2019

A Web based tool for securing digital evidence

Collins Sebastian Warutumo
Faculty of Information Technology (FIT)
Strathmore University

A WEB BASED TOOL FOR SECURING DIGITAL EVIDENCE

Warutumo Collins Sebastian

Master of Science in Information Systems Security

2019

A WEB BASED TOOL FOR SECURING DIGITAL EVIDENCE

Warutumo Collins Sebastian

Submitted in partial fulfilment of the requirements for the Degree of Master of Science in Information Systems Security

Faculty of Information and Technology

Strathmore University

Nairobi, Kenya

June, 2019

Declaration

I declare that this work has never been previously submitted and approved for the award of a degree by Strathmore University or any other university. To the best of my knowledge and belief, this dissertation contains no material previously published or written by another person except where due reference is made in the dissertation itself.

Warutumo Collins Sebastian

12th June 2019

Approval

The dissertation of Warutumo Collins Sebastian was reviewed and approved by the following:

Dr. Humphrey Njogu,
Senior Lecturer, Faculty of Information Technology
Strathmore University

Dr. Joseph Orero,
Dean, Faculty of Information Technology
Strathmore University

Professor Ruth Kiraka,
Dean, School of Graduate Studies
Strathmore University

Abstract

Digital forensics is defined as a scientific knowledge and methods applied to the identification, acquisition, preservation, examination, and analysis of information stored or transmitted in binary form in a manner acceptable for application in legal matters. Digital forensics has increased its importance as there have been increase in the number of cyber cases involving digital forensics, official cybercrime report predicts the cases will be quadruple and will cost $6 trillion dollars by 2021. Preserving integrity of evidence in digital investigations is important as in helps the courts in delivering fair judgements.

The aim of this dissertation is to develop an automated tool that helps investigators to maintain the integrity of digital evidence at acquisition phase, so as it is used to deliver a fair judgement in a court of law. The tool preserves the integrity of evidence using encryption, hashing and access controls amongst other controls. This ensures that evidence is secure as it has all attributes of security (confidentiality, availability and integrity).There are a variety of available solutions which preserve the integrity of evidence but they are not effective in terms of integrity of evidence. The developed system has the addressed the existing gaps. The study uses agile methodology, this is because it allows for fast implementation of prototype in a in short period of time hence making it efficient. Agile methodology guided on the development of the tool that is accurate, robust and secures. The main components of the system are the evidence collection and reporting modules. The result of the solution is to enhance efficiency in digital investigations by ensuring integrity of evidence.

The focus of this research is integrity of evidence. The problem addressed in this research is evidence alteration at the acquisition phase which interferes with the integrity of data. The tests conducted evaluated the system's performance which showed that resource retrieval speed averaged a few seconds leading to a high-performance rating. The response rate of the system is high, this is shown by the turnaround time of receiving requests from the server. The system's compatibility tests show it is accessible in many browsers. The system exhibited high accuracy results in terms on preservation of integrity of evidence.

Keywords

Digital Forensics, Digital Evidence

Table of Contents

Declaration ii

Abstract iii

List of Figures viii

List of Tables x

List of Abbreviations xi

Acknowledgements xii

Chapter 1: Introduction 1

1.1 Background 1

1.2 Problem Statement 2

1.3 General Objective 3

1.4 Research Questions 3

1.5 Justification 3

1.6 Scope and Limitations 4

Chapter 2: Literature Review 5

2.1 Introduction 5

2.2 Overview of Digital Forensics 5

2.3 Understanding Digital Forensics Investigations Process 6

2.4 Technologies for the Preserving Integrity of Evidence 7

2.5 Existing Tools Used in Digital Evidence Security 10

2.6 Conceptual Model Diagram 14

2.7 Conclusions 15

Chapter 3: Methodology 16

3.1 Introduction 16

3.2 Agile Methodology 16

3.2.1 System Requirements Phase 18

3.2.2 System Planning Phase 19

3.2.3 System Design 19
3.2.4 System Development 20
3.2.5 System Release 23
3.2.6 System Track and Monitor 23
Chapter 4: System Design and Architecture 24
4.1 Overview 24
4.2 Functional Requirements 24
4.2.1 Digital Evidence Encryption 24
4.2.2 Digital Evidence Decryption 25
4.3 Non-Functional Requirements 26
4.4 System Architecture 26
4.4.1 Phase 1 27
4.4.2 Phase 2 27
4.4.3 Phase 3 27
4.4.4 Phase 4 27
4.5 System Design Tools 28
4.5.1 Context Diagram 28
4.5.2 Dataflow Diagram 29
4.5.3 Use Case Diagram 30
4.5.4 Sequence Diagram 35
4.5.5 Entity Relationship Diagram 37
4.6 Network Design 40
4.7 Security Design 41
4.8 Wireframes 42
Chapter 5: System Implementation and Testing 46
5.1 Introduction 46
5.2 Implementation Environment 46

5.2.1 Hardware Requirements 46
5.2.2 Software Requirements 46
5.2.3 Network Requirements 47
5.2.4 Security Requirements 47
5.3 System Modules 49
5.3.1 Dashboard 49
5.3.2 Registration and Login 49
5.3.3 Adding a Case 50
5.3.4 Encrypting Evidence 50
5.3.5 Decrypting Evidence 52
5.3.6 Evidence Reporting 55
5.3.7 System Logs 58
5.3.8 Application Programming Interface 59
5.3.9 Evidence Retention 60
5.4 Tests Results 60
5.4.1 Functionality Tests 60
5.4.2 Non functionality tests 61
5.4.3 Usability Tests 61
5.4.4 Compatibility Testing 63
5.4.5 Unit Testing 63
5.4.6 Integration Testing 64
5.5 Validation 64
Chapter 6: Discussion of Key Results 65
6.1 Overview 65
6.2 Objective One 65
6.3 Objective Two 65
6.4 Objective Three 66

6.5 Objective Four 66
Chapter 7: Conclusions, Recommendations and Future Work 67
7.1 Conclusions 67
7.2 Recommendations 67
7.3 Future Work 67
Appendix A: Questionnaire Results 73
Appendix B: Usability Test Questionnaire 78
Appendix C: Manual Form Used by the Investigators 80
Appendix D: Turnitin Results 81
Appendix E: Screen Shots 82
Appendix F: Evidence Retention Code 85
Appendix G: Technical User Manual 86

List of Figures

Figure 2.1 Digital Forensics Investigation Frameworks 7
Figure 2.2 Paperless Evidence Systems 11
Figure 2.3 Smart Mobile Containers 12
Figure 2.4 Conceptual Model Diagram 14
Figure 3.1 Agile Methodology 18
Figure 4.1 Counter Mode Encryption 25
Figure 4.2 Evidence Decryption 26
Figure 4.3 System Architecture 27
Figure 4.4 Context Diagram 28
Figure 4.5 Dataflow Diagram Level 1 29
Figure 4.6 Use Case Diagram 30
Figure 4.7 Sequence Diagram 35
Figure 4.8 Class Diagram 36
Figure 4.9 Entity Relationship Diagram 37
Figure 4.10 Add Case 42
Figure 4.11 Encryption form 43
Figure 4.12 Decryption Module 44
Figure 4.13 Reports Module 45
Figure 5.1 URL Security 47
Figure 5.2 Linux File Permissions 48
Figure 5.3 Dashboard 49
Figure 5.4 Adding a Case 50
Figure 5.5 Documenting Evidence 51
Figure 5.6 Encrypted Database 51
Figure 5.7 Sample Evidence Files 51
Figure 5.8 List of Evidences 52
Figure 5.9 Decryption of Evidence 53
Figure 5.10 Decrypting Evidence 54
Figure 5.11 Successful Decryption 54
Figure 5.12 Failed Decryption 55
Figure 5.13 Decryption of Evidence 55
Figure 5.14 Evidence Report 56

Figure 5.15 Password protected Evidence Documents 56
Figure 5.16 Reports 57
Figure 5.17 Document Number 57
Figure 5.18 Report 58
Figure 5.19 User Activity Logs 59
Figure 5.20 API Interface 59
Figure 5.21 Functionality Tests 61
Figure 5.22 Non-Functionality Test Results 61
Figure 5.23 Implementation Results 63
Figure 5.24 Compatibility Test Results 63

List of Tables

Table 4.4.1 Login Use Case 31
Table 4.4.2 Add Investigator Use Case 32
Table 4.4.3 Add Evidence Use Case 33
Table 4.4.4 Add Evidence Use Case 34
Table 4.5 Users Table 38

List of Abbreviations

AES	-	Advanced Encryption Standard
API	-	Application Programming Interface
CBC	-	Cipher Block Chaining
CSS	-	Cascading Style Sheets
DoD	-	Department of Defense
ERD		Entity Relationship Diagram
GDPR	-	General Data Protection Regulation
HTML	-	Hypertext Markup Language
ISO/IEC	-	International Organization for Standardization/International Electrotechnical Commission
IV	-	Initialisation Vector
URL	-	Uniform Resource Locator
MVC	-	Model View Architecture
PHP	-	Hypertext Preprocessor
PDF	-	Portable Document Format

Acknowledgements

I would like to acknowledge my supervisor Dr Humphrey Njogu whose guidance, dedication and insight was been instrumental in conducting research and preparing this dissertation document; @iLabAfrica, for granting us this opportunity. I would also want to acknowledge classmates, colleagues, who offered encouragement and positive critique during the entire duration in which I carried out this research; finally, my mum Ann Warutumo for always believing in me and regularly reminding me the value of prayer and self-belief.

Chapter 1: Introduction

1.1 Background

Cybercrime is the use of a computer as an instrument or a victim to further illegal ends such as committing fraud, stealing identities and violating privacy (Norton, 2017). Cybercrime also referred to as computer crime is of three different forms namely computer as a target, computer as a tool or computer as an accomplice to crime (International Telecommunications Union, 2017). Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government. This is a result of the development and improvement of information technology over the years (Interpol, 2016).

The development and improvement of information technology have impacted on the openness of various forms of cybercrimes committed by individuals and groups. Cybercrime is a serious threat to individuals, institutions and countries in which the amount of losses globally might equal to national income of a country. For instance, in the first half of 2017, there were 78,238 cases of cybercrime and the number increased to 144,284 in the first half of 2016 in the world (PWC, 2018). It is estimated that cybercrime damages will cost the world an amount equivalent to six trillion dollars annually by 2021 (Herjavec Group, 2017). However, this only pertains to what is reported and a lot remains unreported. This has led to an increase of the demand for digital forensics in determining court cases.

Digital forensics is defined as a scientific knowledge and methods applied to the identification, acquisition, preservation, examination, and analysis of information stored or transmitted in binary form in a manner acceptable for application in legal matters (Casey, 2011). Digital evidence is defined as information and data of value to an investigation that is stored on, received or transmitted by an electronic device (Carrier & Spafford, 2004).

Digital evidence integrity is key in investigations (United States Department of Justice, 2002). Digital evidence integrity is done through evidence preservation by investigators to enhance security of evidence. Evidence preservation is done using hashing, encryption and drive imaging (United States Department of Justice, 2002). Evidence preservation should be maintained in accordance with the condition when it was first discovered until later presented in the court. Evidence integrity has to be maintained throughout the process of acquisition, collection, analysis of evidence, time records as well as contextual information, which

includes case labelling, and the unit and laboratory that process evidence (Prayudi & Azhari, 2015).

As a result of digital advancement, digital evidence has become very important to the law enforcement agencies when conducting investigations and to the judges in the courts while delivering the verdict in cases. Laws such as the GDPR have been the main countermeasure against cybercrime (Goddard, 2017). This has necessitated the developments of acts of law to govern how evidence is handled around the world.

There are existing solutions which attempt to maintain the integrity of evidence but they fail short. Some of the challenges include, they do not offer authentication procedures, they are very costly, the user interface is not friendly to the users as they do not have a graphical user interface and they do not provide user activity logs to ensure follow up in case the system is compromised (Irons & Ophoff, 2016). Examples of some of the existing solutions include Encase, Paperless Evidence Tool and Smart Containers Evidence Tool. These gaps were addressed in the developed tool effectively (Carrier & Spafford, 2004). The main countermeasure for cybercrime advancement has been laws to govern the handling of evidence. Therefore, there exists a need for a technological solution in the form of a web-based evidence security tool which will preserve the integrity of evidence.

The focus of the study revolves around the integrity of evidence. The integrity of evidence is key in prosecuting criminals (Guo, Slay, & Beckett, 2009). This is attributed to evidence tampering often done by investigators either unknowingly or knowingly (Anuradha, 2013). This research will come up with a solution to help solve the loss of integrity of evidence especially in the acquisition phase of digital forensics investigation. It is in the acquisition phase where evidence is most likely to be tampered with (Casey, 2011).

1.2 Problem Statement

Investigators face problems in preserving the integrity of evidence at the acquisition phase of digital forensics investigations. Some of the problems include failure to applying secure processes during evidence acquisition which results to corrupted evidence (Kiarie, 2014). Existing solutions are costly, the user interface is not friendly and they secure the integrity of evidence by using outdated methodologies and technologies (Wangui, 2016). Example of the

existing solutions include; Encase, Paperless evidence tool and Smart container tool; the gap that will be addressed in this study is evidence integrity (Čisar & Maravic, 2011). Lack of preserving the integrity of evidence could result in using corrupted evidence in the courts of law; this could lead to unfair judgement (Walker, 2015).

1.3 General Objective

To develop a forensics tool which will help the investigators in securing digital evidence by assuring the integrity of evidence, specifically in evidence acquisition in digital forensics cases this will result in enabling evidence admissibility in courts hence successful prosecution of cases. The specific objectives are:

Specific Objectives

1. To identify common challenges faced by investigators in maintaining evidence integrity in digital forensics investigations.
2. To review existing solutions used in securing digital evidence.
3. To design, develop and test a tool that helps the investigators in preserving the integrity of evidence.
4. To validate the effectiveness of the tool.

1.4 Research Questions

1. What challenges do the investigators face while preserving the integrity of evidence?
2. What are the gaps in the existing solutions?
3. How can the proposed tool preserve the integrity of evidence?
4. What is the effectiveness of the developed tool?

1.5 Justification

In today's digital society, the issue of evidence security is important considering the number of cybercrime activities that occur (National Digital Forensics Incorporation, 2016). This is one of the consequences of development in information technology and the telecommunication infrastructure improvement that makes it easier to connect every individual to access the internet in an environment that is not limited.

Forensics experts claim that criminals exploit the current situation and committing digital forensics crimes. Additionally, there are many innocent people who could be languishing in prison after being wrongly convicted this is because of having evidence that was altered, resulting to wrong evidence details being documented (Kiarie, 2014).

This dissertation would contribute to the body of knowledge of digital forensics investigations by ensuring that evidence has attributes of integrity, confidentiality and authenticity and by applying comprehensive best practices such as standards in the process of investigations. This would ensure that the evidence is accessible to the law enforcement and admissible to the courts wherever needed. This tool will ensure that evidence is accepted in court and cases determined fairly.

1.6 Scope and Limitations

This dissertation focuses on digital forensics cases. It concentrates on the integrity of digital evidence security in the acquisition phase. However, the tool does not cover conduct identification of evidence, evidence examination and evidence analysis.

Chapter Two

Chapter 2: Literature Review

2.1 Introduction

This chapter explores the literature review with the purpose of identifying the need for an automated tool which enhances the integrity of evidence. This is followed by research on digital forensic frameworks and an overview look at existing solutions that are currently in use.

2.2 Overview of Digital Forensics

Digital forensics is a branch of forensic science which comprises the recovery and investigation of material found in digital devices such as mobile phones and computer hard disk drives. The technical aspect of a digital forensic investigation is divided into computer forensics, network forensics, forensics data analysis and mobile device forensics (Casey, 2011).

There are numerous frameworks A framework is defined as a set of ideas or facts that provide support for something (Merriam Webster, 2014). Digital forensics investigation framework is the basic structure that underlines investigations from the forensics point of view. Frameworks are important as they make investigations easier since they guide the investigators on which process to follow and a lot of research is already done on them making them very suitable for investigations (Interpol, 2016).

Digital forensics has made the digital investigation process automated. It also shortens the turnaround time in the evidence extraction process, thus saving the cost and time of the digital investigation process (Anuradha, 2013).Most of the frameworks contain the five phase processes which are universally accepted. These frameworks are accredited to ISO- 17025 (International Organisation for Standardization, 2017).

Digital forensics is important in structuring investigation findings as well as in identifying relevant patterns of events to be incorporated during the presentation of potential digital evidence. The frameworks also assist law enforcement agencies in determining the validity, weight and admissibility of any potential digital evidence presented (Karie & Venter, 2010). Digital forensics could be of applied investigation of the following aspects:

1. Investigating inappropriate use of computer systems.
2. Investigating a security breach.
3. Detection of disloyal employees.
4. Collecting evidence for disputed dismissals.
5. Helping in malicious file identification.
6. Assisting in investigating theft of information assets.
7. Assist in helping to know the forgeries of documents.

2.3 Understanding Digital Forensics Investigations Process

Digital forensics generally follow a universally accepted five phase process (National Digital Forensics Incorporation, 2016), figure 2.1 shows an image that explains more. The first phase is the identification (Identify) phase, it involves generally means seeking an audience with the crime and the devices involved including determine type of incident or case. The second phase is the preservation phase, data and documents containing evidence are secured in this phase. Preserving digital evidence early in the investigation process, is a critical first step toward increasing the chances of successful investigation, litigation, or incident response (Kamble & Jain, 2015).

The third phase is collection, collection also known as acquisition, involves the data collection, data extraction and recovering data if data is hidden (Walker, 2015). Major activities done in this phase, include collecting equipment containing digital information such as mobile devices and laptops and recording the information on some medium and examination of evidence. Examination of evidence is done on on a copy of the original evidence. The original evidence should be acquired in a manner that protects and preserves the integrity of the evidence (Kamble & Jain, 2015).

The fourth phase is the analysis, it involves the analysis of the collected data to determine the useful data and the unnecessary data to be used in the investigation process. Evidence could be found in unnecessary and necessary data (National Digital Forensics Incorporation, 2016). The analysis stage involves determination of the significance, reconstructing fragments of data and drawing conclusions based on evidence found. During the analysis an investigator usually recovers evidence material using a number of different methodologies and tools, often beginning with recovery of deleted material on the device.

The final phase is reporting and documenting of facts and findings. Main activities done in this phase include summarizing of evidence, preparation of testimonies if needed and documenting of facts and findings; this information is then captured in the report. Facts and findings are reported in a form suitable for nontechnical individuals (Kigwana, Kebande, & Venter, 2017).

Reports may also include audit information and other meta-documentation. (Kamble & Jain, 2015). This stage involves an in-depth systematic search of evidence relating to a suspected crime. The physical and digital evidence is presented in court or to corporate management (Čisar & Maravic, 2011). This dissertation will focus more on the integrity of evidence in the acquisition and reporting phases of the digital forensics' investigations process.

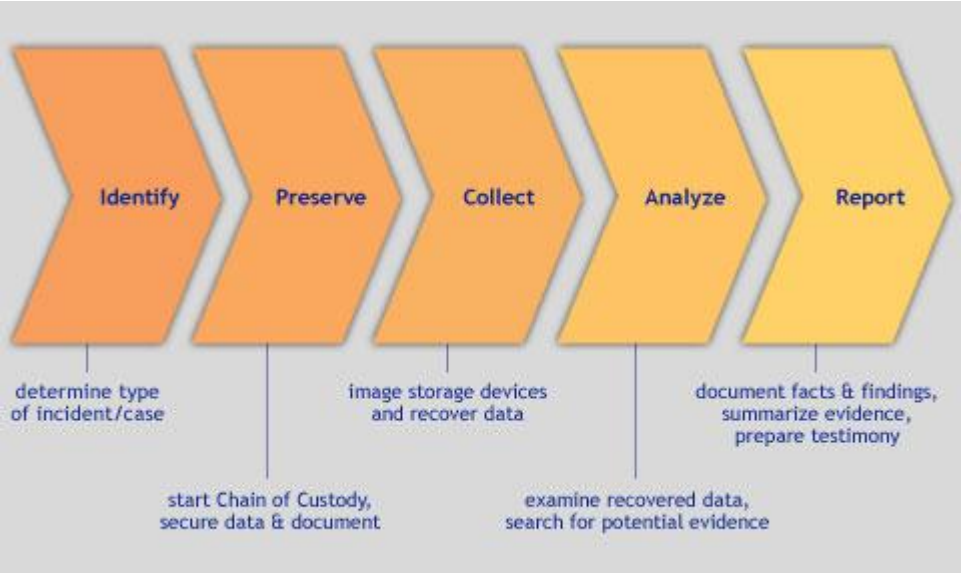


Figure 2.1 Digital Forensics Investigation Frameworks

Source: National Digital Forensics Incorporation, 2016

2.4 Technologies for the Preserving Integrity of Evidence

a) Encryption

This is the process of encoding a message so as only authorised parties can access it. Encryption does not prevent interference but denies the content from being intercepted. Encryption was almost exclusively used only by governments and large enterprises until the late 1970s when the Diffie-Hellman key exchange and RSA algorithms were first published and the first personal computers were introduced. By the mid-1990s, both public key and

private key encryption were being routinely deployed in web browsers and servers to protect sensitive data (Elizabeth & Denning, 2017).

Encryption is now an important part of many products and services, used in the commercial and consumer realms to protect data both while it is in transit and while it is stored, such as on a hard drive, smartphone or flash drive which carry data at rest. Devices like modems, set-top boxes, smartcards and SIM cards all use encryption (Elizabeth & Denning, 2017).

High-risk data is the prime candidate for encryption every step on the way. This includes during acquisition, processing and subsequent storage (RSA or AES). Well-encrypted data is inherently safe; even in cases of a data breach, the data will be useless and irrecoverable to attackers.

b) Data masking

Masking specific areas of data can protect it from disclosure to external malicious sources, and also internal personnel who could potentially use the data. For example, the first 12 digits of a credit card number may be masked within a database (Walker, 2015).

c) Data erasure

There are times when data that is no longer active or used needs to be erased from all systems. For example, if a customer has requested for their name to be removed from a mailing list, the details should be deleted permanently (Elizabeth & Denning, 2017).

d) Data resilience

By creating backup copies of data, organisations can recover data should it be erased or corrupted accidentally or stolen during a data breach (Carrier & Spafford, 2004). Backups are a method of preventing data loss that can often occur either due to user error or technical malfunction. Backups should be regularly made and updated. Regular backups will impose an additional cost to your company, but potential interruptions to your normal business operations will cost even more. Data of low-importance does not have to be backed up as often, but sensitive data does. Such backups should be stored in a safe place, and possibly encrypted. It is advisable not to store sensitive data in the cloud (Gupta & Shrivastava, 2014).

e) Data destruction

Data destruction might not seem like a protection method at a first glance, but in fact it is. The data is being protected this way against unauthorised recovery and access. Under the GDPR (General Data Protection Regulation), you have the obligation to delete data that is not needed. Sensitive data warrants more comprehensive methods of destruction such as degaussing and DoD wipe (International Telecommunications Union, 2017).

Degaussing is a process of decreasing or eliminating a remnant magnetic field stored on tape and disk media such as computer and laptop hard drives, diskettes, reels, cassettes and cartridge tapes (Christensson, 2014). Hard disks are most often destroyed using degaussing, whereas paper documents, compact disks and tape drives are shredded into tiny pieces. On-site data destruction is recommended for sensitive data. Encrypted data can easily be deleted simply by destroying the decryption keys. This guarantees the data will be unreadable, at least the next few decades, after which it will likely become obsolete anyway (Anuradha, 2013).

Types of data destruction include DoD (Department of defense) 5220.22M and data degaussing. DoD 5220.22M was developed by National Industrial Security Program (NISP) of the United States. DoD 5220.22M is a software-based data sanitization method which renders data unrecoverable. Data degaussing, which involves using magnet to erase data on magnetic media such as hard drives or tapes (Ilyas & Zahra, 2014).

f) Pseudonymisation

It is defined as the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to secure data to ensure that the personal data are not attributed to an identified or identifiable natural person (Goddard, 2017).

Pseudonymisation is another method advocated in the GDPR (General Data Protection Regulation) that increases data security and privacy of the individuals. It works well with larger sets of data, and consists of stripping identifying information from snippets of data. For instance, this could be done by replacing the names of persons with randomly generated

strings. The identity of a person and the data they supplied therefore become impossible to link together (Čisar & Maravic, 2011).

2.5 Existing Tools Used in Digital Evidence Security

a) Paperless Evidence Storage for Digital Devices

Danny Bowman, Jason Bowman, David Lewis and Richard Paisley invented a paperless system for identifying and controlling digital devices evidence and managing essential information associated with each device. The tool provides a database that stores information that relates to the device (Khan, 2017). Each device is placed in a forensics lab for forensics examination. An electronic tag is attached to the devices for tracking purposes and for remote non-contact recording and reading of data stored inside those containers (United States of America Patent No. US20020076819A1, 2002).

The tool also provides improved methods for controlling the identity of the devices through coordinating the relay of the evidence remote evidence collection sites and reference laboratories. Managing essential information associated with the devices is done using the electronic memory tags. The evidence is then analysed and then a report is generated. The report generated by the tool contains a summary of events from the time the digital devices arrived in the forensics lab and the evidence that each device has (United States of America Patent No. US20020076819A1, 2002). The limitation of this tool is that it does not produce a system logs showing who was the last person to access the evidence. A diagrammatic illustration is shown in figure 2.2.

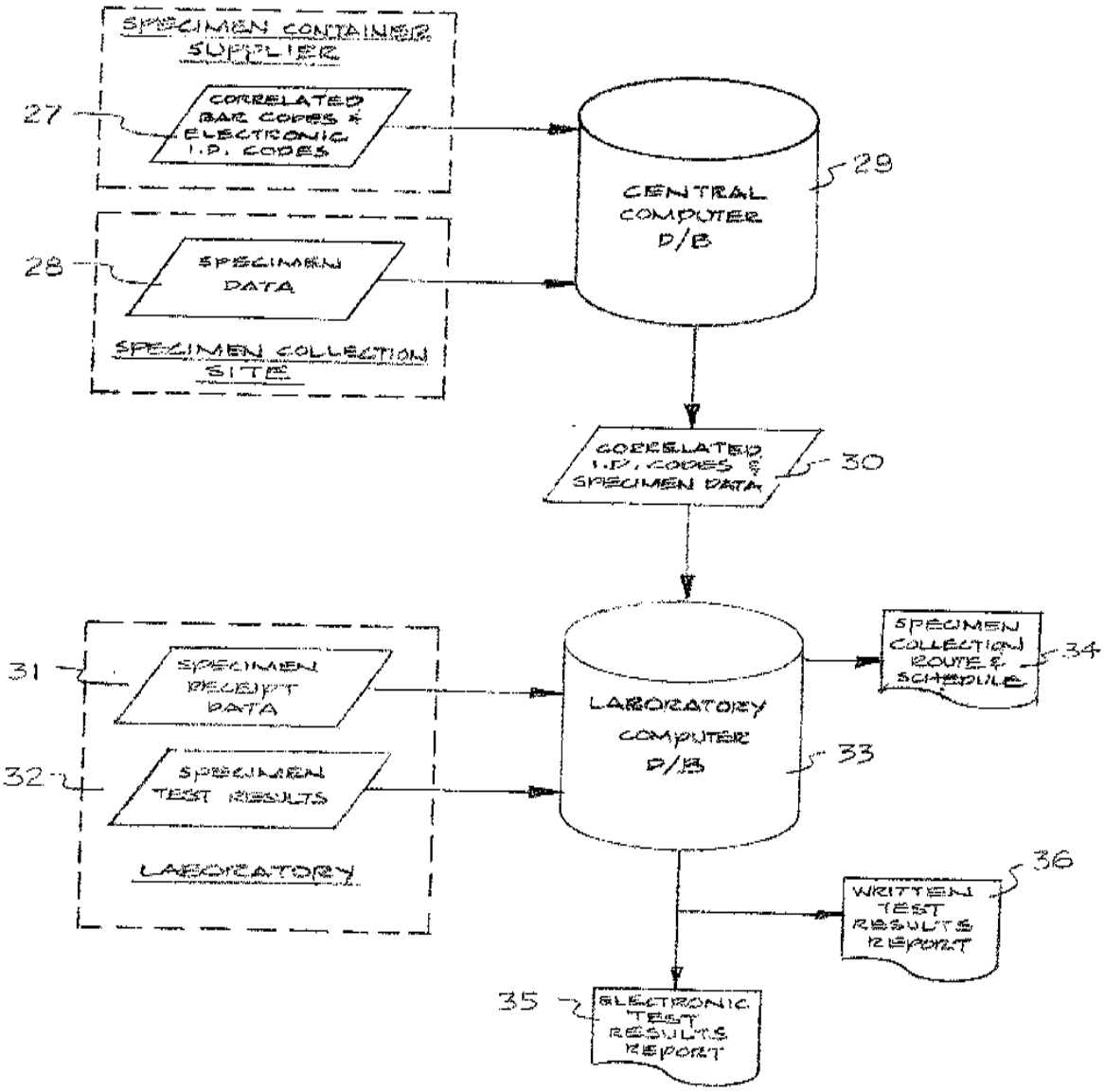


Figure 2.2 Paperless Evidence Systems

Source: Gupta and Mohammed, 2017

b) Smart Mobile Containers for Storing Evidence in Digital Forensics Investigations

Smart Mobile Container is an electronic device, generally connected to other devices or networks through different wireless protocols such as Bluetooth and operate interactively and autonomously (Mohammed & Hamada, 2016). This is an evidence preservation system which uses application specific auditable traceable secure smart mobile containers (SMC) for securely storing evidence items that are collected at crime scenes and search locations pursuant to subpoenas or warrants.

Each SMC includes an electronics package that can read radio frequency (RF) tags applied to evidence bags or totes placed in the SMC or for oversized items, associated with the event or scene, that are tagged with active radio frequency tags. The electronics package also includes condition sensors and radio frequency transmitter module to permit remote reporting and monitoring of GPS/RSSI location and condition of the evidence.

The SMC includes an electronic lock that provides access security and an audit trail of all opening, closing evidence and investigation, and other events related to the crimes during the investigation process up to the time of evidence presentation in a court of law (United States of America Patent No. US8068023B2, 2011). This tool uses the encapsulated approach framework as the smart containers hide the chain of custody. The main limitation for this tool is that it does not produce the chain of custody report. This is illustrated in figure 2.3 diagrammatically.

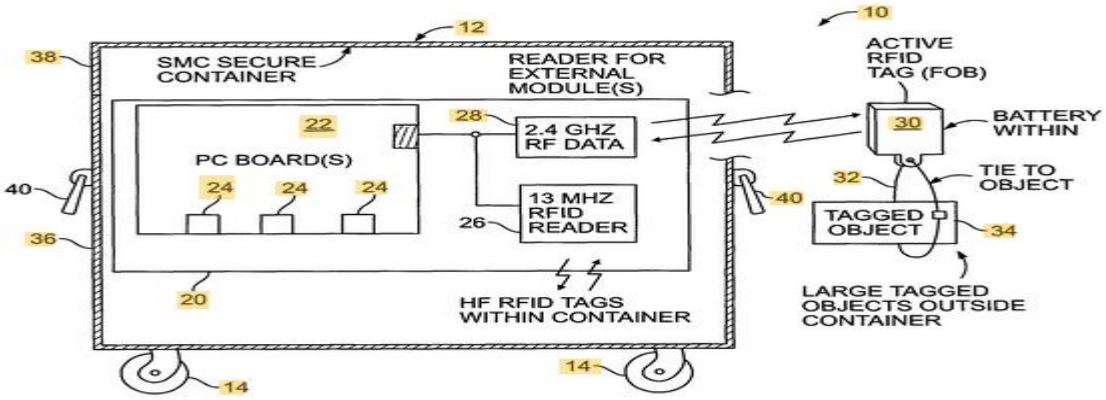


Figure 2.3 Smart Mobile Containers

Source: (Mohammed & Hamada, 2016)

c) Physical Form Method

The cybercrime and forensics unit at the Directorate of Criminal Investigation, uses a manual form to a maintain the digital chain of custody as shown in Appendix D. Forensics tools such as Encase and Xplico are used in the digital investigation process to feed information to the form (Muraya, 2017).

Evidence is stored in storage cabinets and is not accessible to other parties except for those people who are involved in the investigation process. The evidence details are recorded in forms. The forms are distinguished by the case number which is normally unique in all forms.

The form is divided into three parts which capture the description of evidence, change of log or custody and description of the investigation officer. These forms are then presented in courts.

The disadvantage of this methodology is that it does not ensure the security of the chain of custody. The limitation of this method is does not capture such as important data such as time, day and the investigating officers' names which could hinder the admissibility of the evidence report in courts. It does not follow any forensic investigation framework.

d) The Encapsulated Tool

Encapsulated approach framework hides evidence until the phase of reporting where all findings are reported. Encapsulating approach is making the evidence or findings of a certain investigation are only limited to a group of people, who in many cases are the investigating officers. It gives a step-by-step procedure, that is from identification of facts and evidence to presentation of results by the investigating officer in front of investigating organisation (Gupta & Shrivastava, 2014). The main advantage of this framework the security that it provides to the chain of custody which encompasses of the restricted access to only those investigating officers assigned to the case. The major disadvantage of the framework is that it can be very complex for investigating officers with no experience in encapsulation.

e) Event Based Tool

In an event based digital forensics investigation framework, the investigation model is based on physical crime scene procedures. This tool considers each digital device is considered a digital crime scene. This device acts as the crime scene where the crime was conducted. This model is based on the investigation phases (Carrier & Spafford, 2004).

The phases include readiness, deployment and physical crime scene data collection, presentation of evidence and lastly preservation of the digital device involved. The investigation includes the preservation of the digital device, the search for digital evidence, and the reconstruction of digital information. The focus of the investigation is on the reconstruction of data using evidence so that hypotheses is developed and tested (Carrier & Spafford, 2004).

The main advantage of this framework is that maximum concentration is given to the physical locations which tend to explain more about the digital device found in the crime scene. The major disadvantage is that it only concentrates on the physical crime scene whereas most of the data is found on the digital devices in digital forensic investigations hence important details could be left out in the chain of custody, the chain of custody cannot stand in a court of law.

f) FTK Imager

Forensics toolkit is a computer forensics toolkit abbreviated as Ftk Imager. It is a forensics tool made by AccessData. Digital evidence is secured by calculating message digest algorithm five (MD5) and zipped. This evidence is stored in a report. The limitation of the tool is that there is no functionality that can verify who is extracting the evidence (Walker, 2015).

g) Encase Tool

The encase digital investigations tool made by Guidance Software tool. The limitation of the encase tool is it does not provide the functionality to verify the person who is extracting the evidence and it is does not have a graphical interface, hence the tool is not friendly to users (Prayudi & Azhari, 2015).

2.6 Conceptual Model Diagram

Figure 2.4 shows the conceptual diagram which consists of three phases namely input, processes and outputs. Inputs mainly deal with data that the tool depends on for it to run. The tool needs digital evidence as input. Security is then applied on the input. Security may be applied as encryption, URL obfuscation, secure authentication and confidentiality. Controls are then put in place to enhance the security of data; controls may include data backup and secure system logs.

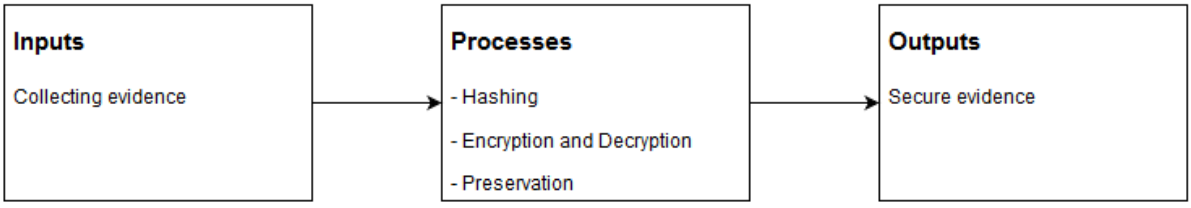


Figure 2.4 Conceptual Model Diagram

2.7 Conclusions

The chapter has indicated various techniques of evidence as well as how current software are using those techniques so as to preserve integrity. Existing solutions include Paperless Evidence Tool, Encase and Ftk Imager. The literature has also revealed that a number of gaps exists to ensure that evidence is secure. The gap includes not having not producing system reports, system logs and lacking authentication while using the tool. The gaps in the later chapters.

Chapter 3: Methodology

3.1 Introduction

This chapter shows various methodologies to be used to meet the research objectives. The research objectives are addressed under the various phases of Agile Methodology. The first and second objective was addressed in the requirements and planning phase. The third objective is addressed in the system design, develop and release phase. Lastly, validation objective was covered in the track and monitor phase. The methodology used is Agile methodology.

3.2 Agile Methodology

A system development methodology refers to the framework that is used to structure, plan and control the process of developing a prototype that intends to solve a problem. It covers many activities from understanding why the system should be built, studying the feasibility of the project as well as looking at other existing tools of a similar nature, analysing problems involved, choosing the system design and architecture, implementing, validating and testing it up to delivering the system to the user as a product (Myers, Badgett, & Sandler, 2012).

Agile software development refers to a group of software development methodologies that are based on similar principles (McLaughlin, 2007). We adopt agile methodology for the following reasons:

1. It is a project management process that encourages frequent inspection of the project and adaptation.
2. It encourages a leadership philosophy that encourages self-organisation and accountability.
3. It encompasses a set of engineering best practices that allow for rapid delivery of high-quality software.
4. It is a business approach that aligns development with customer needs and company goals.

The methodology is broken into phases, diagrammatically shown in figure 3.1 which is explained further below. The phases include:

1. System requirements phase: This phase involves defining the problem, objectives or need that requires resolution and the functional and quality requirements of the system. It involves system designers, developers and users. The requirements include end user functional needs and technical and physical attributes defining operational and engineering parameters.

2. System planning phase: Based on the requirements provided a plan is developed to provide an estimate of project scope and application requirements are done at this phase.

3. System design phase: It involves the actual development of the system through programming, testing, and integration activities. The requirements defined in the first phase is used to establish a baseline of system and subsystem specifications that describe the parts of the system, how they interface, and how the system will be implemented using the chosen hardware, software and network facilities. Generally, the design also includes program and database specifications.

4. System development phase: It involves the development of the system as per the plan, design and requirements of all the stakeholders listed in the first three stages. Various level of testing occurs in this phase to verify and validate what has been developed. This includes all unit and system testing and several iterations of user acceptance testing.

5. System release phase: It involves establishing the actual operation of the new system developed. The final iteration of user acceptance testing and user sign-off is conducted in this phase. The system also may go through checks to ensure that it is effective in meeting its intended objectives as per the requirements phase.

6. System tracking and monitor phase: Following the successful implementation of the system. The system is kept on random checks which may include simultaneous audit to assess the effectiveness of the system in meeting the desired objectives.

Figure 3.1 Agile Methodology

Source: Sommerville, 2015

3.2.1 System Requirements Phase

This was done through garnering initial support from the investigators who are the main stakeholders, this was conducted using questionnaires and the literature review where the gaps in the current solutions are explained in-depth. The investigators who deal with cybercrime and forensics are located at the Directorate of Criminal Investigations, Cybercrime and Forensics Unit Department. This step helped us to understand the problems that the investigators face while conducting digital forensics investigations. A feasibility study was conducted using a questionnaire (see Appendix A).

Five investigators officers were given the questionnaire to fill. The five investigators were selected randomly. This is because a small sample size is manageable, efficient and is able to enhance information accuracy, analysis and efficiency (Hamlin, 2000). The responses guide

in building an initial architecture is modelled and comprises of a general idea which is improved as the system continued being developed.

3.2.2 System Planning Phase

This is done by reviewing the literature review so as to understand how other tools work and understand the aspects being covered and so as to understand the scope not covered. The information collected helps in identifying business needs, project scope, constraints, and system requirements. The scope not covered helps in building the tool.

Information from secondary sources such as journals, conference proceedings and Kenya Judicial Services were vital in helping to build insights on existing systems' weaknesses and strengths as well as the gap exhibited with the current systems. The requirements were analysed to ascertain if they are specific and attainable. Those features that qualified to be incorporated in the system were added while those considered as extras were left out.

3.2.3 System Design

The technique used was the object-oriented technique (Sommervile, 2015). This technique involves grouping of objects into classes where these objects represent a real-world entity. The tool development was divided into modules. The focus of this phase is the designing the specifications of the tool.

The following were used: database schema, conceptual schema, Unified Modelling Language (Rumbaugh, Jacobson, & Booch, 2004), class diagram, data flow diagram level one, context diagram (Rumbaugh, Jacobson, & Booch, 2004) and lastly entity relationship diagram (Rumbaugh, Jacobson, & Booch, 2004) for modelling. The tools used for designing include: Microsoft Visio 2016: It was used in drawing the modelling diagrams used in the design phase of the tool. This tool is owned by Microsoft Incorporation. [1]

The database is important for storing the cases and their evidence, evidence encryption as well as helping in access control. The modelling diagrams were used in this phase are Entity Relationship Diagram (Brunty, 2013)**,** which shows the graphical representation and relationships of database entities (Brunty, 2013). Use Case diagram**,** this diagram shows the

relationships between a user who is also referred to as an actor and a system (Grobler & Louwrens, 2010). Lastly sequence diagrams, this is an interaction diagram that shows object interactions in relation to the time sequence in which the interactions will be used by the system (Teorey, Lightstone, & Nadeau, 2006).

3.2.4 System Development

In this phase, the design was converted into a complete tool. Activities done in this stage includes testing, compiling and debugging code. This phase was allocated most of the time. Those features considered important to be in the system, were incorporated. The following tools were used:

1. Xampp SQL database: It was used in access control as well as evidence storage. It is an open source project which belongs to Apache Friends.[2]
2. Sublime Text 3: This is an editor that was used in writing the code.[3]
3. Laravel PHP Framework version 5.5, It helped in simplifying the development process, it was used.[4]
4. Windows operating system: This is the platform where the above tools were installed. It is owned by Microsoft Corporation. [5]

System Testing

Testing is a crucial step that is taken before an application is deployed. The application is executed so that the errors can be found and debugged to solve the errors. Five testers, selected randomly, tested components of the system. There were five modules in the system each were tested individually with functional, non-functional, structural, security and usability and unit testing methods.

[1]The setup can be downloaded from(https://www.apachefriends.org/download.html).
[2]This is an open source tool which can be downloaded from (https://www.sublimetext.com/download)
[3]The framework can be accessed from (https://laravel.com/docs/5.5).
[4]It is available from (https://www.microsoft.com/en-us/windows/).
[5]The setup can be downloaded from (https://www.microsoft.com/enus/download/confirmation.aspx?id=53055).

a) Functional Testing

Functional testing involves aspects of the tool which directly affects the functioning of the system such as the features (Dumas & Redish, 1999). The functional testing on the tool was conducted on the following aspects:

1. Evidence storage in the system database.
2. Security of the evidence which includes checking on aspects of data encryption, URL obfuscation and password hashing.
3. Installation and deployment of the setup in different environments and platforms.
4. Access control to the system.
5. Test for core application features such as encryption and decryption of evidence, system logs and reports.

b) Non-Functional Testing

These tests are conducted to the application on aspects that are not directly related to the functioning of the system. The non-functional testing of the tool was done to the following areas:

1. Quality assurance was conducted to the source code to ascertain whether it meet logical requirements.
2. Enhancing user interface.
3. Testing on resource optimization in terms of storage and speed in accessing resources.

c) Structural Testing

In structural testing, tests are derived from the knowledge of the software's structure or internal implementation (Sommervile, 2015). Structural testing is critical because the output of the tool is meant for the forensics process. The use of an existing framework helped in reducing the number of errors because the bugs had been identified and improved on. The development process involved constant peer review to counter check the logic of the code.

d) Usability Testing

User testing refers to a technique used in the design process to evaluate a product, feature or prototype with real users (Dumas & Redish, 1999). The primary goal of usability test was to prove that the product can be used in an actual investigation scenario. This can be seen as an

irreplaceable usability practice, since it gives direct input on how real users use the system. This is in contrast with inspection methods where experts use different methods to evaluate a user interface without involving users. Usability testing focuses on measuring a human-made product's capacity to meet its intended purpose (Sommervile, 2015). A total of thirty-three randomly selected users were used to conduct this testing using a questionnaire (see Appendix B) after evaluating a live demo of the system.

e) Unit Testing

This is the most important type of testing (Dumas & Redish, 1999).It involves breaking the program into pieces and subjecting each piece into a series of tests and testing individual modules. The tests were run periodically after every change to the source code to limit future problems (Dumas & Redish, 1999). A set of test cases which focus on the control structure of the procedural design were used. Tests included checking whether the helper classes returned the right results and whether the internal operation of the program performs according to specification.

f) Integration Testing

It is a test that evaluates the connection of two or more components that pass information from one area to another. The objective was to take unit-tested modules and build an integrated structure dictated by design. The term integration testing is also used to refer to tests that verify and validate the functioning of the application under test with other systems, where a set of data is transferred from one system to another (Dumas & Redish, 1999).

g) Compatibility Testing

Tests that were done in the compatibility testing included browser compatibility testing which was the most important compatibility test. It checked compatibility of the three major browsers which are Chrome (version 65.0.3325.181 (Official Build) (64-bit)), Firefox (version 59.0.2 (64-bit)) and Microsoft Edge (version 38.14393.2068.0) to check the compatibility of the software applications. The next test involved the hardware. Checks included software compatibility with the host hardware configuration such as allocated memory and processor time. A network test was also carried out to evaluate the performance of the system in a network with varying parameters such as Bandwidth, Operating speed and Capacity.

3.2.5 System Release

This phase is where system specification was converted into an executable system. This phase deals with addressing these issues that may not have been considered in other phases that came before. In this phase the end user who in this case is the investigators is trained on system use and also given the documentation. The end gets intensive support, hyper-care, required during initial use of the new system. In this phase is where the system is handed over to the support team or the end user (Myers, Badgett, & Sandler, 2012).

3.2.6 System Track and Monitor

System track and monitor deals with collecting the user feedback and work it into the requirements for the next project. This phase was conducted by conducting the validation of the tool, which is the fourth objective of the dissertation. Once the system was complete, system validation is done to ensure that the developed tool tackles the challenge of maintaining the integrity of digital evidence. The system was validated by an investigator of the department of cybercrime of the Kenya Police. The validation included carrying out an assessment to ascertain the ease or difficulty an experienced hacker would have trying to access the evidence and altering it. This objective would effective if the evidence would remain intact despite unauthorized attempts to get it.

Chapter 4: System Design and Architecture

4.1 Overview

This chapter covers the architecture and design of the digital evidence integrity tool, which satisfy all the requirements that were discovered and gathered during the requirement planning and user design phases.

4.2 Functional Requirements

Functional requirements involve aspects of the tool which directly affects the functioning of the system such as the features (Dumas & Redish, 1999). A function is described as a specification of behaviour between outputs and inputs of the system. The functional requirements are derived from the research objective two, which addresses the gaps found in existing systems of a similar nature. The functional requirements of the tool are:

1. Evidence storage in the system database.
2. Security of the evidence which includes checking on aspects of data encryption, URL obfuscation and password hashing.
3. Evidence hashing, file encryption and decryption. This will be implemented using Mcrypt PHP package, the counter mode and AES standard were used for encryption and decryption
4. Access control to the system.
5. Availability of secure reports.

4.2.1 Digital Evidence Encryption

Symmetric encryption was used for evidence encryption as it fairly fast as compared to asymmetric encryption. Symmetric encryption allows for confidentiality and authencity (Terashima, 2002). The PHP package used for the symmetric encryption was MCrypt. MCrypt is a popular data encryption package available for use with PHP. Mcrypt was configured to use the cipher block chaining which is referenced by CBC abbreviation. PHP Mcrypt package will be used is used to generate a key, zip evidence and hash the filename of the evidence file. Mcrypt is a popular data encryption package available for use with PHP (Suzumura & Trent, 2016).

Mcrypt will be configured to use the counter mode (CTR) and AES al. CTR mode turns a block cipher into a stream cipher. It generates a keystream block by encrypting successive

values of a counter. A counter is any function which produces a sequence is guaranteed not to repeat for a long time. CTR is a unique mode since each block is decrypted without depending on other blocks hence making the processes safer and lastly the encryption of blocks can happen in parallel which will increase the performance of the tool (Kaushal & Sobti, 2012). Figure 4.1 illustrates more. Evidence is encrypted using the CTR mode

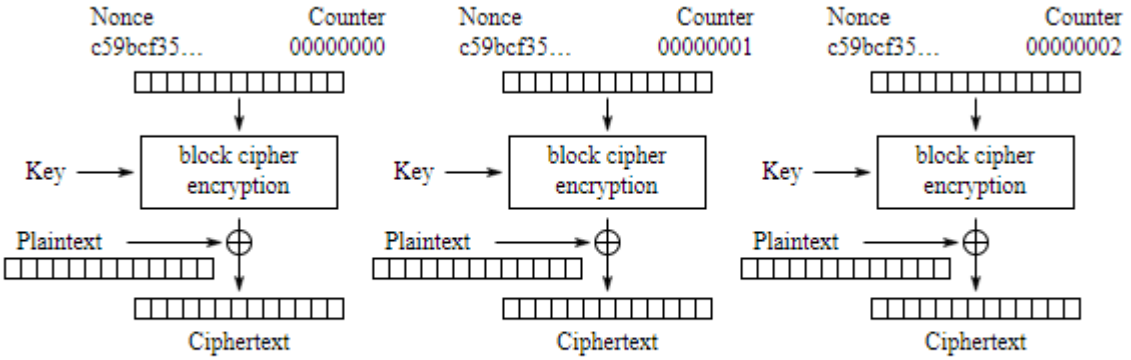


Figure 4.1 Counter Mode Encryption

4.2.2 Digital Evidence Decryption

CTR decryption mode ensures that each block is decrypted independently as shown in figure 4.2, this mode is secure as the IV/nonce is not repeated. Evidence will be decrypted in blocks. The key used to encrypt the evidence, will be the same key to be used during decryption. Decryption will only accessible for the authenticated users. Evidence be decrypted if the user provides a correct key which matches evidence file to be decrypted. A zipped file should be uploaded together with the corresponding key. If the key matches the file, the evidence is decrypted and a zipped file is made available for the user to download it. The evidence needs to have a key. Decrypting evidence with while the user is not authenticated results to failed decryption process. It is important to track the person who was last to alter evidence in order to enhance the integrity of evidence.

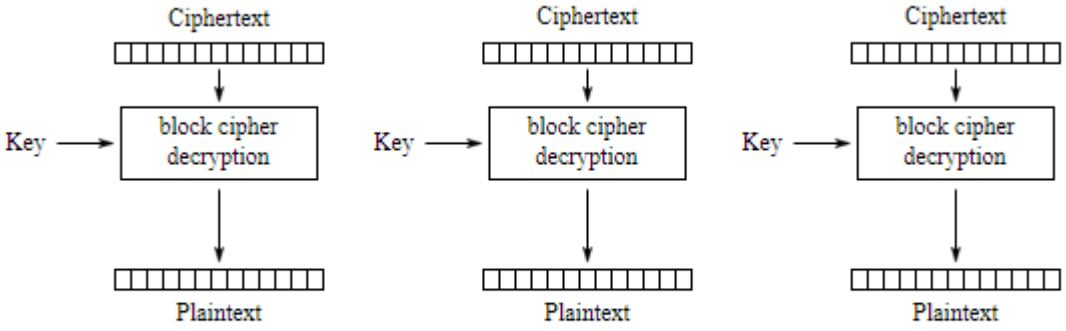


Figure 4.2 Evidence Decryption

4.3 Non-Functional Requirements

These are the functionalities that are not directly related to the core purpose of the system. The non-functional requirements are derived from the research objective one, which addresses the challenges the investigators face while maintaining the integrity of evidence and research objective two which addresses the gaps in the existing systems of the similar nature. They include the following areas:

1. Quality assurance was conducted to the source code to ascertain whether it met logical requirements.
2. Enhancing the user friendliness of the tool in aspects such as the navigation menu
3. Enhancing efficiency in resource usage, to ensure available resources are used optimally.

4.4 System Architecture

The developed system is based on the three-tier architecture; namely the client, application and database tiers. The client tier includes the web browsers installed on client machines. It enables the users of the system to request for resources, upload resources and interact with the system. The application tier is the main layer of the system as it carries the security logic which includes encryption, decryption, hashing and URL obfuscation. It also enables the client to interact with the database. The final tier is composed of a database server which is protected from direct access by the client hosts. The database tier houses all the data (evidence) and files uploaded and requested by end users. Figure 4.3 shows an illustration of the architecture. The inputs are the evidence, the processes applied are encryption (evidence), hashing (Key, evidence file name and password) and decryption of evidence the outputs are secure evidence and reports,

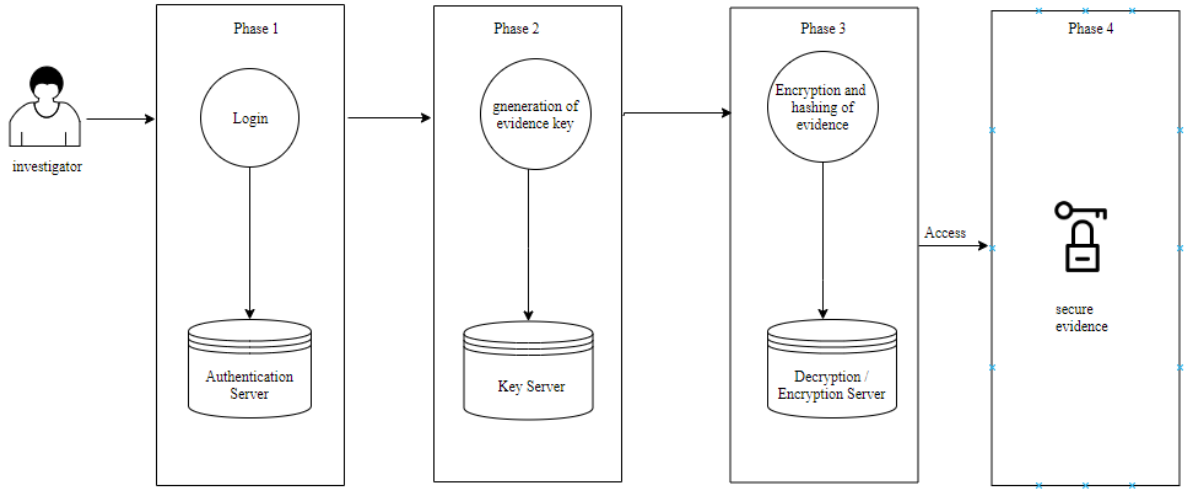


Figure 4.3 System Architecture

4.4.1 Phase 1

The investigator is authenticated into the system, the processes available in the system require that users are authenticated. Authentication server verifies the user details if the user details are correct, phase 2 will be the next step, wrong details will return the user to phase 1.

4.4.2 Phase 2

A key to be used in the evidence encryption is generated, the key is unique to every evidence uploaded, the same key will be used to decrypt the evidence, so it should store in the database.

4.4.3 Phase 3

In phase 3, the evidence is encrypted and then zipped. Evidence is zipped for resource optimization. A hashed filename is then generated and stored in the database. Database details are encrypted.

4.4.4 Phase 4

The evidence is then secure and can be accessed by providing the same key which encrypted the evidence. A report is also made available in this phase, it can be accessed by providing the hash of the evidence key which acts as a password. The importance of hashing is to enhance integrity of the evidence report. The key is stored in the database.

4.5 System Design Tools

This section includes a discussion on the system design which is supported by use case diagram description tables, a sequence diagram, a class diagram and an entity relationship diagram.

4.5.1 Context Diagram

Figure 4.4 shows the relationship between the user and the system. The major inputs in the system involves authentication and evidence collection while the major output involves secure evidence and reports.

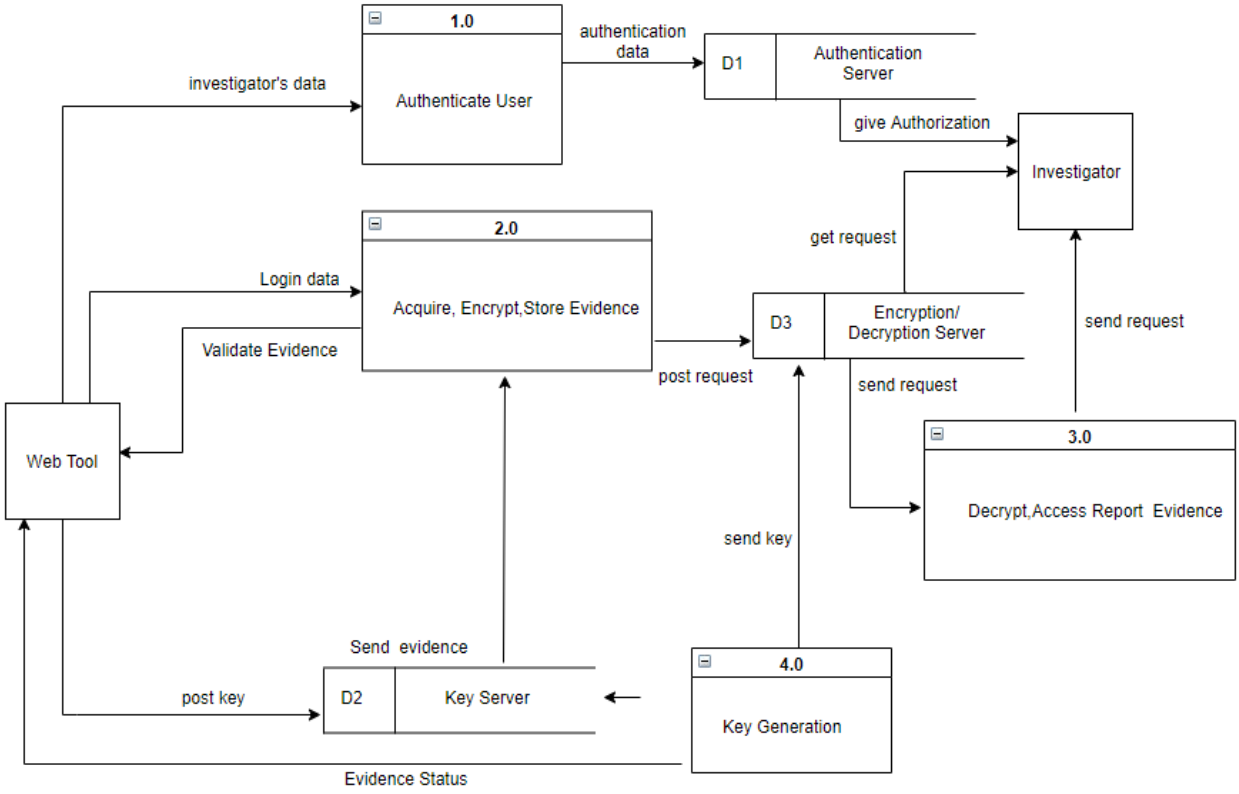


Figure 4.4 Context Diagram

4.5.2 Dataflow Diagram

Figure 4.5 shows the dataflow diagram; the inputs are evidence and investigator's login data. The processes include collection of evidence, evidence encryption and decryption and the outputs are secure evidence.

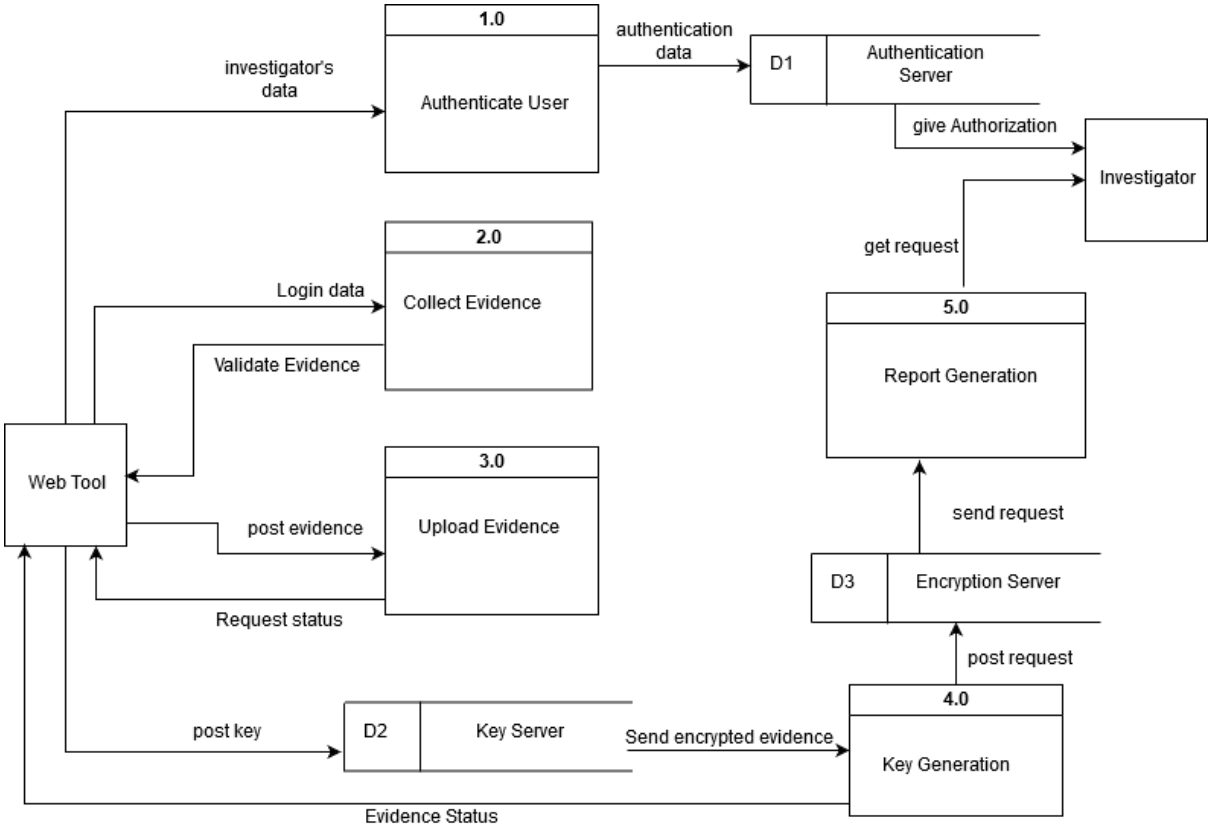


Figure 4.5 Dataflow Diagram Level 1

4.5.3 Use Case Diagram

A use-case diagram shown in figure 4.6, represents the behavior of the system, a subsystem or class. It is more important for visualising, specifying and making systems and subsystems approachable.

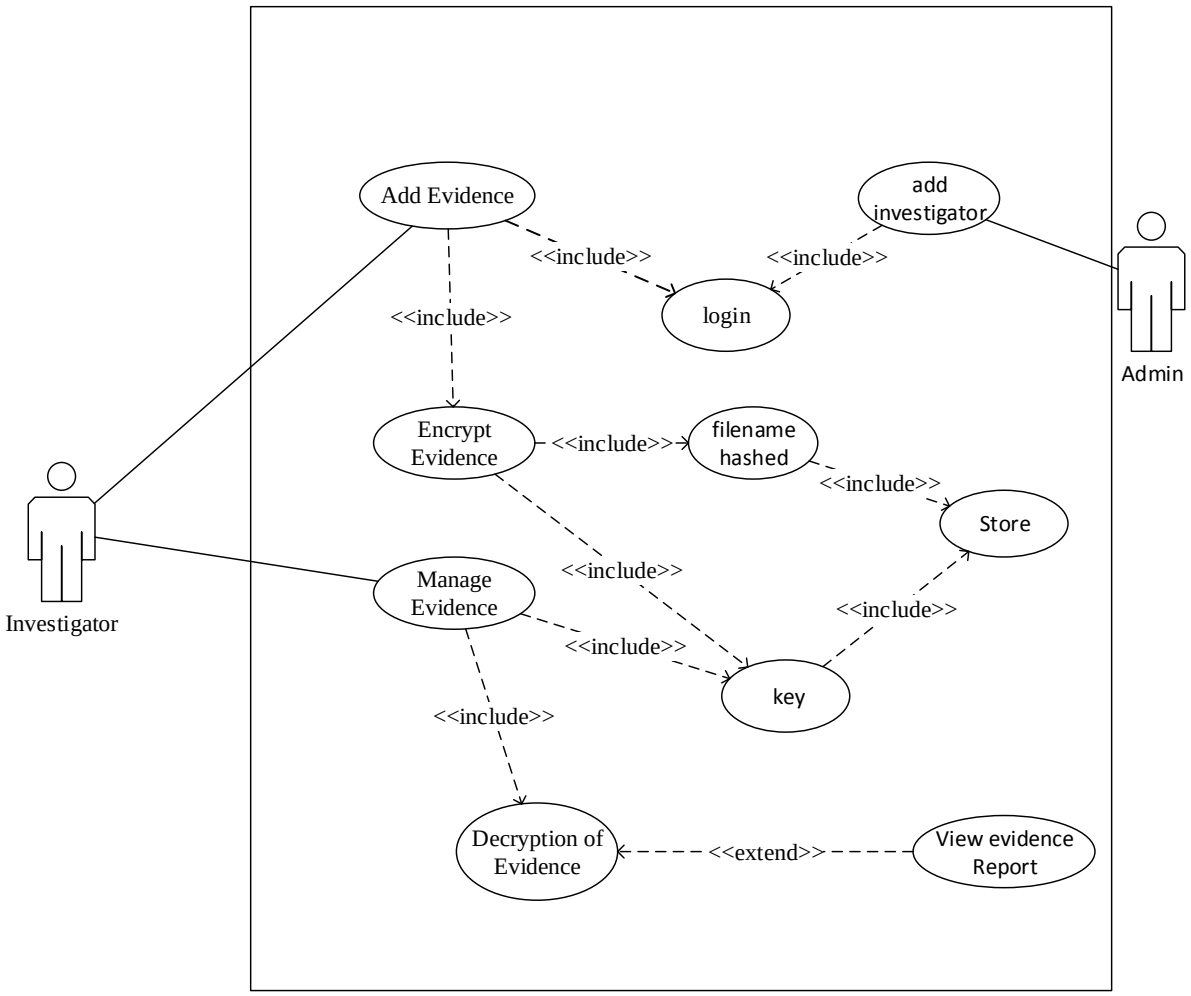


Figure 4.6 Use Case Diagram

4.5.3.1 Use Case Diagram Descriptions

Login Use Case

This use case shows the necessary steps that takes to enable a user get authentication. Table 4.1 shows the steps followed.

Table 4.4.1 Login Use Case

Use Case Name	login
Description	This use case allows for users to log into the system to access the relevant functions based on the user's role. The various user roles are chief investigator and investigator. To log into the system, all users must enter their email addresses and password. Upon successful login, the system displays the homepage.
Actors	Admin / Investigator
Precondition	The user must have an account
Postcondition	The system displays the relevant homepage
Main Flow	1. The user enters the email address, password and the captcha 2. The user submits the email address, password and captcha 3. The system validates the email address, password and captcha 4. The system verifies the email address and password 5. The system authenticates the user, stores user details on the logs and redirects to the homepage 6. User and computer details recorded in the system logs 7. The use case ends
Alternative Flows	3a Missing email address/password or username 1. The system prompts for email address/password or captcha 2. Use case resumes at main flow step 1 4a Invalid email address/password or captcha 1. The system displays "invalid email address/password" message 2. The system prompts for email address/password or captcha 3. Use case resumes at main flow step 1 4. Unsuccessful login recorded in the system logs

Add Investigator Use Case

This use case shows the necessary steps that takes to enable an administrator to add an investigator. Table 4.2 shows the steps followed.

Table 4.4.2 Add Investigator Use Case

Use Case Name	Add Investigator
Description	This use case enables the admin to add investigators in the system. If the user is added successfully, the system displays a success message. When an investigator is added he/she will be able to access the system with the credentials assigned to him/her. The default password assigned can be changed upon firs log in.
Actor	Admin
Precondition	The admin must be authenticated first
Postcondition	The system displays the relevant homepage
Main Flow	1. The admin enters the investigator's email address, username and password 2. The admin submits the email address, password and the username 3. The system validates the email address, password and the username 4. The system sends the investigator's details to the system database. 5. The system then returns a success message. 6. The process above is then captured on the system logs 7. The use case ends
Alternative Flows	3a Missing email address/password or username 1. The system prompts for email address/password or captcha 2. Use case resumes at main flow step 1

Add Evidence Use Case

Table 4.4 shows the use case description for the record cases component.

Table 4.4.3 Add Evidence Use Case

Use Case name:	addEvidence
Description:	The user should add new evidence using the case number.
Actor:	Investigator
Include use case:	1. Evidence is encrypted 2. Evidence Key is generated 3. Evidence is preserved 4. File name is hashed.
Preconditions:	1. User must have been authenticated 2. There must be an existing case
Postconditions:	1. The system displays a success message
Main Flow:	1. The user creates evidence 2. The system creates evidence number. 3. The system encrypts the evidence details. 4. The above activities are then captured in the system logs. 5. The use case ends
Alternative Flows:	1.Evidence details not saved

Manage Evidence Use Case

Table 4.5 shows the use case description for the record cases component.

Table 4.4.4 Add Evidence Use Case

Use Case name:	manageEvidence
Description:	The user should add new evidence using the case number.
Actor:	Investigator
Include use case:	1. The user must have the same key used to encrypt the evidence 2. System activity is stored in the logs
Preconditions:	1. User must have the manage evidence permission 2. Evidence should be approved 3. System updates the database
Postconditions:	1. The system displays a success message
Main Flow:	1. The user creates evidence 2. The system creates evidence number. 3. The key and filename are saved in the database 3. The system encrypts the evidence details. 4. The above activities are then captured in the system logs. 5. The use case ends
Alternative Flows:	1.Evidence details not saved

4.5.4 Sequence Diagram

The sequence diagram in the Figure 4.7, starts from the left where an investigator requests for authentication. The investigator will add evidence to an already existing case. The tool provides a key and the file name is hashed. The user then saves the evidence file and the key alongside the evidence to the database. This information is encrypted and saved to the database. If the investigator wants to decrypt the evidence, the investigator uses the key the decrypt the evidence. A report is then made available provided you have a key that was used to encrypt the evidence. These processes are then captured in the user logs.

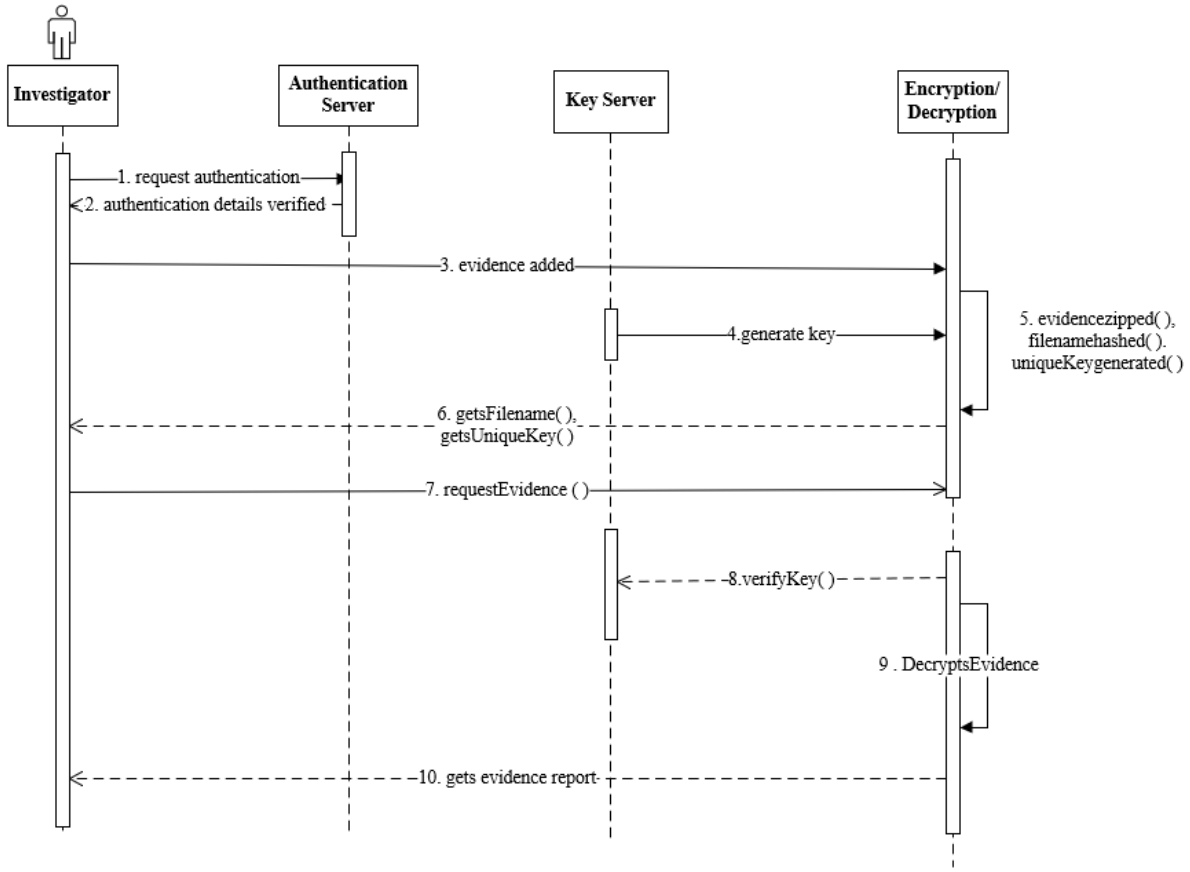


Figure 4.7 Sequence Diagram

The figure 4.8 shows a class diagram of the main classes which are users, evidence, evidencedetails, reports and cases and how they relate. The add, edit and update operations can be done in all tables. The table columns are a mix of integer and varchar character types.

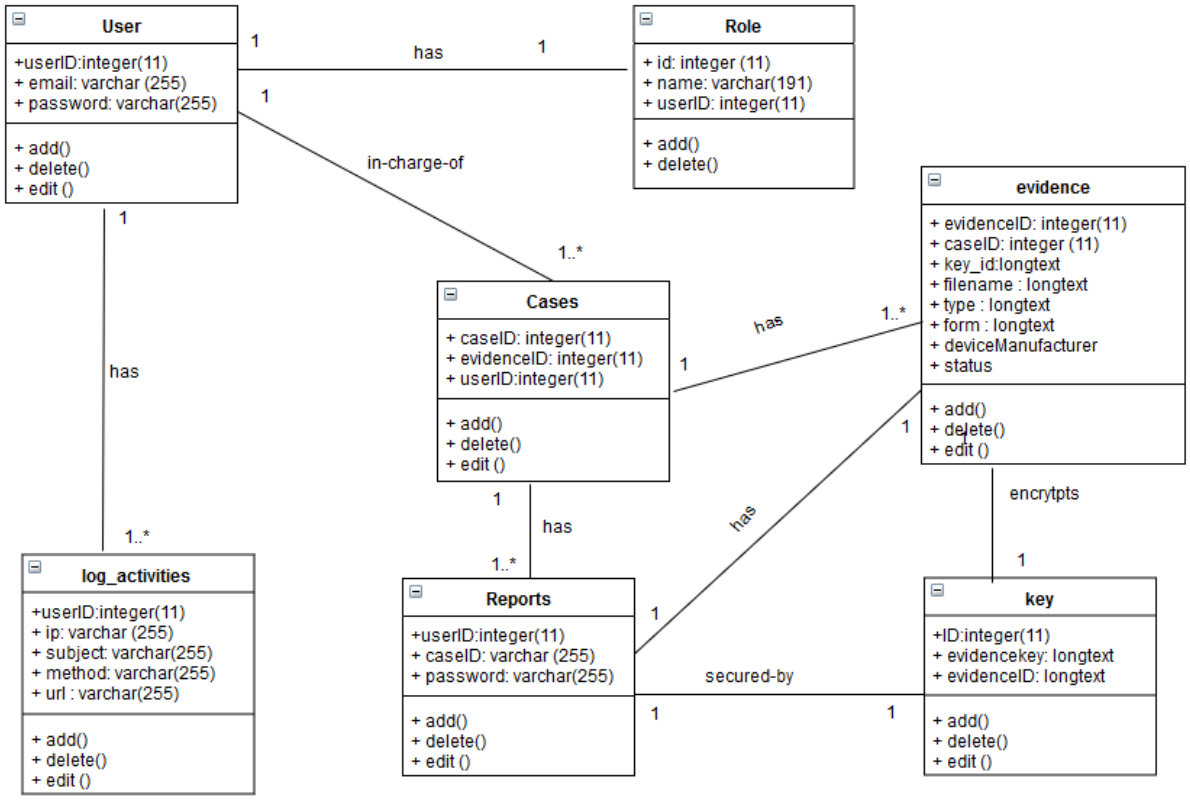


Figure 4.8 Class Diagram

4.5.5 Entity Relationship Diagram

The entity relationship diagram consists of four tables namely evidence, cases, reports and users. The user's table has a relationship with all tables this is because it appears as a foreign key in all tables. The user is also able to add many evidences and many cases. One user can have many log activities. One case can have many evidences. One report contains only evidence. This is illustrated in figure 4.9

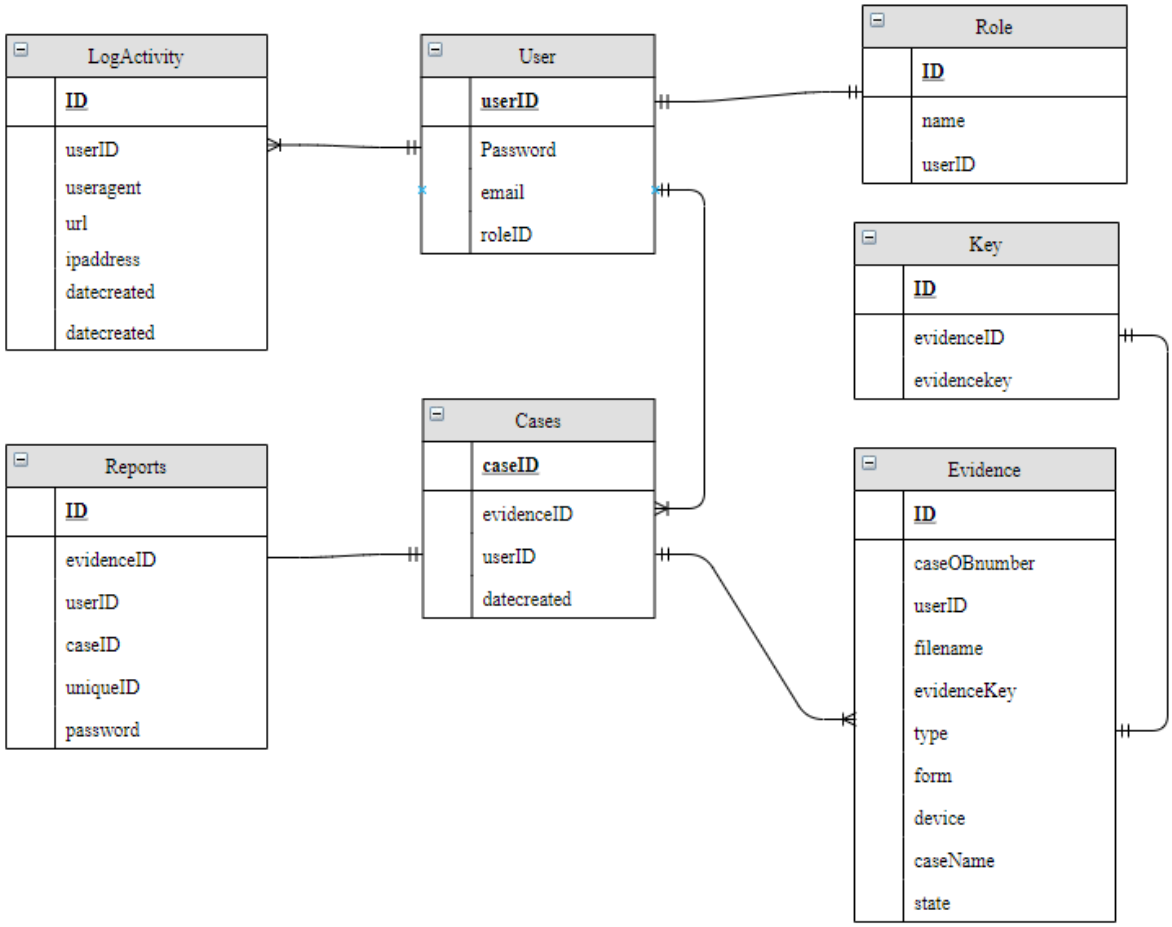


Figure 4.9 Entity Relationship Diagram

The tables below describe the main attributes of the tables contained in the diagram. The foreign key is abbreviated as FK, whereas primary key is abbreviated PK.

Users Table

The table 4.6 shows the users table which holds the user's details.

Table 4.5 Users Table

Field	Data Type (Field Length)	Details	Notes
userID	Integer (11)	AI, PK	Auto increments with every new user registration. It also serves as the primary key for each record
email	Text (255)	UNIQUE	Each active user should have a unique email address that is used during login.
Password	Password		Captures the hashed password field
Role_id	Text (255)		References users table to the roles table

Evidence Table

The table 4.7 show evidence table which holds evidence data.

Table 4.7 Evidence Table

Field	Data Type (Field Length)	Details	Notes
ID	Integer (11)	AI, PK	Auto Increments with every new user registration. It also serves as the primary key for each record
caseOBnumber	Integer (11)	FK	Captures the caseId
userID	Integer (11)	FK	Captures the userID
filename	Text (255)		Captures the filename of the evidence
Created_at	Timestamp		Captures the time which the record was captured.
EvidenceKey	longtext	FK	References this table to the key table.
state	Text (255)		Captures the state of evidence
form	longtext		Captures the form of evidence
type	Text (255)		Captures the type of evidence
DeviceManufacturer	Timestamp		Captures the manufacturer of the device

Cases Table

The table 4.8 show cases table which holds cases data.

Table 4.8 Cases Table

Field	Data Type (Field Length)	Details	Notes
CaseId	Integer (11)	AI, PK	Auto Increments with every new user registration. It also serves as the primary key for each record
Evidence_id	Integer (11)	FK	Captures the Evidence_id
userID	Integer (11)	FK	Captures the userID
name	Text (255)		Captures the name of the case
Created_at	Timestamp		Captures the time which the record was captured.

Key Table

The table 4.9 shows the key table which holds details of digital evidence.

Table 4.9 Keys Table

Field	Data Type (Field Length)	Details	Notes
id	Integer (11)	AI, PK	Auto increments, it serves as the primary key for each record
evidenceID	Integer (191)	FK	References this table to the evidence table
datecreated	Timestamp		Captures the time which the record was captured.
EvidenceKey	longtext		Captures the encrypted key

Roles Table

The table 4.10 shows the roles table which roles data.

Table 4.10 Roles Table

Field	Data Type (Field Length)	Details	Notes
id	Integer (11)	AI, PK	Auto increments, it also serves as the primary key for each record
name	Varchar (191)		It captures the name of the role
datecreated	Timestamp		Captures the time which the record was captured.
userID	longtext		References the user's table

Log Activity Table

Table 4.11 shows the table which holds the user log data.

Table 4.11 Logs Table

Field	Data Type	Details	Notes
id	Integer (11)	AI, PK	Auto Increments. It also serves as the primary key for each record
url	Varchar (191)		Captures the url visited
Time	Timestamp		Captures the time which the record was captured.
ip	Varchar (191)		Captures the ip address
useragent	Varchar (191)		Captures the details of the computer used
userID	Integer (11)	FK	Captures the userID
subject	longtext		Captures the details of the logs
method	longtext		Captures the http method

Reports Table

Table 4.12 shows the table which holds the reports information.

Table 4.12 Logs activity table

Field	Data Type	Details	Notes
id	Integer (11)	AI, PK	Auto Increments with every new rating. It also serves as the primary key for each record
Created at	Timestamp		Captures the time which the record was captured.
uniquid	Varchar (191)		Captures the unique ID of the report
userID	Integer (11)	FK	Captures the userID which retrieved the evidence report
password	Varchar (191)		Captures the password of the report

4.6 Network Design

The network used was the client server network, a client server network is a network where by one centralised and powerful computer called server is connected to a less powerful personal computer. The client server network was chosen as it allows for scalability for the client and centralization of control for the dedicated server. Through the centralisation of control, the integrity of evidence is enhanced as it denies access to unauthorised clients. The network is able to support many investigators as it allows for scalability in the network.

4.7 Security Design

The system has implemented the various controls such as access controls, which are important in handling authentication and authorisation of users. Least privilege principle (PoLP) has been implanted in all the three architectures of the system and will work alongside the access control. This will ensure that users of the system do not have permissions and privileges that they do not need. This is important in auditing user actions in the system and making the users accountable (Kaushal & Sobti, 2012). In addition to the access controls, comprehensive best practices have been adopted in encryption and hashing of evidence. This is important in enhancing data privacy within the system.

The cryptographic protocols have been used in the encryption and decryption processes of evidence. The protocol used is SSH and HTTPS while the encryption algorithm used is AES in conjunction with the CTR mode. The cryptographic protocols are widely used for secure application level data transport. The cryptographic protocols include key establishment, entity authentication, symmetric encryption, secured application level data transport, non-repudiation method, secret sharing methods and lastly secure multi part computation (Kaushal & Sobti, 2012). The design principle implemented is the principle of open design, which states that the security of a mechanism should not depend on the secrecy of its design and implementation (Bishop, 2002). This design was preferred as the investigator could decide to give the key hence compromising the evidence, complexity does not add security.

4.8 Wireframes

Add Case

Figure 4.11 shows wireframe for the add case view.

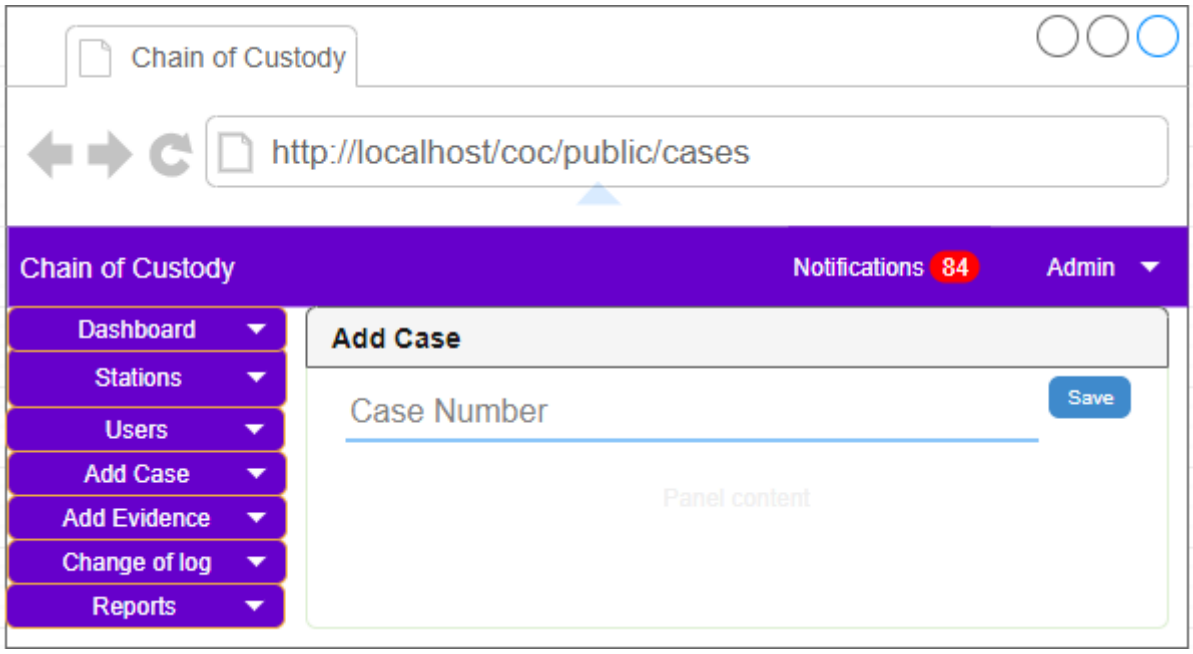


Figure 4.10 Add Case

Evidence encryption

Figure 4.12 shows a wireframe diagram of the page that allows investigators to access the evidence page. The page is divided into four main sections. The first section is the navigation bar located at the left. The second section provided is the encryption form. The form encrypts evidence and produces a unique key and filename which is already hashed. Below the encryption form, the third section which contains a form that enables the user to saves the unique key, filename and evidence key to the database. The final section is the top bar, it displays the logged in user and the number of notifications that the user currently has.

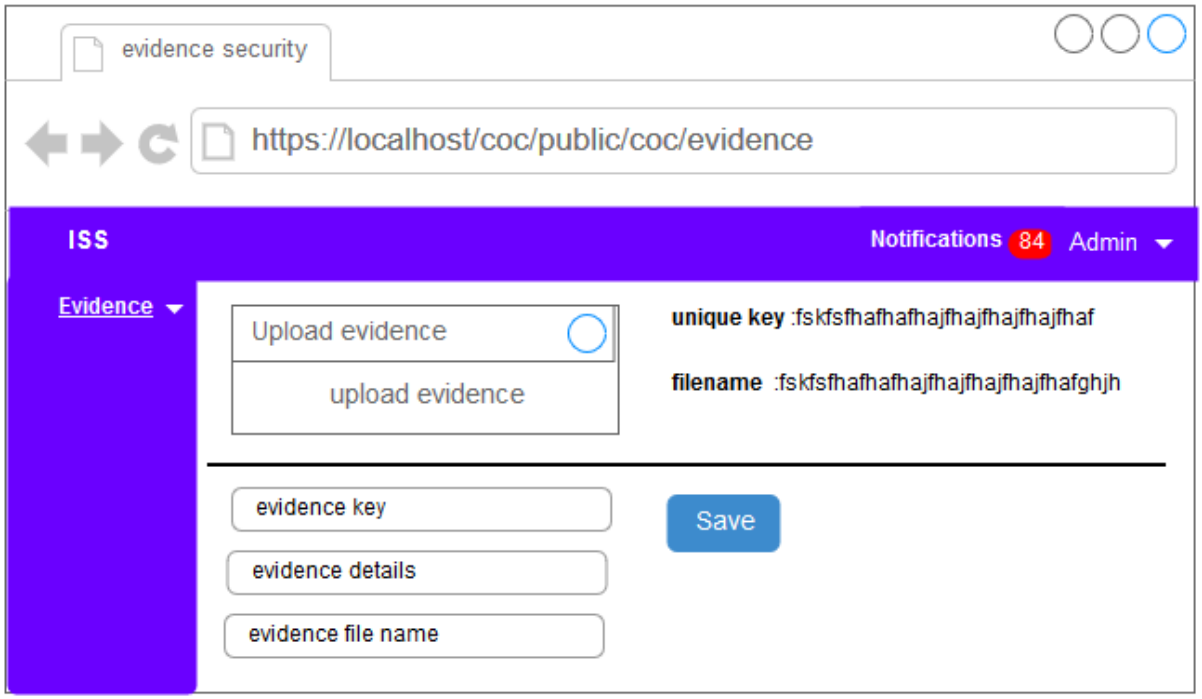


Figure 4.11 Encryption form

Decryption Module

Figure 4.13 shows the module which decrypts evidence. For evidence to be decrypted, a user must upload the decrypted file and also the key. If successful the file will be decrypted using the AES algorithm and the CTR mode that was used.

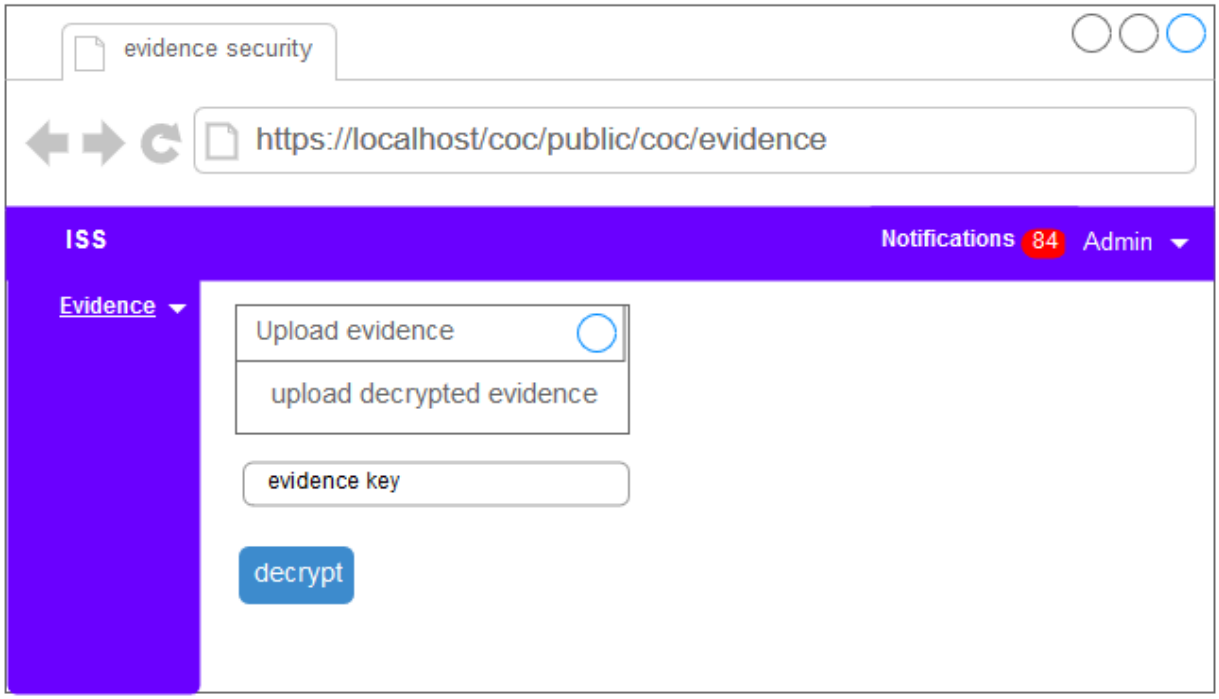


Figure 4.12 Decryption Module

Reports Module

Fig 4.11 shows the module where a user can view available reports. Reports downloaded will require a password.

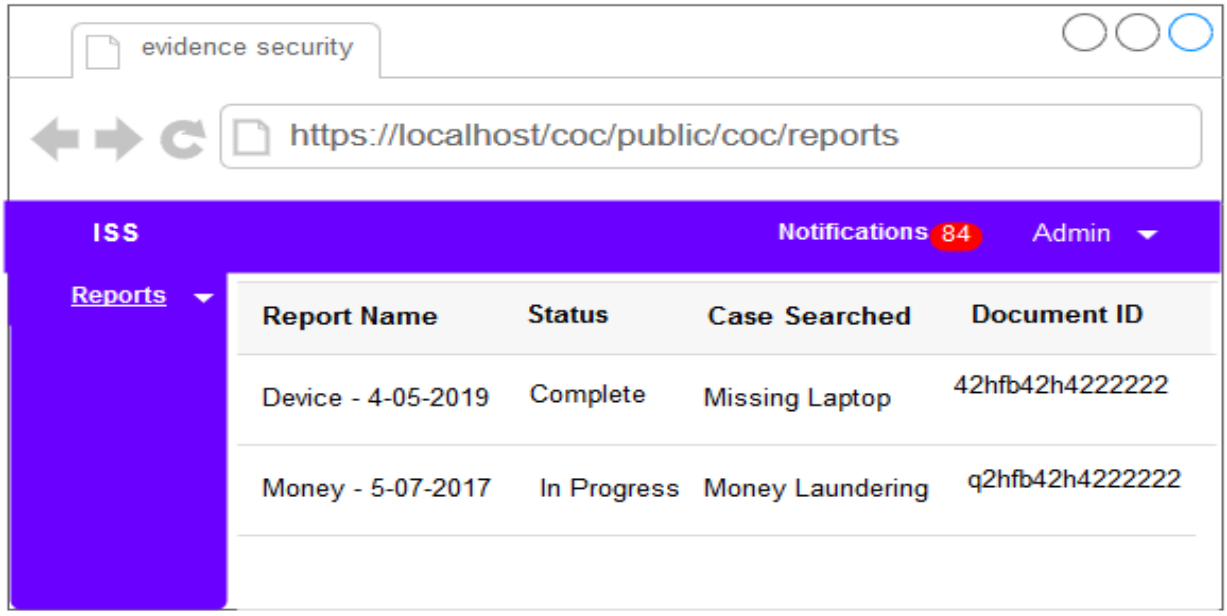


Figure 4.13 Reports Module

Chapter 5: System Implementation and Testing

5.1 Introduction

This chapter discusses the implementation of the evidence security tool and highlights the significant functionalities. This section will include screenshots of important system interface and tests that were carried out on the system.

5.2 Implementation Environment

5.2.1 Hardware Requirements

Minimum requirements needed for the tool to operate optimally are:

1. The processor was dual core with 2.4 GHz speed and was core i5.
2. The computer had an 8GB RAM.
3. The hard drive was of 320 GB capacity.

5.2.2 Software Requirements

Overall, the system is divided into several modules which include user authentication, user management, evidence documentation which involves case and evidence and reports. The following are the software requirements which were used;

a) The developed tool was implemented using PHP v7.0.0. PHP was selected because it is enables server-side software development and that it is platform independent and it is fast as compared to Java and C programming languages (Suzumura & Trent, 2016).

b) Bootstrap version four was used as it includes CSS and HTML and primarily because it offers many design components such as forms, buttons, modals, typography and many others. Bootstrap is an open source framework used for design and fast web development (Dingli & Cassar, 2014).

c) MySQL version 5.1.73. The relational database management system was adopted. MySQL was preferred because it is open source and cross platform (Suzumura & Trent, 2016).

d) The tool was developed using the open source Laravel platform, which uses the MVC architecture and JavaScript. that conforms to the ECMAScript specification (Suzumura & Trent, 2016). JavaScript has curly-bracket syntax, dynamic typing, prototype-based object-orientation, and first-class functions. JavaScript was used as it

has prebuilt functions. Laravel is a free open source PHP framework used to develop web applications using the MVC architecture (Dingli & Cassar, 2014).

e) The platform under which the above softwares were utilised was the windows version ten operating system. Windows was used as it is compatible with many softwares used in the implementation of the project.

5.2.3 Network Requirements

The network used was the client server network, a client server network is a network where by one centralised and powerful computer called server is connected to a less powerful personal computer. The client server network was chosen as it allows for scalability for the client and centralisation of control for the dedicated server. Through the centralisation of control, the integrity of evidence is enhanced as it denies access to unauthorised clients. The network is able to support many investigators as it allows for scalability in the network.

5.2.4 Security Requirements

The system has implemented access controls such as authentication using login, file hashing, database encryption in order to preserve the integrity of evidence. The documents generated by the system are password protected. Hashing has been used in securing the file names of evidence filenames, passwords and the URLs. The primary key is hashed upon record retrieval as shown in figure 5.1.

Figure 5.1 URL Security

(Source: Owner's Work)

The Laravel framework has handled form security, this has been done by. having a token in all forms on the application. This enables protection against SQL injection, cross site request forgery and protection against cross site scripting.

The application was deployed on a Linux server as a control to restrict access to unauthorized people. Linux was chosen as it has comprehensive file permissions as shown in figure 5.2. Virus distribution is very low as compared to other operating systems (Kaspersky Lab, 2019). This is ensured that the application key is protected and cannot be accessed from an outside

source. The file which holds the application key has access levels (700). Permissions were only given to the owner to read, write and execute files. Other groups of users had no permissions at all.

Owner	Group	Other
read & write	read & write	read, write & execute
4+2=6	4+2=6	4+2+1=7

0 – no permission
1 – execute
2 – write
3 – write and execute
4 – read
5 – read and execute
6 – read and write
7 – read, write, and execute

Figure 5.2 Linux File Permissions

Source: (Linux Foundation, 2019)

5.3 System Modules

5.3.1 Dashboard

This page shows the summary of the database contents such as number of cases, evidences, users and stations which are labs of investigations. Graphs to illustrate more are plotted below to illustrate more. Figure 5.3 illustrates more.

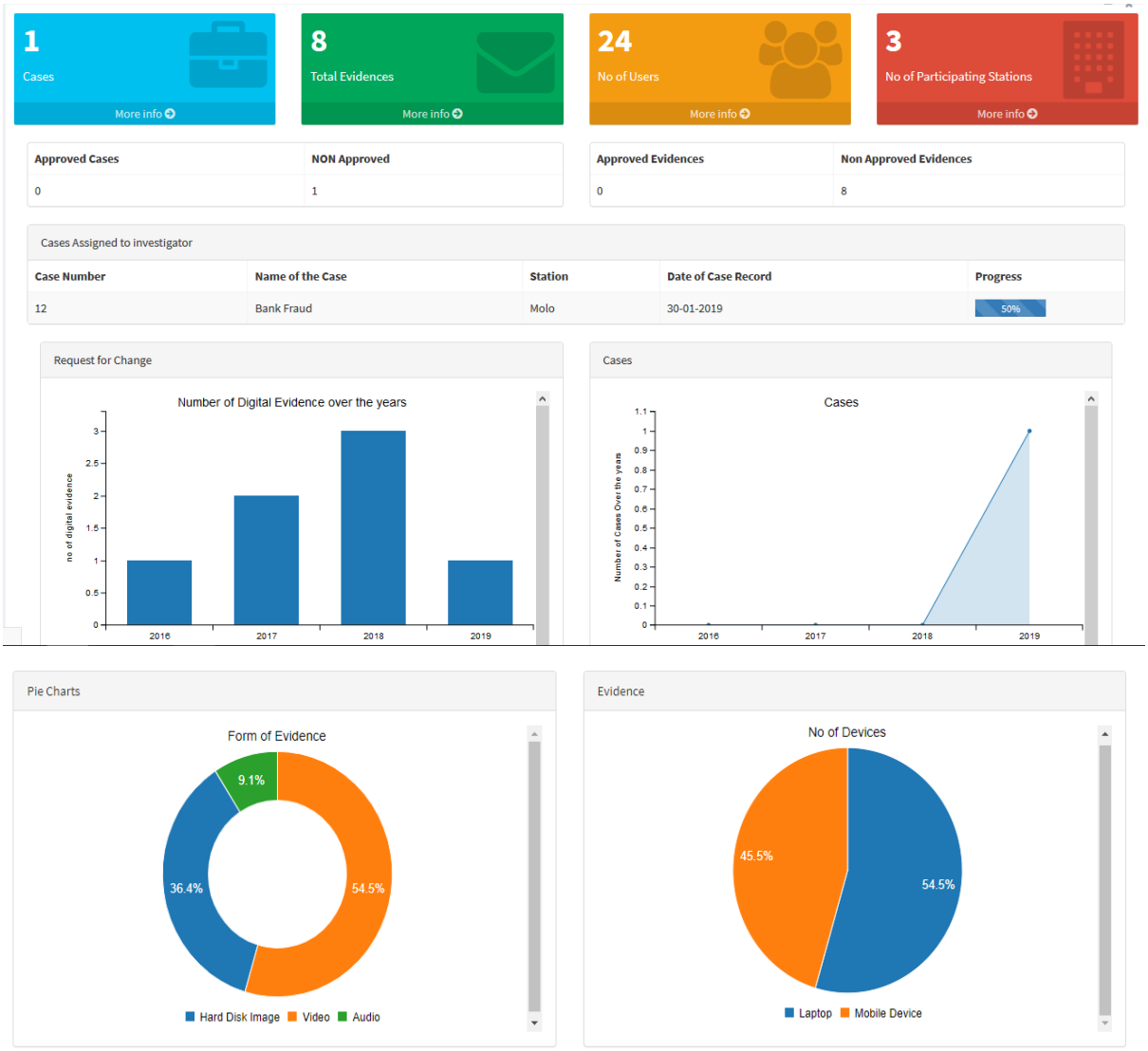


Figure 5.3 Dashboard

5.3.2 Registration and Login

Users are added by an existing user, so as to ensure the privacy of evidence is maintained and to ensure that only authorised users are allowed to use the tool. Existing users are presented with a form which they can use to input their details of a new user. In case the user details are captured in the system, the user is able to log in.

5.3.3 Adding a Case

Evidence can be added only to an existing case, a case is added using the below form, figure 5.4. Once the user submits the form, the form is validated to checks for empty inputs, if there are no empty inputs, general case details are encrypted and saved into the database.

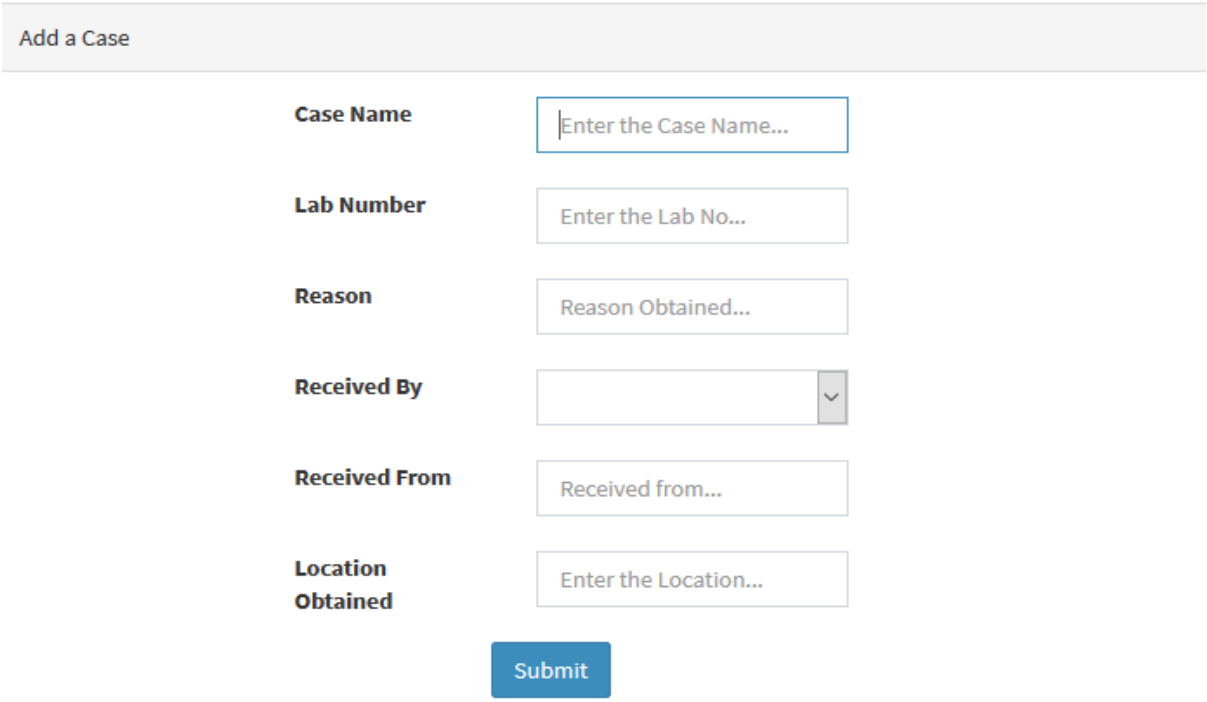


Figure 5.4 Adding a Case

5.3.4 Encrypting Evidence

Evidence is encrypted by passing a key, IV/nonce, encryption algorithm, evidence and the encryption mode. The IV/nonce is random and will be combined together with the counter using any lossless operation (concatenation, addition, or XOR) produce the actual unique counter block for encryption. The key used in evidence encryption is the same key to be used in evidence decryption. The initialization vector is used to ensure distinct ciphertexts are produced even when the same plaintext is encrypted multiple times independently with the same key. The formula used for CTR is where g(i) is any deterministic function, Yi=F (Key, IV + g(i)); IV=token (); and the ciphertext is Plaintext XOR Yi.

Evidence is zipped after decryption and a random file name is generated for the evidence as shown in figure 5.7. Evidence is zipped for resource optimization, zipping reduces file size and the cost of storage (RarLab Corporation, 2019).

The figure 5.5 shows the module that allows for the documentation of evidence in accordance with the case selected. Unique evidence key and filename are generated. The evidence is zipped when the evidence is uploaded in the system. The evidence key, evidence file name and evidence details are inputted in a form as shown in figure 5.5. This information is then saved into the database alongside the evidence details such as type of evidence, form of evidence, state of evidence, manufacturer and the case name. These details are stored in the database while they are already encrypted to preserve integrity as shown in figure 5.6.

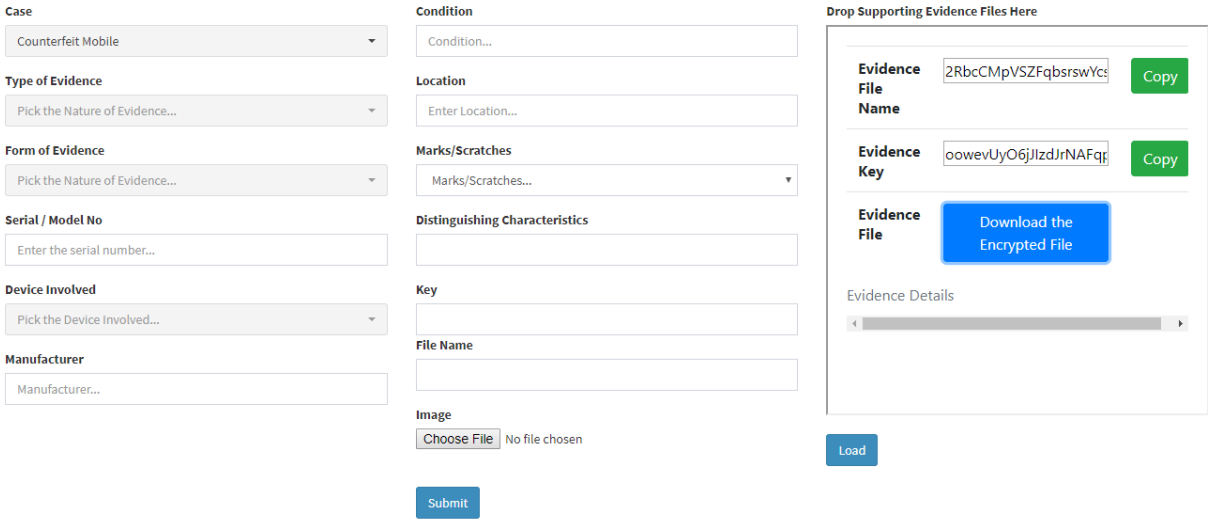


Figure 5.5 Documenting Evidence

form	type	device
eyJpdiI6IlIp5RWR0dGhja3dQdnhhOVJSZkpla2c9PSIsInZhbH...	eyJpdiI6IlVERVFiRW1DZ2FLWFdVcnBBSksxbnc9PSIsInZhbH...	eyJpdiI6ImxURGZXaDNUTURBZEdWZHlOYXdkOGc9PSIsInZhbH...
eyJpdiI6IkJVeVBudDc4VVQ1d0hOajZMcmVNVHc9PSIsInZhbH...	eyJpdiI6InhJcFRhcXFCWm5NYzdmTE9nS3h3Rmc9PSIsInZhbH...	eyJpdiI6IjA4VHVpOEtzd1hEblpTeFFyUFBUNEE9PSIsInZhbH...
eyJpdiI6IlNLY3VlWDQ4MFFrMHNaMjZaK1R3REE9PSIsInZhbH...	eyJpdiI6IkMxSFFUWEhaZWdlMHJ3aCtLWVI0aHc9PSIsInZhbH...	eyJpdiI6IlZZMFwvQkVBYzlvZGFoTXhCcVRiRit3PT0iLCJ2YW...
eyJpdiI6Ik9peE9cL1wvYUg2SWl5QlwvU3k5bUNlYVE9PSIsIn...	eyJpdiI6InVCMXZGRWlid2poOUt3OElQZlZWbXc9PSIsInZhbH...	eyJpdiI6ImdYajlqS29QWUpjMklmZzhGcVUwd2c9PSIsInZhbH...
eyJpdiI6IjFFVlINWVAzN1Y1TWx5TDBVVElUaXc9PSIsInZhbH...	eyJpdiI6Ik4wd2wwSEVSdkc5QXNveERPN2RmbUE9PSIsInZhbH...	eyJpdiI6InRTbWRONkZpXC9iYklGZGxQM1NOdXRRPT0iLCJ2YW...
eyJpdiI6InliT0hpR1NSUnNDeVI5TTdOWkhDQlE9PSIsInZhbH...	eyJpdiI6IkluK2pRcEc2RUxsTmhRQk1lbUhNVkE9PSIsInZhbH...	eyJpdiI6IkZDSE1ueFlQS1FDT25mQVpOSEp1WWc9PSIsInZhbH...
eyJpdiI6IjF1XC9zMVNzK1VzMHIxXC9tNStWZzFBUT09Iiwidm...	eyJpdiI6IkN5bFVpM1JuZ0ZFRVJjdzAwNlwvRmRBPT0iLCJ2YW...	eyJpdiI6IjhsakFrYnV2R3VtNGc5RTVsUWRuWVE9PSIsInZhbH...
eyJpdiI6IjdBblgzQ2dKRXpJNnMzOFJiK1o4eWc9PSIsInZhbH...	eyJpdiI6Im50WTM5QU1QSDFuSnVkT0tyR1djdFE9PSIsInZhbH...	eyJpdiI6IjRBcTRjek1mZ3hVUHJ5cTFJeERTT1E9PSIsInZhbH...

Figure 5.6 Encrypted Database

Name	Date modified	Type	Size
4EYJjZDQwNuOsZmTlr4KEYrMP06usq4d	27-May-19 1:48 PM	WinRAR ZIP archive	372 KB
7KF1OLPuCeFxY0ieoH92rMAin01kXVfB	15-Apr-19 8:31 AM	WinRAR ZIP archive	156 KB
uZLbxakDKQbxdoEeBXVKhrKQKsyCA6nk	17-May-19 11:21 ...	WinRAR ZIP archive	888 KB
z3mQqlZml2wAKo9cBqZ00Q0HfeMQ5egW	22-May-19 2:20 PM	WinRAR ZIP archive	1,309 KB

Figure 5.7 Sample Evidence Files

5.3.5 Decrypting Evidence

All evidences are listed together as shown in figure 5.8. This page is only accessible for the authenticated users. Evidence be decrypted if the user provides a correct key which matches evidence file to be decrypted.

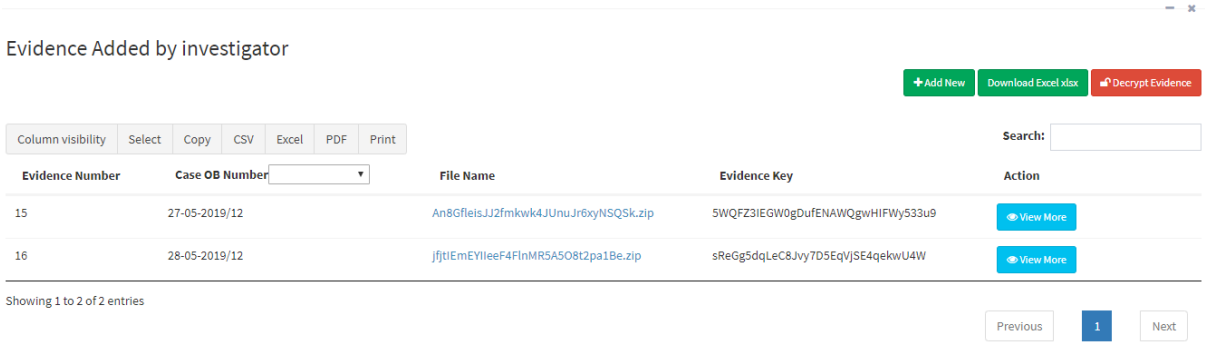
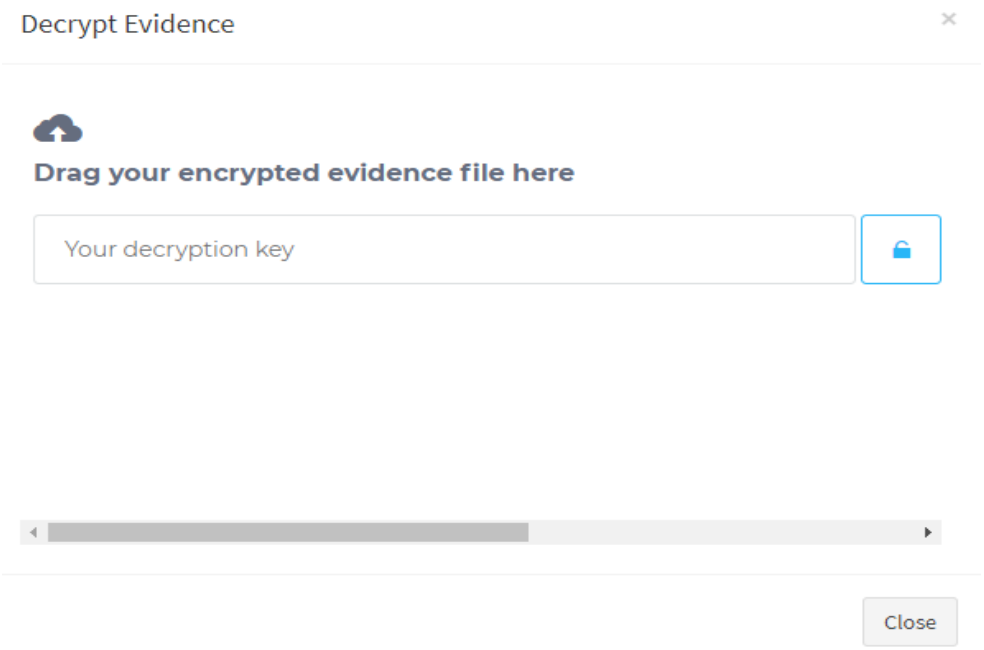


Figure 5.8 List of Evidences

Figure 5.9 shows the modal which displays the field for evidence decryption. A zipped file should be uploaded and the key entered. If the key matches the file, the evidence is decrypted and a zip file with a unique name is made available for the user to download it as shown in figure 5.11. unzipping a decrypted file will unzip a folder without having errors.



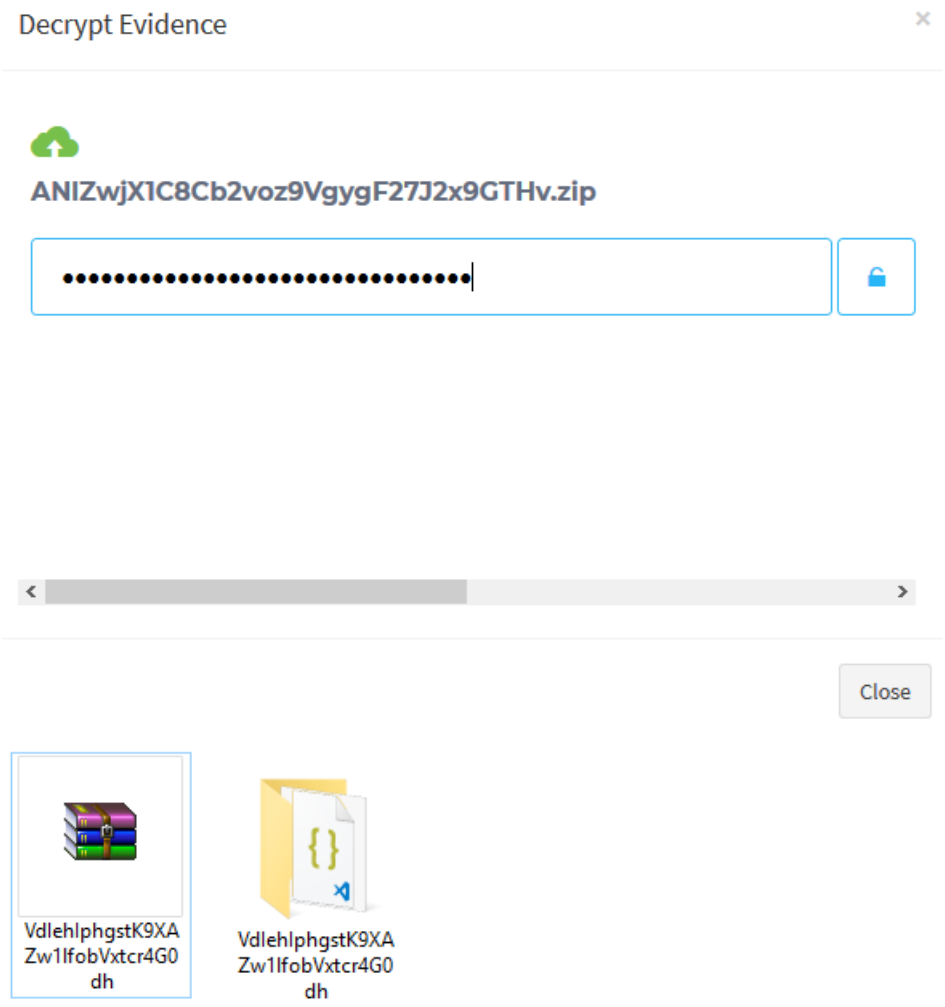


Figure 5.9 Decryption of Evidence

The figure 5.10 below, shows the evidence dialog where decrypted evidence is dropped. The evidence needs to have a key. If a wrong key is used, the message “You entered a wrong key” is displayed as shown as in figure 5.10. Where a correct key is inputted and a corresponding evidence file name, a file name is generated and the user can download the evidence as shown in figure 5.11.

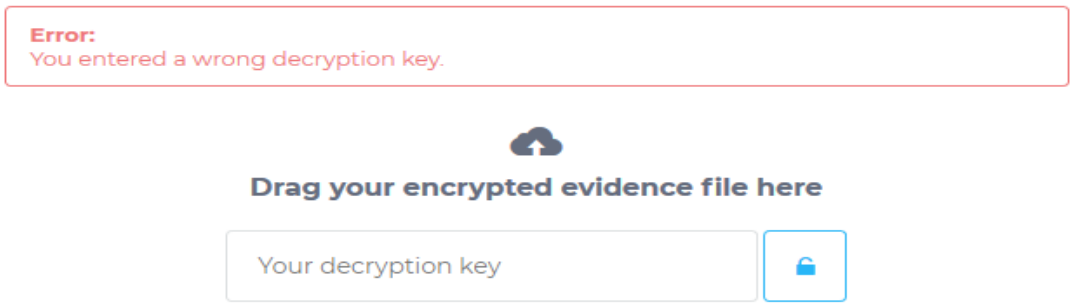


Figure 5.10 Decrypting Evidence

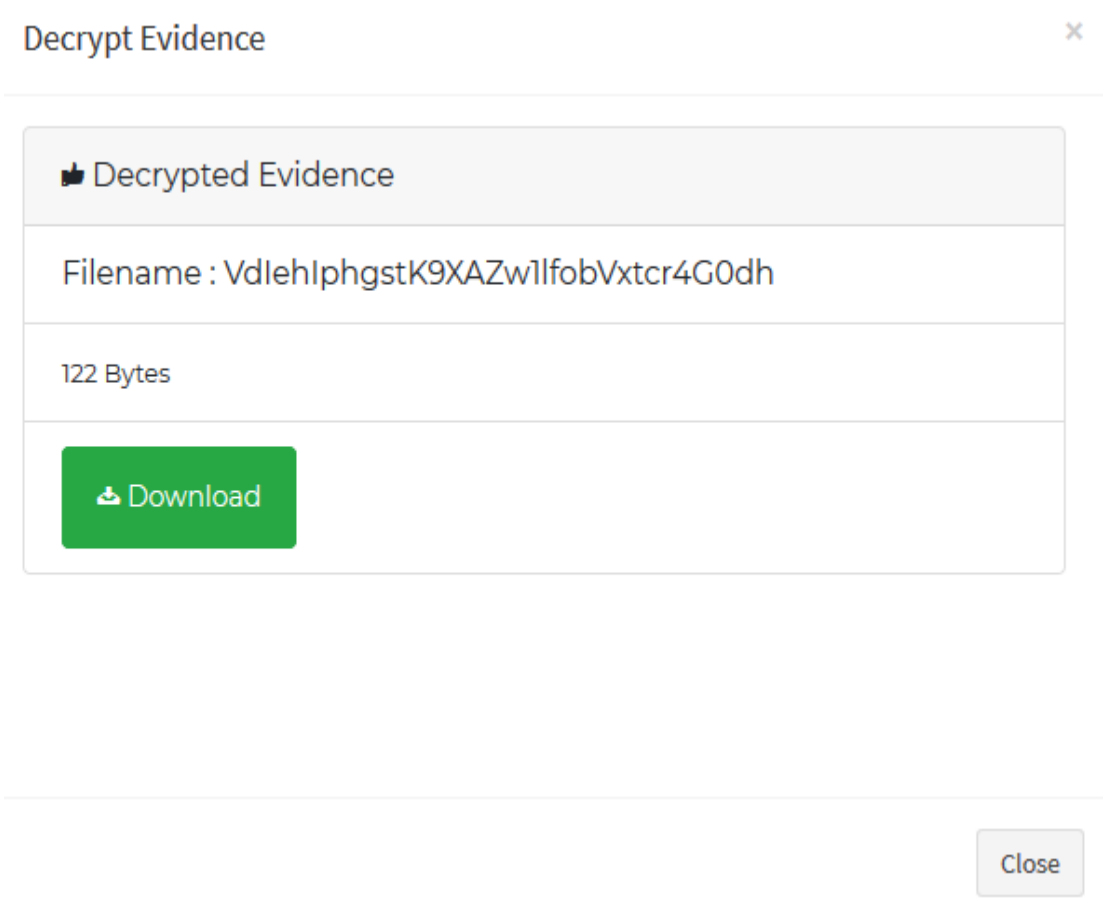


Figure 5.11 Successful Decryption

Decrypting evidence with while the user is not authenticated results to failed decryption process as shown in figure 5.12. It is important to track the person who last altered evidence.

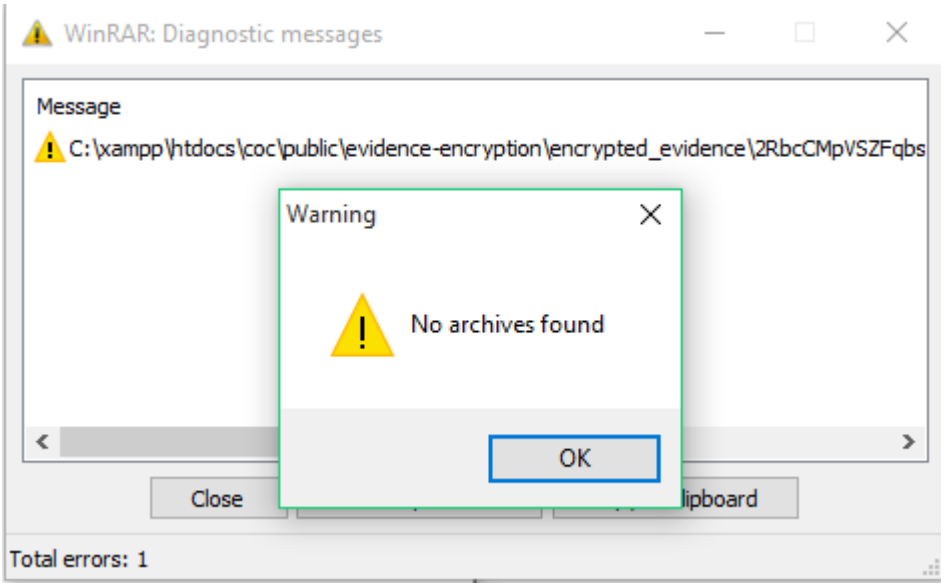


Figure 5.12 Failed Decryption

On successful decryption, the following view should occur as shown in figure 5.13

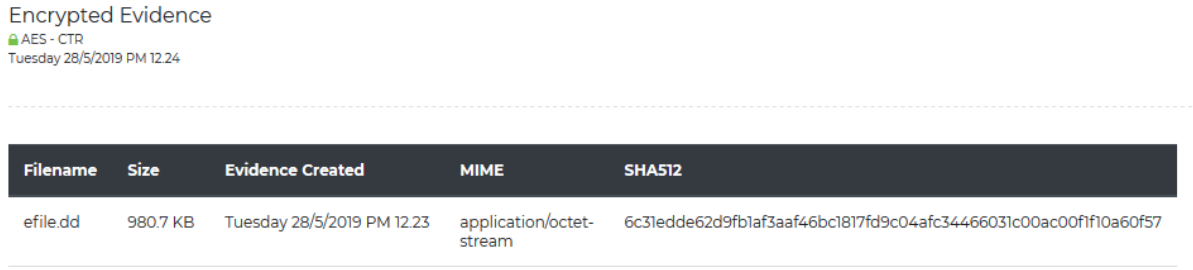


Figure 5.13 Decryption of Evidence

5.3.6 Evidence Reporting

Figure 5.14 below the evidence reporting. This page shows specific evidence details. The report can be downloaded from the pdf button. The pdf would require a password to open report content which is the same key used to decrypt the evidence. The key is hashed using SHA512 and used as a password to be used after the user has downloaded the evidence report as shown in figure 5.15. The report downloaded contains a unique document number which can be used to verify if the report is genuine as shown in figure 5.17. The unique document number is important in validating the origin of the document. Document numbers are stored in the database for verification purposes.

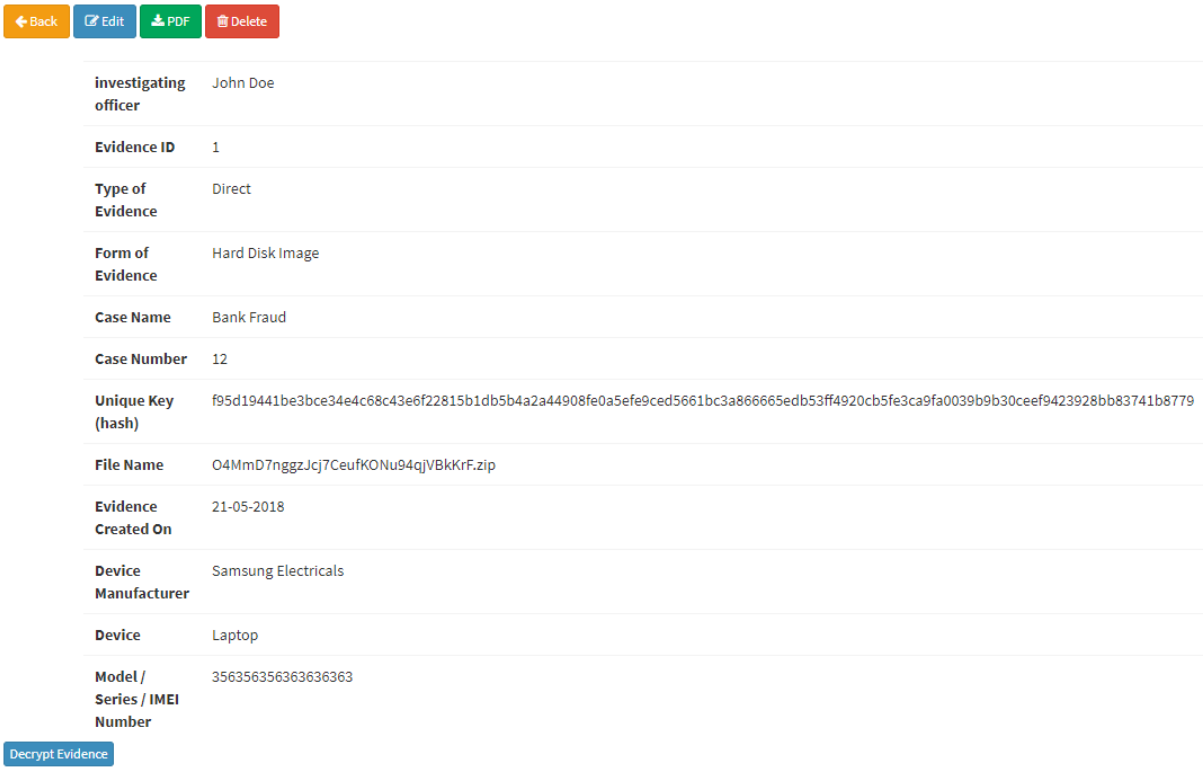


Figure 5.14 Evidence Report

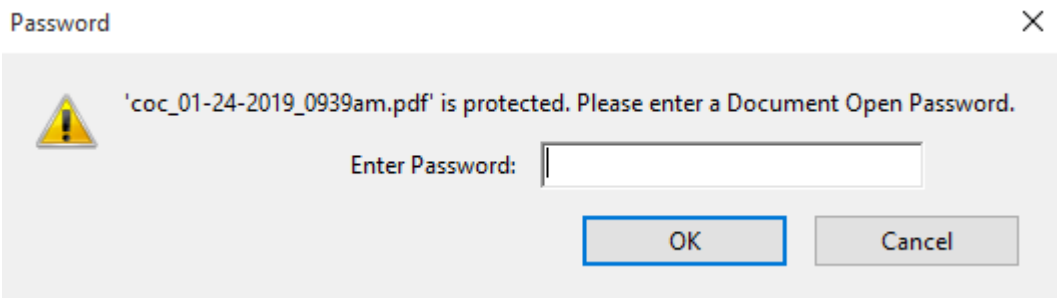


Figure 5.15 Password protected Evidence Documents

Figure 5.16 shows the table that has available reports in the system, the reports will be deemed authentic if the unique document number shown in figure 5.14 appears in the table. Reports are can be downloaded and opened with the hash key of the evidence information that it contains; a sample report is shown in figure 5.18. Reports are PDF/A compliant.

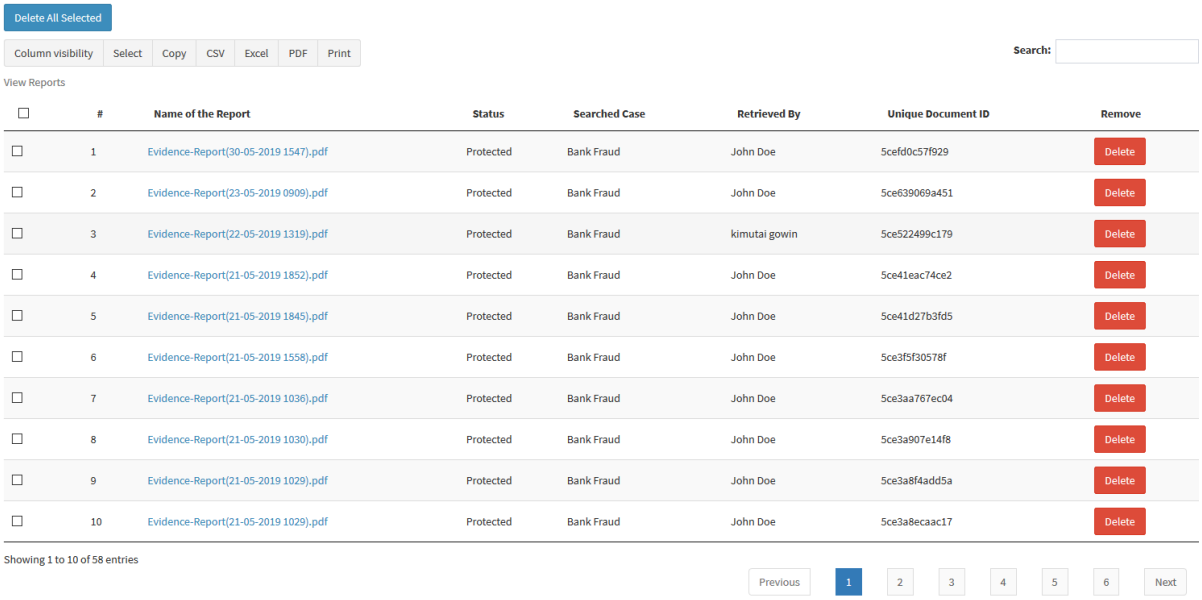


Figure 5.16 Reports

Figure 5.17 Document Number

Document No **5cefa0632f4f9** Report Generated on 30-05-2019 at 12:20 by John Doe

Case Name : test

Case Creation Date : 27-05-2019

Lab : ccu-123

investigating officer	John Doe
URL	http://localhost/coc/public/report-download/k8mep2bMyJ
IP ADDRESS	::1
User Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Evidence ID	7
Type of Evidence	Circumstantial
Evidence Form	Network
Case Name	test
Case Number	1
Unique Key (hash)	147626f4be17779674e9c3f495a2b111e4c8992f0ed068cdfb8fc46b73764a64c20877c888b50e2b958e6c6da80cb0d4253997f64f3ef8b25fcd58fd9518c2a3
File Name	I9rOtsrIaDOfDRavrcMtxU0Snj16TniG.zip
Last Update Done on	2019-05-28 13:25:55
Hash Used	SHA 512
Encryption Algorithm	AES

Figure 5.18 Report

5.3.7 System Logs

The figure 5.19 shows user activity logs. All activity of the user is recorded in a table. They are important in providing an audit trail, which is important in providing a follow in case of a system failure.

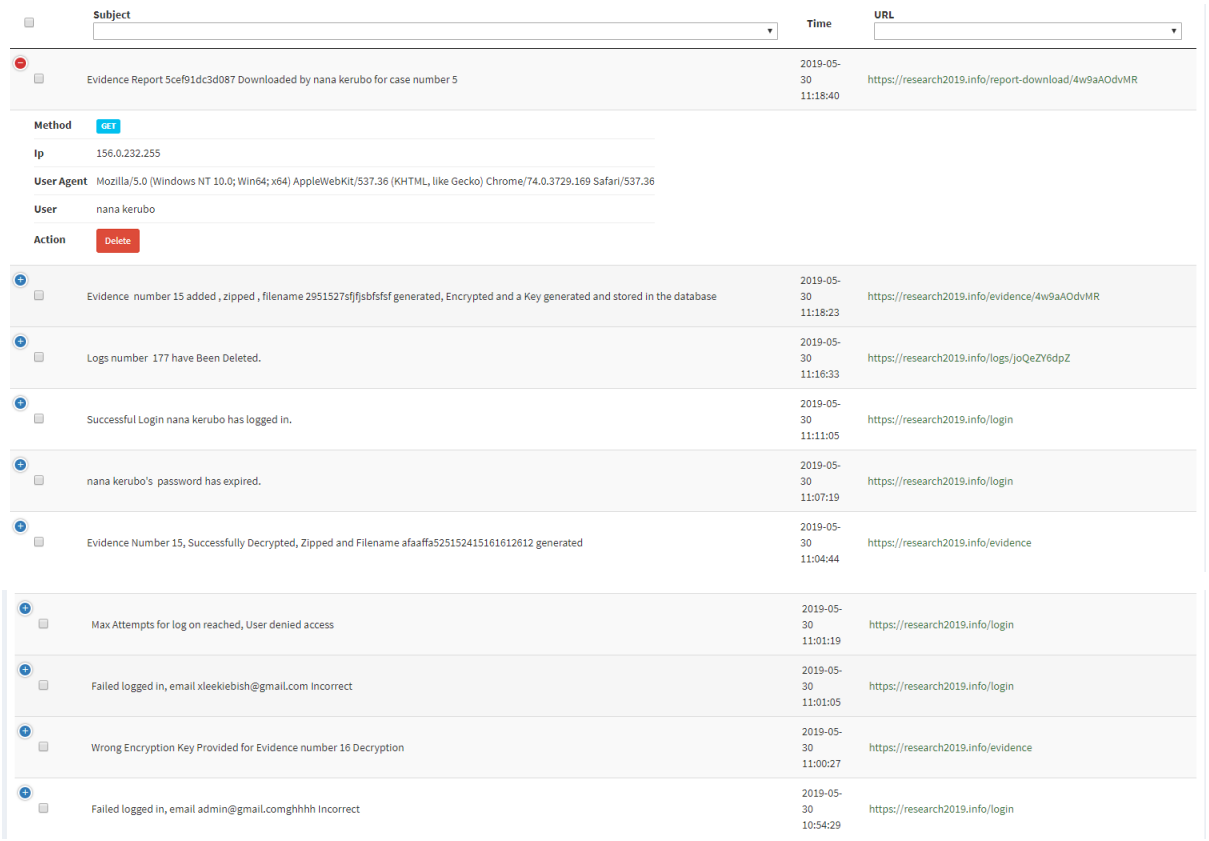


Figure 5.19 User Activity Logs

5.3.8 Application Programming Interface

To allow for efficient integration with other phases of investigation, an API module is available as shown in figure 5.20. The data is encrypted, the other application will require the application key to be able to consume the data.

Figure 5.20 API Interface

5.3.9 Evidence Retention

The system will only retain evidence for as long as is required, a strict time limit is established by the investigator. The system has implemented and is compliant with the GDPR data retention rules covered in Article 5(e) and Recital 39 (Goddard, 2017). Evidence will also be in the system for as long as is it is being used for investigation purposes. The system automatically deletes evidence after a specified period of time alongside with the key used for decryption, a sample code has been attached (see Appendix G). This is important considering that the longer the evidence files are been kept the harder it becomes to be able to prove the accuracy and integrity of evidence.

5.4 Tests Results

The types of testing done were system testing, functionality tests, usability tests, compatibility tests, unit tests and lastly integration tests. The Kenya Police provided sample evidence that were used to test the system

5.4.1 Functionality Tests

Functionality tests were meant to check if the system had met its functional requirements. The web testers identified that encryption, decryption, hashing, key generation, authentication, report generation and evidence storage were working as planned. Evidence management was checked and results were positive as, addition, edit, viewing and deletion of evidence functionality worked. Key generation was effective as the key was unique upon uploading evidence to the database. Encryption at the database level was successful as test evidence was added and encrypted and decrypted upon user authentication. Results in figure 5.21 show this test was successful as the ten respondents agreed to the question.

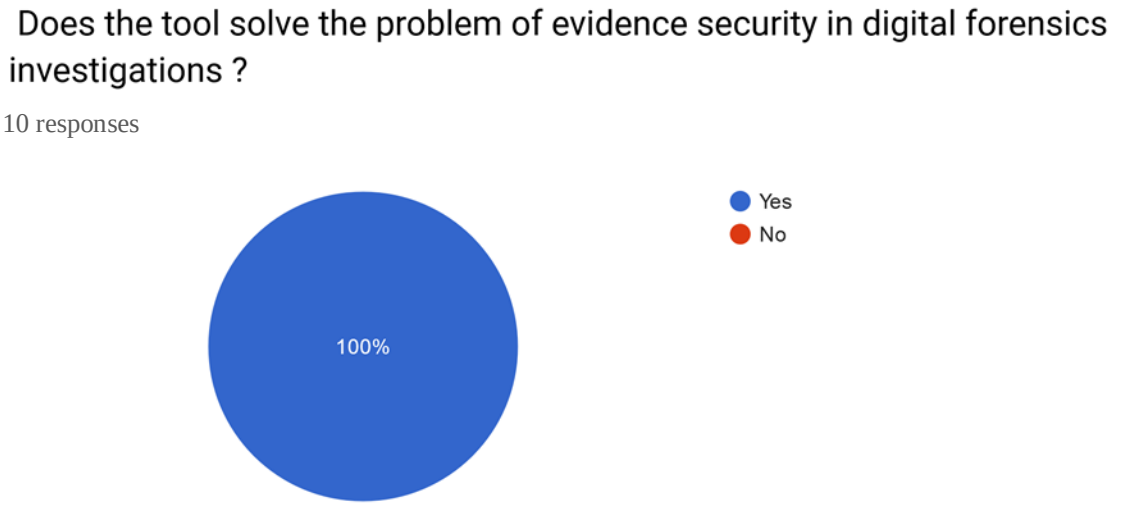


Figure 5.21 Functionality Tests

5.4.2 Non functionality tests

Non functionality tests meant to ensure that non-core functionalities worked. Test included the tool navigation and segregation of duties test. Segregation of duties tests were done to ensure that user roles work and have separate responsibilities, this is important as it ensures accountability. The tool navigation test was successful as testers found that the navigation menu and other system links that navigated to different pages and functions were easily visible and consistent on all webpages, this is evidenced by figure 5.22.

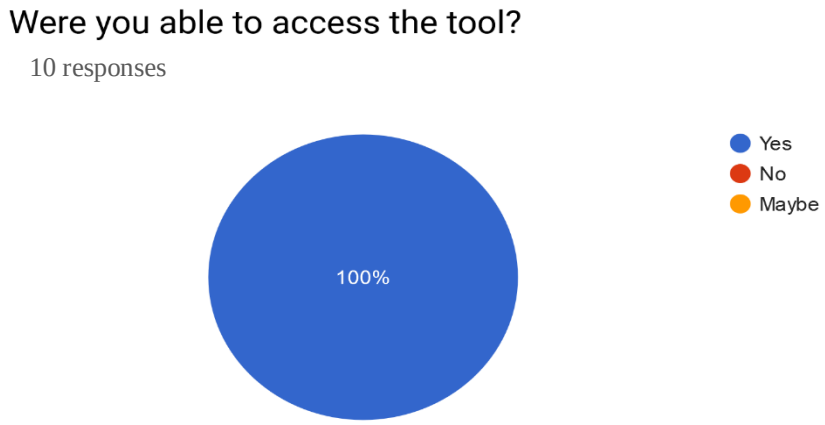


Figure 5.22 Non-Functionality Test Results

5.4.3 Usability Tests

With regards to usability testing, the testers found that the navigation menu and other system links that navigated to different pages and functions were easily visible and consistent on all webpages. Given that the content was user generated, the system maintained and secured the

evidence as it had been uploaded. No changes were made to the data by the system unless initiated by the user. This ensured data integrity when the data was saved in the system.

The testers also noted that the design was intuitive, ensuring an easy learning curve for the user. There was a constant theme throughout the website. Postman was used in testing the API. The test was successful in all requests. This is important in making sure that there is interoperability with the existing solutions.

Questionnaires were used to collect feedback from respondents. This feedback was analyzed to demonstrate that the solution fulfills its intended purpose as shown in figure 5.23. None of the respondents who participated in testing experienced login problems as well as other problems associated with the tool's modules. 97.1% of the respondents believed that the investigators would implement the tool as shown in figure 5.23. All users did not have trouble accessing the system, all users were able to access the system as shown in figure. Respondents cited corruption, illiteracy, lack of electricity as some of the hurdles the investigators will face when implementing the evidence integrity tool.

The feedback received from the testing team was mainly positive. The testers found it easy to document evidence, decrypt evidence, encrypt evidence and view reports. Accessing the dashboard and other modules was straight forward and easy to do. Navigation around the website was easy due to consistency of the navigation menu location. Testers also found the menu headings easy to understand.

The testers also found the process of creating and managing evidence was straight forward. The application programming interface was tested using the post man application; the conclusion was that it was easy for the tool to acquire data and to export data to existing tools in the investigators. The soft delete and the restore functionality were tested. The testers also discovered that once deleted, user accounts could be reactivated again. The testers also tested the responsiveness of the tool on different browsers and the test was positive.

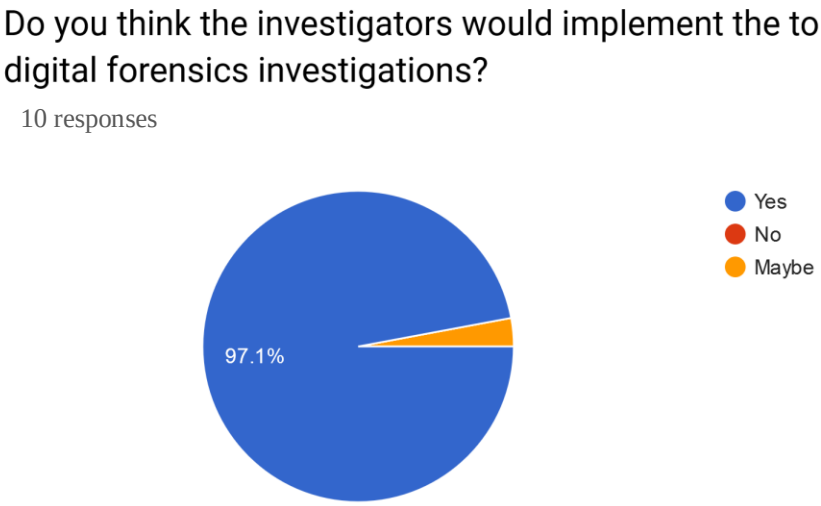


Figure 5.23 Implementation Results

5.4.4 Compatibility Testing

The testers were able to ascertain that the website could display properly on a number of browsers, namely Chrome, Firefox and Microsoft Edge, although most users preferred Google chrome as shown in figure 5.24. It was noted that the Application Programming Interface, enabled the tool to exchange data the existing tools in regards to adding, deleting, updating, downloading data.

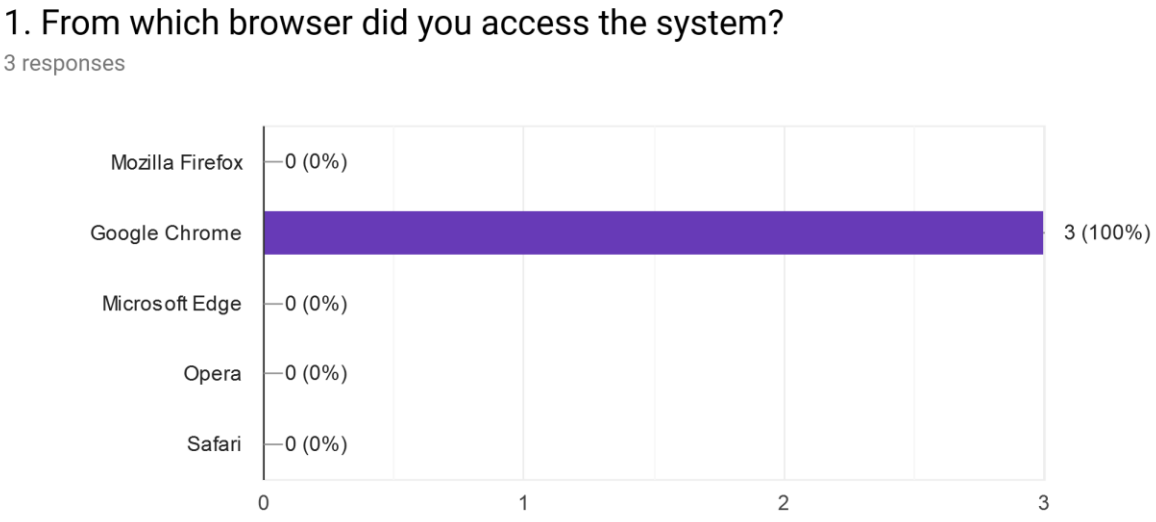


Figure 5.24 Compatibility Test Results

5.4.5 Unit Testing

Unit testing was performed throughout the development phases. Individual tests were conducted in all modules. Individual components were tested and the results were successful.

5.4.6 Integration Testing

Post man application (Appendix E) was used for this test. The investigators having tools which are able to integrate with the developed tool, it was necessary to check the viability of modules such as login, case and evidence modules.

5.5 Validation

The evidence used for validation and testing was provided by the Kenya Police. Validation was done in conducted in two ways; the first way was done by using mock evidence and later comparing the output against the evidence act of 2014, comprehensive best practices and global standards such as ISO/IEC 27001:2013 so ascertain the admissibility of evidence in court. The second validation technique was done by using an evaluation from an experienced hacker with knowledge of information system auditing.

The hacker conducted a series of tests. The hacker was presented evidence files and asked to disclose the contents of the zip file. The hacker was presented with a report generated from the system and asked to bypass the credentials

In summary, the validation proved that the system is secure as an intruder should be able to have either the key to the evidence files to see the contents of the evidences. The system has employed uniform resource locator (URL) hash to hide contents of the specific evidence file.

Chapter 6: Discussion of Key Results

6.1 Overview

This chapter analyses the findings obtained during the dissertation formed the basis on which the tool was developed. The tool was tested to ascertain that it met all requirements. This chapter analyses the findings in relation to the research objectives and the extent to which the findings concur with the literature review.

6.2 Objective One

The first objective of this research was identifying challenges that investigators face while maintaining the integrity of evidence. The literature revealed that cybercrime is on the rise as a result of increased adoption of technology and the internet, this is shown by well publicised attacks which have resulted to global losses. This has resulted to many court cases relying on digital evidence. Investigators have been using physical forms to collect and track evidence. These forms are then stored in storage cabinets which have restricted physical access. These forms are not secure and they could be tampered with. A sample of the form has been attached in Appendix C.

Challenges of handling evidence integrity revolve around lacking secure processes such as encryption and hashing, failing to effect controls such as access controls and lack of knowledge on the importance of evidence integrity. Evidence is stored in evidence bags, which are not secure as they available to unauthorized people. Access controls are important as they bring about the authenticity of evidence, when implemented it is possible to ensure that evidence is available to authorised users of the systems. Lacks of automated logs are another challenge; logs are important from a security point of view as they provide important insights on the processes being used. This relevant information provided the researcher with enough incentive to develop an automated evidence security tools to fill the gaps.

6.3 Objective Two

The second research objective was to identify and review existing tools and techniques used to maintain evidence integrity. The literature revealed there are a lot of techniques used, this is a result of emerging rules and regulations such as GDPR (General Data Protection Regulation) by the European Union and the increase of the rates cybercrime globally. Tools such as exist but they do not offer authentication as part of evidence security making it

difficult to be able to trail the people who viewed the evidence. Most of the tools use the command line interface which is not friendly to the users of the took. It is also evident a large number of the existing solutions follow the digital forensics frameworks.

Findings reveal that tools which preserve the integrity of evidence are available but they are very costly and hence not available to the majority of investigators, this leads to the use of unconventional methods of preserving evidence integrity. The questionnaire indicated most of the investigators are not aware of different technologies that are used to protect evidence integrity. The questionnaires also revealed that a number of the tools use one operating system only hence limiting other users

6.4 Objective Three

The third research objective was to design, develop and test a tool that enhances the integrity of evidence. This objective was achieved through the design and implementation and testing of the tool. It was developed mainly by PHP language. The tests conducted included the compatibility tests in accessing the tool and extracting evidence. The users were not able to see the evidence without going through the decryption processes. The evidence could not be extracted if the user was not authenticated.

6.5 Objective Four

The fourth objective was to validate the effectiveness of the developed tool and ensure it tackles the challenge of evidence integrity, which was met. Validation was carried out by an investigator from the cybercrime and forensics department of Kenya Police whose findings have been discussed in section 5.4. These findings indicate that the system fully meets its design objective for users with intermediate skills of computer skill.

Chapter 7: Conclusions, Recommendations and Future Work

7.1 Conclusions

The research focus was on the development of a tool that would enhance evidence integrity during digital forensics investigations. This was intended to help the law courts deliver fair judgement. Present evidence This tool has been developed and it was able to fulfil this requirement successfully. The solution was able to make use of comprehensive best practices such as standards which enhanced the effectiveness of the tool.

7.2 Recommendations

The system is best suited in an investigative environment. The server to host the tool should have a Secure Server Certificate to ensure that every transaction between the server and the client is encrypted in order to ensure security for the data being shared between the platforms. Additionally, the system logs should be reviewed periodically provide insights of any abnormalities such as failed login attempts so as to enhance evidence security enhance productivity. Users of the system should change their passwords periodically to reduce the risk of hackers gaining unauthorised access since the evidence key depends on the tool's security.

The users of the tool should ensure that the database is backed up at all times, this is important as the availability of the tool would be ensured in case of any breach. This would be a preventive control in the case of an attack.

7.3 Future Work

Future work of this project includes areas such as, portability, evidence storage, key security, backups, use of evidence metadata, logs management and access control.

The system generates a large number of logs. Analysing the logs could be very tedious especially if the system was to be deployed in a busy environment. Future work could include the integration of an automated log analyser to the system. This would be important as it would alert on suspicious system activity on a real time basis.

Evidence backups are very crucial as courts would refer to them in require other case's judgements. Future work would include the backups are automated, this control would be a

correcting control to ensure that the tool goes back to the previous state it was before in case it was compromised, this would ensure availability.

The second area of focus could be on the use of Public Key Infrastructure to securely distribute keys to users to verify their identity and securely exchange evidence over the network.

The user's metadata should be appended on the evidence such that in case of a breach of the evidence, the user who last tampered with evidence can be known. This would a good measure of enhancing evidence security.

In terms of authentication, biometric could be used in addition to the current authentication to enhance evidence security. Biometric authentication systems compare biometric data capture to stored and confirmed authentic data in the database It involves having finger print or facial recognition authentication integrated into the login system as part of the two-step authentication system in a bid to ensure security and to reduce chances of system hacking.

In terms of evidence storage, it is foreseen that the storage resource will be limited considering the large amount of information the forensics field has. Forensics is broadening in terms of expertise. To manage this risk, a multidisciplinary approach is required. Future work could include scaling the tool to handle large amount of evidence and user data. However, this could be addressed as computers will become up to seven times faster not even considering the development of quantum computing (Irons & Ophoff, 2016).

References

Anuradha, G. (2013). Privacy preserving efficient digital forensic investigation framework. *Contemporary Computing* (pp. 3-4). Noida: IEEE.

Bishop, M. (2002). *Computer Security: Art and Science* (1st ed.). Boston: Addison-Wesley Professional.

Bowman, D. C., Bowman, J. T., Lewis, D. M., & Paisley, R. K. (2002). *United States of America Patent No. US20020076819A1*.

Brunty, J. (2013). *Validation of Forensic Tools and Software.* London: AusCert.

Carrier, B. D., & Spafford, E. H. (2004). An Event-Based Digital Forensic Investigation Framework. *Digital Forensic Research Workshop* (pp. 1-12). West Lafayette: Purdue University.

Casey, E. (2011). *Digital Forensics.* Amsterdam: Elsevier Incorporation.

Christensson, P. (2014, August 15). *TechTerms*. Retrieved April 2, 2019, from Technology Terms: https://techterms.com

Čisar, P., & Maravic, S. (2011). Methodological frameworks of digital forensics. *IEEE 9th International Symposium on Intelligent Systems and Informatics* (pp. 8-10). Serbia: IEEE.

Dingli, A., & Cassar, S. (2014). An intelligent framework for website usability. *Advances in Human-Computer Interaction*, 3-6.

Dulin, J. M., Berland, K., Berland, P., Reid, D., Brackmann, R., & Kossnar, D. (2011). *United States of America Patent No. US8068023B2.*

Dumas, J. S., & Redish, J. C. (1999). *Practical Guide to Usability Testing.* Oregon: Intellect Books.

Elizabeth, D., & Denning, R. (2017). *Cryptography and Data Security.* Boston: Addison-Wesley Longman Publishing.

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. *International Journal of Market Research*, 3-10. doi:https://doi.org/10.2501/IJMR-2017-050

Grobler, C. P., & Louwrens, C. P. (2010). Digital Evidence Management Framework. *Information Security for South Africa* (pp. 23-25). Johannesburg: IEEE.

Guo, V. Y., Slay, J., & Beckett, J. (2009). Validation And Verification Of Computer ForensicSoftware Tools-Searching Function. *Digital Forensic Research Conference* (pp. 1-12). Montreal: DFRWS.

Gupta, B. B., & Shrivastava, G. (2014). An Encapsulated Approach of Forensic Model for digital investigation. *2014 IEEE 3rd Global Conference on Consumer Electronics (GCCE)* (pp. 5-6). Tokyo: IEEE.

Hamlin, R. (2000). *Why Small Samples Can Increase Accuracy*. Otago: University of Otago.

Herjavec Group. (2017). *2017 Cycbercrime Report.* Ontario: Cybersecurity Ventures.

Ilyas, M., & Zahra, R. (2014). Case Oriented Digital Evidence Similarity Framework. *Journal of Applied Environmental and Biological Sciences*, 1-4.

International Organisation for Standardization. (2017, July 3). *International Organisation for Standardization*. Retrieved January 3, 2019, from Standards: https://www.iso.org/standards.html

International Telecommunications Union. (2017). *Global Internet Report.* Geneva: ITU.

Interpol. (2016, May 3). *Interpol*. Retrieved from International Criminal Police Organization: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

Irons, A., & Ophoff, J. (2016). Aspects of Digital Forensics in South Africa. *Interdisciplinary Journal of Information, Knowledge, and Management*, 273-283.

Kamble, D. R., & Jain, N. (2015). DIGITAL FORENSIC TOOLS: A COMPARATIVE. *International Journal of Advance Research In Science And Engineering*, 157-170.

Karie, N. M., & Venter, H. S. (2010). Towards a Framework for Enhancing Potential. *Information Security for South Africa* (pp. 4-7). Johannesburg: IEEE.

Kaspersky Lab. (2019, May 29). *Resource Center*. Retrieved May 29, 2019, from What Is Linux and Is It Really Secure?: https://usa.kaspersky.com/resource-center/definitions/linux

Kaushal, P. K., & Sobti, R. (2012). Random Key Chaining (RKC): AES Mode of Operation. *International Journal of Applied Information Systems*, 39-45.

Khan, M. J. (2017). Data Protection and Cybersecurity. *Managing Data Protection and Cybersecurity—Audit's Role*.

Kiarie, J. (2014). *Standard Media.* Retrieved from Standard Digital: https://www.standardmedia.co.ke/article/2000103657/why-it-s-easy-to-commit-murder-in-kenya-and-get-away-with-it

Kigwana, I., Kebande, V. R., & Venter, H. S. (2017). A proposed digital forensic investigation framework for an eGovernment structure for Uganda. *IST Africa Week Conference* (pp. 4-5). Pretoria: IEEE.

McLaughlin, M. (2007, March 5). *Agile Methodologies*. Retrieved from Version One: https://www.versionone.com/agile-101/agile-methodologies/

Merriam Webster. (2014, September 4). *In Merriam-Webster.com*. Retrieved from https://www.merriam-webster.com/dictionary/framework

Mohammed, T. Y., & Hamada, M. (2016). Role of Smart Devices in Information System Security. *Information Technology Based Higher Education and Training* (p. 3). Abuja: IEEE.

Muiruri, F. (2015, December 1). *Kenyan Woman*. Retrieved from Gender Based Violence: http://kw.awcfs.org/article/poor-management-of-crime-scene-and-evidence-greatly-affects-determination-of-sgbv-cases/

Muraya, J. (2017). *Capital News*. Retrieved from Capital FM: http://www.capitalfm.co.ke/news/2016/07/police-forensic-lab-ready-early-2017-boinnet/

Myers, G. J., Badgett, T., & Sandler, C. (2012). *A Self-Assessment Test, in The Art of Software Testing.* New Jersey: John Wiley & Sons, Inc.

National Digital Forensics Incorporation. (2016, May 5). *National Digital Forensics Incorporation*. Retrieved from Forensics: https://www.natldf.com/services.php

Norton. (2017, June 30). *How to recognize and protect yourself from cybercrime*. Retrieved from Internet Security: https://us.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html

Prayudi, Y., & Azhari, S. N. (2015, March). Digital Chain of Custody : State of the Art. *International Journal of Computer Applications, 114*, 1-9.

PWC. (2018). *Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector.* New York: PWC.

RarLab Corporation. (2019, May 31). *RarLab*. Retrieved from Win Rar: https://rarlab.com/

Rumbaugh, J., Jacobson, I., & Booch, G. (2004). *The Unified Modelling Language Reference Manual* (2nd ed.). Boston: Pearson Education Incorporation.

Sommervile, I. (2015). *Software Engineering* (10th ed.). Edinburgh Gate: Pearson Education.

Suzumura, T., & Trent, S. (2016). Performance Comparison of Web Service Engines in PHP, Java and C. *IEEE Web Services* (pp. 5-9). Beijing: IEEE.

Teorey, T., Lightstone, S., & Nadeau, T. (2006). *Database Modelling and Design* (4th ed.). San Francisco: Morgan Kaufmann.

Terashima, N. (2002). *Intelligent Communication Systems.* Cambridge: Elsevier Incorporation. doi:https://doi.org/10.1016/B978-0-12-685351-3.X5000-8

United States Department of Justice. (2002, April 16). *Cybercrime*. Retrieved 12 July, 2018, from DOJ: https://www.justice.gov/criminal/cybercrime/s&smanual2002.pdf

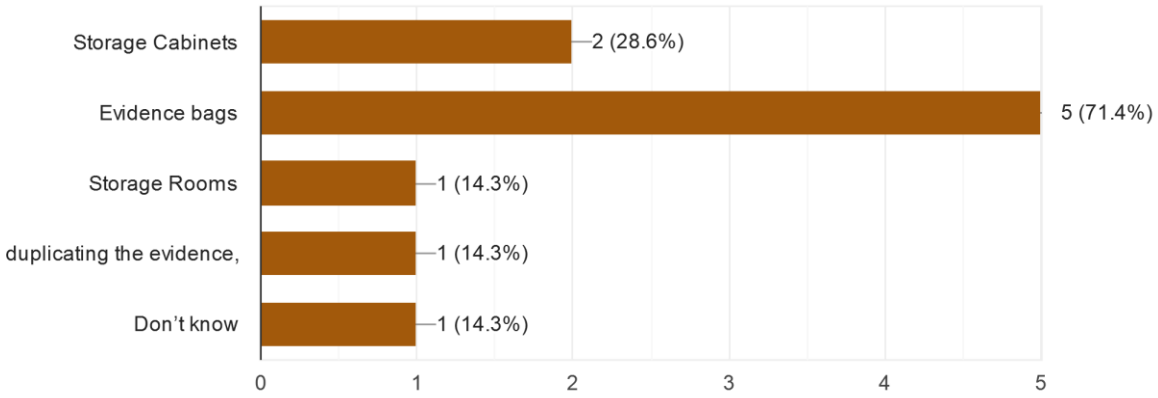
Walker, C. (2015). Computer Forensics: Bringing the Evidence to Court. *Infosec*, 4-7.

Wangui, J. (2016, March 8th). *The Star*. Retrieved March 23rd, 2018, from Lifestyle: https://www.the-star.co.ke/news/2016/03/08/why-justice-is-elusive-for-many-rape-victims_c1299272

Appendix A: Questionnaire Results

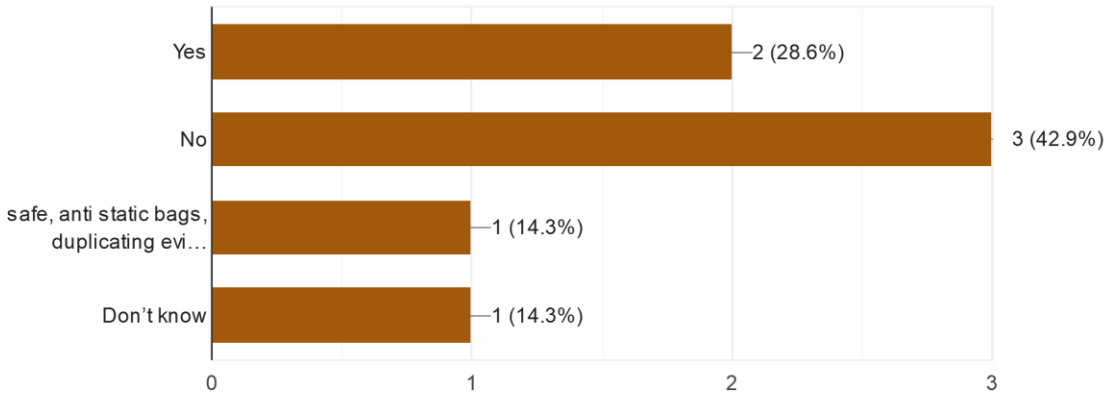
1. What methodologies are used in evidence /exhibit preservation?

10 responses



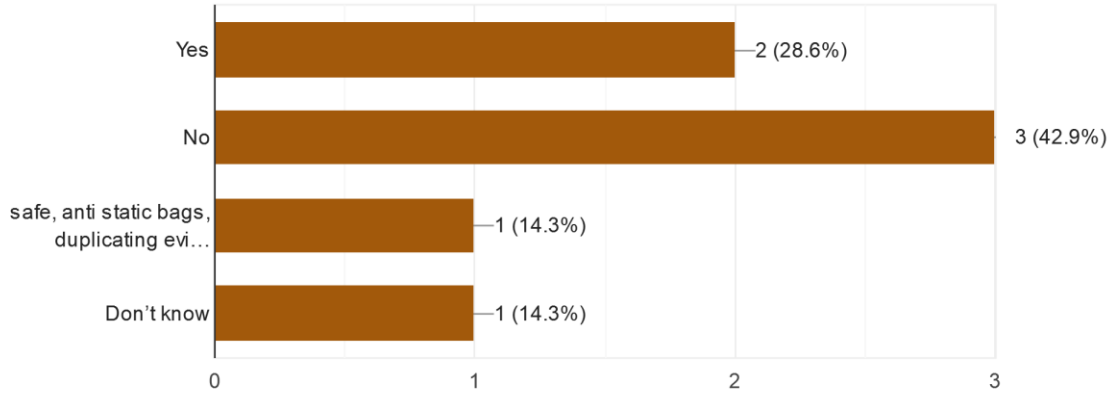
2. Are there tools (e.g encase , ftk imager) that are used in securing evidence in digital forensic investigations?

10 responses



2. Are there tools (e.g encase , ftk imager) that are used in securing evidence in digital forensic investigations?

10 responses



3. If your answer is Yes, on the question above. What is the name(s) of the tool?

10 responses

5
2
Digital Cameras Hard Drives to duplicate digital data
Task,based on TCT

4. List the problems that investigators face while securing digital evidence?

10 responses

tampering
Don't know
Protocols to be observed when accessing the chain of custody items
Retrieving information from the manual files.
Computer illetracy, lack of tools
Lack of proper communication leading to tampering of evidence
differing media formats, encryption, steganography, anti-forensics, live acquisition and analysis., jurisdictional issues, privacy issues and a lack of standardized international legislation.,Resource challenges – e.g. volume of data

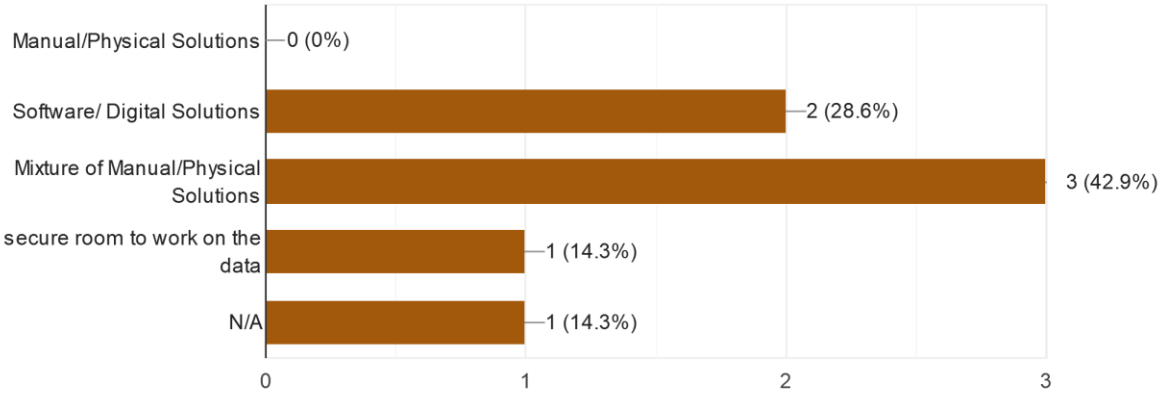
5. What are some of the improvements that should be made on the current methodologies on evidence security used on digital forensics investigations?

10 responses

Embracing technological advancements in digital forensics
Proper security should be enforced to ensure confidentiality and integrity of the data.
digitizing the process
Adoption of advanced technologies that improve the effectiveness of digital forensics study
Proper training to police officers and forensic officers on best practices
find ways to make it less costly,make it part of the core curriculum for police academies

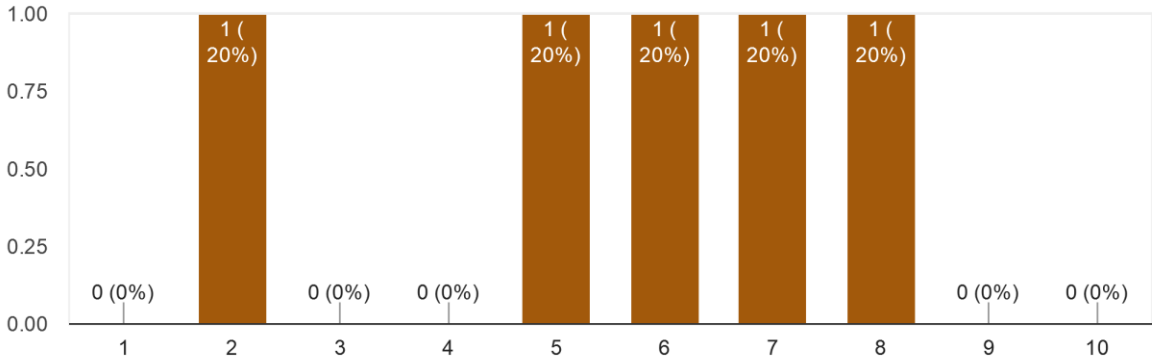
6. What existing solutions or tools do you use in maintaining integrity of evidence in digital forensic investigations?

10 responses



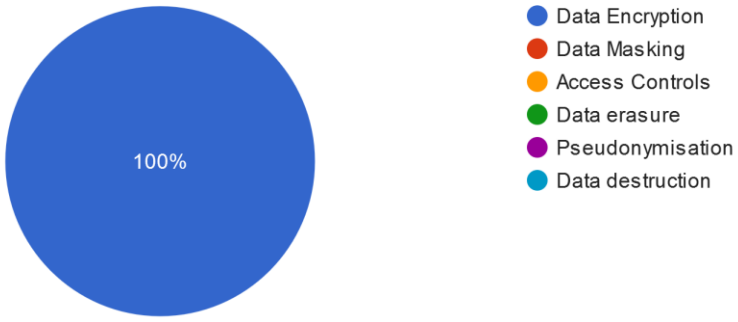
7 . On a scale of 1 to 10, what is your rating on the probability of digital forensic cases being admissible in courts in the last five years?

10 responses

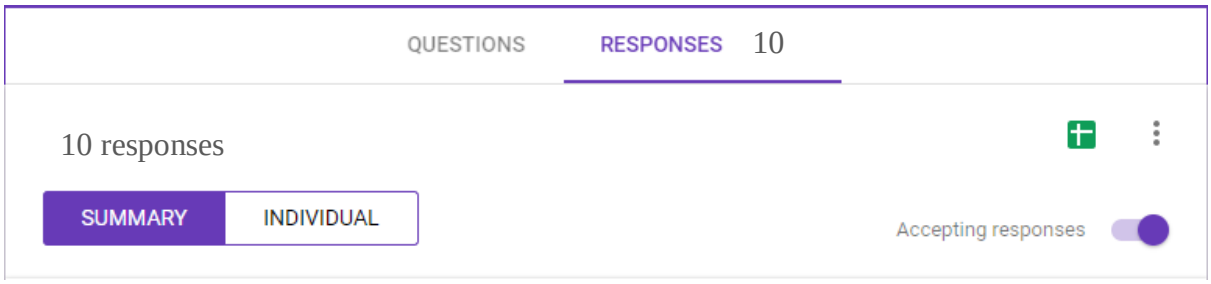


8. What are current technologies used in evidence security

10 responses



Appendix B: Usability Test Questionnaire



Does the tool solve the problem of evidence security in digital forensics investigations ? *

- Yes
- No

...

If the above answer is No, please list the reasons

Your answer

Do you think the investigators would implement the tool in cases involving digital forensics investigations?

- Yes
- No
- Maybe

If the above answer is No, please list the reasons

Your answer

What hurdles might the investigators face while conducting system implementation?

Long answer text

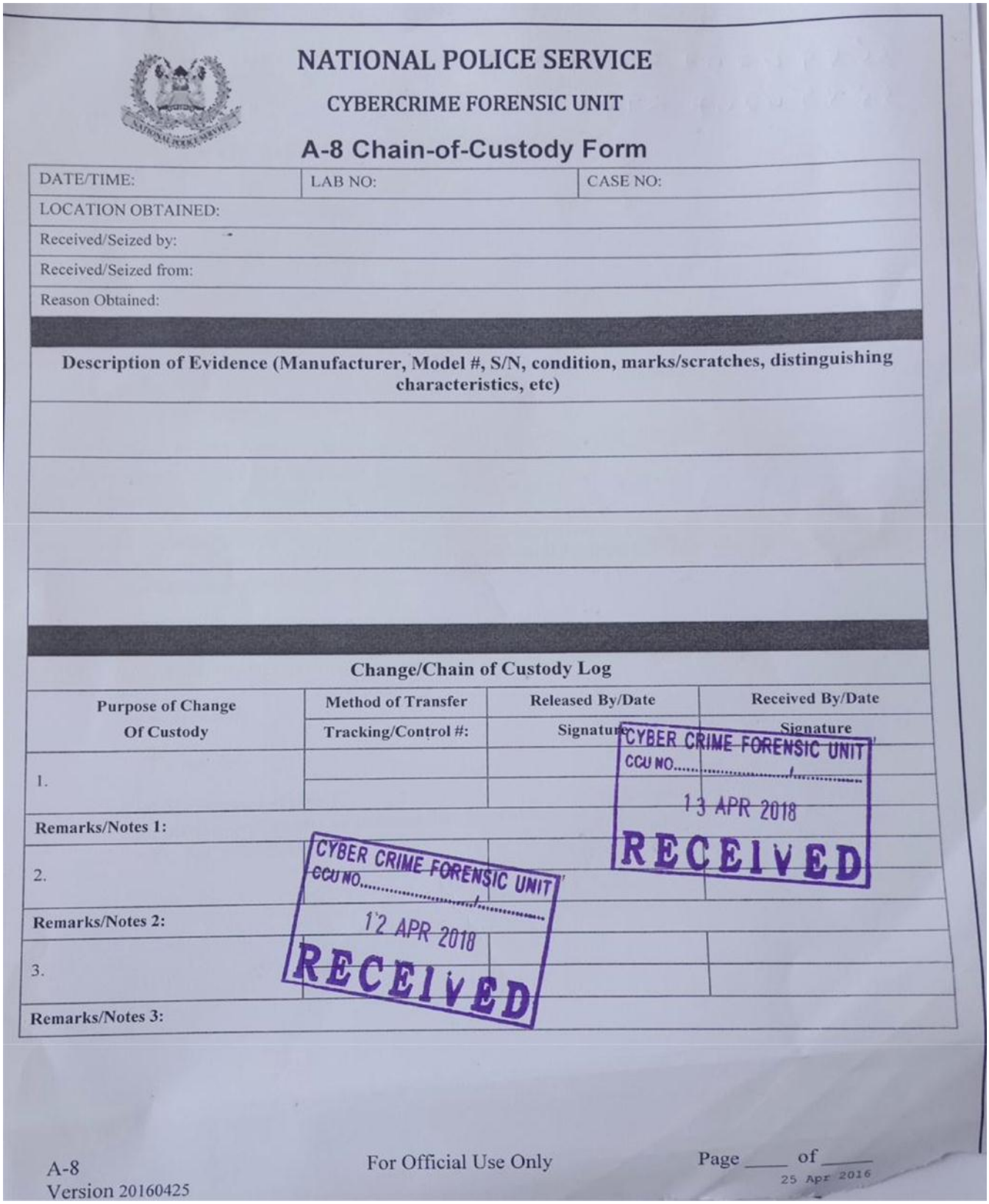
Were you able to access the tool? *

- Yes
- No
- Maybe

If the above answer is No, please list the difficulties you encountered

Long answer text

Appendix C: Manual Form Used by the Investigators



NATIONAL POLICE SERVICE

CYBERCRIME FORENSIC UNIT

A-8 Chain-of-Custody Form

DATE/TIME:	LAB NO:	CASE NO:
LOCATION OBTAINED:		
Received/Seized by:		
Received/Seized from:		
Reason Obtained:		

Description of Evidence (Manufacturer, Model #, S/N, condition, marks/scratches, distinguishing characteristics, etc)

Change/Chain of Custody Log

Purpose of Change Of Custody	Method of Transfer / Tracking/Control #:	Released By/Date / Signature	Received By/Date / Signature
1.			
Remarks/Notes 1:			
2.			
Remarks/Notes 2:			
3.			
Remarks/Notes 3:			

CYBER CRIME FORENSIC UNIT
CCU NO.....
13 APR 2018
RECEIVED

CYBER CRIME FORENSIC UNIT
CCU NO.....
12 APR 2018
RECEIVED

A-8
Version 20160425

For Official Use Only

Page ____ of ____

25 Apr 2016

Appendix D: Turnitin Results

ense Submission | Post-defense Submission

	Start Date	Due Date	Post Date	Marks Available
hecker 2019 (Submission Link) - Post-defense	18 Mar 2019 - 12:30	30 Jun 2019 - 12:30	25 Mar 2019 - 12:30	100

Refresh Submissions

	Submission Title	Turnitin Paper ID	Submitted	Similarity	Grade	Overall Grade	
Digital Receipt	A Web Based Tool For Securing Digital Evidence	1138335560	31/05/19, 14:53	24%	--/100	--	Submit Pap

turnitin

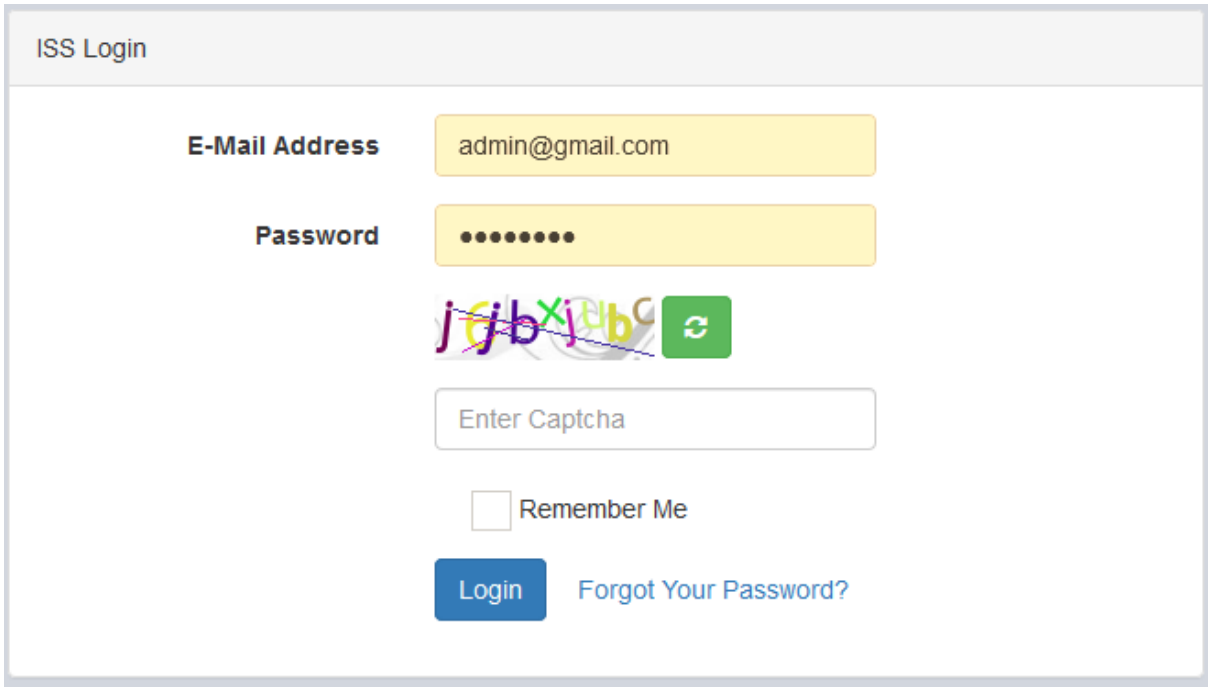
Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

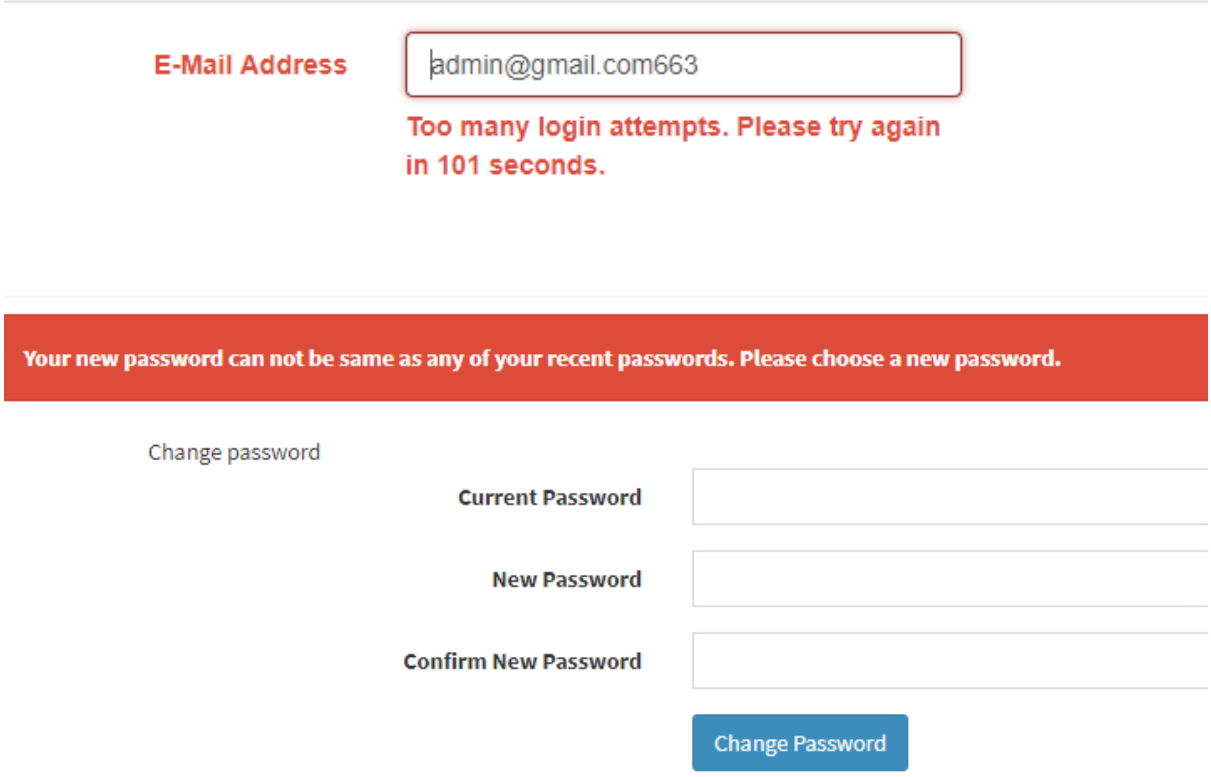
Submission Author	Sebastian Warutumo Collins
Turnitin Paper ID (Ref. ID)	1138335560
Submission Title	A Web Based Tool For Securing Digital Evidence
Assignment Title	Plagiarism Checker 2019 (Submission Link)
Submission Date	31/05/19, 14:53

Appendix E: Screen Shots

Login page.



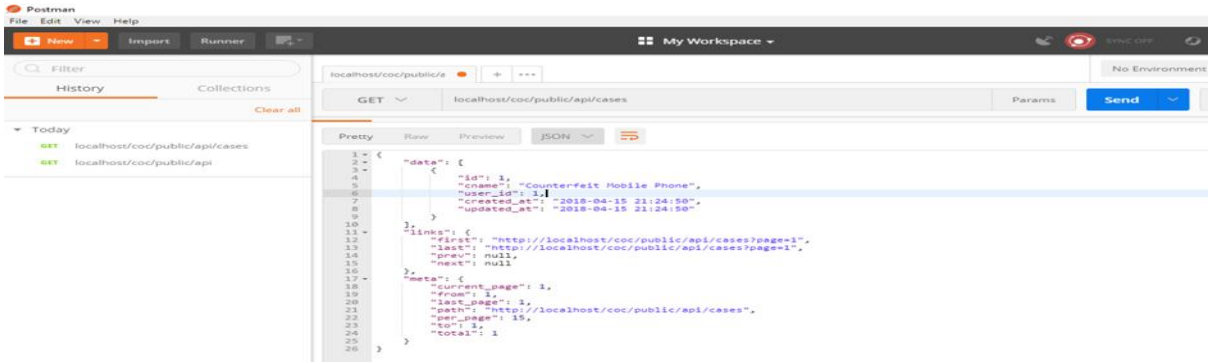
Security design



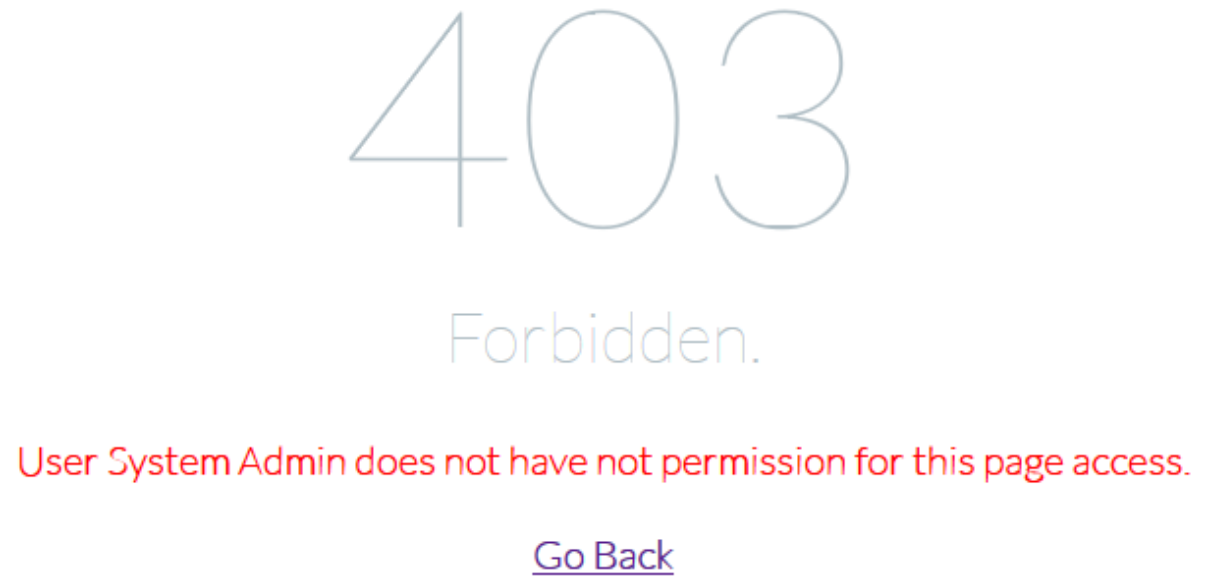
Database Encryption with AES 256 standard.

form	type	device	model
eyJpdiI6IjFqYnFWVXoxaHl6Y1VZYXlZWU9yRUE9PSIsInZhbH...	eyJpdiI6ImQ0R3RaaXJKcUxUTDdPKzRkclImd3c9PSIsInZhbH...	eyJpdiI6IkJldGpqeWE2Qm9pVjJvd3NPd2hCN3c9PSIsInZhbH...	eyJpdiI6IlZrNlNqd1BQS3VGV2s3TEVhT0hTY3c9PSIsInZhbH...
eyJpdiI6Im5cL0RNU0lkdjF0aHlSS2kxenZtQ0x3PT0iLCJ2YW...	eyJpdiI6IkJOS05EMndqUlhuYVRhdE9UTkdVMHc9PSIsInZhbH...	eyJpdiI6IkxyZ25BU1BvY3NLOUYwbGE1a0h2TGc9PSIsInZhbH...	eyJpdiI6IjdcL3pDNFBFbVdpdU54ZUcwU3J6dFVnPT0iLCJ2YW...
eyJpdiI6Ijh6K0s0UGpiQXhKbVJCR1pEWk1vYVE9PSIsInZhbH...	eyJpdiI6ImtNN0pkNDIxTWRKczVwWm1DRzdoc2c9PSIsInZhbH...	eyJpdiI6InpZTDVsb1dnbEg5RW5uSnF2TXU0WHc9PSIsInZhbH...	eyJpdiI6ImZoVXNiRW9jcjFXTVY3Y1k5UVFWeGc9PSIsInZhbH...
eyJpdiI6InFBN2VjeDZRNUFwYTBKdHhoTlRtQkE9PSIsInZhbH...	eyJpdiI6Im9KcVh3aFQwMVpcL1dvQWJoRGZTWHd3PT0iLCJ2YW...	eyJpdiI6InRVcjJFeU4yOUhzemlxR3RGSklSWGc9PSIsInZhbH...	eyJpdiI6InMwZExERHdBZkRjdkE0cVJtVnZNNUE9PSIsInZhbH...

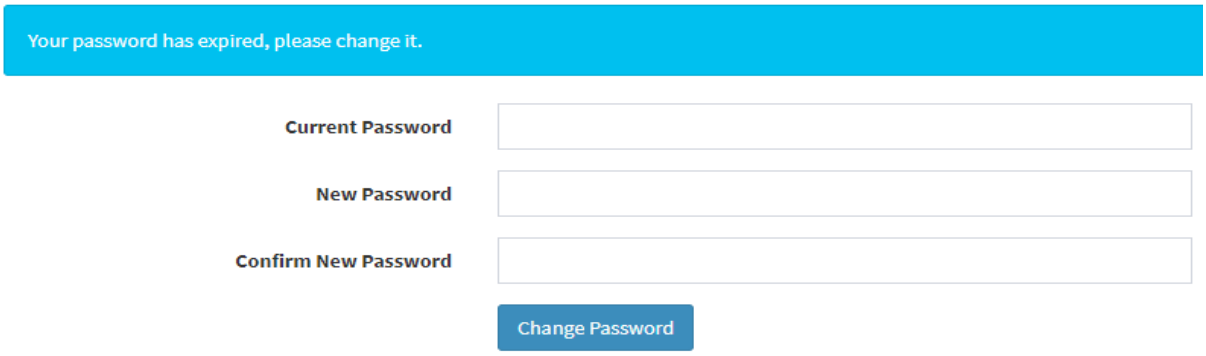
API Test Tool



Lack of user rights



Password Change View



Appendix F: Evidence Retention Code

```
if( is_array($evidnce_expire) ) {
/* Delete all Session files */
foreach( $evidence_expire as $evidence_key => $ex ) {
    if( is_dir(SESSION_DIR . $ex['key']) ) {
        if( $ex['expires'] < time() ):
        $tools->deldir(SESSION_DIR . $ex['key']);
        unset( $expire[$evidence_key] );
        endif;

    } else {
        unset( $expire[$evidence_key] );
    }

}
```

Appendix G: Technical User Manual

Installation

The tool being web based it does not need to be installed. An administrator is supposed to create access for a user and the user is able to log in.

Backing up information

The backing up can be done through the database and can be done manually or automatically.

Trouble shooting

The tool can be troubleshooted by clearing the cache. If the method fails, the tool can be reinstalled. The data will not be lost as it is stored in a separate entity known as the database.