Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2023, 10(8):28-39**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Design and implementation of computer based security and monitoring system for forensic experts

Daniel A[1]., Suleiman, I.A[2]

[1]Department of Computer Engineering, Faculty of Engineering, Edo State University Uzairue, Km7, Auchi-Abuja Road, Iyamho-Uzairue Edo State, Nigeria
[2]Department of Agricultural & Bioenvironmental Engineering, School of Engineering Technology, Auchi Polytechnic, Auchi, PMB 13, Auchi, Edo State
Email: aliu.daniel@edouniversity.edu.ng

Abstract Log is an important document produced and retained by the computer system, it records a large number of criminals using computers to commit crimes, and it's a very important source of clues and evidence against computer crime. To well using log to implement computer forensics, there are two problems that need to be solved: one is in a timely manner to the log system protection, in accordance with the procedure of computer forensics to extract the log; second is how to log analysis, find out the crime of "traces", as valid evidence demonstrating to the court. In this project, the process and steps of computer forensics technology are discussed. And existing problem in this project, the status of the computer forensics technology and research of log, analyzes the computer systems of all kinds of log files and format, proposed a relatively perfect supporting computer forensics security audit log method, and according to our current level of technology, design a more suitable for law enforcement agencies in the application of the computer log forensics system.

Keywords Log file; computer forensics; electronic evidence; computer crime; security audit.

1. Introduction

A computer is an electronic device, which accepts and processes data by following sets of instructions (program) to produce an accurate and efficient result (information). Since the ultimate aim of computer is to produce information, the act of computing is often referred to as information processing. The values of computer lie solely on its, high speed (due to its electronic nature), ability to store large amount of data, the unfailing accuracy and precision. These account for its supremacy over manual computation (Dija et al., 2011, Eichin and Rochlis, 2009, Endicott-Popovsky, et al., 2007, Govind, 2014).

The production of computers began late forties with a very small initial investment and has been increasing both in strength and importance. Computer Technology keeps on advancing with remarkable increase in speed, accuracy and reliability. Computing in whatever field, science, business and industry is reaching directly or indirectly into various aspects of our society thereby, without loss of generality has shrunk the world into such a compactness that no part can afford to lag behind or live in isolation (Yu, 2016).

This advent of computer technology, have played a very important role in the aspect of graphics designs, electronic programming, documentation, etc in our society today. It has eliminated the manual system by introduction of computerized system which saves time and conserves human energy in terms of designs and documentations.

This infinite knowledge from the advent of this machine (computer) lead to the study and development of Artificial Intelligence (AI) project like computer based security and monitoring system for forensic experts (Endicott-Popovsky, et al., 2007, Govind, 2014).

According to Wikipedia in 2015 by John McCarthy; artificial intelligence (AI) is the intelligence exhibited by machines or software. It is also the name of the academic field of study in computer science which studies how to create computers and computer software that are capable of intelligent behavior. Major artificial intelligence researchers and other sources define this field as the study and design of intelligent agents, in which an intelligent agent is a system that perceives its environment and takes actions that maximize its chances of success. John McCarthy, who coined the term as far back as 1955, defines it as the science and engineering of making intelligent machines (Ziese, 2016).

Artificial intelligence is a branch of Computer Science concerned with the study and creation of computer systems. Artificial intelligence exhibits some form of intelligence by way of introducing systems that learn new concepts and tasks and also have the ability to reason and draw useful conclusions about the world. Artificial intelligence systems also can understand a natural language or perceive and comprehend a visual scene, and perform other types of feats that require human types of intelligence (Govind, 2014)).

The world is becoming a smaller place in which to live and work. A technological revolution in communications and information exchange has taken place within business, industry and homes. Most developed and developing countries are substantially more invested in information processing and Management than manufacturing goods, and this has affected their professional and personal lives. We bank and transfer money electronically and we are much more likely to receive an E-mail than a letter. It is estimated that the worldwide internet population is 349 million (Gross, 2017).

In this information technology age, some traditional crimes especially those concerning finance and commerce, continue to be upgraded technologically.

Crimes associated with theft and manipulations of data are detected daily. Crimes of violence also 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 or hard disk drive rather than on paper in a notebook. Just as the workforce has gradually converted from manufacturing goods to processing information, criminal activity has to large extent also converted from physical dimension. There calls a need for computer forensic experts and computer based monitoring and security system investigation activity and analysis to be adopted and used in checking the reason for a crime committed (Kohno et al., 2005).

The field of computer forensics has become a critical part of legal systems throughout the world. As early as 2002 the FBI (Federal Bureau of Investigation) stated that, “fifty percent of the cases the FBI now opens involve a computer" (Hayes, 2002). However, the accuracy of the methods and therefore the extent to which forensic data should be admissible is not yet well understood. Therefore, it is not yet safe to make the kinds of claims about computer forensics that can be made about other kinds of forensic evidence that has been studied more completely, such as DNA (Deoxyribonucleic Acid) analysis. The accuracy of DNA analysis is well understood by experts, and the results have been transformational both in current and previous court cases. DNA evidence has been instrumental in convicting criminals, and clearing people who have been wrongly convicted and imprisoned. DNA evidence condenses to a single number (alleles) with a very small, and well defined, probability of error. On the other hand, computer forensic evidence has matured without foundational research to identify broad scientific standards, and without underlying science to support its use as evidence. Another key difference between DNA and computer forensic data is that DNA evidence takes the form of tangible physical objects" created by physical events. Contrast these to computer objects that are created in a virtual world by computer events (Kohno et al., 2005).

Computer-based evidence has only recently become common in court proceedings, but its impact in the legal system has been significant. Cases are frequently decided on evidence obtained from computer systems evidence that many experts claim is unreliable. Consider the recent case State of Connecticut v. Julie Amero in Norwich, Connecticut (Pollitt, 2007). An elementary school substitute teacher, Ms. Amero was accused, tried, and convicted of contributing to the delinquency of minors because a spyware-infected school computer in her class displayed pornographic sites pop-ups during her lecture. The legal system's lack of technical awareness resulted in a conviction that was eventually overturned but permanently impacted Ms. Amero's life and diminished the credibility of our legal system. Judges and juries make in appropriate assumptions because they expect that computer forensic evidence in real life is as reliable and conclusive as it is on television. The impact

of these assumptions cannot be undone merely by reversing a court decision. In many cases such as these, the forensic tools being used are accurate, but the assumptions made about them are wrong. Most judges and lawyers do not understand actions and objects inside computer systems well. Therefore, the legal system is often in the dark as to the validity, or even the significance, of computer evidence. In many ways, computer forensics is behind other methods such as fingerprint analysis, trace evidence of soil samples, cigar ash, the timing of insect infesting corpses, and the chemical traces of poisoning (Kohno et al., 2005) because there have been fewer efforts to measure and improve its accuracy.

For example, one problem arises when the traces of an attack have been altered so that the attack is hidden (Pollitt, 2007). In this case, the data itself can be inaccurate or misleading. In other cases, the data may be accurate but not support the conclusions that are drawn. As an example, Mary may own a file, but there is no way to show that Tom was logged in to Mary's account during the time period in question (Spafford and Weeber. 2012).

Many technical disciplines used in forensic testimony produce results with well-defined margins of error (Stefan, 2011). When technical evidence is presented, an expert witness is frequently asked to answer specific questions (How fast would the car have had to be going for the metal to have crumpled like this. But in computer forensics, analysts are asked to tell complete stories the meaning of a series of events, how those events were triggered, and who triggered them. Unfortunately, an expert may not be able to justify their answer rigorously because the limits of the methods used in computer forensics are not understood as well as those in, say, DNA analysis (Pollitt, 2007).

With the evolution of computer and the internet which has made the world a global village, so has criminals also taken advantage of this technological advancement to engage in different forms of cybercrime ranging from terrorism, internet fraud to the release of sophisticated viruses which is difficult to trace the perpetrators due to lack of sophisticated software that can retrieve information of such activities. This led to the design of a computer based security and monitoring system for forensic experts which will help in tracking the activities of internet users and for recovery of digital evidence of crime committed in a computer system.

The recent innovations and increase in development of expert systems with the introduction of artificial intelligence (AI) in the field of science and technology, yielded positive solutions in solving the problem of tracking system, facial and biometric captures etc built my appetite in developing this system (Security And Monitoring System). The aim of this project is to design and implement a security and monitoring system for forensic experts. This system when implemented will be able to collect captured pictures of the crime scenes, store the data captured and retrieves it in cases of investigation or for analysis. This project is designed to capture the current state of a crime scene and moved for thorough investigation to fish out the possible outcome and evidence. The project employed HTML, MySQL, JavaScript, and PHP scripting programming language in ensuring the design and implementation of a Computer Based Security and Monitoring system that will aid forensic experts in analyzing their investigations and detection of possible reasons of a cause (Spafford and Weeber. 2012).

2 System Study

The three main steps in any computer forensic investigation are acquiring, authenticating, and analyzing of the data. Acquiring the data mainly involves creating a bit-by-bit copy of the hard drive. Authentication is ensuring that the copy used to perform the investigation is an exact replica of the contents of the original hard drive by comparing the checksums of the copy and the original. Analysis of the data is the most important part of the investigation since this is where incriminating evidence may be found. This system research involves an in-depth and thorough study with the operations of the existing manual system and proposing change to the system.

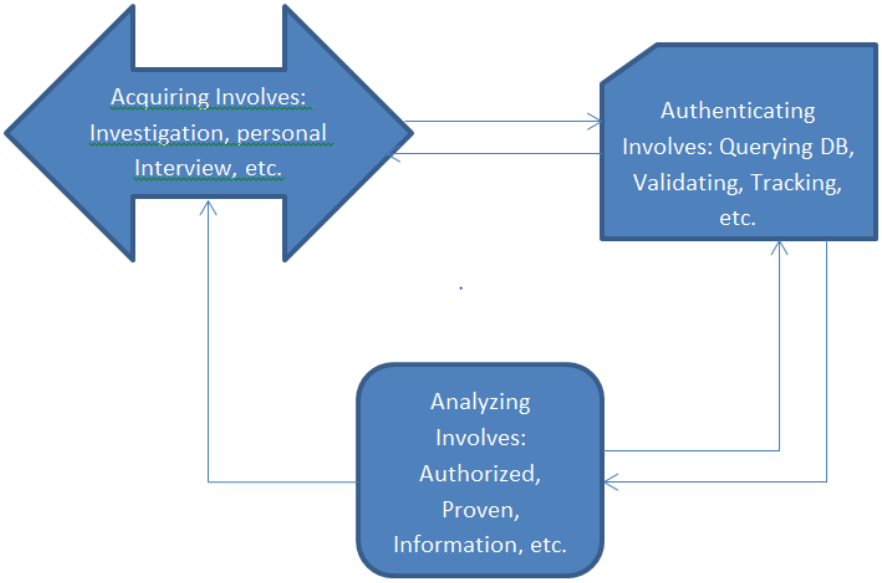

Figure 1: Detailed description of the system

2.1 Analysis of electronic evidence

The analysis of the electronic evidence and the result report is whether the electronic evidence can be displayed in court, as an important process of the criminal evidence of computer crime. Analysis involves the use of a series of keyword search to obtain the most important information; on file attributes, file digital abstract and log analysis; analysis windows exchange files, document fragments and unallocated space data; the electronic evidence do some intelligent correlation analysis, namely: To explore the links between different evidence of the same event. After the completion of the analysis of the electronic evidence the proof of experts give, the ordinary criminal investigation when forensic role similar. To involve the computer crime and the date and time, the hard disk partition, operating system and version, running the forensics tool data and operating system integrity, computer virus assessment, file type, the software license and forensic experts on electronic evidence analysis and evaluation report, etc. file form can be provided to the court of the electronic evidence (Spafford and Weeber. 2012).

2.2 Analysis of the existing system

The existing system operates in a quasi-electronic system. The law enforcement agency simply lack internet policing capability. Nigerian law enforcement agencies are basically technology illiterate; they lack computer forensics training and often result to conducting police raids on Internet service site mainly for the purpose of extortion.

Due to their ineptitude, cybercrime in Nigeria is difficult to prove as it lacks the traditional paper audit trail, which requires the knowledge of specialists in computer technology and internet protocols. They usually mess up fact that would be used against these criminals. They just visit the scene of crime and seize the computer without the knowledge of what to do. Even when an expert is invited, by then the evidence would have been tampered with and the culprit goes scot free due to lack of proof.

2.3 Problems of the existing system

The problems faced by the existing system are as follows:

i. A major problem is that Nigerian law enforcement agencies are basically technology illiterate.
ii. The law enforcement agency does not have a Central Computer Crime Response Wing to act as an agency to advise the state and other investigative agencies.
iii. The activities of cyber cafés and service providers are not monitored.
iv. Most of the officers who are supposed to fight crime are corrupt.

v. User activities on a computer system especially those connected to the internet are not properly monitored.

2.4 Solutions to the problems of the existing system

The possible solutions to the problems faced by the existing system are as follows:

i. Nigerian law enforcement agencies should engage in training forensic experts and employ technology literate personnel's.
ii. The law enforcement agencies develop or build a central data base for tracking any individual's in terms of investigation.
iii. The Nation should enact laws to govern the activities of cyber cafés and service providers.
iv. The Nation should enforce penalty on any law enforcement agency, found violating stipulated laws governing computer crimes.
v. Every User activities on the internet should be properly monitored.

3 Proposed new system

The problems of the existing system are numerous as analyzed in section above. These are enough justification for the new system coupled with the advancement in technology, which has outgrown the existing system. Hence, the entire system has to be changed to the computerized, user friendly system for efficient and reliable results. The existing method needs modification and introduction of the computer design that does not require an expert to operate and collate facts to enable efficient work, output and report generation. The new system captures the system processes and screen shots of the user in intervals of seconds or minutes.

This new system runs at startup and is invisible to the user. It is very reliable, accurate in operation and very comprehensive. Storage and retrieval of cases and reports are adequate and fast searching and a lot is achieved in less time (Stefan, 2011).

3.1 Justification of the proposed new system

The new system is automatic, timely, comprehensive and very accurate in report. The new system was designed and developed to take care of problems of the existing system. It is "its facilities and advantages that justify its integration over the existing system".

3.2 System architecture

The architectural design of a system emphasizes on the design of the systems architecture which describes the structure, behavior and more views of that system and analysis (Mark, 2000).

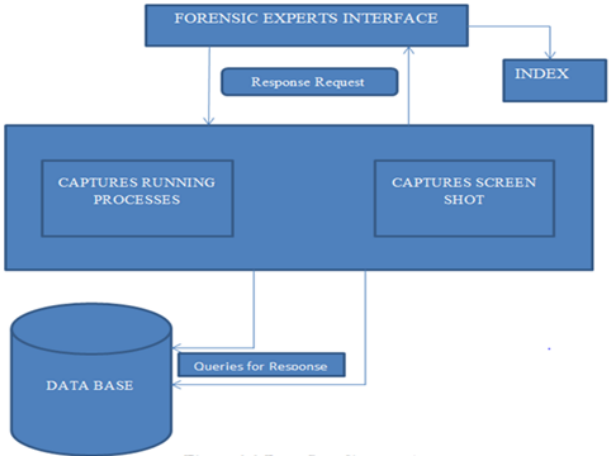

Figure 2: System Architectural Design

3.3 System design

Systems design is the activity of proceeding from an identified set of requirements for a system to a design that meets those requirements. Design of a system can be defined as the process of making detailed plan of the form

or structure of something, emphasizing features such as its appearance, convenience, and efficient functioning. System is a pattern showing how the program can be operated for the purpose of this project. A relational database using SQL will be designed which contains all processes details and report tracked by the system, within work station (Saltzer, et al, 1984). "End to End Argument in System Design" ACM Transactions in Computer System".

3.4 Database Design

Table 1: Admin Login Data Base.

S No	Admin	User Name	Password
1	Officer	E Mail Address	XXXXXXX
2	Officer	E Mail Address	XXXXXXX
3	Officer	E Mail Address	XXXXXXX

Table 2: Tracked Activities by Forensic System From Data Base.

S No	Account Name	Login History	Date	Time
1	Info55@gmail.com	System Action	15/01/95	00:05
2	Dadabool@ya.com	System Action	16/01/95	04:00
3	Ekios4@gmail.com	System Action	18/01/95	14:30
4	Akim1@gmail.com	System Action	01/02/96	12:00
5	Askdem4ify.com	System Action	23/04/00	23:30

4. Methodology

i. The SSADM (Structured Systems Analysis and Design Method) algorithm was used to modify the capturing and storing of information by the system. The SSADM is a structured methodology and it is very popular with the system analysts, it is just like recipe for building computer system, and it is also a lay down steps that should be followed in a clear order. SSADM is made up of a number of stages such like feasibility study etc.

ii. A relational database was developed using SQL (structured query language) version 5 to enhance ease of interaction within the codes, and tracking of all information or processes that occurred in a particular work station.

iii. Setting up the web frame work, SDK (software development kit), and libraries for enhancing coordination of the program.

iv. Coding (Designing the basic interface) of the program to view all activities that has happened within the work station through queries of PHP syntax to the database.

v. Verifying the system performance.

5. System Requirements

System requirements or software requirements are listings of what software programs or hardware devices are required to operate the program or game properly. These are the necessary specifications your computer must have in order to use the software or hardware, (computer hope, 2013).

5.1 Hardware Requirements

Hard Disk	Not less 80GB.
RAM:	Not less 1GB (that is, 1.00).
Processor Speed:	Not less than 1.30GHz

5.2 Software Requirements

Operating System:	Windows not below windows 7 version.
Compiler (Code Editor):	Sublime.
Database software:	SQL SERVER VERSION 5.

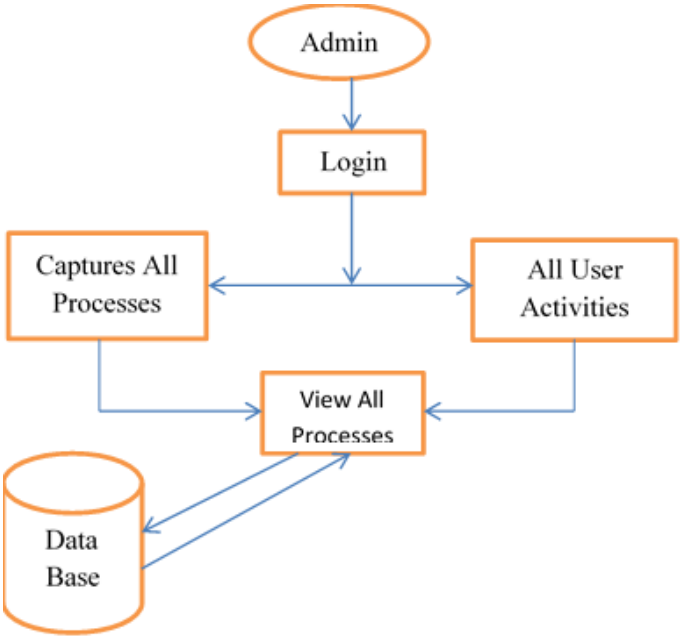

Figure 3: Data Flow Diagram

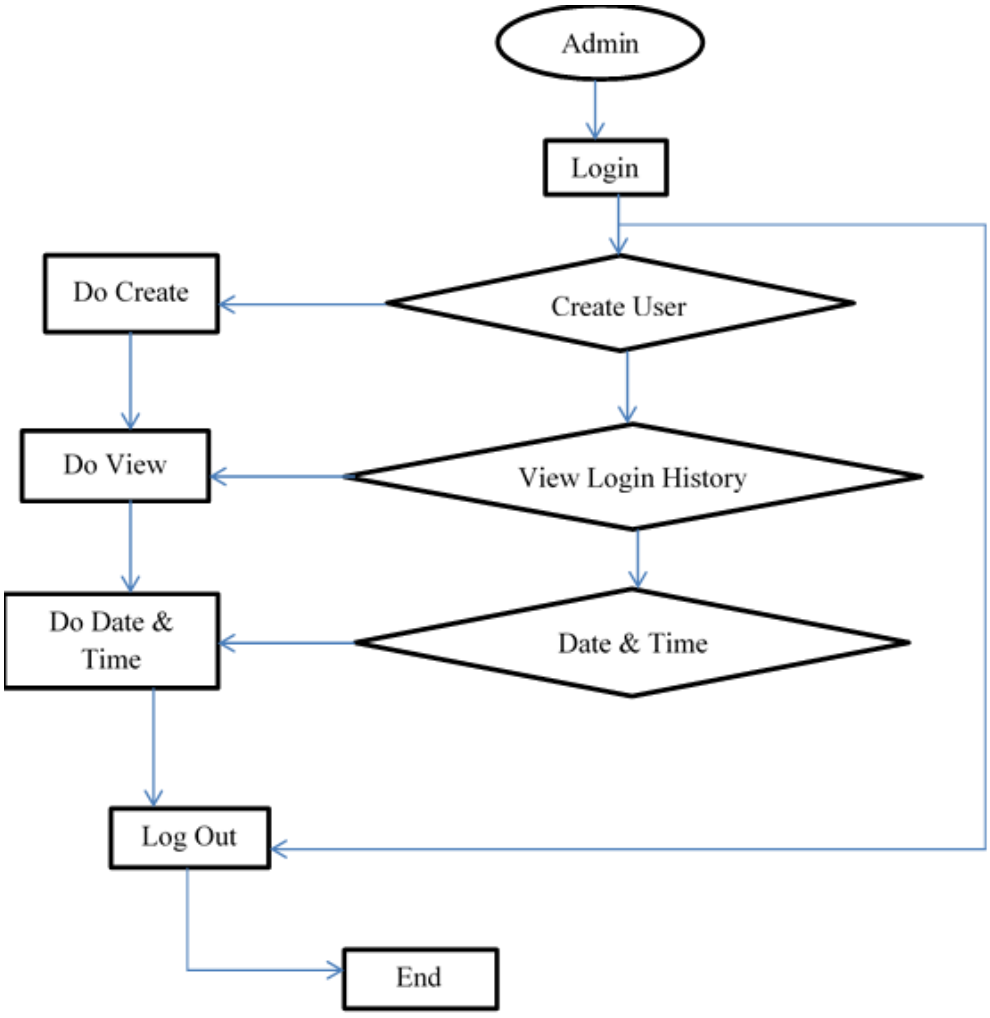

Figure 4: FlowChart

6. Results and Discussion

6.1 System Development

System development is the process of defining, designing, testing, and implementing a new software application or program. It could include the internal development of customized systems, the creation of database systems, or the acquisition of third party developed software. Written standards and procedures must guide all information systems processing functions. The organization's management must define and implement standards and adopt an appropriate system development life cycle methodology governing the process of developing, acquiring, implementing, and maintaining computerized information systems and related technology (System Development Textbook, 2013).

6.2 System implementation

System implementation is putting a planned system into action. It is also the carrying out, execution or practice of a plan, a method, or any design for doing something. In an information technology context, implementation encompasses all the processes involved in getting new software or hardware operating properly in its environment, including installation, configuration, running, testing and making necessary changes (Roxes, 2012).

6.3 Test Run

This testing was carried out by executing the program on a computer system, Sublime text Editor is used for designing and configuring the Security API. The purpose of this test run is as follows

i To check if there is any bugs in the system.
ii To check the effectiveness, efficient operations of the system.
iii To check and make sure that the new system meets the organization or user requirements.

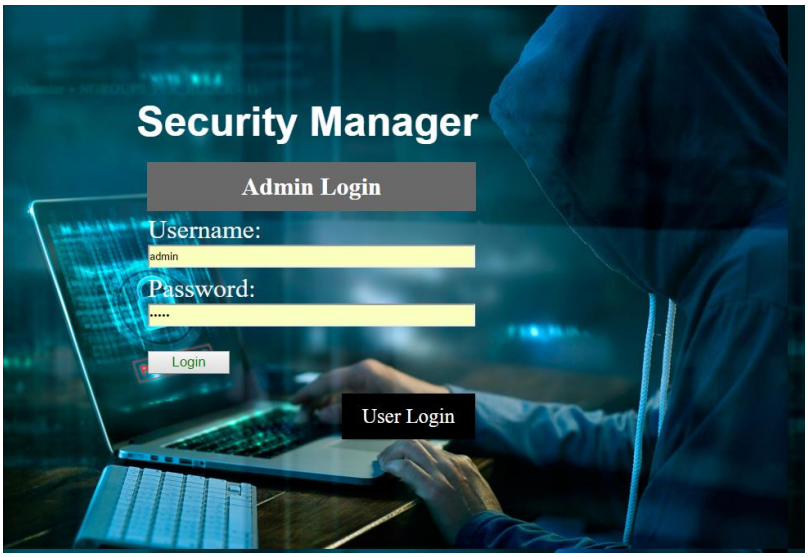

Figure 5: Login Page

Figure 6: Forensic Admin Page

User ID	Login	Login Time	IP Address	MAC Address
10	bilal	2018-03-25 18:12:56	192.168.31	38-59-F9-9D-0A-70
65	usama	2018-03-25 18:14:12	192.168.45	38-59-F9-9D-0A-56
10	bilal	2018-03-25 18:14:23	192.168.87	38-59-F9-9D-0A-45
10	bilal	2018-03-25 18:15:12	192.168.45	38-59-F9-9D-0A-98

Figure 7: View of Login History

User ID	login	password	name	email	country	city	createdon
1	admin	admin	admin	admin	Pakistan	Lahore	2018-03-16 23:23:22
10	bilal	123	bilal	bilal@live.com	China	Shengai	2018-03-20 23:23:25

Figure 8: View of Created User

Figure 9: Forensic User Login Page

Figure 10: Forensic User Page

Documentation

Program Author: NWAOFUFE NNEKA PHILIPPER.
Reg. No: HNDCS2017-068.
Department: COMPUTER SCIENCE.
Program Title: COMPUTER BASED SECURITY AND MONITORING SYSTEM FOR FORENSIC EXPERTS.
Program Purpose: TO MINIMIZE CYBER CRIME.
Program Year: 2020.

7. Conclusion

With the development of computer technology and the popularization of information technology, all kinds of computer crime is becoming more and more serious. How to carry on the computer forensics, obtain the electronic evidence related to computer crime, the computer criminals to justice, become a major problem to be solved in the judicial department. Unlike traditional forensic analysis, as far as possible from the evidence in the sample to obtain more information, the computer forensics analysis is from massive and real-time data to obtain evidence information, making the computer forensics technology is more complex.

8. Recommendations

Having successfully developed the Computer Based Security and Monitoring System for Forensic Experts, I recommend the following for better performance of the application.

i. "Digital Forensics in the Cloud," authors (Marturana, 2012). Recommend that evidence should be collected taking into account the volatility.

ii. (Jang & Kwak, 2015) recommend the recording of video for gathering evidence in order to guarantee the integrity of the process; also, the authors state that is not advisable that just one person collects the evidence

iii. It is recommended the use of forensic images of the digital evidence before performing the analysis.

References

[1]. Dija S, Balan C, Anoop V and Ramani B. "Towards Successful Forensic Recovery of BitLocked Volumes". In Proceedings 6th International Conference on System of Systems Engineering (SoSE), pp. 317--322, Albuquerque, NM, 27-30 June 2011.

[2]. Eichin M. W. and J. A. Rochlis. With Microscope and Tweezers: An Analysis of the Internet Virus of November 2009. In Proceedings of the 2009 IEEE Symposium on Security and Privacy, Oakland, CA, 2009.

[3]. Endicott-Popovsky, J. D. Fluckiger, and D. A.Frincke. Establishing Tap Reliability in Expert Witness Testimony: Using Scenarios to Identify Calibration Needs. In Proceedings of the 2nd International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE), pages 131{144, Seattle, WA, April 2007.

[4]. Govind Singh Tanwar and Dr. Ajeet Singh Poonia, "Live Forensics Analysis: Violations of Business Security Policy", International Conference on Contemporary Computing and Informatics pp. no: 971-976, 2014.

[5]. Gross H.. Analyzing Computer Intrusions. PhD thesis, University of California, San Diego, Department of Electrical and Computer Engineering, 2017.

[6]. Hayes D. (February 14 2007) (quoting Scott C. Williams, supervisory special agent for the FBI's computer analysis and response team in Kansas City). KC to join high-tech fight against high-tech crimes: FBI to open $2 million center here. Kansas City Star, page A1, April 26 2002. E. J. Wagner (2006) The Science of Sherlock Holmes. Wiley, 2006.

[7]. Kohno T., A. Broido, and kc cla_y. Remote physical device _ngerprinting. IEEE Transactions on Dependable and Secure Computing (TDSC), 2(2):93{108, April{June 2005.

[8]. Pollitt M. M.. An Ad Hoc Review of Digital Forensic Models. In Proceedings of the 2nd International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE), pages 43{52, Seattle, WA, April 2007.

[9]. Spafford E. H. and S. A. Weeber. Software forensics: Can we track code to its authors?Technical Report CSD-TR 92-010, Department of Computer Science, Purdue University, 2012.

[10]. Stefan Bolagh, Matej Pondelik. "Capturing Encryption Keys for Digital Analysis", In Proceedings 6th International Conference on Intelligent Data Acquisition and Advanced Computing Systems(IDAACS), pp. 759--763, Prague, 15-17 September 2011.

[11]. Yu Li. Computer forensics and its standard discussion on. computers and Telecommunications. No. 03. (2016). door fly, Jiang Xin, Chen Kangkang. Research and design of computer forensic system. digital technology and application. No. 08. (2013)

[12]. Ziese K. J.. Computer based forensics a case study U.S. support to the U.N. In Proceedings of MAD IV: Computer *Misuse and Anomaly Detection, 2016.*