UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA
Denkleiers • Leading Minds • Dikgopolo tša Dihlalefi

Digital Forensic Evidence Acquisition to Mitigate Neighbourhood Crime

by

Stacey Angela Omeleze

Submitted in fulfilment of the requirements for the degree

Master of Science (Computer Science)

in the

Faculty of Engineering, Built-Environment and Information Technology

at the

UNIVERSITY OF PRETORIA

SUPERVISED BY

Prof. H. S. VENTER

July, 2017

Table of Contents

List of Tables

List of Figures

Declaration

I declare that this dissertation, which I submit in fulfilment of the requirements for the degree of Master of Science in Computer Science at the University of Pretoria, is entirely my own work and has not been submitted anywhere else for the award of a degree or otherwise. Four national and international peer-reviewed conference papers were published from this dissertation, while two conference papers are in-press. Likewise two journal articles have been submitted to a national and an international peer-reviewed scientific journal. Any errors in thinking or delivery as well as any omissions are entirely my own responsibility.

I, **Stacey Angela Omeleze**, declare that this dissertation entitled, “**Digital Forensic Evidence Acquisition to Mitigate Neighbourhood Crime**” and the work presented in it are my own.

Dedication

Dedicated to the UNIVERSE for its infinite resources...

Acknowledgements

I sincerely grateful to my supervisor, Prof. Hein S. Venter, who in his infinite wisdom has a way of knowing when I am demotivated, and who then finds a way to motivate my flagging spirit. Thank you very much Prof for everything

For my academic and personal growth, I am most grateful to the staff and students of the Computer Science Dept., University of Pretoria. The positive impact of the financial support I received from the University of Pretoria Postgraduate bursary contributed to the completion of this research.

Knowledge sharing and the continuous advice from members of my research group and colleagues have been some of my greatest strengths through this journey. You all have been inspiring and gracious. While I mention a few of them, I sincerely thank everyone - Abisoye, Ayanda, Chawezi, Dagney, Enos, Eunice, Fikile, Gilbert, Itumeleng, Irene, Makura, Mluleki, Nickson, Sayo, Sedzani, Victor, Werner and of course all the amazing SITners and ICSAners. I will like to acknowledge the contributions of Mamelo Seopela, Collen Mphabantshi and Pule Legodi. Thank you my people!

None of this would have been possible without the encouragement and continuous support of my family. Thank you Family, with you by me, everything is possible...I am the most blessed.

Abstract

Mobile devices form an integral part of our daily lives and have the potential to be used as tools to curb crime. In recent years, many criminal activities have gone unsolved due to a lack of sufficient evidence to convict the perpetrators. Together with recent developments and advances in research, technology such as mobile devices (popularly known as ’smart phones’) is now capable of acting as devices for capturing real-time potential digital evidence. The continued advancement in the features of mobile devices such as photos, as well as video and voice-recording options, has enhanced their applicability as capturing devices for real-time potential digital forensic evidence. In digital forensic investigation, one of the challenges that law enforcement agencies encounter is to corroborate the findings at the crime scene with digital evidence of the crime. By using a mobile and portable device as a tool for acquiring real-time potential digital evidence in the form of photos or video and voice recordings, this challenge can be greatly overcome. The problem is that it is difficult to ascertain, the integrity of the captured digital evidence of a crime scene when using the advanced capabilities of these mobile and portable devices. The research in hand proposes an online neighbourhood watch (ONW) system that can overcome these challenges. The ONW system is a tool that can be used to acquire potential digital evidence (PDE) and preserve the integrity of the captured PDE. Access to the stored PDE in an ONW system’s repository is strictly monitored and controlled in order to maintain the confidentiality and integrity of the PDE. The ONW system enables members of a community in South Africa to upload PDE of a crime scene in the form of audio, video and digital images to the ONW repository. The PDE is then made available to the law enforcement agents and digital forensics analysts to assist them in furthering investigations or in solving the crimes involved. The ONW system balances public safety with the privacy rights of the PDE generators and the possible offenders whose images have been captured. It takes into consideration the privacy policies, laws and ethics that may apply due to the devices’ generated metadata of users’ personal details, especially during a digital evidence presentation in a court of law.

Part I

INTRODUCTION

The first part of this dissertation focuses on introducing the research in its entirety. It sets out the aim and scope of the research, outlines the problems to be examined, acknowledges some limitations, and describes the methodology used in addressing the identified problems.

Chapter 1

INTRODUCTION

1.1 *Introduction*

Technology is an empowering factor that provides some means to address challenges encountered by people, governments and organisations, that otherwise would remain unresolved. The enormous scientific and technological growth as is currently experienced in information and communication technology (ICT) developments such as internet connectivity, self-driving cars and mobile devices have improved the lives of the ICT users [1]. Mobile devices have made many positive contributions to our lives. For example, our cellphone as a mobile device is a case in point of how technology has enhanced our lives, and it has become one of the most used electronic gadgets in the world [2]. However, mobile devices have also been used as a means to perpetrate criminal activities and other anti-social behaviour. For example, the increase in cyber bullying, sexting and other online-related crimes has resulted from the increased number of mobile device users. Apart from the new phenomenon of online crime, other more traditional forms of crime still occur at an unacceptably high rate.

The high crime figures in South Africa may be linked to the low rate of criminals being arrested and convicted. According to the crime report statistics revealed by the South African Police Service (SAPS) for the period April 2012 to 31 March 2013, arrests were made in only in 47.9% of cases in the category of serious and property-related crime [3] [4] [5]. Furthermore, SAPS claims that most murders, assaults and rape cases occurred between people who knew each other and live in the same neighbourhood [3]. These crimes are rarely premeditated and are often exacerbated by alcohol and other substance abuse. Therefore, an effective means of preventing crime and violent behaviour, may typically require a long-term measure, such as neighbourhoods and community members working together to combat these crimes. One of the major reasons crime perpetrators are never brought to justice is insufficient evidence.

This implies that there is need for a means to capture and store potential evidence of these crimes to show that the criminals were at the scene when the alleged crime occurred. Evidence is defined according to Dutelle [6] as anything that can aid in proving or disproving that a crime occurred. However, actions employed in the process of collecting the evidence must be clearly documented. The responsibility of producing essential evidence tying criminals to their crimes, lies not only with the law enforcement agents, but also with members of the communities in which these crimes often take place [7]. Due to the high crime rate and the low rate of arrests and conviction, better crime prevention techniques are clearly necessary.

Research by Van, Mayhew and Nieuwebeerta [8] shows that some Western countries have recorded a fall in crime rates which was attributed to effective crime prevention techniques and the use of new technologies. New technology like close circuit television (CCTV) and speed cameras in particular have proved to be successful in reducing crime. However, in the African context, the task of crime prevention cannot be left to the law enforcement agents (LEAs) and the judiciary alone. Rather, the scientific community and the general public must participate in the fight against crime. For example, neighbourhood watch schemes, which began in America during the 1960s and have been operational in Europe and other parts of the world since then, have according to Bennett et al., [9] been quite successful in reducing crime. Now, half a century later, the current research aims to revitalise this concept of community policing by harnessing the use of the most commonly available electronic devices to assist the LEAs in crowd-sourcing potential digital evidence to be used in the fight against crime.

Now that the scene of this dissertation has been set and the aim established, the reader should note that the remainder of this chapter is structured as follows:

- **Section 1.2 focuses on identifying the problems to be addressed by this research.**
- **Section 1.3 highlights the limitations of this research.**
- **Section 1.4 explains the motivation for the research to address the identified problems.**
- **Section 1.5 covers the objectives and describes the tactics that are employed in addressing the identified problems.**
- **The methodology used in this study is referred to in Section 1.6.**
- **Finally, the overall structural layout of this research is presented in Section 1.7, with a short conclusion to this chapter in Section 1.8.**

According to Bunge [10], before any form of research can commence, the problem that the study aims to tackle must be stated clearly. To this effect, the next section presents the problem statement of this research. The identified problem is then broken-down into smaller elements that are addressed in the course of this dissertation.

1.2 *Problem Statement*

One of the challenges encountered by the law enforcement agents is to corroborate crime events with the evidence at/of a crime scene. Due to this, numerous criminal cases either remain undiscovered, or the crimes detected remain unsolved due to a lack of sufficient evidence placing the criminal at the scene of the crime. Successful prosecution of the perpetrators is sometimes simply impossible to achieve. It is therefore essential to involve members of the community in potential evidence crowd-sourcing efforts, to make available potential evidence that provides concrete proof that shows a crime was perpetrated. The potential evidence provided by the community members must be made available to law enforcement agents, digital forensic investigators and the judicial system, to aid the prosecution of offenders and resolve neighbourhood crimes and/or other civil cases pending in various courts of law.

Meanwhile, everyday technology such as mobile devices can be employed to great effect in the generation of the potential evidence. However, the zeal of the legal system to ensure equity and justice for all, may sometimes introduce barriers to the employment of digital data evidence accrued from these devices.

The main problem that this research addresses is that there is often insufficient evidence to corroborate crime scene evidence related to alleged neighbourhood crimes. Eye-witness accounts, profiling and other forms of evidence are considered hear-say [11] [12], in legal proceedings and are therefore not able to show the proof of a criminal's physical presence where a crime occurred, thereby unable to prove a crime indeed occurred.

To address the challenge of insufficient evidence, this dissertation divides the research problem into sub-problems, where each of the sub-problems is addressed individually in order to tackle the main research problem. These sub-problems are formulated as follow:

- For individuals or citizens who wish to harness the current growth in mobile technology, there is no viable storage repository to store captured potential digital evidence (PDE) of criminal behavior, especially in a crime-riddled neighborhood. If such a repository were to be available, citizens would have the facility to capture and store the PDE of a crime. A PDE is a raw digital data evidence gathered from a cyber crime or physical crime scene that has the potential to be an admissible evidence in a litigation [13] [14] [15]. A PDE, when validated, can be used by law enforcement agents (LEAs) during crime investigation.

- There are no easy ways to capture a PDE that can be deemed admissible evidence in a court of law. The integrity of the captured PDE needs to be ensured by maintaining the forensic soundness of the PDE and implementing access control on the stored PDE [16]. These are required in order to comply with the admissibility requirements of electronic data as specified in the South African legal system [11] [17] or in any other jurisdiction that might have similar legal requirements.

- Anonymity must be guaranteed to the citizen who captures the PDE, while at the same time, the PDE metadata needs to retain contents that provide originality of the captured and stored PDE. Therefore the requirement for a user to remain anonymous poses a further challenge. If the user who captured the PDE is to achieve complete anonymity, it may be impossible to ascertain the originality of the PDE or link the PDE to a particular incident. This may lead to the inadmissibility of the PDE in a litigation.

- The South African Electronic Communications and Transactions (ECT) Act, Act 25 of 2002 [17] requires that for digital data evidence to be admissible in a litigation, it must attain evidential weight. In other words, the credibility of an evidence should be beyond question. In another vein, the Protection of Personal Information (PoPI) Act, Act 4 of 2013 [18] [19] also restricts the use of personal information without the explicit consent of the user. These legal requirements also pose certain challenges that must be addressed by this research.

The researcher identified the sub-problems above as adjunct to the main problem of this study. However some issues are beyond the scope of this dissertation. These limitations are presented next.

1.3 *Limitation of this research*

The following issues are given only cursory attention as they are beyond the scope of this research:

- The ECT Act, Act 25 of 2002, section 15(1), (2) and (3) defines the evidential weight of data information and the best evidence rule to be allowed in the usage of digital evidence in a South African court of law [17]. This requirement of the ECT Act in respect to evidential weight is determined solely by the presiding Judge in a case. Because of this power exercised by the Judiciary, not all PDE captured and uploaded to the repository may be deemed usable for a crime investigation or be accepted as 'real evidence' in a court of law.
- The study places little to no emphasis on human factors such as the psychological state of the witness who captures and uploads PDE, and also does not consider how the citizen decides on what exactly constitutes a potential crime. Such human factors are issues beyond the scope of this research.
- It is simply assumed that users' mobile devices are able to acquire digital images such as audios, videos and photos. No specific attention is given in this study to proving the truth of this assumption.
- It is also assumed that users can use their personal devices to capture PDE from a safe distance away from the crime to avoid self-endangerment. Again no specific attention is given in this study to proving the truth of this assumption.
- This study did not develop or attempt to design new or improved cryptographic functions. Rather, the study implemented the existing cryptographic mechanisms that have been developed in the Android encryption library and on the web-application side .

With the problems and the limitations established, the motivation for this research is dealt with next.

1.4 *Motivation*

The rise in crime has weakened the sense of community in many South African societies. The high crime rate has prompted the need for a proactive measure to mitigate neighbourhood crime. The motivation for this research lies in the conviction that mobile devices can be utilised as tools for gathering potential evidence to combat such neighbourhood crime. According to the Institute for Security Studies [20] and the South African Police Service (SAPS), local crime statistics show that murder and robbery continue to rise and that contact and property-related crimes committed in 2013 were perpetrated by people from the neighbourhood where the alleged crime took place [3].

Most of these crimes remain unsolved or proof is inconclusive due to a lack of concrete or sufficient evidence that puts the offender(s) at the scene of the alleged crime. This hinders the prosecution of the crime perpetrators.

By using a mobile device application as a tool to curb crime, communities are empowered to identify and fight crime in their neighbourhoods. The motivation for this research is therefore to employ the techniques of crowd-sourcing and the social media method of ’capture and upload’ to empower and motivate communities to engage in the fight against crime and thus build safer South African communities.

Inspired by these motives, the objectives of this research are presented in the following section.

1.5 *Objectives*

The main objective of this research is to create an online neighbourhood watch (ONW) system that encourages members of communities to use their mobile device to reduce crime in their neighbourhood. The captured PDE can be used in multiple scenarios such as cases of domestic violence, molestation, bullying, robbery, and other crime incidents, which may require concrete evidence to prove culpability in a litigation. However, for the PDE to be useful in a legal proceeding or criminal investigation, the integrity, reliability, and authenticity (originality) must be proven beyond reasonable doubt. In addition to the primary aim of creating the ONW system, the objectives of this research also include the following:

- To explore relevant literature on digital forensics, digital evidence, information security services and techniques, as well as software requirements specifications that can enhance the admissibility of a digital evidence and complies with the laws and standards pertaining to the admissibility of digital evidence in South Africa and other parts of the world.

- To ascertain the forensic soundness of the captured PDE from the crime scene by means of mobile devices through the application of cryptographic techniques, such as hashing algorithm, digital signature, and encryption algorithm. This will ensure that the acquired PDE has not been tampered with. This is another challenge that will be addressed by this research.
- To leverage the built-in features of mobile device, such as camera and audio- recording functions, to curb neighbourhood crime in South Africa. In the process, to increase the volume of available digital evidence to enhance success in neighbourhood crime litigation [21].
- To design, and develop a conceptual model for an online neighbourhood watch (ONW) system that encompasses the mechanisms which can address information security services and secure storage functions.
- To evaluate (proof of concept) the developed model using a case study that determines the state in which the captured PDE can be used during crime investigation.

The next section outlines the methods employed in achieving the above objectives of this research.

1.6 *Methodology*

The procedure for finding the solution to a problem will depend on the nature of the problem[10]. The current research adopts the following scientific methods to approach the identified problems:

(i) Conducting an extensive literature review and background analysis of digital forensics, digital evidence, information security services, digital evidence integrity, and its application in accordance with the South African rules of evidence.

(ii) Formulating a model to illustrate the various aspects of the proposed system. The model focuses on the users capturing of the PDE and how the forensic soundness of the captured PDE is maintained. The modelling goes a step further to show how access of the authorised users is managed. It then implements a case study to illustrate the use of the ONW system in a real-world scenario. In the context of this research, the authorised user is defined as any user that has permission to carry out any number of functions on the ONW system.

(iii) Applying requirements engineering specifications process that focuses on identifying the use cases of the system, the architectural requirements and the various constraints that the system must take into account at design and development.

(iv) A prototype of the ONW system is developed using Python, Java, MySql database, Django and Bootstrap frameworks, Android development kit, application program interfaces (APIs), and various integrated development environments (IDEs).

(v) Evaluating the proposed system in relation to a related literature survey that focused on digital evidence capturing, usage and storage, and evaluating this literature in relation to the contributions of this research.

Having highlighted some of the methods that are to be used to address the identified problems, and in the process fulfilling the objectives of this research, the next section provides a narrative and graphic description of the entire dissertation layout.

1.7 *Layout*

This research is structured in five parts as shown in Figure 1.1, with the following overview of the various parts.

PART I: The first chapter constituted the entire Part I and introduced this research. It focused on the aims and scope of the research, outlined the problems to be addressed, acknowledged certain limitations to the scope of the research, and also described the methodology to be employed in addressing the problem statement.

PART II: Part II comprises of chapters 2, 3, and 4. Chapter 2 reviews literature on forensic science, focusing on digital forensics and focuses on digital evidence in particular. It continues by taking a closer look at the security requirements for PDE and zooms in on technologies that achieve confidentiality, integrity, and availability (CIA). Chapter 3 examines the legal requirements by focusing on digital evidence admissibility and the means employed to bridge the gap between technology and legal standards. Chapter 4 explores requirements engineering specifications.

PART III: In part III, the conceptual ONW model is proposed. Chapter 5 presents the online neighbourhood watch (ONW) model and focuses on the methods utilised in achieving integrity of the ONW model. Chapter 6 considers the access control measures proposed in the ONW model.

PART IV: Part IV deals with the prototype proposed in this research. Chapter 7 introduces the requirements specifications of the ONW proposed system, outlines the main architectural requirements, and provides the design scope, quality requirements and architectural requirements specifications. Chapter 8 presents the prototype itself.

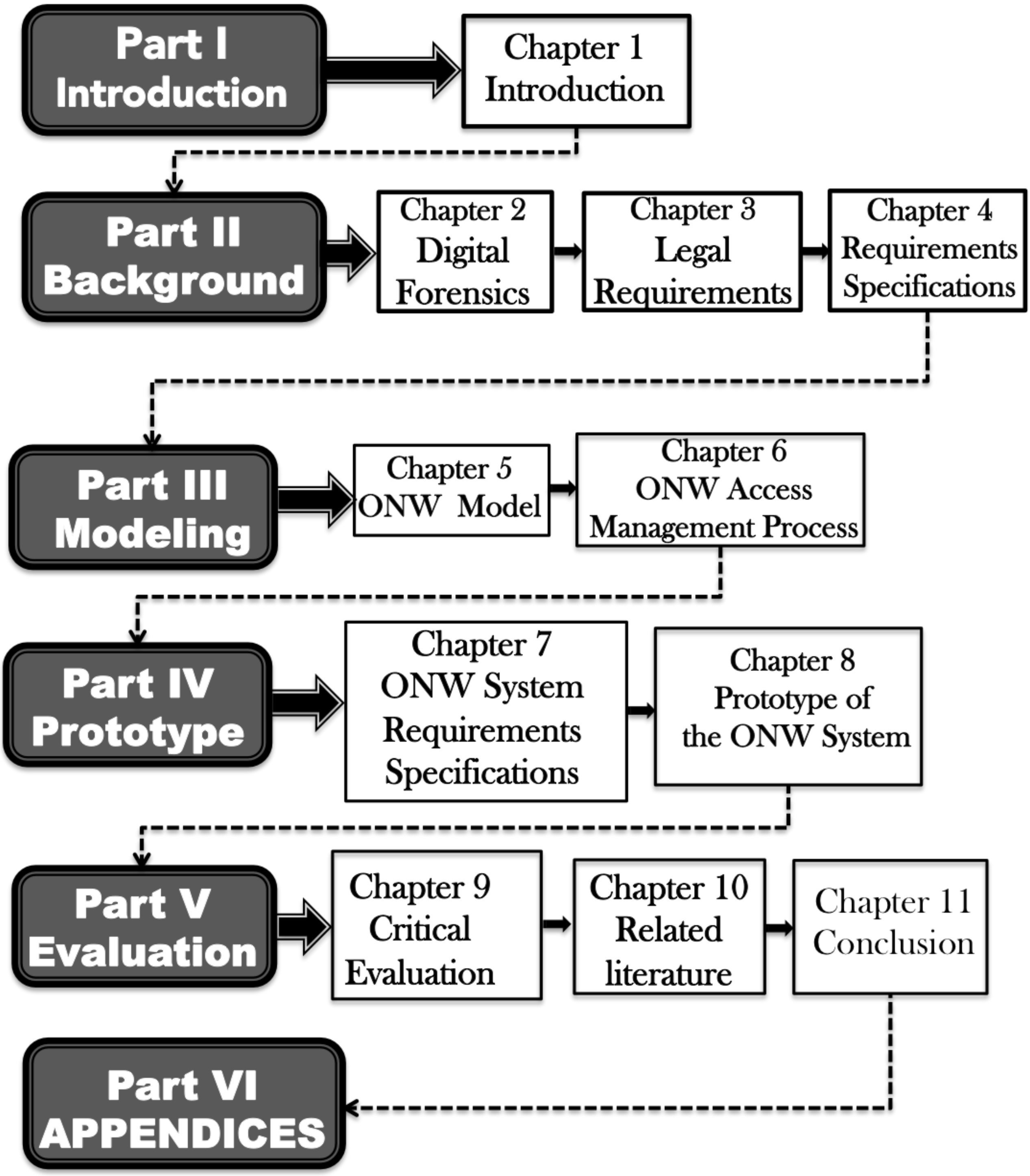


Fig. 1.1: Dissertation Chapters Layout

PART V: Part V evaluates and concludes this research. Chapter 9 takes a look at some related literature and compares it with the contributions made by the current research. Chapter 10 evaluates, critiques and analyses the ONW system and Chapter 11 delivers this dissertation's summary and conclusion.

PART VI: The Appendix section presents the technical details of the ONW system's prototype, the SAPS crime statistics and the peer-reviewed publications published as a result of the findings of this research.

1.8 *Conclusion*

The overall aim of this research is finding a means to generate admissible digital evidence of neighbourhood crime. The process to be employed to generate potential digital evidence was outlined in this introductory section. Having introduced the scope of this research, the researcher's focus shifts to the contextual material related to this research, as the next three chapters embark on a literature review that guides this study.

Part II

BACKGROUND

Part II comprises of chapters 2, 3, and 4. Chapter 2 reviews literature on forensic science, focusing on digital forensics and digital evidence in particular. It continues by taking a closer look at the security requirements and zooms in on technologies that achieve confidentiality, integrity, and availability (CIA) of digital evidence. Chapter 3 examines the legal requirements, focusing on digital evidence admissibility and the means employed to bridge the gap between technology and legal standards. Chapter 4 explores the requirements engineering specifications for digital forensic tools.

Chapter 2

DIGITAL FORENSICS

2.1 *Introduction*

The background chapters of this dissertation start in Chapter 2.2 with a brief overview of forensic science, digital forensics, digital evidence and digital evidence integrity as the core background topics covered in this research. This is followed by a section focused on the various information security techniques that are used to fulfil the requirements of digital evidence forensic soundness so as to attain admissibility in any court of law. The background chapters continue with Chapter 3 focusing on the legal requirements as they apply to digital evidence admissibility in the context of the South African legal system. Chapter 4 concludes the background chapters with a look at requirements engineering specifications for software applications, especially as far as digital forensic tools are concerned.

Since this dissertation deals with the generation of potential digital evidence (PDE) to be used by law enforcement agents (LEAs) and forensic investigators in their battle against crime, it is necessary to situate this study within the subject field of digital forensics. Digital forensics emerged from forensic science, which is a larger body of knowledge in which science is used to solve crime [22] [23]. In discussing digital forensics, therefore, there is a need to firstly introduce the concept of forensic science.

2.2 *Defining Forensic Science and Digital Forensics*

According to the American Academy of Forensic Sciences (AAFS), the field of forensic science comprises of different areas of interest, including forensic anthropology, forensic biology/pathology, digital forensic science, forensic jurisprudence, as well as digital and multimedia sciences (also known as digital forensics) [24] [25] [26]. In this dissertation however, the focus is on digital and multimedia sciences, which is referred to as digital forensic science or digital forensics.

Forensic science originated from an overwhelming need to determine the cause of events during investigations or in legal proceedings [27]. It involves the use of scientific techniques in uncovering activities surrounding incidents, especially related to crime [28] [29]. The Oxford English Dictionary, 2013 [30] [31] also defines forensic science as the application of scientific methods and techniques in the investigation of crime. It is indeed a way of answering questions that assists in investigating and adjudicating criminal and civil cases using scientific methods [32]. This further leads to the examination of the behaviour people, locations, and physical of an incident under investigation.

2.2.1 *Digital Forensics*

Digital forensics is a young science that emerged from the field of forensic science. The latter was developed in conjunction with biological, cognitive and other sciences to assist in the identification of patterns of incidents under investigation [29] [10]. In a nutshell, digital forensics is a relatively new field of science arising out of the need to solve crimes that involve digital data and digital devices [33]. Various definitions of digital forensics exist, some of which are examined in this dissertation, and in the process, a conclusive definition is derived and proposed. This definition of digital forensics is subsequently adopted throughout this dissertation.

The Digital Forensic Research Workshop (DFRWS) [34] defines digital forensics to be the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorised actions shown to be disruptive to planned operations. The DFRWS definition of digital forensics covers the broad spectrum of digital forensics ranging from digital data acquisition, analysis and storage to the legal aspects on which it has an impact. The extensive nature of this definition makes it one of the most referred to definitions of digital forensics.

Cohen [35] defines digital forensics as a subject that started between art and craft, and that contains a scientific body of knowledge with an underlying scientific methodology consisting of four basic elements. These elements are: (i) the study of previous and current theories and methods; (ii) conducting experiments to prove the theories; (iii) the identification of inconsistencies between theories; and (iv) the repeatability of these experiments in correlation with expert witnesses. In other words, digital forensics - unlike other research areas - is a practitioner-oriented field [36]. As a result, both researchers and industrialists concurrently develop proactive, reactive or coactive methods to solve or analyse various incidents as they are encountered. In doing so, various means are adopted to achieve the objective of digital forensic investigation and at the same time advance the field of digital forensics.

John [37] defines digital forensics as the use of scientifically derived and proven methods toward the validation, identification, interpretation, documentation and presentation of digital evidence derived from digital sources, such as mobile devices, computers and networks, for the purpose of facilitating an investigation or for the reconstruction of events involving crime, data recovery, cybercrime, fraud, and intellectual property theft. This definition focuses on digital forensics as a method for the investigation of events involving data in digital format, and it emphasises the use of scientific methods.

The current dissertation draws from these definitions (among others) and understands digital forensics to be the use of scientifically derived, mathematically proven methods and algorithms in the acquisition, preservation, validation, identification, analysis, interpretation and documentation of digital evidence for the purpose of facilitating or furthering the reconstruction of events found to be criminal, and also to anticipate unauthorised actions shown to be disruptive to planned day-to-day operations [38] [35] [39].

From looking at these definitions it can be seen that there are three dimensions to digital forensic science, namely proactive, reactive and coactive. Proactive digital forensics is a means of detecting potential criminal acts and it is also referred to as digital forensic readiness [40]. The reactive dimension involves investigating a digital incident that has occurred and constitutes the bulk of digital forensic science.

The success of digital forensic science depends on establishing and following processes that are outlined in the Daubert guidelines [41], which are used by a presiding Judge in a legal proceeding to determine when an expert's scientific testimony is based on reasoning or scientifically valid methodologies. The Daubert guidelines require that the digital forensic process or methodologies must be tested and peer-reviewed, have a level of acceptance in the scientific communities and a known potential error rate, with standards and controls. Therefore, one of the crucial tasks of a forensic investigator is to compare and ensure the repeatability of processes employed. This is possible using digital forensic applications and digital forensic processes. These processes must be replicable in order to obtain similar results when used with similar measures. The overall goal of all digital forensic investigations is to establish what happened and how it happened. Therefore, to commence any form of digital forensic investigation, there must be digital evidence consisting of sequences of bit and binary values. The next section focuses on digital evidence.

2.2.2 *Digital Evidence*

The use of electronic devices such as mobile devices, computers and networks in today's world has resulted in the generation, storage and distribution of a huge amount of information. Much of this data has the potential to be used as evidence in criminal investigations or in other civil proceedings. Due to the growth in available data, digital forensic investigators and law enforcement agencies must introduce a means to accommodate the demand for preciseness and validity of the required details of digital evidence for a case under investigation and during digital evidence analysis [42].

Digital evidence consists of bits in series of zeros and ones forming information clusters that provide a means to aid the preclusion of criminal-related offences. A digital item is considered digital evidence once it complied with the requirements that satisfy its integrity and authenticity in a court of law. Until it satisfies these requirements however, the digital data can be termed as potential digital evidence (PDE). Therefore, PDE is raw data (material), especially when collected from a crime scene, but has the potential to become real evidence once its integrity has been satisfactorily proven [17] [13]. Digital evidence can be in the form of digital videos, digital audios, digital images and documents. For data to be used as digital evidence, its integrity must be proven beyond doubt. This means that the data must still be in its original and uncontaminated state.

Casey [29] defines digital evidence as any stored or transmitted data obtained from electronic devices that could support or refute the theory of how a digital data incident occurred. Digital evidence enables the commencement of any investigation, in order to establish facts relevant to the case under investigation. Casey [29] also outlines eight principles all digital evidence should adhere to, in order for it to be admissible in a court of law. These are:

(i) **Evidence Exchange**
Evidence is created by the exchange made through the interaction between the victim and the offender. Locard's exchange principle states that in every crime scene, the perpetrator takes and leaves something during the period of entering and exiting the scene [43].

(ii) **Evidence Characteristics**
During the exchange that occurs between a person and the crime scene, trace evidence is produced that belongs to two categories, namely class characteristics and individual characteristics. Class characteristics refer to general characteristics that fall in the category of items that cannot be used to identify an individual. Individual characteristics refer to exceptional characteristics that are unique and can be linked to a specific individual.

(iii) **Forensic Soundness**
Casey and McKemmish [29] [33] defines forensic soundness as resulting from the application of a reliable and accurate digital forensic process that conserves digital evidence to be used in a court of law. Evidence must be associated with documentation in the form of a time stamp and location, as well as all alterations made to the evidence. The authenticity and integrity of the documentation must be preserved and validated.

(iv) **Authentication**
The digital evidence must be certified as reliable, as the original copy with its date reflecting the date it was captured, and as satisfactory to the court of law [44]. Casey defines the authentication principles as a two-way step, whereby (i) an individual who

is familiar with or has captured the data can testify for its authenticity and state if it has been changed and (ii) a system administrator can thereafter testify that the log files have been taken from his/her system.

(v) **Chain of Custody**
The chain of custody is the defined means of keeping track of the processes employed when handling evidence. Chain of custody documentation traces back and records who transferred and analysed data, as well as when and where. It must further answer specific questions, such as what is the evidence that is being dealt with, how was the evidence gathered, when was it collected, who handled the evidence, why did the person handle the evidence and where has it been transported to and stored [45]. This document is helpful when digital evidence is used in court, as it can be authenticated by calling the person who handled the data to certify that the evidence is unchanged.

(vi) **Evidence Integrity**
Hash algorithms are used to compute a message digest of the evidence during its collection so that it can be used at a later stage to verify the integrity of the data when retrieved and used.

(vii) **Objectivity**
Evidence is presented in a manner that is self-descriptive and easy to analyse, and it allows conclusions to be drawn from it.

(viii) **Repeatability**
Documenting the steps that were taken to find and analyse evidence is an effective way of allowing repeatability, as it enables one to repeat the steps done and redo an analysis.

Evidence alters or determines the flow of major decisions in criminal or civil investigations [29] [11]. It establishes the occurrence of an incident or a crime and so constitutes the basis for initiating an investigation to further establish the facts relevant to the incident. Hargreaves [46] defines digital evidence as a reliable object that can uphold or refute a hypothesis in legal or civil proceedings. For digital evidence to be admissible, its integrity must therefore be proven with a certain degree of reliability.

During the process of analysing and interpreting digital evidence, a digital forensic investigator must demonstrate that the potential digital evidence has not been altered before, during or after its acquisition, in order for the said evidence to be admissible in a court of law. Digital forensic analysis must ensure and provide proof that PDE has been acquired, retrieved and stored in a forensically sound manner, and that it can stand up to scrutiny in a court of law.

This next section looks at digital evidence integrity in detail and discusses the methods of preserving the integrity of digital evidence during acquisition and storage.

2.2.3 *Digital Evidence Integrity*

In forensic science, the most crucial aspect of all inquiry is establishing that material presented as evidence is authentic and has not been manipulated. With the advent of digital data being used as evidence, the potential for tampering and manipulation has become even greater. Proving the authenticity and integrity of digital evidence in criminal or civil proceedings is a major task. Duren and Hosmer [47] describe digital integrity to be a property where digital data has not been altered in an unauthorised manner from the time of acquisition, through to analysis and storage. Whitman, Michael, Mattord and Herbert [48], as well as Pfleeger and Pfleeger [49] argue that data integrity is based on the overall validity, correctness, completeness, accuracy and consistency of any piece of data. Furthermore, ISO/IEC 27037 [50] [51] affirms that data integrity and admissibility is a huge requirement during digital forensic investigation. Providing proof of digital evidence integrity requires that the approach to planning, design, quality assurance and access control must be such that it safeguards digital evidence, and so enhances digital evidence admissibility. However, Flowerday and von Solms claims that 100% information integrity is not ‘currently’ achievable due to various limitations [16]. Other requirements for digital evidence integrity include secure storage, as well as maintenance of the chain of evidence and chain of custody. As mentioned earlier, chain of custody is the accurate documentation of the processing and movement of digital evidence from source A to source B, or from person 1 to person 2, from the time when such digital evidence was acquired through its analysis and/or storage, and until it has been presented to stakeholders.

Finally, according to the factors established in the case of Daubert v. Merrell Dow Pharmaceuticals Inc., 1993 [41], the four exclusive factors that must be evaluated to establish the reliability and integrity of digital evidence are the following: evidence must be authentic, accurate, complete, and it must conform with the common law and legislative rules of evidence admissibility. The weight of the evidence is, however, the measure of the evidence validity based on the content and the circumstance of the evidence [11]. The weight assists the Judge or jury in making a decision.

In discussing digital evidence, the values of confidentiality, integrity and availability (CIA) have been emphasised [49]. Confidentiality is ensuring the safety of digital evidence from any form of intercepting, viewing or editing, from the time of acquisition through analysis and storage. Integrity is proving that digital evidence is authentic and free of any form of degradation, whether due to mechanical or human error. Availability means that the acquired, analysed and stored digital evidence is available when required. However, numerous security tools must be implemented in order to achieve the goal of CIA for digital evidence. These security tools enable digital forensic investigators to perform integrity verification so as to make digital evidence available to law enforcement agents and the justice system to determine the coherence and consistency of digital evidence in cases under investigation or at legal proceedings. The security features used to enforce data integrity include cryptography, digital signatures, cryptographic hash functions and digital watermarking, which are used in collaboration with eyewitness accounts, time stamps and geographical location (geolocation) [52] [46] [53] [54]. These methods of securing digital evidence integrity are elaborated on in the next section.

2.3 *Information Security Services*

Security is the ability to concretely explore confidentiality, integrity and availability (CIA) of any system's requirement [49] [45]. A system is said to be secure when confidentiality, integrity and availability functions are in place and well balanced. Forensic soundness, on the other hand, is ensuring evidentiary weight. McKemmish [33] defines forensic soundness as the application of a reliable and accurate digital forensic process that conserves digital evidence to be used in a court of law. However, for purposes of this dissertation, forensic soundness is the requirements needed to ensure that digital evidence retains its evidentiary weight as stipulated by law, from the time of potential evidence acquisition to the time of its use - whether in a criminal, civil or organisational enquiry [15]. For potential digital evidence to attain its admissibility status, the process employed to achieve forensic soundness should be clearly shown. In this research, however, cryptography is used in conjunction with a cryptographic hash function. The hash value of the digital evidence is encrypted, which results in a unique stamp [55]. In doing so, non-repudiation is proved, as only the intended recipient of the message can decrypt the message with a private or public key. To guarantee forensic soundness and prove PDE integrity in this dissertation, information security services, such as cryptography, digital signatures and cryptographic hash functions are used, along with access control measures [52] [46] [53] [54]. These security methods are discussed in the next paragraphs.

2.3.1 *Confidentiality*

Confidentiality is ensured using encryption to protect digital data. Encryption scrambles plain data during transmission and storage to a level where it can be processed, accessed or viewed by the intended user only. The sender of digital data employs encryption to enhance the confidentiality of the sent data, while the receiver decrypts the data using predefined keywords and also known passcode as provided by the sender [49][37]. The public key infrastructure (PKI) system of encryption is used where there is absolute need to secure digital data. It is used as a method of assuring the confidentiality, authenticity and non-repudiation of electronic communications and data storage.The intended recipient of the data must possess a corresponding private key to access the received digital data. PKI, which is also known as the asymmetric encryption system, uses a two-key pair called public and private keys to encrypt or decrypt messages [56].

The asymmetric encryption system is denoted as follows: $P = E(K_E, P); D(K_D, P)$ [57], where P is the plaintext, decryption is D, encryption is E, and K is the key. The use of encryption effectively preserves the integrity and proves the authenticity of digital evidence [49]. The advanced encryption standard (AES) algorithm was defined by a Federal Information Processing Standards (FIPS) publication [58] as a symmetric block cipher with the ability to encrypt and decrypt information.

Furthermore, it has the capability to make use of cryptographic keys of 128, 192 and 256 bits to encrypt and decrypt data into blocks of 128 bits. For the symmetric encryption requirements of this dissertation, the AES encryption was employed, while the Secure Sockets Layer (SSL) was used for the asymmetric encryption which served as a point to point secure transporting of digital data. Cryptography is a method of storing and transmitting digital data in such a way that only the intended recipient can process the digital data [48] [59] [56]. Cryptography is often synonymous with scrambling plaintext into cipher text by using an encryption and decryption process [60], thereby ensuring the secrecy of digital data (digital evidence). Where additional computation is required to be performed on the cipher text, a mechanism termed homomorphism can be introduced. According to Yi et al.,[61], *"Homomorphic encryption is a form of encryption which allows specific types of computations to be carried out on cipher texts and generate an encrypted result which, when decrypted, matches the result of operations performed on the plaintext"*. This description is also in line with the assertions in Armknecht et. al., [62], and Gentry [63]; that homomorphic encryption is, principally, an encryption technique that allows for arbitrary computation on an encrypted data. Intuitively, the cryptographic service-requirement for this study does not require any additional computation to be performed on the stored cipher text. Cryptography enhances the authenticity of digital evidence. The objectives of cryptography are to address confidentiality, integrity, authentication, authorisation and non-repudiation. These objectives are discussed in more in the following subsections.

2.3.2 *Integrity*

Integrity measures the validity of digital data and checks its originality to ensure it has not been tampered with [13]. Integrity therefore addresses the questions of the reliability of digital evidence, i.e. is the digital evidence in its original form? [44]. Furthermore, a password can be used as a form of integrity check. Having a password management policy is a recommendation of the ISO/IEC 27002 [64] with a guideline for managing the security of a system effectively. According to ISO/IEC 27002, password selection must comply with certain requirements, such as minimum length and strength of a password, maintenance of previous password records to avoid repeatability, and the storage and encryption of a user's password by using a one-way algorithm. Password protection is a further attempt to ensure confidentiality and integrity of a system. The cryptographic hash functions as one of the means to ensure integrity is discussed next.

A cryptographic hash function is a mathematical function that makes it computationally impractical to acquire two distinct values that hash into a common value, simply because it uses a computationally efficient function by mapping binary strings of random length to binary strings of fixed length [64]. Cryptographic hash function is a one way encryption to prove the integrity of a data message. A message is encrypted using this function and its message digest is later compared to see if the message has been altered or not. Since two distinct messages will never produce the same message digest [65], this would prove that a message was unaltered if its message digest remains the same. Cryptographic hash function techniques when applied to digital data evidence is able to identify any tampering of digital evidence. The type of cryptographic hash algorithms that one can use to implement cryptographic hashing, varies from message digest (MD), secure hash algorithm (SHA) and hashed message authentication code (HMAC). They also have different versions, where each version opts to enhance the effectiveness of the algorithm. Using cryptographic hash functions is essential when data integrity is a priority. In proving the integrity of a digital message, cryptographic hash functions are used to generate hash values that put a seal on a digital message. These generated hash values are then used to detect when changes occur in the stored digital message or PDE. Cryptographic hash functions therefore constitute a technique that can be used to realise integrity. For this dissertation, a hashed message authentication code (HMAC), a secure hash algorithm (SHA) that generates a 160-bit hash value and a SHA-2 that generates a unique 256-bit (32-byte) signature for every piece of digital data (evidence) received, is used [52] [49]. SHA-256 is a repeated cryptographic hash function that is based on a function that apprises the eight 32-bit variables conferring to the values of 16, 32-bit words of the message [66]. One-way functions, further ensure that the sealed digital data is the same at retrieval and usage. A one-way function is a mathematical function that can easily be computed in one direction (i.e. the forward direction), whereas computing the inverse based on the forward directions might not be possible [56]. For example, the function $y = x^2$ has no inverse, because there are only two possibilities, that $2\sqrt{y} : +x$ and $-x$ [49].

While these methods discussed above are necessary and effective for preserving data integrity, they can all be undermined and rendered void if digital evidence falls into the wrong hands. Therefore, there is a need for authentication and authorisation techniques, which are presented next.

2.3.3 *Authentication and Authorisation*

Authentication provides a means of identifying a user, where a user typically enters a valid username and valid password in order to gain access to stored digital data. Each user has a unique set of criteria for gaining access. Following authentication, a user is granted authorisation to carry out certain tasks.

When logging into a system, a user's authorisation access determines the functions he/she is allowed to carry out in the system [15]. Authorisation is the process of enforcing policies that determine the type or quality of activities, resources or services a user is permitted to perform or use on a system [67]. The authorisation process determines when a user has the authority to carry out any function or access a system's content. Authorisation occurs within the context of authentication. Once a user is authenticated, he/she may be authorised for different types of access rights.

Access control is one of the paramount requirements when dealing with digital evidence integrity. It maintains the CIA security requirements of integrity, availability and confidentiality. Control over the access to potential digital evidence stored in a repository, as employed to this dissertation, is dealt with next.

2.3.3.1 Access control

Access control, the selective restriction of access to digital data resources [68][49], comprises four access principles of security. These are obtaining the identity of the entity requesting access (identification), confirming the identity of the entity seeking access (authentication), determining which action(s) an authenticated entity can perform (authorisation) and documenting such activities (accountability and auditability) [69]. Digital evidence consistency is determined to a certain degree if access to the stored digital evidence is controlled and granted only to legitimate and authorised users. In the context of this research, authorised user is any user with permission to carry out any number of function. A user has access to a system's resources when the user's credentials and identity have been authenticated and authorised. However, access to resources and the policies governing them are dynamic, and they change as the user's responsibility changes. Access control is concerned with the confidentiality and availability of the system's resources.

There are numerous models of access control such as access control list (ACL), role-based access control (RBAC) and attribute-based access control (ABAC).

2.3.3.2 Access Control List

An access control list (ACL) is used to determine the permission level of users within a group, that is, the access rights to a system's object by a user or group of users in a list [70]. The object in the case uses unique attributes to identify users with access privileges to the said group, for example a read, write or delete privilege. In this dissertation however, RBAC and ABAC are considered as the models that are best suited to protecting the confidentiality and maintaining the integrity of digital data [67] [71] [72] [73] [74].

2.3.3.3 Role-Based Access Control (RBAC)

RBAC is a means of restricting access to a system to authorised users only [73] [72] [67]. It is an access control method that grants or denies permission to a user or system based on a set of specified rules (policies) indicating what can and cannot happen between a subject and an object. For example, a subject (law enforcement agent) should meet a set of predefined policies before he/she can access an object (potential digital evidence). The basic concept of RBAC is granting privileges by using policies. Privileges are granted based on permissions, while permissions are based on functional roles. Permissions are assigned to roles and users acquire these permissions by being members of the roles in a group [75]. The elements and entities of RBAC are roles, policies, permissions and subjects in relation to the types and functions performed.

2.3.3.4 Attribute-Based Access Control (ABAC)

ABAC is a method of access control that relies on the attributes of the subject in correlation to the object [76], the attributes of the person seeking access, and the attributes of what is to be accessed. This narrows down the scale of required access of a role holder to strictly access only the attributes that meet the requirements determined by policies. ABAC elements include attributes, objects, policies and permissions.

Access control is one of the requirements to uphold digital data integrity. It is imposed by legal standards so as to enable the admissibility of digital data. In the next chapter, the legal requirements that must be compiled with to ensure the admissibility of digital evidence are identified and discussed.

2.3.4 *Non-Repudiation*

Non-repudiation is the assurance of non deniability of a user in an information system and storage domain. It is the ability that ensures that a party to a communication cannot deny the authenticity of their signature on a message and the originality of the data message [77][78]. To address non-repudiation, this research used certification authority (CA), which signs the digital certificate for the communicating parties. The CA is a trusted third party that is an entity that issues digital certificates. A digital certificate certifies a public key of a subject which allows others to rely upon signatures made with the private key that corresponds to the certified public key [**?**]. In this research however, the use of the application encryption library and the asymmetric key pair of the communicating partners are employed at various stages of information verifications, encryption and storage to confirm the users identity and to achieve the signing. Furthermore, digital signature mechanism is used to address the issues of non-repudiation through out this research. A digital signature is a mathematical scheme used to demonstrate the non-repudiation, authenticity and integrity of a message by embedding a sign that is unique to digital data evidence. In using a digital signature, the non repudiation and integrity of digital data is protected [79]. When data is digitally signed before being sent across a network, the receiver uses a digital certificate to verify the attached digital signature and so ensures the integrity of the data. Using the digital signature, the communication initiator encrypts (hash and sign) the data message using its private key pair. The information on digitally signed certificate is unhidden, rather it shows the certificate identity information like the name of the user, address, and name of organisation of the users . The information on digital certificate must be verifiable by the parties involved.

In this research, a digital signature is used to place a “tamper proof seal" and "non-deniability" function on potential digital evidence (PDE) as it is acquired and stored. The digital signature is created by first creating the hash value of the original image and then encrypting the hash value using private key pair. The digital signature can be verified by the receiver using the corresponding public key of the sender.

Chapter 3

LEGAL REQUIREMENTS

3.1 *Introduction*

In recent years, crimes that are based both on electronic and non-electronic devices have increasingly been solved or prosecuted using digital evidence [80]. In legal terms, evidence is any information or object that is admissible in a court of law and which has an influence on the outcome of the case [11]. Digital evidence enables the commencement and determination of an investigation in order to establish facts relevant to the case under investigation [29] [11]. Digital evidence constitutes crucial pieces of data that may answer the fundamental questions relating to crime, for instance the sequence of events, the relationship between the events, the source of the digital evidence and its attributes [81]. The Irish Law Reform Consultation Documentary on electronic evidence of 2009 estimated that about 80% of corporations' data is created and stored in electronic format [11]. Legal teams are constantly trying to take advantage of today's technological solutions in litigation. Electronic and digital evidence is becoming more and more relevant to the legal and judicial community in determining cases and investigations. This has led to the enactment of legislation to adopt digital data as evidence in criminal and civil proceedings [82].

Potential evidence admissibility in a court of law has been accepted and supported by various pieces of South African legislation that governs the use of digital evidence. These are the Electronic Communications and Transactions (ECT) Act, Act 25 of 2002: the Privacy of Personal Information (PoPI) Act, Act 4 of 2013; and the Regulation of Interception of Communications and Provision of Communication-Related Information (RICA) Act, Act 70 of 2002. These Acts and others as applied to digital evidence and the citizens using it are explored in the sections that follow.

3.1.1 E*lectronic Communications and Transactions Act*

The ECT Act, Act 25 of 2002 [17] was adapted from the Model Law of the United Nations General Assembly on International Trade Law (UNCITRAL) [83]. The Model Law regulates electronic documents. The ECT Act [17] states that digital evidence must not be excluded in court and its weight must be accessed by considering factors such as the reliability with which the evidence was generated, stored and transmitted. In this context, reliability focuses inter alia on how the integrity of the evidence is maintained and what the origin of the evidence is. Furthermore, the rules of evidence according to the ECT Act, Sections 15 (1)(2) and (3) [17], state that for evidence to be admissible, it must attain evidential weight. Evidential weight is achieved by demonstrating evidential integrity. There must be integrity and reliability in the handling of evidence generation, collection, storage and the algorithm employed in implementing the integrity of the evidence [11] [84]. Although the meaning of reliability may vary between jurisdictions, the general rule is to ensure that digital evidence is in its correct state in compliance with the evidential weight principle, which states that when the authenticity and accuracy of evidential data is demonstrated, evidential weight is achieved. In another vein, Dutelle [6] defined evidence as anything that can aid in proving or disproving that a crime has occurred and who are/is the crime perpetrator.

Section 15(2) of the ECT Act states that information in a digital form must be given due evidential weight to be allowed and used as digital evidence in a South African court of law. The evidential weight is measured to ensure that the authenticity and accuracy of the PDE is in a sound state in order to comply with the admissibility criterion [11] [84]. Furthermore, the following should be considered by a South African court when assessing the evidential weight of digital evidence [11]:

(i) The reliability of the manner in which the digital evidence was generated, stored, or communicated.

(ii) The reliability of the manner in which the integrity of the digital evidence was maintained.

(iii) The reliability of the manner in which the origins of the digital evidence were established.

(iv) The use of integrity verification algorithms. Other guidelines are in line with the Common Law requirements for evidence admissibility:

  (a) Relevant production of the digital evidence.

  (b) Presentation of the evidence in its original form when required.

  (c) Proof of the authenticity of the potential digital evidence[11].

In Section (16)(a)(b) and (c) of the ECT Act, the retention of digital information is prescribed in more detail. The data message must be accessible as well as useful for subsequent reference; the data message must be in its original generated format and its storage location must be proven to be free of irregularity. Furthermore, Section 51(1) of the ECT Act states that data collected can be used without permission from the subject, so long as the requirement of the law, such as a warrant, is adhered to. The integrity and preservation of digital data are further iterated in Section (16)(b) and 53(a) by stating the requirements for the protection of information that may otherwise affect national security and the economic and social wellbeing of the citizens. Such requirements may include the use of encryption, firewalls and access control [17], all of which should improve digital data sharing while maintaining control of the data.

3.1.2 *Protection of Personal Information Act*

The PoPI Act, Act 4 of 2013 introduced certain conditions to promote the protection of individual's information processed by public and private organisations [18]. This Act deals with protecting the rights of persons regarding unsolicited electronic communications and automated data gathering, and it regulates the flow of personal information across the borders of South Africa, especially as it applies to cloud computing.

The PoPI Act [18] [19] states that one can collect, process, store and share another entity‘s personal information in a responsible manner. Furthermore, the Act states that a court of law can accept gathered data (i.e. PDE captured of the perpetrator) that helps to identify a person who carried out unlawful activities as evidence, without the person's consent.

In Section 6 (c) (i) and (ii) and Section 37 (2) (a) and (b) of this Act, the exclusions and exemptions to an individual's privacy rights are outlined. These exemptions apply when the interests of national security are at stake and when they involve the prevention, detection and prosecution of criminal behaviour [82].

3.1.3 *Regulation of Interception of Communications and Provision of Communication-Related Information Act*

The RICA Act, Act 70 of 2002 [85] [86][87] enables the telecommunication providers to use equipment that allows for the interception of communication made on their networks. The Act regulates this interception, which is designed largely to prevent crime. Sections 5 and 16 (5) of the RICA Act outline how the Act encourages the interception of communication in order to protect public health, safety and security in South Africa, while Section 47 directs how evidence gleaned from such interception can be used in criminal proceedings. The RICA Act enables law enforcement agents to use digital information with the assistance of the postal service providers, telecommunication service providers and other stakeholders to carry out criminal investigations. This Act allows law enforcement agents to access information on digital devices, especially when it involves criminal activity. This information could include the geographical location as well as the time and frequency signal of the device.

3.1.4 *Criminal Procedures Act*

The CPA Act, Act 51 of 1977, Section 203 [88] is also relevant to this discussion on PDE and its use in mitigating crime. This Act is invoked by persons or individuals who, to ensure the safety of their life or to avoid self-endangerment, could invoke the non-compellable witness clause. This clause makes it possible for testimony by or potential evidence from a witness to be admissible in a court of law without the witness's physical presence to corroborate the alleged incident. Employing the CPA Act when using potential digital evidence renders null and void the requirement that an eyewitness needs to testify in relation to what was seen at the scene of an alleged crime.

The South African legislation discussed here regulates the use of digital evidence and the importance of digital data accuracy, integrity and consistency of collected digital evidence. The Acts mentioned (ECT, POPI CPA and RICA) [85] [88] [82] form the basis of legislation that enables this research to overcome obstacles posed by personal privacy concerns and the use of mobile devices in generating PDE information that could be employed in civil or criminal proceedings.

3.2 *Conclusion*

Having presented a brief overview of digital forensics, digital evidence, information security services and legal requirements as necessary to buttress the concepts used in this dissertation, the three background chapters conclude with a descriptive overview of requirements engineering specifications.

Chapter 4

REQUIREMENTS SPECIFICATIONS

4.1 *Introduction*

Requirements specifications (also referred to throughout this dissertation as requirements engineering specifications) denotes the processes applied in the design and development of software systems [89] [90] [91]. Requirements engineering specifications of a software system focus on the quality of software products. They take into account the various aspects of a system's design decisions and the conditions needed to solve a system's problems in order to achieve the system's objectives[89]. The success of a software system is measured by the extent to which the various conflicting aspects and stakeholders needs are managed, while adhering to the system's intended purpose. However, to effectively convey these requirements, proper communication aligned to the application's functional requirements, architectural requirements and architectural constraints must constitute the foundation for achieving a proper and solid system design [90] [92]. Figure 4.1 is a structural summary of the literature reviewed on the various aspects of requirements engineering specifications, the figure attempts to summaries various of existing studies.

Adopting the presentation of requirements engineering focusing on literature from various authors [90] [92] [89] [91], the author uses Figure 4.1 to illustrate the elements of a software system. In any software system's design, requirements engineering specifications employed must include the identification of the system's functional requirements (also known as the user's requirements), as well as the architectural requirements and the architectural constraints [89] [90]. The requirements and the processes employed to realise them are elaborated on in the sections that follow.

4.2 *Functional Requirements*

The functional requirements of a system identify and define the set of system components, inputs, the behaviour of the inputs at processing, and the expected resulting output during the design stage of the system [90] [93]. Functional requirements are the user's identified needs of the system that are presented in a natural, plain and understandable language to all stakeholders. It focuses on the behavioural requirements that describe

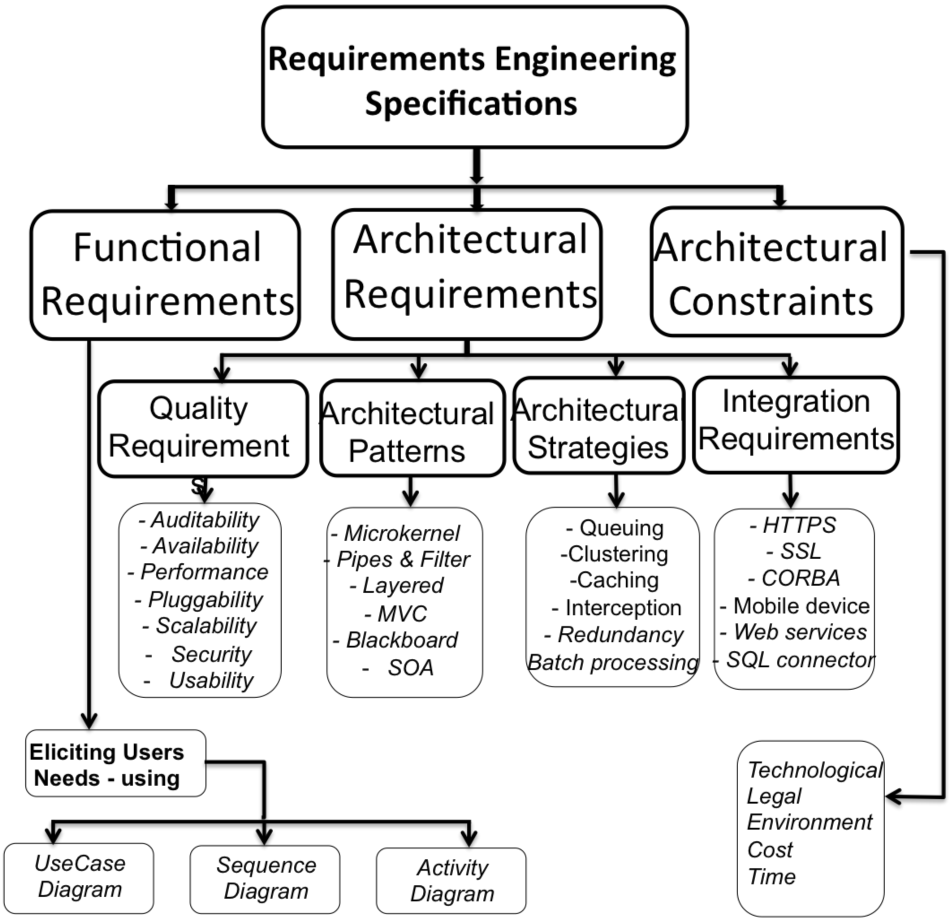


Fig. 4.1: Structural summary of the various literature on Requirements Engineering Elicitation

the use cases by capturing the role of the system's users and applying their various functions to the system [89] using use case diagrams to identify the services/components. Subsequently, sequence or activity diagrams are used to represent the transactions flow of the services/components as elicited from the use case diagrams.

A use case diagram is a representation of a user's interaction with a system [94]. It shows the relationship between the users and the various components/services within a system to be designed. Activity diagrams describe the dynamic aspects of the system using a flow chart to represent the flow of one activity to the next. A sequence diagram, on the other hand, shows the way components interact with one another in a particular sequential-ordered manner [95]. The identified needs of these users are mapped to the architectural requirements of the system, which are discussed next.

4.3 *Architectural Requirements*

Architectural requirements are the components of a system that are required to commence its high-level infrastructural design [96] [90]. The architectural requirements are the various non-functional requirements of a system, such as its quality requirements, the architectural patterns and architectural strategies that are used to address the core quality attributes of a system. The architectural requirements must meet the end-user‘s requirements and address the various stakeholders concerns [89]. Delivering the quality attributes of a system is critical to the success of the system's core objectives. The quality attributes of a system are concretely addressed using quality requirements, architectural patterns and architectural strategies, which are dealt with next.

4.3.1 *Quality Requirements*

The quality requirements of any system are the infrastructural elements that enable the system to meet the stakeholders' concerns. It is a means to concretely align the desired system's objectives with the architectural roadmap by using metrics and scales to quantify the system's expected output, as well as by identifying the trade-offs of quality requirements realised [91]. For example, in fulfilling the flexibility requirements of a system, it may be necessary to trade off security. Likewise, in realising the performance requirements of a system, reliability may be traded off. Some quality requirements (when overlooked at the system design stage) may require a complete rebuild of the system to incorporate the forgone quality requirements [96]. Quality requirements are grouped in terms of the various stakeholders needs of the system. For example, availability, flexibility, reliability and usability are more important to the system's end-users than are maintainability, portability, reusability and testability quality requirements, which are essential to the system designer or developer [89]. In a typical system, the following are some of the quality requirements:

(i) Security: A system is said to be secure when it can protect data against unauthorised user access and relinquish access to authorised users. Security is mostly characterised by the criteria of confidentiality, integrity and availability (CIA) [49]. Some strategies/tactics to achieve security include detecting attack, resisting attack and recovering from attack.

(ii) Usability: It is the degree to which the system can be used to achieve the intended goals with ease and accomplish a desired task effectively and efficiently, to the satisfaction of the intended users [96] [90]. The use of a three-tier architectural pattern, in conjunction with the Model-View-Controller (MVC) pattern, could be considered to enhance the usability of a system. The layered system will help to separate out the access tier, the business logic tier and the persistence tier, to realise the separation of concerns and to enhance flexibility, pluggability and durability of the system.

(iii) Availability: This refers to the ability of a system to mask or repair faults that minimise service outage time by mitigating faults and failures [90]. In discussing availability, faults, repair and failure must be mentioned. Although a fault causes failure of a system, faults can be prevented, tolerated, forecast or totally removed to help the system. A failure, on the other hand, is a deviation of the system from its specifications that are visible to the users, while repair refers to the time that a failure is not observable. Availability is calculated as the probability of a system to realise its specific service within a time interval, using the derivation of availability. It is mathematically represented as *(MTBF / MTBF + MTTR)*. This formula is employed to determine the level of availability of a system, especially when preparing its service level agreement (SLA) [90].

(iv) Scalability: It is the ability of a system to handle a certain amount of concurrent user traffic at the same time. It is determined by the resource needs of the entire system's users. Scalability can be achieved vertically or horizontally. Horizontal scaling occurs by scaling out some resources or by adding more resources. Vertical scaling involves a resource scale-up, such as using additional physical units. Some architectural strategies to address scalability include the use of concurrencies, support for scheduling, event queueing and resource scaling. Architectural patterns like black board, layered and service-oriented architecture (SOA) can be used to achieve scalability [89] [90].

(v) Performance: Performance is how well the system's resources function and the anticipated response time or waiting time while the system accesses, queries and retrieves information from the databases. Load balancing, stress, soak, spike and configuration testing could be employed to determine the performance metric [97]. Performance can be achieved by scaling up resources and managing resource demands by using spread load across resources, in other words, balancing loads and using concurrencies.

4.3.2 *Architectural Patterns*

Architectural patterns (also known as architectural styles) are reusable architectural solutions that enable innovation to be incorporated into systems and applications during the design phase [91] by providing infrastructures to be used to realise the quality requirements of any software system [96]. Architectural patterns focus on realising the multiple quality requirements of a system. As was listed in Figure 4.1, examples of architectural patterns include the following:

(i) The microkernel architectural pattern is the core service bus that provides the integration infrastructure for other layers of a system to connect with the system's main core. The microkernel architectural pattern focuses on achieving quality attributes such as security, modifiability and pluggability.

(ii) The pipes-and-filters architectural pattern is used to complement the abstraction layer of a system, such as employed in a reference architecture to realise a level of flexibility within the architecture. It can also be used to complement other architectural patterns to design a system [92]. For example, in a layered architectural pattern design, pipes and filters could be added at the first, second or third layer to strengthen the system's security.

(iii) Layered architectural patterns allow for the separation of concerns in a modular, componentalised system in order to decouple the activities of the system. Flexibility, pluggability, and modularity are achieved when a layered architectural pattern is employed [90].

(iv) Model-view-controller (MVC) architectural patterns are mostly used for user interfaces design and assist a system in the separation of concerns during design phase. The MVC makes provision for a separation of the components of a system, where the various parts of the system are divided into three interconnected parts, in order to successfully separate internal (inner working components of the system) and external (user interaction part) components of the system.

4.3.3 *Architectural Strategies*

Architectural strategies (also known as architectural tactics) are used to concretely address each one of the quality requirements of a system at a time. It specifies how a design must be carried out in order to concretely fulfil a single requirement of a system's core requirements [90]. Clustering, redundancy, resource monitoring and active rollback point are strategies used to achieve a system's availability, auditability and reliability (see Figure 4.1).

4.3.4 *Integration Requirements*

System integration is the process of bringing together the components/services of a software system's identified use cases to function as one system [89]. Integration requirements are therefore the artefacts that ensure that these subsystems (components) can function as one entity without adversely affecting the overall operations of the software application. In order to successfully link the various components of the system to function as one software system, Figure 4.1 identifies some artefacts to facilitate the software integration process.

4.4 *Architectural Constraints*

Architectural constraints are conditions attached to a system's requirements specifications, mostly by the stakeholders [89]. These architectural constraints can be in the form of technological, infrastructural, environmental, economic, legal or time factors, that could restrict the desired output of a system. The system is then required to find a way to incorporate the identified constraints at the architectural design phase of the system, while at the same time meeting the specified requirements. In summary, requirements engineering specifications are employed during the design and development stage of an application in order to determine the state of the application in terms of the required output or final product.

4.5 *Conclusion*

The presentation of requirements engineering specifications in this chapter completes the background section. The background chapters introduced the various aspects of the research, as well as keywords and terminologies that are meant to shed light on the contributions chapters. The presentation of the online neighbourhood watch (ONW) system is the first of these contribution chapters, which begins the next section.

Part III

MODELLING

This part comprises two chapters. The first chapter introduces the online neighbourhood watch (ONW) model and the security measures put in place to ensure that captured potential digital evidence (PDE) retains its originality and validity. The second chapter focuses on the roles of the PDE authorised users, while expanding on the security measures of the PDE in the ONW model. In the context of this research, the authorised user is regarded as any user with permission to carry out any number of functions on the ONW system.

Chapter 5

ONLINE NEIGHBOURHOOD WATCH MODEL

5.1 *Introduction*

Scientifically, a system is represented conceptually using a model, algorithm or prototype to mimic the intended system's structure and output [98] [99]. A model represents an example to be followed when a system is proposed [31] [100]. A conceptual model on the other hand is an abstraction of the activities that describe system objects in the real world. The ONW system's conceptual model serves as a structural plan to design the functionality of the ONW system. Data flow modelling (DFM), unified modelling language (UML) and a workflow model [100] are used in designing the conceptual model of the system. In addition, mathematical notations are used to formulate tuples that present and evaluate the forensic soundness of PDE captured using the ONW system. This chapter introduces the online neighbourhood watch (ONW) system's conceptual model as depicted in Figure 5.1.

The ONW system focuses on the processes employed by the uploader (citizens) to capture potential digital evidence (PDE), that is part A. Part B is on the download side and operated by the law enforcement agents. It involves the downloading and storage of PDE as well as the maintenance of chain of custody. Figure 5.1 shows the two parts of the proposed ONW system model consists of two parts - A and B. Part A of the ONW model is designed as a mobile device application termed - uWatch, to be used by citizens on the PDE capturing side. The uWatch application side of the ONW system also maintains the forensic soundness of captured PDE. The PDE captured by the community members is stored in a PDE repository (termed the ONW system's repository or NWS repository, this term is used interchangeably throughout this dissertation). It also shows how the captured PDE maintains its forensic soundness by employing the information security services as defined by the ISO/IEC 7498/2 [101][102] [33], in combination with the artfacts identified by this research as the forensic soundness indicators (FSIs). Forensic soundness, according

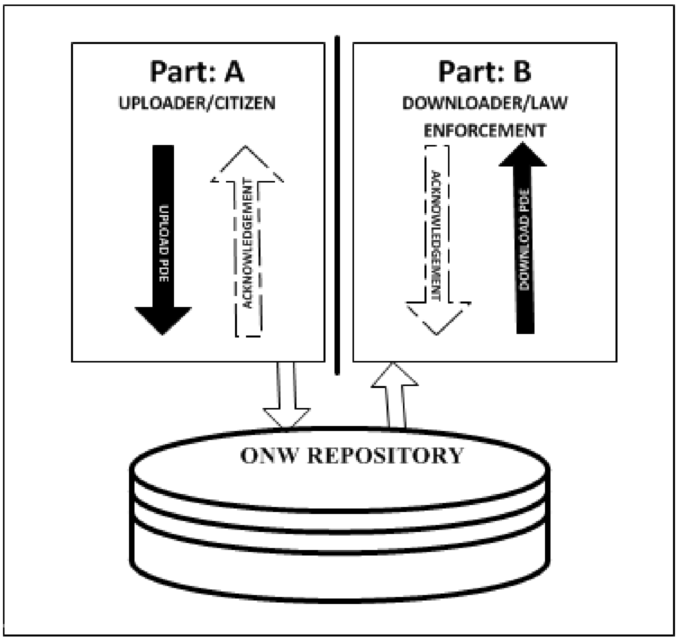


Fig. 5.1: High-level view of the ONW Model indicating Parts A and B and the ONW system's repository

to McKemmish [33] involves applying a transparent digital forensic process that preserves the original meaning of data that can be presented in any court.

Employing the FSIs by the ONW system maximises the usefulness of the captured PDE, as well as providing readily available potential evidence to law enforcement agents (LEA). Forensic soundness can be view in the context of this research, to be the content of a potential digital evidence (PDE) and the amount of the PDE metadata that can further be validated using the information security services implemented mechanisms. Forensic soundness therefore, is measured by the combination of information security services implementation and the amount of metadata preserved in the captured PDE.

The standard process of evidence admissibility only requires the integrity to be ensured as stipulated by the ECT Act, Act 25 of 2002. Traditionally, a law enforcement agent (LEA) would need to manually implement hashing on captured data (this level of forensic soundness is hereinafter termed "level 0" (R_{Lo}). Such a manual process presents the potential for integrity to be omitted, resulting in the potential for evidence to be manipulated, which can consequently lead to evidence inadmissibility. For instance, a LEA could compromise the integrity of evidence by (inadvertently) altering the content of the evidence prior to performing the hashing operation on the evidence. However, such inadvertent modifications are mitigated in the proposition presented in this study.

In the context of this research, PDE is digital data evidence gathered from physical crime scenes that has the potential of becoming admissible evidence. The gathered PDE can further be validated by an expert witness, and be used by LEAs or other authorised users in crime investigations. Therefore, PDE is considered evidence that can be used in any court of law when appropriate legal authorisation/permission is employed in its extraction, transmission, processing, storage and retrieval [103] [15].

The remainder of this chapter is structured as follows:

- **Section 5.2 focuses on the high-level view of the ONW model Part A.**
- **Section 5.3 gives a detailed description of Part A of the ONW model.**
- **Section 5.4 shows the process used to ensure the forensic soundness of PDE captured with the ONW system**
- **Section 5.5 discusses the realised process for user's privacy protection.**
- **Section 5.6 concludes this chapter.**

5.2 *High-Level View of the ONW System's Model - Part A*

Part A of the ONW system enables citizens in a neighbourhood to capture and store PDE as audio, video or photographs of potential crime that they witness in and around their communities using their mobile device on the uWatch environment. Figure 5.2 provides the high-level view of Part A of the ONW system, that is the uWatch application side of the system. It comprises of seven processes as shown in Figure 5.2, namely (i) Install (ii) Capture PDE (iii) Authenticate (iv) Apply FS (v) Upload PDE (vi) Audit Log (vi) Acknowledgment. These processes are further split up to derive the lower-level functionalities to be carried out by the users of the ONW system. The detailed functions of the ONW system's model as depicted in Figure 5.3 are elaborated on in subsection 5.3.

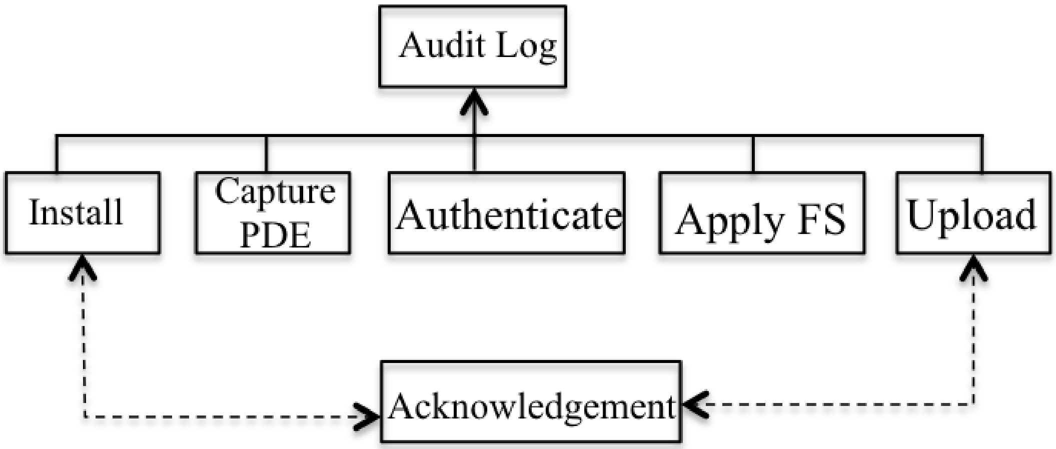


Fig. 5.2: High-Level Process of the ONW System Part A - uWatch

Figure 5.2 provides the high-level view of Part A of the ONW system, that is the uWatch application side of the system using a flow diagram. This diagram reveals a sequential interactive communication flow of components of the ONW system.

5.3 *Detailed Process flow of Part A of the ONW System Model - uWatch*

The captured PDE is stored in the ONW system and the stored PDE is made available to the law enforcement agents (LEAs), digital forensic investigators (DFIs) and the justice system. Throughout this research, an authorised user is defined as any user that has been assigned a role and has been given permission to carry out any number of functions on the ONW system. The goal of the ONW system is to increase the volume of available potential evidence to enhance success in the prosecution of neighbourhood crime, thereby securing the conviction of the actual culprits, while at the same time ensuring, confidentiality, integrity and non-repudiation of the captured and stored digital data. As highlighted in Section 1.3, this research did not design a new cryptographic algorithm. Rather, it utilised already existing cryptographic mechanisms, which are inbuilt in the Android encryption library and in the web-application encryption library. Figure 5.3 is the process flow of Part A of the ONW system model, that is, the citizen side used to capture potential digital evidence - uWatch application. The forensic soundness addressed by this part focuses on confidentiality, non-repudiation and integrity represented throughout this research as "level 1" $\Rightarrow \mathrm{R}_{\mathrm{L}1}$.

The sequential flow of events from the time a citizen captures potential evidence to its final upload to the NWS repository is shown in Figure 5.4a and Figure 5.6a. *Note that the sequence presented in Figure 5.6a is the continuation of the sequence in Figure 5.4a, which were originally one figure. However, for ease of reading and comprehension, the figures are separated by a number of pages in order to bring them closer to their respective discussion in the dissertation. Therefore, Figures 5.4a and 5.6a should be read as one figure, where applicable.* The PDE uploading process begins with a sequence of activities as follows:

1. A request from the NWS for a certificate authority (CA) to verify the identity of the uWatch application and the NWS. This is followed by the creation of an asymmetric key pair by the encryption library by both uWatch and the NWS.
2. Encryption of Username and Password using the NWS public key and the decryption of uWatch username and password by the NWS for verification of the user id
3. Symmetric key exchange process between the uWatch and the NWS and
4. Upload of the captured payload and the audit log files. Details of these components that formed the process of the uWatch and NWS communication chain are elaborated on in the sections of the components in the flow diagram of Figure 5.3

5.3.1 *Install uWatch Application*

The process flow diagram of the uWatch application is shown in Figure 5.3. It shows that citizens who wish to participate in PDE crowd-sourcing are required to install the ONW

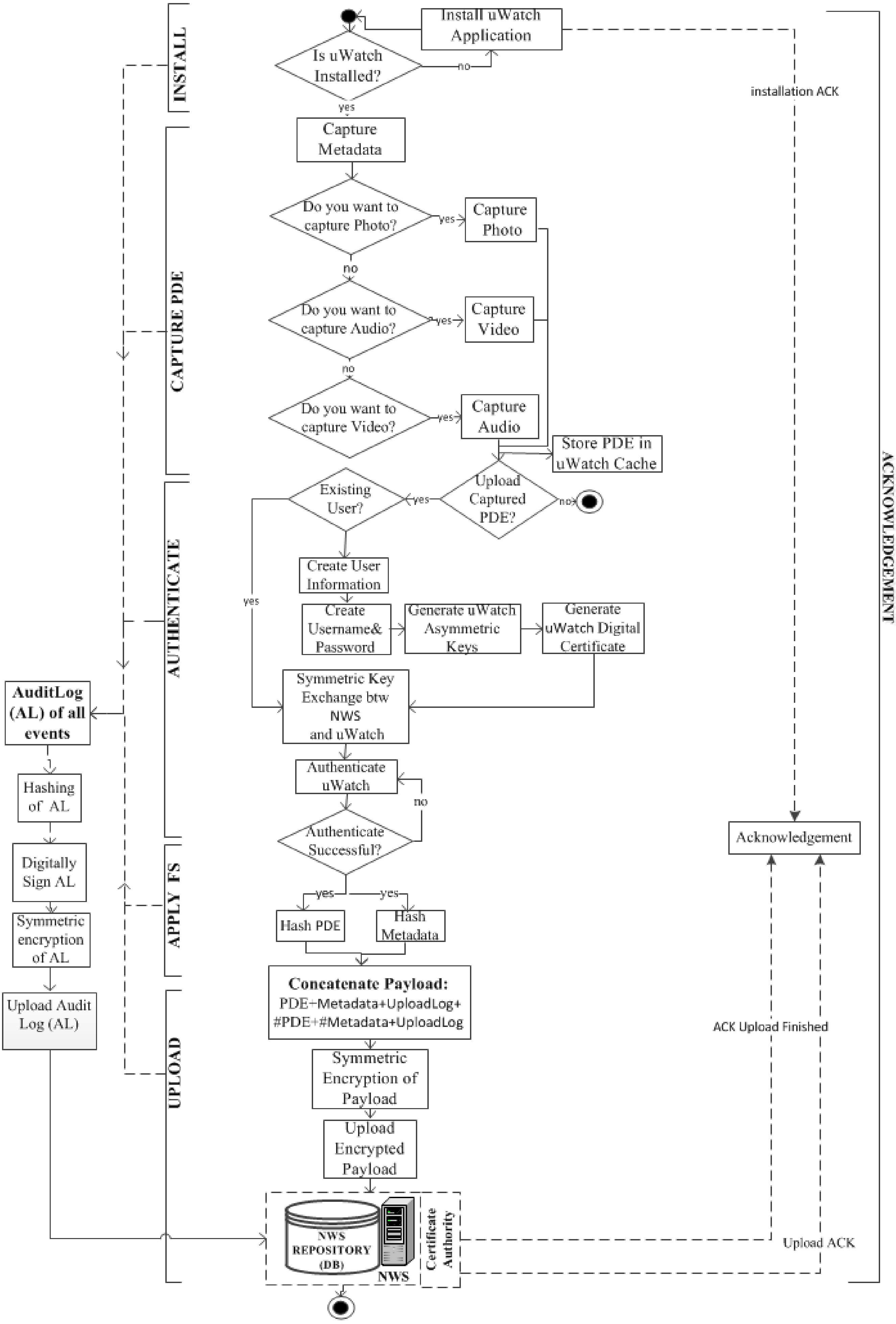


Fig. 5.3: Low-Level View of the ONW Model Part A - Focusing on R_{L1}

system‘s application (uWatch) on their mobile device to commence the PDE-capturing. The uWatch application installation is a mandatory requirement a citizens must abide by.

5.3.2 *Capture Metadata and Potential Digital Evidence*

Capturing PDE and PDE metadata is the process used by community members to generate PDE of potential crime in their neigbourhourhood. The PDE are in the form of video, audio or photo. The PDE metadata on the other hand, include (i) device name/type (ii)time / date stamp (ii) geographical location (geolocation) (iv) International mobile equipment identity (IMEI) (v) WiFi connection identifier (vi) GSM data connection. These are combined with the mechanisms that address information security services to achieve forensic soundness.

The PDE payload captured is categorised as PDE, plus metadata since they are split at the upload process. The PDE-capturing process begins when a citizen witnesses an incident related to a criminal act. The hypothesis of this research is based on the assumption that the citizen has a mobile device capable of capturing digital data, i.e., audio or video or digital photo images (termed as PDE) as shown in Figure 5.3. The PDE must be captured on the uWatch application - that is the ONW system’s application domain - to retain the forensic soundness of the captured PDE and therefore enhance its admissibility. As depicted in Figure 5.3, the PDE forensic soundness is applied from the moment a citizen captures the PDE. The forensic soundness indicators (FSIs) were adopted to ensure that the PDE captured with the uWatch application meets the admissibility requirements, especially in South Africa. This forensic soundness implementation process adopted by this research is such that confidentiality, integrity, authentication, authorisation and non-repudiation is automated in the PDE capturing process.

5.3.3 *Store PDE in uWatch Cache*

For users (citizens) to participate in the PDE sourcing process of the ONW system, they firstly have to install the application to their mobile device. As depicted on Figure 5.3, on the installation of the uWatch application, users may create their user information before commencing PDE capture, which then leaves the users with the option to log-in when PDE is captured and ready to be uploaded to the NWS repository. The users could perform three functions at their download of the application (i) Create user information (iii) Log-in to upload (ii) or to upload the captured PDE. A captured PDE is either sent forth to the NWS repository immediately after capture, or stays in the uWatch application’s cache until the user is ready to send. The upload process (termed authentication), which also includes the certificate authority (CA) creation $\mathrm{CA}_{\mathrm{pub}}$ and $\mathrm{CA}_{\mathrm{priv}}$ verifications of users, asymmetric key pair generations $\mathrm{N}_{\mathrm{pub}}, \mathrm{N}_{\mathrm{priv}}$ and $\mathrm{U}_{\mathrm{pub}}, \mathrm{U}_{\mathrm{priv}}$, symmetric key generation and exchange (K) are all addressed when a user initialises PDE payload upload.

5.3.4 *Create User Information*

As depicted in Figure 5.3, the citizen who opts to participate in the ONW system, (uWatch application and NWS), is required to create a user information. The user information creation ensures a chain of custody and chain of evidence is in place as part of PDE validity checking. The citizen can upload the acquired PDE to the repository once his/her profile has been created. An already existing user does not need to register but is required to logon to upload PDE. To enhance PDE admissibility, the user profile creation is a compulsory function.

5.3.5 *Create username and Password*

The access process is designed such that an existing user can login to upload captured PDE, while a first time user is required to provide user information by creating a user profile to upload captured PDE. This is when the uWatch application creates the user information identification. The encryption library of uWatch then creates its public and private key, the CA subsequently uses the user's created information ID for the certificate generation.

5.3.6 *Generate uWatch Asymmetric key pair and Digital Certificates*

As seen in Figure 5.3 the uWatch application's encryption library creates and manages the asymmetric key pair generation - termed U_{pub} and U_{priv}. The encryption library uses U_{pub} and U_{priv} for its secure communication and verifies the uWatch identity, as well as other encryption requirements of uWatch. For uWatch to communicate with the NWS, the asymmetric key pair is necessary. The certificate authority (CA) is self-signed and is hosted within the ONW system. This is in order to manage cost efficiency, thereby removing the burden of cost on the part of the uWatch clients. Obtaining the uWatch client certificates and public/private key pair is an essential means to ensure non-repudiation. The CA is self-signed to enable the uWatch and the NWS act as trusted parties. The CA uses the public key and identification information of the uWatch and that of the NWS to verify their identity, then sign them to enable the two parties communicate. The CA is managed within the ONW system for cost elimination on the part of the citizen. The certificate generation process is depicted in Figure 5.4a, and the public key, plus the uWatch generated certificate identity information is sent through to CA. The certificate identification information (Cert. ID info) refers to the name, address, email address, telephone numbers and any other user information that can be used to identify the actual user of a certificate. The uWatch and NWS creates their certificate identification information (Cert. ID info). The Cert. ID info is sent to the certificate authority (CA) for signing. The signed process is depicted in Figure 5.4a as follows; (a) The CA verifies the request, (b) creates a hash of the U_{cert} = H(U_{cert}) (c) signs the $U_{cert_{DS}}$= E(CA_{priv}, U_{cert}). The $U_{cert} + U_{cert_{DS}}$ are then the signed certificates. For clarity, the signed certificate for uWatch application is termed $\mathrm{U_{cert}}$. After signing $\mathrm{U_{cert}}$, the uWatch is considered a trusted party and can communicate using the signed certificate $\mathrm{U_{cert}}$ as one of its authentication mechanisms.

5.3.7 *Symmetric Key Exchange between NWS and uWatch*

As depicted in Figure 5.4a, the symmetric key exchange occurs between the NWS and uWatch to be used for the encryption of payload. The symmetric key exchange process only commences after the verification of the user's identity by the certificate authority (CA). The CA at this stage of key exchange has signed and verified the uWatch and the NWS system. The exchanged key (K) is to be encrypted and stored by the NWS for use at payload download.

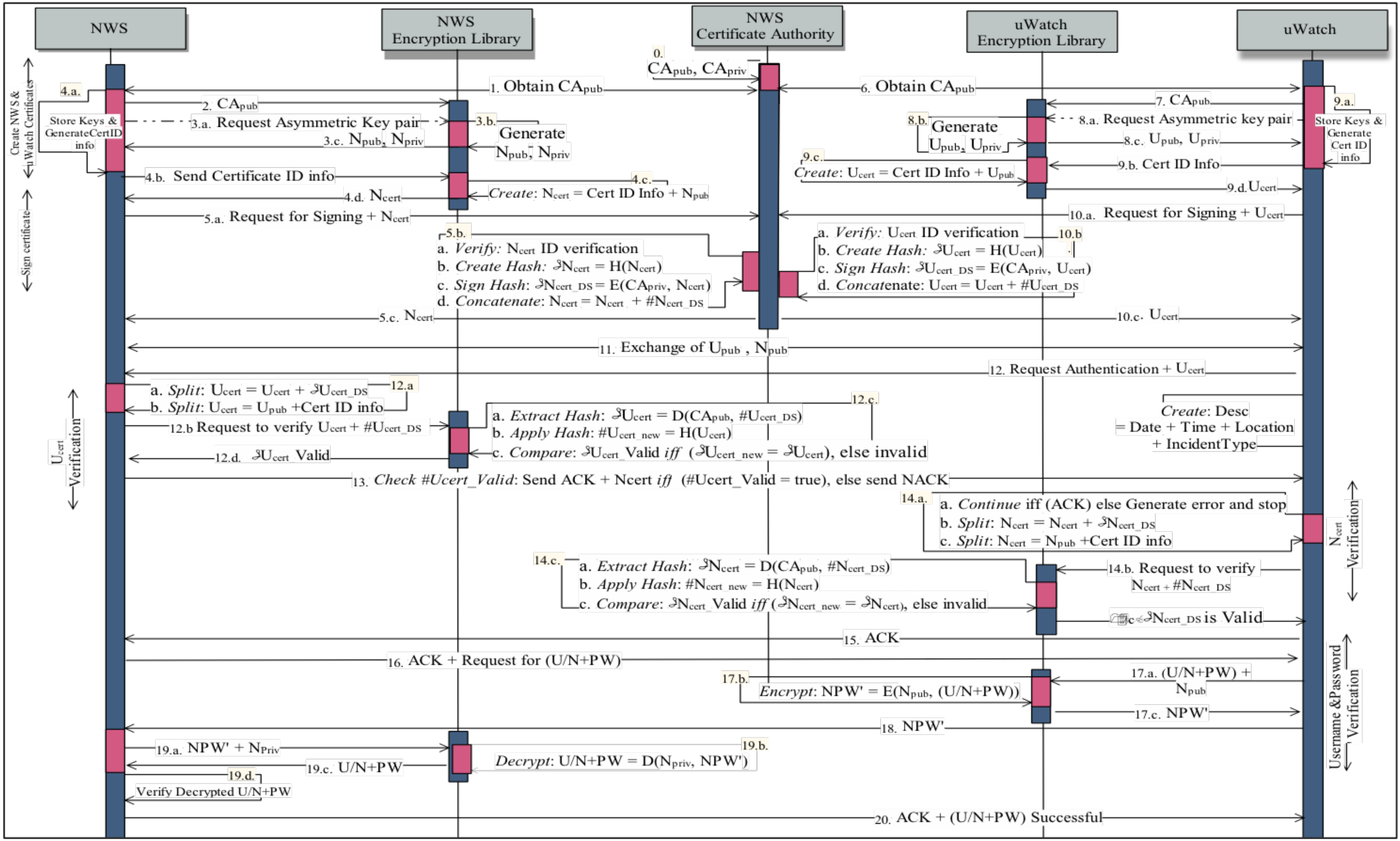

NWS
NWS Encryption Library
NWS Certificate Authority
uWatch Encryption Library
uWatch
0. CA_{pub}, CA_{priv}
1. Obtain CA_{pub}
6. Obtain CA_{pub}
Create NWS & uWatch Certificates
4.a.
Store Keys & GenerateCertID info
2. CA_{pub}
3.a. Request Asymmetric Key pair
3.b.
Generate N_{pub}, N_{priv}
3.c. N_{pub}, N_{priv}
4.b. Send Certificate ID info
4.c.
Create: N_{cert} = Cert ID Info + N_{pub}
4.d. N_{cert}
7. CA_{pub}
9.a.
Store Keys & Generate Cert ID info
8.a. Request Asymmetric key pair
8.b.
Generate U_{pub}, U_{priv}
8.c. U_{pub}, U_{priv}
9.b. Cert ID Info
9.c.
Create: U_{cert} = Cert ID Info + U_{pub}
9.d. U_{cert}
Sign certificate
5.a. Request for Signing + N_{cert}
5.b.
a. Verify: N_{cert} ID verification
b. Create Hash: ℑN_{cert} = H(N_{cert})
c. Sign Hash: ℑN_{cert_DS} = E(CA_{priv}, N_{cert})
d. Concatenate: N_{cert} = N_{cert} + #N_{cert_DS}
5.c. N_{cert}
10.a. Request for Signing + U_{cert}
10.b
a. Verify: U_{cert} ID verification
b. Create Hash: ℑU_{cert} = H(U_{cert})
c. Sign Hash: ℑU_{cert_DS} = E(CA_{priv}, U_{cert})
d. Concatenate: U_{cert} = U_{cert} + #U_{cert_DS}
10.c. U_{cert}
11. Exchange of U_{pub} , N_{pub}
12. Request Authentication + U_{cert}
U_{cert} Verification
a. Split: U_{cert} = U_{cert} + ℑU_{cert_DS}
12.a
b. Split: U_{cert} = U_{pub} +Cert ID info
12.b Request to verify U_{cert} + #U_{cert_DS}
12.c.
a. Extract Hash: ℑU_{cert} = D(CA_{pub}, #U_{cert_DS})
b. Apply Hash: #U_{cert_new} = H(U_{cert})
c. Compare: ℑU_{cert} Valid iff (ℑU_{cert_new} = ℑU_{cert}), else invalid
12.d. ℑU_{cert} Valid
Create: Desc = Date + Time + Location + IncidentType
13. Check #Ucert_Valid: Send ACK + Ncert iff (#Ucert_Valid = true), else send NACK
14.a.
a. Continue iff (ACK) else Generate error and stop
b. Split: N_{cert} = N_{cert} + ℑN_{cert_DS}
c. Split: N_{cert} = N_{pub} +Cert ID info
N_{cert} Verification
14.b. Request to verify N_{cert} + #N_{cert_DS}
14.c.
a. Extract Hash: ℑN_{cert} = D(CA_{pub}, #N_{cert_DS})
b. Apply Hash: #N_{cert_new} = H(N_{cert})
c. Compare: ℑN_{cert} Valid iff (ℑN_{cert_new} = ℑN_{cert}), else invalid
ℑN_{cert_DS} is Valid
15. ACK
16. ACK + Request for (U/N+PW)
17.a. (U/N+PW) + N_{pub}
17.b.
Encrypt: NPW' = E(N_{pub}, (U/N+PW))
17.c. NPW'
Username &Password Verification
18. NPW'
19.a. NPW' + N_{Priv}
19.b.
Decrypt: U/N+PW = D(N_{priv}, NPW')
19.c. U/N+PW
19.d.
Verify Decrypted U/N+PW
20. ACK + (U/N+PW) Successful

Fig. 5.4a: Communication Sequence between NWS and uWatch Application

5.3.8 *Authenticate uWatch*

As shown in Figure 5.3, the authentication between uWatch and NWS commence when the citizen chooses to upload captured PDE. The PDE uploading process is on the mobile application side (uWatch) of the ONW system. The neighbourhood watch system side (NWS) undergoes a series of processes to transmit captured PDE from the user (citizen) to the NWS repository. This process maintains the chain-of-evidence, ensures the chain-of-custody, addresses some information security services (confidentiality, integrity, and non-repudiation) of the captured PDE as well as upholds and protects the personal information of the uploader (citizen). As highlighted in the limitation section of this study (1.3), this research adopted existing encryption mechanisms in order to ensure that the various information security services of the captured PDE are forensically sound.

The PDE payload is uploaded from the ONW system's mobile application side (uWatch application) to the ONW system's downloader side (NWS system). The assumption however is that the certificate authority (CA) is self-signed and that the CA is managed within the NWS. Firstly, the certificate authority (CA) generates its own asymmetric public and private keys, which are then used in the signing and verification of the two parties (i.e. uWatch and NWS) who requires them for communication. Other steps involved include the asymmetric key exchange, digital certificate creations and symmetric key generation and exchange. The steps taken to achieve the authentication process are presented in Figures 5.4a and 5.6a, and explained as follows:

1. The CA creates its own $\mathrm{CA_{pub}}$ and $\mathrm{CA_{priv}}$
2. The $\mathrm{CA_{pub}}$ is sent to the NWS and the uWatch application
3. The NWS and uWatch application each uses their encryption library to request and create their respective asymmetric key pair $(\mathrm{N_{pub}}, \mathrm{N_{priv}}$ and $\mathrm{U_{pub}}, \mathrm{U_{priv}})$
4. The NWS and uWatch application create their certificate ID information, and then request the CA to sign certificate IDs by sending their public keys $(\mathrm{N_{pub}}$ and $\mathrm{U_{pub}})$, which are then used by the CA to do the following:
   (a) The CA verifies the request of uWatch and NWS
   (b) The CA creates a hash of the $\mathrm{U_{cert}}$ = H $(\mathrm{U_{cert}})$
   (c) The CA signs the i.e., $\mathrm{U_{cert_{DS}}}$ = E $(\mathrm{CA_{priv}}, \mathrm{U_{cert}})$ and consequently do the same for $\mathrm{N_{cert}}$. The signed$\mathrm{U_{cert}} + \mathrm{U_{cert_{DS}}}$ and $\mathrm{N_{cert}} + \mathrm{N_{cert}}$ form the signed certificate respectively. For clarity, the signed certificate is referred to as $\mathrm{N_{cert}}$ or $\mathrm{U_{cert}}$ for NWS and uWatch respectively.
5. The signed $\mathrm{N_{cert}}$ and $\mathrm{U_{cert}}$ are sent back to their respective sides of the system.

6. The NWS and the uWatch application exchange their $\mathrm{N}_{\mathrm{pub}}$ and $\mathrm{U}_{\mathrm{pub}}$ asymmetric keys to be able to effect key exchange later and so are able to commence/initialise subsequent communications.

7. The uWatch then requests for authentication and sends along its $\mathrm{U}_{\mathrm{cert}}$, along with the uWatch authentication request. The NWS receives this request, sends the received $\mathrm{U}_{\mathrm{cert}}$ to NWS encryption library to be hashed using $\mathrm{CA}_{\mathrm{pub}}$ and compared the digest (hash). To perform this check, the NWS library does the following:

   (a) It splits $\mathrm{U}_{\mathrm{cert}}$ into $\mathrm{U}_{\mathrm{cert}}$ + $\mathrm{U}_{\mathrm{cert}_{\mathrm{DS}}}$

   (b) It splits $\mathrm{U}_{\mathrm{cert}}$ to $\mathrm{U}_{\mathrm{pub}}$ + Cert ID information

   (c) It extracts the hash from $\mathrm{U}_{\mathrm{cert}}$ using $\mathrm{CA}_{\mathrm{pub}}$ i.e., (D $(\mathrm{CA}_{\mathrm{priv}}$, #$\mathrm{N}_{\mathrm{cert}})$

   (d) It applies a new hash to $\mathrm{U}_{\mathrm{cert}}$ to get $\mathrm{U}_{\mathrm{cert}_{\mathrm{n}}\mathrm{ew}}$, then compares the original hash of the $\mathrm{U}_{\mathrm{cert}}$ sent by uWatch to the hash created by its encryption library called #$\mathrm{U}_{\mathrm{cert}_{\mathrm{n}}\mathrm{ew}}$. If they match, the $\mathrm{U}_{\mathrm{cert}}$ is valid. The NWS the sends acknowledgment plus $\mathrm{N}_{\mathrm{cert}}$ to uWatch.

8. The uWatch performs a similar operation on $\mathrm{N}_{\mathrm{cert}}$ using its encryption library and $\mathrm{CA}_{\mathrm{pub}}$ to decrypt and verify the hashes in order to determine if $\mathrm{N}_{\mathrm{cert}}$ is valid. At the validation and verification of this process, NWS requests for a username and password from uWatch.

9. The uWatch then encrypts its username and password using $\mathrm{N}_{\mathrm{pub}} \Rightarrow$ NPW' $\Rightarrow$ E$(\mathrm{N}_{\mathrm{pub}}$, U/N+PW). The NWS decrypts the password using its private key $\mathrm{N}_{\mathrm{priv}}$, and then verifies the username and password. Finally, NWS sends acknowledgement of password success to the uWatch application.

5.4 *Forensic Soundness Levels*

This section continue as in Figure 5.3 but focuses on describing the detailed process employed to add automated forensic soundness implementation to the PDE captured and stored with the ONW system (uWatch and NWS). The process as depicted in Figure 5.3 focusing on 1. Hashing PDE; 2. Hashing metadata, 3. Payload concatenation 4. Symmetric key generation and 5. Encrypting PDE payload and upload. are used to addressed the forensic soundness level - which is the minimum level of forensic soundness known as "level 1" L_1forensic soundness. Through out this research, "level 0" L_0, "level 1" L_1 and "level 2" L_2 are used to denote the various levels of forensic soundness of PDE.

Using an automated process to ensure forensic soundness of PDE captured using the uWatch application averts the challenges often associated with potential evidence accrued from untrained citizens (like from the social media platform). Furthermore, the automated process added two-levels of forensic soundness on PDE. This is necessary because, digital evidence is summarily rejected and thrown out of court as evidence in legal proceedings, when there are any element of doubt as to the originality of the evidence [104].

5.4.1 *The Information Security Services*

The FSIs involve the use of the information security services i.e., confidentiality, integrity, authentication, authorisation and non-repudiation (CIA_tA_zN) [105] [33] [106][107]. As shown in Table 5.1, these are termed (C I$(A_tA_z$ N) which is summarily called $(\mathrm{R}_{\text{Mechanisms}})$. These $(\mathrm{R}_{\text{Mechanisms}})$ are combined with the PDE metadata properties $(\mathrm{R}_{\text{Metadata}})$ and the captured PDE $(\mathrm{R}_{\text{PDE}})$ to achieve forensic soundness of all captured and stored PDE of the ONW system.

Table 5.1: The Information Security Services

Information security Services (CIA_tA_zN)	**Particular mechanisms used to implement the CIA_tA_zN services in this Study**
Confidentiality (C)	*Application of symmetric and symmetric encryption* - This is a means to protect the identity of the PDE uploader (citizens), encrypt PDE using both asymmetric and symmetric encryption. Therefore confidentiality (addresses the privacy of the captured and stored PDE data)
Integrity (I)	*Hashing* - Integrity is where PDE is ensured of no alteration on transit or at storage between the uploading citizen and the downloader. A cryptographic hash function is employed to guarantee integrity
Authententication (A_t)	*Username and password* - Users are required to provide login information of username and password. Authentication deals with who created or sent the data
Authorisarion (A_z)	*Role based access control (RBAC).* The restriction of PDE usage to the intended authorised users (i.e. the law enforcement agents, the digital forensic investigators and the judiciary). Authorisation is implemented using session authenticator, digital certificates, access control and message authentication codes (MACs).
Non repudiation (N)	*Digital certificate + digital signature + asymmetric encryption* - This is achieved when the uploader's original intention is upheld. For example, the uploader of PDE cannot deny at a later time, his/her intentions in the creation or transmission of the PDE. The identity of the uploader is associated with the uWatch application, its public and private keys, the certification identification information and the symmetric key exchange, in which the other pair is only associated with a user.

The information services (CIA_tA_zN) that is, $R_Mechanisms := (C, I, A_t, A_z, N)$ where C ⇒ confidentiality, I ⇒ integrity, A_t ⇒ authentication, A_z ⇒ authorisation are used in implementing the PDE forensic soundness are summarised in Table 5.1

Apart from integrity, the remainder of these services serves as an extension to the standard hashing process, which usually address evidence integrity. The extended integration, which includes confidentiality, non-repudiation, authentication and authorization, are categorized into two extended forensic soundness levels (hereinafter termed L_1, and L_2 respectively). This study, thus, extends the premise of admissibility to include confidentiality and non-repudiation as (L_1) as well as authentication and authorization as (L_2).

5.4.2 *Relational Representation of Forensic Soundness Levels*

Assuming that the forensic soundness (FS) of an item of evidence identified by a unique id can be defined by the natural joining of three sets of tuples relation where the three sets are respectively defined as follows, $x - tuples \in$ PDE, y - tuples $\in$ Metadata, z - tuples $\in$ Mechanisms as expressed in equation 5.1

$$R_{FS} = (R_{PDE} \bowtie (R_{Metadata} \bowtie R_{Mechaisms})) \tag{5.1}$$

Where;
R_{PDE} := (id, p, a, v);
id ⇒ identifier, p ⇒ photo, a ⇒ audio, v
$Rightarrow$ video

$R_{Metadata}$:= (id, C_{nw}, C_{wf}, D$_t$,D_n,D_i,T_s,D_s,G), where $C_{nw} \bigoplus C_{wf}$;
id ⇒ identifier, D$_t$ ⇒ Device type, D$_n$ ⇒ Device name, D$_i$ ⇒ Device IMEI, T$_s$ ⇒ Timestamp, D$_s$ ⇒ Date/stamp, G ⇒ Geolocation, C_{nw} ⇒ network connection, C_{wf} ⇒ WiFi connection.
$R_{Mechanisms}$:= (id, CIA_tA_zN)
where
id ⇒ identifier, C⇒ confidentiality, I ⇒ integrity, A$_t$ ⇒ authentication, A$_z$ ⇒ authorisation, N⇒ non-repudiation.
The (C_{nw}) and (C_{wf}) are however mutually exclusive $\bigoplus$ where by at any given circumstance, the capture PDE (i.e.,R_{PDE}) should have been captured and uploaded using WiFi connection (C_{wf}) or with the use of mobile network connection (C_{nw}). The (C_{nw}) and (C_{wf}) attributes of $R_{Metadata}$ are such that, the intersection between the (C_{nw}) and (C_{wf}) - will yield an empty set$(\emptyset)$ - $C_{nw} \cap C_{wf} = \emptyset$.

5.4.3 *Forensic Soundness Instances*

The number of probable instances that satisfy each forensic soundness level can be denoted using the relational algebra formal expression in equation below (**??**).

Then, a relation of the logical representation for the minimum forensic soundness R_{L0} can be defined as shown in equation 5.2.

$$R_{L0=}\begin{cases}\sigma PDE = "\beta" \wedge M_{echaism} = "\alpha" \wedge M_{etadata} = "\phi" \wedge M_{etadata} = "C_{nw}" \wedge (R_{FS}) \\ \sigma PDE = "\beta" \wedge M_{echaism} = "\alpha" \wedge M_{etadata} = "\phi" \wedge M_{etadata} = "C_{wf}" \wedge (R_{FS})\end{cases}$$

where
$\alpha = "I"$;
$\phi = D_t, D_n, D_i, T_s, D_s, G$;
$\beta = p, a, v$
(5.2)

The expression in equation 5.2 states that the generated PDE is a selection from a probable combination of PDE, the metadata, and the mechanism, indicating a minimum forensic soundness level of R_{L0}. The expression in equation 5.2 is the generic representation for the selection of R_{L0} at an instance when integrity is used. Similarly, the expression for the proposed extended forensic soundness for R_{L1} and R_{L2} are presented in equation 5.2 and 5.2 respectively.

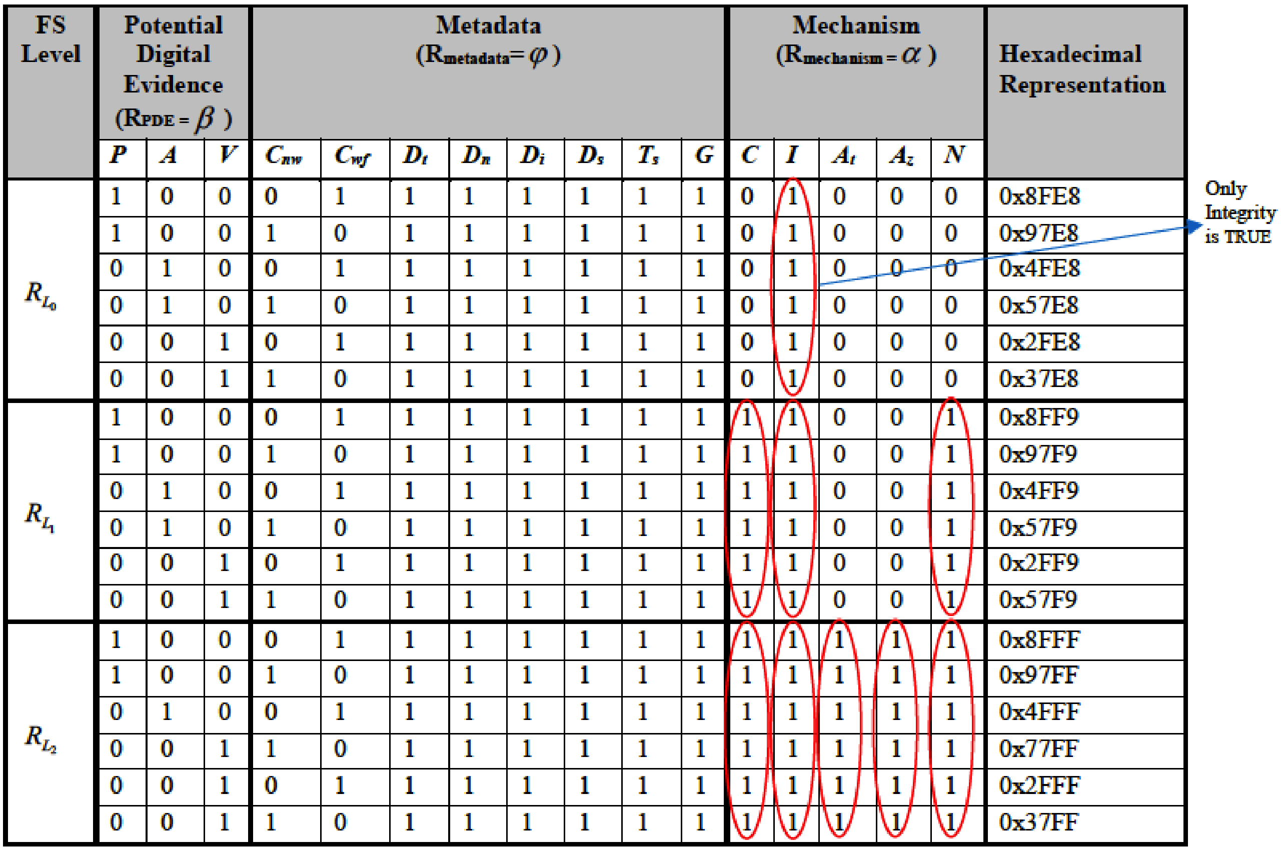
$$R_{L1} = \begin{cases}\sigma PDE = "\beta" \wedge M_{echaism} = "\alpha" \wedge M_{etadata} = "\phi" \wedge M_{etadata} = "C_{nw}" \wedge (R_{FS}) \\ \sigma PDE = "\beta" \wedge M_{echaism} = "\alpha" \wedge M_{etadata} = "\phi" \wedge M_{etadata} = "C_{wf}" \wedge (R_{FS})\end{cases}$$

where $\alpha = C, I, N$;
$\phi = D_t, D_n, D_i, T_s, D_s, G$;
$\beta = p, a, v$
(5.2)

$$R_{L2} = \begin{cases}\sigma PDE = "\beta" \wedge M_{echaism} = "\alpha" \wedge M_{etadata} = "\phi" \wedge M_{etadata} = "C_{nw}" \wedge (R_{FS}) \\ \sigma PDE = "\beta" \wedge M_{echaism} = "\alpha" \wedge M_{etadata} = "\phi" \wedge M_{etadata} = "C_{wf}" \wedge (R_{FS})\end{cases}$$

where $\alpha = C, I, A_z, A_t, N$;
$\phi = D_t, D_n, D_i, T_s, D_s, G$;
$\beta = p, a, v$
(5.2)

These representations are further expanded to illustrate all probable states of the forensic soundness of the captured PDE using binary logic, as shown in Table 5.5.



FS Level	Potential Digital Evidence ($R_{PDE} = \beta$)			Metadata ($R_{metadata} = \varphi$)								Mechanism ($R_{mechanism} = \alpha$)					Hexadecimal Representation
	P	A	V	C_{nw}	C_{wf}	D_t	D_n	D_i	D_s	T_s	G	C	I	A_t	A_z	N	
R_{L_0}	1	0	0	0	1	1	1	1	1	1	1	0	1	0	0	0	0x8FE8
	1	0	0	1	0	1	1	1	1	1	1	0	1	0	0	0	0x97E8
	0	1	0	0	1	1	1	1	1	1	1	0	1	0	0	0	0x4FE8
	0	1	0	1	0	1	1	1	1	1	1	0	1	0	0	0	0x57E8
	0	0	1	0	1	1	1	1	1	1	1	0	1	0	0	0	0x2FE8
	0	0	1	1	0	1	1	1	1	1	1	0	1	0	0	0	0x37E8
R_{L_1}	1	0	0	0	1	1	1	1	1	1	1	1	1	0	0	1	0x8FF9
	1	0	0	1	0	1	1	1	1	1	1	1	1	0	0	1	0x97F9
	0	1	0	0	1	1	1	1	1	1	1	1	1	0	0	1	0x4FF9
	0	1	0	1	0	1	1	1	1	1	1	1	1	0	0	1	0x57F9
	0	0	1	0	1	1	1	1	1	1	1	1	1	0	0	1	0x2FF9
	0	0	1	1	0	1	1	1	1	1	1	1	1	0	0	1	0x57F9
R_{L_2}	1	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	0x8FFF
	1	0	0	1	0	1	1	1	1	1	1	1	1	1	1	1	0x97FF
	0	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	0x4FFF
	0	0	1	1	0	1	1	1	1	1	1	1	1	1	1	1	0x77FF
	0	0	1	0	1	1	1	1	1	1	1	1	1	1	1	1	0x2FFF
	0	0	1	1	0	1	1	1	1	1	1	1	1	1	1	1	0x37FF

Only Integrity is TRUE

Fig. 5.5: Summary of Probable Forensic Soundness States using Binary representations

For each forensic soundness level, $R_{L_2}R_{L_1}$ and R_{L_0} there exist a probable relation among PDE, Metadata, and Mechanism for which forensic soundness can be defined. The binary representation can also be used to show the forensic soundness, where each row corresponds to a **'True'(1)** or a **'False'** **(0)** for any of the hexadecimal representation of the concatenated binary logic is further given in the last column of Table 5.5. For example, the sequence $(P(C_{nw}, D_t, D_n, D_i, T_s, D_s, G), I) = 0X8FE8$ belongs to the minimum forensic soundness level R_{L_1} of a photo. Similarly $(P(C_{nw}, D_t, D_n, D_i, T_s, D_s, G), C, I, N) = 0x8FF9$ and $(P(C_{nw}, D_t, D_n, D_i, T_s, D_s, G), C, I, A_t, A_z, N) = 0X8FFF$ belongs to the moderate R_{L_1}) and high (R_{L_2}) forensic soundness level R_{L_1} of a photo respectively. A relational illustration of the three forensic soundness levels is further shown in Figure 5.6.

As depicted in Figure 5.6 relation R_{L_1} comprises a more specific attribute that measures forensic soundness level than

A probable combination which encompasses the preservation of confidentiality, integrity, authentication, authorization and non-repudiation (CIA_tA_zN) is represented by R_{L_2}. The transition of R_{FS} in the form $R_{L_0} \Rightarrow R_{L_1} \Rightarrow R_{L_2}$ represents the transition from a lesser forensically sound PDE, to a more specific forensically sound PDE. Figure 5.6 is relational illustration of the three forensic soundness levels.

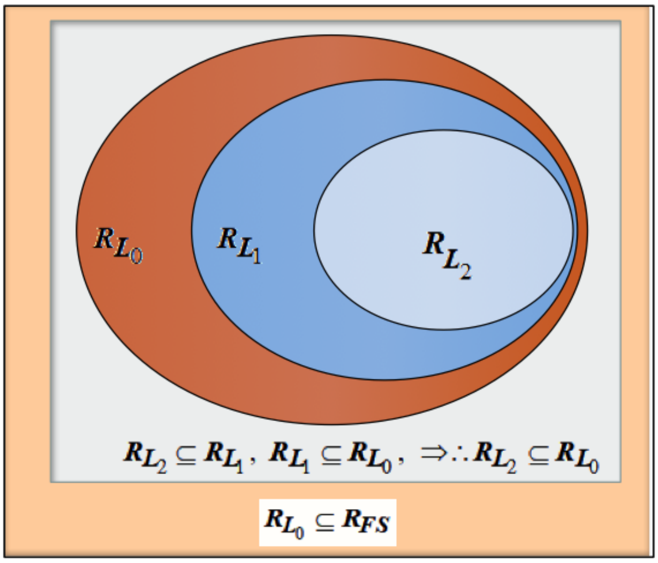

R_{L_0}
R_{L_1}
R_{L_2}
$R_{L_2} \subseteq R_{L_1},\ R_{L_1} \subseteq R_{L_0},\ \Rightarrow \therefore R_{L_2} \subseteq R_{L_0}$
$R_{L_0} \subseteq R_{FS}$

Fig. 5.6: A Representation of Forensic Soundness Level

5.4.4 *Hash PDE*

As shown in Figure 5.3, the captured PDE consists of metadata and the PDE. They are split into PDE and metadata. Each data item is hashed and the hashed metadata plus the PDE are joined at storage to become payload. A similar process is also applied to the PDE metadata.

5.4.5 *Hash Metadata*

The FSIs indicators consist of metadata of the captured PDE comprising of device type, timestamp, geographical location tag, international mobile station equipment identity (IMEI) identifier, WiFi connection identifier or GSM data connection - termed $R_{Metadata}$. This metadata is hashed as part of the payload that is joined to the PDE media at the time of upload.

The PDE metadata properties ($R_{Metadata}$) used to address forensic soundness are the following: (i) Device type (D_t) (ii) Timestamp (T_s) (iii) Datestamp (D_s) (iv) Geolocation (G) (v) International mobile equipment identity (IMEI) (D_i) (vi) WiFi connection identifier (C_{wf}) (vii) Network connection (C_{nw})

5.4.6 *Concatenate Payload*

After the password verification process to upload PDE payload, as depicted in Figure 5.6a the NWS generates a symmetric key (K) which it encrypts ⇒ K' = E(U_{pub}, K) using the uWatch public key. The encrypted key (K') is sent to uWatch. uWatch decrypts (K) ⇒ K = D(U_{priv}, K') using its uWatch private key. The symmetric key (K) is then used to encrypt payload data (photo, video, audio) plus metadata, extracted time and date stamp and geolocation from the payload. The metadata is hashed, signed using U_{priv} of uWatch, the PDE is hashed, then all of these are concatenated to form payload data which is then encrypted using symmetric key (K). The same process is applied to auditlog files, then concatenated with payload data plus payload auditlog, which is the payload uploaded to the NWS repository. As depicted in Figure 5.3 payload consists of the encrypted symmetric key (K') that was shared with uWatch, the captured PDE is joined with the metadata of the PDE, the hashed value of the PDE, the hashed value of the metadata, and the digitally signed metadata. These are joined and encrypted for storage at the NWS repository.

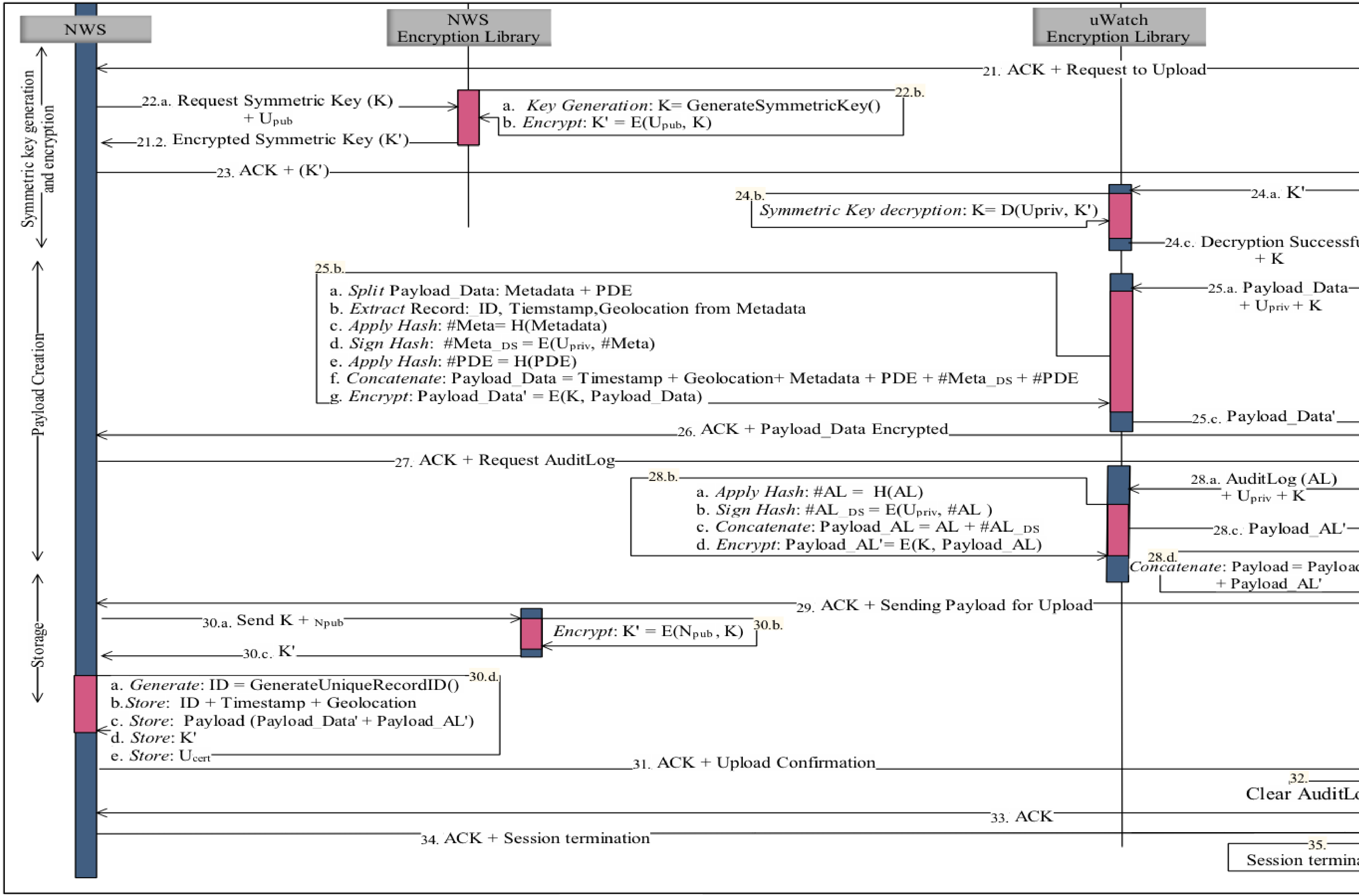

NWS
NWS Encryption Library
uWatch Encryption Library
Symmetric key generation and encryption
Payload Creation
Storage
21. ACK + Request to Upload
22.a. Request Symmetric Key (K) + Upub
22.b.
a. Key Generation: K= GenerateSymmetricKey()
b. Encrypt: K' = E(Upub, K)
21.2. Encrypted Symmetric Key (K')
23. ACK + (K')
24.a. K'
24.b.
Symmetric Key decryption: K= D(Upriv, K')
24.c. Decryption Successfu
+ K
25.a. Payload_Data
+ Upriv + K
25.b.
a. Split Payload_Data: Metadata + PDE
b. Extract Record:_ID, Tiemstamp,Geolocation from Metadata
c. Apply Hash: #Meta= H(Metadata)
d. Sign Hash: #Meta_DS = E(Upriv, #Meta)
e. Apply Hash: #PDE = H(PDE)
f. Concatenate: Payload_Data = Timestamp + Geolocation+ Metadata + PDE + #Meta_DS + #PDE
g. Encrypt: Payload_Data' = E(K, Payload_Data)
25.c. Payload_Data'
26. ACK + Payload_Data Encrypted
27. ACK + Request AuditLog
28.a. AuditLog (AL)
+ Upriv + K
28.b.
a. Apply Hash: #AL = H(AL)
b. Sign Hash: #AL_DS = E(Upriv, #AL)
c. Concatenate: Payload_AL = AL + #AL_DS
d. Encrypt: Payload_AL'= E(K, Payload_AL)
28.c. Payload_AL'
28.d.
Concatenate: Payload = Payload
+ Payload_AL'
29. ACK + Sending Payload for Upload
30.a. Send K + Npub
30.b.
Encrypt: K' = E(Npub , K)
30.c. K'
30.d.
a. Generate: ID = GenerateUniqueRecordID()
b.Store: ID + Timestamp + Geolocation
c. Store: Payload (Payload_Data' + Payload_AL')
d. Store: K'
e. Store: Ucert
31. ACK + Upload Confirmation
32.
Clear AuditLo
33. ACK
34. ACK + Session termination
35.
Session termina

Fig. 5.6a: Communication Sequence between NWS and uWatch Application–continued

5.4.7 *Symmetric encryption of payload and Upload encrypted Payload*

As depicted in Figure 5.6a, after the password verification process, in order to upload the PDE (while ensuring the confidentiality of the upload data), the following steps are taken.

(a) The NWS generates a symmetric key (K).

(b) The generated key (K) is encrypted using the public key of uWatch ⇒ K' = E $(U_{\text{pub}},$ K).

(c) The encrypted key (K') is then sent to uWatch. uWatch decrypts (K) ⇒ K = D(U_{priv}) using the private key of uWatch using the uWatch public key and sends the encrypted key (K') to uWatch.

(d) The symmetric key (K) is then used to encrypt the PDE data (photo, video, audio) plus metadata. Before performing this encryption, the time / date stamp, and geolocation from the payload is extracted.

(e) The metadata is hashed, and then digitally signed using the private key of uWatch (signed-digest). In addition, the PDE is hashed (PDE - digest), which is then followed by a concatenation process that combines the signed-digest, and the PDE digest to form the payload data.

(f) NWS exchange the generated and encrypted symmetric key (K) with uWatch.

(g) uWatch decrypts (K') ⇒ K = D (U_{priv}) using uWatch private key. The symmetric key (K) is then used to encrypt payload data (photo, video, audio) plus metadata, extracted time and date stamp, geolocation from the payload. The metadata is hashed and signed using U_{priv}, the PDE is also hashed, then all these are concatenated to form payload data, which is then encrypted using symmetric key (K). The same process is applied to audit log of the entire process which is then concatenated with payload data plus payload audit log as the payload uploaded to the NWS repository.

(h) This is then encrypted using the symmetric key (K). The same process is applied to the audit log file to generate the audit log data.

(i) The payload data and the auditlog data is then concatenated ⇒ payload data plus payload audit log. This combination is then referred to as the $uploaded_payload$, which is sent to the NWS repository.

(j) Upon PDE upload confirmation by the NWS, the session is then terminated by the NWS.

5.4.8 *Audit Log (AL) of all events*

The audit trail of all events for both uWatch and NWS undergo a similar process of forensic soundness implementation as the captured PDE. The audit log files are firstly (i) hashed, (ii) the digest of the hashed audit log is digitally signed (iii) the hashed, signed digest and the AL files are concatenated (iv) The concatenated AL objects are encrypted using (K) (v) Finally the AL is stored in the NWS repository. For the uWatch to NWS and the LEA to NWS communication transmission processes, two audit log processes are used to check the PDE chain of custody, chain of evidence and integrity of the entire processes. The first audit log is called an audit log (upload). This audit log is captured from the start of the certificate ID creation process of both uWatch and NWS to the PDE encryption processes. This audit log is uploaded and stored with the PDE final payload storage. The second audit log occurs when an LEA requests the NWS to search for PDE using time / date stamp plus incident geolocation. When the required is record is found (or not found) by the NWS, the found record is encrypted with the public key of LEA. A continuous audit log process runs concurrently with this process, which is then sent and termed $download_auditlog$.

5.4.9 *Acknowledgement*

Acknowledgement is a service component that provides feedback from various connected components, while receiving input from internal and external components of the ONW model as depicted in Figure 5.3. It is the means through which the ONW model communicates with the users and other components of the system, while keeping audit trails of processes and activities. As shown in Figure 5.2, the communication flow of the ONW model (denoted by a straight line) is a component-to-component interaction, while the dotted lines is the component-to-user interaction. For example, the acknowledgement component function is carried out by the system, while the other components require human users. The acknowledgement function of the ONW system's model receives its input from all components, while the human users receive notifications at various times in the course of the PDE transaction process as indicated below:

(i) At the installation of the uWatch application (ii) When the citizen creates a user information (profile) (iii) When a captured PDE undergoes FSI checks, either a success or fail feedback is received by the citizen. The citizen, however, has the option to de-activate any of the acknowledgement notifications at any time. (iv) When the citizen authenticates to upload captured PDE (v) When the citizen's uploaded PDE is downloaded by an authorised user to be used in criminal or civil investigation or as real evidence in any court of law

5.4.10 *NWS Repository*

The NWS repository stores PDE payload. The PDE payload contents stored in the ONW repository include photo, video or audio PDE captured from a potential crime scene. After the citizen has captured and authenticated to upload the PDE, to encrypt and store the PDE payload, the following occurs: (a) The captured PDE is split into metadata and media (photo, video or audio) (b) The time / date stamp is extracted from the record (c) hash is applied to the metadata $\Rightarrow \#meta = H(metadata)$ (d) The hashed value (digest) of the metadata is signed with the uWatch private key ($\mathrm{U}_{\mathrm{priv}}$) ⇒# $\mathrm{Meta}_{\mathrm{DS}}$ = E ($\mathrm{U}_{\mathrm{priv}}$, #Meta) (e) The PDE is also then hashed #PDE = H(PDE) (f) The #PDE + Metadata + PDE + #Meta + $\#\mathrm{Meta}_{\mathrm{DS}}$ +Time / date stamp + geolocation are concatenated to form the PDE payload. (g) The payload is then encrypted ⇒ $Payloaddata$ = E (K, $Payload_{data}$). The encrypted payload data, K' and audit log file are stored in the NWS repository. Then the uWatch application upload session terminates here.

The NWS side manages to ensure that uploaded PDE is securely stored to retain originality and ensure admissibility in court. It also maintains the access management functionality of the ONW system and maintain the role creations and validation of the three downloaders - i.e., law enforcement agent (LEA), digital forensic investigator (DFI) and the judiciary as shown in Figure 6.5

The access management function also ensures that the citizen's information (obtained during the PDE- capturing process) is stored securely using an encryption mechanism for the preservation of confidentiality, which further protect such information [106],[107]. Sometimes the information of citizens who captured PDE is required to attain meaning and usefulness of the stored PDE. When an authorised user requires an uploader's information to corroborate PDE, the authorised user is required to provide a corresponding decryption key. Nevertheless, the design of the ONW system is such that it ensures that only PDE required to make progress in a particular investigation is made available to authorised users.

In the ONW system, data privacy is achieved using encryption during data processing as well as data storage. As depicted in Figure 5.6a, the data processing phases used the symmetric key encryption scheme using the session key K. Data storage, on the other hand, uses both the symmetric and asymmetric encryption schemes by first exchanging a generated symmetric key K using asymmetric key encryption to do so, and then simply using K in symmetric fashion to encrypt the bulk of the data. This process ensures that user information are secure and confidentiality is preserved.

5.5 *User Privacy*

According to Reddy and Venter [108], privacy violations are often as a result of breaches in security like unauthorised access. However, data security breaches could occur when the information of a user is used inappropriately by an authorised user. To address these concerns of Reddy and Venter [108], the ONW system requires an authorised user to undergo various processes when information of a citizen (uploader) is required to identify or validate a PDE. These processes are as follows: (i) The authorised user (e.g., LEA) makes a request to NWS. (ii) The NWS validates the request, if the required information is indeed necessary. (iii) The NWS then decrypts and extracts the necessary user information as uploaded by u Watch.

Recall that the uWatch hashed user information using uWatch private key (U_{priv}), the uWatch further encrypts the hashed value of the user data plus other captured information of the users using symmetric key (K), which is then included on the PDE metadata for upload. Therefore only an authorised user with the corresponding symmetric key (K) and asymmetric key pair (N_{pub}) could decrypt the hashed user information. For LEA or any authorised user to access uWatch user's personal information, the NWS must decrypt the information, then encrypt the requested information back to the authorised user using the user's public key (for example (L_{pub} in the case of the LEA (see Figure 6.3a)).

As depicted in Figure 5.6a, the same encryption process applied to PDE payload for upload is applied to the information of user. For example, an authorised user (LEA) requires a corresponding key to obtain a citizen's information when needed to corroborate a crime or a first respondent's report during neighbourhood crime investigation. The NWS provides to the downloader the necessary information required to validate PDE payload at the payload download.

Finally, a citizen could choose to invoke the non-compellable witness clause of the Criminal Procedures Act (CPA), Act 51 of 1977, Section 203 [88]. This Act makes it possible for citizens who witness a crime or capture PDE to choose not to testify or provide their personal information.

5.6 *Conclusion*

This chapter introduced the ONW conceptual model and focused on Part A of the ONW system. It demonstrated a means to capture PDE in a forensically sound manner, using forensic soundness indicators, and store the PDE in the NWS system's repository.

Access management of the PDE in the ONW system's repository is the next stage in maintaining forensic soundness. This is Part B of the ONW system and is dealt with next in Chapter 6.

Chapter 6

ONW SYSTEM ACCESS MANAGEMENT PROCESS

6.1 *Introduction*

This chapter presents Part B of the ONW system's conceptual model as shown in Figure 5.1, which is the access management and PDE download process side of the ONW system. The ONW system's access management process ensures that access is granted to authorised users focusing only on the PDE they require for an on-going investigation. This is achieved by using user's role allocation, incident attributes, PDE attributes and parameters. The term authorised user in the context of this chapter is used to refer to users that have been given permissions, based on their role in crime investigation and litigation. The authorised users refers to downloaders, law enforcement agents (LEA), digital forensic investigators (DFI), the judiciary and any other individual who is authorised by law to employ PDE captured with and stored in the ONW system. These permitted users are required to also undergo the same level of authentication as applied to all users. The access management process seeks to preserve the privacy rights of all users of the ONW system in accordance with the PoPI Act 4 of 2013 [18].

6.2 *Access Management Process*

The ONW access management process focuses on the means to manage access granted to authorised users of the ONW system model.

The proposed ONW system automates the PDE capturing process, upholding the forensic soundness of the captured PDE. In the process, it adds two-levels of forensic soundness defined as R_{L_1} and R_{L_2} to the captured and stored PDE. As presented in chapter 5, the ONW system focuses on maintaining confidentiality, integrity and non-repudiation $\Rightarrow R_{L_1}$. This chapter of the ONW system maintains all the elements of R_{L_1}, and adds authentication and authorisation which is termed R_{L_2} to ensure that PDE captured with the ONW system maintains its evidential weight. This chapter is structured as follows:

- **Section 6.3 presents the high-level overview of the access management process, which is described in detail in Section 6.4.**
- **Section 6.6 presents a case study scenario description of a real-world incident where the ONW model is employed in neighbourhood crime investigation.**
- **Section 6.7 concludes this chapter.**

6.3 *High-Level Overview of the ONW system's Model Part B - Access Management Process*

The ONW access management process focuses on the access management and access granted to authorised users of the ONW system's model. An authorised user can gain access to stored PDE data using the PDE parameters, attributes and case in relation to an incident to be investigated or under investigation. Part B is a web front-end application - termed neigbourhood watch system (NWS). The NWS functions incorporate the roles of authorised users and deals with the access management of PDE.

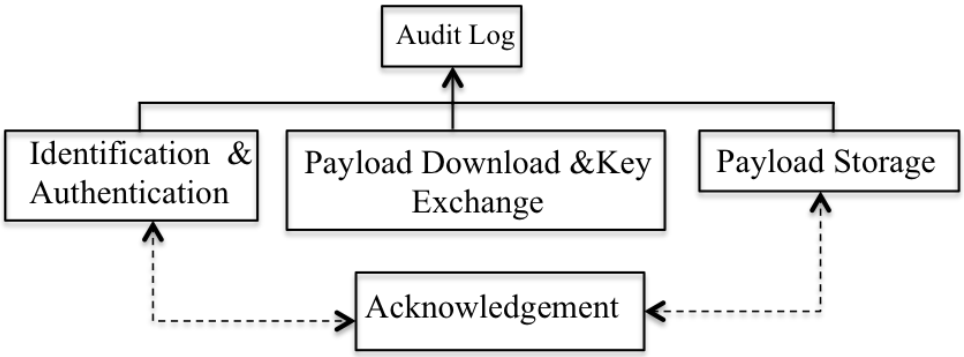

Audit Log
Identification & Authentication
Payload Download &Key Exchange
Payload Storage
Acknowledgement

Fig. 6.1: An High-level Overview of the ONW System's Model Part B - Access Management Process

Figure 6.1 is the overview of the ONW system's access management process and its relationship to the information security services, i.e., confidentiality, integrity, authentication, authorisation and non-repudiation. (C I $A_t A_z$ N). As depicted in Figure 6.1 the ONW access management process has five sub-processes, with each addressing one or two CIAAN mechanisms. These are; *(i)* Identification and authentication; *(ii)* Payload download and symmetric key exchange; *(iii)* Payload storage; *(iv)* Acknowlegdement. Each of these sub-processes forms a block of the detailed description of the ONW system's access management process as shown in the flow diagram of Figure 6.5.

6.4 *Detailed Process of the Access Management of the ONW System*

The data flow diagram as shown in Figure 6.5 is a detailed description of the ONW access management process.

6.5 *Introduction*

The primary aim of the access management process of the ONW system is to protect PDE stored in the NWS repository and maintain a minimum level of forensic soundness known as "level 1" L_1 or a higher level of forensic soundness known as "level 2" L_2 forensic soundness. Through out the research, "level 0" L_0, "level 1" L_1 and "level 2" L_2 are used to denote the various levels of forensic soundness of PDE.

The neigbourhood watch system (NWS) is used by the system administrator, and all authorised users (LEA, DFI and Judiciary) to gain access to the NWS. The NWS is the downloader side of the ONW system. For the purpose of this presentation and as depicted in Figure 6.5 and 6.3a the LEA is used to illustrate the download process of the system. This process is applicable to the DFI, the judiciary and any other assigned roles that are required to use the PDE stored in the ONW system.

6.5.1 *Generate user Asymmetric keys and Digital Certificates*

As shown in Figure 6.5 the generation of user asymmetric key pair, digital certificates and the verification of the certificates are subsections of the identification and authentication block. The NWS and the LEA generate the asymmetric key pair using the inbuilt encryption library of Android and web-application. Note that the author did not propose novel crypto functions. The crypto functions used in this dissertation were simply employed from existing encryption libraries. However, for the sake of completeness, all crypto steps employed for the PDE download functions and processes in the dissertation are shown in figures 6.3a and 6.4a. Throughout this research therefore, the asymmetric key pairs for the LEA is defined as $\mathrm{L_{pub}}$ and $\mathrm{L_{priv}}$ and that of NWS is $\mathrm{N_{pub}}$ and $\mathrm{N_{priv}}$. The encryption library uses $\mathrm{L_{pub}}$ and $\mathrm{L_{priv}}$ for its secure communication and verifies the NWS identify and does other encryption requirements of the LEA side of the system. For the LEA to communicate with the NWS system, the asymmetric key pairs is required. After the $\mathrm{L_{pub}}$ and $\mathrm{L_{priv}}$ are created by the encryption library of the LEA and the digital certificate generation process as depicted in Figure 6.3a follows. Recall that the certificate authority (CA) is self-signed and is hosted within the ONW system. This is in order to eliminate the cost burden on the users of the ONW system. The LEA, DFI or Judiciary are required to obtain the certificates and public/private key pairs to ensure non-repudiation. The CA is self-signed to enable the uWatch and the NWS act as trusted parties. The certificate authority (CA) generates its $\mathrm{CA_{pub}}$ and $\mathrm{CA_{priv}}$. The LEA sends its CertID information plus $\mathrm{L_{pub}}$ to CA for signing. The following process applies for CA to sign and create the LEA's digitally signed certificate.

1. The CA creates its own $\mathrm{CA_{pub}}$ and $\mathrm{CA_{priv}}$.
2. The $\mathrm{CA_{pub}}$ is sent to the NWS and the LEA, at this stage, the NWS and LEA use their encryption library to request and create their asymmetric key pair (i.e., $\mathrm{N_{pub}}$, $\mathrm{N_{priv}}$ and $\mathrm{L_{pub}}$, $\mathrm{L_{pub}}$).

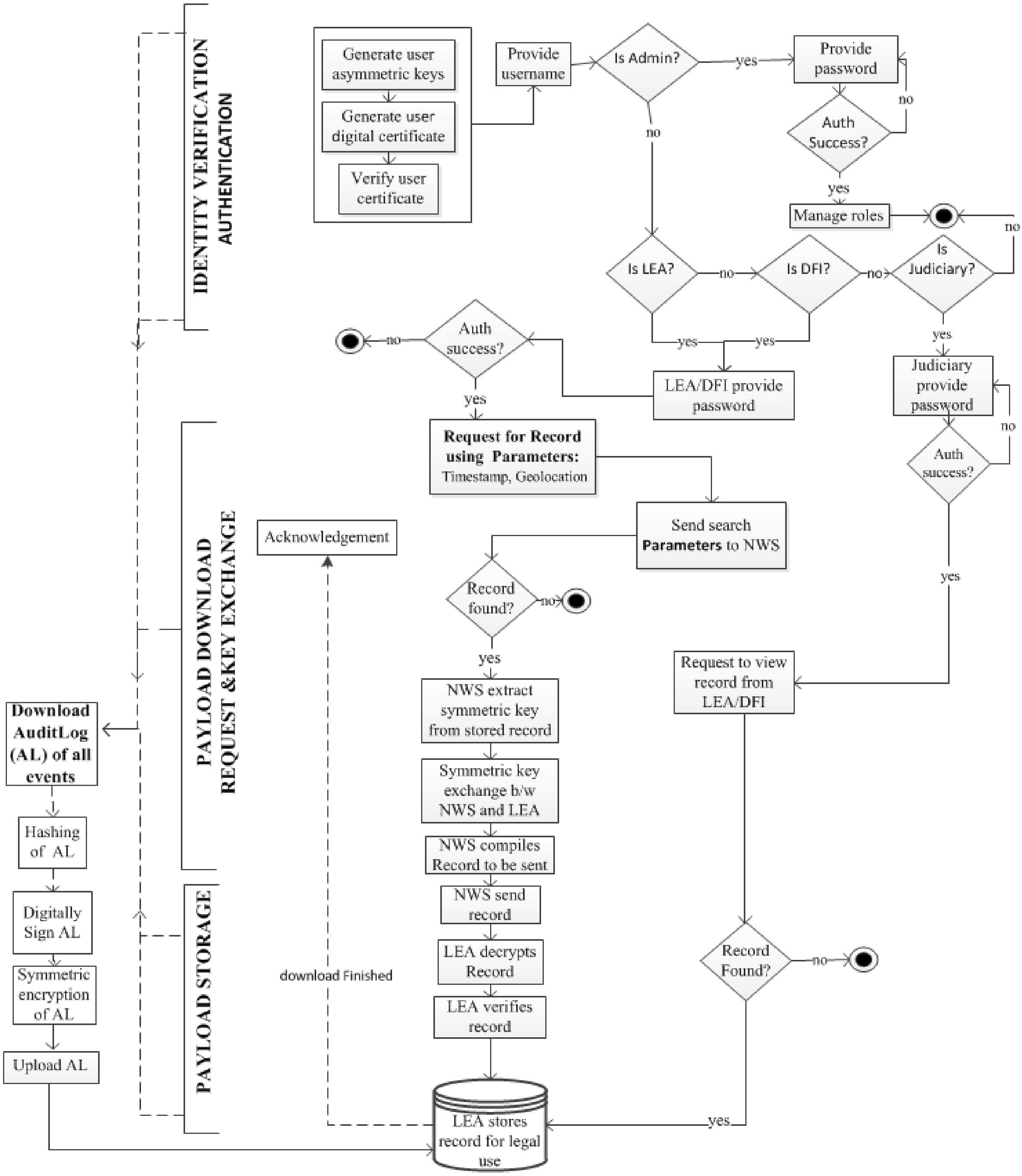


Fig. 6.2: The ONW System Part B - NWS - Focusing on L_2

3. The NWS and LEA creates their certificate ID information, then request the CA to sign. This is done by sending public keys (N_{pub} and L_{pub}) to the CA to do the following: (i) The CA verifies their request, (ii) Creates hash of the L_{cert} = H (L_{cert}) (iii) Signs the L_{cert}, using CA private key i.e., $L_{cert_{DS}}$ = E (CA_{priv}, L_{cert}) and consequently do the same for N_{cert}. (iv) The signed L_{cert} + $L_{cert_{DS}}$ and N_{cert} + $N_{cert_{DS}}$ are then defined as the signed certificates. This research will refer to the signed certificate as N_{cert} or L_{cert} for the NWS and LEA respectively. (v) The signed N_{cert} and L_{cert} are sent back to their respective sides of the system. (vi) The NWS and LEA exchange their L_{pub} and L_{pub} asymmetric keys to initiate communication. (vii) The LEA and the NWS are considered trusted parties after the asymmetric key exchange and certificate signing. Therefore the LEA and NWS can now communicate using the signed certificate.

6.5.2 *Authentication - LEA to NWS*

Authentication is necessary at all levels of the ONW system, to ensure confidentiality and uphold the PDE's originality. The download-side known as the neigbourhood watch system (NWS) is the process employed by the LEA to download and use stored PDE from the NWS repository. This side of the process maintains chain of evidence, ensures chain of custody, addresses confidentiality, integrity and non-repudiation, while adding access control functions. At the role allocation, a user is required to authenticate and choose his/her role as identified during the registration process. To view or download PDE, an authorised user must authenticate with his/her username, password and confirm his/her role as established at user registration. The PDE download process starts with the LEA user requesting download access from the NWS using the search parameters of time/date stamp and geolocation used by the LEA to request a data query to the NWS. The certificate authority (CA) is also required to generate the CA_{pub} and CA_{priv} that makes provision for digital signing of the asymmetric key pair of LEA. The LEA sends its Cert ID information plus L_{pub} to CA for signing. The following process applies.

1. The LEA sends its Cert ID information plus L_{pub} to CA for signing.
2. The CA creates its own CA_{pub} and CA_{priv}
3. The public key of CA i.e., CA_{pub} is sent to NWS and LEA
4. The NWS and LEA uses their encryption library to request and create their asymmetric key pair (N_{pub}, N_{priv} and L_{pub},L_{priv})
5. The NWS and LEA creates their certificate ID information, then request CA to sign by sending their public key (n_{pub} and L_{pub}) to CA to do the following: (a) CA verifies their request, (b) Creates hash of the L_{cert} = H(L_{cert}) (b) Signs the $L_{cert_{DS}}$ = E(CA_{priv}, L_{cert}) and consequently do the same for N_{cert}. The signed L_{cert}+ $L_{cert_{DS}}$ and N_{cert}t + $N_{cert_{DS}}$ are then the signed certificates. For clarity, the signed certificates are referred to as N_{cert} or L_{cert} for NWS and LEA respectively.

6. The signed $\mathrm{N_{cert}}$ and $\mathrm{L_{cert}}$ is sent back to their respective clients.

7. The NWS and LEA exchange their $\mathrm{N_{pub}}$ and $\mathrm{L_{pub}}$ asymmetric keys to initiate communication.

8. The LEA sends a request for authentication and in conjunction its $\mathrm{L_{cert}}$ to the NWS. The NWS receives this request, sends the received $\mathrm{L_{cert}}$ to its own encryption library in addition to the public key of the CA $\mathrm{CA_{pub}}$. The $\mathrm{L_{cert}}$ is hashed and then compared to the received digest. To perform this check, the NWS library does the following (a) It splits $\mathrm{L_{cert}}$ to $\mathrm{L_{cert}}$ + $\mathrm{L_{cert_{D}S}}$ (b) It splits $\mathrm{L_{cert}}$ to $\mathrm{L_{pub}}$ + Cert ID information (c) Extracts the hash of $\mathrm{L_{cert}}$ using $\mathrm{CA_{pub}}$ (D $(\mathrm{CA_{priv}}, \#\mathrm{L_{cert}})$ (d) Applies hash to $\mathrm{L_{certnew}}$, then compares the $\mathrm{L_{cert}}$ sent by LEA to that hashed created by its encryption library called $\#\mathrm{L_{certnew}}$, once they match and are valid, the NWS sends acknowledgment plus $\mathrm{N_{cert}}$ to the LEA.

9. The LEA performs a similar operation on $\mathrm{N_{cert}}$ using its encryption library and $\mathrm{CA_{pub}}$ to decrypt and $\mathrm{N_{cert}}$ verifies the hash. At the validation and verification of the process, NWS requests for the LEA username and password.

10. The LEA then encrypts its username and password using $\mathrm{N_{pub}} \Rightarrow$ NPW‘ = E($\mathrm{N_{pub}}$, U/N+PW). NWS decrypt the password using its private key $\mathrm{N_{priv}}$ then verifies the username and password. Upon confirmation, it then send acknowledgment plus password success to the LEA.

11. The NWS decrypts K using $\mathrm{N_{pub}}$, then encrypt K using the public key of LEA $(\mathrm{L_{pub}})$ and attaches the found record (FR) plus the encrypted symmetric key (K‘), which is then sent to LEA.

12. 14. The LEA then (a.) Decrypts the symmetric key (K) using $(\mathrm{L_{priv}})$. (b) Decrypts the FR using the decrypted key. (c) Sends acknowledgement (if no error occurs) to the NWS. (d) Terminates the session.

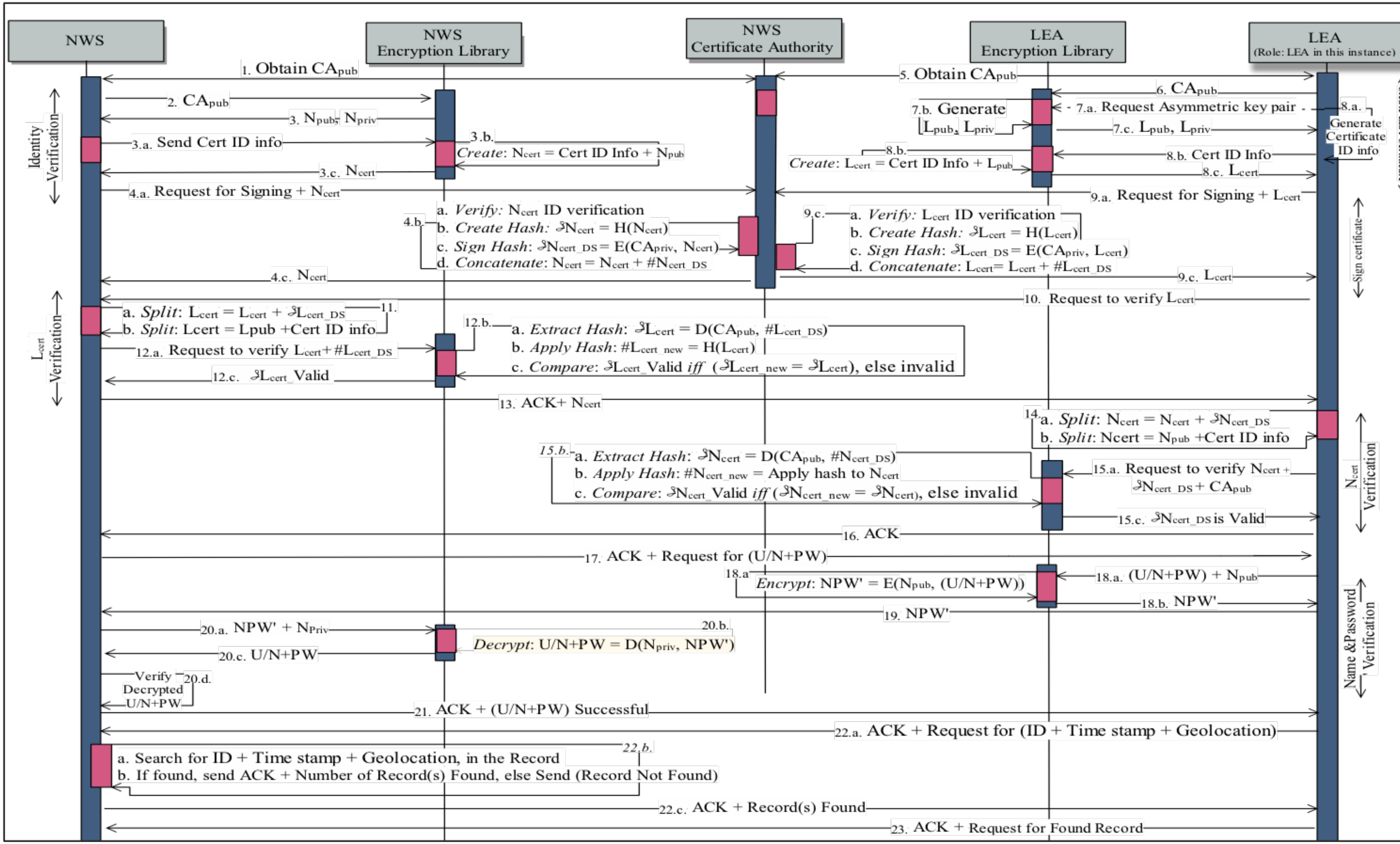

NWS
NWS Encryption Library
NWS Certificate Authority
LEA Encryption Library
LEA (Role: LEA in this instance)
1. Obtain CA$_{pub}$
2. CA$_{pub}$
3. N$_{pub}$, N$_{priv}$
3.a. Send Cert ID info
3.b. *Create*: N$_{cert}$ = Cert ID Info + N$_{pub}$
3.c. N$_{cert}$
4.a. Request for Signing + N$_{cert}$
4.b. a. *Verify:* N$_{cert}$ ID verification
b. *Create Hash:* ∌N$_{cert}$ = H(N$_{cert}$)
c. *Sign Hash:* ∌N$_{cert\_DS}$ = E(CA$_{priv}$, N$_{cert}$)
d. *Concatenate*: N$_{cert}$ = N$_{cert}$ + #N$_{cert\_DS}$
4.c. N$_{cert}$
5. Obtain CA$_{pub}$
6. CA$_{pub}$
7.a. Request Asymmetric key pair
7.b. Generate L$_{pub}$, L$_{priv}$
7.c. L$_{pub}$, L$_{priv}$
8.a. Generate Certificate ID info
8.b. *Create*: L$_{cert}$ = Cert ID Info + L$_{pub}$
8.b. Cert ID Info
8.c. L$_{cert}$
9.a. Request for Signing + L$_{cert}$
9.c. a. *Verify:* L$_{cert}$ ID verification
b. *Create Hash:* ∌L$_{cert}$ = H(L$_{cert}$)
c. *Sign Hash:* ∌L$_{cert\_DS}$ = E(CA$_{priv}$, L$_{cert}$)
d. *Concatenate*: L$_{cert}$ = L$_{cert}$ + #L$_{cert\_DS}$
9.c. L$_{cert}$
Identity Verification
Sign certificate
10. Request to verify L$_{cert}$
11. a. *Split*: L$_{cert}$ = L$_{cert}$ + ∌L$_{cert\_DS}$
b. *Split*: Lcert = Lpub +Cert ID info
L$_{cert}$ Verification
12.a. Request to verify L$_{cert}$+ #L$_{cert\_DS}$
12.b. a. *Extract Hash*: ∌L$_{cert}$ = D(CA$_{pub}$, #L$_{cert\_DS}$)
b. *Apply Hash*: #L$_{cert\_new}$ = H(L$_{cert}$)
c. *Compare*: ∌L$_{cert}$_Valid *iff* (∌L$_{cert\_new}$ = ∌L$_{cert}$), else invalid
12.c. ∌L$_{cert}$_Valid
13. ACK+ N$_{cert}$
14. a. *Split*: N$_{cert}$ = N$_{cert}$ + ∌N$_{cert\_DS}$
b. *Split*: Ncert = N$_{pub}$ +Cert ID info
15.a. Request to verify N$_{cert}$ + ∌N$_{cert\_DS}$ + CA$_{pub}$
15.b. a. *Extract Hash*: ∌N$_{cert}$ = D(CA$_{pub}$, #N$_{cert\_DS}$)
b. *Apply Hash*: #N$_{cert\_new}$ = Apply hash to N$_{cert}$
c. *Compare*: ∌N$_{cert}$_Valid *iff* (∌N$_{cert\_new}$ = ∌N$_{cert}$), else invalid
15.c. ∌N$_{cert\_DS}$ is Valid
N$_{cert}$ Verification
16. ACK
17. ACK + Request for (U/N+PW)
18.a. *Encrypt*: NPW' = E(N$_{pub}$, (U/N+PW))
18.a. (U/N+PW) + N$_{pub}$
18.b. NPW'
19. NPW'
20.a. NPW' + N$_{Priv}$
20.b. *Decrypt*: U/N+PW = D(N$_{priv}$, NPW')
20.c. U/N+PW
20.d. Verify Decrypted U/N+PW
Name &Password Verification
21. ACK + (U/N+PW) Successful
22.a. ACK + Request for (ID + Time stamp + Geolocation)
22.b. a. Search for ID + Time stamp + Geolocation, in the Record
b. If found, send ACK + Number of Record(s) Found, else Send (Record Not Found)
22.c. ACK + Record(s) Found
23. ACK + Request for Found Record

Fig. 6.3a: Communication Sequence between NWS and LEA Application

6.5.3 *Provide Username & Provide Password*

The function to provide username must be implemented firstly before the password request. The provison of user name is a separate function as depicted in Figure 6.5. The user must provide a username, a check is carried out to identify their role. Once their role is verified, the user must then provide their password. This is a function that checks if the user has the role access right to log into the NWS. When a user logs in, they are either an law enforcement agent (LEA), digital forensic investigator (DFI), judiciary member or an system Administrator. At successful check, the user is then required to enter his/her password.

The creation and management of users identity is a requirement of the system that must be fulfilled at various stages of the process and managed by the system administrator. When an authorised user needs to log into the system therefore, they are required to provide their username and their user role is checked against the system specifics. At this stage a username and role allocation function has been performed by the system administrator as depicted in Figure 6.5. The next step is for the user to provide their password if their role is valid.

6.5.4 *Manage Roles*

The manage and allocate roles function of the NWS is maintained by the system administrator. As discussed above, a user is only granted access when they have provided a user credential that is validated by the system. For a user to have access to the system the CA must have validated the user’s identity and a digital certificate would be created for the user. The NWS would have shared the NWS public key with the user, and the user is also required to have their public key shared with the NWS and CA. The authorised users of the NWS are as follows: (i) System Manager (System Administrator) (ii) The law enforcements agents (LEAs) (iii) Digital forensic investigators (DFIs) (iv) Members of the judiciary

In a typical crime investigation, roles are allocated to LEAs, DFIs or the Judiciary. The roles are managed by the System administrator. PDE consists of objects and attributes PDE objects are either video, audio or photo objects, while attributes include metadata ($\mathrm{R}_{\mathrm{Metadata}}$) that consist of time, date, geolocation and other metadata of an incident. For example, a photo PDE object possesses a file type, i.e., .png, .jpg or .gif, with attributes such as geolocation, WiFi connection and other $\mathrm{R}_{\mathrm{Metadata}}$ as applied to the captured PDE. These PDE objects are however allocated to an authorised user (LEA) by the NWS based on the search parameters provided by the LEA to the NWS for an incident under investigation.

6.5.5 *Request for Record using Parameters*

The LEA is able to employ PDE in the NWS repository, by requesting for access using time/date stamp and location of an alleged crime to request for NWS to search for incidents or crimes in relation to the cases they are to investigate.

The parameters used by the LEA to request for PDE download from the NWS system is the time / date stamp and geolocation which are used to store the incident at upload. The case category (as it concerns the type of offences - robbery, road rage, or theft), while the required PDE must correlate with the time / date stamp, location of the crime as well as the user requesting access must meet the set authentication and authorisation criteria of the ONW system.

Attribute-based access control (ABAC) focuses on the finer-grain level of access management. The fine grain are the PDE attributes such as time of crime incident, location, and data type of the captured PDE are allocated to authorised user by the NWS based on the output of the users search parameters. The NWS uses the date, time, location and file type attributes as outline to search for the user required record. Example of PDE objects are described in Table 6.1. The PDE objects (video, audio and photo) and PDE attributes (time, date, location) have a one-to-many relationship, where one case may require many PDE objects and attributes to complete its investigation. The NWS repeat the search, decrypt and encrypt process for every found record. The use of attributes provides a preciseness to the required PDE.

Object_ID	**PDE Object**	**Case 1**	**Attributes**
0001v	*Video*	*Incident 1*	*File type e.g. .MP4*
0004a	*Audio*	*Incident 2*	*.MP3*
0001p	*Photo*	*Incident 1*	*Date/Time*
0004p	*Photo*	*Incident 2*	*Date/Time*
0002v	*Video*	*Incident 4*	*Location*
0003v	*Video*	*Incident 3*	*File type e.g. .MP4*
0003p	*Photo*	*Incident 3*	*.Jpeg*

Table 6.1: PDE Objects and Attributes

6.5.6 *Send search Record to NWS using Parameters*

When the search parameter sent to NWS finds a record of an incident matching the parameters, the PDE payload is then allocated to the LEA by the NWS based on the incidents. The PDE payload is searched for by the NWS in relation to the case or alleged crime offence under investigation. As depicted in Figure 6.5, an authorised user (LEA) is required to select a role that correlates with their permission level and there must be a crime incident to be investigated. The PDE payload uploaded to the NWS consists of PDE attributes. Using the PDE attributes, authorised users are able to identify the exact contents of the PDE required for an investigation based on the search parameters the NWS decrypts the payload, extract the required record, then encrypt the PDE required by the LEA, using the public key of the LEA, then send to the record to the LEA.

6.5.7 *NWS extract and Exchange Symmetric key (K) with LEA*

As depicted in Figure 6.5 after the parameters search has been sent to NWS by the LEA, the NWS search through the stored payload for the requested record. If the record the LEA requested is available, the NWS then request for the username and password of the LEA, follows by the verification of the LEA as depicted in Figure 6.4a. Next phase NWS share key K with the LEA, the symmetric key (K) is encrypted using LEA public key ⇒ K' = E (L_{pub}, K). The LEA receives and decrypt K using its private key ⇒ K = D(L_{priv}). The symmetric key (K) is then used to decrypt the found record (FR). Recall that the symmetric key (K) was shared between the uWatch and the NWS. The same key (K) was encrypted and store by the NWS with the payload upload by uWatch application. The NWS need not generate a new (K) to communicate with LEA, therefore the need to stored the originally generated K. Therefore K for uWatch and LEA are the same but encrypted by NWS at any given point in communication between LEA and uWatch. To initiate the encryption process of PDE payload by the LEA, K is required. Therefore NWS uses the public key of LEA N_{pub} to encrypt (K), then share key (K) with the LEA. The (K) is then exchanged between LEA and NWS in order for the LEA to download payload.

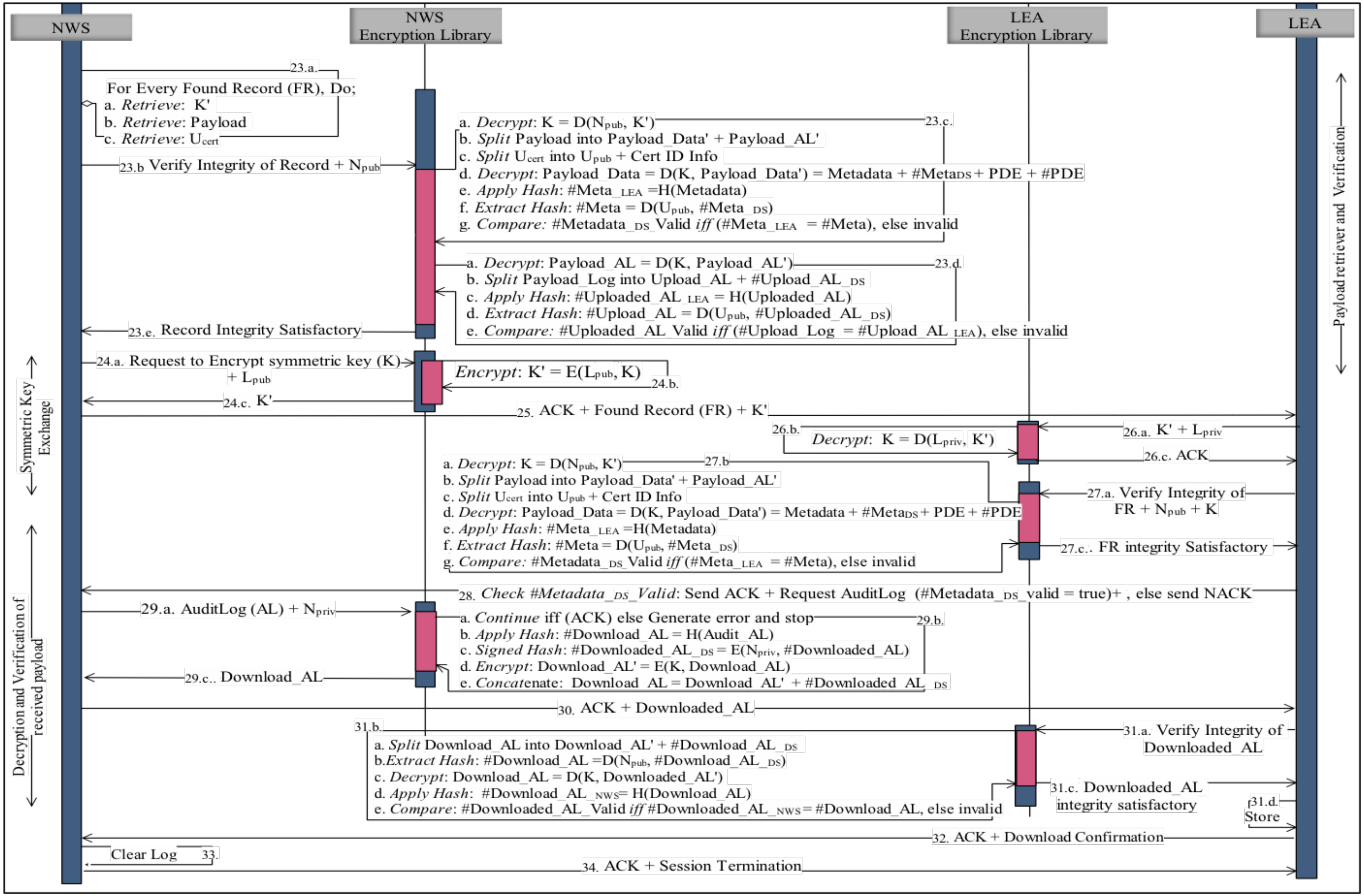

NWS
NWS Encryption Library
LEA Encryption Library
LEA
23.a.
For Every Found Record (FR), Do;
a. Retrieve: K'
b. Retrieve: Payload
c. Retrieve: Ucert
23.b Verify Integrity of Record + Npub
a. Decrypt: K = D(Npub, K')
23.c.
b. Split Payload into Payload_Data' + Payload_AL'
c. Split Ucert into Upub + Cert ID Info
d. Decrypt: Payload_Data = D(K, Payload_Data') = Metadata + #MetaDS + PDE + #PDE
e. Apply Hash: #Meta_LEA =H(Metadata)
f. Extract Hash: #Meta = D(Upub, #Meta_DS)
g. Compare: #Metadata_DS Valid iff (#Meta_LEA = #Meta), else invalid
a. Decrypt: Payload_AL = D(K, Payload_AL')
23.d.
b. Split Payload_Log into Upload_AL + #Upload_AL_DS
c. Apply Hash: #Uploaded_AL LEA = H(Uploaded_AL)
d. Extract Hash: #Upload_AL = D(Upub, #Uploaded_AL_DS)
e. Compare: #Uploaded_AL Valid iff (#Upload_Log = #Upload_AL LEA), else invalid
23.e. Record Integrity Satisfactory
Payload retriever and Verification
24.a. Request to Encrypt symmetric key (K) + Lpub
Encrypt: K' = E(Lpub, K)
24.b.
24.c. K'
Symmetric Key Exchange
25. ACK + Found Record (FR) + K'
26.b.
Decrypt: K = D(Lpriv, K')
26.a. K' + Lpriv
26.c. ACK
a. Decrypt: K = D(Npub, K')
27.b
b. Split Payload into Payload_Data' + Payload_AL'
c. Split Ucert into Upub + Cert ID Info
d. Decrypt: Payload_Data = D(K, Payload_Data') = Metadata + #MetaDS + PDE + #PDE
e. Apply Hash: #Meta_LEA =H(Metadata)
f. Extract Hash: #Meta = D(Upub, #Meta_DS)
g. Compare: #Metadata_DS Valid iff (#Meta_LEA = #Meta), else invalid
27.a. Verify Integrity of FR + Npub + K
27.c.. FR integrity Satisfactory
28. Check #Metadata_DS Valid: Send ACK + Request AuditLog (#Metadata_DS valid = true)+ , else send NACK
29.a. AuditLog (AL) + Npriv
a. Continue iff (ACK) else Generate error and stop
29.b.
b. Apply Hash: #Download_AL = H(Audit_AL)
c. Signed Hash: #Downloaded_AL_DS = E(Npriv, #Downloaded_AL)
d. Encrypt: Download_AL' = E(K, Download_AL)
e. Concatenate: Download_AL = Download_AL' + #Downloaded_AL DS
29.c.. Download_AL
Decryption and Verification of received payload
30. ACK + Downloaded_AL
31.b.
a. Split Download_AL into Download_AL' + #Download_AL DS
b.Extract Hash: #Download_AL =D(Npub, #Download_AL_DS)
c. Decrypt: Download_AL = D(K, Downloaded_AL')
d. Apply Hash: #Download_AL NWS= H(Download_AL)
e. Compare: #Downloaded_AL Valid iff #Downloaded_AL_NWS= #Download_AL, else invalid
31.a. Verify Integrity of Downloaded_AL
31.c. Downloaded_AL integrity satisfactory
31.d. Store
32. ACK + Download Confirmation
Clear Log
33.
34. ACK + Session Termination

Fig. 6.4a: Communication Sequence between NWS and LEA Application continued from 6.3a

6.5.8 *NWS Compiles and Send Record*

The NWS searches for the record based on the search parameters and attributes sent by the LEA as depicted in Figure 6.3a and Figure 6.5. When the requested record is found, the found record (FR) is then sent to the LEA plus the symmetric key (K) of NWS. At the NWS storage, incidents captured by the citizens are stored in categories using attributes such as location of the incident, the type of incident and the data type (video, audio or photo). The requested access to download the stored PDE payload by the LEA is then received by the NWS, who processes the request and sends back the found record (FR) to the LEA as depicted in Figure 6.4a.

For the uWatch to NWS and LEA to NWS communication transmission processes, there are two auditlog processes that are stored for checking of the PDE chain of custody, chain of evidence and originality of the entire ONW system's process. Auditlog (upload) is at the uWatch side. The second auditlog is at the time of the LEA and NWS request, search and receive PDE payload process. Recall that for an authorised user to use PDE from the NWS, they are required to send a search parameter to the NWS. The search parameters must consist of time/date stamp and geolocation of an incident they are investigating. The search parameter is then used by the NWS to locate the requested PDE data. The found record (FR) which was based on the search parameters is then decrypted and extracted by the NWS. The NWS then encrypts the PDE found record (FR) with the requesting authorised user's public key (for example $\mathrm{N}_{\mathrm{pub}}$) before sending the FR to the requesting party.

As this process is performed by the NWS, the audit log trail is continually updated. The updated auditlog trail of the NWS activities during its search, and subsequent finding of the required record is also documented in a forensically sound manner. This is then hashed, the hash is digitally signed and audit log file is encrypted. The audit log acquired at this process is termed download log. The audit download log is then concatenated to the found record (FR), then encrypted and sent as FR to the LEA.

6.5.9 *LEA decrypts Record*

Decrypting occurs for all downloaded PDE, as encryption is one of the forensic soundness indicators (FSIs). Decryption of PDE is part of the process of verifying its forensic soundness and includes validity checks for the properties such as the checksum, geotag, IMEI, device type, time stamp, date stamp and digital signature (see Figure 6.5).

The found records are decrypted by the LEA. They then uses the records to search for crime incidents reported or incident under investigation. Incidents are placed in various case categories such as traffic incidents, accidents and reckless driving and other like incidents are categorised as incident A. Incidents like property vandalism and home invasion are placed in another incident category. The grouping of incidents in cases based on offence makes it possible for an investigator to select case attributes in relation to the PDE attributes from FR.

6.5.10 *LEA verifies record*

A subsequent function in this process is the acceptance or rejection of the downloaded PDE, this is where the LEA verifies the FR by checking the forensic soundness, using the forensic soundness level applied as L_1 and that of level L_2. When PDE fails the forensic soundness verification process, the PDE is considered not valid and therefore must be discarded. On the other hand, when all forensic soundness requirements have been met, the PDE can be validly employed in a crime investigation.

6.5.11 *LEA Stores Record for Legal use*

After downloading the PDE, the LEA/DFI proceeds to analyse the PDE, but only when its forensic soundness has been verified and satisfied. With the PDE proven to be valid, it can be used by the LEA or DFI to conduct investigations. PDE that has satisfied the requirements for forensic soundness can also be employed by the judiciary. A prosecutor can use the PDE to prepare a case for prosecution, or a defense counsel can examine the evidence to prepare a defense. The attested forensically sound PDE can even be used by the presiding advocate (Judge) in conducting a pre-hearing or a trial-within-a-trial.

6.5.12 *Verify PDE Forensic Soundness*

Forensic soundness is implemented when PDE is captured and uploaded to the NWS repository. At PDE download, however, a comparison is made to check the validity of the PDE by means of 'verify forensic soundness' function. For example, two digital images can be assured to be identical if and only if the hash value generated from each piece of digital data using the same cryptographic hash function is identical. As depicted in Figure 5.4a, Figure 5.6a, Figure 6.3a and Figure 6.4a at any given hashing carried out in both PDE upload and download, verification of the digest value is checked by decrypting the hashed value by requesting the CA to use its $\mathrm{CA}_{\mathrm{priv}}$ to decrypt the hash for the NWS, LEA or uWatch as the case may be.

The forensic soundness verification process tests the originality of the PDE and metadata to ascertain that the PDE has remained in its original state from upload, during storage to download. For example, the hash function must be consistent with the originally generated cryptographic hash function when the PDE was captured and uploaded. Once the checksum is found to be valid, the LEA, uWatch or the NWS must also cross-check on their side of the system to ascertain validity. Once the checks and comparisons are found to be correct, the PDE can be assumed to be valid and admissible. However, if PDE fails to pass any of these checks, it must be discarded [75] [46].

6.5.13 *Download Audit Log (AL) and Acknowledgement*

The audit log of all processes of events from the log-in of an authorised user (LEA) as depicted in Figure 6.3a to when the found record (FR) is sent to the LEA are captured by the system. The encryption processes similar to that which was applied to the PDE payload at capture and upload is also applied to the audit log files. This is to show the chain of events as they unfold on the LEA and NWS system. As shown is Figure 6.5, the captured download process audit log (AL) of events is firstly hashed ⇒ H (Download A_L), the hashed values are digitally signed using $\mathrm{N}_{\mathrm{priv}}$ ⇒, #Download$_{ALDS}$ = $\mathrm{N}_{\mathrm{priv}}$, Download$A_{LDS}$ + Download$_{AL}$). The download audit log is then encrypted using LEA's public key $\mathrm{L}_{\mathrm{pub}}$ ⇒ Download$_{A'_L}$ = E ($\mathrm{L}_{\mathrm{pub}}$, Download$_{A_{LDS}}$+ #Download$_{AL}$ + Download $_{AL}$). The encrypted audit log, that is Download$_{AL}$' is then sent to the LEA storage repository.

The audit log or trail is one of the means that is used to eliminate doubts about the cycle of the chain of evidence [109][50]. The audit log of the ONW system is the component that manages the acknowledgement function that integrates community members who capture and upload PDE with the authorised user (s) (downloaders). The ONW system's audit log is able to generate a trail of system activity that provides information for both the ONW system and human users alike. Finally, the ONW system's audit log ensures a sufficient trail that provides a clear chain of evidence as well as a chain of custody of all transactions. This ensures that PDE downloaded from the ONW system and used as evidence in a court is reliable.

The acknowledgement keeps human users informed of the usage of their generated potential evidence, it gives feedback with regard to successful or failed PDE upload and continuously updates the users, especially when the user opts for this function on the ONW system.

Having described the PDE access management process, a case study scenario where the ONW system could be employed in a real-world situation is presented next.

6.6 *ONW System Case Study Scenario*

To further illustrate the application of the online neighbourhood watch system's model (i.e., the uWatch and the NWS) to the investigation and apprehension of an offender who perpetrated a neighbourhood crime, a case study scenario is presented as depicted in Figure 6.5. The LEA is considering using the PDE stored in the ONW system to narrow down the search for offenders of a neighbourhood crime incident and sends an access request to the NWS. Included in the request are the date/timestamp and location parameters which help to establish what happened and who is responsible for the alleged crime. The case study scenario illustrates the use of PDE captured and stored using the ONW system to provide potential evidence of a neighbourhood crime, in order to promote community policing and improving the relationships between communities and law enforcement agents.

6.6.1 *Scenario of a case under investigation*

This case study scenario involves an incident of reckless driving that resulted in a hit-and-run accident injuring a teenager. In other words, a teenager was run down by an on-coming vehicle, but the driver of the vehicle neither stopped to assist the victim nor did the offender report the accident to the law enforcement authority. The scenario portrays a situation where PDE in the NWS system's repository is employed to assist in an investigation. According to Figure 6.5, which is a pictorial representation of the scenario, the role players in the case study scenario are (i) the LEA; (ii) the teenager who was hit and injured in the accident (T); (iii) the reckless driver (D); and (iv) the onlooker (O) who witnessed the incident, captured the incident using the uWatch application and finally uploaded the PDE to the NWS to be used by the LEA.

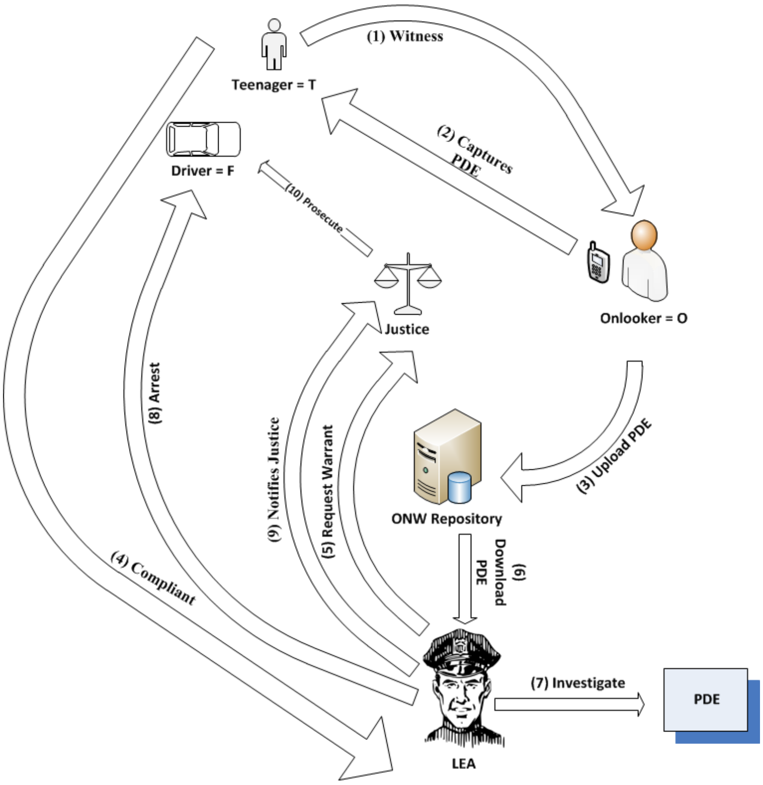


Fig. 6.5: Flow of events in a scenario employing PDE

The processes involved in the alleged incident are numbered from 1 to 10 (see Figure 6.5).

(i) The first event is the witness who saw the alleged incident (accident) and captured the incident in the uWatch application.

(ii) The witness uploads PDE of the alleged crime scene to the NWS repository.

(iii) In another event, the family of the victim (complainant) reports the alleged incident to the LEA.

(iv) The LEA requests a warrant to access the stored incidents in relation to the complainant‘s report.

(v) The LEA gets its asymmetric key pairs, certified by the certificate authority (CA) and exchanges the LEA's public key $\mathrm{L}_{\mathrm{pub}}$

(vi) The LEA using the search parameters of time/date and location attributes to request for PDE in relation to the reported crime to NWS, the NWS shares its symmetric key (K) with the LEA while sending the found record.

(vii) The LEA downloads the PDE payload.

(viii) The LEA examines and validates the downloaded PDE payload to ascertain the creditability of the stored PDE. The LEA also correlates the incidents from the NWS repository in relation to time, date and location of the complainant's report. When such a match is found, the found incident is then used by the LEA to further the investigations, as well as request a warrant to arrest the offender.

(ix) The LEA arrests the suspected offender based on the evidence available to the LEA from the NWS repository. The arrest is justified in conjunction with other evidence such as the physical crime scene, an eyewitness account and reported incident's metadata.

(x) The LEA notifies the judiciary by arraigning the offender before the court of law for prosecution.

(xi) Finally, the judiciary prosecutes the offender by assigning the necessary requirements of the law.

6.6.2 *Describing the case study scenario*

This section briefly describes the details of a case under investigation, where PDE acquired by a citizen using the uWatch and downloaded by the LEA using NWS can be employed as relevant potential evidence to commence and conclude an investigation into a crime committed by a road user in a South African neighbourhood (see Figure 6.5).

The driver of the vehicle allegedly ran over a teenager at an intersection of Street 'Q' in Town 'Y'. An onlooker saw the incident occurring and captured the accident using a mobile device while the alleged vehicle sped out of view. The onlooker captured an image of the incident scene which revealed the vehicle's brand, model and licence plate. The onlooker uploaded the captured PDE to the NWS repository. In other event, an accident was reported to the law enforcement agencies, who checked the NWS to cross-check for similar incidents based on the incident time frame and the location of the alleged incident. In this example, the case of the hit-and-run accident was reported to the LEA who was assigned to investigate the case. Table 6.2 indicates PDE attributes and objects that can be employed in the investigation of the alleged crime.

As shown in Figure 6.5, the LEA requires access to PDE in the NWS repository in respect of case attributes that include reckless driving, pedestrian accidents, time, date, location, mp4, photo type (.jpg) and audio (.mp3) objects of any incidents matching the hit-and-run accident. In this example, pedestrian accidents, reckless driving or other traffic offences (see Table 6.2) are the case attributes that must be aligned with the date, time and location of incidents

Role	Case attributes	Permission	PDE Objects &Attributes
LEA	*Case A:Reckless driving*	*Grant access to Case A*	*Date: 01 Aug. 2014, Photo*
LEA	*Case C: Vehicle offences*	*Grant access to Case C*	*Location: Midrand, Audio: mp3*
LEA	*Case D: Pedestrian accidents*	*Grant access to Case D*	*Time: 8:00 - 14:00*

Table 6.2: Using Attributes of a Case and PDE in an Investigation

fitting the profile presented. During the analysis of the investigation, the LEA enlisted the help of a digital forensic investigator (DFI). The system administrator authorises the DFI's access right to mimic the role of the LEA in order to allow the DFI to gain access to the NWS repository. The LEA, who used the system before, has already created a profile, so he logs in to authenticate and access PDE of the alleged incident. The LEA selects case attributes like hit-and-run, pedestrian accident, traffic offences, all of which are aligned to his hit-and-run investigation. He then selects PDE attributes such as date, time and location [110] of the alleged incident as shown in Table 6.2, and proceeds to download the PDE. The LEA then begins the forensic soundness verification process to ascertain PDE integrity. Once the PDE has been verified as valid, the LEA examines the PDE and is able to identify the driver of the vehicle. The LEA obtains a warrant to arrest the driver (D) and is ready to commence other forms of forensic investigation that result in a successful prosecution of the offender.

This case study scenario demonstrates the usefulness of PDE that is captured and stored using the ONW system. It also shows the access management processes required by an authorised user where only PDE related to an alleged case is assigned to an investigator against the option of full access to all stored PDE by authorised users. The purpose of the ONW access management process is to ensure that the privacy rights of users whose offences are stored in the NWS repository are maintained.

6.7 *Conclusion*

The proposed NWS automates the PDE capturing process in order to ensure integrity and also provides the necessary audit logs to prove that the automation was done successfully, should there be an enquiry or any scrutiny of the automation and the process result. The NWS repository employs access management measures that use role-based and attribute-based access control policies to manage the access and download of PDE payload. The access management policy complements the mechanisms for maintaining the forensic soundness of the PDE that is the "level 2" L_2 of the PDE. The NWS shows the processes used to ascertain the PDE originality and to validate the authorised users that were given access to the system. This process therefore retains a sufficient degree of assurance that the PDE abided by the evidential weight requirements, rule of law and other guidelines on the use of digital data. The PDE can therefore be used as admissible evidence or supported by an expert witness in the prosecution of a neighbourhood crime in any court of law.

Part IV

PROTOTYPE

Part IV presents the design and prototype of the ONW system. It comprises of Chapter 7, which focuses on the design of the ONW system using software engineering requirements specifications, while Chapter 8 describes the development of the ONW system's prototype.

Chapter 7

ONW SYSTEM REQUIREMENTS SPECIFICATIONS

7.1 *Introduction*

This chapter introduces the requirements specifications of the ONW system. In Chapter 4 requirements engineering (RE) was defined as the process used to design an application to ensure that various aspects of an application are maintained.

Employing a requirements specifications process that is aimed specifically at digital forensic (DF) applications is necessary to keep pace with the constant advancements in hardware devices and the frequent upgrades in devices' operating systems (OS). Requirements specifications that apply specifically to a DF application are necessary especially because, in no distance future, digital evidence may be the most common form of evidence available to show or prove a case, to conduct any form of investigation, or to serve as real evidence in a court of law. However, digital evidence presented to a court of law may be brought under scrutiny, for instance the validity of the digital forensic application used in the analysis of PDE may be questioned. A DF application requirements process allows for incremental pluggability and modifiability, where every aspect of the DF application is detachable to ensure continuous maintainable and pluggable functions of the overall system's requirements. The process also accommodates changes that are inherent in digital forensic investigation practices, in line with legal standards, and it keeps digital forensics up to date with current trends in information security. In addition to being in tune with technological changes, digital forensic applications must adhere to the latest legal standards.

This chapter proposes a digital forensic application requirements specifications (DFARS) process for designing digital forensic applications that take into account requirements engineering specifications. The chapter goes a step further and applies the DFARS process to design the ONW system.

The remainder of this chapter is structured as follows:

- **Section 7.2 proposes the DFARS process.**
- **Section 7.4 applies the proposed DFARS process to design the ONW system.**
- **Section 7.5 summarises and concludes this chapter.**

7.2 *The Proposed Digital Forensic Application Requirements Specifications (DFARS) Process*

To effectively design a DF application, the research in hand proposes a digital forensic application requirements specifications (DFARS) process. The DFARS process determines the user's and application's needs of a DF application, while incorporating the architectural requirements and constraints at all levels of the application design. The DFARS process is necessary for an easy re-build of a DF application to accommodate changes that are inherent in digital forensic investigation practices, in line with legal standards and in keeping with the latest trends in information security. Therefore, employing the DFARS process to design an effective DF application requires the identification of the DF application's functional requirements (user's needs), the architectural requirements (the DF application's needs) and the architectural constraints (the issues that must be dealt with in the course of the DF application's design and development). Figure 7.1 depicts the high-level components of the DFARS process.

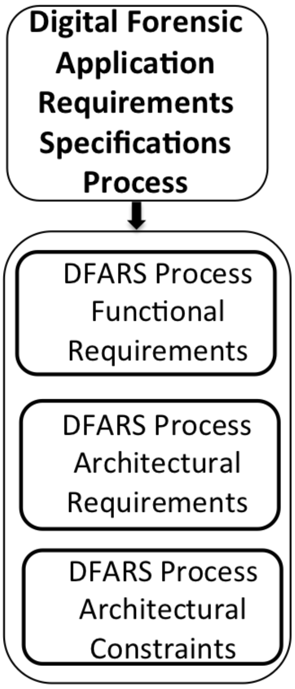

Digital Forensic Application Requirements Specifications Process
DFARS Process Functional Requirements
DFARS Process Architectural Requirements
DFARS Process Architectural Constraints

Fig. 7.1: Sub-processes of the DFARS Process Requirements Specifications (DFARS) Process

The DFARS process consists of three sub-processes, each of which is discussed and broken down to show how they are used when designing a DF application. The sub-processes are as follows:

(i) DFARS Process functional requirements *(ii)* DFARS Process architectural requirements *(iii)* DFARS Process architectural constraints The remaining sections are structured as follows: Section 7.3 details the DFARS process functional requirements specifications. Section 7.3.1 presents the DFARS process for architectural requirements specifications and Section 7.3.2 focuses on the DFARS process that deals with the inherent constraints that arise when designing DF applications.

7.3 *DFARS Process for Functional Requirements*

The purpose of the DFARS process for functional requirements is to elicit the activities and expected output to be accomplished by the DF application [**?**]. The DFARS process functional requirements are used to determine what the user needs from a DF application. Therefore, defining the needs of any DF application requires the identification of functional requirements. The users of any DF application are: *(i)* the end-users;*(ii)* the application; and *(iii)* other stakeholders (see Figure 7.3).

These three sets of needs represent different requirements for the DF application. Figure 7.2 shows that there are common needs that are essential to the identified users, and these are usually the core requirements of the DF application. The point of convergence reveals the core needs of the DF application and must be prioritised (see Figure 7.2). The core requirements of DF applications must withstand all constraints and must take precedence over other requirements as the DF application is being designed.

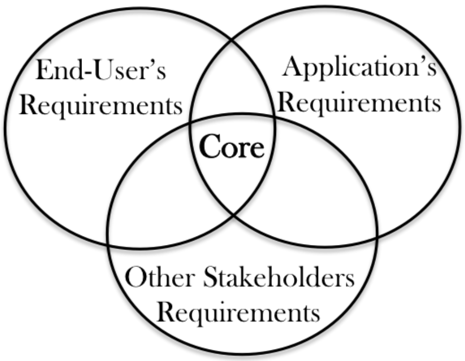


Fig. 7.2: Core users that Identify the Functional Requirements of DF Applications

For example, a DF application that is to determine the number of messages (short message services (SMSs)) received by a mobile device since it became operational should focus its core requirements on auditability functions. Therefore, when such an application is designed, its core design decisions must be focused on the SMSs messaging protocol and the global system for mobile communications (GSM) network provider. Since the messaging protocol becomes one of the core requirements of the DF application, any identified constraint must defer to its primary need for auditing.

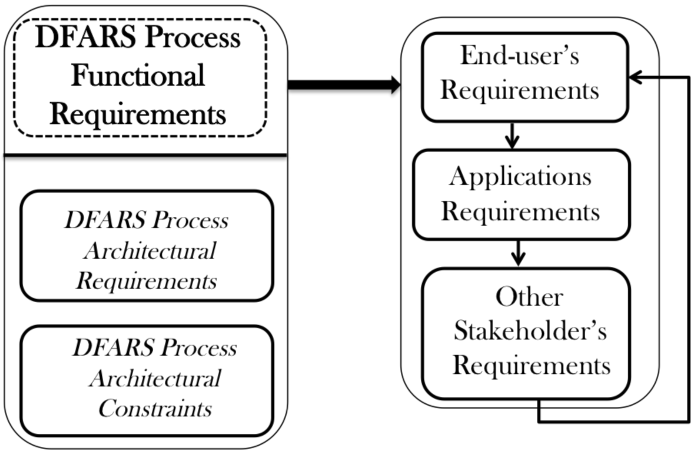

DFARS Process Functional Requirements
DFARS Process Architectural Requirements
DFARS Process Architectural Constraints
End-user's Requirements
Applications Requirements
Other Stakeholder's Requirements

Fig. 7.3: DFARS Process for Functional Requirements

The DFARS functional requirements determine the needs of the DF application's end-users, stakeholders and developers, which are subsequently interpreted using a use case diagram [94]. The use case diagram shows the user's interaction with the various use cases of the DF application. Each of the identified use cases of the DF application is treated as a component or micro service. Each component is an entity, such that detaching a component or micro service from the DF application does not necessary affect the functioning of other components of the DF application. The functional requirements of an application are constantly reviewed by all the stakeholders to meet the DF application's needs, as well as to accommodate the current trends in digital forensics (see Figure 7.2). The following process is proposed to arrive at the functional requirements of a DF application:

(i) End-users' Requirements: Firstly, identify the needs of the application's end-users, since these needs hold a unique position in the design decisions of any DF application. The DFARS process functional requirements are used to interpret the end-users' requirements by using use case, activity or sequence diagrams [94]. The use case diagram shows user interaction with the various components of the DF application. These user needs, depicted as use case components, are constantly reviewed by all users of the DF application to keep up to date with the current trends in digital forensics as well as adhere to the core needs of the DF application. Another advantage of clearly specifying end-users' requirements of a DF application is to present the DF application to a non-technical audience at its early stages of design. Usability and the deliverable of the DF application to an end-user's expected output in a simple and easy-to-understand DF application therefore constitute a core requirement when eliciting the end-user's needs. The DFARS process for functional requirements involve eliciting the activities and expected output to be accomplished by the DF application. For example, usability is one of an end-user's typical requirements for any application. This is

because an expert witness or a digital forensic investigator reporting on an incident in a court of law may need to explain the processes employed that brought about the conclusion of the crime investigation [111]. A DF application designed with usability as one of its core concerns can be easily explained to a non-technical audience. Usability and delivering the end-user's expected output of a simple and easy-to-use application is a basic requirement of a DF application.

(ii) The system's requirements are intertwined with those of the end-users, in that the end-user's needs are interpreted and addressed. These needs are used to determine the best technology and techniques that will realise the DF application's requirements. The developers interpret the application's needs and base its specifications on the architectural and integration requirements that will best address the DF application's overall goal.

(iii) As far as other stakeholder requirements are concerned, the DF application incorporates the needs of users other than the end-users during the design and development of a DF application. Incorporating these needs into the application's requirements specifications is ensured during the design phase of any DF application to ensure continuity and maintainability. The constraints of stakeholders ranges from technology preference to identifying quality requirements that are essential. When incorporated at the early stages of a DF application's functional requirements specifications, these stakeholders constraints can ensure an efficient DF application.

In summary, to elicit the functional requirements of a DF application, the requirements of the end-users, stakeholders and application respectively are considered. Having identified the process to be adopted when eliciting the functional requirements of a DF application, the next section focuses on the architectural requirements specifications.

7.3.1 *DFARS Process for Architectural Requirements*

The DFARS process for identifying the architectural requirements of a DF application involves assembling the information required to design its architecture. The architectural requirements of any application consist of the DF application's quality requirements, the architectural patterns and strategies, plus the integration requirements that are used to realise the DF application's functional requirements.

7.3.1.1 DFARS Process for Quality Requirements

The DFARS quality requirements are used to address the identified needs specified in the elicited functional requirements of any DF application. DFARS quality requirements are realised using architectural patterns and architectural strategies (see Figure 7.4). Quality requirements are the measurable properties that quantify an application's expected output

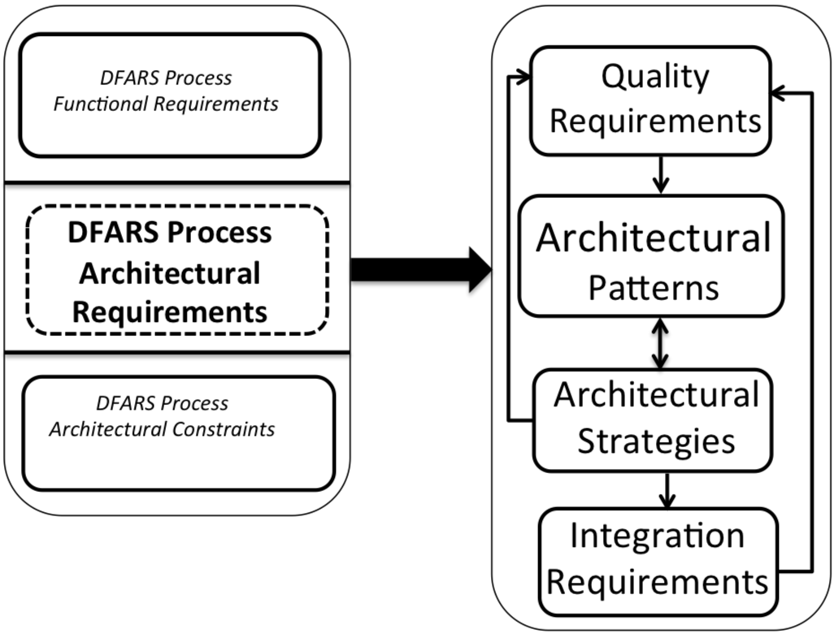


Fig. 7.4: Architectural Requirements Specifications Artefacts of a DF Application

[93]. The DFARS process proposed to identify and define the quality requirements of a DF application includes the following two step:

(i) Align the identified functional requirements: To identify the quality requirements of a DF application, the user's requirements (i.e. the functional requirements) must be revisited (e.g. using the DFARS process to design a DF application that identifies the number of SMSs a mobile device has received/sent in the last few months, whether deleted or saved SMSs). The user's requirements of the DF application are to identify the number of SMSs sent/received, the details of the recipients of the SMSs, as well as the locations where the SMSs were received. The user requirements must be aligned with the application's core requirements by using quality requirements.

(ii) Interpret the use case components: The user's identified requirements are interpreted in respect of each use case components to transcend to the quality requirements of the DF application. The core quality requirements required by the use case components of the DF application are addressed using integrability, accessibility, auditability and other requirements. These quality requirements are identified and added to the DF application's architectural design. The DF application that identifies the SMSs sent/received by a device in the last few months will need to show the various components, where each of the use cases of the DF application is a use case to identify cellphone tower locations using the location area code (LAC), the mobile network code (MNC) and the mobile country code (MCC)[112].

The quality requirements of a DF application are realised by the architectural patterns that are further explored in the next section.

7.3.1.2 DFARS Process for Architectural Patterns

Architectural patterns address multiple quality requirements of a DF application. It is critically important to choose the best architectural patterns to address the quality requirements of any application that is to be designed. Therefore, to determine the architectural patterns that best address the identified quality requirements of a DF application using the DFARS process, the researcher proposed the following two steps:

(i) Use the identified quality requirements to determine architectural patterns. Decisions around the DF application's overall architectural responsibilities must be made, then addressed using the architectural patterns. For an application where security requirements are the highest priority, ensuring users' privacy and maintaining access control constitute the architectural responsibilities of the DF application. Architectural patterns are then used to address the privacy issues and access control requirements of the DF application. For example, the architectural patterns used to ensure security responsibilities are typically layered, MVC, pipes-and-filters and microkernel architectural patterns.

(ii) Identity the choice of architectural pattern by using the critical quality requirements. For example, if the priority of the DF application is focused on security, the microkernel architectural pattern is considered at the first level of granularity, while pipes-and-filters, layered or MVC architectural patterns are employed at the second or third level of granularity. Furthermore, choices like MVC architectural patterns are to allow for proper separation of concerns, where modular application design and development incorporating micro services are used, where the micro services address each component as an entity.

Architectural patterns address the multiple quality requirements of any software application, whereas architectural strategies focus on addressing one aspect of a quality requirement. The architectural strategies employed to ensure that the various quality requirements of the DF application are concretely addressed, are discussed next.

7.3.1.3 DFARS Process for Architectural Strategies

Architectural strategies consist of individual approaches that specify the means to concretely address an aspect of an identified quality requirement of a DF application. Architectural strategies allow a system's design to conceptually determine how a quality requirement should be realised. Architectural strategies must be aligned with the architectural patterns to fulfil one aspect of a quality requirement. The researcher again identified two steps for determining architectural strategies in the DFARS process:

(i) Identify the architectural strategies that best address each of the individual needs of the DF application as aligned with a quality requirement. For example, to design a DF application where data originality and authenticity are the major concerns of the application, cryptographic hash and digital signatures will be some of the architectural strategies to focus on. On the other hand, for the security requirements of an application that has preventing data breach as one of its main concerns, encryption and access control are some of the architectural strategies to utilise. Architectural strategies also involve making explicit trade-off decisions as to which feature of a quality requirement is more important to address, in order for a DF application to meet its stakeholder's requirements.

(ii) Architectural strategies must however be selected in order of importance to address the quality requirements. Firstly, select strategies based on the priorities allocated to the core needs of the DF application as demonstrated in Figure 7.2. For example, if privacy is the priority of the DF application, then encryption must be considered before other aspects of security requirements (like limited access or event logging) can be considered. Secondly, select architectural strategies that can assist in addressing the identified architectural patterns. The fact that two or more strategies can be used to address one aspect of a quality requirement can enhance the efficiency of the architectural patterns.

Integration requirements are the artefacts that ensure that the various components of a DF application can function effectively as one entity using communication channels. The next section gives the details of the DFARS process for integration requirements.

7.3.1.4 DFARS Process for Integration Requirements

DF applications are often required to interact with internal and external resources and should therefore harness the advantages of resources such as WiFi connections, GSM networks and other forms of connections that are required to conduct a concrete digital forensic investigation. Integration is the interaction of a DF application with humans and other systems' access channels. Identifying the integration requirements ensures flexibility of the various components of the DF application, and this flexibility in turn accommodates future upgrades and add-on possibilities during the lifespan of the DF application.

In relation to the SMS example, the integration requirements are used to integrate with the GSM network grids and internet protocol that enable users to receive/send SMSs without the GSM service provider's standard communications protocols. The DF application's design must also ensure that the auditability functions are reliable, easy to use, upgradable and can be integrated with other existing system components for the DF application's overall usefulness. Moreover, integration requirements are the artefacts that ensure that the various components of a DF application can function as one entity by effectively using communication channels and without adversely affecting the overall operations of the application. Integration requirements clarify the needs of DF applications in order to achieve consensus on the priority of the DF application.

In designing a DF application, the integration of various channels using adapters, protocols and messaging channels is a key requirement. To determine the integration requirements of a DF application using the DFARS process, the following are considered:

(i) Clarify the scope of the DF application's integration requirements, so that the application's expected output is achieved and the integration artefacts are specified. For example, designing a DF application to capture external network traffic of a personal computer (PC) should focus its design on two aspects: firstly, on the interaction and data-capturing process when the PC is connected to the internet; and secondly on identifying the various possible protocols that could transmit or receive data from the PC.

(ii) Identify the interconnected activities to be performed by the DF application so as to clearly define each input and expected output in relation to other tasks and activities of the DF application.

(iii) Define both the machine and human actors of the DF application and their roles to clearly identify which integration requirement best addresses the functions of all actors.

Identifying the integration requirements of any DF application paves the way for addressing the DF application's constraints, as is done in the next section.

7.3.2 *DFARS Process for Architectural Constraints*

DF architectural constraints revolve around the other sub-processes of the DFARS process, i.e. the functional, architectural and integration requirements. An efficient DF application design must accommodate the constant change in devices and maintain forensic soundness of the DF application, while adhering to the requirements of the application's end-users. Architectural constraints are the concerns of the stakeholders that must be considered when the functional and architectural design decisions of a system are made.

As shown in Figure 7.5, the common architectural constraints that must be taken into account during the design phase of a DF application are jurisdictional, legislative and technological. The DFARS process for incorporating architectural constraints is as follows:

(i) Identify the jurisdictional constraints of the DF application as they can influence the design and development of the DF application. The prescriptions, norms and laws of the jurisdiction where the DF application is to be used must be considered during its architectural decision stages. For example, the data retention/ownership requirements of one domain may differ from those of another domain [17] [88].

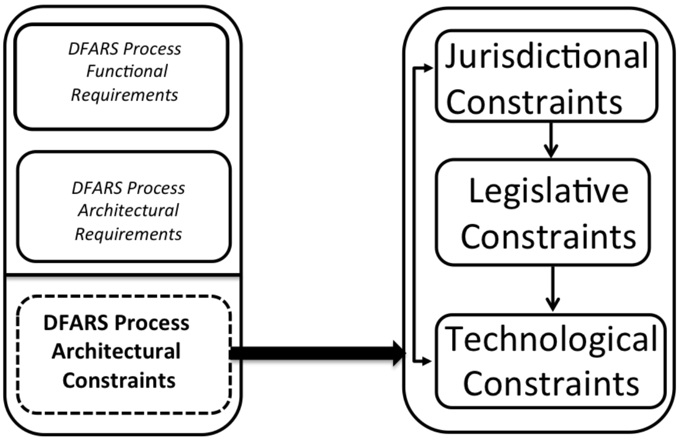

DFARS Process Functional Requirements
DFARS Process Architectural Requirements
DFARS Process Architectural Constraints
Jurisdictional Constraints
Legislative Constraints
Technological Constraints

Fig. 7.5: DFARS process to define Architectural Constraints

(ii) Identifying the legislative constraints involved, as the prescriptions of legislation and the Constitution of the country where the application is developed and used must be adhered to. A DF application design must pay attention to legislation that governs digital evidence admissibility, for example the PoPI and ECT Acts of South Africa [17] [17] [88].

(iii) Identify the potential technological constraints, for instance the impact of the updating of the features of mobile devices is a constraint that must be factored in when a DF application is designed.

Taking into account the architectural constraints of a DF application is the final part of the DFARS process and the next section summarises the DFARS process.

7.3.3 *Summary of the DFARS Process*

While each of the previous sections described a step in the DFARS process, this section summarises the DFARS process in its entirety.

(i) Identify the functional requirements specifications, while scoping the DF application (using UML use case diagrams) to identify the DF components. Then define the processes of the scoped DF application by using activity diagrams to show the DF application and the processes employed in addressing each of the scoped components.

(ii) Interpret the identified functional requirements of the DF application to determine the architectural requirements that best address and realises the DF application's core needs.

(iii) Use the architectural responsibilities to select the most effective architectural patterns that best define the quality requirements of the DF application.

(iv) In the same vein, the best architectural strategies that address a single concrete aspect of the DF application's quality requirements are also selected in order of importance.

(v) Architectural constraints imposed by stakeholders must be addressed to align them with the DF application's requirements. The technologies and techniques that best incorporate the architectural constraints are employed, while addressing the overall needs of the DF application.

(vi) Finally, the integrability of both the internal and external components of the DF application must be defined. This is to ensure continuous upgrade and maintainability of these components without affecting the overall productivity of the DF application.

Having completed the discussion of the DFARS process, the next section applies this process in designing the online neighbourhood watch (ONW) system.

7.4 *Applying the Proposed DFARS Process to the ONW system*

In this section, the DFARS process is represented as it applies to the design of the ONW system. The DFARS process begins with the identification of the functional requirements of the ONW system. The identified functional requirements attributes of the ONW system as depicted in Figure 7.6 are discussed first.

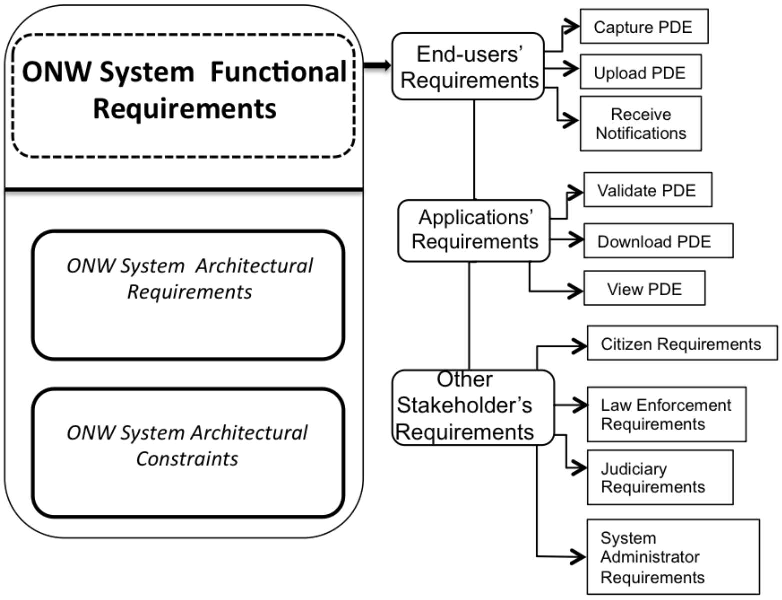

ONW System Functional Requirements
ONW System Architectural Requirements
ONW System Architectural Constraints
End-users' Requirements
Capture PDE
Upload PDE
Receive Notifications
Applications' Requirements
Validate PDE
Download PDE
View PDE
Other Stakeholder's Requirements
Citizen Requirements
Law Enforcement Requirements
Judiciary Requirements
System Administrator Requirements

Fig. 7.6: Applying the DFARS process to Identify the Functional Requirements of the ONW System

7.4.1 *Functional Requirements Specifications of the ONW System*

In the proposed DFARS process for designing DF applications, the first sub-process of the DFARS process is to identify the functional requirements to address the user's needs of the DF application. as shown in Figure 7.6, the core functions and requirements components of the ONW system are expanded into three categories, namely (i) the end-user's requirements, (ii) stakeholder's requirements (iii) and the application's requirements. These three components are further aligned to the users of the system as (i) The Citizen (community member) captures PDE (ii) The system ensures forensic soundness of PDE (iii) The system stores the captured PDE (iv) The stored PDE is made available to authorised users (e.g. LEA, DFI or Judiciary) (v) The System administrator maintains access management role of stored PDE. Each of these use cases are discussed next.

7.4.1.1 The Citizen

The citizen or human user (actor) interface of the ONW system is mapped to the use case that captures PDE, in other words the person in the street who captures and uploads the PDE of an incident. The uploader captures PDE of a potential crime using his/her mobile device and uploads the captured PDE to the ONW system's repository. The citizen receives an acknowledgement at successful upload of the PDE, when the PDE is downloaded to be used as potential evidence in a neighbourhood crime investigation, or when it is presented as evidence in a court of law.

Capture PDE This is the first point of contact with the ONW system, when citizens use their mobile devices to capture PDE of a crime. The captured data is either an audio, photo, or video of what the citizen perceives to be a crime. At this point the captured digital data is potential digital evidence (PDE). It will be up to the judiciary and law enforcement agents to determine if the PDE is actual evidence that is admissible in court.

Upload PDE After capturing PDE of a crime scene either as a photo, video or audio, the citizen can then upload the captured payload PDE to the NWS repository after going through the encryption process. To commence the encryption process, the password verification process that enables the citizen to upload PDE is initiated. The NWS generates a symmetric key (K) which is the encrypted K‘ = E(U_{pub}, K). The encrypted key (K‘) is then sent to the uWatch application. The uWatch decrypts the (K) ⇒ K=D (U_{priv}, K‘ using its uWatch private key. The symmetric key(K) is used to encrypt payload data (i.e., either photo, video, audio) plus metadata, extracted time and date stamp, geolocation from the payload. The metadata is hashed, signed using U_{priv} of uWatch, the PDE is also hashed. All this data is concatenated to form PDE payload data which is then encrypted using symmetric key (K). There is also the function of upload at a later time, this function enables the uploader (citizen) to upload later, rather than at the time of PDE capturing. This function is most useful for a citizen who may feel endangered near a crime scene, or in the case of when data connection is not immediately accessible.

Receive Acknowledgement(s) The ONW system communicates with the citizen at various times throughout the PDE lifecycle. The citizen receives the first acknowledgement at a successful upload of the PDE. The second acknowledgements is received when the LEA or DFI downloads the PDE uploaded by the citizen. A third acknowledgement is received by the citizen when PDE is used as evidence in court. Receiving acknowledgements is a feature of the ONW system that encourages and motivates the citizen to participate and stay involved in the community policing process. Furthermore, citizens are motivated to participate when they realise what difference their generated PDE makes in crime solving.

7.4.1.2 The Law Enforcement Agent and The Judiciary

The task of the law enforcement agents (LEAs) is to download PDE to corroborate their physical crime scene investigation and validate the potential evidence. The LEAs accept the potential evidence as valid and useful to their investigation, or reject and discard PDE when any form of inconsistency is discovered [15]. The role of the LEA actor can also be that of a DFI who may assume both roles when necessary or based on investigation requirements. In practice, a situation may arise where PDE captured and stored is to be utilised as real evidence in order to shed light on a case in a court of law. The judge, court clerk or legal counsel of the plaintiff or defendant may need to view the alleged PDE, which can be made available to the aforementioned parties as decided by the presiding judge. The PDE may further enhance the presiding Judge understanding of the case under prosecution and, in terms of the South African legal system, the presiding judge makes the final decision as to the admissibility of any potential evidence [84] [88] [113]. The ONW system sheds light on what happened in an alleged incident and assists the legal teams of both the prosecutor and the defendant to prepare legal arguments. The role of the judiciary in using PDE stored in the ONW system is one of the core requirements for the ONW system to operate successfully within legal constraints.

Validate PDE This function is carried out by the LEA or the DFI when they ensure that the PDE is valid by checking the forensic soundness indicators. When PDE is tampered with in any way or found to be invalid, it should be discarded.

View PDE This function is carried out by the members of the judiciary, who need to view the PDE as it relates to a case before them in court. However, the members of the judiciary are not allowed direct access to the ONW system's repository. By viewing the stored PDE, the presiding Judge can assess the PDE relevance and determine its evidential weight, and thereby enabling the prosecuting and defense counsels to use the evidence when necessary in arguments preparation.

Download PDE Download PDE is one of the functions of the LEA or DFI which is performed only when the PDE they require from the NWS repository is found and sent to the LEA or DFI by the NWS. The PDE download and access management function is maintained by the NWS. The system administrator manages the roles of the authorised users. When the LEA or DFI is satisfied that the PDE is forensically sound, he/she proceeds to download the PDE to store for legal use.

Validate Audit Log The audit log keeps track of all actions taken by users who access the ONW system. The function is shared by both the PDE downloader and the system administrator who also keep tracks of the system's activity. In other words who accessed various cases, what downloads they made and whether any changes made to the cases data were certified with time stamps to specify when the data was changed.

7.4.1.3 System Administrator

The system administrator manages the roles of the authorised users (LEA, DFI and Judiciary) in the NWS system. These functions are to implement PDE access management, and user allocation management. The system management ensures that acquired PDE upholds the information security services requirements that encompass confidentiality, integrity, authorisation, authentication and non-repudiation (CIA_tA_zN), as well as the properties of the forensic soundness indicators (FSIs) at all interaction levels of PDE components.

User Role Allocation and Management User role allocation management is the use case that manages actors/agents in the system as well as the case that they are allocated as it concerns investigations. The system manager (System Administrator) manages the roles of users such as the LEA, DFI or judiciary on the system. Managing user allocation ensures that only authorised users are allowed to login to the system. After users have been registered, at their first-time login they are required to change their password, as a generic password was generated by the ONW system administrator at user allocation.

However, this functionality is only available for cases that contain PDE uploaded by law enforcement agents or digital forensic investigators. In crime investigation, the collection and preservation of evidence are crucial steps and if done incorrectly, the evidence may be rejected in the court of law. The audit log serves as a proof of confidentiality and integrity of the PDE during the investigation of a case and it can be used as a chain of custody when the PDE is admitted in court. The audit log documentation can trace back to who, when and where the data was transferred and analysed at any given point in the ONW system‘s life cycle.

The functional requirements specifications of the ONW system, as elaborated here, constitute the first sub-process of the DFARS process. The next section deals with the architectural requirements specifications of the ONW system‘s design.

7.4.2 *Architectural Requirements Specifications of the ONW System*

As proposed by the DFARS process at the architectural requirements specifications phase, the quality requirements of a DF application are identified using the functional requirements of the DF application. As is clear from Figure 7.7, this section applies the DFARS process to identify the architectural requirements of the ONW system.

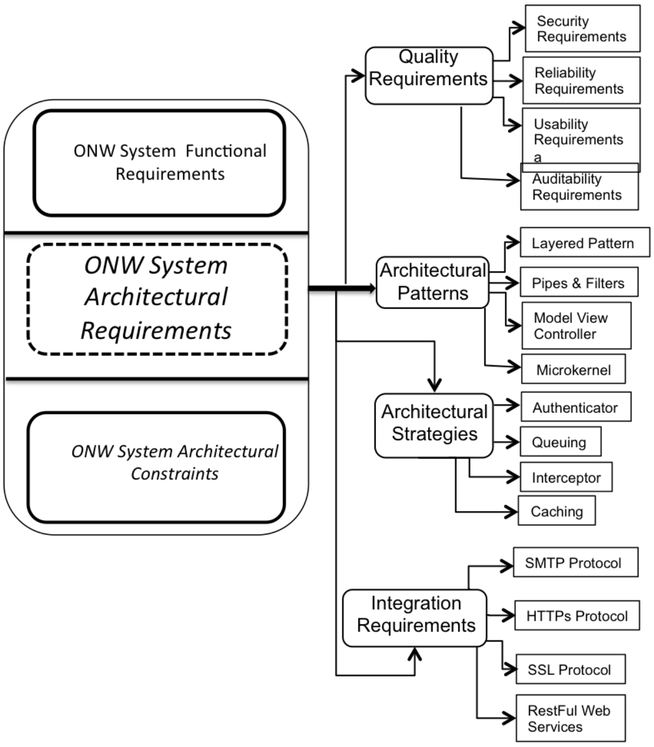


Fig. 7.7: Applying the DFARS process to Identify the Architectural Requirements of the ONW System

The architectural requirements of the ONW system are identified by analysing the quality requirements, architectural patterns, architectural strategies and integration requirements. These are used in turn to address the identified functional requirements of the ONW system by focusing on its architectural responsibilities. Each of the attributes of the ONW system‘s architectural requirements (see Figure 7.7) is used to define the architectural structure of the ONW system (as will be shown later in Figure 7.8). The requirements specifications identified during the design of the ONW system are later addressed when developing the ONW system’s proof of concept using application program interfaces (API) and frameworks. This is because the architectural structure, which is like the building bricks of the system, must be defined to develop the ONW system. Technologies such as APIs, IDEs and frameworks that best address the ONW system's architectural strategies and patterns are used. Therefore the identified quality requirements of the ONW system are discussed next.

7.4.3 *Quality Requirements of the ONW System*

The identified quality requirements of the ONW system are hereby presented in detail, and the discussion focuses on the various aspects of the system and addresses each of the quality requirements. The quality requirements of the ONW system as determined by the functional needs of the system are as follows (see Figure 7.7):

(i) Security requirements; *(ii)* Reliability requirements; *(iii)* Usability requirements; *(iv)* Auditability requirements; *(v)* Testability requirements.

The strategies, patterns and technologies employed to realise these quality requirements of the ONW system are discussed in the sections that follow.

Security Requirements of the ONW System The security requirements of the ONW system are achieved using the CIA_tA_zN information security services [102]. The CIA_tA_zN services employed to implement the security requirements are as follows:

(i) Confidentiality - To maintain the confidentiality of PDE stored in the NWS system repository, an advanced encryption standard (AES) 256 bits symmetric encryption algorithm is used to ensure that stored PDE payload remain confidential even in an event of data breach. Furthermore, confidentiality is preserved especially to protect the usefulness of PDE and attain admissibility [17]. The ONW system is accessed via https for a secure communication link between the front-end and the back-end. This also ensures that PDE is not altered in transit or at storage.

(ii) Integrity - An unauthorised user, process or program should not be able to access or modify data in the ONW system. With the integrity functions in place, data modification can only be achieved by authorised users. The cryptographic hash function SHA512 is one of the integrity options used for the ONW system. All captured PDE is hashed using the SHA512, after which the hashed value of the PDE is encrypted and stored in the database relative to the PDE to enhance the integrity of the PDE. The integrity of the PDE is also ensured using the forensic soundness indicators (FSIs) of geolocation, timestamp and other metadata.

(iii) Authorisation - Authorisation is the process during which access rights of PDE resources are given to the LEAs/DFIs and other authorised users. The ONW system implements its authorisation functions by using the combined functions of role-based access control (RBAC) and attribute-based access control (ABAC) and assigning tokens to all users. An authorisation enforcer pattern handles the authentication logic across all actions within the Web tier/layer.

It provides a centralised authorisation service to abstract the authorisation code from the application code.

(iv) Authentication - The ONW system uses a session authenticator and username, as well as a password for its authentication. A user provides a username and password in order to be logged in and a session is then created. The created session is applicable to all users who require access to the ONW system when they provide their login credentials. These are then authenticated with the details stored in the user's profile database. The aligned functions apply across all users of the ONW system. For example, although a citizen is required to authenticate to upload PDE to the repository, the PDE-capturing process does not require authentication. Citizen authentication at PDE upload is necessary to identify who uploaded a particular piece of PDE and to ensure that the uploader is who he/she claims. Furthermore, at three wrong attempts of login credentials, the user is required to solve a challenge-response text using captcha. This helps to distinguish between a machine (via brute force attack) and a human user. The same process of authentication applies to the downloaders.

(v) Non-repudiation - The non-repudiation function is achieved using certificate authority and generating a digital signature for the citizens and law enforcement agents, therefore upholding the user original intention. For example, the uploader of a piece of PDE data may not later deny his/her intentions in the creation or transmission of the PDE data as the entire process is signed using their digital foot print.

The security requirements of the ONW system are addressed using microkernel, MVC and pipes-and-filters architectural patterns, which are placed on a layered architectural pattern at the first level of granularity of the ONW system structure. By using these architectural patterns in conjunction with architectural strategies, the security of the ONW system is achieved.

Reliability Requirements of the ONW System The strategies used to comply with the reliability requirements of the ONW system are as follows: *(i)* Faults detection is implemented using deadlock detection, logging, checkpoint evaluation and error communication to constantly update the system's status to all components. It involves the ability to roll back database changes, should an error occur during the change transition.

(ii) Resource locking is for example used to lock each session that a user is currently accessing, as well as to lock the session when idle for a certain amount of time. This is to ensure that, during any given transaction, a thread is created so that no other thread or user

can use or change this particular thread while another user is engaged in the transaction, or data transfer is in progress.

(iii) To achieve reliability, fault prevention is adhered to by means of thorough system testing, the use of resource locking at service processing, and the removal of any single point of failure. In this way, failure is mitigated before there is any need for repairs [90].

(iv) Reliability qualities ensure the elimination of resource bottlenecks by using clustering and throttling architectural strategies. In this way resource overconsumption by one component at the expense of another component of the ONW system is avoided.

(v) Furthermore, the microkernel architectural pattern is used at the second level of granularity of the ONW system. The microkernel architecture bus maintains reliable communication channels between the access points to various components, detects alteration of PDE at upload and maintains a tamper proof system throughout the ONW system's life cycle.

(vi) Another architectural pattern that ensures reliability is pipes and filters. The pipes encapsulates the encryption and decryption features of the ONW system and at the same time manages attacks such as eavesdropping and data interception. The pipes also act as alternative secure communication channels that are capable of transmitting encrypted data.

(vii) In the unlikely event of system failure or unauthorised access, passive redundancy is employed on the database front. Backup as well as active rollback is also applied in the design phase to ensure that the reliability requirements are met.

Reliability functions are in place to ensure that the ONW system is maintained, while usability functions make sure that users' usage experience is incorporated in the design phase of the ONW system.

Usability Requirements of the ONW System Usability is a measure of the amount of effort that a user must put in to use the ONW system. The following usability strategies are employed:

(i) The ONW system provides users with the required features for easy familiarity with the system, and it also anticipates users' needs.

(ii) Exception and bug reporting are enabled to allow users to report on and/or send bug reports to the system. In addition, logging, crashes experienced and other feedback are used to enhance the usability of the ONW system.

(iii) The ONW system remembers users' tasks, such as the last-typed URL, and it recalls usernames and passwords (especially when using the same device). It minimises a user's efforts, thereby providing an easy-to-use application.

(iv) Exception communication and notifications are thrown at various stages of the system's functioning. Depending on the type of exception thrown, either users or the system is notified

for the authorised component or user to resolve the exception. For example, a server-side database that does not respond throws an exception.

(v) The Model-View-Controller (MVC) architectural pattern realises the flexible user interface that allows for a component-oriented design and easy separation of concerns. This separation of concerns restricts the dependence of various components, where each components is treated as an individual entity to avoid components' re-design when user interfaces change. For example: (i) The Model- manages the data and logic of the software. A DBMS (Database Management Software) is used to model the data and control the data flow. (ii) View - data is represented and structured using HTML. The data is represented on interchangeable platforms using Android for mobile and web-application version for all other devices. JavaScript Object Notation (JSON) is used for lightweight transfer of data and AJAX to communicate with the server and access the system. (iii) Controller - accepts the user's input and converts it into commands that the model or the view can understand. PHP Processor will execute the commands between the view and model.

Auditability/Monitorability Requirements of the ONW System Auditability provides the functional service that enables the ONW system to log the input and output activities of the internal and external resources of the system, in order to track system and user activities. The following strategies are used to achieve auditability/monitorability requirements of the ONW system:

(i) In the event of the ONW system crashing, the rollback function is in place to return the ONW system to its last stable state.

(ii) Date and time stamps are placed on activities as they occur on the ONW system in order to make them retraceable. This helps to pinpoint when an activity took place, which can be especially helpful when it concerns the unlikely event of a system crash or unauthorised access.

(iii) Forensic soundness indicators are also employed in determining the current state of PDE reliability at any given time in the ONW system's life cycle.

Testability Quality Requirements of the ONW system Testing is used to ascertain code quality and ensure that adequate software engineering techniques are employed in the design and development of any system [114]. Testing quality requirements of the ONW system ensure that at authentication, human-to-component, and component-to-component or component-to-human interaction is adequately validated and they enforce a minimum format default for all captured PDE. For example, when a citizen captures a non-valid PDE format, the validation method checks to confirm that the format of the PDE is photo, audio or video. This validation check is performed again before upload, to ensure consistency. However, when inconsistency with the minimum default format is detected, the upload function on the citizen‘s device is turned off, thereby disabling upload functionalities. The exception error message output to the citizen (uploader) from the ONW application is the invalid PDE format exception handler. Testing the various quality requirements of the ONW system ensures that all services provided meet the set pre-conditions and are realised at post-conditions after the functions/methods called services have been provided.

Two testing functions are carried out in the ONW system: *(i)* The first function unit testing [115], which is applied in smaller units like classes and methods of the ONW system. These tests mock all the dependencies and isolate the single class from the main system. The unit tests of each of the classes, functions and methods are carried out to validate the business logic of the ONW system. This ensures that every class is an entity, where a failure in one class does not affect the others.

(ii) The other test, integration testing [116][117], is targeted at testing the behaviour of the various components of the ONW system. Integration testing is employed to ensure that every added or updated component of the ONW system meets the minimum requirements to uphold forensic soundness at all levels of the system, using Maven integration testing framework [118][116]. It verifies that the whole system functions as it was intended to, using multiple classes, database or queue for the test process.

As proposed in the DFARS process, the architectural patterns specifications of a DF application are used to address the identified quality requirements of the DF application. The next section focuses on the architectural patterns used in the structural designs of the ONW system's quality requirements.

7.4.4 *Architectural Patterns of the ONW system*

Architectural patterns is a set of principles that can be adapted for systems [119] [120]. For the ONW system, the 3-tier layered architecture, microkernel, as well as pipes-and-filters architectural patterns were considered and employed. The layering architecture is employed at the highest-level of the system to allow for a clear separation of the functionality of the system, where each layer is treated as an independent layer that can be easily managed, therefore providing a loose coupled, high cohesive and encapsulated system [119] [120]. The communication between the layers is one directional, a lower layer cannot initiate a communication with a higher layer, a component within a layer can communicate with one another and every layer has a set of functionality it provides that is needed by its higher layer [119].

The detailed descriptions of the various architectural patterns can be found in the background Section 4.3.2. Figure 7.8 contains a visual representation of the architectural design of the ONW system using various architectural patterns and strategies to address the quality requirements.

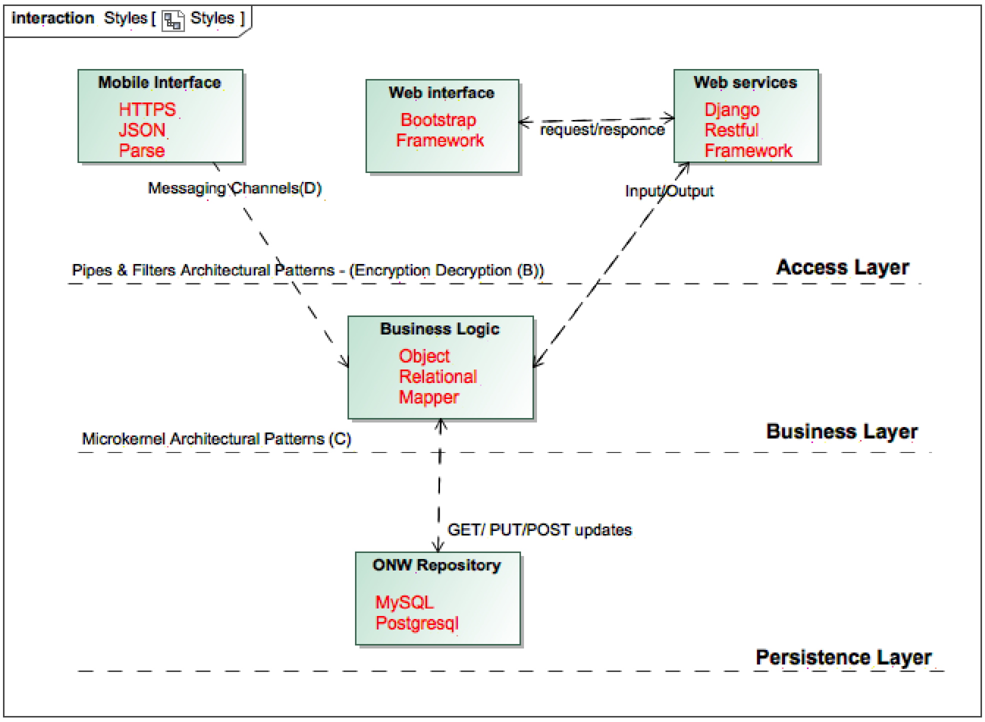


Fig. 7.8: Architectural Structure of the ONW System

7.4.4.1 Layered Architectural Pattern of the ONW system

A layered architectural pattern at the first level of granularity was chosen to ensure that the security concerns of the ONW system are maintained. The layered architectural pattern is supported by other architectural patterns, such as MVC, microkernel, pipes-and-filters and decorator patterns. The MVC architectural pattern is used at the access layer to ensure a separation of concerns, while pipes-and-filters and microkernel architectural patterns are used to support the business logic and the persistence layers so as to ensure security, reliability and stability of the system. Each of these architectural patterns contains layers to address the various requirements of the ONW system. The extra architecture patterns are added at each layer, which means that at the second and third level of granularity of the ONW system, pipes-and-filters and micro kernel architecture patterns are used. For example, the parts labelled ‘B’ and ‘D’ in Figure 7.8 rely on the pipes-and-filters pattern to ensure a secure messaging channel, encryption and decryption processes, while the part labelled ’C’ is the microkernel architectural pattern to support the security features of the ONW system. The way in which each of these architectural patterns addresses the requirements is explained below (see Figure 7.8).

(i) The MVC pattern supports the web-tier interface to separate the business logic from the access layer in order to avoid direct access to the back-end content of the ONW system. MVC also controls events responses between the business logic (I/O) and the persistence layer.

(ii) The interceptor pattern is used to align components or users with activities in the ONW system's transaction processes.

(iii) The adapters of the microkernel pattern enable the addition of external systems and ensure flexible communication channels between the access, business logic and persistence layers.

(iv) The microkernel architectural pattern of the ONW system's structure enforces the maintenance of the CIAAN services security features of all captured and stored PDE. The provisions of SSL and HTTPs are incorporated at the structural design of the ONW system using the microkernel architecture's bus as its connectivity adapters.

(v) The pipes-and-filters architectural pattern ensures that the ONW quality requirements (i.e. security, auditability, usability and pluggability) are realised. The encrypted audit-log is incorporated in the ONW system design by mean of pipes-and-filters architecture and microkernel adapters.

(vi) As shown in Figure 7.8, the microkernel and pipes-and-filters architectural patterns are encapsulated in the layered pattern to concretely address the security, reliability and auditability quality requirements of the ONW system. For example, for the encryption of captured PDE at upload and its decryption at download, the pipe (i.e. labelled ‘B’) is used to host the secure messaging channel. The microkernel bus (label ’C’) hosts the business logic of the system and provides stability functions as well as the adapter to allow for connections of additional components between the access layer and the persistence layer.

(vii) Another merit of using a layered architectural pattern is to realise flexibility, as well as pluggability quality requirements. The layered architecture allows for a technology-neutral design that frees the ONW system from technology lockdown [121]. The layered architectural pattern facilitates easy add-on to components in the access layer. For example, MySQL and PostgreSQL databases are employed during the design of the ONW system. However, should the need arise to change the database from its current state of MySQL and PostgreSQL to a document-oriented database, e.g. MongoDB or a graph-oriented database such as Neo4j, new databases can be added at any stage of the ONW system‘s life cycle, without the need for ONW system's re-designing.

Some of the benefits of using layered architecture at the highest-level of the ONW system is its manageability, scalability, flexibility and availability features[120]. The presentation layer consist of the web interface to interact with the system and the web services used to communicate with the business layer. The business tier is the business logic that carries the input/output operations of the system. The database tier provides storage and persistency of data within the ONW system.

7.4.4.2 The Persistence Layer

The persistence layer using pipes and filter architecture, holds the data access layer that encapsulates and exposes PDE data for access by other layers and components of the ONW system. The persistence layer supports object-relational mapper (ORM), and provides for the application programming interface (API) that presents a means to manage the stored PDE in the ONW repository.

Despite making the careful choices of architectural requirements to align with the identified functional requirements of the ONW system, there are some constraints that are required to be incorporated into the ONW system at its design specifications, and these are discussed next.

7.4.5 *Architectural Constraints of the ONW System*

Applying architectural constraints to the ONW system following the DFARS process focuses on the technological, legislative and jurisdictional constraints (see Figure 7.9). The different constraints are discussed in the next sections.

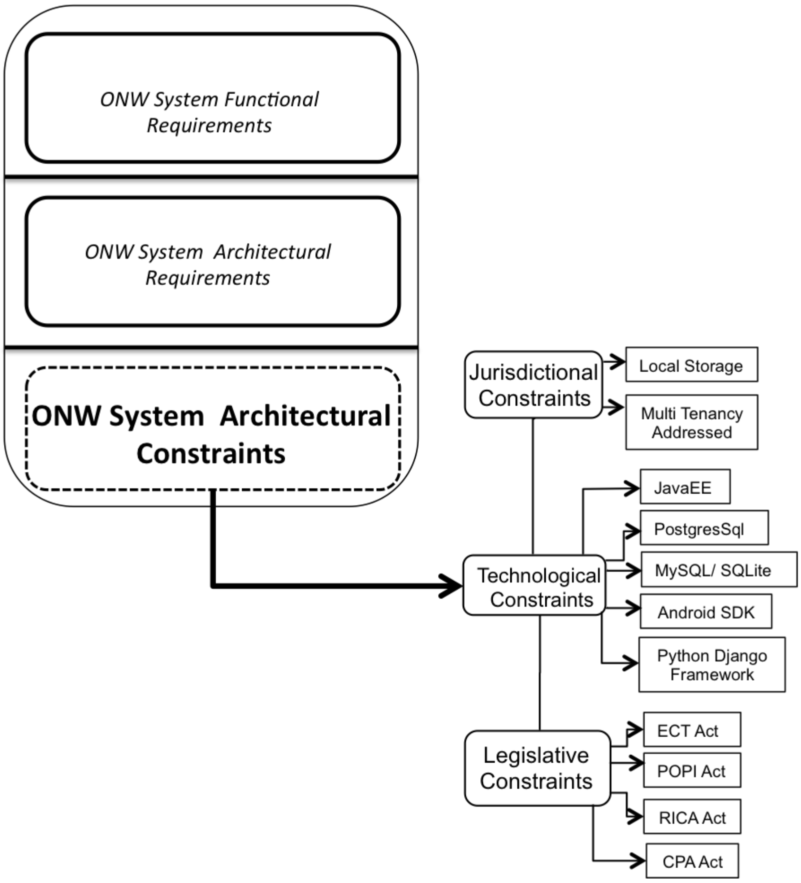

ONW System Functional Requirements
ONW System Architectural Requirements
ONW System Architectural Constraints
Jurisdictional Constraints
Local Storage
Multi Tenancy Addressed
Technological Constraints
JavaEE
PostgresSql
MySQL/ SQLite
Android SDK
Python Django Framework
Legislative Constraints
ECT Act
POPI Act
RICA Act
CPA Act

Fig. 7.9: Applying DFARS Process for ONW Architectural Constraints

7.4.5.1 Jurisdictional Constraints of the ONW system

Since the ONW system is designed and developed to function in the jurisdiction of South Africa, the laws and Constitution of South Africa are adhered to. Thus, the constraints around PDE storage are implemented in the ONW system to accommodate PDE tenancy regulations and allow for effective admissibility of PDE.

As can be seen in Figure 7.9, the ONW system is focused on South African legislation and communities, and the ONW repository (storage) is hosted in South Africa to avoid hosting in other regions with multi-tenancy law. The latter may render captured PDE invalid and inadmissible in South Africa.

7.4.5.2 Technological Constraints of the ONW system

The ONW system is required to have a mobile client (mobile app) that can be used by citizens, and a web interface for use by the LEA, DFI and the judiciary. These are incorporated in the ONW system as technological constraints as depicted in Figure 7.9.

The ONW system incorporates the following technological constraints at its design:

(i) The Android application contains primarily Java code. Java networking capabilities and features allow the mobile application to communicate with other components at the server side.

(ii) The web tier side of the ONW system is developed using JavaEE, GlassFish Server Open Source Edition Glass [122] and python Django Framework. MySQL and PostgreSQL are used as the database.

(iii) Persistency is accomplished using the object-relational mapper (ORM) that comes hand in hand with the Django Framework, and web services using REST Django framework.

(iv) The web interface can be accessed using browsers that support the standard HTTPs protocol.

7.4.5.3 Legislative Constraints of the ONW System

The Acts that must be adhered to in designing the ONW system to attain PDE validity and admissibility were outlined in Chapter 3 of this dissertation. For citizens to participate in the PDE-sourcing process, privacy rights must be shown to be indemnified even at the architectural specifications phase of the ONW system. The measures put in place to uphold legal requirements regarding evidential weight, hearsay, rule of relevance and completeness are as follows:

(i) Encryption is applied to protect citizens‘ personal information gathered during user registration. Encrypting the user’s information is to ensure confidentiality and protect the privacy of individual users of the ONW system. The ONW system uses a 2-way function encryption type for securing a citizen‘s personal information. In the event of the latter’s information being necessary to validate the authenticity of PDE, the LEA is required to obtain a court warrant and provide a matching key to decrypt the citizen’s personal details.

(ii) The non-compellable witness clause of the Criminal Procedures Act (CPA), Act 51 of 1977, Section 203 [88] makes it possible for a citizen who uploads PDE to choose whether to testify or provide his/her personal information to corroborate captured and stored PDE.

(iii) Session authentication is used to disable sessions that have been idle for a certain length of time and traditional usernames and passwords are used, applying password rules to increase users’ awareness. The use of session authentication to disable sessions after idle for a certain time length and the use of traditional username and password, applying password rules to increase user’s awareness.

Incorporating the architectural constraints into the ONW system design is the final building block of the ONW system architecture. It brings to completion the application of the DFARS process in the design and development of the ONW system.

7.5 *Conclusion*

In conclusion, this chapter proposed a process for designing a digital forensic application, termed digital forensic applications requirements specification (DFARS) process. This process takes into account the constant changing and upgrading of digital devices, and therefore makes provision for incorporating modifiability functions during the design of any DF application.

The DFARS process was employed in the design of the ONW system to demonstrate how the DFARS process can be applied to design any DF application. It began by identifying the functional requirements of the ONW system and focused on the ONW application‘s and users’ core requirements. These core requirements were subsequently mapped to identify the quality requirements of the ONW system. The quality requirements were addressed using architectural patterns and strategies, which led to addressing the ONW system’s architectural constraints.

With the design of the ONW system and identification of the core needs of the system now completed, the next stage is to use this ONW system’s design specifications to determine the best technology to develop the ONW system. The prototype of the ONW system is presented in the next chapter.

Chapter 8

PROTOTYPE OF THE ONLINE NEIGHBOURHOOD WATCH SYSTEM

8.1 *Introduction*

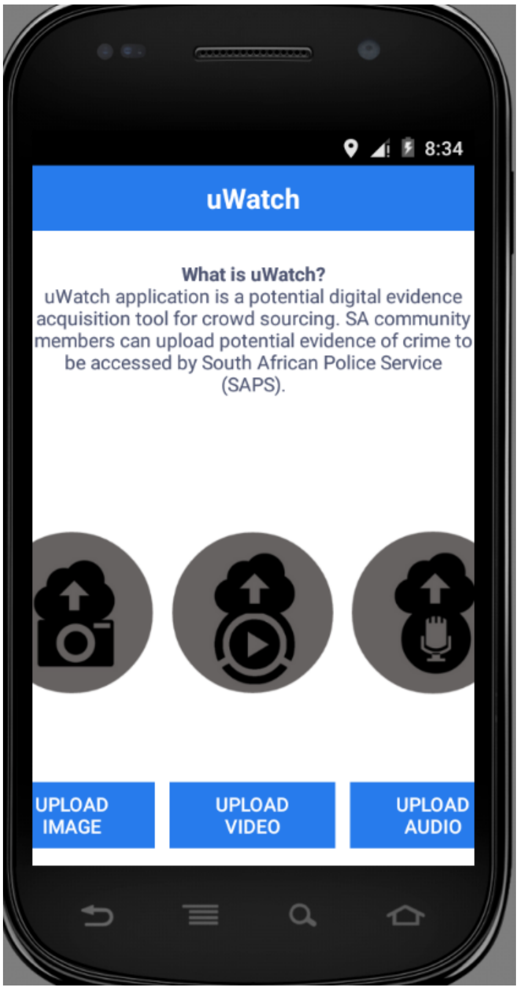
In the previous chapter, the online neighbourhood watch (ONW) system's design was described by making use of requirements engineering specifications. The specifications identified the main functionality of the system as functional requirements. The functional requirements were used to determine the architectural requirements specifications, which then resulted in a structural design of the ONW system's architecture [123].

This chapter presents the prototype of the ONW system [124]. It explains the ONW system prototype in the form of a user manual, thereby providing a guide to use the ONW system. Chapter 8 further elaborates on the ONW system prototype using a case study scenario. The remainder of this chapter is structured as follows:

- **Section 8.2 presents the uWatch application and uses the case study scenario suggested in Chapter 6.6. The uWatch application is the mobile client-side, in other words the uploader's side of the ONW system - Part A [13].**
- **Section 8.3 details the neighbourhood watch system (NWS), that is the downloader's side and Part B of the ONW system [15]. It further uses the same case study scenario.**
- **Section 8.4 summarises the ONW system using the case study scenario as discussed in Chapter 6.6. It describes the PDE upload, storage, and investigation procedures that can lead to the resolution of a neighbourhood crime.**
- **Section 8.5 introduces the technical implementation of the uWatch application and the NWS. The detailed implementation, and code example of the uWatch application, as well as its interaction with the NWS is presented in Appendix A.3.**
- **Section 8.6 concludes this chapter.**

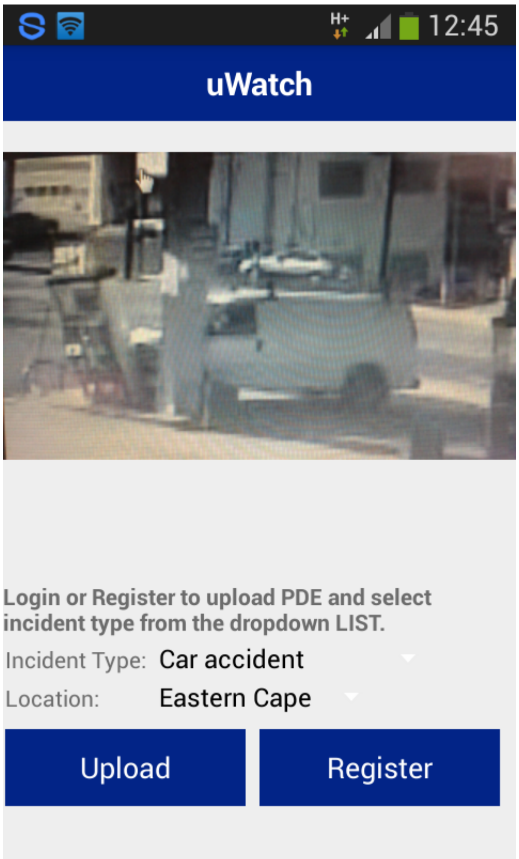
8.2 *uWatch Application*

The uWatch application is the client-side of the ONW system, i.e. Part A, which is designed as a mobile device application utilised by the citizens. It is developed using Android APIs and employs the services of existing functionalities of Android devices such as the mobile devices camera and microphone to do PDE-capturing. The uWatch application is designed to present a simple, easy-to-use community policing application front-end. At the launch of the uWatch application, the citizen is prompted to select the PDE data type i.e. photo image, video or audio of an alleged criminal activity. When any of the option buttons are selected (see Figure 8.1), the built-in camera and audio features of the Android device are activated to commence PDE-capturing. Figure 8.1 depicts the first user interface when the uWatch application is launched. By touching the photo, audio or video icon, the PDE-capturing process is activated. Every captured PDE incident is furnished with PDE attributes that focus on the offence type, the date/time of the alleged crime and the location of the incident, as well as other metadata associated with the captured PDE.



What is uWatch?
uWatch application is a potential digital evidence acquisition tool for crowd sourcing. SA community members can upload potential evidence of crime to be accessed by South African Police Service (SAPS).

Fig. 8.1: uWatch Application Welcome



Login or Register to upload PDE and select incident type from the dropdown LIST.

Incident Type: Car accident
Location: Eastern Cape

Fig. 8.2: uWatch Application Citizens Upload Functions

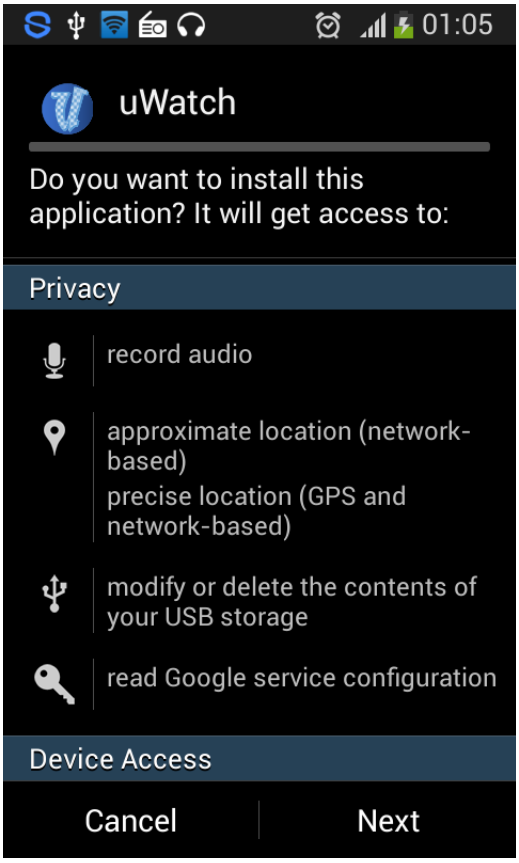
The uWatch application enables members of the community (citizens) to capture photo images, videos or audios as potential evidence of criminal behaviour perpetrated by individuals or groups within their neighbourhood. Using the case study scenario as discussed in Chapter 6.6, the citizen termed as onlooker 'O' touches the photo icon to photograph the vehicle used by the hit-and-run driver. The mobile device captures the brand and number plate of the vehicle in a photo, after which the photo is uploaded by 'O' to the ONW system's repository. The metadata logged from the mobile device shows that the photograph was captured on the 1 of August 2015, at 14:00 in Midrand, Gauteng.

8.2.1 *Download and Installation of uWatch Application*

To start with, the citizen is required to download and install the uWatch application on his/her mobile device. This is where the encryption library of uWatch provide the public (U_{pub}) and private (U_{priv}) key for uWatch application at the uWatch download and install. The uWatch application then requests for the approval of the user in order to access the microphone, camera and the GPS functions of the mobile device (reference Figure 8.3, this occurs at the installation process, prior to the user capturing any PDE). This request process is also considered as another vetting process put in place for the ONW system to check that a citizen that chooses to participate in the PDE sourcing process, is indeed a human. The vetting ensures that the citizen is not just human, but is actually in a physical location verified by the GPS coordinates using the geolocation metadata at the uWatch application side. It also further acts as verification and validation of the PDE received from this user during the life-span of the uWatch application on the device of the user. The citizen may allow this request by enabling the functions or disallow the request. In the latter case, disallowing the uWatch application from using these functions of the user's device automatically disables the PDE-capturing process, which in-turn defeats the purpose of the uWatch application. However, to ensure a successful uWatch application installation and usage, this option is to be accepted by the citizen (see Figure 8.4). The purpose of this step is to acquire accurate location information of an alleged crime and indicate the location where the PDE was captured. The parameters entered here are part of the search parameters used by the LEA when requesting PDE from the NWS. The metadata is used in collaboration with the PDE and other metadata artifcates to enhance the forensic soundness of the captured and stored PDE payload. The PDE payload retains PDE validity, chain of evidence and eventually supports the admissibility of the PDE during crime investigations, or as real evidence in a court proceeding in conjunction with expert witness. Figures 8.3 and 8.4 depict the user installation of the uWatch application and the permission access request.

8.2.2 *Capturing of Potential Digital Evidence*

The actual process of capturing PDE occurs when a citizen witnesses a crime. The citizen selects the option to capture PDE, either as a photo image or video or audio recording (see Figure 8.1). After PDE capturing, the citizen is given the option to enter some description



01:05

uWatch

Do you want to install this application? It will get access to:

Privacy

record audio

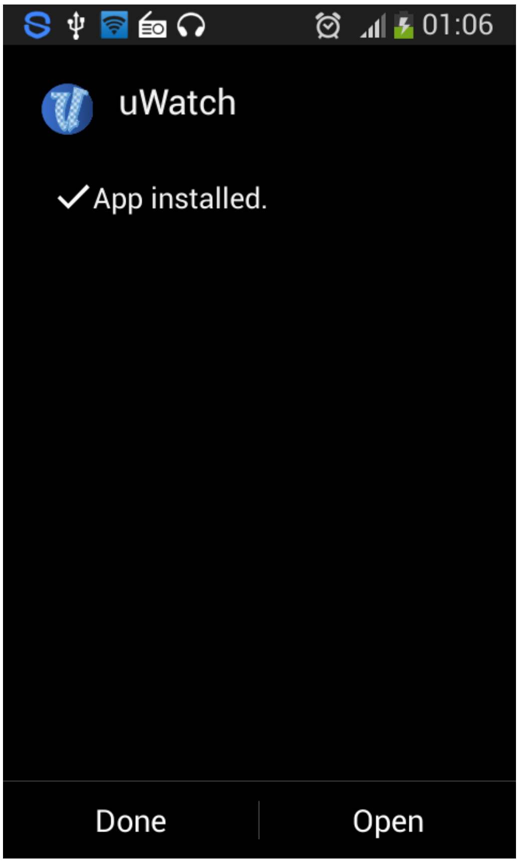
approximate location (network-based)
precise location (GPS and network-based)

modify or delete the contents of your USB storage

read Google service configuration

Device Access

Fig. 8.3: uWatch Application Requesting User's Permission



01:06

uWatch

✓ App installed.

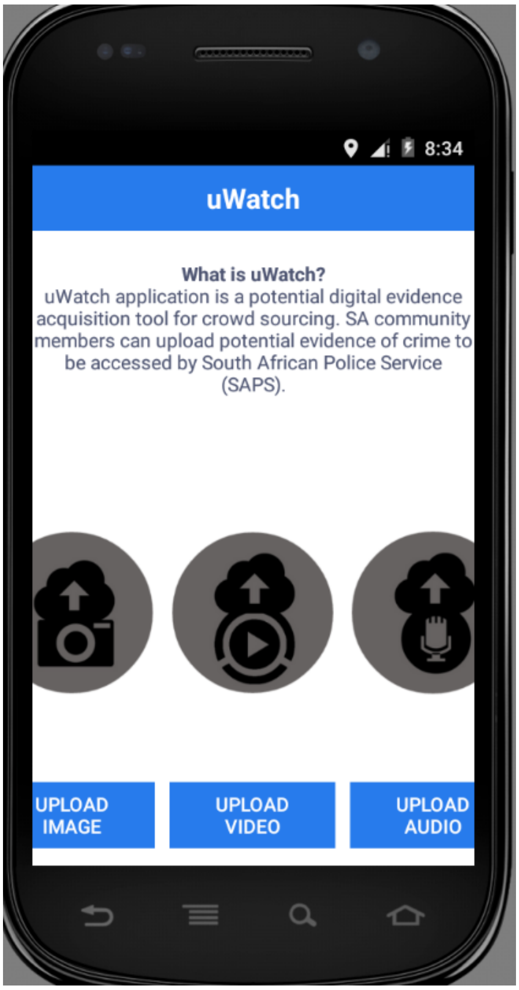
Fig. 8.4: uWatch Application after Installation Screen

of the captured PDE. For the safety of the citizen who captures PDE, the upload can be carried out at any time or at a place away from the original location of the alleged crime. However, both the PDE-capturing locations and upload locations are shown in the audit log, together with metadata of the PDE. Because the uWatch application enabled the 'capture-now-upload-later' function, PDE can be captured and uploaded at any time. Say for instance a situation arises where PDE can be captured by an eyewitness (onlooker 'O') with or without a WiFi or cellular network data connection. On the architecture side, provision is made for offline upload by using the message queue protocol. With the message queue functions, citizens can upload the captured PDE at a later time, such as when Internet connection is available to the device of user or when in a safe location, away from the crime incident. The 'capture-now-upload-later' function of the uWatch application is also used in a scenario where the citizen cannot immediately upload the captured PDE to the NWS repository. In the case study scenario, 'O' uploaded the PDE immediately after capture, as the scene of the alleged crime did not pose any danger to her. This is because the hit-and-run driver sped away from the scene after the accident. 'O' added the incident scene description attributes.

The descriptive information parameters entered by the citizen provides an enhanced account of the alleged crime as perceived by the citizen. As is clear from Figure 8.6, this descriptive information constitutes the keywords that are used to categorise the cases in relation to the uploaded PDE with regard to various incidents as stored in the NWS repository. The description, for example, includes the type of crime the citizen perceived to be occurring, the location of the incident and the circumstances under which the alleged crime occurred. The uWatch application gives a drop-down menu from which the citizen may select the appropriate description, and can add more descriptions when necessary.

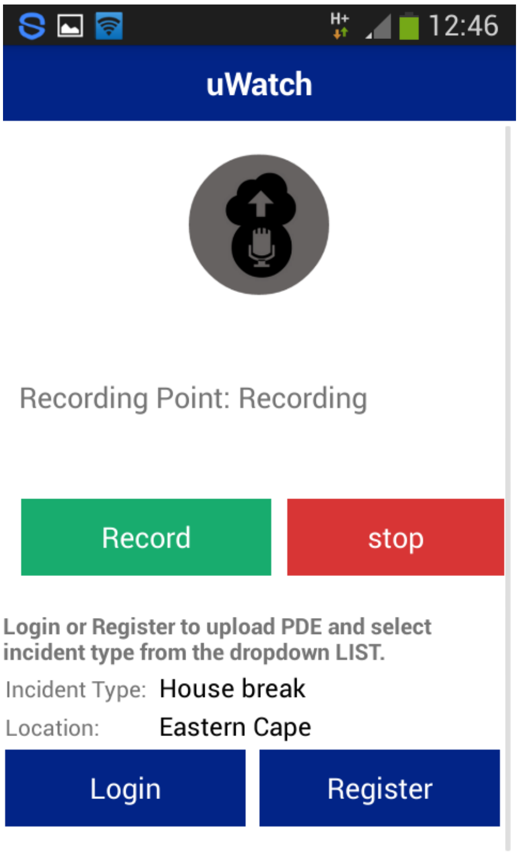
8.2.3 *User Authentication and Login Process*

As presented in Section 5.3.8 for an upload of captured PDE to the NWS repository to occur, the citizen is required to provide user information which follows a sequence of hand-shake protocols (see Figure 5.4a, 5.6a). This is because to upload the captured PDE, the citizen is first required to register or login (see Figure 8.5). In the hit-and-run scenario, 'O' registered at time of uWatch application download to her device. For citizen 'O', authentication is required to upload the captured PDE of the photo of the hit-and-run vehicle, since this was her first-time to upload after the uWatch application had been installed. In a nutshell, authentication is only necessary when a user wishes to upload the captured PDE to the ONW system.



What is uWatch?
uWatch application is a potential digital evidence acquisition tool for crowd sourcing. SA community members can upload potential evidence of crime to be accessed by South African Police Service (SAPS).

Fig. 8.5: Citizens Capturing PDE



Recording Point: Recording

Login or Register to upload PDE and select incident type from the dropdown LIST.

Incident Type: House break

Location: Eastern Cape

Fig. 8.6: Citizen's PDE Upload Process

8.2.4 *Feedback and Acknowledgement*

The feedback and acknowledgement mechanism is one of the ways to achieve communication between the uWatch application and the community members who take part in the PDE-sourcing processes. Feedback is used as a means of encouraging community members, to continually participate in the PDE crowd-sourcing process. The uWatch application receives feedback from the ONW system when processes have been completed, such as a successful PDE upload, when PDE uploaded by a citizen is used for crime investigation and/or when PDE is used in a court of law. In the case study scenario, when ‘O’ completed the upload of the captured photo to the ONW system, she received an email acknowledging the upload as successful, followed by a generic expression of appreciation. At the download of the PDE, ‘O’ received another acknowledgement, and a final one when the photo PDE was used to prosecute the hit-and-run driver. The active feedback mechanism of the uWatch application sends an email to the citizen’s registered address and/or a message via the on-screen pop-up window on the user’s mobile device. The user can choose to deactivate the feedback function at any time, and may select whether to receive email or on-screen feedback. Other feedback on the uWatch application occurs when there is an error or exception at registration, at the login, or at upload of captured PDE. These feedback messages are all captured in the audit log.

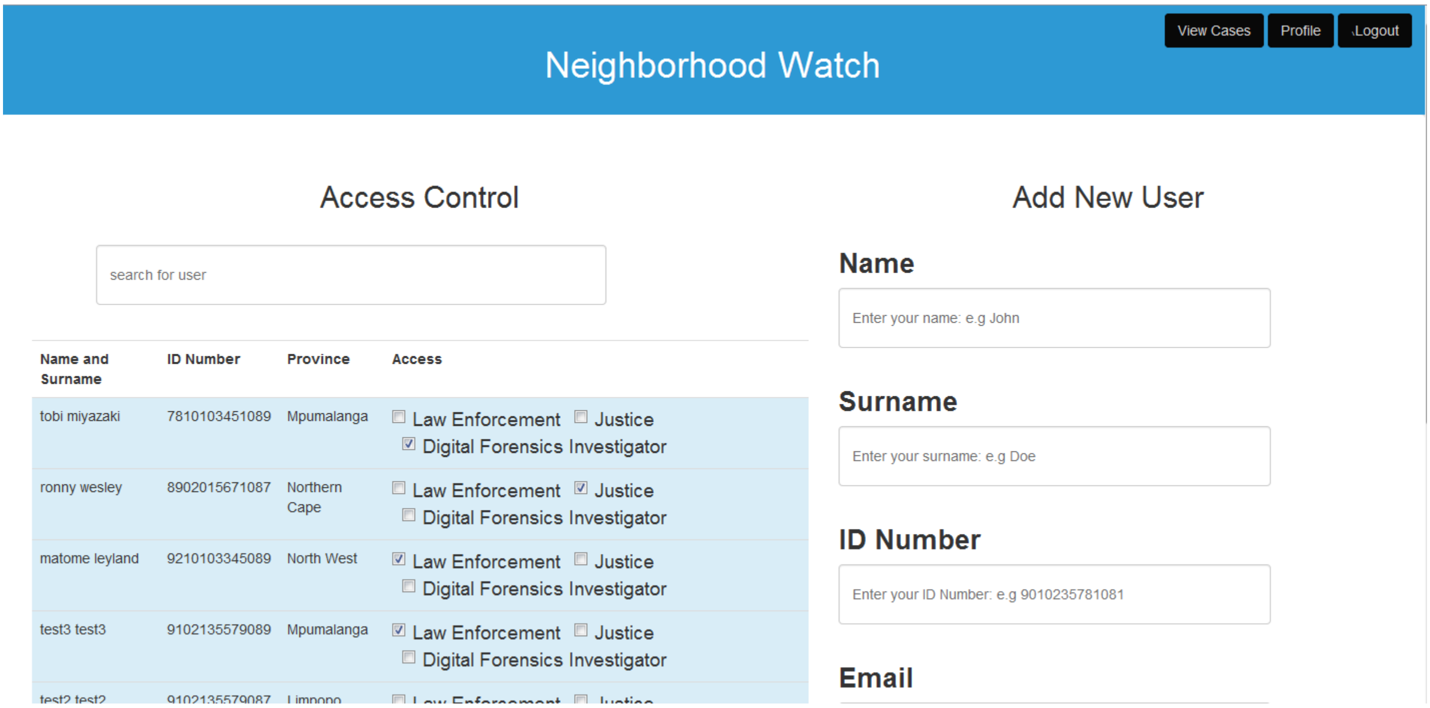
To achieve the main objectives of the PDE crowd-sourcing process, a user must always open the uWatch application and capture PDE from within the uWatch application domain. Any PDE captured outside the uWatch domain is discarded at an upload attempt due to uncertainty about its forensic soundness. PDE discarding also occurs when a user attempts to upload either a video, audio or photo from the device’s storage gallery, as this could potentially lead to uploading a photo that is not forensically sound. Only PDE captured from within the uWatch application domain is accepted at upload. The onlooker (as in this case study scenario) can be any person who witnesses a crime and has the uWatch application installed on his/her mobile device.

The uWatch application is developed in conjunction with the neighbourhood watch system (NWS). The uWatch application falls under Part A of the ONW system and is discussed in Chapter 5, while the NWS falls under Part B and is discussed in the ONW system‘s modelling in Chapter 6. The uWatch application and the NWS communicate and interact with one another to generate an audit trail of both systems. The audit trail that is generated formulates a chain of evidence [45] [125], from the time of the uWatch application’s launch on the citizen‘s device to the time when the captured PDE is downloaded from the ONW system’s repository by the authorised users.

The sections above presented the uWatch application and illustrated it with the case study scenario described in Chapter 6.6, while the next section describes the Neighbourhood Watch system (NWS) that is Part B of the ONW system.

8.3 *Neighbourhood Watch System*

The neighbourhood watch system (NWS) is used to store, retrieve and maintain PDE captured with the uWatch application. The system is managed by the System Administrator. The potential users of the NWS are the law enforcement agents (LEAs), digital forensic investigators (DFIs) and judiciary, as allocated by the System Administrator. Each of these authorised users maintains a level of access as allocated by the System Administrator. Figure 8.7 shows the access management functions of the System Administrator who creates the access rights of a LEA or DFI in order to download stored PDE from the ONW system's repository.



Neighborhood Watch

Access Control

search for user

Name and Surname	ID Number	Province	Access
tobi miyazaki	7810103451089	Mpumalanga	□ Law Enforcement □ Justice ☑ Digital Forensics Investigator
ronny wesley	8902015671087	Northern Cape	□ Law Enforcement ☑ Justice □ Digital Forensics Investigator
matome leyland	9210103345089	North West	☑ Law Enforcement □ Justice □ Digital Forensics Investigator
test3 test3	9102135579089	Mpumalanga	☑ Law Enforcement □ Justice □ Digital Forensics Investigator
test2 test2	9102135579087	Limpopo	□ Law Enforcement □ Justice

Add New User

Name

Enter your name: e.g John

Surname

Enter your surname: e.g Doe

ID Number

Enter your ID Number: e.g 9010235781081

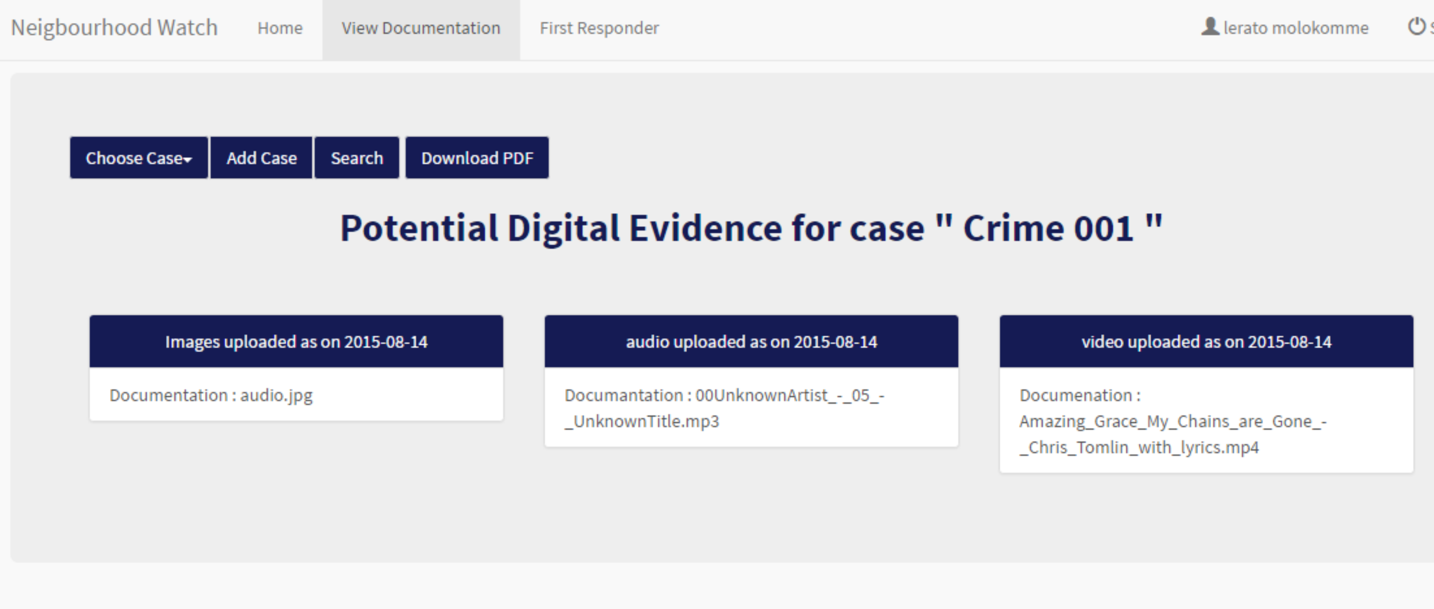
Email

Fig. 8.7: NW System Administration Login

The case study scenario is used to further illustrate the interaction of authorised users such as LEAs, who are required, for instance to investigate the incident of the of hit-and-run accident in the Midrand neighbourhood of Gauteng. The LEA requires access to the NWS from the System Administrator. The required access is created in relation to the attributes of the case, in other words the hit-and-run accident using the date (1 August 2014), time (14:00) and location of the alleged crime incident (Midrand). Using these attributes, the LEA creates the incident profile and provides partial attributes of the alleged offender.

8.3.1 *Authorised Users of the NWS*

The System Administrator is the only user who can add other authorised users to gain access to the NWS. The functions of the system administrator includes to adds users and cases, assigns cases to authorised users (see Figure 8.7), remove users access or decrypt the information of the citizen's details of upload. An authorised user‘s access is created using his/her specific user details such as identity number, name, surname, email, and a random password, which the user is required to change. At the creation of the user‘s account, an email is forwarded to his/her setup email account, with an activation link to enable him/her to update the random password and other profile details. However, this link is only valid for 24 hours, after which it becomes invalid. Furthermore, the identity (ID) information of an authorised user is static and constitutes the primary key for such an authorised user. The ID of the user is pre-added and cannot be altered. All processes on the NWS generate audit logs that are stored and are available as chain of custody.



Potential Digital Evidence for case " Crime 001 "

Images uploaded as on 2015-08-14

Documentation : audio.jpg

audio uploaded as on 2015-08-14

Documantation : 00UnknownArtist_-_05_-_UnknownTitle.mp3

video uploaded as on 2015-08-14

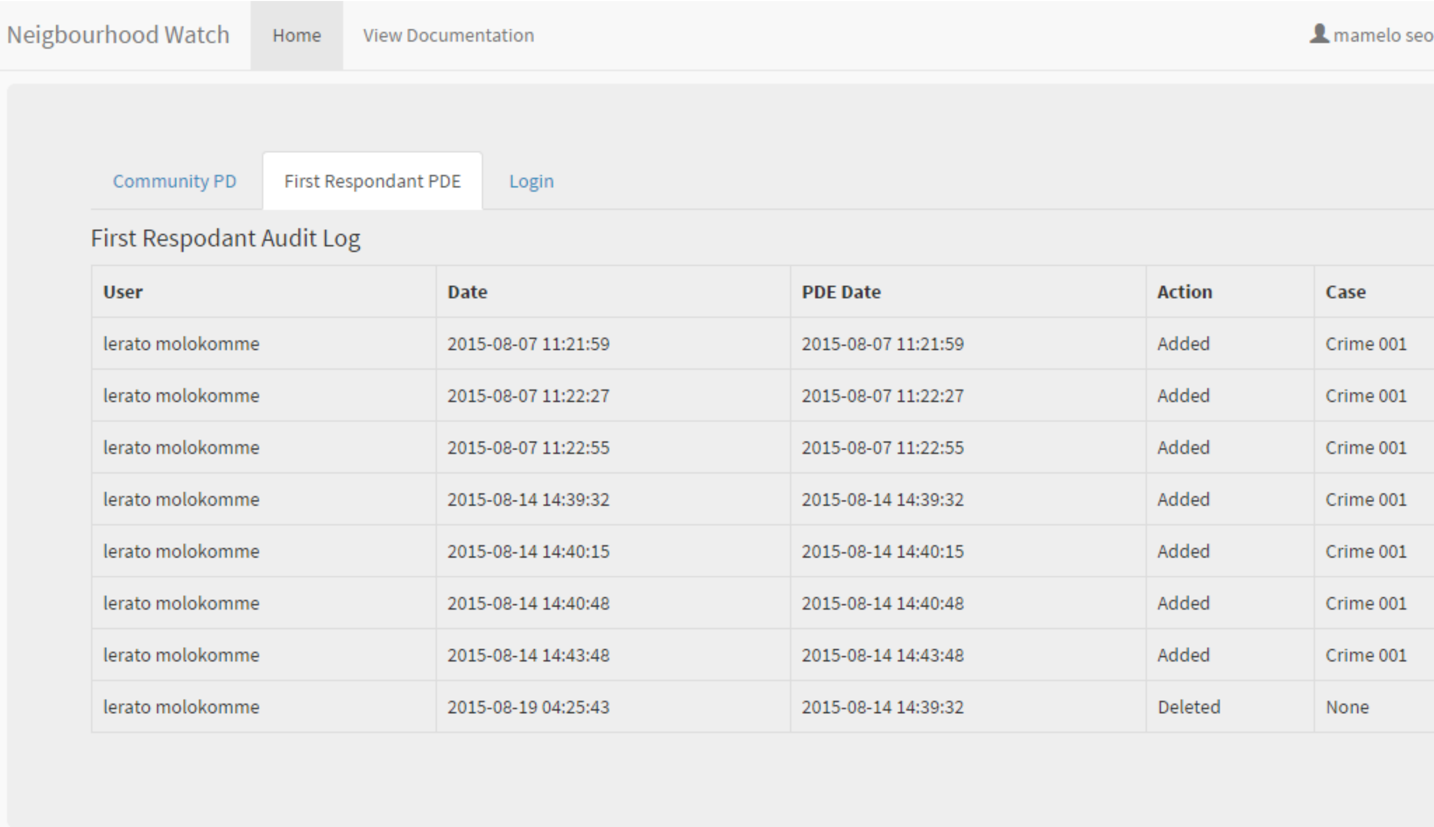
Documenation : Amazing_Grace_My_Chains_are_Gone_-_Chris_Tomlin_with_lyrics.mp4

Fig. 8.8: System Administrator's adding Authorised Users to NW system

Furthermore, in the event that an authorised user who was registered by the System Administrator does not logon, the user's details are automatically deleted from the NWS. In the same vein, a registered authorised user's access is disabled once the case attached to the authorised user is closed. This is in order to ensure that strict access management of the NWS is maintained, even to the authorised users. The attributes of a case under investigation are aligned with the authorised user's access to the crimes uploaded and stored in the ONW system's repository. Therefore, when a case is closed, the authorised user's access to the case content is also closed. Furthermore, to access the NWS for a new case under investigation, an authorised user must be re-activated by the System Administrator, where the System Administrator re-adds the authorised user to the NWS by adding attributes related to the new case. Implementing the restricted authorised user access processes is another means to ensure access control and maintain overall confidentiality in the ONW system.

8.3.1.1 Access to Authorised Users

When investigating a crime the law enforcement agent downloads the uploaded PDE of cases with attributes based on the categories of uploaded PDE, in other words time/date, location, images, video and audio, as they are related to the current case under investigation. Cases are selected using the dropdown option ‘Choose Case’ (see Figure 8.8). The LEA uses the ’Assign Case’ button to assign PDE to various cases. When an authorised user deletes PDE that is not relevant to an investigation, the PDE is only marked for deletion, and not for removal from the ONW system’s repository. The ‘Mark for Deletion’ function renders the PDE inaccessible to the user or other authorised users. Only the System Administrator can permanently delete or undelete PDE marked for deletion from the ONW system’s repository.



First Respodant Audit Log

User	Date	PDE Date	Action	Case
lerato molokomme	2015-08-07 11:21:59	2015-08-07 11:21:59	Added	Crime 001
lerato molokomme	2015-08-07 11:22:27	2015-08-07 11:22:27	Added	Crime 001
lerato molokomme	2015-08-07 11:22:55	2015-08-07 11:22:55	Added	Crime 001
lerato molokomme	2015-08-14 14:39:32	2015-08-14 14:39:32	Added	Crime 001
lerato molokomme	2015-08-14 14:40:15	2015-08-14 14:40:15	Added	Crime 001
lerato molokomme	2015-08-14 14:40:48	2015-08-14 14:40:48	Added	Crime 001
lerato molokomme	2015-08-14 14:43:48	2015-08-14 14:43:48	Added	Crime 001
lerato molokomme	2015-08-19 04:25:43	2015-08-14 14:39:32	Deleted	None

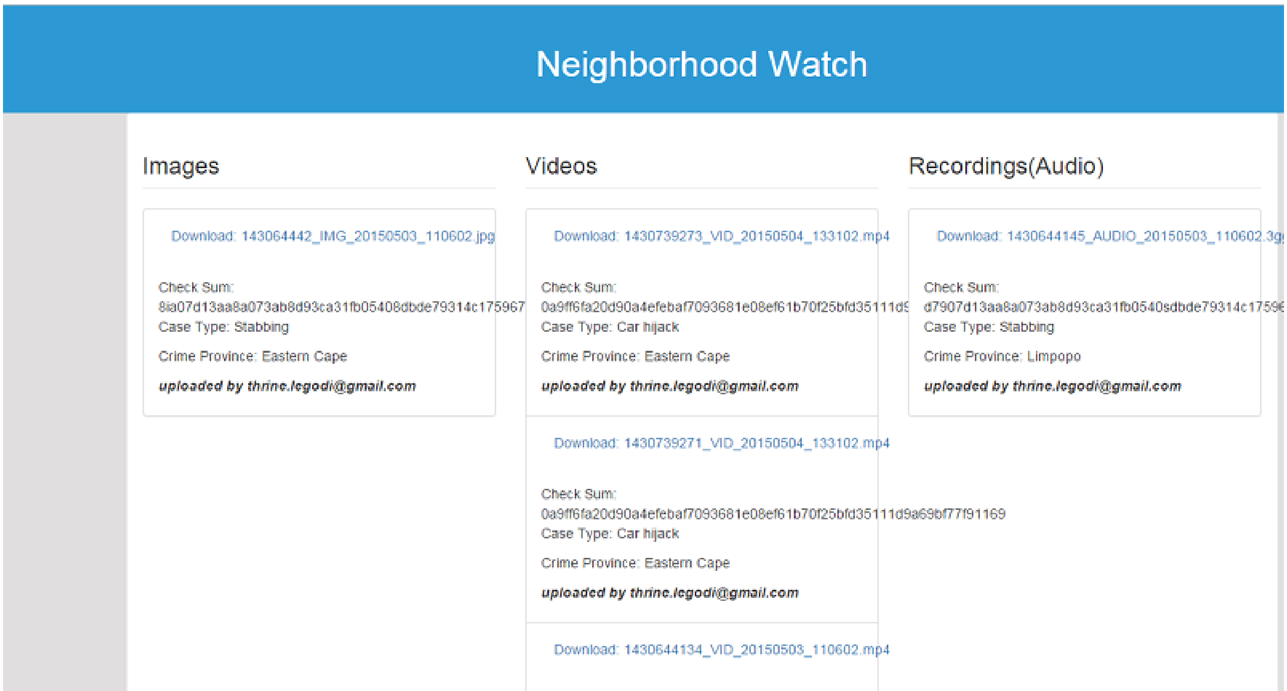
Fig. 8.9: Audit Log File of the ONW system

As seen is Figure 8.2 audit log (AL) of the ONW system is one of the processes used to check and balance the various activities that occur from the moment a citizen installs the uWatch application to their device, to the moment where the captured PDE is downloaded by an authorised user (LEA, DFI or judiciary). Furthermore, as depicted in the Figure 8.9, all actions or components of actions by users in the ONW system are logged and retained in the audit log location. The auditability functions are maintained using MySQL trigger, PHP validation and global interceptor. The triggers automate the auditlog, while rules are created by the rule engine specified at the system's configuration to allow traceability of all users' and components' activities. Figure 8.9 depicts the NWS audit log file view.

In the case study scenario presented, the LEA receives a complaint in respect of the hit-and-run accident victim. He/she begins an investigation into the case with the information supplied by the complainants on reporting the incident. The LEA requests access to the NWS, the NWS searches the PDE payload using the search parameters provided by the LEA such as attributes of the case like hit-and-run accident, date/time and location of the alleged crime. Using the attributes of the hit-and-run incident, the LEA creates a profile that describes the incident. Based on the created incident profile, the LEA creates the potential attributes of the alleged offender to commence investigation. Using PDE payload from the NWS in place, the LEA can get the PDE related to the crime by using the attributes as they concern a hit-and-run incident on 1 August, which was in photo format uploaded by 'O'.

8.3.2 *Verification of PDE's Forensic Soundness*

The process of forensic soundness verification is put in place, so that in the unlikely event of PDE being tampered with, the hashing of the captured PDE - in combination with the forensic soundness indicators - allows the LEA to verify the consistency of PDE at download, especially when it is required to be used for crime investigation.



Neighborhood Watch

Images

Download: 143064442_IMG_20150503_110602.jpg

Check Sum:
8ia07d13aa8a073ab8d93ca31fb05408dbde79314c175967
Case Type: Stabbing

Crime Province: Eastern Cape

uploaded by thrine.legodi@gmail.com

Videos

Download: 1430739273_VID_20150504_133102.mp4

Check Sum:
0a9ff6fa20d90a4efebaf7093681e08ef61b70f25bfd35111d9
Case Type: Car hijack

Crime Province: Eastern Cape

uploaded by thrine.legodi@gmail.com

Download: 1430739271_VID_20150504_133102.mp4

Check Sum:
0a9ff6fa20d90a4efebaf7093681e08ef61b70f25bfd35111d9a69bf77f91169
Case Type: Car hijack

Crime Province: Eastern Cape

uploaded by thrine.legodi@gmail.com

Download: 1430644134_VID_20150503_110602.mp4

Recordings(Audio)

Download: 1430644145_AUDIO_20150503_110602.3g

Check Sum:
d7907d13aa8a073ab8d93ca31fb0540sdbde79314c17596
Case Type: Stabbing

Crime Province: Limpopo

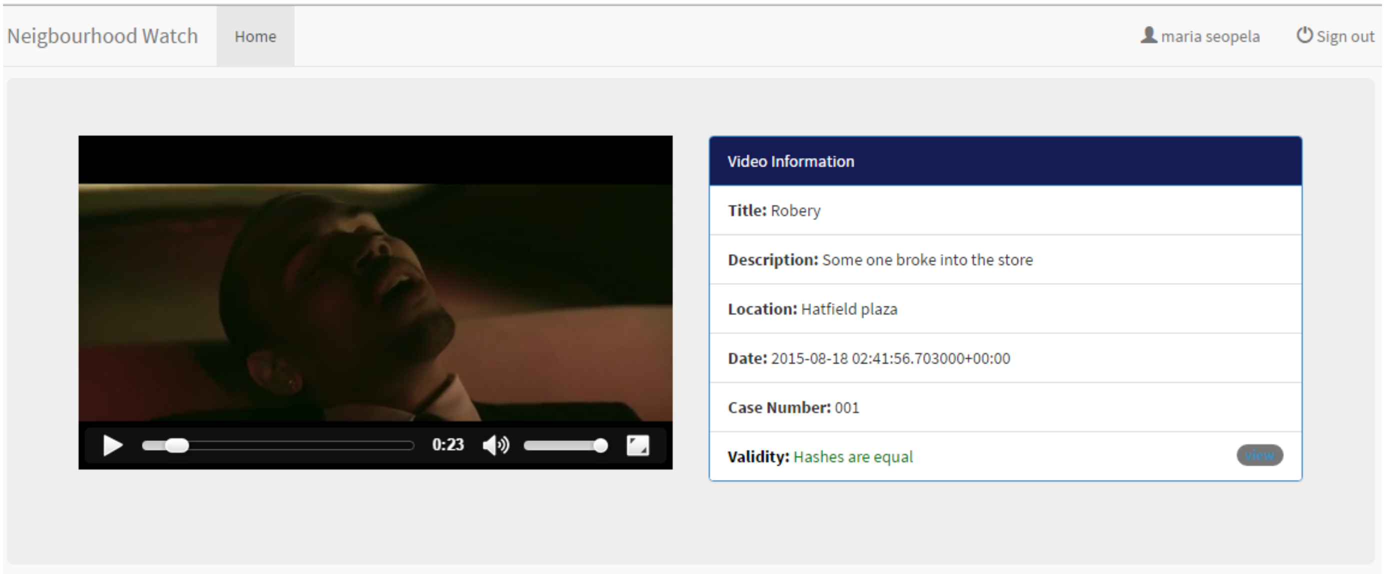
uploaded by thrine.legodi@gmail.com

Fig. 8.10: Stored PDE in the NWS Repository

The hash value of the stored PDE must be the same as the hash value of the downloaded PDE to ensure PDE validity (see Figure 8.10) The NWS strives to protect the citizen's privacy rights and uses encryption to ensure that the information entered into the NWS database on user information creation of the uWatch application side is stored confidentially. As shown in

Figure 8.11, the LEA uses keywords entered by the citizen at PDE upload to identify crime incidents related to the crime under investigation.

The NWS repository stores all captured and stored PDE payload, as well as their checksum value (see Figure 8.10). The NWS repository data base table is categorised based on the PDE data type, i.e. images, videos and audios and well as PDE attribrites. The PDE type is further grouped using the metadata of the device, like the location where the PDE was captured (see for example Figure 8.5, the PDE was captured in the Eastern Cape), as well as the time, date and type of the alleged crime.



Video Information

Title: Robery

Description: Some one broke into the store

Location: Hatfield plaza

Date: 2015-08-18 02:41:56.703000+00:00

Case Number: 001

Validity: Hashes are equal

Fig. 8.11: Stored Video PDE

In the case study scenario, the LEA is required to compare the hash value of the stored photo PDE and that uploaded by ‘O’. On finding the values to correspond (therefore verifying the forensic soundness of the PDE), the PDE is considered tamper free and can be used for further investigation of the hit-and-run accident. The LEA proceeds to download the photo, which leads to the discovery of the offender‘s vehicle licence registration plate number. This enables the LEA to identify both the vehicle and its owner. Using the photo PDE from the NWS repository, and eyewitness accounts of the incident, prosecution of the crime is made.

In this chapter, the scenario of the hit-and-run accident was used to discuss the details of the various aspects of the uWatch application and the NWS focusing on the usability, rather than the technical details. The next section summarises this chapter and focuses on the case study scenario.

8.4 *Summary of the ONW System Interaction using the Case Study Scenario*

The scenario presented describes a case of reckless driving where an on-coming vehicle runs down a teenager. The driver of the vehicle continues onward without rendering assistance to the victim or reporting the accident to an appropriate authority. Citizen 'O' launches the uWatch application already installed on her mobile device and is able to capture the scene of the hit-and-run accident. She uploads the captured photo (PDE) to the NWS. The LEA assigned to investigate the alleged accident routinely makes use of PDE stored in the ONW system and requests access to the NWS to investigate the accident. The case study scenario is summarised in the following steps:

(i) The witnessing of a crime by 'O' is the first event of this process.

(ii) The witness 'O' then captures a photo image of the hit-and-run crime using the uWatch application installed on her mobile device.

(iii) The citizen (witness 'O') logs in (see Figure 8.5) to upload the captured PDE to the ONW system's repository. After successful upload of the captured PDE, the citizen receives an acknowledgement of a successful PDE upload.

(iv) In a different event, a LEA receives a complaint report of a hit-and-run accident stating the date, approximate location and time.

(v) The LEA requests access to stored PDE from the NWS, after passing through the authentication processes than involve asymmetric key pair exchange, certificate authority verifications and the sharing of communication from the System Administrator who then checked to confirm the LEA's role on the system. This therefore mean that the crime investigation can commence.

(vi) The System Administrator creates a case access and allocates access rights to the LEA. Access rights are allocated based on the LEA's role and the parameters plus attributes of the hit-and-run incident.

(vii) The LEA downloads and decrypts the stored PDE.

(viii) The LEA examines the downloaded PDE to validates that the PDE is forensically sound, thus rendering it admissible as evidence in the prosecution of the offender.

(ix) Once the PDE has been verified as forensically sound, the LEA correlates the accidents and matches the PDE with the complainants' reported incident in relation to time, date and location.

(x) Using the findings from the PDE photo, the LEA is able to secure a warrant to arrest the suspected offender.

(xi) The LEA notifies the judiciary by arraigning the offender before the court for prosecution.

(xii) Finally, by using the evidence from the ONW system, the judiciary is able to successfully prosecute the offender.

The scenario above, using the ONW system, is described by using software implementation technologies that are presented in detail in Appendix A.3. The next section gives a brief overview of the technical implementation of the ONW system - that is the uWatch and the NWS.

8.5 *Summary of the Technology used for the ONW System*

Transactions between the uWatch application and the NWS are initiated using servlets to initiate the call function from the access layer to the persistence layer, via the business logic layer. All data is converted to JSON format at creation using schema parse through the HTML, Rest Web services and PHP cluster. Using the JSON objects format allows for easy parsing of the video files, while enhancing the performance of the entire system. This is because JSON objects are faster to parse, lighter, and more flexible with PHP, and they present data in a more readable format in comparison to the XML message transfer protocol. Other technical details regarding the addressing of the various quality requirements of the ONW system are presented in Appendix A.3.

8.6 *Conclusion*

The ONW system prototype discussed in this chapter shows the processes employed in crowdsourcing PDE by the citizens of a community to capture, store and utilise PDE. The uWatch application and the NWS are the main components of the ONW system that function together as one entity to make PDE available to law enforcement agents (LEA) and the judiciary. The processes demonstrated in the ONW prototype all underline the need for co-operation between members of a community and the LEAs in mitigating neighbourhood crime. The prototype shows the technical measures that ensure privacy protection of the citizens involved, and the constant feedback given by the ONW system, which serves to encourage citizens to participate in this community policing initiative.

Part V

EVALUATION

This section evaluates the research conducted for purposes of this study and provides a critical evaluation of the contribution made by this dissertation. Chapter 9 discusses the proposed ONW system, focusing on the pros and cons of the ONW system and its development. Chapter 10 reviews related work that has had an impact on this research.The chapter clearly identifies the contributions of this research and compares these contributions to the reviewed related literature. Chapter 11 concludes the research and highlights some future work.

Chapter 9

CRITICAL EVALUATION

9.1 *Introduction*

This chapter evaluates various aspects of this research. It begins with an overview of the purpose of this study, which is to propose an online neighbourhood watch (ONW) system, a PDE crowd-sourcing tool to mitigate neigbourhood crimes. The ONW system was proposed to provide a forum where citizens of a community, together with law enforcement agents (LEAs), could use potential digital evidence (PDE) to curb neighbourhood crime. By applying information security services and digital forensic techniques, the PDE captured using the ONW system is rendered admissible in any court of law. The remainder of this evaluation chapter is structured as follows:

- **Section 9.2 discusses the benefits of this research.**
- **Section 9.2.8 shows the contribution of this dissertation to the body of knowledge.**
- **Section 9.3 present some shortcomings of this research.**
- **Section 9.4 concludes the chapter.**

9.2 *Benefits of the research*

The ONW system uses mobile devices application (uWatch) as a means to generate PDE of criminal behaviour in a community. The PDE captured by means of the ONW system could be used to corroborate other evidence recovered from crime scenes. Seeing that the ONW system enables citizens to participate in neighbourhood crime eradication, the following are the identified benefits of this research:

9.2.1 *Usability and Accessibility to Citizens*

The proposed ONW system is a community policing application that uses the existing capture and share functions of Android mobile devices. The uWatch application that was developed to feed data into the ONW system, employs the social media approach of image capturing and sharing. However, there is a clear difference in that the ONW system is focused on capturing PDE of neighbourhood crime that can be used by law enforcement agents in crime investigations and eradication. Furthermore, the originality of the PDE is ensured from the point of capture to its usage as potential evidence in a court of law. The uWatch application is user friendly, designed and developed to ensure intuitiveness, and users who are comfortable using an Android device could easily use the system. In fact, any user who has used an Android device will be familiar with the user interface of the uWatch application. In the same vein, the NW system utilised by the LEAs and the judiciary is also developed with usability as one of its key features. The LEAs can use the system with little to no training required.

9.2.2 *A Community Policing instilled with Digital Forensics*

Another benefit of this research is the functions that enable it to explore the use of crowdsourcing techniques in neighbourhood crime eradication, while concretely addressing concerns of digital forensics. Community members in crime-ridden communities can therefore implement a proactive measure to reduce crime using the ONW system to generate potential evidence and be sure that the potential digital evidence generated is applicable and useful in terms of legal requirements.

Community policing is by no means a new concept, and this research merely adapted the concept, to the current digital age where mobile devices are used by people from all walks of life. Furthermore, this research draws on the South African philosophy of Ubuntu as prevalent in traditional African societies, where community spirit is fostered and co-operation is encouraged. The ONW system offers a method where citizens can conveniently participate in crime watch in their neighbourhood. By using their mobile devices, they become the eyes and ears of the law enforcement agents, in identifying criminals and providing evidence of neighbourhood crimes. Communities who co-operate with the LEAs and judiciary in tackling neighbourhood crime become more self-confident and mutual trust is engendered between these communities and government authorities.

9.2.3 *Applying Legal and Ethical Standards*

A clear benefit of this research relates to the way in which it implemented South African legal guidelines and ethical standards. For example, the ECT Act (25 of 2002) [17] [126] states that the ECT Act must rather facilitate digital data (evidence) generation and admissibility than inhibit it. To meet these legal requirements, the ONW system uses the captured PDE to easily connect crime perpetrators with their actual crimes, especially within a neighbourhood. Furthermore, the stored PDE can be employed as potential evidence to reconstruct and understand any crime investigation, thereby determining what actually happened [43]. The PDE from the ONW system can serve both as first respondent account and as incident scene detection. As suggested by Valjarevic and Venter [127] and Omeleze and Venter [128], an incident scene conveys the clue as to what happened and how the alleged crime occurred

[129] [130]. The ONW system provides an adequate start-up point to commence physical crime investigations.

A further benefit of the study in terms of legal requirements and ethics, and the need to employ equity and justice, was proving the validity and originality of any PDE from the ONW system’s repository.

To address this, the ONW system devised a method termed forensic soundness indicators (FSIs) to ensure the originality and correctness of the PDE. The FSIs consist of the information security services, i.e. confidentiality, integrity, availability, authentication, non-repudiation (C IA_t, A_zN) and the PDE metadata, i.e. date, timestamp, geolocation and other mobile device metadata. Subsequently, the FSIs were used to identify the unique elements of all PDE stored in the NWS, thereby ensuring the originality of the PDE. Applying the FSIs to PDE instills confidence in the users (i.e. the uploader and the downloaders), especially since the ONW system demonstrates adequate measures that ensure confidentiality, integrity and transparency of PDE.

9.2.4 *Addressing Privacy and Anonymity Issues*

User privacy has been the topic of a huge debate since the evolution of digital data, both in the information security disciplines and other disciplines. User privacy is also one of the challenges that may impede accomplishment of the full benefits of the ONW system. For users to capture and upload PDE, they need to know that their privacy is protected. The ONW system employed various options to protect the privacy of users, yet complete anonymity could not be guaranteed. The privacy of personal information as prescribed by the PoPI Act, Act 4 of 2013 [18] [19] was dealt with at the design and development of the ONW system. For example, in using personal devices to capture incidents of criminal activity as they occur, personal information such as the location where the incident was captured, the user‘s device type and/or the cellular network tower triangulation may be divulged. However, the ONW system ensures that such user‘s information is encrypted at PDE upload.

This research not only makes provision for citizens to capture and store PDE, but also provides anonymity of the PDE uploader, while at the same time retaining the necessary metadata that ascertains the PDE originality in order to stand up to scrutiny in a court of law.

9.2.5 *Developing the Proposed Conceptual Idea*

This research began by proposing a conceptual idea to employ crowd-sourcing techniques of PDE generation, especially by crime-ridden communities. The research proposed that the capture-and-share style of social media be imitated, but the conceptual idea went further to develop a working and easy-to-use prototype of this conceptual idea (ONW system). Furthermore, it introduced an easy process for both citizens and law enforcement agents to use the system and presented a real-life case study scenario for its illustrations.

The ONW prototype comprises of the uWatch application and the neighbourhood watch system NWS. The uWatch application is an Android application used by the citizen to capture PDE, while the NW system is used to store, retrieve and maintain PDE, and to make the PDE available and accessible to the authorised users such as the LEAs, digital forensic investigators (DFIs), the judiciary and a System Administrator. Each of these authorised users maintains a level of access as allocated by the System Administrator. Table 9.1 recaps the various users of the ONW system in relation to their roles.

Table 9.1: Summary of ONW System Users

S/No.	**uWatch Application**	**NW System**
1	Citizens	Law Enforcement Agents
2	Crime Witness	Digital Forensic Investigator
3	By-Passer/Onlooker in Neighbourhood	System Administrator
4	Other system components	Other members of judiciary
5	Authorised judiciary member	The Justice system

9.2.6 *Proposing a Digital Forensic Application Requirements Specifications Process*

In presenting the prototype of the ONW system, this research employed well-defined standards and principles of software engineering methods in the design and development of the system. Employing this method led to proposing a requirements specifications process specifically for designing digital forensic applications, termed the digital forensic applications requirements specification (DFARS) process. The DFARS process is an easy way to focus on the aspects of a DF application that require upgrading, and therefore it avoids the need to re-design or re-develop the entire DF application when only one aspect of the DF application requires the applicable change. The DFARS process focuses on identifying the functional requirements, which it then uses to determine the architectural requirements of the ONW system. The DF application‘s architectural requirements in turn include quality requirements which are met using architectural patterns and strategies, with the integration requirements and architectural constraints being addressed in the process. The DFARS process also adds a layer of abstraction at the design of a DF application to accommodate device upgrades. Continuous upgrades in devices, especially mobile devices, are a result of the frequent changes in technology and sometimes in legal requirements, as it concerns electronic evidence [129].

9.2.7 *Providing Potential Digital Evidence Repository*

A final benefit emerging from this research is that it provided a unique PDE repository that is reliable because it employs the requirements as specified by the ECT Act, Act 25 of 2002 [17] to enhance digital evidence admissibility. The PDE stored in the NWS repository provides services such as identifying the prolific crime susceptive zones within a neighbourhood. The NWS repository serve as a first point of reference for law enforcement agents in any neighbourhood crime investigation. The system's repository employs digital forensic requirements like chain-of-custody rules, by providing points of reference where PDE from the ONW system could clearly show its audit trail. This audit trail begins from the point when PDE is captured, through storage, to the point where PDE is downloaded to be used in a crime investigation or as real evidence in a legal proceeding. This ensures that the process of PDE capture, upload and storage maintains a clear chain of custody and chain of evidence. Applying the audit trail process, provides chain of custody for PDE in the ONW system, increases the evidential weight of PDE. Hence, potential evidence from the ONW system that has met forensic soundness requirements to guaranteed chain of evidence.

9.2.8 *Contributions to the Body Knowledge*

This section summaries the scientific contribution of this research (i) Extending forensic soundness of potential digital evidence: The standard process of evidence admissibility only requires the integrity to be ensured as stipulated by the ECT Act, Act 25 of 2002 [17]. Checking the digital evidence integrity traditionally requires a law enforcement agent (LEA) to manually implement hashing on captured data. In the context of this dissertation, this process is termed level ($\mathrm{R_{L0}}$) of forensic soundness. This level of forensic soundness ensures that confidentiality, integrity and non-repudiation are achieved by automated means. This new level of forensic soundness level is termed ($\mathrm{R_{L1}}$). This research went on to provide a means to validate captured and stored PDE by the law enforcement agents which contains the authentication and authorisation process, while adhering to the requirements of evidential weight. This level of forensic soundness is termed ($\mathrm{R_{L2}}$). This research went two-steps further to add automated forensic soundness checks to the PDE captured using the ONW system, therefore maintaining sound evidential weight using the following measures: (i) Hash the captured PDE (ii) Hash the metadata of the captured PDE (iii) Digitally sign the hash value of both metadata and PDE (iv) Encrypt the PDE, plus the hashed and the signed metadata (v) Retain PDE originality using the public key system, symmetric key (K) and certificate authority (CA) (digital certificate) in order to identify that a user is who they claimed to be. (vi) Automated forensic soundness process for all captured PDE.

The uWatch application is an automated process of collecting potential digital evidence (PDE) and implementing the PDE forensic soundness. The uWatch application eliminates the traditional approach of manually adding forensic soundness checking that address evidence integrity. In addition, the chain-of-evidence and chain-of-custody are automated, so as to enhance the verifiability of the processes of the PDE capture and storage. The forensic soundness automated process introduced the concept of forensic soundness indicators (FSIs). The FSIs of confidentiality, integrity, authentication, authorisation and non-repudiation are automatically applied to the captured PDE. The PDE captured using the uWatch application averts the challenges often associated with potential evidence accrued from untrained citizens (like from the social media platform). The automated process of the uWatch application eliminates manual evidence validation and adds two-levels of forensic soundness checking of PDE which this research has termed (R_{L1}) and (R_{L2}). This is because digital evidence is summarily rejected and thrown out of court in a legal proceedings when elements of doubt exist as to the originality of the evidence [104].

(ii) Another scientific contribution of this research is employing technicals of software engineering specifications to present a DF application design process, that adds a layer to clearly define the processes employed when designing or developing a DF application to a non-technical audience involved in crime investigations. This is because, the field of digital forensics inherently is a multi- discipline environment where the legal community, judiciary, the government and the accused or defendant are brought together in an attempt to identify what happened in a crime investigation or prosecution. This research therefore proposed the digital forensics application requirements specification (DFARS) process. Valjarevic et al., [14] introduced the concurrent processes for digital forensic investigation as actions which should be conducted in parallel with other processes within the digital forensic investigation process. The concurrent processes aimed to enable efficient and effective digital forensic investigations, while reducing the risk of human error and omissions which result in digital evidence being contaminated. In line with Valjarevic et al. [14], the DFARS process introduced a DF application design process that is user-centric, thereby highlighting the processes employed to designing and developing a DF application to an end-user or other concerned personnel in digital forensic investigation. The behind the scene actions of developing a digital forensic application can be likened to the concurrent processes of the digital forensic investigations, which are something deemed irrelevant to the non-technical audience, but end up creating a level of obscurity to the audience of a crime investigation. The provision of the DFARS process, that shows clear guidelines for presenting how these tools were developed to a non-technical audience, is one means to ease the tension often associated with the use of digital evidence in a court of law.

Furthermore, using the DFARS process with the ONW system as a case scenario, the DFARS process presented an easy application of modifiability, pluggability and reliability features at any point in the life-cycle of a DF application. This thereby accommodates the constant upgrades and changes associated with electronic devices, operating systems, hardware and other requirements. It further shows an easy-to-follow process that is understandable to both technical and non-technical audiences in the field of digital forensics

This section highlighted the many benefits of the ONW system that have accrued from this research. However, there are some shortcomings that are yet to be overcome. These are presented next.

9.3 *Shortcomings*

Ultimately, the bid to minimise crime in crime-riddled communities is not without its difficulties. For example, this research assumes that users (citizens) have mobile devices popularly regarded as ‘smart phones’, that are equipped with basic camera and audio functions. The assumption is that by using these basic functions of a mobile device, citizens could capture digital data images such as audios, videos and photos. However, not all users have mobile devices with these functions. Another drawback is that the uWatch application is an Android-device-focused application, which obviously impedes the participation of citizens without Android devices. There is also the concern that some users may not yet have mastered the efficient use of their smart phones, and are therefore excluded from participating in the PDE-sourcing process. Other limitations of the research are outlined below.

9.3.1 *Privacy Issues*

Personal privacy is an important concern for most users and fears of compromising it may well inhibit many users from participating in the PDE-sourcing process. Since the technical details of how a user’s privacy is protected are not easily presented to the users at the forefront, this may reduce their willingness to participate. In an attempt to protect users’ privacy, this research used information security techniques and technologies, both at the front-end and back-end of the system. However, as conceded in the Privacy of Personal Information (PoPI) Act, Act 4 of 2013 [19], there are exclusions and exemptions to an individual’s privacy rights when the interest of the nation is at stake, or when the prevention, detection and prosecution of criminal offences are involved.

9.3.2 *Evidential Weight and Rule of Evidence*

The ECT Act, Act 25 of 2002 [17], defines the conditions that are necessary for electronic data to have evidential weight. The evidential weight of any digital evidence is determined solely by the presiding Judge, when the case is under adjudication in a court of law. Due to these requirements of the ECT Act and the legal systems of countries like South Africa, some PDE captured and uploaded to the ONW system’s repository may be deemed unusable for a crime investigation or as ‘real evidence’ in a court of law. For example, in the scenario presented, the PDE captured during the hit-and-run accident at Midrand may be discarded as invalid evidence by a presiding Judge, due to certain legal technicalities around the PDE-capturing process. Evidential weight therefore can be a deterrent to the effective use of PDE from the ONW system.

9.3.3 *Reliance on Human Intuition*

An important limitation of the current research is the ONW system‘s reliance on human intuition. For example, human intuition has to be relied on to determine what a potential crime is and when a potential crime is in progress. Nevertheless human intuition has to be relied on to determine various situations. For example, Gedanken experiments found that human senses/thoughts tend to play a great role in determining the current state of the environment [131] [132]. In other words, the observation of the behaviour of a subject triggers responses to stimuli. These responses to environmental stimuli could be the determining factor that drives the citizen to the decision as to what constitutes a potential crime or potential evidence. Furthermore, human intuition is necessary when the LEA and Judiciary have to employ PDE. They have to use their intuition on when to apply the full extent of the law, Constitution and legislation in deciding what an actual crime or potential evidence is, or when an actual crime has been committed in any given circumstance. However, throughout this research, there is little to no emphasis on human factors, such as the psychological state of the citizen who captures and uploads PDE of crime.

9.3.4 *Self-Protection*

Another aspect of the ONW system where human intuition is relied on is users' sense of self-protection. For this reason, the ONW system was designed and developed to ensure user's protection during PDE capturing in a crime environment. The fact that the uWatch application is equipped with the 'capture-now-upload-later' function, specifically to enable citizens to capture PDE and upload later when they are at a safe distance from the crime scene. Determining the level of safety risk while capturing PDE is also a decision that is left to human intuition. This research assumes that citizens would capture PDE at a safe distance from a suspected crime scene to avoid self-endangerment, but this may not always be possible. For example, in the excitement of witnessing a crime, citizens may inadvertently place themselves in danger, which would be a major drawback for the ONW system.

9.4 *Conclusion*

In conclusion to this chapter and to highlight the benefits of systems like the ONW system, it is worth citing an incident that occurred in Cork, Ireland, on 3 June 2016 when a concerned citizen captured a video image of a two-week-old baby left in a hot car, while her parents were shopping [133]. The citizen posted the captured video to social media, which gave rise to an outcry by both the Irish media and the general public and this led the Police in Cork to launch an investigation into the incident. The captured and stored video is PDE of a potential crime, and acted as a first point of reference for the law enforcement agent's investigation. This incident encapsulates some of the main issues raised and addressed by this research. The citizen's action of capturing the video image of the potential crime using her mobile device, shows the willingness of concerned citizens to get involved, in order to discourage dangerous and anti-social behaviour that could be harmful to individuals or groups in a community. The incident also demonstrates how at ease and accustomed people are and have become to uploading data to various repositories or platforms.

It is hoped that the ONW system can be extended to other countries and ultimately become a global crime-fighting tool. There is clearly a need for the proactive involvement of community members in an active drive to eradicate crime through the use of PDE crowd-sourcing, community policing and other forms of crime fighting. The successful implementation and application of the ONW system should not only reduce crime systematically, but also foster better cooperation in matters of neighbourhood crime between the ordinary individuals on the street and the law enforcement authorities.

This chapter outlined the benefits and shortcomings of this research. The next chapter presents some related literature to shed further light on the contributions made by this study.

Chapter 10

RELATED LITERATURE

10.1 *Introduction*

Digital data evidence is becoming one of the most essential types of information used in criminal or civil investigations [134]. This is because information generated in the form of digital photos, records, transaction logs, and research material can now be used in crime investigations or as real evidence in legal proceedings[11]. Generating potential digital evidence (PDE) of a crime in the form of photo, video or audio data is the focus of this research, which was motivated by the rise in neighbourhood crime.

This chapter presents related literature focusing on different areas of digital forensics that have had an impact on this research. The literature is categorised in groups and each category is reviewed in Sections as follows:

- **Section 10.2 - Literature focused on digital evidence integrity & admissibility**
- **Section 10.2.2 - Literature related to digital repositories**
- **Section 10.2.3 - Legal specifications**
- **Section 10.2.4 Literature related to requirements specifications.**

10.2 *Evaluation of Related Work*

The aim of this research is to generate PDE of neighbourhood crime that is admissible in a court. Therefore, this review starts with a focus on literature related to digital evidence integrity.

10.2.1 *Digital Evidence Integrity*

This review starts by referring to the work of Saleem [55], who was focused on digital forensic processes and preserving the integrity of digital evidence, along with protecting basic human rights, as umbrella principles. Saleem [55] surveyed digital forensic models and frameworks to determine the inclusion of human rights in digital forensic frameworks and models, and proposed in his research the 2PasU model. The 2PasU model was developed with four core processes of collection, examination, analysis and reporting, and with three sub-processes of preparation and planning, presentation, archiving, and returning. It also included two sub-processes for overarching principles of the preservation of digital evidence and protection of human rights. While the 2PasU model puts special emphasis on protecting the human rights of the individual being investigated, it is not as thorough as the ISO/IEC 27043 Digital Forensic Process model [135], which was used as a guideline in the design of the ONW system. Saleem claims that digital evidence can be modified without detection, and also asserts from the survey of the literature that cryptographic hashing of digital data is not tamper proof. In view of these assertions, it is worth pointing out that the ONW system does not depend on cryptograph hashing alone for the integrity protection of its PDE data. The ONW system uses encryption, cryptographic hash, digital signature and access control, as well as time/ date stamp, location and other metadata of the captured PDE to ascertain the integrity of the PDE [13] [124] [15] [136].

Casey [29] lists a number of properties that digital evidence must retain in order to be admissible in any legal proceedings. These are authenticity, completeness, reliability, and believability, as well as that digital evidence must be tied to an incident in order to prove that the incident occurred and that the evidence is related to the incident in a relevant way. The research in hand satisfies these properties specified by Casey [29] by implementing timestamp, geolocation and secure hash algorithm (SHA-2) of all captured digital evidence.

McKemmish [33] claims that the term forensically sound, as been used widely in the field of digital forensics, leads to confusion. His research therefore seeks to define the term 'forensic soundness', examining broad range of definitions of digital forensics. According to McKemmish [33] digital forensics has many elements, which can be deduced from the variety of definitions produced by the different digital forensics practitioners. Yet all the definitions share a common element - the need to maintain evidentiary weight. McKemmish [33] concludes that when evidentiary weight is maximised, the digital forensics community agrees that the evidence is forensically sound. This led him to pose two key questions: What does forensically sound mean and how does one know if data is forensically sound? McKemmish [33] arrives at a definition for forensic soundness, which involves applying a transparent digital forensic process that preserves the original meaning of data. The two crucial aspects to this definition are that a forensic process must be verifiable and acceptable, and the technology employed must be reliable and accurate. McKemmish concludes his paper by proposing four criteria for ascertaining the forensic soundness of a digital forensic process. Forensic soundness is at the core of the ONW system, where the forensic soundness indicators (FSsI) are used as a means to verify PDE reliability and integrity. Furthermore, evidentiary weight of PDE from the ONW system is strengthened by the strict access control policies implemented.

Ani et al.,[137] conducted research on the conceptual framework for preserving digital evidence integrity in a virtual environment and used VMware hypervisor as a case study. They enumerated appropriate algorithms for the implementation of digital evidence integrity to include secured hash algorithm (SHAx), digital signature, encryption and message digest algorithm (MD5). They also analysed the threats to the integrity of digital evidence and used the VMware hypervisors to strengthen the hash function and incorporate reliability rating factors, as a means of conceptualising integrity levels of digital data. Still on digital data integrity, Richter et al., [138] claimed that using digital signatures and non-repudiation is not enough to ensure digital evidence integrity. They presented an embedded system that is able to collect admissible digital evidence through an automated process focusing on the non-repudiation of the digital evidence data by designing a secure environment and adding all relevant parameters to the measured data such as the location, identity of the device, timestamp, and the current status of the system. The ONW system adopted the integrity measures proposed by Ani et al.,[137] and Richter et al., [138] however, this dissertation went a step further to add forensic soundness indicators to not only increase the integrity of PDE, but also to enhance the admissibility of PDE captured by means of the ONW system.

Grobler et al., [40] proposed a framework to guide the implementation of proactive digital forensics in organisations. They gave a detailed description of digital evidence gathering over networks for investigation of incidents and how to preserve the integrity of stored data. They also proposed a strategy to be employed when conducting investigations based on the evidence gathered over networks and suggested an integrated view of digital forensics consisting of three components, namely pro-active, active and reactive digital forensics. Their pro-active digital forensics process dealt with the acquisition of digital evidence over networks by means of an intrusion detection system. This detection system activates the incident response protocol and integrates the protocol with a live forensic investigation protocol, thereby capturing digital evidence and applying integrity measures in a re-active as well as an active digital forensic process. Although Grobler et al., [40] proposed a digital evidence-gathering process over networks for preserving data integrity, they did not include the use of mobile devices to acquire PDE, store the PDE in a forensically sound manner, and maintain the PDE integrity. Furthermore, making the PDE stored in the ONW system‘s repository available to authorised users, and maintaining access management to the stored PDE were not included in their research either. Even though the ONW system is similar to this framework of Grobler and others, the live feeds captured in the ONW system are from physical crime scenes.

In 2006, Turner [104] proposed a Digital Evidence Bag, an approach towards the acquisition and processing of digital evidence obtained from disparate sources. Turner’s main concern was to acquire and store digital evidence in a forensically sound manner. According to his research this was achieved using hash functions. For the ONW system, PDE integrity is ensured using the information security services for maintaining confidentiality, integrity, authentication, authorisation and non-repudiation (CIA_tA_z N), by employing mechanisms such as cryptographic hash function, session authentication and digital signature, in conjunction with the forensic soundness properties of timestamp, geographical location tag, device tag, IMEI identifier and WiFi or GSM network identifier. Turner's use of a digital evidence bag to store digital evidence acquired from disparate sources made no mention of whether or how his work contributes to the reduction of neighbourhood crime or improvement of community security. The ONW system therefore offers a new concept in the use of photos, audios, or videos captured by means of mobile devices to reduce preventable crime in crime-riddled communities.

Mylonas et al.,[139] proposed the Themis system for the acquisition of sensor data from criminals' smartphones. Themis was developed to find more evidence of criminal activity. Their focus was on three types of sensors, namely location sensors (GPS), motion sensors (accelerometer, gyroscope) and environmental sensors (magnetometer which measures proximity, light, temperature, pressure). Mylonas et al.,[139] geared their research towards the proactive area of digital forensics that can provide context awareness and aid the prevention of a crime. The removal of data is done remotely and on an ad hoc basis because sensor data is time-sensitive and volatile and most sensor data is not retrievable for 'post mortem' forensics. Mylonas et al.,[139] drew in this paper heavily from their previous paper, where they claimed that sensor data is a source of data for forensic investigation and can lawfully be used to deduce a criminal's context. The most specific claim of their paper is that sensor data can aid the rejection or acceptance of an alibi in a forensic investigation. The paper stressed that such sensor tracking can only be used for "serious crime like pedophilia and for issues that affect national security", and identified its main users as the 'Law Enforcement Entity'.

Mylonas et al.,[139] covered some of the terrain of the research in hand, because both studies deal with acquiring evidence of crime from a mobile device. The legal implications, especially around the privacy rights of the smartphone users, are a challenge that is also similar to both. Acquiring data that can be used as PDE, maintaining its forensic soundness and transferring it to a location for analysis are common elements in both the Themis and the ONW system. However, the Themis system transfers data to a live workstation via a secure wireless channel, in contrast to the storing of PDE data in the ONW repository. Mylonas et al.,[139] assume the integrity of law enforcement agents who handle this very sensitive data, in contrast to the current research that dedicates an entire chapter to access management of the PDE stored in the ONW system.

10.2.2 *Literature Related to Digital Repositories*

The State University's Centre for Telecommunications and Network Security and the Defense Cyber Crimes Centre developed a Digital Forensic Knowledge Repository [80]. The system provides a means for efficient investigation and information sharing among foreign intelligence agencies, the criminal intelligence agency and cyber intelligence agencies in order to enhance the quality of evidence data for cross-referencing cases under investigation in the effort to eradicate cyber crime. The research focused on cyber warfare and effective collaboration between the various investigation and prevention of online crime. The research has made a worthwhile contribution to the aspects of evidence storage and sharing. One of the major differences between the system as presented by Weiser et al.,[80] and the ONW system is that the ONW system focuses on capturing potential evidence of a physical crime, while allowing community members and law enforcement agents to be involved in the crime eradication process. Community members use their mobile devices in the fight against physical crime around their neighbourhoods, while the enforcement agents use PDE stored in the ONW system's repository as additional evidential material in a physical crime.

In another research study, Hedstrom [140] explores the concept of digital libraries with regard to preserving digital material due to technology change. According to her research, technology changes in cycles of three to five years, therefore artefacts used in the preservation of digital data may soon be out of date. The technique becomes outdated due to obsolete preservation methods and exposes digital material to falling prey to attacks due to technological obsolescence. The ONW system took cognisance of the research of Hedstrom [140] when it implemented a component-based design for the uWatch application and the NW system. The component based design of the ONW system caters for technology change, so that if any component becomes obsolete, that component can be re-developed without necessarily affecting the entire state of the ONW system. The ONW system has been developed as a flexible component-based system that uses layered, microkernel and pipes-and-filters architectural patterns to enable pluggability, upgrading or changing of one aspect of the system without affecting the entire system's functionality.

Zuccala et al.,[141] conducted an exploratory examination of digital repositories and in particular examined the role of repository managers. They argued that a repository must be sustainable, trusted, well supported and well managed. As far as the ONW system‘s repository is concerned, this is true, as it is not an open repository and can be accessed only by authorised users and according to strictly role-based criteria. The management of the ONW system repository uses the attributes of the PDE and the role of the authorised user to determine access. The use of access policies furthermore ensures that even a role holder who does not meet the necessary attribute requirements of a PDE is refused access. For the sake of the ONW system‘s security, encryptions are employed to keep anonymous the details of citizens who captured PDE. Zuccala et al.,[141] also advocate training for digital repository managers, which is hardly necessary for the ONW system, since the system is user friendly and designed for use by persons who have no technical training. Moreover, the authorised users of the ONW system are law enforcement agents who mostly have years of experience in dealing with crime and interpreting crime scenes, as in the case with PDE stored in the ONW system's repository.

Schatz et al.,[142] focused on an alternative architecture to design a repository for digital evidence and termed the alternative repository “Digital Evidence Bags”. These Digital Evidence

Bags are designed for a common storage format for digital evidence in order to enhance inter-organisational digital evidence sharing. Their research also focused on promoting interoperability between forensic analysis tools, using semantic web technology and applying a globally unique identification scheme as a representational approach to the integration of digital evidence metadata [142]. Whereas Schatz et al.,[142] did not clearly specify the details of the processes or means of getting the digital evidence to the “Digital Evidence Bags", the research in hand explicitly elaborated a detailed process of capturing potential digital evidence [13]. The process showed clearly how PDE is preserved and how access to the stored PDE is controlled [15].

Cohen et al.,[35] presented the Advanced Forensic Format (AFF), which is a new specification and toolset. They redesigned the architecture of the AFF to make it the basis for a globally distributed evidence management system. The new architecture is capable of storing multiple heterogeneous data types that could arise in modern digital investigations, including data from multiple storage devices, new data types and extracted logical evidence. The ONW system, on the other hand, is designed using the DFARS process, which incorporates software engineering methods to address the need for DF applications to be easily interpreted by any non-technical user, as well as to easily accommodate the upgrade of devices susceptible to DF investigation.

10.2.3 *Legal Specifications*

According to Hamidovic [84], the bulk of legislation governing electronic evidence around the world is based on laws enacted by the United Nations Commission on International Trade. The Model Law, which governs Electronic Commerce and Electronic signatures, constitutes the basis for many countries’ laws for governing the storage and use of electronic data as evidence in a court of law. The Model Law assesses evidential weight according to the manner in which electronic documents are generated and stored, and how the integrity of digital data evidence is maintained. At the design and development of the ONW system, the processes employed to ensure forensic soundness (integrity) are analysed using mathematical illustrations, thereby adhering to the legislative standard of the Model Law.

Watney [126] and Papadopoulos et al., [11] listed the Common Law requirements for digital evidence admissibility as follows: production, in other words the digital evidence must be relevant; presentation, in other words the digital evidence must be in its original form; and authenticity, in other words the digital evidence must be provable. Papadopoulos et al.,[11] also listed the requirements of a South African court in the application and assessment of evidential weight as the reliability of the manner in which the digital evidence was generated, stored or communicated, the manner in which the integrity of the said has been maintained, and the originality of the evidence.

10.2.4 *Literature related to Requirements Specifications*

Garfinkel et al.,[143] are concerned with the state of digital forensics and argued that digital forensic practitioners need tools that search and prevent, but also tools for reconstruction, analysis, clustering, and data mining. Furthermore, the Authors noted that the tools must be tested in order to generate accurate results, which are surprisingly low in digital forensics. The research highlighted the need for reproducible techniques and results, as well as for employing a standardized scientific process in designing a digital forensic application, especially since digital forensics is a science. Worthy of note is that the research by Garfinkel et al.,[143] provided the motivation for the proposal of the digital forensic application requirements specifications (DFARS) process. The DFARS process is a partial response to the argument raised by Garfinkel et al.,[143], namely that there is a need to develop statistical and other approximation techniques to ensure that the interpretation of digital evidence is grounded in facts and science and not simply upon opinion.

Valjarevic et al.,[14], introduced the concurrent processes for digital forensic investigation process model as actions which should be conducted in parallel with other processes within the digital forensic investigation process. The concurrent processes aimed to enable efficient and effective digital forensic investigations while reducing the risk of human error and omissions which result in digital evidence being contaminated. In line with Valjarevic et al., [14], the DFARS process introduces a DF application design process that is user-centric, thereby highlighting the processes employed to design and develop a DF application to an end-user or other digital forensic stakeholders, in the digital forensic investigation. The background actions of developing a digital forensic application can be likened to the concurrent processes of the digital forensic investigations, which are something deemed irrelevant to the non-technical stakeholders, but end up creating a level of obscurity to the stakeholders of a crime investigation. The provision of DFARS process which shows a clear guideline on how these DF tools were developed (to a non-technical stakeholders) is one means to ease the ambiguity often associated with the use of digital evidence in a court of law.

In another study, Herlea et al., [144] dealt with the integration of behavioural requirements specifications within compositional knowledge engineering. They defined requirement engineering as addressing the development and validation of methods for eliciting, representing, analysing and confirming system requirements. Their research argues that requirements engineering is a consultative process that must take place over time and involve all stakeholders. This process should combine the discussion of requirements and scenarios that are continually honed over time to arrive at a system description that satisfies all the stakeholders.

Herlea et al., [144] emphasised the involvement of users, who are considered the experts at the critical early stage of software development. However, not only the users are important participants in the consultation, but all stakeholders, who include domain experts, system customers, managers, and developers. The contributions of Herlea and others to the requirements engineering literature are significant for the fact that they highlight the need to involve the users in a consultative process. This dissertation took cognisance of this need in creating the DFARS process that was used to design the uWatch application and the NW system, the components of the ONW system. For example, in determining the functional requirements, the DFARS process takes into account the needs of the uWatch application users, the stakeholders and the application itself. However, the ONW system went beyond what Herlea et al., [144] suggested in spelling out how requirements specification are to be implemented.

Grispos el at., [145] argued that in an event of data breach, the majority of organisations commence investigations to ascertain what happened and how it happened. However, the required data to conclude the forensic investigation may be lost due to a variety of reasons ranging from physical access, short data retention times and the costs associated with conducting such investigations. The authors called for the need to maximise potential use of evidence and minimise the costs of an investigation by ensuring that systems and infrastructure are forensic-ready in design and development. The research went further to use a survey to identify the various requirements of user groups of digital forensics in an organisation in order to identify their main 'individual' needs of digital forensics for their various organisations. The research findings show also that organisations consider requirements for forensics during various stages in the development process especially at post-delivery. The research of Grispos el at.,[145] is in-line with the DFARS process focusing on integrating the forensic readiness in DF application designs at the beginning of a DF tool design, thereby addressing the needs of potential evidence that may arise at the time of an DF incident investigation. The DFARS process further aligned its focus on the DF application at the architectural level in order to carry-along the various stakeholders in the DF investigation. The DFARS process presents a process that supports the use of a forensically ready design, as well as make the design process comprehensible to non-technical stakeholders in digital forensics. The DFARS process proposes a add-ons of requirements specifications that address the issues that are inherent in organisations that are not are forensically-ready, and went further to bring in the human-centric aspects of DF application design phases.

In yet another research, Reith et al.,[146] presented a model to address the shortcomings of digital forensic models focusing on tools for evidence collection. In their solution, a provision of a consistent framework for digital forensic tool development and mechanisms for applying the framework to future technologies, was proposed. The paper argued that there is no standard or consistent digital forensic methodology but rather, procedures and tools built from the experiences of law enforcement agents, system administrators, and hackers. It advocates the use of ad hoc tools and techniques, from the scientific community. In this paper however, the technology referred to was analog based like videotapes and audio recordings, and paper documents. On the other hand, the DFARS process being digital focused, considered the various users and their needs to ensure that a DF applications used in DF investigations are easily presentable to all stakeholders when such need arises. The DFARS process attempts to absorb the needs of both technical and non technical observers of digital forensics

Literature on requirements engineering specifications, focusing on digital forensic application design, is at a minimum at the time of this work. However, the author acknowledges the contributions of Grispos el at., [145], Ab at el.,[147] in eliciting the requirements specifications for DF application. The author focused on the importance of requirements engineering in digital forensics (as presented by Garfinkel et al.,[143] and Herlea et al., [144]), she identified the need for a comprehensive design of the ONW system‘s requirements specifications. Garfinkel and colleagues called for definitive standards for designing DF software applications, while Herlea et al.,[144] highlighted the need for a consultative approach in the process of designing DF applications. Both these requisites were adhered to in the design and development of the ONW system. The DFARS process not only provided a definitive process as an approach to designing DF software tools or applications, but it also presented a case study of the DFARS process being employed in the design of the ONW system.

Having presented some selected literature, the next section summarises the literature and identifies the contribution of this research in comparison to the related literature presented here.

10.3 *Summary of the Related Work*

To clearly indicate the contributions of this research, the summary in Table 10.1 shows authors and keywords representing their various contributions in relation to this research, where each checkmark (✓) represents a contribution of the author’s research.

Table 10.1: Summary of Related Literature (where "✓" indicates authors' area of contributions and "X" indicates aspects not addressed by authors discussed

Authors and Keywords	Forensic Soundness	Encryption	Integrity	Repository	Digital Evidence	Mobile Device	Legal Requirements	RequirementsSpec	Access Ctrl
Saleem [55]	X	X	✓	X	✓	X	X	X	X
Hedstrom [140]	X	X	X	X	✓	X	X	X	X
Hamidovic [84]	X	X	X	X	X	✓	X	X	X
Papadopoulos [11]	X	X	X	X	X	X	✓	X	X
Mylonas et al., [139]	X	X	X	X	X	X	✓	X	X
McKemmish [33]	✓	X	X	X	✓	X	X	X	X
Herlea et al.,[144]	X	X	X	X	X	X	X	✓	X
Watney [126]	X	X	✓	X	X	X	✓	X	X
Weiser et al.,[80]	X	X	X	✓	X	X	X	X	X
Garfinkel [143]	X	X	✓	X	X	X	X	✓	X
Turner [104]	X	✓	✓	X	X	X	X	X	X
Grobler et al., [40]	X	X	X	X	✓	X	X	X	X
Richter et al., [138]	X	✓	X	X	✓	X	X	X	X
Reith et al., [146]	X	X	X	X	✓	X	X	✓	X
Ani et al.,[137]	X	✓	✓	X	X	X	X	X	X
Casey [29]	X	X	X	X	✓	X	X	X	X
Cohen et al.,[35]	X	X	X	X	✓	X	X	X	X
Schatz et al.,[142]	X	X	X	✓	✓	X	X	X	X
Zuccala et al.,[141]	X	✓	X	✓	X	X	X	X	X
Valjarevic et al., [14]	X	X	X	X	✓	X	✓	X	X
Grispos el at., [145]	X	X	✓	X	✓	X	X	✓	X
This Research	✓	✓	✓	✓	✓	✓	✓	✓	✓

10.4 *Conclusion*

To complete this chapter, the researcher examined some work of authors who have conducted research in the area of digital evidence integrity and admissibility, as well as requirements engineering. From the quoted related literature reviews, it can be seen that a lot of work has been carried out to ensure that digital evidence is reliable, authentic and can stand up to scrutiny in a court of law. The ONW system takes into account the requirements posed by these authors, since generating evidence that is admissible is essential to the success of the ONW system. Furthermore, it is also clear from the literature that there does not yet exist a comprehensive model that enables citizens to use their mobile devices to gather potential evidence that can be used in crime investigations or as “real evidence” in a court of law. This research therefore focused on closing this gap. The ONW system’s process of generating and storing evidence, not only takes account of this literature, but also aims to satisfy all the requirements of the South African legal system under whose jurisdiction the system is to be implemented.

The next chapter, which concludes this research, takes a broader look at the problem statement, how well the problems were addressed and suggested future work.

Chapter 11

Conclusion

11.1 *Introduction*

This research capitalises on the wide availability of mobile devices, the social media era of capture and upload, and the willingness of citizens to contribute to the physical safety of their communities by means of neighbourhood policing. Chapter 11 gives a re-cap of this dissertation and summarises the contributions as presented in each chapter. The remainder of this chapter is structured as follows:

- **Section 11.2 gives a brief summary of all chapters of this research.**
- **Section 11.3 recaps the problem statement.**
- **Section 11.4 points to future work.**
- **Section 11.5 presents a table showing the unique contributions of this research**
- **Section 11.6 brings this research to its final conclusion.**

11.2 *Disseration Summary*

This section gives a condensed chapter-by-chapter description of the research. It is provided for the convenience of the reader and aims to improve the readability of this dissertation where each chapter is revisited in a brief summary.

(i) Chapter 1 introduced this research focusing on the problem statements. The chapter continued by outlining the objectives and the methodology to be used to address the identified research problems.

(ii) Chapter 2 focused on background literature of digital forensics and information security requirements, and gave an overview of terminologies used in digital forensics and information security used throughout this dissertation.

(iii) Chapter 3 provided the background of legal requirements as pertains to the use of electronic or digital data.

(iv) Chapter 4 introduced background literature on software requirements engineering.

(v) Chapter 5 introduced the ONW model and focused on modelling the system using a diagrammatic representation. Chapter 5 however, concentrated on modelling Part A of the system, in other words the process employed by users to capture and upload PDE. The chapter further gave a mathematical illustration of the forensic soundness of the captured PDE.

(vi) Chapter 6 is an extension of the ONW model presented in chapter 5. Chapter 6 presented Part B of the ONW model, that is the downloading process and the use of the downloaded PDE. Chapter 6 also presented a case scenario in which PDE captured and stored was employed in a neighbourhood crime investigation.

(vii) Chapter 7 designed the ONW system using software requirements engineering specifications. It went a step further to propose an easy-to-use process for designing digital forensic applications (DFARS). Later in the chapter, the proposed DFARS process was applied to design the ONW system.

(viii) Chapter 8 presented the prototype of the ONW system, where Parts A and B of the ONW system, as discussed in Chapters 5 and 6 were developed as a mobile device application termed uWatch and a web-application termed Neighbourhood Watch System (NWS) respectively.

(ix) Chapter 9 concentrated on evaluating this research and focused on its benefits and shortcomings.

(x) Chapter 10 reviewed related literature, and examined the contributions of such authors compared to the contributions of this dissertation.

(xi) Finally, chapter 11 summarises and concludes this research, and points to future work.

The next section revisits the problem statement and shows to what extent the problems were addressed.

11.3 *Recap of the Problem Statement*

The current research set out to address the problem of lack of sufficient evidence to connect neighbourhood crimes to the actual perpetrators. The insufficiency of evidence sometimes makes it impossible to corroborate the evidence found in a crime scene and successfully prosecute the offender. The extent to which each of the sub-problems were addressed is explained as follows:

(i) One of the research sub-problems is that there is no easy way to acquire potential digital evidence (PDE) of neighbourhood crime that can be used as admissible digital evidence in a court of law. This research therefore addressed this problem by designing and developing the uWatch application to enable the capturing of PDE of crime, as the crime unfolds.

(ii) The lack of a viable, secure and reliable repository dedicated to storing and managing PDE is a second sub-problem identified in this research. The problem was addressed by developing a repository for the ONW system and by maintaining the forensic soundness of captured and stored PDE using that information security services mechanisms. Forensic soundness indicators (FSIs) were introduced to enhance the originality and validity of the captured and stored PDE, as well as to address the legal requirements concerning electronic data, as required by the ECT Act, Act 25 of 2002 [17].

(iii) A third sub-problem addressed by this research is the concern of citizens to remain completely anonymous in the PDE-capturing and uploading process. The design and development of the ONW system requires that a citizen‘s personal information acquired at user registration be encrypted. In the unlikely event that the details of an uploader are required to ascertain the validity of PDE, a legal process such as obtaining a warrant, an authentication and authorisation process from the NWS side is also required. This is because, the user signed and encrypted the information of users using $\mathrm{N_{priv}}$ and $\mathrm{N_{pub}}$ respectively. Therefore only the NWS can decrypt any information encrypted by the uWatch application.

Furthermore, a citizen who uploaded PDE could choose to invoke the non-compliance law, which allows a witness the choice to testify or not in a court of law in respect of a crime they witnessed. Nonetheless, other metadata information that ensures the evidential weight of PDE, such as the location where the evidence was captured, as well as date and time stamps will clearly show the PDE chain of custody, when required by the LEAs or other authorised users to ascertain the validity of PDE.

11.4 *Future Work*

The implementation of the ONW system is hoped to give the fight against crime in South Africa a significant boost. However, during the investigation of the problems posed by this research, some new research areas falling outside the scope of the current research were triggered, and these can be considered for future work:

(i) To extend the uWatch application to accommodate the operating systems of other mobile devices.

(ii) To convert the NWS to a software-as-service cloud-based system for elasticity in order to accommodate anticipated growth, due to an increase in citizen participation.

(iii) To design and develop the uWatch application to include a component that self-detects when a crime is occurring. For example, in the situation where a citizen’s heart-rate or other human metric accelerates, the uWatch application should be able to trigger the

camera to commence video or audio recording. The recorded PDE can subsequently be uploaded if the citizen deems the recording to be valid potential evidence. The research in hand also acknowledges the limitations that such metrics may pose, but these are left for future work and more research.

(iv) To design and develop an algorithm for the ONW repository to identify what constitutes a potential crime image, a process system that could differentiate between valid PDE and non-valid PDE would greatly enhance the ONW system. For example, blank images, unclear videos or incomprehensible audio recordings could be considered invalid PDE.

(v) The current vetting mechanism adopted in this study is limited to the uWatch application. This does not ensure the vetting of the behavior of the citizen, as to what constitutes appropriate citizen behavior. Future works will consider the development of a reliable vetting mechanism, through which more reliable potential digital evidence capturing can be ensured.

(vi) As at the time of the conceptualization of the study, incident-category mapping was not considered within the scope of the study. However, this will be considered as part of the future studies. Incidents will be categorised based on scientific approaches in areas such as good practices for incident management, incident and risk categorization, as well as a method of categorising digital incidents for effective classification. Methods to be considered could include the Kepner and Tregoe analysis for incident mapping [148].

11.5 *Summary of Research Benefits and Shortcomings*

It is worthwhile to state that the PDE captured during a crime-in-progress can prove that a crime did indeed occur, as well as show who the actual crime perpetrators were. Table 11.5 summarises the benefits and limitations of the current research.

11.6 *Final Conclusion*

Although the ONW system was developed to aid the fight against neighbourhood crime in South Africa, it can be applied in other parts of the world with similar legal requirements. The ONW system demonstrates a means to acquire PDE and at the same time maintain the forensic soundness of the acquired PDE. The forensic soundness of a photo image or video recording is upheld by the use of digital signature, cryptographic hash function, encryption, date/time stamp and metadata obtained from the device. These forensic soundness indicators, coupled with access control measures, ensure adequate protection of the integrity, confidentiality and non-repudiation of the acquired and stored PDE. The result is that the PDE acquired through the ONW system can be legitimately used as admissible evidence to investigate and prosecute perpetrators of neighbourhood crime.

Table 11.1: Summary of Benefits and Shortcomings

S/N	Benefits	Shortcomings/Limitations
1	Developed the uWatch application and NWS	The uWatch application is limited to Android devices only and NWS web based
2	The source PDE process is automated, therefor eliminating tampering that may be associated with untrained users. The generated PDE may be useful in crime investigations	Reliance on human intuition
3	An easy-to-use application for all audience users. User friendly and intuitive application	User must launch the uWatch App to commence PDE capture
4	Community members and law enforcement agents work together to eradicate neighbourhood crime.	The legal system requires only the presiding Judge to determine PDE's usefulness to a case, to the privacy of citizens may sometimes not be complete anonymous to obtain credibility and relevance of the PDE.
5	Implementation of the ONW system in line with legal and ethical standards. In addition, using automated process in a mobile application to address chain-of-evidence and chain-of-custody, so as to enhance the verifiability of the processes of the PDE capture and storage.	-
6	The design and prototype of a crime storage repository in form of audio, video or photo is a boost to enhance crime investigations	-
7	Proposed the user-centric DFARS process following the software engineering techniques that is specific to the design of DF applications.	-
8	Designed and Developed a forensically sound PDE storage repository (the ONW system's repository)	-

The ONW system was designed using the DFARS process in order to provide an easy and detailed understanding of how a DF application used for crime investigation or prevention is created. The DFARS process, with its easy-to-comprehend steps, was created by this research to design Digital Forensic applications. Therefore the ONW system can be utilised by law enforcement personnel to demonstrate to non-technical audiences how the authenticity of PDE captured by means of the ONW system can be ensured. A notable strength of the DFARS process is that it is a scalable and extensible process that allows for future device upgrades, and so the ONW system or any DF application can easily be developed further as technology advances or crime patterns change. In this sense, this research serves more as a foundation than as a work with a final conclusion.

In this era of networking and interdisciplinary co-operation, the ONW system provides a means for communities to be pro active in assisting law enforcement agencies to reduce crime in their neighbourhoods. In the past, police visibility on the street was seen as a deterrent to criminals. In future, however, when uWatch and the ONW system have been widely implemented in neighbourhoods, criminals should be slower to commit crime as every citizen with a mobile device could be a potential participant in a community policing initiative appropriate for this digital age. No longer will neighbours feel powerless amid rising crime rates in their communities, but in collaboration with law enforcement agents they will be given a powerful tool to tackle crime and build safer communities not only in South Africa, but ultimately in the world at large.

Part VI

APPENDICES

An appendices section is provided to shed more light on some of the contents presented in this research dissertation. *Appendix A* provides crime report statistics as provided by the South African Police Services (SAPS). *Appendix B* presents more technical details of the ONW system's prototype development. *Appendix C* elaborates on the source code and shows the storage location link of the ***GIT Repository: GitHub*** for the ONW system‘s code. *Appendix D* shows the notation tables. Finally, *Appendix E* lists the publications that were achieved as a result of the findings of this research.

Appendix A: Crime Statistics of South Africa

A *Introduction*

In the motivation section of Chapter 1, the need for research such as in this dissertation was argued in view of rising local crime statistics. These statistics were one of the motivating factors to develop the ONW system. The crime reports below provide a detailed breakdown of various crime statistics that are known or have officially been reported in South Africa.

A.1 *Crime Report - Assaults*

The crime report on assault and sexual offences [20] states the following:

(a) Assaults with the intent to inflict grievous bodily harm - 182, 556, which implies an increase of 0.1% in 2013.

(b) Common assaults - 161, 486, which implies a 2.8% decrease since 2013.

(c) Sexual offences - 53, 617, which implies a 5.4% decrease.

A.2 *Crime Report - Murder and Robbery*

In the same vein, the crime rates related to murder and robbery [20] are as follows for 2013:

(a) Murders - 17, 805, which implies 4.6% increase. There were 49 murders and 48 attempted murders per day. The murder rate per 100, 000 in South Africa was 33 compared to the global average of 6.2.

(b) Aggravated robbery - 129, 045, which implies 8.5% increase. Altogether 354 aggravated robberies, 56 home robberies and 35 vehicle hijackings took place per day. There were 20, 281 house robberies, which implies a 5% increase and 12, 773 vehicle hijackings, which equals a 14% increase.

A.3 *Crime Report - Vandalism*

Another aspect of the report deals with property vandalism [20].

(a) Burglaries - 253, 716, which implies a 2.3% decrease. On average 195 shoplifting cases and 695 house burglaries were reported per day. Commercial crime has been reduced by 12% since 2013.

(b) Car thefts - 55, 090, which a implies 2.7% decrease. According to the report there were 398 thefts from cars and 151 car thefts per day. Stock theft has increased by 1.8%.

Appendix B: Technical Details of the ONW System

B *Introduction*

In developing the ONW system, the researcher had to report on some highly technical design and development details that would hinder the flow of reading. Thus she decided to place these technical details in the appendix section. Another reason for this decision was the fact that the rapid growth in software developments (IDEs, APIs, frameworks and packages) could very well render some of the technologies obsolete in a few years.

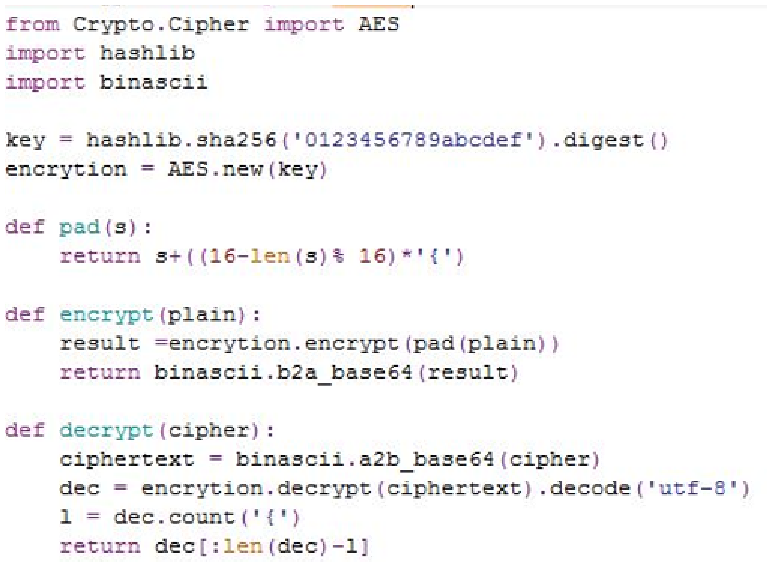
Appendix C.1 introduces the technical details of the ONW system such as the application program interfaces (APIs), and applying the architectural decisions, frameworks and code implementations of the interactive processes between the uWatch application and the NW system. It details the call functions using servlets to initiate a call function from the uWatch application that is at the access layer of the ONW system's architecture via the business logic layer to the persistence layer. These processes of security and usability address the architectural patterns, strategies and the quality requirements of the ONW system.

B.1 *Security*

In this research, two access control mechanisms were employed to design and develop the ONW system. These are the Role-Based Access Control (RBAC) and the Attribute-Based Access Control (ABAC) mechanisms which were also used for the NWS. The code example using Python decorator is depicted in Figure .4. Another technical aspect of the NWS is that it uses the Advanced Encryption Standard (AES) encryption to encrypt all uploader (citizen) information so ensure a certain degree of privacy. On the code side, the Python plugin Pycrypto, version 2.6.1, contains the AES algorithm as depicted in Figure .1.

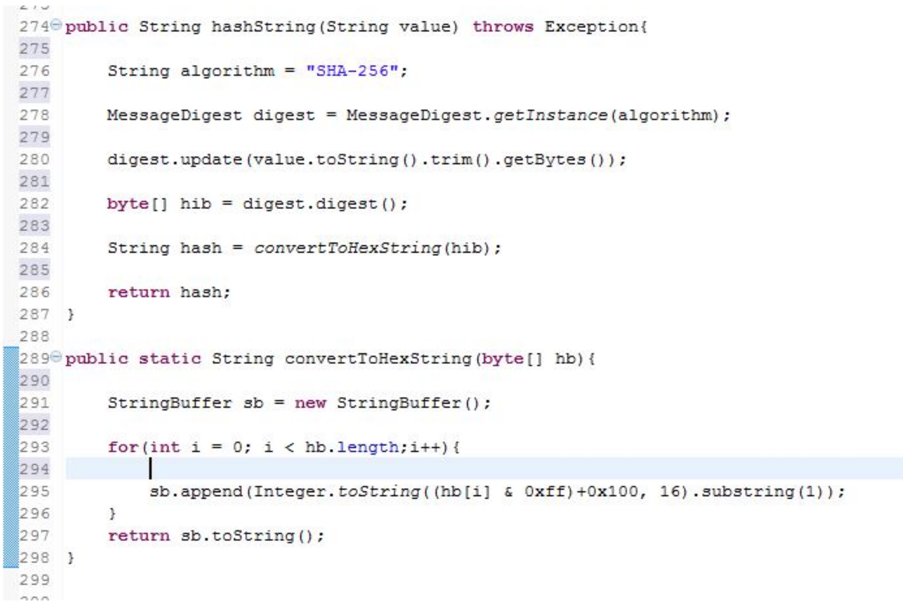
Since AES requires the input size to be a multiple of 64 bits, the pad function is used to add curly brackets to the input if it is not a multiple of 64 bits when encrypting, and decrypting. Furthermore, at storage to the ONW repository, the encrypted data is converted to ASCII using the **binascii** Python library [149], which is a method to convert between binary and various ASCII-encoded binary representations using wrapper modules like **uu**, **base64** or **binhex**[149]. Subsequently, the key used for the encryption is the hashed key using SHA256 (see in Figure .2) using the **hashlib** Python library.

As mentioned earlier, the ONW system is accessed via HTTPs for a secure encryption communication link between the uWatch application (front-end) and the NW system (back-end). When an authorised user enters incorrect login credentials three times, he/she is required to solve a challenge-response text using reCAPTCHA (see Figure .3) [150]. The reCAPTCHA function helps to in distinguish between a machine via brute force or botnet



```
from Crypto.Cipher import AES
import hashlib
import binascii

key = hashlib.sha256('0123456789abcdef').digest()
encrytion = AES.new(key)

def pad(s):
    return s+((16-len(s)% 16)*'{')

def encrypt(plain):
    result =encrytion.encrypt(pad(plain))
    return binascii.b2a_base64(result)

def decrypt(cipher):
    ciphertext = binascii.a2b_base64(cipher)
    dec = encrytion.decrypt(ciphertext).decode('utf-8')
    l = dec.count('{')
    return dec[:len(dec)-l]
```

Fig. .1: Encryption and Decryption Process of the NW System

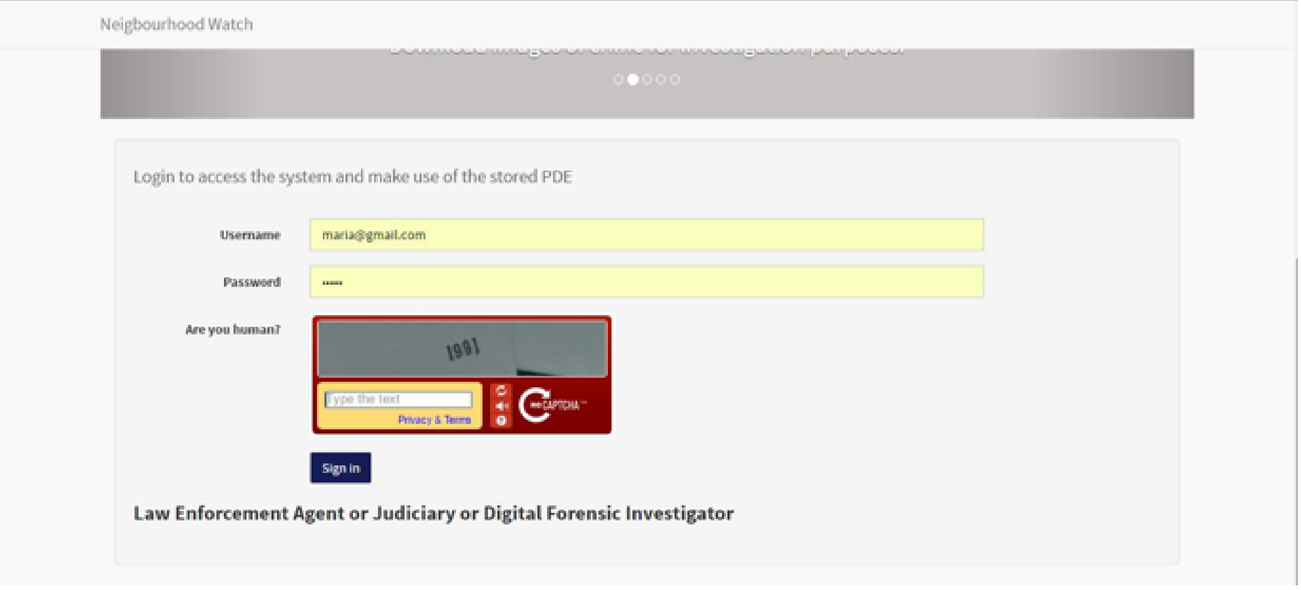


```
public String hashString(String value) throws Exception{

    String algorithm = "SHA-256";

    MessageDigest digest = MessageDigest.getInstance(algorithm);

    digest.update(value.toString().trim().getBytes());

    byte[] hib = digest.digest();

    String hash = convertToHexString(hib);

    return hash;
}

public static String convertToHexString(byte[] hb){

    StringBuffer sb = new StringBuffer();

    for(int i = 0; i < hb.length;i++){

        sb.append(Integer.toString((hb[i] & 0xff)+0x100, 16).substring(1));
    }
    return sb.toString();
}
```

Fig. .2: Cryptographic Hashing and Piping of the Captured PDE

attacks and a human user. The reCAPTCHA-client version 1.0.6. a Python plugin library was used to implement this aspect of the ONW system [150][151]. An authorised user is logged out of the system when the NW system has been left idle for 10 minutes.

All database forms created are converted to JSON schema parse through the HTML using Rest Web service and PHP cluster. The JSON objects format is used for its fastness to parse, the fact that it is lighter flexible with PHP, as well as because presents data in a more readable format over the XML message transfer protocol.



Login to access the system and make use of the stored PDE

Username maria@gmail.com

Password ••••••

Are you human?

Law Enforcement Agent or Judiciary or Digital Forensic Investigator

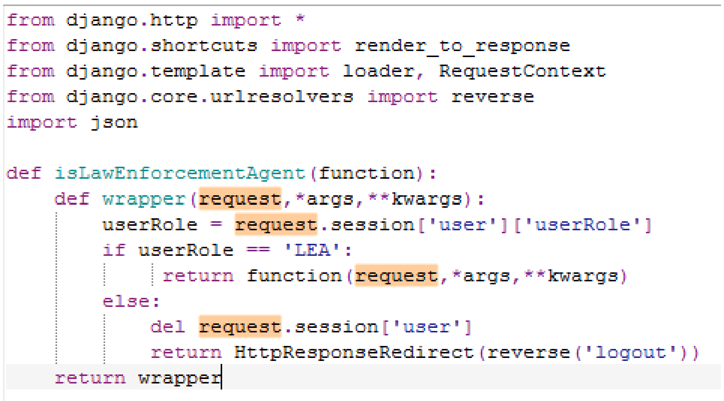
Fig. .3: Login Management - CAPTCHA required after three Login attempts

B.2 *Usability*

The usability of the ONW system is realised by using a decorator pattern and Bootstrap framework to enhance the better user experience. The decorator pattern and Bootstrap framework make the ONW system easy to operate with little to no training required for either citizens or the LEAs. The uWatch application uses SQLite to store and send PDE - both online or offline - to a queue that is synchronised as JSON objects via HTTPS when parsed to the ONW repository.

On the other hand, the NW system uses PostgreSQL, MySQL and PHP for its PDE storage. The rationale behind the choice of these databases is to enable the insertion of binary data to the database tables. The platform and scalable functionalities of MySQL enable the NW system to handle concurrent user bases, while captured PDE is stored as a JSON object.

In the overall compilation of the ONW system, the JavaEE framework comprising of Python, Django framework with BootStrap framework, PostgreSQL, MySql, SQLite, Android Studio and PHP were used. These technologies have been chosen to comply with identified functional requirements (core needs of the system), as well as to adhere to the architectural specifications of the ONW system. For example, the Django framework accommodates databases and connectors, such as Java Database Connectivity (JDBC) driver for MySql (Connector/J). Furthermore, the PHP server that uses **MySqlnd** makes for easier storage of audios, videos and photo images. This is due to the framework's high abstraction level in web development using the Bootstrap framework to absorb Hypertext Mark-up Language (HTML), Cascading Style Sheets (CSS) and Javascript at the usability design process [122].



```
from django.http import *
from django.shortcuts import render_to_response
from django.template import loader, RequestContext
from django.core.urlresolvers import reverse
import json

def isLawEnforcementAgent(function):
    def wrapper(request,*args,**kwargs):
        userRole = request.session['user']['userRole']
        if userRole == 'LEA':
            return function(request,*args,**kwargs)
        else:
            del request.session['user']
            return HttpResponseRedirect(reverse('logout'))
    return wrapper
```

Fig. .4: Session Authentication and Access Management

Figure .4 presents a view of a python function taking a web request to return a web response. This is used for the web services, right before accessing the business logic. It is a permission-based validation made to allow a request to the NW system (back-end), if and only if the authorised user is allowed to access/perform the requested action.

Appendix C: Source Code

C *Source Code*

The ONW system was developed using scrum methodologies as depicted in Chapter 7, as well as an agile approach where every aspect of the system is a component. To achieve a standardised software development using agile the *GitHub GIT Repository* was employed. Therefore all source codes of the ONW system's implementation can be found here:

C.1

GitHub:- `https://github.com/Sty123/ONW` and `https://github.com/Sty123/ONW` and `https://github.com/CollenMphabantshi/Online-Neighbourhood-Watch` and `https://github.com/u12094847/LookyFindMeandhttps://github.com/ceboMakeleni/crime_loud`

Appendix D: Crime Statistics of South Africa

Appendix D

D *Notation Table*

This section shows the table of notation.

Table A1a: Notation Table

Notation	**Description**	**Entities involved**
CA	Certificate Authority	uWatch, NWS
$\mathrm{CA}_{\mathrm{pub}}$	Certificate Authority public key	uWatch, NWS
$\mathrm{CA}_{\mathrm{priv}}$	Certificate Authority private key	CA
$\mathrm{c}_{\mathrm{ert}}$	Signed certificate	uWatch, NWS
$\mathrm{c}_{\mathrm{ert}}$	Encrypted and signed certificate	uWatch, NWS
LEA	Law enforcement agent	LEA and NWS
NWS	Neigbourhood watch system	uWatch, NWS
uWatch	uWatch Mobile application	uWatch, NWS, LEA
E	Encrypted item	uWatch, NWS
$\mathrm{U}_{\mathrm{c}_{\mathrm{ert}}}$	Neigbourhood watch systems encrypted certificate	uWatch, NWS
$\mathrm{U}_{\mathrm{pub}}$	uWatch Mobile applications public key	uWwatch, NWS
$\mathrm{U}_{\mathrm{c}_{\mathrm{ert}}}$	uWatch Mobile applications encrypted certificate	uWatch, NWS
$\mathrm{U}_{\mathrm{priv}}$	uWatch Mobile applications private key	uWatch
$\mathrm{L}_{\mathrm{pub}}$	LEA public key	NWS
$\mathrm{L}_{\mathrm{priv}}$	LEA private key	NWS
$\mathrm{L}_{\mathrm{c}_{\mathrm{ert}}}$	LEA Certificate	NWS
$\mathrm{L}_{\mathrm{c}_{\mathrm{ert}}}$	LEA Certificate encrypted	NWS, LEA and CA
$\mathrm{N}_{\mathrm{pub}}$	Neigbourhood watch systems public key	uWatch, NWS, LEA, CA
$\mathrm{N}_{\mathrm{priv}}$	Neigbourhood watch systems private key	
$\mathrm{N}_{\mathrm{c}_{\mathrm{ert}}}$	Neigbourhood watch systems certificate	uWatch, NWS
$\mathrm{N}_{\mathrm{c}_{\mathrm{ert}}}$	Neigbourhood watch systems certificate encrypted	uWatch, NWS
H()	Hashing H(dataString)	uWatch, LEA and CA

Table A1b: Notation Table

Notation	Description	Entities involved
E()	E(*encryptionKey, plainTextData*)	uWatch, NWS, LEA and CA
D()	Decryption D (*decryptionKey, cipherTextData*)	uWatch, NWS, LEA and CA
K	Symmetric Key	uWatch, NWS
K'()	Encrypted Symmetric Key	uWatch, NWS, LEA and CA
PAL	Payload auditlog	uWatch, NWS
ACK	Acknowledgement	uWatch, NWS
PL	Encrypted payload	uWatch, NWS
Payload	E(K, payload)	LEA
HAL	Hash of AuditLog	NWS
HAL'	Encrypted hash of Auditlog	NWS
N_{Ds}	NWS is Digitally signed	NWS. uWatch
U_{Ds}	uWatch is Digitally signed	CA, NWS, uWatch
H	Hashed variable	uWatch, NWS
NPW'	Encrypted username and password	uWatch, NWS and
U/N+PW	Username and Password	uWatch, LEA, NWS
Download$_{Log}$	Downloaded log file	LEA
FR	Found Record	uWatch, NWS and
L_{DS}	LEA is Digitally signed	LEA
PDE	Potential digital evidence	uWatch, NWS
R_{L0}	Forensic soundness level that implement integrity	uWatch, NWS
R_{L1}	Forensic soundness level that implement integrity + Confidentiality + non repudiation	uWatch, NWS
R_{L2}	Forensic soundness level that implement integrity + Confidentiality + non repudiation + authentication + authorisation	uWatch, NWS
Cert ID Info	Certificate identity information	CA, uWatch, NWS
NACK	No acknowledgment	CA, LEA, NWS
A_t	Authentication	CA, LEA, NWS
A_z	Authorisation	CA, LEA, NWS

Appendix E : Publications

E *Introduction*

This dissertation has resulted in some double-blind, peer-reviewed conferences and journal publications. Chapters 5,6 and 7 each produced a paper for a peer-reviewed conference, namely [13] [15] [136] respectively. Furthermore, Chapter 7 was later extended and submitted as a journal article [123]. Chapter 8 served as the basis for yet another paper [124] and has also been extended to an article.

E.1 *Publications*

Publications based on this research are listed below, and their links are provided for easy access.

(1) Stacey Omeleze and Hein S. Venter. **Towards a Model for Acquiring Digital Evidence using Mobile Devices.** ***Presented and published*** *at the 10th International Network Conference (INC 2014) and WDFIA 2014 Plymouth, University, UK, pages 114. Plymouth University, UK, 2014.* h*ttps://goo.gl/0vMxnC*

(2) Stacey Omeleze and Hein S. Venter. **A Model for Access Management of Potential Digital Evidence.** ***Presented and published*** *at the 10th International Conference on Cyber Warfare & Security (ICCWS), pages 491-501. CSIR, University of Vender and Academic Conferences Limited, 2015.: https://goo.gl/XwdzkR*

(3) Stacey Omeleze and Hein S. Venter. **A Proof of Concept of the Online Neighbourhood Watch System** ***Presented and published with Springer*** *International Conference on e-Infrastructure and e-Services for Developing Countries, at the Proceedings of AFRICOMM, 15 and 16 December 2015, Benin Republic, West Africa. ISBN-Online.*

(4) Stacey Omeleze and Hein S. Venter. **Architectural requirements specifications for designing digital forensic applications.** ***Presented and published*** *at the 15th European Conference on Cyber Warfare and Security ECCWS-2016, 2016. 0045-0618 (Print), 1834-562X (Online).: https://goo.gl/lRZfKQ*

(5) Stacey Omeleze and Hein S. Venter. **Digital forensic application requirements specifications.** ***Accepted for publication*** *by the - Australian Journal of Forensic Sciences. Australian Journal of Forensic Sciences. url: http://anzfss.org/australian-journal-of-forensic-sciences/.*

(6) Stacey Omeleze and Hein S. Venter. **Acquisition and Retention of Potential Digital Evidence of Neighbourhood Crime**, Pages 1 to 10. ***Presented and published*** *at the Proceedings of IST-Africa 2017 Conference - May 2017, Windhoek, Namibia* h*ttp://http://www.ist-africa.org/Conference2017/*

Bibliography

[1] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, “User acceptance of information technology: Toward a unified view,” *MIS quarterly*, pp. 425–478, 2003.

[2] M. A. Gunawan, F. Sulaiman, T. A. Putra, C. Daniel Hasudungan, and R. F. Sari, “Object-following robot using adaptive cruise control algorithm with ioio,” in *Intelligent Green Building and Smart Grid (IGBSG), 2014 International Conference on*. IEEE, 2014, pp. 1–5.

[3] S. A. P. S. SAPS, “Submission of the Annual Report to the Minister of Police,” South African Police Service Annual Report, 2012/2013, Tech. Rep., 2014, http://goo.gl/PAgPI1 - - Accessed on the 20 August, 2014.

[4] C. Gould, J. Burger, and G. Newham, “The saps crime statistics: what they tell us–and what they dont,” *South African Crime Quarterly*, vol. 42, pp. 3–12, 2014.

[5] S. C. S. AfricaCheck, “Factsheet south africa: Official crime statistics for 2012/13,” 2013.

[6] A. W. Dutelle, “An introduction to crime scene investigation.”

[7] S. O. Victor R Kebande, Nickson M Karie, “A mobile forensic readiness model aimed at minimizing cyber bullying.”

[8] J. Van Kesteren, P. Mayhew, P. Nieuwbeerta, N. M. of Justice, Research, D. Centre, and Netherlands, “Criminal victimization in seventeen industrialised countries: Key findings from the 2000 international crime victims survey,” 2001.

[9] T. Bennett, K. Holloway, and D. Farrington, “The effectiveness of neighbourhood watch,” *Unfinished review forthcoming in The Campbell Collaboration Reviews of Intervention and Policy Evaluations (C2-RIPE), Philadelphia: Campbell Collaboration*, 2005.

[10] M. Bunge, *Philosophy of Science: From Problem to Theory*. Transaction Publishers, New Brunswick, 1998.

[11] S. Papadopoulos and S. Snail, *Cyberlaw at South AfricaIII-The law of the Internet in South Africa*, 3rd ed. Van Schaik Publishers, 2012, iSBN:10(13) 9780627028076.

[12] v. d. M. DP, “Information and communications technology law,” *LexisNexis, Durban*, 2008.

[13] S. Omeleze and H. S. Venter, “Towards a model for acquiring digital evidence using mobile devices.” in *INC*, 2014, pp. 173–186.

[14] A. Valjarevic and H. S. Venter, “Introduction of concurrent processes into the digital forensic investigation process,” *Australian Journal of Forensic Sciences*, vol. 48, no. 3, pp. 339–357, 2016.

[15] S. Omeleze and S. H. Venter, "A model for access management of potential digital evidence," in *10th International Conference on Cyber Warfare & Security (ICCWS)*. CSIR, University of Vender and Academic Conferences Limited, 2015, pp. 491–501.

[16] J. Fadenrecht, "Community policing and total quality: Tools for effective police resource management," *Campus Law Enforcement Journal*, vol. 25, no. 1, pp. 23–25, 1995.

[17] G. Gazette, "Electronic Communications and Transactions Act, Act 25 of 2002," PDF Scanned by Sabinet [Online - Accessed 08 February, 2014], Tech. Rep., August 2002, south Africa Government Gazette - Legislation - South Africa - National/Acts and Regulations/E/Electronic Communications And Transactions Act No. 25 Of 2002/The Act.

[18] G.-G. POPI-Act, "Privacy and data protection - discussion paper 109 (project 124) - south african law reform commission (2005-10)," [Online - Accessed 08 August, 2014], Tech. Rep., August 2013, south Africa Government Gazette - Legislation - South Africa - National/Acts - Privacy and data protection Act No.4 of 2013. [Online]. Available: http://www.sabinetlaw.co.za/justice-and-constitution/legislation/protection-personal-information

[19] M. Mujinga, "Privacy and legal issues in cloud computing-the smme position in south africa," 2013.

[20] ISS. (2015) ISS Africa iss crime hub. [Online]. Available: https://www.issafrica.org/crimehub/media-room/videos-and-infographics

[21] A. Bellengere, R. Palmer, C. Theophilopoulos, B. Whitcher, L. Roberts, and N. M. et al, *The Law of evidence in South African -Basic Principles-Procedural Law*. Oxford University Press, Southern Africa, 2013.

[22] J. Sammons, *The basics of digital forensics: the primer for getting started in digital forensics*. Elsevier, 2012.

[23] M. M. Houck and J. A. Siegel, *Fundamentals of forensic science*. Academic Press, 2009.

[24] AAFS, "American Academy of Forensic Sciences (AAFS)," http://www.aafs.org/resources/academy-news-pdf-library/, 2014, "[Online; accessed 10-July-20014]".

[25] M. W. Andrew, "Defining a process model for forensic analysis of digital devices and storage media," in *null*. IEEE, 2007, pp. 16–30.

[26] B. D. Carrier, "Digital forensics works," *IEEE Security & Privacy*, no. 2, pp. 26–29, 2009.

[27] I. R. Adeyemi, S. A. Razak, and N. A. N. Azhan, "A review of current research in network forensic analysis," *International Journal of Digital Crime and Forensics (IJDCF)*, vol. 5, no. 1, pp. 1–26, 2013.

[28] W. J. Tilstone, K. A. Savage, and L. A. Clark, *Forensic science: An encyclopedia of history, methods, and techniques*. ABC-CLIO, 2006.

[29] E. Casey, *Digital Evidence and computer crime Forensics science computers and and the internet*, 3rd ed. Elsevier Inc, 2011.

[30] M. Webster, “The merriam webster dictionary (2013).”

[31] J. A. Simpson, E. S. Weiner *et al.*, *The Oxford english dictionary*. Clarendon Press Oxford, 1989, vol. 2.

[32] M. M. Houck and J. A. Siegel, *Fundamentals of forensic science*. Academic Press, 2010.

[33] R. McKemmish, “When is digital evidence forensically sound?” *Advances in digital forensics IV*, pp. 3–15, 2008.

[34] T. C. DFRWS Workshop *et al.*, “A road map for digital forensic research:dfrws technical report,” DTR-T001-01 Final, Tech. Rep., August 2001.

[35] F. A. Cohen, *Digital Forensic Evidence Examination*, 3rd ed. Fred Cohen and Associates out of Livermore, 2009.

[36] K. Nance, B. Hay, and M. Bishop, “Digital forensics: defining a research agenda,” in *System Sciences, 2009. HICSS’09. 42nd Hawaii International Conference on*. IEEE, 2009, pp. 1–6.

[37] J. L. John, “Digital forensics and preservation,” *Digital Preservation Coalition - DPC Technology Watch Report*, 2012, http://dx.doi.org/10.7207/twr [Online; accessed 13 December, 2013].

[38] D. Barske, A. Stander, and J. Jordaan, “A digital forensic readiness framework for south african (sme)s,” in *Information Security for South Africa (ISSA), 2010*. IEEE, 2010, pp. 1–6.

[39] R. Rowlingson, “A ten step process for forensic readiness,” *International Journal of Digital Evidence*, vol. 2, no. 3, pp. 1–28, 2004.

[40] C. Grobler, C. Louwrens, and S. H. von Solms, “A framework to guide the implementation of proactive digital forensics in organisations,” in *Availability, Reliability, and Security, 2010. ARES’10 International Conference on*. IEEE, 2010, pp. 677–682.

[41] S. Orofino, “Daubert v. merrell dow pharmaceuticals, inc. the battle over admissibility standards for scientific evidence in court,” *J. Undergrad. Sci. 3: 109-111(Summer 1996)*, 1996.

[42] A. E. Manual, *Digital Evidence Gathering*, International Competition Network-Cartel Working Group, March 2010. [Online]. Available: http\www.internationalcompetitionnetwork.org

[43] W. J. Chisum and B. Turvey, “Evidence dynamics: Locard’s exchange principle & crime reconstruction,” *Journal of Behavioral Profiling*, vol. 1, no. 1, pp. 1–15, 2000.

[44] B. Carrier, “Defining digital forensic examination and analysis tools using abstraction layers,” *International Journal of digital evidence*, vol. 1, no. 4, pp. 1–12, 2003.

[45] J. Ćosić and M. Bača, “A framework to (im) prove chain of custody “in digital investigation process,” in *CECIIS-2010*. IEEE, 2010, pp. 43–438.

[46] C. J. Hargreaves, “Assessing the reliability of digital evidence from live investigations involving encryption,” Ph.D Thesis, Dept of Informatics and Sensors, Cranfield University,UK, 2009.

[47] M. Duren and C. Hosmer, "Can digital evidence endure the test of time?" in *Proceedings of the Second Digital Forensic Research Workshop*, vol. 2002, 2002.

[48] E. Michael and J. Herbert, *Management of Information Security*, 3rd ed. Course Technology, Boston, M 02210, USA. ISBN-13, 2009.

[49] P. C. Pfleeger and S. L. Pfleeger, *Security in Computing*, 4th ed. Prentice Hall Publication, Upper Saddle Rivers, NJ, Boston USA ISBN, 2006, iSBN:0132390779.

[50] A. Mouhtaropoulos, M. Grobler, and C.-T. Li, "Digital forensic readiness: an insight into governmental and academic initiatives," in *Intelligence and Security Informatics Conference (EISIC), 2011 European*. IEEE, 2011, pp. 191–196.

[51] I. T. S. Techniques, "Iso/iec 27037:2012 information technology security techniques guidelines for identification, collection, acquisition, and preservation of digital evidence," ISO/IEC - The standard was published in October 2012, Tech. Rep., 2012. [Online]. Available: http://www.iso27001security.com/html/27037.htmlandhttps//sites.google.com/a/ist033.org.uk/public/home/4/cg-ip/27043

[52] Q. Dang, "Recommendation for applications using approved hash algorithms," *Computer Security Division Information Technology Laboratory*, August 2012.

[53] L. Cheng-Shain and J.-J. Tsay, "Passive approach for video forgery detection and localization," *The Second International Conference on Cyber Security*, 2013.

[54] C. M. Robert, "Audio forensic examination - authenticity, enhancement, and interpretation," *IEEE Signal Processing Magazine*, 2009.

[55] S. Saleem, "Protecting the integrity of digital evidence and basic human rights during the process of digital forensics," 2015.

[56] M. T. Sakalli, E. Bulus, and F. Büyüksaraçoğlu, "Cryptography education for students," in *Information Technology Based Higher Education and Training, 2004. ITHET 2004. Proceedings of the FIfth International Conference on*. IEEE, 2004, pp. 621–626.

[57] P. Charles and S. L. Pfleeger, *Analyzing Computer Security: A Threat/vulnerability/countermeasure Approach*. Prentice Hall, 2012.

[58] N.-F. Standard, "Announcing the advanced encryption standard (aes)," *Federal Information Processing Standards Publication*, vol. 197, pp. 1–51, 2001.

[59] G. C. Kessler, "An overview of cryptography," *Gary C. Kessler*, 2003.

[60] W. J. Caelli, E. P. Dawson, and S. A. Rea, "Pki, elliptic curve cryptography, and digital signatures," *Computers & Security*, vol. 18, no. 1, pp. 47–66, 1999.

[61] X. Yi, R. Paulet, and E. Bertino, *Homomorphic encryption and applications*, 2014, vol. 3.

[62] D. J. Abadi, "Consistency tradeoffs in modern distributed database system design: Cap is only part of the story," *Computer*, no. 2, pp. 37–42, 2012.

[63] C. Gentry, *A fully homomorphic encryption scheme*, 2009.

[64] A. Calder, S. Watkins, and I. Governance, "A manager's guide to data security and iso 27001/iso 27002," *Kogan Page*, 2008.

[65] J. E. Silva, "An overview of cryptographic hash functions and their uses," *GIAC*, vol. 6, 2003.

[66] F. Mendel, N. Pramstaller, C. Rechberger, and V. Rijmen, "Analysis of step-reduced sha-256," in *International Workshop on Fast Software Encryption*. Springer, 2006, pp. 126–143.

[67] R. Sandhu, D. Ferraiolo, and R. Kuhn, "The nist model for role-based access control:towards a unified standard," in *ACM workshop on Role-based access control*, vol. 2000, 2000.

[68] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed nist standard for role-based access control," *ACM Transactions on Information and System Security (TISSEC)*, vol. 4, no. 3, pp. 224–274, 2001.

[69] M. Whitman and H. Mattord, *Management of information security*. Cengage Learning, 2013, 13: 978-0-8400-3160-0.

[70] J. Qian, S. Hinrichs, and K. Nahrstedt, "Acla: A framework for access control list (acl) analysis and optimization," in *Communications and Multimedia Security Issues of the New Century*. Springer, 2001, pp. 197–211.

[71] S. Osborn, R. Sandhu, and Q. Munawer, "Configuring role-based access control to enforce mandatory and discretionary access control policies," *ACM Transactions on Information and System Security (TISSEC)*, vol. 3, no. 2, pp. 85–106, 2000.

[72] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed nist standard for role-based access control," *ACM Transactions on Information and System Security (TISSEC)*, vol. 4, no. 3, pp. 224–274, 2001.

[73] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, "Guide to attribute based access control (abac) definition and considerations," *NIST Special Publication*, vol. 800, p. 162, 2014.

[74] G. Makungo, M. Dlamini, and H. Venter, "Access control in a cloud-based collaborative network," January 2013, bsc (Honours) Project-Dissertation, Submitted to Dept of Computer Science, University of Pretoria,South Africa.

[75] V. C. Hu and K. A. Kent, *Guidelines for access control system evaluation metric*. US Department of Commerce, National Institute of Standards and Technology, September 2012. [Online]. Available: http://dx.doi.org/10.6028/NIST.IR.7874-Accessed18April,2014

[76] E. Yuan and J. Tong, "Attributed based access control (abac) for web services," in *IEEE International Conference on Web Services (ICWS'05)*. IEEE, 2005.

[77] T. Coffey and P. Saidha, "Non-repudiation with mandatory proof of receipt," *ACM SIGCOMM Computer Communication Review*, vol. 26, no. 1, pp. 6–17, 1996.

[78] J. Zhou and D. Gollman, "A fair non-repudiation protocol," in *Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on*. IEEE, 1996, pp. 55–61.

[79] S.-C. Cha, Y.-J. Joung, Y.-C. Tseng, S.-C. Huang, G.-H. Chen, and C.-T. Tseng, "Ensuring the integrity and non-repudiation of remitting e-invoices in conventional channels with commercially available nfc devices," in *Software Engineering, Artificial*

Intelligence, Networking and Parallel/Distributed Computing (SNPD), 2014 15th IEEE/ACIS International Conference on. IEEE, 2014, pp. 1–6.

[80] M. Weiser, D. P. Biros, and G. Mosier, "Development of a national repository of digital forensic intelligence," *Glenn S. Dardick, Editor-in-Chief Longwood University Virginia, USA*, p. 5, 2006.

[81] E. Casey, *Handbook of digital forensics and investigation.* Academic Press, 2009.

[82] M. Mujinga, "Privacy and Legal Issues in Cloud Computing-the SMME Position in South Africa," *SRI Security Research Institute, Edith Cowan University, Perth, Western Australia - [Online;accessed 17 March, 2014*, 2013.

[83] S. E. Blythe, "Digital signature law of the united nations, european union, united kingdom and united states: Promotion of growth in e-commerce with enhanced security," *Rich. JL & Tech.*, vol. 11, pp. 6–8, 2005.

[84] H. Hamidovic, "How to maximize evidential weight of electronically stored information recommendations of bs 10008," *ISACA Journal*, 2012. [Online]. Available: http://www.isaca.org/Journal/Past-Issues/2012/Volume-4/Documents/12v4-How-to-Maximize-Evidential-Weight.pdf

[85] R. A.-J. Department.

[86] H. N. Olinger, J. J. Britz, and M. S. Olivier, "Western privacy and ubuntu: influences in the forthcoming data privacy bill," *Ethics and New Information Technology, CEPE*, pp. 291–306, 2005.

[87] S. Snail, "Cyber crime in south africa–hacking, cracking, and other unlawful online activities," *Journal of Information, Law and Technology*, vol. 1, pp. 2009–1, 2009.

[88] P.-J. Schwikkard and S. E. Van der Merwe, *Principles of evidence.* Juta and Company Ltd, 2009, iSBN: 978 0 7021 79501.

[89] K. Pohl, *Requirements engineering: fundamentals, principles, and techniques.* Springer Publishing Company Incorporated, 2010, iSBN:3642125778 9783642125775.

[90] R. K. Len Bass, Paul Clements, *Software Architecture in Practice, 3rd Edition.* Addison-Wesley Professional. Part of the SEI Series in Software Engineering series, 2012, iSBN-13: 000-0321815734 ISBN-10: 0321815734 3rd Edition.

[91] S. T. Albin, *The art of software architecture: design methods and techniques.* John Wiley & Sons, 2003, vol. 9.

[92] F. Solms, "What is software architecture?" in *Proceedings of the South African Institute for Computer Scientists and Information Technologists Conference.* ACM, 2012, pp. 363–373.

[93] D. Leffingwell and D. Widrig, *Managing software requirements: a use case approach*, 2003, iSBN-13: 978-0321122476, ISBN-10: 032112247X.

[94] I. Jacobson, G. Booch, J. Rumbaugh, J. Rumbaugh, and G. Booch, *The unified software development process.* Addison-Wesley Reading, 1999, vol. 1.

[95] D. Bell, "Uml basics: The sequence diagram," *IBM Global Services http://www. ibm. com/developerworks/rational/library/3101. html timestamp={2010.03. 04}*, 2004.

[96] F. Solms. (2010) Fritz solms website and hounors lecture notes sofware architecture 2012, 2013, computer science dept., university of pretoria - software architecture. [Online]. Available: http://www.solms.co.za/training/courses/[accessed-23rdMarch, 2012]

[97] I. Sommerville and G. Kotonya, *Requirements engineering: processes and techniques*. John Wiley & Sons, Inc., 1998.

[98] B. J. Oates, *Researching information systems and computing*. Sage, 2005, 978-1-4129-0224-3. [Online]. Available: www.sagepublications.com

[99] V. Vemuri, *Modeling of complex systems: an introduction*. Academic Press, INC., 111 Fifth avenue New York 10003, 1978, 0-12-716550-9.

[100] R. Knackstedt, M. Heddier, and J. Becker, “Conceptual modeling in law: An interdisciplinary research agenda,” *Communications of the Association for Information Systems*, vol. 34, no. 1, p. 36, 2014.

[101] O. ISO, “Iec 7498-2: 1989 information processing systems-open systems interconnection-basic reference model,” 1984.

[102] H. Susanto, M. N. Almunawar, and Y. C. Tuan, “Information security management system standards: A comparative study of the big five,” 2011.

[103] O. S. Kerr, “Searches and seizures in a digital world,” *Harvard Law Review*, pp. 531–585, 2005.

[104] P. Turner, “Selective and intelligent imaging using digital evidence bags,” *digital investigation*, vol. 3, pp. 59–64, 2006.

[105] C. J. Alberts and A. Dorofee, *Managing information security risks: the OCTAVE approach*. Addison-Wesley Longman Publishing Co., Inc., 2002.

[106] M. Mogollon, *Cryptography and Security Services: Mechanisms and Applications: Mechanisms and Applications*. IGI Global, 2008.

[107] B. Von Solms, J. Eloff, and E. Smith, *Information security*. Amabhuku, 2000.

[108] K. Reddy and H. Venter, “A forensic framework for handling information privacy incidents,” in *IFIP International Conference on Digital Forensics*. Springer, 2009, pp. 143–155.

[109] K. D. Mitnick and W. Simon, *The art of deception: Controlling the human element of security*. John Wiley Sons, 2001.

[110] H. Pieterse, M. Olivier, and R. Van Heerden, “Reference architecture for android applications to support the detection of manipulated evidence,” 2016.

[111] B. Carrier, E. H. Spafford *et al.*, “Getting physical with the digital investigation process,” *International Journal of digital evidence*, vol. 2, no. 2, pp. 1–20, 2003.

[112] S. Ahern, M. Davis, S. King, M. Naaman, and R. Nair, “Reliable, user-contributed gsm cell-tower positioning using context-aware photos,” in *Adjunct Proceedings of the Eighth International Conference on Ubiquitous Computing (UbiComp 2006)*, 2006.

[113] C. Assembly. As Adopted on 8 May 1996 and amended on 11 October 1996 by the Constitutional Assembly, 1996. [Online]. Available: http://www.gov.za/sites/www.gov.za/files/images/a108-96.pdf

[114] K. Naik and P. Tripathy, *Software testing and quality assurance: theory and practice*. John Wiley & Sons, 2011.

[115] P. Tahchiev, F. Leme, V. Massol, and G. Gregory, *JUnit in action*. Manning Publications Co., 2010.

[116] P. M. Duvall, S. Matyas, and A. Glover, *Continuous integration: improving software quality and reducing risk*. Pearson Education, 2007.

[117] O. A. L. Lemos, I. G. Franchin, and P. C. Masiero, "Integration testing of object-oriented and aspect-oriented programs: A structural pairwise approach for java," *Science of Computer Programming*, vol. 74, no. 10, pp. 861–878, 2009.

[118] Q. Yang, J. J. Li, and D. M. Weiss, "A survey of coverage-based testing tools," *The Computer Journal*, vol. 52, no. 5, pp. 589–597, 2009.

[119] D. Kung, *Object-oriented Software Engineering: An Agile Unified Methodology*. McGraw-Hill Higher Education, 2013.

[120] J. Meier, D. Hill, A. Homer, T. Jason, P. Bansode, L. Wall, R. Boucher Jr, and A. Bogawat, "Microsoft application architecture guide," *Microsoft Corporation*, 2009.

[121] F. Solms and D. Loubser, "Urdad as a semi-formal approach to analysis and design," *Innovations in Systems and Software Engineering*, vol. 6, no. 1-2, 2010.

[122] A. Holovaty and J. Kaplan-Moss, *The definitive guide to Django: Web development done right*. Apress, 2009.

[123] S. Omeleze and S. H. Venter, "Digital forensic application requirements specifications," in *Submitted to the - Australian Journal of Forensic Sciences*. Australian Journal of Forensic Sciences, 2016, 0045-0618 (Print), 1834-562X (Online).

[124] S. Omeleze and H. S. Venter, "A proof of concept of the online neigbourhood watch system." Presented at AFRICOMM 2015, 2015, pp. 1–12, iSBN: ISBN-Online.

[125] J. Cosic and Z. Cosic, "Chain of custody and life cycle of digital evidence," *Computer technology and application*, vol. 3, no. 2, 2012.

[126] M. Watney, "Admissibility of electronic evidence in criminal proceedings an outline of the south african legal position," *Journal of Information*, 2009.

[127] A. Valjarevic and H. S. Venter, "Towards a digital forensic readiness framework for public key infrastructure systems," in *Information Security South Africa (ISSA), 2011*. IEEE, 2011, pp. 1–10.

[128] S. Omeleze and H. S. Venter, "Testing the harmonised digital investigation process model using an android mobile phone," in *Information Security for South Africa, 2013*. IEEE, 2013, pp. 1–8.

[129] O. S. Kerr, "Digital evidence and the new criminal procedure," *Columbia Law Review*, pp. 279–318, 2005.

[130] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer security incident handling guide," *NIST Special Publication*, vol. 800, p. 61, 2012.

[131] T. S. Kuhn, “Rationality and theory choice,” *The Journal of Philosophy*, pp. 563–570, 1983.

[132] J. J. Clement, “The role of imagistic simulation in scientific thought experiments,” *Topics in cognitive science*, vol. 1, no. 4, pp. 686–710, 2009.

[133] C. S. Maria, *Digital Reporter*, 03 June, 2016, accessed - 5th June, 2016. [Online]. Available: http://www.theweathernetwork.com/news/articles/newborn-left-in-hot-car-for-20-minutes-while-parents-shop/68556

[134] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, Volume 1*. Academic, 2000 edition, illustrated, 2000.

[135] A. Valjarevic and H. S. Venter, “Harmonised digital forensic investigation process model,” in *ISSA*. IEEE, 2012, pp. 1–10. [Online]. Available: DBLP:conf/ISSA/2012

[136] S. Omeleze and H. Venter, “Architectural requirements specifications for designing digital forensic applications,” in *European Conference on Cyber Warfare and Security*. Academic Conferences International Limited, 2016, p. 405.

[137] U. P. D. Ani, G. Epiphaniou, and T. French, “A novel evidence integrity preservation framework (eipf) for virtualised environments: A digital forensic approach,” in *The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec2013)*. The Society of Digital Information and Wireless Communication, 2013.

[138] J. Richter, N. Kuntze, and C. Rudolph, “Security digital evidence,” in *Systematic Approaches to Digital Forensic Engineering (SADFE), 2010 Fifth IEEE International Workshop on*. IEEE, 2010, pp. 119–130.

[139] A. Mylonas, V. Meletiadis, L. Mitrou, and D. Gritzalis, “Smartphone sensor data as digital evidence,” *Computers & Security*, vol. 38, pp. 51–75, 2013.

[140] M. Hedstrom, “Digital preservation: a time bomb for digital libraries,” *Computers and the Humanities*, vol. 31, no. 3, pp. 189–202, 1997.

[141] A. Zuccala, C. Oppenheim, and R. Dhiensa, “Managing and evaluating digital repositories,” *Information Research*, vol. 13, no. 1, p. 3, 2008.

[142] B. Schatz and A. J. Clark, “An open architecture for digital evidence integration,” 2006.

[143] S. Garfinkel, P. Farrell, V. Roussev, and G. Dinolt, “Bringing science to digital forensics with standardized forensic corpora,” *digital investigation*, vol. 6, pp. S2–S11, 2009.

[144] D. E. Herlea, C. M. Jonker, J. Treur, and N. J. Wijngaards, “Integration of behavioural requirements specification within knowledge engineering,” in *Knowledge Acquisition, Modeling and Management*. Springer, 1999, pp. 173–190.

[145] G. Grispos, J. Garcia-Galan, L. Pasquale, and B. Nuseibeh, “Are you ready? towards the engineering of forensic-ready systems,” *arXiv preprint arXiv:1705.03250*, 2017.

[146] M. Reith, C. Carr, and G. Gunsch, “An examination of digital forensic models,” *International Journal of Digital Evidence*, vol. 1, no. 3, pp. 1–12, 2002.

[147] N. H. Ab Rahman, W. B. Glisson, Y. Yang, and K.-K. R. Choo, “Forensic-by-design framework for cyber-physical cloud systems,” *IEEE Cloud Computing*, vol. 3, no. 1, pp. 50–59, 2016.

[148] V. Kapella, “A framework for incident and problem management,” *International Network Services whitepaper*, 2003.

[149] “Python Plugin recaptcha service,” http://docs.python.org/3.1/library/binascii.html, accessed: 2014-09-16.

[150] “Python Plugin recaptcha service,” http://https://pypi.python.org/pypi/recaptcha-client?, accessed: 2014-09-06.

[151] Z. Pan, X. Yang, and Z. Xie, “A middleware: Python plugin transform on different gis platforms,” in *Geoinformatics, 2015 23rd International Conference on*. IEEE, 2015, pp. 1–6.