (2012), “Workforce Localization Policies in Saudi Arabia: The Determinations of Successful Implementation in Multi-National Enterprises”, Management Knowledge and Learning International Conference, PP 957 – 968.

Alkaabi, A., Mohay, G. M., McCullagh, A.J. and Chantler, A.N. (2010) ‘Dealing with the problem of cybercrime’, Proceedings of the 2nd International ICST Conference on Digital Forensics & Cyber Crime, 4–6 October 2010, Abu Dhabi.

Almarzooqi, A., & Jones, A. (2016). A Framework for Assessing the Core Capabilities of a Digital Forensic Organization. In IFIP International Conference on Digital Forensics (pp. 47-65). Springer International Publishing.

Amann, P., & James, J. I. (2015). Designing robustness and resilience in digital investigation laboratories. Digital Investigation, 12, S111-S120.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., ... & Savage, S. (2013). Measuring the cost of cybercrime. In The economics of information security and privacy (pp. 265-300). Springer Berlin Heidelberg.

Assuncao, M. D., Calheiros, R. N., Bianchi, S., Netto, M. A., & Buyya, R. (2015). Big Data computing and clouds: Trends and future directions. Journal of Parallel and Distributed Computing, 79, 3-15.

Balouga, J., (2012), “Nigerian Local Content: Challenges and Prospects”, International Association for Energy Economies, pp. 23-26

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. Computers in Human Behavior, 48, 51-61.

Bennett, D. (2012) 'The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations', Information Security Journal: A Global Perspective, Vol. 21, 3.

Bryman, A. and Bell, E. (2011) Business Research Methods, Oxford University Press.

Cantrell, G., Dampier, D., Dandass, Y. S., Niu, N., & Bogen, C. (2012). Research toward a partially-automated, and crime specific digital triage process model. Computer and Information Science, 5(2), p29.

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press.

Choo, K. and Martini, B. (2012) 'An integrated conceptual digital forensic framework for cloud computing', Digital Investigation, Vol. 9, 2, pp 71–80.

Cohen, M.I., Bilby, D. and Caronni, G. (2011) 'Distributed Forensics and Incident Response in the Enterprise'. Digital Investigation, 2011(8), p. 101-110.

Cole, K. A., Gupta, S., Gurugubelli, D., & Rogers, M. K. (2015, May). A Review of Recent Case Law Related to Digital Forensics: The Current Issues. InProceedings of the Conference on Digital Forensics, Security and Law (pp. 95-104).

Curtis, B., Hefley, B., & Miller, S. (2009). People capability maturity model (P-CMM) version 2.0 (No. CMU/SEI-2009-TR-003). Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst.

Dagher, G. G., & Fung, B. C. (2013). Subject-based semantic document clustering for digital forensic investigations. Data & Knowledge Engineering, 86, 224-241.

Damshenas, M., Dehghantanha, A., Mahmoud, R. and bin Shamsuddin, S. (2012) 'Forensics investigation challenges in cloud computing environments', Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference.

Daniel, G. G. (2013). Artificial neural network. In Encyclopedia of Sciences and Religions (pp. 143-143). Springer Netherlands.

Domingos, P. (2012). A few useful things to know about machine learning. Communications of the ACM, 55(10), 78-87.

Flory, C. (2014, March). Making the case of digital forensics field training for parole services. In Proceedings of the 15th Annual Information Security Symposium (p. 41). CERIAS-Purdue University.

Floyd, K., & Yerby, J. (2014). Development of a Digital Forensics Lab to Support Active Learning. Development, 4, 14-2014.

Garfinkel, S.L. (2010) 'Digital forensics research: The next 10 years'. Digital Investigation, 2010, 7, p. 64-73.

Glasser, D., & Taneja, A. (2014). A Routine Activity Theory-Based Framework for Combating Cybercrime. Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance, 398.

Gonzalez, C. (2013). The boundaries of Instance-Based Learning Theory for explaining decisions from experience. Decision making: Neural and behavioural approaches, 202, 73-98.

Gonzalez, C., & Dutt, V. (2011). Instance-based learning: Integrating sampling and repeated decisions from experience. Psychological review, 118(4), 523.

Gourova, E., Dragomirova, M., & Toteva, K. (2016). Knowledge profiles of employees. In Proceedings of the 21st European Conference on Pattern Languages of Programs (p. 11). ACM.

Gupta, J. N., Kalaimannan, E., & Yoo, S. M. (2016). A heuristic for maximizing investigation effectiveness of digital forensic cases involving multiple investigators. Computers & Operations Research, 69, 1-9.

Gupta, J. N., Kalaimannan, E., & Yoo, S. M. (2016). A heuristic for maximizing investigation effectiveness of digital forensic cases involving multiple investigators. Computers & Operations Research, 69, 1-9.

Hajek, J., Hykš, O., Koliš, K., & Veber, J. (2015). Digital Forensics Laboratory Process Model. In Information Systems: Development, Applications, Education(pp. 61-69). Springer International Publishing.

Hannan, M. (2004) 'To revisit: What is Forensic Computing?', Proceedings of the Second Australian Computer, Network and Information Forensics Conference, p. 103a.

Hargreaves, C., & Patterson, J. (2012). An automated timeline reconstruction approach for digital forensic investigations. Digital Investigation, 9, S69-S79.

Harrington, P. (2012). Machine learning in action (Vol. 5). Greenwich, CT: Manning.

Hassitt, A. (2014). Computer programming and computer systems. Academic Press.

Hegarty, R. C., Lamb, D. J., & Attwood, A. (2014). Digital Evidence Challenges in the Internet of Things. In Proceedings of the Tenth International Network Conference (INC 2014) (p. 163).

Helbing, D. (2015). What the Digital Revolution Means for Us. In Thinking Ahead-Essays on Big Data, Digital Revolution, and Participatory Market Society (pp. 177-187). Springer International Publishing.

Humphrey, W. S. (1988). Characterizing the software process: a maturity framework. IEEE software, 5(2), 73-79.

James, J. I. (2014). Multi-Stakeholder Case Prioritisation in Digital Investigations. Journal of Digital Forensics, Security and Law, 9(2), 59-72.

James, J. I., & Breitinger, F. (Eds.). (2015). Digital Forensics and Cyber Crime: 7th International Conference, ICDF2C 2015, Seoul, South Korea, October 6-8, 2015. Revised Selected Papers (Vol. 157). Springer.

James, J. I., & Gladyshev, P. (2013). A survey of digital forensic investigator decision processes and measurement of decisions based on enhanced preview. Digital Investigation, 10(2), 148-157.

James, J. I., Shosha, A. F., & Gladyhsev, P. (2014). Determining Training Needs for Cloud Infrastructure Investigations Using I-STRIDE. In Digital Forensics and Cyber Crime (pp. 223-236). Springer International Publishing.

Jang, Y. J., & Kwak, J. (2014). Digital forensics investigation methodology applicable for social network services. Multimedia Tools and Applications, 1-12.

Jiang, J. G., Yang, B., Lin, S., Zhang, M. X., & Liu, K. Y. (2015, April). A Practical Approach for Digital Forensic Triage. In Applied Mechanics and Materials (Vol. 742, pp. 437-444).

Jones, A., & Valli, C. (2011). Building a Digital Forensic Laboratory: Establishing and Managing a Successful Facility. Butterworth-Heinemann.

Kamarudin, S., & Mohammad, M. I. (2011). File Security based on Pretty Good Privacy (PGP) Concept. Computer and Information Science, 4(4), p10.

Karie, N. M., & Venter, H. S. (2015). Taxonomy of challenges for digital forensics. Journal of forensic sciences, 60(4), 885-893.

Kerrigan, M. (2013). A capability maturity model for digital investigations. Digital Investigation, 10(1), 19-33.

Kim, Y., & Ross, S. (2012). Digital forensics formats: seeking a digital preservation storage container format for web archiving. International Journal of Digital Curation, 7(2), 21-39.

Kohn, M. D., Eloff, M. M., & Eloff, J. H. (2013). Integrated digital forensic process model. Computers & Security, 38, 103-115.

Kohn, M., Olivier, M. S., & Eloff, J. H. (2006, July). Framework for a Digital Forensic Investigation. In ISSA (pp. 1-7).

Kruse II, W. G., & Heiser, J. G. (2001). Computer forensics: incident response essentials. Pearson Education.

Lejarraga, T., Dutt, V., & Gonzalez, C. (2012). Instance-based learning: A general model of repeated binary choice. Journal of Behavioral Decision Making, 25(2), 143-153.

Madi, M. Selim, H., and Rutledge, E. (2012), "Emiratisation: determining the factors that influence the recruitment decisions of employers in the UAE", The International Journal of Human Resource Management, Vol. 23, No. 2, PP 406–421

Mansour, A. M.E., (2014), "The Impact of Privatization on the United Arab Emirates (UAE) Federal Public Sector", International Public Management Review, Vol 9, No. 2, PP 66-89

McKemmish, R. (1999) 'What is Forensic Computing', Trends and Issues in Crime and Criminal Justice, Vol.118.

Mercuri, R. (2005) 'Challenges in Forensic Computing', Communications of the ACM, Vol. 48, 12, pp. 17-21.

Mohamed, A. F. A. L., Marrington, A., Iqbal, F., & Baggili, I. (2014). Testing the forensic soundness of forensic examination environments on bootable media.Digital Investigation, 11, S22-S29.

Montasari, R. A. (2016). Formal Two Stage Triage Process Model (FTSTPM) for Digital Forensic Practice. Int. J. Comput. Sci. Secur, 10, 69-87.

Moser, A., & Cohen, M. I. (2013). Hunting in the enterprise: Forensic triage and incident response. Digital Investigation, 10(2), 89-98.

Nahar, K. (2012). Artificial neural network. COMPUSOFT, An international journal of advanced computer technology, 1(2), 25-27.

Nassif, L. F., & Hruschka, E. R. (2013). Document clustering for forensic analysis: an approach for improving computer inspection. Information Forensics and Security, IEEE Transactions on, 8(1), 46-54.

Noblett, G., Pollitt, M. and Presley, A. (2000) 'Recovering and Examining Computer Forensic Evidence'. Forensic Science Communications, Vol. 2, 4.

Oliver, J. J., & Hand, D. J. (2016). On pruning and averaging decision trees. In Machine Learning: Proceedings of the Twelfth International Conference (pp. 430-437).

Paulk, M. C., Curtis, B., Chrissis, M. B., & Weber, C. V. (1993). Capability maturity model, version 1.1. IEEE software, 10(4), 18-27.

Pollitt, M. M. (2007, April). An ad hoc review of digital forensic models. InSystematic Approaches to Digital Forensic Engineering, 2007. SADFE 2007. Second International Workshop on (pp. 43-54). IEEE.

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.

Raghavan, S. (2013). Digital forensic research: current state of the art. CSI Transactions on ICT, 1(1), 91-114.

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. International Journal of Digital Evidence, 1(3), 1-12.

Rokach, L., & Maimon, O. (2014). Data mining with decision trees: theory and applications. World scientific.

Ruan, K. (2012) Cybercrime and Cloud Forensics: Applications for Investigation Processes, University College Dublin, Ireland.

Rutkowski, L., Jaworski, M., Pietruczuk, L., & Duda, P. (2014). Decision trees for mining data streams based on the gaussian approximation. IEEE Transactions on Knowledge and Data Engineering, 26(1), 108-119.

Sainath, D., & Narayana, K. (2014). A Novel Method for Digital Forensic Analysis through Document Clustering. International Journal of Emerging Engineering Research and Technology, 2(4), 134-138.

SANS Institute (2002) An Uneven Playing Field: The Advantages of the Cyber Criminal vs. Law Enforcement—and Some Practical Suggestions. Reading Rooms Sans, 2002.

Scanlon, M. (2016). Battling the digital forensic backlog through data deduplication. In Innovative Computing Technology (INTECH), 2016 Sixth International Conference on (pp. 10-14). IEEE.

Shah, J. J., & Malik, L. G. (2014, February). An approach towards digital forensic framework for cloud. In Advance Computing Conference (IACC), 2014 IEEE International (pp. 798-801). IEEE.

Sibiya, G., Venter, H. S., Ngobeni, S., & Fogwill, T. (2012, August). Guidelines for procedures of a harmonised digital forensic process in network forensics. InInformation Security for South Africa (ISSA), 2012 (pp. 1-7). IEEE.

Simon, M. and Choo, K-K. R. (2014) 'Digital forensics: Challenges and future research directions'. Korean Institute of Criminology: Seoul, South Korea, pp. 105-146.

Simon, M., & Choo, K. K. R. (2014). Digital forensics: challenges and future research directions. Simon M and Choo KK R, 105-146.

Souvignet, T., & Frinken, J. (2013). Differential power analysis as a digital forensic tool. Forensic science international, 230(1), 127-136.

Sozu, T., Sugimoto, T., Hamasaki, T., & Evans, S. R. (2015). Convenient Sample Size Formula. In Sample Size Determination in Clinical Trials with Multiple Endpoints (pp. 41-58). Springer International Publishing.

Stephen, W., (2012), "Human resource development through vocational education in the United Arab Emirates: the case of Dubai Polytechnic", Journal of Vocational Education and Training, Vol. 54, No. 1, pp. 5-26

Strom, K. J., Ropero-Miller, J., Jones, S., Sikes, N., Pope, M., & Horstmann, N. (2009). Survey of Law Enforcement Forensic Evidence Processing 2007.

Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2014). Digital crime and digital terrorism. Prentice Hall Press.

Thorpe, S., Grandison, T., & Blake, M. B. (2014, March). Cloud computing log forensics-the new frontier. In SOUTHEASTCON 2014, IEEE (pp. 1-4). IEEE.

Wang, L., & Alexander, C. A. (2015). Big Data in Distributed Analytics, Cybersecurity, Cyber Warfare and Digital Forensics. Digital Technologies, 1(1), 22-27.

Wang, X. G. (2014, October). Research on digital forensics and its relevant problems. In Electronics, Information Technology and Intellectualization: Proceedings of the International Conference EITI 2014, Shenzhen, China, 16-17 August 2014 (p. 43). CRC Press.

Wilkins, S. (2010), "International briefing 9: training and development in the United Arab Emirates", International Journal of Training And Development, Vol. 5, 2, pp. 153-165.

Witten, I. H., Frank, E., Hall, M. A., & Pal, C. J. (2016). Data Mining: Practical machine learning tools and techniques. Morgan Kaufmann.

Yang, B., Li, N., & Jiang, J. (2016). A new triage process model for digital investigations. In Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), 2016 IEEE (pp. 712-717). IEEE.

Appendix A

Gender	Education	Age	Rank	Career Experience	Years in the Organization	Years in Current Position	Years in Digital Forensics	Digital forensics is mainly concerned about cybercrimes	The organization has clear procedures to handle all aspects of digital investigation	IT department is controlling digital forensics operations	Delivering and acquiring information regarding digital investigation are very organized	Each digital forensics case has its own plan of operations and processes	The organization has the ability to examine any digital device regardless of its complexity	The organization has clear guidelines about storing and transferring digital evidences	Digital investigators in the organization are well trained and they have all necessary skills to perform any operation in digital forensics	The organization needs to increase number of digital investigators	Most types of criminal investigations in the organization use digital forensics	Achievements of digital forensics team are well-known throughout the organization	The organization needs to acquire more technologies and tools for digital forensics	The organization has the ability to develop new digital forensics tools that can be used by other organizations	The organization depends on digital forensics teams of third parties to help with digital investigations	Digital forensics team has influence on drawing the general policy and strategy of the organization	The organization helps other organizations in term of digital forensics	Digital forensics team has full access to all information in any assigned case	There are established programs to train and develop human resources for digital forensics positions	Employees of digital forensics can easily work IT department without additional training and vice versa	The organization conducts seminars to familiarize stakeholders with operations of digital forensics in the organization
Male	Bachelor	46	Major	25	25	2	0	Strongly Disagree	Neutral	Strongly Agree	Neutral	Strongly Agree	Strongly Agree	Strongly Agree	Disagree	Neutral	Strongly Disagree	Disagree	Disagree	Neutral	Agree	Disagree	Disagree	Disagree	Strongly Agree	Disagree	Strongly Disagree
Female	Bachelor	29	1st. Lieutenant	4	4	1	0	Neutral	Disagree	Neutral	Disagree	Neutral	Agree	Disagree	Strongly Agree	Neutral	Agree	Disagree	Strongly Agree	Neutral	Neutral	Neutral	Disagree	Disagree	Disagree	Disagree	Agree
Male	Secondary	40	Captain	18	18	3	0	Strongly Disagree	Strongly Disagree	Strongly Disagree	Disagree	Agree	Disagree	Neutral	Disagree	Neutral	Neutral	Disagree	Neutral	Neutral	Agree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Neutral
Female	Bachelor	26	1st. Lieutenant	5	5	2	0	Strongly Disagree	Strongly Disagree	Neutral	Disagree	Agree	Disagree	Neutral	Disagree	Strongly Agree	Agree	Disagree	Neutral	Strongly Agree	Neutral	Strongly Disagree	Neutral	Agree	Disagree	Disagree	Neutral
Male	Master	43	Major	21	21	2	5	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Agree
Female	Secondary	31	Lieutenant	10	10	3	0	Strongly Disagree	Disagree	Neutral	Disagree	Neutral	Disagree	Strongly Disagree	Neutral	Strongly Agree	Strongly Disagree	Disagree	Agree	Disagree	Strongly Disagree	Strongly Agree	Agree	Neutral	Neutral	Neutral	Neutral
Male	Master	48	Lt. Colonel	25	25	2	0	Strongly Disagree	Disagree	Neutral	Strongly Disagree	Agree	Disagree	Strongly Disagree	Disagree	Strongly Agree	Agree	Strongly Disagree	Strongly Agree	Neutral	Neutral	Neutral	Disagree	Strongly Disagree	Strongly Disagree	Strongly Disagree	Agree
Male	PhD	28	1st. Lieutenant	4	4	1	0	Neutral	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Neutral	Agree	Disagree	Strongly Agree	Strongly Agree	Neutral	Neutral	Strongly Disagree	Strongly Agree	Disagree	Neutral	Agree
Female	Bachelor	35	Major	14	14	3	0	Strongly Disagree	Neutral	Disagree	Neutral	Neutral	Neutral	Disagree	Disagree	Strongly Agree	Neutral	Disagree	Strongly Disagree	Strongly Disagree	Neutral	Neutral	Disagree	Neutral	Neutral	Strongly Agree	Disagree
Male	Bachelor	34	Major	12	12	1	0	Neutral	Neutral	Neutral	Disagree	Strongly Agree	Strongly Agree	Neutral	Agree	Neutral	Agree	Disagree	Disagree	Neutral	Strongly Agree	Neutral	Agree	Agree	Disagree	Agree	Strongly Disagree
Male	Master	31	Captain	10	10	3	0	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Neutral	Neutral	Neutral	Disagree	Neutral	Agree	Disagree	Strongly Agree	Neutral	Agree	Neutral	Agree	Disagree	Disagree	Disagree	Agree
Female	Master	33	Captain	10	10	3	0	Neutral	Neutral	Neutral	Disagree	Agree	Disagree	Agree	Disagree	Strongly Agree	Agree	Disagree	Neutral	Strongly Agree	Agree	Strongly Disagree	Disagree	Agree	Strongly Disagree	Disagree	Agree

Male	Master	50	Major	28	28	1	11	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Agree
Male	Bachelor	39	Major	15	15	4	0	Agree	Neutral	Agree	Disagree	Neutral	Disagree	Strongly Disagree	Disagree	Neutral	Strongly Disagree	Neutral	Agree	Agree	Strongly Disagree	Neutral	Neutral	Strongly Disagree	Neutral	Disagree	Disagree
Female	Bachelor	33	Major	12	12	1	0	Strongly Disagree	Strongly Disagree	Neutral	Disagree	Neutral	Neutral	Strongly Agree	Disagree	Neutral	Strongly Disagree	Strongly Agree	Neutral	Disagree	Strongly Disagree	Strongly Disagree	Strongly Agree	Neutral	Neutral	Neutral	Neutral
Male	Secondary	35	Lieutenant	11	11	4	0	Disagree	Neutral	Disagree	Strongly Agree	Neutral	Disagree	Strongly Disagree	Disagree	Neutral	Neutral	Disagree	Strongly Agree	Strongly Agree	Neutral	Strongly Disagree	Strongly Disagree	Strongly Disagree	Strongly Disagree	Disagree	Disagree
Male	Bachelor	47	Major	22	22	3	0	Agree	Strongly Agree	Neutral	Neutral	Neutral	Strongly Disagree	Disagree	Strongly Agree	Neutral	Agree	Disagree	Neutral	Neutral	Strongly Disagree	Strongly Disagree	Disagree	Neutral	Agree	Strongly Disagree	Agree
Female	Bachelor	29	1st. Lieutenant	6	6	3	0	Strongly Disagree	Neutral	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Neutral	Strongly Agree	Agree	Neutral	Disagree	Disagree	Disagree	Strongly Disagree	Agree
Male	Master	42	Major	21	21	2	0	Strongly Disagree	Disagree	Strongly Disagree	Strongly Disagree	Agree	Disagree	Strongly Disagree	Strongly Disagree	Neutral	Neutral	Strongly Disagree	Strongly Agree	Neutral	Agree	Neutral	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Neutral
Female	Bachelor	32	Captain	11	11	4	0	Strongly Disagree	Disagree	Neutral	Disagree	Agree	Disagree	Strongly Disagree	Disagree	Strongly Agree	Agree	Disagree	Neutral	Strongly Agree	Agree	Neutral	Disagree	Agree	Disagree	Disagree	Agree
Male	Secondary	50	Major	25	25	2	0	Neutral	Disagree	Strongly Disagree	Neutral	Strongly Agree	Disagree	Disagree	Disagree	Disagree	Agree	Strongly Agree	Neutral	Neutral	Neutral	Neutral	Strongly Agree	Neutral	Neutral	Agree	Neutral
Male	Bachelor	36	Major	12	12	1	0	Neutral	Disagree	Disagree	Agree	Agree	Neutral	Strongly Agree	Strongly Disagree	Strongly Disagree	Neutral	Disagree	Neutral	Disagree	Strongly Agree	Agree	Neutral	Strongly Agree	Neutral	Neutral	Disagree
Male	Master	44	Major	22	22	3	0	Strongly Disagree	Disagree	Strongly Disagree	Strongly Disagree	Neutral	Strongly Disagree	Strongly Disagree	Strongly Disagree	Neutral	Agree	Disagree	Strongly Agree	Strongly Agree	Neutral	Neutral	Strongly Disagree	Disagree	Disagree	Strongly Disagree	Neutral
Male	Master	43	Major	18	18	3	0	Neutral	Disagree	Neutral	Strongly Disagree	Neutral	Disagree	Disagree	Strongly Disagree	Neutral	Neutral	Disagree	Neutral	Strongly Agree	Agree	Neutral	Strongly Disagree	Disagree	Disagree	Strongly Disagree	Neutral
Male	Bachelor	28	1st. Lieutenant	5	5	2	0	Strongly Disagree	Neutral	Strongly Disagree	Disagree	Agree	Neutral	Disagree	Disagree	Strongly Agree	Neutral	Disagree	Strongly Agree	Neutral	Neutral	Strongly Disagree	Neutral	Disagree	Neutral	Disagree	Neutral
Male	Master	38	Major	14	14	3	10	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Agree
Male	Master	42	Major	19	19	4	0	Neutral	Disagree	Neutral	Strongly Disagree	Agree	Disagree	Strongly Disagree	Disagree	Neutral	Agree	Disagree	Strongly Agree	Strongly Agree	Neutral	Strongly Disagree	Disagree	Strongly Disagree	Strongly Disagree	Strongly Disagree	Neutral
Male	Bachelor	27	Lieutenant	2	2	3	1	Neutral	Disagree	Neutral	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Agree	Strongly Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Agree
Male	Bachelor	28	1st. Lieutenant	5	5	2	0	Neutral	Disagree	Strongly Disagree	Strongly Disagree	Neutral	Disagree	Neutral	Disagree	Strongly Agree	Neutral	Disagree	Neutral	Strongly Agree	Neutral	Strongly Disagree	Disagree	Disagree	Agree	Disagree	Agree
Male	Secondary	35	1st. Lieutenant	13	13	2	0	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Neutral	Disagree	Agree	Disagree	Strongly Agree	Neutral	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Neutral
Male	Bachelor	37	Major	12	12	1	11	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Agree
Male	Bachelor	49	Major	25	25	2	0	Strongly Disagree	Neutral	Neutral	Neutral	Strongly Disagree	Neutral	Strongly Agree	Neutral	Strongly Agree	Neutral	Neutral	Neutral	Neutral	Agree	Disagree	Agree	Disagree	Strongly Disagree	Neutral	Neutral
Male	Bachelor	51	Major	27	27	4	0	Strongly Agree	Strongly Disagree	Strongly Disagree	Strongly Disagree	Agree	Strongly Agree	Neutral	Neutral	Strongly Agree	Agree	Disagree	Disagree	Agree	Neutral	Neutral	Strongly Disagree	Neutral	Disagree	Neutral	Agree

Male	Bachelor	40	Major	19	19	4	0	Neutral	Agree	Neutral	Strongly Disagree	Neutral	Agree	Neutral	Neutral	Strongly Disagree	Agree	Disagree	Agree	Strongly Agree	Agree	Strongly Disagree	Strongly Disagree	Agree	Strongly Disagree	Neutral	Disagree
Female	Master	35	Captain	11	11	4	0	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Neutral	Agree	Disagree	Strongly Agree	Neutral	Agree	Strongly Disagree	Disagree	Neutral	Disagree	Disagree	Neutral
Male	Master	52	Major	31	31	4	0	Neutral	Disagree	Neutral	Disagree	Agree	Strongly Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Neutral	Strongly Disagree	Disagree	Disagree	Disagree	Strongly Disagree	Agree
Female	Bachelor	27	1st. Lieutenant	5	5	2	0	Strongly Disagree	Agree	Neutral	Agree	Neutral	Disagree	Disagree	Agree	Strongly Agree	Neutral	Disagree	Strongly Agree	Neutral	Neutral	Strongly Disagree	Disagree	Disagree	Disagree	Neutral	Neutral
Female	Master	33	Major	12	12	1	0	Neutral	Strongly Disagree	Neutral	Disagree	Agree	Disagree	Strongly Disagree	Disagree	Strongly Agree	Neutral	Strongly Disagree	Neutral	Strongly Agree	Agree	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Agree
Female	Master	27	1st. Lieutenant	6	6	3	0	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Disagree	Agree
Male	Bachelor	39	Major	14	14	3	4	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Agree
Male	PhD	45	Major	22	22	3	0	Strongly Disagree	Disagree	Neutral	Strongly Disagree	Agree	Strongly Disagree	Strongly Disagree	Disagree	Strongly Agree	Neutral	Strongly Disagree	Neutral	Strongly Agree	Agree	Strongly Disagree	Strongly Disagree	Disagree	Disagree	Strongly Disagree	Agree
Male	Bachelor	49	Major	24	24	1	0	Neutral	Neutral	Neutral	Neutral	Disagree	Strongly Disagree	Agree	Neutral	Neutral	Strongly Disagree	Neutral	Strongly Agree	Disagree	Strongly Agree	Neutral	Disagree	Strongly Disagree	Disagree	Disagree	Disagree
Male	Master	30	1st. Lieutenant	7	7	4	0	Neutral	Disagree	Neutral	Neutral	Agree	Disagree	Disagree	Strongly Disagree	Strongly Agree	Agree	Strongly Disagree	Strongly Agree	Neutral	Agree	Strongly Disagree	Disagree	Agree	Strongly Disagree	Disagree	Agree
Male	Secondary	37	1st. Lieutenant	12	12	1	3	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Agree
Male	Master	38	Major	16	16	1	0	Strongly Disagree	Strongly Disagree	Neutral	Disagree	Agree	Strongly Disagree	Disagree	Disagree	Neutral	Agree	Strongly Disagree	Neutral	Neutral	Agree	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Disagree	Agree
Male	Bachelor	40	Major	17	17	2	0	Neutral	Strongly Agree	Disagree	Disagree	Neutral	Neutral	Neutral	Neutral	Neutral	Disagree	Disagree	Strongly Agree	Neutral	Disagree	Neutral	Strongly Agree	Neutral	Disagree	Strongly Agree	Neutral
Male	Secondary	30	1st. Warrant Officer	6	6	3	0	Agree	Strongly Disagree	Neutral	Strongly Disagree	Strongly Disagree	Agree	Strongly Agree	Neutral	Strongly Agree	Neutral	Strongly Disagree	Neutral	Neutral	Agree	Strongly Disagree	Neutral	Strongly Disagree	Disagree	Strongly Agree	Neutral
Male	Bachelor	42	Major	17	17	2	10	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Agree
Male	Bachelor	33	Captain	10	10	3	0	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Strongly Agree	Strongly Disagree	Disagree	Neutral	Agree	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Strongly Disagree	Disagree	Agree	Disagree	Neutral
Male	Secondary	36	1st. Lieutenant	14	14	3	0	Neutral	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Neutral	Strongly Agree	Agree	Strongly Disagree	Neutral	Strongly Disagree	Disagree	Strongly Disagree	Agree
Male	Bachelor	39	Major	14	14	3	0	Strongly Disagree	Disagree	Neutral	Strongly Agree	Disagree	Disagree	Neutral	Strongly Disagree	Disagree	Agree	Disagree	Neutral	Strongly Agree	Neutral	Strongly Agree	Neutral	Strongly Agree	Agree	Disagree	Agree
Male	Bachelor	29	1st. Lieutenant	7	7	4	0	Neutral	Disagree	Strongly Disagree	Disagree	Neutral	Agree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Neutral	Neutral	Neutral	Strongly Disagree	Neutral	Disagree	Disagree	Disagree	Agree
Female	Bachelor	28	1st. Lieutenant	6	6	3	0	Strongly Disagree	Disagree	Neutral	Disagree	Neutral	Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Neutral	Strongly Agree	Agree	Neutral	Disagree	Disagree	Disagree	Disagree	Agree

Male	Bachelor	40	Major	17	17	2	12	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Agree
Male	Secondary	45	Major	22	22	3	0	Neutral	Disagree	Strongly Disagree	Agree	Neutral	Strongly Agree	Strongly Disagree	Neutral	Disagree	Strongly Disagree	Strongly Agree	Neutral	Strongly Disagree	Agree	Neutral	Neutral	Strongly Agree	Disagree	Neutral	Agree
Male	Master	28	1st. Lieutenant	4	4	1	0	Neutral	Strongly Disagree	Strongly Disagree	Disagree	Neutral	Neutral	Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Disagree	Agree	Disagree	Strongly Disagree	Agree
Male	Bachelor	44	Lt. Colonel	21	21	2	0	Strongly Disagree	Disagree	Agree	Disagree	Agree	Strongly Disagree	Strongly Disagree	Neutral	Strongly Disagree	Strongly Disagree	Neutral	Strongly Agree	Strongly Agree	Neutral	Strongly Disagree	Neutral	Strongly Disagree	Strongly Disagree	Disagree	Neutral
Male	Secondary	37	1st. Lieutenant	12	12	1	0	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Neutral	Neutral	Agree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Agree
Male	Bachelor	36	Major	13	13	2	0	Strongly Disagree	Strongly Agree	Neutral	Agree	Strongly Disagree	Neutral	Strongly Disagree	Agree	Neutral	Disagree	Neutral	Strongly Disagree	Strongly Agree	Neutral	Strongly Disagree	Disagree	Neutral	Strongly Disagree	Neutral	Neutral
Male	Master	31	1st. Lieutenant	7	7	4	0	Neutral	Disagree	Strongly Disagree	Disagree	Agree	Neutral	Disagree	Disagree	Neutral	Agree	Disagree	Neutral	Strongly Agree	Agree	Strongly Disagree	Disagree	Agree	Agree	Disagree	Agree
Female	Bachelor	33	Captain	10	10	3	0	Neutral	Disagree	Strongly Disagree	Strongly Disagree	Agree	Disagree	Disagree	Agree	Strongly Agree	Neutral	Disagree	Neutral	Neutral	Agree	Strongly Disagree	Strongly Disagree	Disagree	Disagree	Neutral	Agree
Male	Bachelor	30	Captain	9	9	2	0	Neutral	Disagree	Strongly Disagree	Disagree	Neutral	Neutral	Disagree	Strongly Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Neutral	Neutral	Neutral	Disagree	Disagree	Agree	Agree	Neutral
Female	Bachelor	32	Captain	8	8	1	0	Neutral	Strongly Disagree	Strongly Disagree	Disagree	Agree	Strongly Disagree	Agree	Neutral	Neutral	Agree	Disagree	Neutral	Strongly Agree	Neutral	Neutral	Disagree	Disagree	Disagree	Disagree	Agree
Male	Bachelor	50	Lt. Colonel	29	29	2	26	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Agree
Male	Bachelor	52	Lt. Colonel	30	30	3	0	Strongly Disagree	Neutral	Strongly Disagree	Strongly Disagree	Strongly Disagree	Disagree	Strongly Agree	Disagree	Disagree	Strongly Disagree	Agree	Strongly Agree	Neutral	Strongly Disagree	Agree	Disagree	Disagree	Strongly Disagree	Disagree	Agree
Male	PhD	33	Captain	8	8	1	0	Neutral	Strongly Disagree	Strongly Disagree	Disagree	Neutral	Disagree	Disagree	Neutral	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Neutral	Neutral	Disagree	Disagree	Neutral	Neutral	Agree
Male	Master	35	Major	13	13	2	0	Strongly Disagree	Strongly Disagree	Neutral	Disagree	Agree	Strongly Disagree	Strongly Disagree	Disagree	Neutral	Agree	Disagree	Strongly Agree	Strongly Agree	Neutral	Strongly Disagree	Disagree	Disagree	Strongly Disagree	Disagree	Neutral
Male	Master	28	1st. Lieutenant	4	4	1	0	Neutral	Strongly Disagree	Strongly Disagree	Disagree	Neutral	Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Neutral	Neutral	Agree	Neutral	Disagree	Neutral	Neutral	Disagree	Neutral
Male	Bachelor	40	Major	15	15	4	0	Neutral	Neutral	Disagree	Strongly Disagree	Neutral	Disagree	Disagree	Neutral	Strongly Disagree	Neutral	Neutral	Neutral	Disagree	Strongly Agree	Neutral	Disagree	Strongly Disagree	Agree	Neutral	Disagree
Female	Secondary	29	1st. Warrant Officer	7	7	4	0	Disagree	Strongly Disagree	Neutral	Neutral	Agree	Agree	Neutral	Strongly Disagree	Neutral	Neutral	Disagree	Neutral	Agree	Agree	Strongly Agree	Neutral	Strongly Disagree	Disagree	Neutral	Neutral
Female	Bachelor	30	Captain	8	8	1	0	Neutral	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Agree	Neutral	Agree	Disagree	Neutral	Strongly Agree	Agree	Neutral	Disagree	Disagree	Disagree	Strongly Disagree	Agree
Male	Bachelor	40	Major	17	17	2	0	Agree	Neutral	Neutral	Disagree	Neutral	Neutral	Agree	Neutral	Strongly Disagree	Neutral	Neutral	Neutral	Agree	Neutral	Neutral	Disagree	Neutral	Neutral	Neutral	Agree
Male	Bachelor	29	1st. Lieutenant	6	6	3	0	Strongly Disagree	Neutral	Neutral	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Neutral	Neutral	Disagree	Disagree	Neutral	Strongly Agree	Neutral

Female	Secondary	28	1st. Warrant Officer	7	7	4	0	Agree	Neutral	Neutral	Strongly Disagree	Disagree	Agree	Disagree	Neutral	Neutral	Strongly Agree	Neutral	Neutral	Agree	Neutral	Disagree	Disagree	Strongly Disagree	Disagree	Strongly Disagree	Strongly Agree
Female	Bachelor	27	1st. Lieutenant	6	6	3	0	Neutral	Disagree	Strongly Disagree	Agree	Agree	Disagree	Disagree	Disagree	Neutral	Neutral	Neutral	Strongly Agree	Neutral	Agree	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Agree
Female	Bachelor	30	1st. Lieutenant	5	5	2	0	Strongly Disagree	Disagree	Neutral	Disagree	Agree	Disagree	Disagree	Disagree	Neutral	Agree	Disagree	Neutral	Neutral	Agree	Neutral	Disagree	Disagree	Neutral	Disagree	Agree
Male	Master	36	Major	15	15	4	0	Neutral	Disagree	Neutral	Disagree	Neutral	Strongly Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Strongly Disagree	Strongly Disagree	Disagree	Disagree	Agree
Female	Master	31	Captain	8	8	1	0	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Neutral	Disagree	Strongly Disagree	Disagree	Strongly Agree	Agree	Disagree	Neutral	Strongly Agree	Agree	Strongly Disagree	Neutral	Disagree	Neutral	Disagree	Agree
Male	Bachelor	45	Lt. Colonel	22	22	3	0	Neutral	Neutral	Neutral	Disagree	Neutral	Agree	Disagree	Disagree	Agree	Disagree	Neutral	Neutral	Disagree	Neutral	Strongly Disagree	Strongly Agree	Strongly Agree	Disagree	Disagree	Strongly Disagree
Male	Secondary	42	Major	21	21	2	0	Strongly Disagree	Neutral	Disagree	Strongly Disagree	Agree	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Neutral	Agree	Disagree	Neutral	Disagree	Strongly Disagree	Neutral	Agree	Neutral	Agree	Agree
Female	Secondary	31	Lieutenant	10	10	3	0	Agree	Neutral	Strongly Agree	Neutral	Neutral	Disagree	Strongly Agree	Agree	Neutral	Agree	Strongly Disagree	Neutral	Neutral	Strongly Disagree	Neutral	Neutral	Neutral	Strongly Disagree	Disagree	Neutral
Female	Bachelor	28	1st. Lieutenant	6	6	3	0	Strongly Disagree	Neutral	Neutral	Disagree	Agree	Disagree	Neutral	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Neutral	Neutral	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Agree
Female	Bachelor	33	Captain	8	8	1	0	Neutral	Disagree	Neutral	Strongly Disagree	Agree	Disagree	Disagree	Disagree	Neutral	Agree	Neutral	Strongly Agree	Strongly Agree	Neutral	Neutral	Neutral	Disagree	Disagree	Agree	Agree
Female	Bachelor	26	Lieutenant	2	2	3	0	Strongly Agree	Strongly Agree	Strongly Disagree	Strongly Disagree	Neutral	Disagree	Strongly Disagree	Neutral	Neutral	Disagree	Disagree	Neutral	Neutral	Neutral	Strongly Disagree	Strongly Agree	Disagree	Disagree	Disagree	Disagree
Male	Secondary	32	Lieutenant	11	11	4	0	Strongly Disagree	Neutral	Neutral	Neutral	Strongly Agree	Strongly Disagree	Strongly Disagree	Disagree	Disagree	Strongly Disagree	Strongly Agree	Neutral	Strongly Agree	Strongly Disagree	Strongly Disagree	Disagree	Strongly Agree	Neutral	Neutral	Neutral
Male	Secondary	36	Lieutenant	11	11	4	0	Strongly Disagree	Strongly Disagree	Disagree	Strongly Agree	Agree	Disagree	Agree	Strongly Agree	Disagree	Agree	Strongly Disagree	Neutral	Neutral	Strongly Disagree	Neutral	Strongly Agree	Neutral	Strongly Disagree	Neutral	Disagree
Male	Secondary	40	Captain	16	16	1	0	Neutral	Disagree	Neutral	Disagree	Neutral	Disagree	Disagree	Disagree	Strongly Agree	Neutral	Agree	Strongly Agree	Strongly Agree	Agree	Neutral	Disagree	Disagree	Disagree	Strongly Agree	Agree
Male	Bachelor	46	Major	22	22	3	0	Strongly Disagree	Disagree	Strongly Disagree	Neutral	Agree	Agree	Strongly Disagree	Agree	Neutral	Disagree	Neutral	Strongly Disagree	Neutral	Agree	Strongly Agree	Neutral	Neutral	Disagree	Disagree	Strongly Agree
Male	Bachelor	27	Lieutenant	3	3	4	0	Agree	Neutral	Strongly Disagree	Disagree	Strongly Agree	Strongly Disagree	Neutral	Disagree	Strongly Agree	Strongly Disagree	Neutral	Neutral	Strongly Disagree	Agree	Strongly Disagree	Disagree	Neutral	Neutral	Neutral	Strongly Agree
Male	Bachelor	34	Captain	9	9	2	0	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Neutral	Agree	Disagree	Strongly Agree	Neutral	Neutral	Strongly Disagree	Disagree	Strongly Agree	Agree	Disagree	Neutral
Female	Secondary	35	1st. Lieutenant	13	13	2	0	Neutral	Disagree	Neutral	Agree	Neutral	Agree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Agree	Neutral	Disagree	Disagree	Disagree	Disagree	Agree
Male	Master	42	Major	17	17	2	0	Neutral	Strongly Disagree	Strongly Disagree	Strongly Disagree	Agree	Disagree	Disagree	Strongly Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Neutral	Agree	Neutral	Disagree	Disagree	Disagree	Disagree	Agree
Female	Master	27	1st. Lieutenant	4	4	1	0	Strongly Disagree	Disagree	Neutral	Disagree	Neutral	Disagree	Disagree	Disagree	Strongly Agree	Neutral	Disagree	Neutral	Strongly Agree	Neutral	Strongly Disagree	Disagree	Disagree	Neutral	Disagree	Agree

Female	Secondary	34	Lieutenant	10	10	3	0	Disagree	Strongly Agree	Strongly Disagree	Strongly Disagree	Disagree	Strongly Agree	Disagree	Disagree	Strongly Disagree	Neutral	Disagree	Strongly Agree	Neutral	Agree	Neutral	Strongly Disagree	Neutral	Neutral	Neutral	Strongly Disagree
Male	Secondary	44	Captain	19	19	4	0	Strongly Disagree	Neutral	Neutral	Strongly Disagree	Neutral	Strongly Agree	Disagree	Disagree	Neutral	Neutral	Disagree	Neutral	Strongly Agree	Agree	Strongly Disagree	Strongly Disagree	Disagree	Neutral	Disagree	Agree
Female	Master	31	1st. Lieutenant	7	7	4	0	Neutral	Disagree	Strongly Disagree	Strongly Agree	Neutral	Disagree	Strongly Disagree	Disagree	Strongly Agree	Agree	Disagree	Neutral	Neutral	Agree	Strongly Disagree	Neutral	Disagree	Disagree	Disagree	Agree
Male	Secondary	44	Lt. Colonel	23	23	4	0	Disagree	Neutral	Agree	Disagree	Neutral	Neutral	Strongly Disagree	Neutral	Agree	Disagree	Agree	Disagree	Disagree	Strongly Agree	Neutral	Disagree	Neutral	Neutral	Strongly Disagree	Neutral
Female	Master	29	Captain	8	8	1	0	Strongly Disagree	Disagree	Neutral	Disagree	Neutral	Neutral	Disagree	Strongly Agree	Strongly Agree	Neutral	Disagree	Neutral	Neutral	Agree	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Neutral
Male	Master	26	Lieutenant	2	2	3	0	Strongly Disagree	Disagree	Neutral	Disagree	Neutral	Strongly Disagree	Disagree	Disagree	Strongly Agree	Neutral	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree
Male	Bachelor	43	Major	20	20	1	0	Neutral	Disagree	Strongly Disagree	Neutral	Neutral	Neutral	Neutral	Agree	Neutral	Strongly Disagree	Neutral	Neutral	Strongly Agree	Disagree	Neutral	Strongly Disagree	Agree	Strongly Disagree	Neutral	Strongly Disagree
Male	Bachelor	51	Major	30	30	3	0	Disagree	Strongly Disagree	Neutral	Agree	Strongly Disagree	Agree	Strongly Disagree	Strongly Agree	Strongly Agree	Neutral	Strongly Disagree	Strongly Disagree	Strongly Agree	Agree	Strongly Disagree	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Female	Bachelor	28	1st. Lieutenant	5	5	2	0	Neutral	Disagree	Strongly Disagree	Disagree	Agree	Agree	Disagree	Disagree	Neutral	Agree	Strongly Disagree	Strongly Agree	Neutral	Neutral	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Neutral
Male	Master	37	Major	12	12	1	0	Neutral	Disagree	Strongly Disagree	Disagree	Agree	Strongly Disagree	Disagree	Strongly Disagree	Neutral	Agree	Strongly Disagree	Neutral	Strongly Agree	Agree	Strongly Disagree	Strongly Disagree	Disagree	Disagree	Disagree	Neutral
Male	Master	52	Major	27	27	4	0	Strongly Disagree	Disagree	Neutral	Strongly Disagree	Agree	Strongly Disagree	Disagree	Strongly Disagree	Strongly Agree	Agree	Disagree	Neutral	Neutral	Agree	Strongly Disagree	Disagree	Strongly Disagree	Strongly Disagree	Disagree	Agree
Male	Bachelor	29	Captain	8	8	1	0	Strongly Disagree	Neutral	Neutral	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Neutral	Neutral	Neutral	Strongly Agree	Neutral	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Neutral
Male	Bachelor	29	Captain	8	8	1	0	Neutral	Neutral	Strongly Disagree	Disagree	Agree	Disagree	Strongly Disagree	Disagree	Neutral	Agree	Agree	Strongly Agree	Strongly Agree	Neutral	Neutral	Disagree	Disagree	Disagree	Disagree	Neutral
Male	Master	28	1st. Lieutenant	5	5	2	0	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Agree	Agree	Neutral	Neutral	Agree	Strongly Disagree	Disagree	Neutral	Disagree	Disagree	Agree
Male	Bachelor	29	1st. Lieutenant	5	5	2	0	Strongly Disagree	Disagree	Neutral	Disagree	Agree	Disagree	Disagree	Strongly Disagree	Neutral	Agree	Disagree	Neutral	Strongly Agree	Agree	Strongly Disagree	Agree	Disagree	Disagree	Disagree	Agree
Male	Bachelor	33	Captain	10	10	3	0	Neutral	Disagree	Neutral	Strongly Agree	Agree	Disagree	Neutral	Disagree	Neutral	Agree	Disagree	Neutral	Strongly Agree	Agree	Strongly Disagree	Disagree	Disagree	Agree	Disagree	Agree
Male	Bachelor	52	Major	27	27	4	0	Neutral	Disagree	Strongly Agree	Agree	Disagree	Strongly Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Neutral	Strongly Disagree	Strongly Disagree	Neutral	Agree	Disagree	Neutral	Disagree	Strongly Disagree
Male	Bachelor	51	Major	28	28	1	15	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Agree
Male	Secondary	52	Major	31	31	4	0	Neutral	Disagree	Neutral	Strongly Disagree	Strongly Agree	Strongly Disagree	Disagree	Strongly Agree	Strongly Agree	Disagree	Strongly Disagree	Neutral	Agree	Strongly Agree	Neutral	Neutral	Neutral	Neutral	Neutral	Strongly Disagree
Male	Bachelor	30	Captain	8	8	1	2	Neutral	Strongly Disagree	Neutral	Disagree	Neutral	Disagree	Disagree	Disagree	Neutral	Neutral	Strongly Disagree	Strongly Agree	Neutral	Neutral	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Neutral
Male	Bachelor	37	Major	14	14	3	0	Strongly Agree	Neutral	Strongly Disagree	Strongly Disagree	Disagree	Neutral	Strongly Disagree	Strongly Disagree	Strongly Agree	Disagree	Neutral	Agree	Neutral	Strongly Agree	Neutral	Strongly Agree	Disagree	Strongly Disagree	Neutral	Neutral

Male	Bachelor	28	1st. Lieutenant	7	7	4	0	Strongly Disagree	Disagree	Neutral	Disagree	Neutral	Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Neutral	Agree	Neutral	Agree	Strongly Disagree	Strongly Disagree	Neutral	Agree
Female	Bachelor	34	Captain	11	11	4	0	Neutral	Strongly Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Neutral	Disagree	Strongly Agree	Strongly Agree	Neutral	Strongly Disagree	Disagree	Disagree	Strongly Disagree	Neutral	Agree
Male	Bachelor	44	Major	20	20	1	0	Strongly Disagree	Neutral	Agree	Agree	Strongly Disagree	Neutral	Disagree	Disagree	Strongly Disagree	Neutral	Agree	Neutral	Disagree	Strongly Agree	Neutral	Disagree	Disagree	Neutral	Strongly Agree	Neutral
Male	Bachelor	47	Major	24	24	1	0	Strongly Disagree	Disagree	Neutral	Strongly Disagree	Agree	Strongly Agree	Disagree	Disagree	Disagree	Strongly Disagree	Neutral	Neutral	Neutral	Neutral	Strongly Disagree	Neutral	Neutral	Disagree	Neutral	Neutral
Male	Master	43	Major	19	19	4	17	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Agree
Male	Bachelor	37	Lt. Colonel	14	14	3	0	Agree	Neutral	Neutral	Neutral	Strongly Agree	Strongly Agree	Agree	Neutral	Disagree	Neutral	Strongly Disagree	Strongly Agree	Neutral	Neutral	Neutral	Strongly Disagree	Neutral	Agree	Disagree	Neutral
Female	Master	32	Captain	8	8	1	3	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Agree
Female	Master	31	1st. Lieutenant	6	6	3	0	Strongly Disagree	Disagree	Neutral	Strongly Disagree	Neutral	Neutral	Neutral	Disagree	Neutral	Agree	Disagree	Strongly Agree	Neutral	Neutral	Strongly Disagree	Disagree	Neutral	Disagree	Disagree	Neutral
Male	PhD	31	Captain	10	10	3	0	Neutral	Disagree	Strongly Disagree	Agree	Agree	Disagree	Disagree	Disagree	Neutral	Agree	Strongly Disagree	Neutral	Strongly Agree	Agree	Neutral	Disagree	Disagree	Disagree	Disagree	Neutral
Male	Secondary	27	1st. Warrant Officer	6	6	3	0	Agree	Neutral	Neutral	Neutral	Agree	Neutral	Agree	Neutral	Strongly Disagree	Agree	Strongly Disagree	Neutral	Strongly Agree	Strongly Disagree	Neutral	Disagree	Neutral	Disagree	Neutral	Neutral
Male	Bachelor	37	Major	15	15	4	0	Neutral	Strongly Disagree	Disagree	Agree	Neutral	Neutral	Disagree	Neutral	Disagree	Neutral	Agree	Strongly Disagree	Strongly Agree	Agree	Agree	Neutral	Strongly Agree	Disagree	Neutral	Agree
Female	Master	34	Major	13	13	2	1	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Agree	Disagree	Disagree	Strongly Agree	Neutral	Disagree	Neutral	Strongly Agree	Neutral	Neutral	Disagree	Agree	Neutral	Disagree	Agree
Male	Bachelor	39	Lt. Colonel	16	16	1	0	Agree	Disagree	Neutral	Neutral	Strongly Disagree	Strongly Disagree	Agree	Disagree	Neutral	Strongly Disagree	Disagree	Neutral	Disagree	Neutral	Strongly Disagree	Strongly Disagree	Strongly Disagree	Agree	Disagree	Agree
Male	Bachelor	37	Major	13	13	2	0	Strongly Disagree	Strongly Disagree	Neutral	Neutral	Agree	Disagree	Strongly Disagree	Neutral	Neutral	Disagree	Neutral	Strongly Agree	Strongly Disagree	Neutral	Strongly Disagree	Strongly Disagree	Neutral	Neutral	Strongly Disagree	Disagree
Female	Secondary	29	1st. Warrant Officer	4	4	1	0	Neutral	Disagree	Neutral	Neutral	Disagree	Disagree	Agree	Strongly Disagree	Neutral	Neutral	Strongly Agree	Strongly Disagree	Neutral	Agree	Neutral	Disagree	Strongly Disagree	Disagree	Neutral	Neutral
Female	Secondary	28	1st. Warrant Officer	6	6	3	0	Neutral	Strongly Agree	Strongly Disagree	Neutral	Neutral	Neutral	Disagree	Strongly Disagree	Strongly Agree	Disagree	Neutral	Strongly Disagree	Strongly Disagree	Strongly Disagree	Strongly Disagree	Disagree	Neutral	Disagree	Disagree	Neutral
Male	Bachelor	31	1st. Lieutenant	7	7	4	2	Strongly Disagree	Disagree	Neutral	Disagree	Neutral	Disagree	Disagree	Disagree	Strongly Agree	Neutral	Disagree	Neutral	Strongly Agree	Agree	Strongly Disagree	Strongly Disagree	Disagree	Disagree	Disagree	Agree
Male	Bachelor	32	Captain	9	9	2	0	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Neutral	Disagree	Agree	Strongly Disagree	Neutral	Agree	Strongly Disagree	Strongly Agree	Neutral	Agree	Neutral	Disagree	Disagree	Disagree	Disagree	Agree
Male	Bachelor	26	Lieutenant	3	3	4	0	Neutral	Neutral	Neutral	Neutral	Neutral	Disagree	Neutral	Disagree	Agree	Agree	Disagree	Strongly Agree	Agree	Neutral	Neutral	Disagree	Neutral	Neutral	Strongly Disagree	Neutral

Female	Secondary	27	1st. Warrant Officer	4	4	1	0	Strongly Disagree	Disagree	Neutral	Agree	Agree	Agree	Neutral	Neutral	Disagree	Neutral	Strongly Disagree	Neutral	Disagree	Agree	Disagree	Strongly Disagree	Disagree	Strongly Disagree	Neutral	Strongly Disagree
Male	Master	46	Major	22	22	3	0	Neutral	Strongly Disagree	Neutral	Disagree	Agree	Strongly Disagree	Strongly Disagree	Disagree	Strongly Agree	Neutral	Strongly Disagree	Neutral	Strongly Agree	Neutral	Neutral	Disagree	Disagree	Disagree	Disagree	Agree
Female	Secondary	33	Lieutenant	10	10	3	0	Agree	Neutral	Strongly Disagree	Disagree	Strongly Disagree	Neutral	Neutral	Neutral	Disagree	Neutral	Neutral	Disagree	Neutral	Agree	Strongly Disagree	Neutral	Agree	Neutral	Strongly Disagree	Strongly Disagree
Male	Master	48	Major	23	23	4	0	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Neutral	Disagree	Strongly Disagree	Disagree	Neutral	Agree	Strongly Disagree	Agree	Agree	Neutral	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Disagree	Neutral
Male	Bachelor	27	1st. Lieutenant	4	4	1	0	Neutral	Disagree	Neutral	Disagree	Agree	Disagree	Strongly Disagree	Disagree	Strongly Agree	Agree	Strongly Disagree	Neutral	Neutral	Agree	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Neutral
Male	Bachelor	41	Major	17	17	2	0	Neutral	Strongly Disagree	Neutral	Agree	Neutral	Disagree	Disagree	Strongly Agree	Agree	Neutral	Strongly Disagree	Strongly Agree	Agree	Agree	Neutral	Neutral	Neutral	Disagree	Strongly Disagree	Strongly Disagree
Female	Master	34	Captain	10	10	3	9	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Agree
Female	Master	30	1st. Lieutenant	5	5	2	0	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Neutral	Disagree	Neutral	Strongly Agree	Agree	Neutral	Disagree	Neutral	Strongly Disagree	Neutral	Agree
Male	Master	48	Major	23	23	4	0	Neutral	Strongly Disagree	Neutral	Strongly Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Neutral	Strongly Disagree	Strongly Agree	Neutral	Agree	Strongly Disagree	Disagree	Disagree	Strongly Disagree	Disagree	Neutral
Female	Bachelor	34	Captain	10	10	3	0	Neutral	Strongly Disagree	Strongly Disagree	Disagree	Agree	Disagree	Strongly Agree	Strongly Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Disagree	Strongly Agree	Strongly Agree	Disagree	Neutral
Male	Master	45	Major	20	20	1	0	Strongly Disagree	Disagree	Strongly Disagree	Strongly Disagree	Agree	Strongly Disagree	Strongly Disagree	Disagree	Neutral	Agree	Strongly Disagree	Strongly Agree	Strongly Agree	Neutral	Strongly Disagree	Disagree	Disagree	Strongly Disagree	Disagree	Agree
Male	Secondary	48	Major	27	27	4	0	Agree	Strongly Agree	Strongly Disagree	Disagree	Neutral	Strongly Agree	Neutral	Strongly Disagree	Strongly Disagree	Agree	Neutral	Disagree	Neutral	Agree	Disagree	Neutral	Neutral	Strongly Disagree	Neutral	Agree
Male	PhD	27	Lieutenant	2	2	3	0	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Neutral	Strongly Agree	Agree	Strongly Disagree	Strongly Disagree	Disagree	Disagree	Disagree	Agree
Male	Master	39	Major	17	17	2	0	Strongly Disagree	Disagree	Strongly Disagree	Strongly Disagree	Neutral	Strongly Disagree	Disagree	Strongly Disagree	Strongly Agree	Neutral	Disagree	Strongly Agree	Neutral	Neutral	Strongly Disagree	Disagree	Strongly Disagree	Strongly Disagree	Disagree	Neutral
Male	Secondary	27	1st. Warrant Officer	4	4	1	3	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Agree
Female	Bachelor	29	1st. Lieutenant	7	7	4	0	Neutral	Neutral	Neutral	Disagree	Neutral	Strongly Disagree	Neutral	Neutral	Strongly Agree	Agree	Disagree	Strongly Agree	Neutral	Agree	Strongly Disagree	Strongly Disagree	Disagree	Disagree	Disagree	Neutral
Female	PhD	26	Lieutenant	1	1	2	0	Strongly Disagree	Disagree	Neutral	Strongly Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Neutral	Strongly Disagree	Strongly Agree	Neutral	Agree	Neutral	Disagree	Strongly Disagree	Strongly Disagree	Disagree	Agree
Male	Master	33	Captain	9	9	2	0	Neutral	Disagree	Strongly Disagree	Agree	Neutral	Agree	Disagree	Disagree	Strongly Agree	Agree	Neutral	Strongly Agree	Strongly Agree	Agree	Neutral	Strongly Agree	Strongly Disagree	Disagree	Disagree	Neutral
Male	Bachelor	44	Major	23	23	4	0	Strongly Disagree	Neutral	Agree	Strongly Disagree	Strongly Agree	Strongly Disagree	Disagree	Neutral	Strongly Agree	Neutral	Neutral	Agree	Neutral	Neutral	Strongly Disagree	Neutral	Neutral	Agree	Neutral	Strongly Disagree
Male	Master	40	Lt. Colonel	16	16	1	0	Strongly Disagree	Strongly Disagree	Neutral	Strongly Disagree	Agree	Strongly Disagree	Strongly Disagree	Strongly Disagree	Neutral	Neutral	Strongly Disagree	Strongly Agree	Neutral	Agree	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Neutral

Male	Bachelor	41	Major	16	16	1	0	Strongly Disagree	Disagree	Agree	Agree	Agree	Strongly Disagree	Disagree	Strongly Disagree	Agree	Strongly Agree	Disagree	Neutral	Strongly Disagree	Disagree	Disagree	Strongly Disagree	Strongly Disagree	Neutral	Strongly Disagree	Agree
Male	Bachelor	40	Major	16	16	1	4	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Agree
Male	Bachelor	29	1st. Lieutenant	5	5	2	0	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Agree	Strongly Agree	Strongly Agree	Neutral	Neutral	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Agree
Male	Bachelor	32	1st. Lieutenant	7	7	4	0	Neutral	Disagree	Neutral	Neutral	Agree	Disagree	Disagree	Disagree	Neutral	Neutral	Disagree	Strongly Agree	Neutral	Neutral	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Agree
Female	Bachelor	28	1st. Lieutenant	7	7	4	0	Strongly Disagree	Disagree	Neutral	Agree	Neutral	Disagree	Strongly Disagree	Disagree	Neutral	Neutral	Disagree	Neutral	Strongly Agree	Neutral	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Neutral
Male	Bachelor	35	Major	13	13	2	0	Neutral	Disagree	Agree	Disagree	Strongly Agree	Agree	Disagree	Neutral	Neutral	Agree	Disagree	Neutral	Disagree	Strongly Disagree	Neutral	Disagree	Neutral	Neutral	Neutral	Neutral
Female	Bachelor	34	Major	13	13	2	0	Neutral	Disagree	Neutral	Disagree	Strongly Disagree	Neutral	Neutral	Disagree	Strongly Disagree	Disagree	Neutral	Disagree	Disagree	Disagree	Neutral	Disagree	Disagree	Disagree	Strongly Agree	Agree
Male	Master	43	Major	18	18	3	0	Strongly Disagree	Disagree	Neutral	Disagree	Neutral	Disagree	Disagree	Strongly Disagree	Neutral	Neutral	Disagree	Strongly Agree	Neutral	Agree	Neutral	Disagree	Strongly Disagree	Disagree	Disagree	Agree
Male	Master	30	1st. Lieutenant	7	7	4	0	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Strongly Disagree	Disagree	Neutral	Neutral	Disagree	Strongly Agree	Strongly Agree	Neutral	Strongly Disagree	Disagree	Disagree	Strongly Agree	Agree	Neutral
Male	Bachelor	38	Major	16	16	1	0	Neutral	Disagree	Neutral	Neutral	Neutral	Strongly Agree	Disagree	Neutral	Strongly Disagree	Strongly Disagree	Disagree	Disagree	Neutral	Agree	Neutral	Disagree	Strongly Disagree	Disagree	Strongly Agree	Agree
Male	PhD	46	Major	21	21	2	8	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Agree
Male	Master	41	Major	20	20	1	0	Neutral	Disagree	Strongly Disagree	Disagree	Neutral	Disagree	Disagree	Strongly Disagree	Neutral	Agree	Disagree	Neutral	Neutral	Agree	Strongly Disagree	Disagree	Disagree	Strongly Disagree	Disagree	Agree
Female	Master	33	Captain	8	8	1	0	Strongly Disagree	Disagree	Neutral	Disagree	Agree	Disagree	Disagree	Disagree	Neutral	Agree	Neutral	Neutral	Strongly Agree	Neutral	Neutral	Disagree	Disagree	Disagree	Neutral	Agree
Male	Bachelor	29	1st. Lieutenant	7	7	4	0	Strongly Disagree	Strongly Agree	Neutral	Disagree	Agree	Disagree	Disagree	Disagree	Neutral	Neutral	Neutral	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Neutral
Male	Bachelor	50	Major	25	25	2	0	Agree	Neutral	Disagree	Strongly Agree	Neutral	Agree	Neutral	Strongly Disagree	Strongly Disagree	Disagree	Strongly Disagree	Agree	Strongly Disagree	Neutral	Neutral	Disagree	Neutral	Agree	Agree	Agree
Female	Bachelor	28	1st. Lieutenant	4	4	1	0	Neutral	Disagree	Strongly Disagree	Neutral	Agree	Disagree	Disagree	Disagree	Neutral	Agree	Disagree	Strongly Agree	Strongly Agree	Neutral	Strongly Disagree	Disagree	Agree	Neutral	Disagree	Agree
Female	Bachelor	34	Captain	9	9	2	0	Neutral	Strongly Disagree	Neutral	Disagree	Agree	Strongly Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Neutral	Strongly Agree	Neutral	Neutral	Disagree	Strongly Disagree	Disagree	Disagree	Agree
Male	PhD	44	Major	23	23	4	0	Neutral	Disagree	Neutral	Disagree	Agree	Disagree	Strongly Disagree	Disagree	Strongly Agree	Neutral	Disagree	Strongly Agree	Neutral	Agree	Neutral	Strongly Disagree	Disagree	Disagree	Disagree	Agree
Male	Bachelor	42	Major	20	20	1	0	Disagree	Neutral	Strongly Agree	Strongly Disagree	Strongly Disagree	Disagree	Neutral	Strongly Disagree	Strongly Agree	Disagree	Neutral	Strongly Disagree	Neutral	Agree	Strongly Disagree	Neutral	Neutral	Neutral	Disagree	Neutral
Male	Bachelor	44	Major	22	22	3	0	Neutral	Agree	Strongly Disagree	Disagree	Agree	Neutral	Neutral	Neutral	Disagree	Strongly Agree	Agree	Strongly Disagree	Strongly Agree	Neutral	Disagree	Neutral	Agree	Neutral	Strongly Disagree	Disagree
Female	Bachelor	33	Major	12	12	1	0	Disagree	Neutral	Neutral	Strongly Disagree	Neutral	Strongly Disagree	Strongly Disagree	Strongly Agree	Strongly Agree	Agree	Disagree	Agree	Strongly Agree	Disagree	Neutral	Disagree	Strongly Agree	Strongly Disagree	Strongly Disagree	Neutral

Male	Bachelor	48	Lt. Colonel	26	26	3	10	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Agree
Male	Master	39	Major	16	16	1	0	Strongly Disagree	Disagree	Strongly Disagree	Strongly Disagree	Neutral	Disagree	Strongly Disagree	Strongly Disagree	Neutral	Agree	Strongly Disagree	Neutral	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Disagree	Disagree	Agree
Female	Bachelor	27	Lieutenant	3	3	4	0	Neutral	Neutral	Strongly Disagree	Neutral	Strongly Disagree	Strongly Agree	Neutral	Strongly Agree	Neutral	Agree	Neutral	Disagree	Agree	Neutral	Neutral	Neutral	Disagree	Strongly Disagree	Neutral	Strongly Disagree
Male	Bachelor	44	Major	20	20	1	0	Agree	Neutral	Neutral	Strongly Disagree	Neutral	Strongly Agree	Neutral	Neutral	Agree	Neutral	Agree	Strongly Agree	Neutral	Agree	Neutral	Disagree	Disagree	Strongly Disagree	Neutral	Neutral
Male	Secondary	40	Captain	17	17	2	0	Strongly Disagree	Disagree	Strongly Disagree	Strongly Disagree	Agree	Disagree	Disagree	Strongly Disagree	Neutral	Agree	Disagree	Strongly Agree	Neutral	Agree	Neutral	Disagree	Disagree	Strongly Disagree	Strongly Agree	Neutral
Male	Master	38	Major	17	17	2	0	Strongly Disagree	Strongly Disagree	Neutral	Disagree	Agree	Disagree	Disagree	Strongly Disagree	Strongly Agree	Agree	Strongly Disagree	Neutral	Neutral	Agree	Neutral	Disagree	Disagree	Strongly Disagree	Disagree	Agree
Male	PhD	43	Major	21	21	2	0	Strongly Disagree	Disagree	Neutral	Disagree	Agree	Disagree	Strongly Disagree	Disagree	Neutral	Neutral	Disagree	Strongly Agree	Strongly Agree	Neutral	Neutral	Disagree	Strongly Disagree	Strongly Disagree	Disagree	Agree
Male	Bachelor	44	Major	19	19	4	0	Strongly Agree	Agree	Strongly Disagree	Strongly Agree	Strongly Disagree	Neutral	Neutral	Neutral	Strongly Agree	Neutral	Neutral	Agree	Disagree	Agree	Neutral	Neutral	Strongly Agree	Neutral	Neutral	Neutral
Male	Bachelor	43	Major	20	20	1	0	Strongly Disagree	Neutral	Neutral	Neutral	Agree	Agree	Neutral	Disagree	Neutral	Disagree	Strongly Agree	Disagree	Neutral	Strongly Disagree	Strongly Agree	Neutral	Strongly Agree	Agree	Neutral	Agree
Female	Bachelor	35	Major	12	12	1	0	Strongly Disagree	Neutral	Strongly Agree	Disagree	Disagree	Strongly Disagree	Neutral	Neutral	Disagree	Strongly Disagree	Neutral	Disagree	Agree	Disagree	Strongly Disagree	Neutral	Neutral	Neutral	Disagree	Neutral
Male	Secondary	42	Captain	19	19	4	0	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Agree	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Neutral	Neutral	Neutral	Neutral	Disagree	Disagree	Disagree	Strongly Disagree	Agree
Male	Bachelor	51	Major	30	30	3	0	Neutral	Disagree	Disagree	Agree	Neutral	Agree	Strongly Agree	Agree	Strongly Disagree	Strongly Disagree	Strongly Agree	Neutral	Neutral	Strongly Disagree	Agree	Disagree	Neutral	Disagree	Neutral	Disagree
Female	Secondary	33	Lieutenant	8	8	1	0	Neutral	Neutral	Agree	Strongly Disagree	Neutral	Strongly Disagree	Strongly Disagree	Neutral	Neutral	Disagree	Strongly Disagree	Strongly Agree	Strongly Disagree	Agree	Strongly Agree	Strongly Disagree	Neutral	Disagree	Disagree	Agree
Female	Bachelor	26	1st. Lieutenant	5	5	2	0	Neutral	Neutral	Strongly Disagree	Disagree	Neutral	Disagree	Disagree	Disagree	Strongly Agree	Neutral	Disagree	Neutral	Neutral	Agree	Neutral	Disagree	Disagree	Disagree	Neutral	Neutral
Female	Bachelor	32	Captain	10	10	3	1	Strongly Disagree	Strongly Disagree	Strongly Disagree	Disagree	Agree	Agree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Disagree	Disagree	Strongly Disagree	Disagree	Agree
Male	Bachelor	33	Captain	9	9	2	1	Strongly Disagree	Disagree	Neutral	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Strongly Disagree	Disagree	Disagree	Disagree	Neutral
Male	Bachelor	41	Major	17	17	2	0	Strongly Disagree	Neutral	Neutral	Neutral	Strongly Agree	Disagree	Neutral	Strongly Agree	Strongly Disagree	Strongly Disagree	Neutral	Agree	Strongly Disagree	Strongly Disagree	Strongly Disagree	Agree	Neutral	Disagree	Strongly Agree	Strongly Disagree
Male	Bachelor	35	Captain	10	10	3	0	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Strongly Disagree	Disagree	Strongly Agree	Agree	Agree	Neutral	Neutral	Neutral	Neutral	Strongly Disagree	Disagree	Disagree	Strongly Agree	Neutral
Male	Bachelor	38	Major	15	15	4	0	Neutral	Strongly Disagree	Agree	Neutral	Neutral	Disagree	Disagree	Disagree	Disagree	Neutral	Neutral	Disagree	Neutral	Strongly Disagree	Strongly Agree	Neutral	Neutral	Neutral	Disagree	Neutral
Female	Bachelor	33	Major	12	12	1	2	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Strongly Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Disagree	Disagree	Disagree	Disagree	Neutral
Male	Bachelor	26	Lieutenant	2	2	3	0	Neutral	Strongly Disagree	Agree	Agree	Neutral	Agree	Neutral	Agree	Strongly Disagree	Disagree	Disagree	Strongly Agree	Strongly Disagree	Neutral	Strongly Agree	Neutral	Disagree	Agree	Neutral	Disagree

Male	Master	41	Major	20	20	1	0	Strongly Disagree	Strongly Disagree	Neutral	Disagree	Agree	Strongly Disagree	Disagree	Disagree	Strongly Agree	Agree	Disagree	Strongly Agree	Strongly Agree	Neutral	Neutral	Strongly Disagree	Disagree	Disagree	Disagree	Agree
Male	Bachelor	26	Lieutenant	2	2	3	0	Strongly Disagree	Strongly Agree	Strongly Disagree	Strongly Disagree	Neutral	Neutral	Neutral	Disagree	Strongly Disagree	Disagree	Neutral	Strongly Agree	Neutral	Disagree	Neutral	Strongly Disagree	Neutral	Strongly Disagree	Neutral	Strongly Disagree
Male	Bachelor	52	Major	31	31	4	0	Strongly Disagree	Strongly Agree	Neutral	Strongly Disagree	Neutral	Strongly Agree	Strongly Disagree	Neutral	Agree	Neutral	Strongly Disagree	Strongly Disagree	Strongly Agree	Neutral	Strongly Agree	Neutral	Neutral	Neutral	Neutral	Disagree
Male	Bachelor	45	Major	20	20	1	0	Strongly Agree	Agree	Strongly Disagree	Strongly Disagree	Strongly Disagree	Agree	Neutral	Strongly Disagree	Agree	Neutral	Strongly Agree	Disagree	Disagree	Strongly Disagree	Neutral	Neutral	Strongly Agree	Strongly Agree	Neutral	Disagree
Male	Bachelor	34	Captain	10	10	3	0	Neutral	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Strongly Disagree	Disagree	Neutral	Agree	Disagree	Strongly Agree	Strongly Agree	Agree	Strongly Disagree	Disagree	Strongly Agree	Neutral	Disagree	Agree
Male	Bachelor	41	Major	18	18	3	0	Neutral	Strongly Agree	Neutral	Strongly Disagree	Neutral	Neutral	Disagree	Strongly Agree	Strongly Disagree	Strongly Disagree	Strongly Agree	Neutral	Strongly Disagree	Agree	Disagree	Strongly Disagree	Neutral	Strongly Agree	Strongly Disagree	Neutral
Male	Bachelor	50	Major	27	27	4	0	Strongly Disagree	Disagree	Strongly Agree	Disagree	Agree	Neutral	Neutral	Disagree	Strongly Agree	Strongly Disagree	Neutral	Strongly Disagree	Neutral	Disagree	Strongly Agree	Disagree	Strongly Agree	Neutral	Neutral	Neutral
Male	PhD	48	Major	27	27	4	0	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Neutral	Disagree	Disagree	Disagree	Strongly Agree	Neutral	Strongly Disagree	Strongly Agree	Neutral	Agree	Disagree	Disagree	Strongly Disagree	Strongly Disagree	Strongly Disagree	Neutral
Male	Master	48	Major	27	27	4	0	Neutral	Disagree	Strongly Disagree	Disagree	Agree	Disagree	Disagree	Disagree	Strongly Agree	Neutral	Disagree	Neutral	Neutral	Neutral	Neutral	Strongly Disagree	Disagree	Disagree	Strongly Disagree	Agree
Male	Master	45	Major	24	24	1	0	Strongly Disagree	Strongly Disagree	Strongly Disagree	Disagree	Neutral	Disagree	Disagree	Disagree	Neutral	Neutral	Disagree	Strongly Agree	Neutral	Agree	Strongly Disagree	Strongly Disagree	Strongly Disagree	Disagree	Disagree	Neutral
Male	Bachelor	45	Major	21	21	2	0	Strongly Disagree	Disagree	Disagree	Disagree	Strongly Disagree	Disagree	Neutral	Strongly Disagree	Disagree	Neutral	Disagree	Agree	Strongly Disagree	Strongly Disagree	Agree	Strongly Disagree	Strongly Disagree	Agree	Strongly Disagree	Neutral
Female	Bachelor	28	1st. Lieutenant	7	7	4	0	Strongly Disagree	Disagree	Strongly Disagree	Strongly Agree	Agree	Disagree	Disagree	Strongly Disagree	Strongly Agree	Agree	Strongly Disagree	Neutral	Strongly Agree	Agree	Strongly Disagree	Disagree	Strongly Disagree	Disagree	Disagree	Agree
Female	Master	28	1st. Lieutenant	6	6	3	0	Strongly Disagree	Disagree	Neutral	Disagree	Agree	Neutral	Neutral	Disagree	Neutral	Agree	Disagree	Strongly Agree	Neutral	Neutral	Strongly Disagree	Disagree	Disagree	Disagree	Agree	Neutral
Male	Bachelor	44	Major	21	21	2	0	Strongly Agree	Neutral	Neutral	Neutral	Agree	Neutral	Strongly Disagree	Agree	Strongly Agree	Disagree	Neutral	Neutral	Strongly Agree	Neutral	Agree	Strongly Disagree	Disagree	Strongly Disagree	Neutral	Agree

Appendix B

```
import pandas as pd
import numpy as np
survey  =  pd.read_csv("survey_data.csv",  index_col=None,
header=0)
column_names = []
column_names.append('Gender')
column_names.append('Education')
column_names.append('Age')
column_names.append('Rank')
column_names.append('Career Experience')
column_names.append('Years in the Organization')
column_names.append('Years in Current Position')
column_names.append('Years in Digital Forensics')
for i in range(20):
    column_names.append('V'+str(i+1))
survey.columns = column_names


for i in range(20):
    for j in range(209):
        if survey['V'+str(i+1)][j] == 'Strongly Agree':
            survey['V'+str(i+1)][j] = 5
        if survey['V'+str(i+1)][j] == 'Agree':
            survey['V'+str(i+1)][j] = 4
        if survey['V'+str(i+1)][j] == 'Neutral':
            survey['V'+str(i+1)][j] = 3
        if survey['V'+str(i+1)][j] == 'Disagree':
            survey['V'+str(i+1)][j] = 2
        if survey['V'+str(i+1)][j] == 'Strongly Disagree':
            survey['V'+str(i+1)][j] = 1
        if survey['V'+str(i+1)][j] == 'Do Not Apply':
            survey['V'+str(i+1)][j] = np.nan


column_names = []
column_names.append('Years in Digital Forensics')
for i in range(20):
    column_names.append('V'+str(i+1))
survey_values                                           =
survey[column_names].values.astype('float')

survey_values_experts = survey_values[survey_values[:,0] >
5,:]

average_of_experts                                      =
np.nanmean(survey_values_experts[:,1:],axis=0).reshape((1
,-1))

difference_values    =    np.abs(survey_values[:,1:]    -
average_of_experts)

limits_of_answers = np.ones((2,20))
limits_of_answers[1,:] = 5*limits_of_answers[1,:]

maximum_possible_difference_values                      =
np.max(np.abs(limits_of_answers-
average_of_experts),axis=0).reshape((1,-1))

Z = maximum_possible_difference_values.sum()

R = 1 - (np.sum(difference_values,axis=1)/Z)

column_names = []
column_names.append('Gender')
column_names.append('Education')
column_names.append('Age')
column_names.append('Rank')
column_names.append('Career Experience')
column_names.append('Years in the Organization')
column_names.append('Years in Current Position')
column_names.append('Years in Digital Forensics')
survey_bio_values                                       =
survey[column_names].T.to_dict().values()

from sklearn.feature_extraction import DictVectorizer
from sklearn import preprocessing

vectorizer = DictVectorizer()
input_data                                              =
vectorizer.fit_transform(survey_bio_values).toarray()
input_data                                              =
preprocessing.StandardScaler().fit_transform(input_data)

from sklearn import cross_validation

from sklearn import neighbors
from sklearn import svm
from sklearn import tree
from sklearn.ensemble import BaggingRegressor

knn     =     neighbors.KNeighborsRegressor(n_neighbors=1,
weights='distance')
sv = svm.SVR()
dt = tree.DecisionTreeRegressor()
nn = BaggingRegressor()

scores = cross_validation.cross_val_score(knn, input_data,
R, cv=5, scoring='mean_absolute_error')
print("kNN  Error:  %0.2f  (+/-  %0.2f)"  %  (scores.mean(),
scores.std() * 2))
```

```
scores = cross_validation.cross_val_score(sv, input_data,
R, cv=5, scoring='mean_absolute_error')
print("SVM Error: %0.2f (+/- %0.2f)" % (scores.mean(),
scores.std() * 2))

scores = cross_validation.cross_val_score(dt, input_data,
R, cv=5, scoring='mean_absolute_error')
print("Decision Tree Error: %0.2f (+/- %0.2f)" %
(scores.mean(), scores.std() * 2))

scores = cross_validation.cross_val_score(nn, input_data,
R, cv=5, scoring='mean_absolute_error')
print("Neural Network Error: %0.2f (+/- %0.2f)" %
(scores.mean(), scores.std() * 2))
```