ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume IX Issue XII December 2024

The Intelligence System for Cybercrimes Using Forensic Interface

Eben A. Nornormey[1*], Ishmael Gyampah Amoako[2], William Esla Maga[3], Emmanuel Asare[4], Daniel O. Bediako[5], Daniel M. O. Adjin[6], Reine Makafui McEben-Nornormey[7], Felix Okpoti[8]

[1,2,3,5] Department of Electrical/Electronic Engineering, Kaaf University College, Gomoa Fetteh, Ghana

[4]Department of Electrical/Electronic Engineering, Koforidua Technical University, Koforidua, Ghana

[6]Regent University College of Science & Technology, Faculty of Engineering, Computing & Allied Sciences, Accra, Ghana

[7]Department of Mechanical Engineering, University of Technology and Economics, Budapest, Hungary

[8]Department of Marine Electrical Engineering, Regional Maritime University, Nungua, Ghana

DOI: https://doi.org/10.51584/IJRIAS.2024.912040

Received: 16 December 2024; Accepted: 21 December 2024; Published: 15 January 2025

ABSTRACT

This paper discussed several areas of endeavour including financial sectors that cyber-attacker can target. Most often cybercrimes are committed remotely using the internet. This article brings to the fore computer crimes and their various types. It demonstrated the existing laws instituted by international and regional bodies to combat cybercrimes. The authors also described various countries specific laws, aimed at combatting computer crimes. Fighting these kind of crimes demands systems and security measures; the researchers discussed computer forensic interface and application which facilitate analyses and investigations of these crimes. In the forensic application interface, there are three major tabs, namely: view captured screenshot, view captured processes, and view index.dat; the authors explained their various functions. The researchers used system flow chart diagrams to describe the operational flow of the forensic application system and forensic interface. While the forensic application system captured image and process performance, forensic interface visualized the flow of data between the forensic expert interface and the core functionalities of the system.

Keywords: Cyber-Attacker, Computer Crimes, Forensic Interface, Forensic Application, Flow Chart Diagrams, System, Screenshot, index.dat

INTRODUCTION

Usually cyber-attacks against infrastructure of a country typically target several key areas that are critical to the functioning of society and the economy. Some of the most commonly targeted areas are: the energy sector, government and military systems, financial sectors, healthcare systems, and the telecommunication sectors, etc. Such actions may be carried out by organized criminals, by states or by individual criminals, who may operate remotely from another country or state. Such attacks are categorized as cybercrimes, cyber terror or cyber war **[1].**

Computers are used to commit crime and are the target of crime every day. Besides the magnitude and scope of the threat, one of the greatest challenges in fighting computer crime resides in the fundamental nature of the computing world. Within the framework of routine activity theory, the increasing power of computers has increased criminal opportunities for motivated offenders as well as the availability of suitable targets **[2].** Moreover, the worldwide information network has transformed computer crime from a local problem to an international security issue. According to the Department of Homeland Security in the United States, cyber threats usually refer to persons, organizations, and countries that attempt to illegally access a system network or computer device using data communications pathway. The Government Accountability Office of the United States in 2005 provides a cyber-threat table that includes hackers, criminal groups, foreign intelligence services, phishers, spammers, spyware/malware authors, and terrorists. The activities of this office also include

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume IX Issue XII December 2024

but not limited to espionage, hacking, identity theft, crime, and terrorism.

For the purpose of this paper, we are using "computer crime" and "cybercrime" as synonyms and both should be considered a form of "cyber threat". Cyber threats are currently significant enough to become a national security priority in several countries including the United States, United Kingdom, China and the European Union **[3].** In order to better understand the challenges that the United States' information infrastructures are facing, it is necessary to examine how government agencies are addressing the threats posed by those who perpetrate computer based crimes and attacks. On one hand, we know that computer crimes are often a "hi-tech" version of more traditional crimes such as theft, espionage, sabotage, and fraud. On the other hand, the ramifications of many cybercrimes are so extensive and technologically complex that they require specific knowledge to better understand the evolving nature of the threats as well as to develop the needed new tactics and strategies to investigate them.

COMPUTER CRIME

Computer crimes involve unauthorized use of computer technology to manipulate critical user data. They are criminal activities, which involve the use of information technology to gain an illegal or unauthorized access to a computer system with intent of damaging, deleting or altering computer data. Computer crimes also include the activities such as electronic frauds, misuse of devices, identity theft and data, as well as system interference **[4]**. Computer crimes may not necessarily involve damage to physical property. They rather include the manipulation of confidential data and critical information. Computer crimes involve activities of software theft, wherein privacy of the users is tampered. These criminal activities involve the breach of human and information privacy and illegal alteration of system critical information **[5]**. The different types of computer crimes have necessitated the introduction and use of newer and more effective security measures. Computer crime encompasses a broad range of activities generally. However, it may be divided into two categories: Crimes that target computer networks or devices directly and Crimes facilitated by computer networks or devices.

Types of Computer Crime

1. **Identity Theft:** This is one of the most serious frauds as it involves stealing money and obtaining other benefits through the use of a false identity. It is the act of pretending to be someone else by using someone else's identity as one's own. Financial identity theft involves the use of a false identity to obtain goods and services and a commercial identity theft is the using of someone else's business name or credit card details for commercial purposes. Identity cloning is the use of another user's information to pose as a false user. Illegal migration, terrorism and blackmail are often made possible by means of identity theft. Computer crimes involve illegal exploitation of the computer and communication technology for criminal activities. While the advancing technology has served as a benefit to mankind, the destructively directed human intellects are all set to turn technology into a curse.

2. **Writing or Spreading Computer Viruses or Worms**: Computer virus is a computer program that can replicate itself and spread from one computer to another. It is also a malicious code written with an aim to harm a computer system and destroy information.

3. **Industrial Espionage by means of Access to or Theft of Computer Materials:** Espionage or spying involves a government or individual obtaining information considered secret or confidential without the permission of the holder of the information.

4. **Denial- of- Service Attack:** This is a situation where company websites are flooded with service requests and their websites is over loaded and either slowed or crashed completely. Also in computing, a denial-of-service attack is an attempt to make a machine or network resource unavailable to its intended users.

5. **Fraud Achieved by the Manipulation of Computer Records:** Computer fraud is the use of information technology to commit fraud. Fraud is intentional deception made for personal gain or to damage another individual.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume IX Issue XII December 2024

6. **Making and Digitally Distributing Child Pornography:** Child pornography refers to pornography depicting sexually explicit activities involving a child. It may use a variety of media, including writings, magazines, photos, cartoon, video games etc.

7. **Unauthorized Access to or Modification of Programs:** Unauthorized access to computer material can occur, for example, when a person gains access to a computer through a telecommunications network, or when employee accesses information on their employer's computer which they are not entitled to access.

8. **Salami Slicing:** This is the practice of stealing money repeatedly in extremely small quantities.

9. **Extortion (also called Shakedown, out Wresting, and Exaction):** It is a criminal offense of unlawfully obtaining money, property, or services from a person, entity, or institution, through coercion.

10. **Forgery:** This is the process of making, adapting or imitating objects, statistics, or documents with the intent to deceive.

Existing Laws to Combat Cybercrime

There are numerous laws that are promulgated to combat cybercrimes in the world. These crimes have become more complex, sophisticated and syndicated. The laws to fight cybercrimes exist internationally and nationally. These laws focus on cybercrimes such as: hacking, identity theft, fraud, cyber stalking and other online criminal activities. Crime fighters, law enforcers and state authorities all over the world are cooperating actively to help eliminate or reduce to the barest minimum these cancans. To help combat these menaces, the international community has come out with laws and frameworks including United Nations Resolutions 55/63 (December 4, 2000) and 56/121 (December 19, 2001); these resolutions were passed by the United Nations General Assembly **[6].** The aim of these resolutions is to combat criminal misuse of information technologies with emphasize on international cooperation to tackle cybercrime.

The European Union in 2013 passed the Cybercrime Directive law (2013/40/EU); the objective of this directive is to establish common standards across the EU for combating cybercrime, particularly focusing on illegal access to information systems and interference with data **[7].** The European Union in 2016 enacted the Directive on Security of Network and Information Systems law (NIS Directive) **[8].** The aim of this directive is to impose requirement on EU member states to improve cybersecurity by ensuring that essential services and digital services providers are protected from cyber-attacks. The EU also passed in 2018 the General Data Protection Regulation (GDPR) law; this law governs the collection, storage and processing of personal data in the EU **[9].** It imposes significant penalties for data breaches, making it a critical legal framework for combating cybercrime.

The South Asian Nations, passed a regional agreement under the auspices of Association of Southeast Asian Nations (ASEAN) Framework on Cybersecurity in 2018 **[10].** The agreement sought to promote cooperation among their countries to combat cybercrime and improve cybersecurity resilience.

The African Union in a Convention in Malabo in 2014 deliberated on Cybersecurity and Personal Data Protection and set a primary legal framework to combat cybercrime and improve cybersecurity across the continent **[11].**

Apart from the United Nations and Regional Bodies, countries also have their own cybercrimes laws. The United States enacted in 1986 the Computer Fraud and Abuse Act (CFAA); this law sought to criminalize unauthorized access to computers and networks **[12].** The CFAA covers offenses such as hacking, theft of information and damage to computers. Another act, the Identity Theft and Assumption Deterrence Act (ITAD) was passed in 1998; this law criminalizes identity theft and using someone's identifying information to commit fraud **[13].** The US also enacted the Cybersecurity Information Sharing Act (CISA) in 2015; this law encourages companies to share cyber threat data with the Government to help prevent cyber-attacks **[14].**

In Ghana, cybercrime issues are addressed through several legal frameworks and laws including: the

Electronic Transactions Act, 2008, the objective of this law is to prevent unlawful access to electronic systems and unauthorized modification of data **[15].** The Payment Systems and Services Act, 2019; this act governs payment systems and electronic transactions, providing regulations to protect users of electronic payment systems from fraud and unauthorized access. Another act, the Cybersecurity Act, 2020; this law sought to protect the country's critical information infrastructure, promote the development of cybersecurity and combat cybercrime **[16].**

The Budapest Convention on Cybercrime in 2001was the first International treaty with the sole objective of addressing cybercrime **[I7].** This Convention brought together many countries including the United States, Canada, and most of the European Union nations. It provided a comprehensive framework for national laws on computer crimes, defined specific cybercrimes and established procedures for International cooperation.

In addition to these national and international laws, agencies such as Interpol, Europol, ECOWAS Regional Cybersecurity Framework and national cybercrime units collaborate globally to fight cybercrime.

FORENSIC INTERFACE

Crimes associated with theft and manipulations of data are detected daily. Crimes of violence are not immune to the effects of the information age. A serious and costly terrorist act could come from the internet instead of a truck bomb. The diary of a serial killer may be recorded on a floppy disk, hard disk drive or the likes rather than on paper or in a notebook. Just as the workforce has gradually converted from manufacturing goods to processing information, criminal activity has to a large extent also converted from physical dimension to virtual. There is a need for computer forensic experts and computer based monitoring and security system for easy capture of evidence of intruder who compromises a network or computer. Data integrity is very important in today's world; to achieve this, system such as forensic interface is employed. Forensic interface is a means or software used by the intelligent community to analyze, investigate and exhibit physical or digital proof of cyber or computer crime. Crime investigators and legal experts use this interface to methodologically scrutinize data integrity and transparency.

Figure 1 shows data or work flow diagram of forensic expert interface (the researchers are the forensic experts in this scenarios). This interface encapsulates the entire function of the forensic system. The interface application pulls up the content of captured running processes, captured screenshots and content of Index.dat. This is done by making request; the module reacts through a response which displays the user authentication interface. It is imperative to note that, forensic expert interface is a dedicated digital platform with the intension of assisting forensic specialists or professionals to analyze and interpret cybercrime investigations.

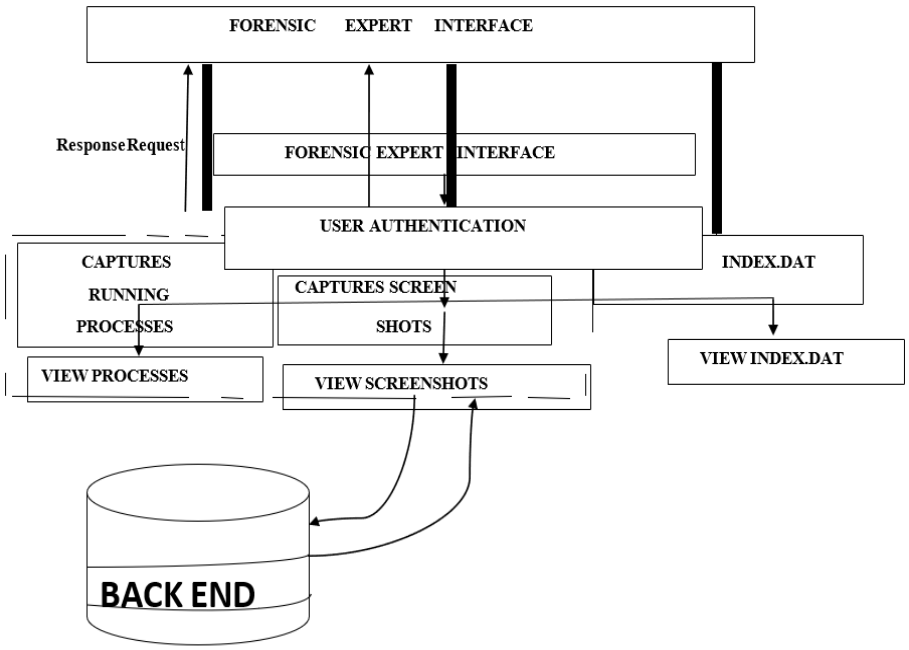

Fig 1: Date Flow Diagram

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume IX Issue XII December 2024

Once the forensic expert passes the authentication test, the forensic application immediately starts running, and displays the interface as shown in a screenshot as captured in figure 2.

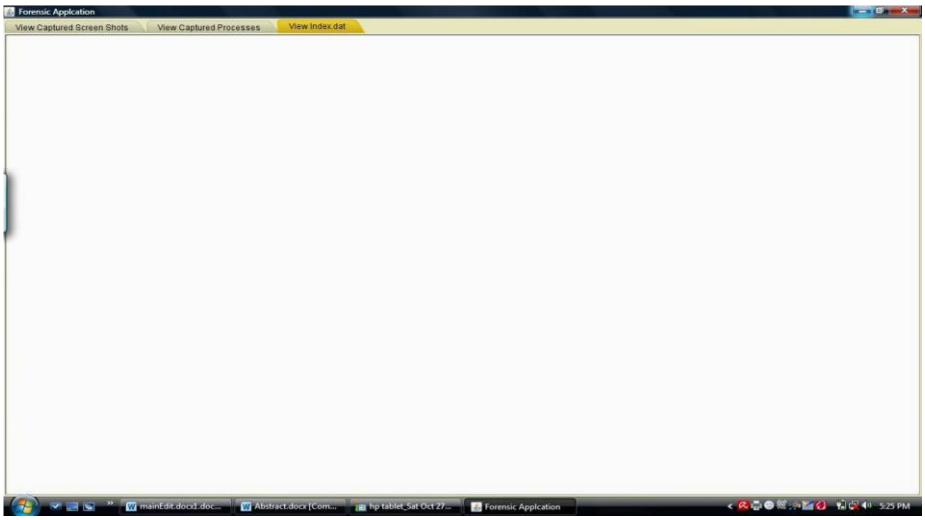

Fig 2: Displayed Forensic Application Interface

This interface shows the three main key tabs (view captured screenshot, view captured processes, and view index.dat) of the forensic application. The forensic expert can click on any of these tabs to view the processes, the screenshots and Index.dat as captured by the forensic application. The specific functionalities of these three tabs in the forensic application Interface are explained as follow:

1. **View Captured Screenshots**: This tab displays the screenshots that the forensic system has captured at regular time intervals as described in the data flow chart in figure 1. When we click on this tab, the application retrieves and displays the saved screenshots of the target system's activities. This enabled us to visually inspect the user's desktop activity over time for any potential forensic evidence.

2. **View Captured Processes:** This tab is used to show the processes that were captured by the forensic system. These are the snapshots of all running processes that the system captures every 11 seconds and logs them in a file. We select this tab to view all the detailed list of processes that were running on the system during the forensic capture period. This information enabled us to detect unauthorized or suspicious applications running on the system.

3. **View Index.dat:** This tab enabled us to display the contents of the Index.dat file which logs internet activities like browsing history in windows system. This tab also gave us the permission to view user activities related to internet browsing, such as visited URLs, and cached (hidden) files by analyzing the index.dat file.

The blank area in the middle of figure 2 represents the space where the data or contents from the captured screenshots, captured processes, and the index.dat would be displayed when we selected tabs. This display area is currently empty because no content is loaded in this instance.

The image provided in Figure 3 is a screenshot of NetBeans IDE 6.7.1., a tool that provided an environment where the forensic application was written, run, debugged and developed. The screenshot shows that the Forensic Application project is currently loaded in the NetBeans Integrated Development Environment, showing its source packages, test packages, libraries and test libraries as indicated in the project pane (window) on the left and it is being prepared for execution. When the Forensic Application was expanded, the context menu (right-click) was opened, and the option 'run' was selected indicating that the user was preparing to run the project. The user performed this running process to test the functionality of the viewing captured screenshots, viewing captured processes, as well as the user activity (index.dat). The whole context suggests that the user was working on or testing the Forensic Application's features, such as viewing captured processes and interacting with a database for forensic data storage.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume IX Issue XII December 2024

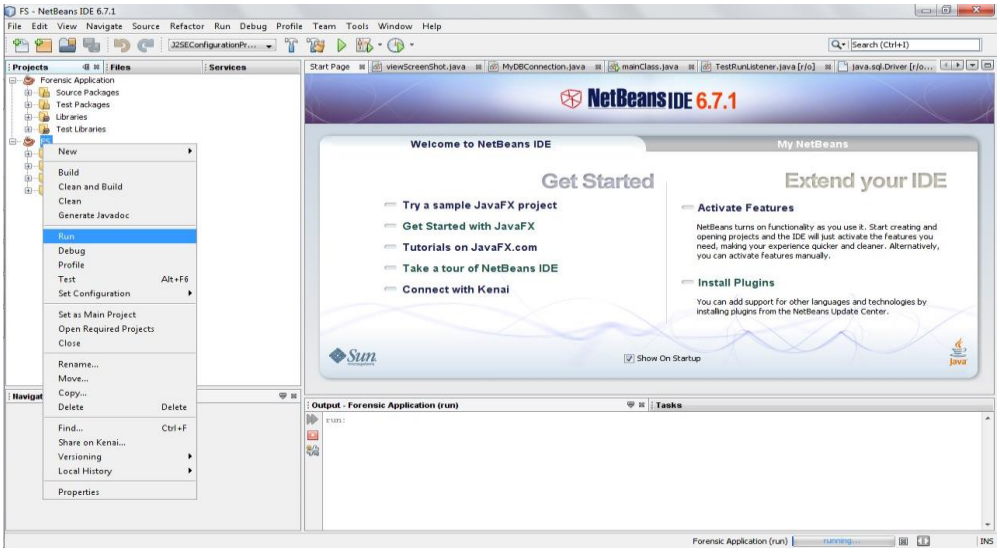

Fig 3: Screenshot of NetBeans IDE 6.7.1: Developed Interface for Testing

Figure 4 shows a screenshot of a scanned image of a West African Senior School Certificate that was opened and viewed in a photoviewer as one of the pictures viewed by a user. This image was captured by the Forensic system as part of a user's activity. For example, if this certificate was captured during an investigation of a fraud or identity-theft case, it could help establish whether the user has been involved in tampering with official documents or using fake credentials. This document, when analyzed in a forensic context, could give a clear insight into the user's activities, such as accessing documents or credentials. Depending on the forensic investigation, this might be evidence of legitimate or fraudulent action.

Fig 4: Screenshot capture opened in photoviewer (One of the pictures viewed by the Researcher).

Figure 5 shows a screenshot of a list of system processes captured by the Forensic application, which was opened in a notepad editor. These processes indicated the activities running on the system at a given time which are important in the context of digital forensics. This image gave a snapshot of the systems active processes, including anti-virus software, and important windows processes. It should be noted that, in forensic investigations, capturing running processes help to determine what activities were occurring, whether any of these processes are potentially harmful, and what security measures were in place.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume IX Issue XII December 2024

Fig 5: Process Captured Opened in a Notepad

Figure 6 is the system flow chart diagram; its main function is to describe the operational flow of the forensic application system, specifically how the system performed the image and process captured. The system works in a way that once it starts running, the image capture timer starts the timing process, the image capture starts, and the image on the screen is captured at a particular time interval. In this paper, every 10 seconds, screenshot was taken, compressed and saved in a folder. The image reference was also saved in a database already created, known as the Forensic database. The image capture continues as far as the user is still logged on and the forensic application is still running. The same goes for the process capture, once the forensic application and the computer user is logged on, the process capture timer starts. So every 11 seconds the process going on in the computer system is captured. The process captured was written in notepad and saved in a folder. The process reference was also saved in the forensic database created. It is important to note that the images and the processes reference captured cannot be viewed in the forensic database created, but can be viewed on the forensic application or in the folders.

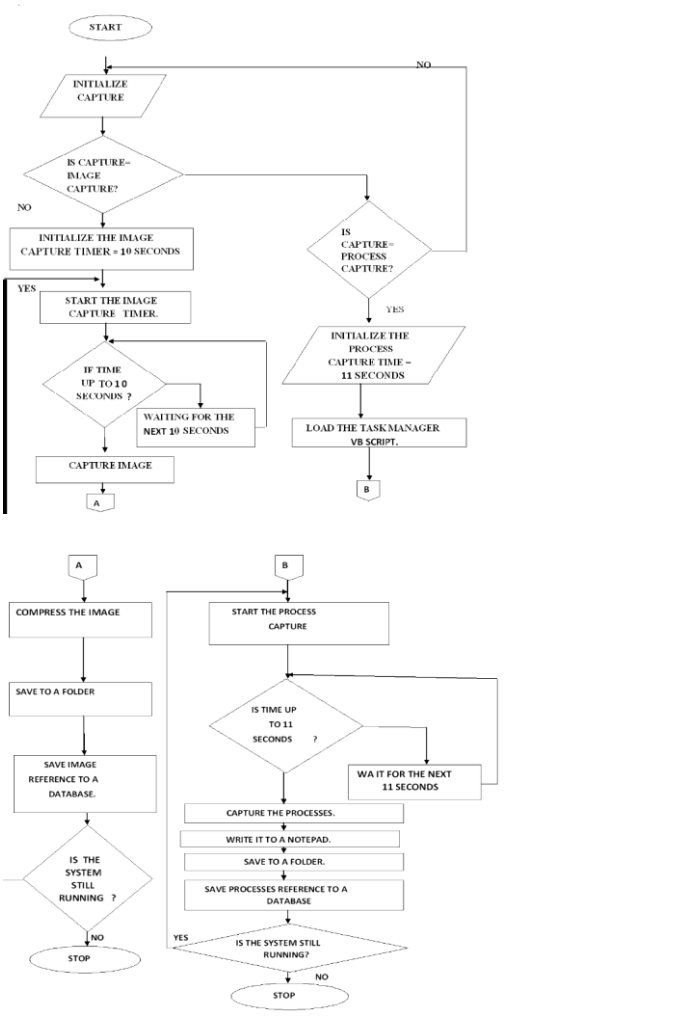

Fig 6: System Flow Chart Describing Operational Flow of Forensic Application System

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume IX Issue XII December 2024

Figure 7 is a flow chart that explains what happens in the forensic interface, it visualizes the flow of data between the forensic expert interface and the core functionalities of the system. In other words, the diagram basically presents a high-level view of how the forensic expert interacts with the system, from authentication to viewing and interacting with captured data. If the forensic expert passes the username and password authentication, the image reference and process database table are loaded, Index.dat are also loaded. When the user wants to view the processes, images captured and Index.dat file, their corresponding references are loaded from the table, for example, process references are loaded from the database process table. The particular reference selected is displayed. One can now select a particular process or image from the list and read it in notepad or view it in photoviewer or the content can be displayed in Index.dat.

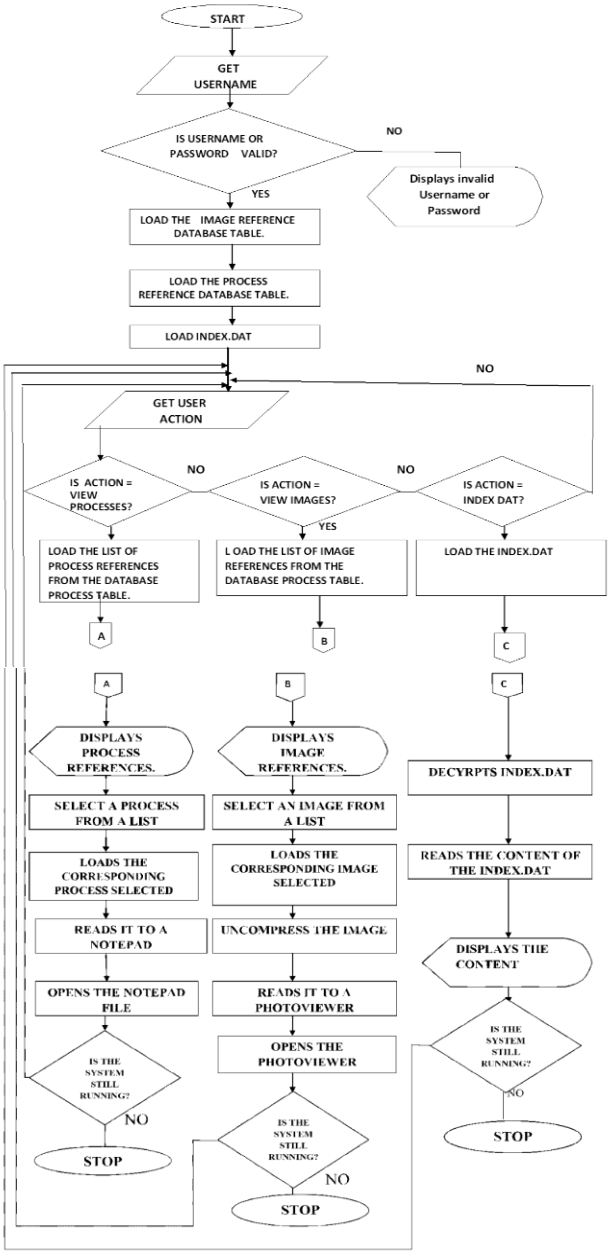

Fig 7: Data Flow Diagram Explaining Processes in Forensic Expert Interface

CONCLUSION

Many criminal investigations in today's technology rich society will involve some aspect of computer forensics. Any individual undertaking cybercrime investigation should be familiar with the basic technologies involved in gathering information; how to properly collect data, and how to ensure that the information will be valid as evidence during trial. It is important to be able to acquire, authenticate and analyze data stored in electronic devices, whether they are run in UNIX, Microsoft operating systems or any other operating systems.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume IX Issue XII December 2024

Furthermore, a competent investigator should understand the technologies involved in tracing and detecting actions of a specific computer user. There are computer crimes everywhere in the world, therefore systems for detecting, monitoring and presenting evidence of computer crimes cannot be undermined and underestimated.

ACKNOWLEDMENT

We are grateful to the Almighty God for the knowledge, wisdom, good hearth and insightfulness given us to write this article.

REFERENCES

1. Valuch, J., Gábriš, T., & Hamuľák, O. Cyber-attacks, information attacks, and postmodern warfare. Baltic Journal of Law & Politics, 10(1), 63-89., 2017.
2. S. Morillo Puent, Cyber Victimization within the Routine Activity Theory, 2022.
3. Reveron, D. S. (Ed.). Cyberspace and national security: threats, opportunities, and power in a virtual world. Georgetown University Press, 2012.
4. Zhang, Y., Xiao, Y., Ghaboosi, K., Zhang, J., & Deng, H., A survey of cybercrimes. Security and Communication Networks, 5(4), 422-437, 2012.
5. Thomas Weigend, Section I-Criminal Law, General Part, Information Society and Penal Law, 2013
6. Dantiki, S. Power through Process: An Administrative Law Framework for United Nations Legislative Resolutions. Geo. J. Int'l L., 40, 655, 2008.
7. European Parliament, European Parliament resolution of 3 October 2017 on the fight against cybercrime (2017/2068(INI)) 2014-2019
8. Markopoulou, D., Papakonstantinou, V., & De Hert, P. The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. Computer Law & Security Review, 35(6), 105336, 2019.
9. Tikkinen-Piri, C., Rohunen, A., & Markkula, J. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review, 34(1), 134-153, 2018.
10. Rui, W., ASEAN Cybersecurity Policy and China-ASEAN Cooperation. China Int'l Stud., 98, p.55, 2023.
11. Akintayo, J. O. AU's cybersecurity policy and its enforcement in Africa. Routledge Companion to Global Cyber-Security Strategy, 608.
12. Curtiss, T. Computer fraud and abuse act enforcement: Cruel, unusual, and due for reform. Wash. L. Rev., 91, 1813, 2016.
13. Perry, S. M., & Brennan, P. K. The prosecution, conviction, and sentencing of techno-criminals: The limits of international cooperation. In Handbook on Crime and Technology (pp. 425-444). Edward Elgar Publishing, 2023.
14. Nolan, A. Cybersecurity and information sharing: Legal challenges and solutions (Vol. 5). Congressional Research Service 2015.
15. Eboibi, F. E. Concerns of cyber criminality in South Africa, Ghana, Ethiopia and Nigeria: rethinking cybercrime policy implementation and institutional accountability. Commonwealth Law Bulletin, 46(1), 78-109, 2020.
16. Alexander Seger, The Budapest Convention on Cybercrime 10 years on, Feb, 16 2012.