GSJ: Volume 11, Issue 2, February 2023
ISSN 2320-9186



# DIGITAL FORENSIC SETUP & DATA ENCRYPTION: UNDERPINNING ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM

[1]DUKUNDANE Nathascha, [2]Dr Sanja Michael Mutongwa (PhD)

[1]Dept of Information Technology
[1]Graduate School of University of Kigali, Rwanda
[1]dukundanenatacha@gmail.com

[2]Institutional Development Research and Innovation
[2]University of Kigali, Rwanda
[2]sanja_michael@yahoo.com /msanja@uok.ac.rw

## ABSTRACT

This dissertation intended to develop a digital forensic setup & data encryption, underpinning Advanced Encryption Standard (AES) Algorithm in Rwanda. It was guided by specific objectives which are to identify common challenges faced by investigators in maintaining the digital evidence's integrity in digital forensics investigations, to review the existing solutions used in securing digital evidence, to design a novel digital forensic model that will help investigators in preserving the integrity of evidence, and to simulate the new digital forensic and data encryption model. The total population was 300 people and the sample size was 171. Both primary and secondary data were used. Questionnaires were sent to the respondents and collected back. With this instrument, questions were being asked to particular respondents. The findings have proven that 31.58% of respondents strongly agreed, 59.06% of respondents agreed, 5.26% of respondents were not sure, 2.93% of respondents disagreed, and 1.17% of respondents strongly disagreed that explosion of complexity is one of the common challenges faced by investigators in maintaining the digital evidence's integrity in digital forensics investigations. The findings indicated that 36.26% of respondents strongly agreed, while 63.74% agreed that back up of data is one of the existing methods used in securing digital evidence. Findings also revealed that 88.88% of respondents strongly agreed, while 11.12% agreed that the use strong passwords is one of the existing methods used in securing digital evidence. Lastly, 25.14% of respondents strongly agreed, 63.74% of respondents agreed, 9.36% of respondents were not sure, while 1.75% of respondents disagreed that taking care when working remotely is one of the existing methods used in securing digital evidence. The findings related to the third objective of this study have indicated that each block will be 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 process. The decryption part ensures that each block is decrypted independently. Evidence will be decrypted in blocks. Evidence be decrypted if the user provides a correct key which matches evidence file to be decrypted. This is being emphasized basing on clear evidence from respondent's views during analysis of the findings. As recommendations from the study. The research results however revealed some areas that still need continuous improvement. Thus , the research has given different recommendations to different people who will intervene in the use of this new forensic setup.

***Keywords:*** *Digital Forensic; Encryption/Decryption; Advanced Encryption Standard (AES)*

## 1. INTRODUCTION

The information technology has become the foundation for communications, banking, transformation etc. Organization's computers, servers and laptops have, therefore, increasingly become targets of crime and tools for committing crimes. The risk of terrorist organizations turning their attention to technology and cyberspace is very real (Mohammed & Hamada, 2016). For investigators to have reliable information about the evidences from different criminals, the forensic audit has to play a considerable role. As technology has advanced, cyber criminals use more advanced tools to commit crimes, posing additional challenges and pressures to improve digital forensic investigation tools, processes, and techniques and to promote further specialization in the sub-fields of digital forensic. Among the most persistent challenges in DF is how to deal with the increasing volume of digital evidence and cases processed through traditional DF investigation methods.

Digital attacks or threats to information technology may have a momentous impact on organizations. Kiarie (2014) believes that corporate security investigators are making increasing use of computer forensics in areas such as fraud, and harassment and traditional criminal investigations need to be supported with digital collection and analysis tools and techniques. This need has led to the development of digital forensic science and specifically computer forensic (Rodgers and Seigfried, 2004). However, the increasing complexity of tools and techniques of digital investigation creates a new challenge for digital forensic investigators and corporate security investigators.

## 2. LITERATURE REVIEW

### 2.1 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).

### 2.2 Digital Evidence

Cole et al. (2007) defined evidence as information presented in court that attempts to prove a crime was committed. Carrier and Spafford (2006) define digital evidence as digital data that support or refute a hypothesis about digital events or the state of digital data. This definition includes evidence that is not only capable of entering into a court of law, but may have investigative value.

### 2.3 Encryption

Encryption is the process of encoding a message so as only authorized 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. 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 (Elizabeth & Denning, 2017).

### 2.4 Symmetric/asymmetric key algorithms

#### 1. Symmetric key algorithms

The sender encrypts a plain text with a shared secret key using an encryption algorithm. On the other side, the receiver decrypts the cipher text by applying inverse of that encryption algorithm (i.e. decryption algorithm).

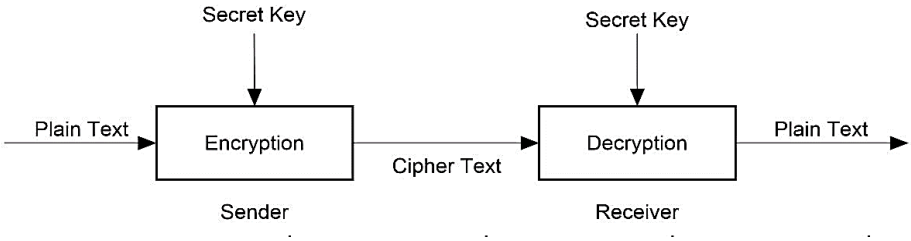


*Figure 1: Symmetric Key Algorithm* (*Behrouz, 2011)*

## 2. Asymmetric key algorithms

Asymmetric *key* algorithms employs the use of two different keys for the purpose of encryption and decryption. The sender encrypts a plain text using his private key, while the receiver utilizes his public key to decrypt the cipher text. It is impossible to deduce a private or public key even if the adversary knows one of the two keys.

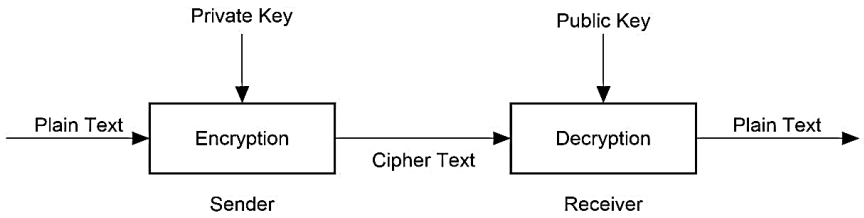


*Figure 2: Asymmetric Key Algorithm (Behrouz, 2011)*

### 2.5 Cryptographic Attacks

### A. Passive attacks

In Passive attacks, an intruder tries to listen to the network connection to gain some information and tries to break the system based upon the packets shared between sender and receiver (Keith, 2012).

**(i) Snooping**

Snooping is a method to access confidential information of a person or some organization by the means of unauthorized access. Snooping includes an attacker observing the emails sent or received by a particular person or by watching some body typing on his system in the real time by using specifically designed software to gain remote access.

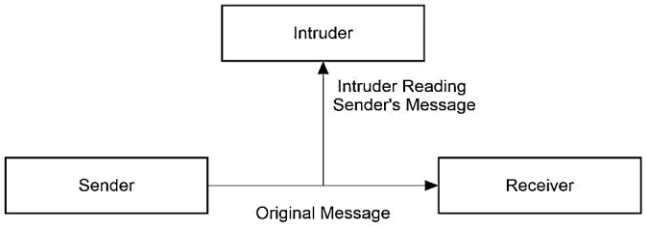


*Figure 3: Snooping Attack* (*Keith, 2012)*

**(ii) Traffic Analysis**

As the name suggests, it is a process of intercepting and extracting meaningful information from the traffic packets that are being transmitted over the network between sender and receiver. Users engaged in the communication are unaware about the fact that their communication lines are being tapped by an attacker.

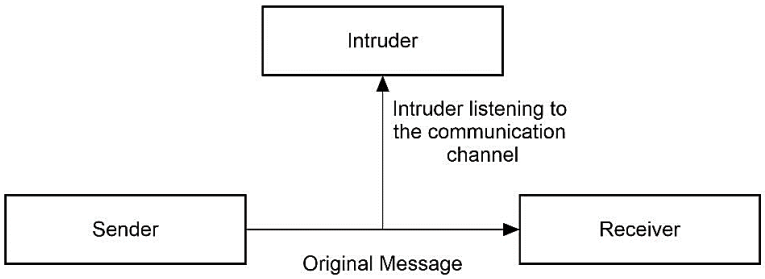


*Figure 4: Traffic Analysis Attack* (*Keith, 2012)*

It can also be performed when the messages that are being transmitted are encrypted and used to find out some meaningful patterns in communication. Moreover, traffic analysis can also reveal confidential information like IP addresses and MAC addresses of the sender and receiver.

**B. Active attacks**

**(i) Masquerade**

It is an attack where an intruder pretends to be the legitimate user in order to gain unauthorized access or higher privileges. Masquerade might work with guessing of usernames and passwords or by finding security loop holes in a system.

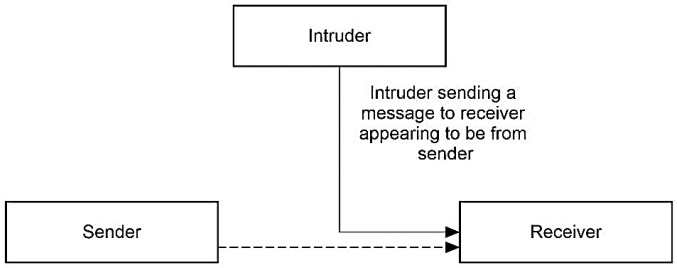


*Figure 5: Masquerade Attack* (*Keith, 2012)*

**(ii) Replay**

It is an attack where the hacker intercepts a message and stores it locally on its own machine, then resend the same message again to the intended receiver.

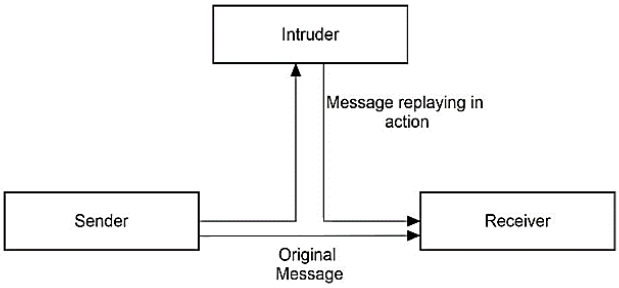


*Figure 6: Replay Attack (Keith, 2012)*

**(iii) Modification**

Attacker modifies the actual contents of an original message for the purpose of gaining personal benefit. Modified message can also be used synchronously with replay attack. Moreover, intruder can also alter the message headers to reroute the same message to some other destination in order to harm the original sender.

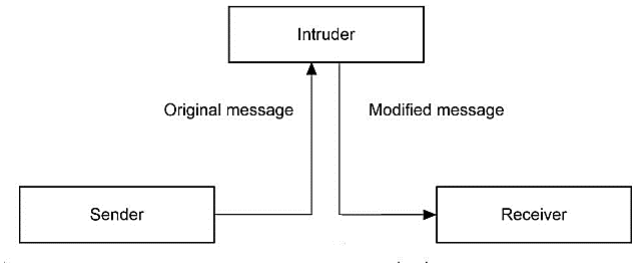


*Figure 7: Modification Attack* (*Keith, 2012)*

**(iv) Denial of Service**

These types of attacks have the potential to temporarily or totally shut down an entire service provided by a dedicated server. Attacker can launch avalanche of service requests to overload a web server which eventually leads to crash.

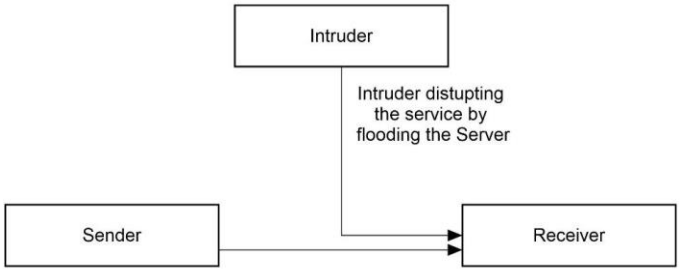


*Figure 8: Denial of service (Keith, 2012)*

## 3. RESEARCH METHODOLOGY

Research Design; Study population; Sample size; Data collection tools

### 3.1 Research Design

Researcher consulted secondary data and experts publications on the subject being studied. Literature to consult was obtained from tangible and/or non-tangible media and Internet media in the form of journals, e-books and other materials relevant to security for digital forensic setup & data encryption underpinning Advanced Encryption Standard (AES) algorithm to find out how to bridge the gap identified in current model.

### 3.2 Study population

The target population was 60 Specialized Crimes staffs, 60 GBV Crimes staffs, 80 Crime Intelligence Collection staffs, 70 Crime Research and Prevention, and 30 Research and Analysis staffs, thus the target population is 300 people.

### 3.3 Sample size

The sample is done in from knowledge gained to represent the entire target under study (Cohen et al., 2011). Sampling is the action of selecting the quantity of observations to include in a statistical sample. The sample size of 171 respondents was drawn from the target population

### 3.4 Tools for data collection

Data collection involves gathering of data using defined techniques in order to answer the pre-determined research question of the study (Sam, 2012). Researcher used questionnaire as an instrument consisting of questions for gathering information from respondents. Researcher used questionnaire because the study concerned with variables that could not be observed such as views, opinions, perceptions, and feelings of the respondents.

## 4. ANALYSIS AND FINDINGS

### 4.1 Encryption/decryption process using AES Algorithm

The keystream block will be generated 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. Each block will be 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 process.

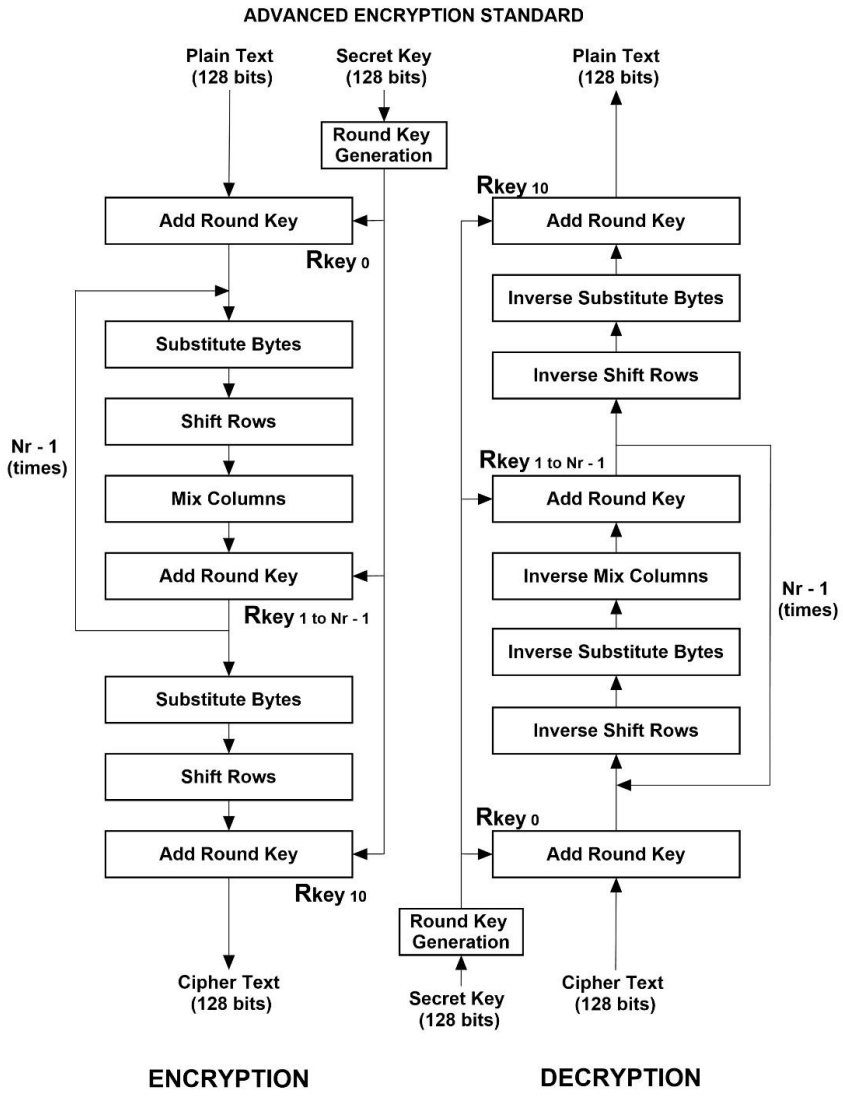


*Figure 9: Encryption/decryption process using AES Algorithm*

The decryption part ensures that each block is decrypted independently. Evidence will be decrypted in blocks. Evidence be decrypted if the user provides a correct key which matches evidence file to be decrypted. The cipher obtained will be stored within a database for further use. If the key matches the file, the evidence will be decrypted and a file will available for the user to download it. The evidence will need to have a key.

### 4.2 Model design

According to Ayub (2015), model involves assembling all of the known components of a system into a coherent whole. The growth of technology is expanding daily and this goes together with safety of data. For the necessity of people to access services that require protection, it is decent to reinforce the systems to provide better services to customers.

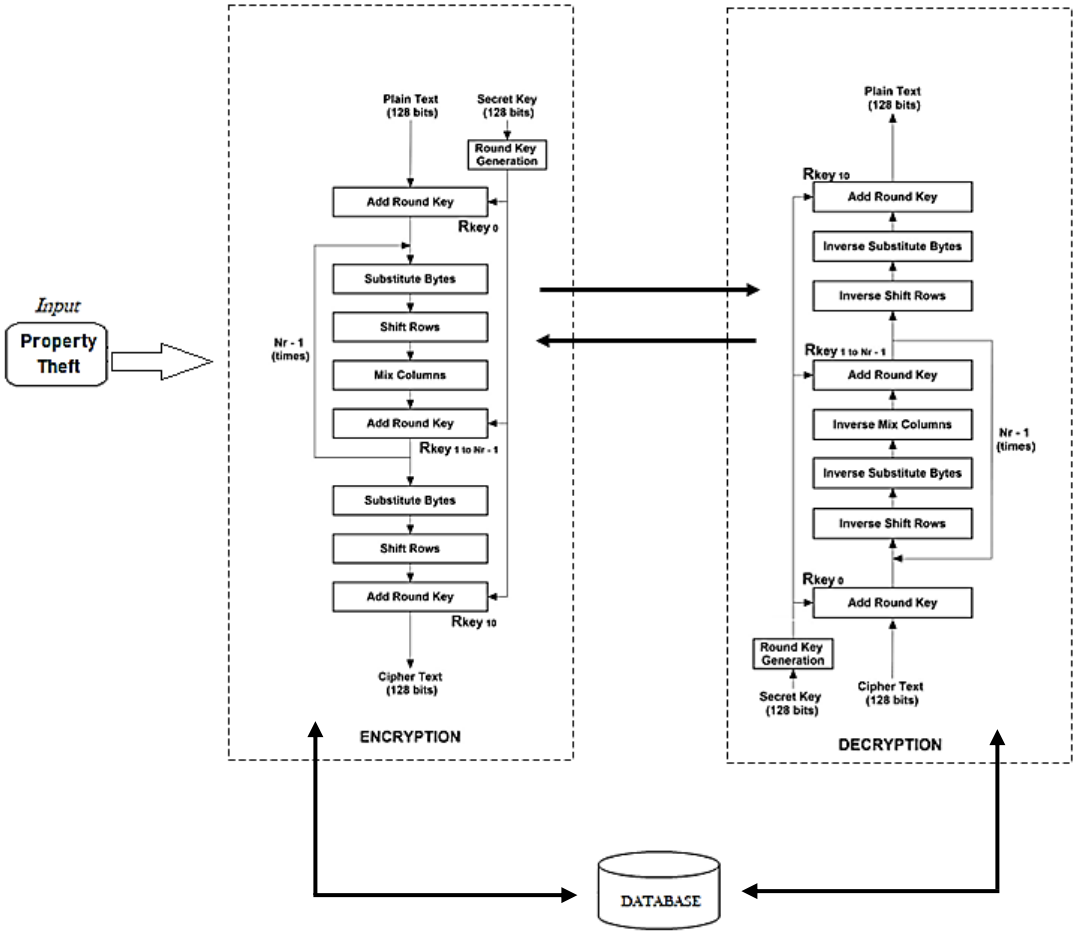


*Figure 10: Proposed Digital Forensic & Data Encryption Model*
*Source: Own drawing*

### 4.3 Model simulation

To encrypt the forensic evidence file, a user is prompted to locate the file in the folder where it is stored. The file to be encrypted, in this case, is a forensic evidence for theft property captured or stored by the administrator in the system which can be of any extension or type such as image, video, audio, document, etc. To do so, the command prompt interface has been generated to allow the process to be possible. The following image shows evidences sorted by their respective types.

The keystream block will be generated 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. Each block will be 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 process.

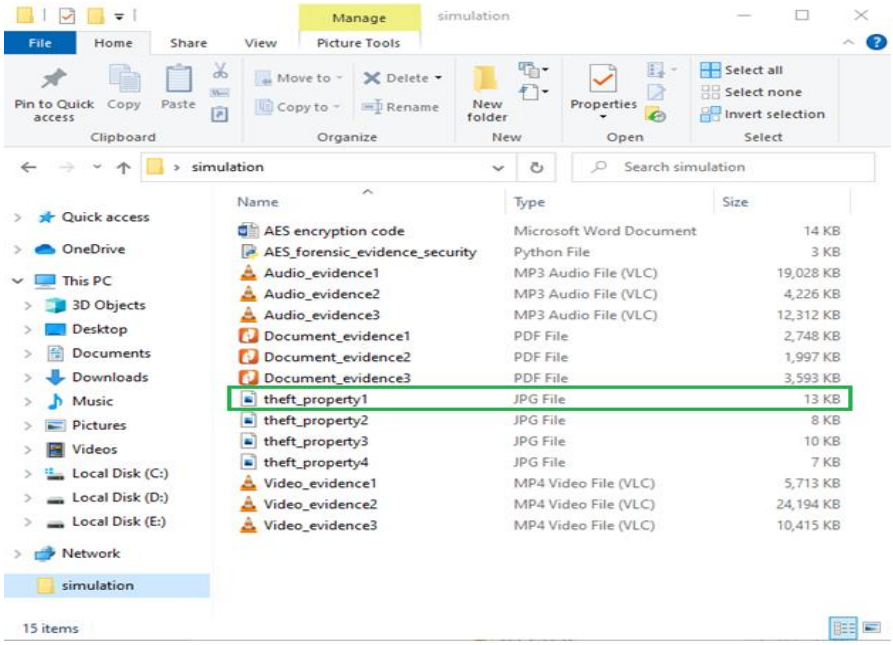


*Figure 11: Storage location of forensic evidence files*

The figure below shows the original file before any operation either encryption or decryption. It is opened to verify if it is corrupted or not, and because it will not be able to be opened once encrypted.

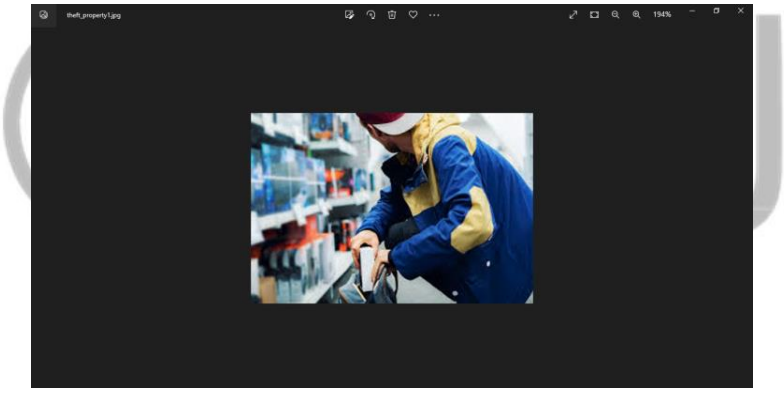

*Figure 12: Opened original forensic file before encryption [ theft_property1.jpg ]*

***Theft image evidence file encryption***

Below is the command prompt showing the process of encryption/decryption. It prompts three choices: PRESS 1 TO ENCRYPT FORENSIC EVIDENCE, PRESS 2 TO DECRYPT FORENSIC EVIDENCE, and PRESS 3 TO EXIT.

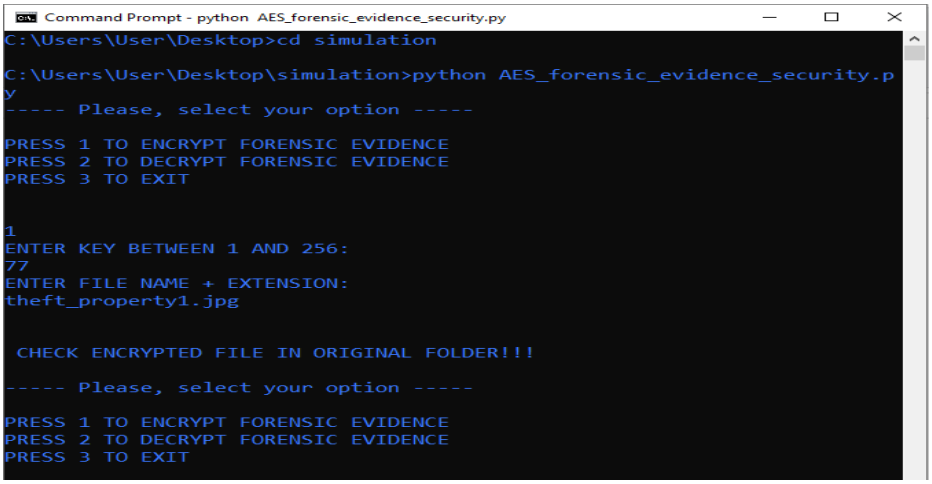


*Figure 13: Interface for forensic evidence file encryption*
*Source: Researcher, 2022*

***Generation of encrypted forensic evidence***

This figure below shows the outcome of the encryption procedure. The resulted file is renamed with the prefix *"Encrypted _"* which is the cipher for the encryption. Now, the forensic evidence is ready to be kept in the store in encryption form.

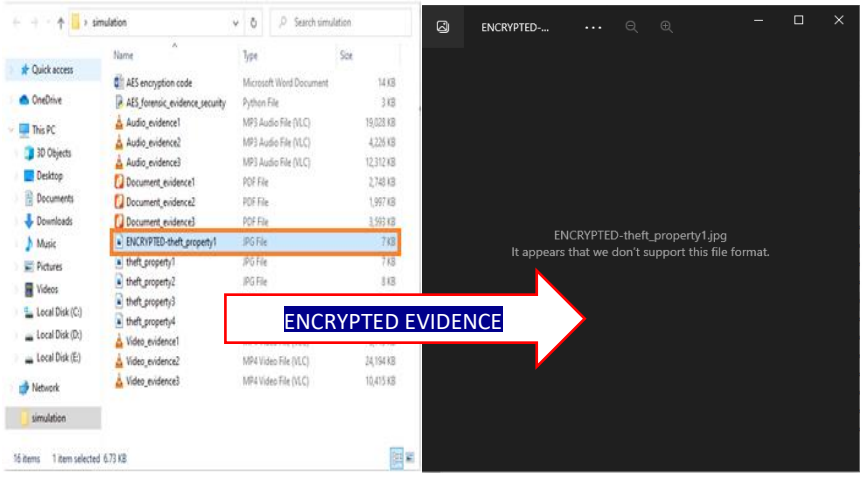


*Figure 14: Generation of encrypted forensic evidence file*
*Source: Researcher, 2022*

This system can be applied for any type of file such as audio files, video files, image files, document files, and so forth.

***Opening encrypted forensic evidence file***

The figure above displays how encoded file looks. The encrypted file called *"CC- forensic evidence"* cannot be opened as normal as other .JPG files. When trying to open the encrypted file, the restriction appears stating that the file is unable to be opened.

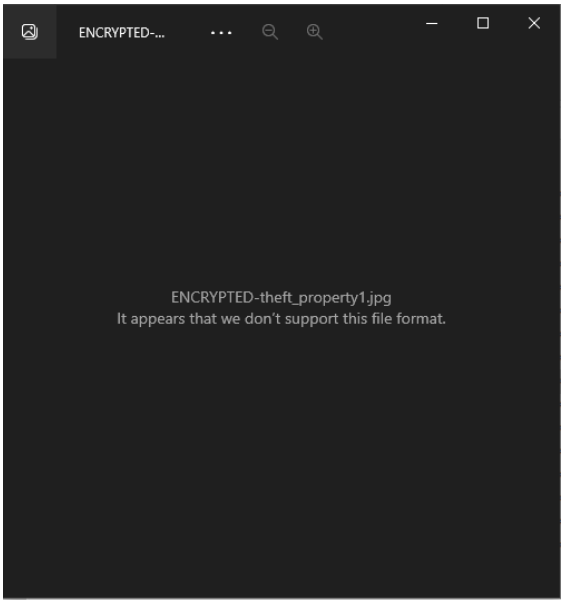


*Figure 15: Opening encrypted forensic evidence file*
*Source: Researcher, 2022*

***Interface for forensic evidence file decryption***

Figure below shows the command-line interface for decryption procedure. If the administration or any other authorized personnel wants to access the file, the decryption id required.

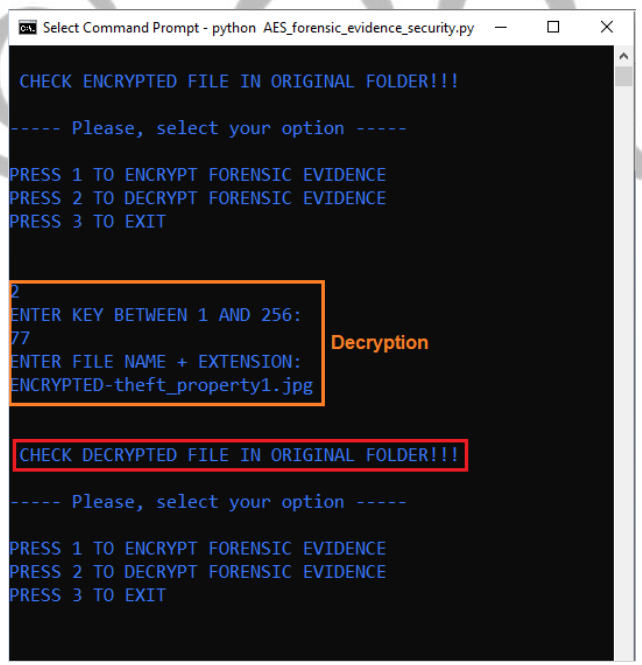


*Figure 16: Interface for forensic evidence file decryption*
*Source: Researcher, 2022*

The same key employed for encryption will again be employed for decryption (as the choice changes to "2" for decryption). The file will be immediately decrypted and then the original file of the similar cipher is produced inside the similar folder of the novel forensic evidence file with the same original file's name.

***Original forensic evidence after decryption***

The figure above shows the original file after decryption using similar key.

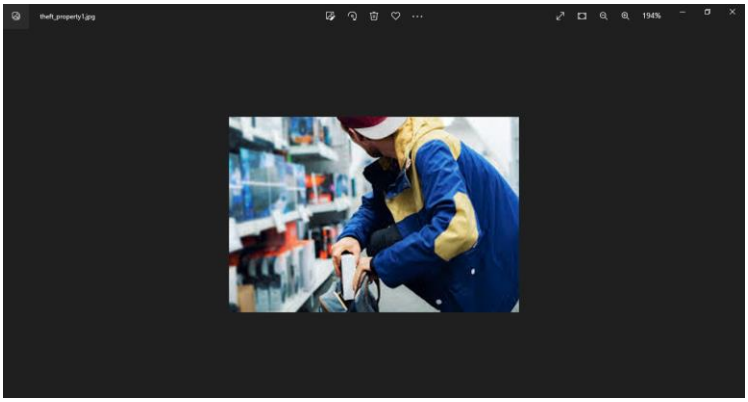

*Figure 17: Original forensic evidence after decryption*
*Source: Researcher, 2022*

## 5. CONCLUSION

The drive of this research was to implement a digital forensic setup & data encryption: underpinning Advanced Encryption Standard (AES) algorithm in Rwanda Investigation Bureau (RIB), Rwanda. During this research, different methods and techniques have been employed to collect and analyze data. Data used in this research were gathered from the selected samples Basing on the total population at RIB of 300, the sample size of 171. The outcomes of the brand new forensic evidence model using AES algorithm were tested with the Python programming language. The data gathering instruments included structured questionnaires and document review. The research has recommended different people who will intervene in the use of this new forensic setup.

## REFERENCES

[1] 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.

[2] Casey, E. (2011). Digital Forensics. Amsterdam: Elsevier Incorporation.

[3] Kiarie, J. (2014). Standard Media. Retrieved from Standard Digital.

[4] 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.

[5] Muiruri, F. (2015, December 1). Kenyan Woman. Retrieved from Gender Based Violence.

[6] Muraya, J. (2017). Capital News. Retrieved from Capital FM.

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

[8] Norton. (2017, June 30). How to recognize and protect yourself from cybercrime. Retrieved from Internet Security.

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

[10] Simon Singh, “The Code Book”, Fourth Estate Publisher, 2015.

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