Computer Forensics and Advanced Methodology

Oghene Augustine Onome

***Abstract:** The field of computer forensics emerged in response to the substantial increase in computer-related crimes occurring annually. This rise in criminal activity can be attributed to the rapid expansion of the internet, which has provided perpetrators with increased opportunities for illicit actions. When a computer system is compromised and an intrusion is detected, it becomes crucial for a specialized forensics team to investigate the incident with the objective of identifying and tracing the responsible party. The outcome of such forensic efforts often leads to legal action being taken against those accountable for the wrongdoing. The methodology employed in computer forensics continually evolves alongside advancements in crime approaches, particularly as attackers leverage emerging technologies. To ensure the accuracy of forensic investigations, it is imperative that the scientific knowledge underlying the forensic process be complemented by the integration of technological tools. A plethora of hardware and software options are available to facilitate the analysis and interpretation of forensic data, thereby enhancing the efficiency and effectiveness of investigations. While the fundamental objectives of computer forensics primarily involve the seamless preservation, identification, extraction, documentation, and analysis of data, the widespread adoption of this discipline is contingent upon the law enforcement community's ability to keep pace with advancements in computing technology. Furthermore, the prevalence of diverse computer devices resulting from the emergence of microcomputer technology also plays a crucial role in shaping the field of computer forensics. This research paper aims to provide a comprehensive overview of computer forensics, encompassing advanced methodologies and detailing various technology tools that facilitate the forensic process. Specific areas of focus include the analysis of encrypted drives, disk analysis techniques, analysis toolkits, investigations involving volatile memory, and the examination of captured network packets. By exploring these aspects, this paper aims to contribute to the existing body of knowledge in the field of computer forensics and support practitioners in their pursuit of effective investigative techniques.*

***Keyword:** Computer Forensics, Encompassing Advanced Methodologies*

I. INTRODUCTION

Technology advancement has changed the traditional patterns of using systems to perform routine tasks within organizations and for individual purposes. Individuals with the intent of defrauding are now leveraging the technology in highly-sophisticated ways to commit crime. And because of this, scammers have improved their strategy to robbing enterprises of all sizes, including government agencies.

Manuscript received on 03 May 2023 | Revised Manuscript received on 23 May 2023 | Manuscript Accepted on 15 June 2023 | Manuscript published on 30 June 2023.
***Correspondence Author(s)**

Dr. Oghene Augustine Onome*, Department of Technology Recovery and Operations Management, eProcess (Ecobank), Abuja, Nigeria. E-mail: augustine.oghene@hotmail.com, ORCID ID: https://orcid.org/0009-0003-0882-2623

With the rapid commercialization of technology as well as the development of the internet, computer crimes continue to increase and evolve in the threat landscape [1]. Moving forward from the 1970s and into the new millennium, computer crimes expanded out from just damage and sabotage into digital crimes such as fraud, denial of service, SPAM, advanced persistent threats (APTs) and extortion. These criminal activities have been going for more than a century, going unnoticed as far back as the 1960s, when the first system crime was perpetrated. As the realization of computer technology started gaining more acceptance universally, corporations, universities, research centers, and government agencies adopted the systems technology to support their data processing functions and were the first to be connected to the outside world. Securing these systems was not on their radar, and the responsibility rested on the system administrators to protect, with a daily routine to ensure the efficiency and accuracy of data processing functions. These were the primary approaches to computer security discipline. Computer systems became a point of interest in the information security, legal, and law enforcement sectors. Before the 1980s, the crime of computers was handled by existing laws. As the crime rate increased, law enforcement agencies made new rules to complement the already existing ones [1]. The first computer crime law, the Florida Computer Crimes Act, was created in 1978 to address fraud, intrusion, and all unauthorized access to computer systems. The progress of computer systems crime during this period automatically led to the formation of the term 'computer forensics' or 'forensic computing'. The IBM personal computer (P.C.) was one of the earliest computers to hit the market, with limited applications and a difficult-to-use interface, which was not too friendly. This then attracted hobbyists to write a program to allow access to the internal peripheral of the systems and operating system. These hobbyists include law enforcement personnel, representatives from government agencies, and organizations who want to share their knowledge on how technology can help gather evidence following a computer crime. Although conducting investigations with this brand of personal computer is relatively simple in comparison to the modern trend of conducting computer forensics investigations, internet development is still at a lower level and not available to every consumer, limiting the scope of most forensics cases and the technology tools required. To accomplish the analysis, forensics investigators must choose between using their talents and using data protection and recovery applications. And evidence is safeguarded by creating logical data backups on magnetic tape, which are then restored to another disk if the data needs to be analyzed. As technology evolves and becomes more accessible, the rate of computer crime rises massively, gaining global attention and driving law enforcement organizations and communities around the world to respond by enacting laws.

According to [1], Canada was the first country in 1983 to amend their Criminal Code, and then other nations began implementing legislation in response to computer crimes. These include the 1984 U.S. Federal Computer Fraud and Abuse Act, the 1989 amendment of the Australian Crimes Act to including Offense Relating to Computers, and the 1990 British Computer Abuse Act. With each country in the world updating its laws, others without fraud cases even began to create new fraud laws. Also, in line with the introduction of the statutes, the forensics society is gaining more publicity.

As a result, most forensics investigators upscaled their skills, which were previously insufficient to get them through a successful forensics job. This resulted in the development of a standard body of knowledge encompassing principles, procedures, and strategies for structuring computer forensics [2]. Also, in line with the introduction of the statutes, the forensics society is gaining more publicity. As a result, most forensics investigators upscaled their skills, which were previously insufficient to get them through a successful forensics job. This resulted in the development of a standard body of knowledge encompassing principles, procedures, and strategies for structuring computer forensics [1]. Between 1995 and 2005, forensics have advanced significantly. As a service delivery facilitator, technology is integrated into our daily lives, allowing people to conduct business from various devices. Furthermore, internet technological innovation has received widespread acceptability because it is freely available to everyone, regardless of location. Therefore, the advancement of technology is viewed as an opportunity for fraudsters to perpetrate cybercrime. The digital evidence of September 11, 2001, for example, was recovered from computers [2].

The field of digital forensics has had to encompass a range of disciplines involving computers, networks, telecommunications, security, law enforcement, and the criminal justice system [1]. This revelation reinforced the fact that criminals were using technology in the same ubiquitous ways as everyday consumers were. The technology evolution has been leveraged to hasten digital crimes resulting in changing the term from computer forensics to digital forensics as the crime is beyond personal computers (P.C.) and cuts across network, printers, or other devices. A digital forensics research workshop in 2001 justified the term ‘computer forensics’ as restricted and recommended the term ‘digital forensics’ to represent entire information technology field [1]. The formalization of digital forensics led to the first publication of digital forensic principles being issued between 1999 and 2000 from the combined works of the International Organization and Computer Evidence, G-8Tech Crime Subcommittee, and the Scientific Working group on the digital proof.

Also, it is essential that the examination of computers and related peripheral devices be expanded to address civil lawsuit concerns for other organizations rather than being restricted to criminal offenses. Because of the ability for any type of device, regardless of size, to have storage space, current technology has allowed hackers to expand their portfolio to include sophisticated models of assaulting their prey. So, the attackers have equally changed the approach making it difficulty to retrieved digital evidence and adapting to new model commercial technology software tools suddenly changes from been functionally specific to digital forensics spill over into other professions that used digital forensics for investigation. The popularity gained by the digital forensics society from inception has resulted in the establishment of multiple law enforcement agencies, organizations and creative agencies and leading to a consistent model of performing forensics investigation with similar principles, methodologies, and techniques globally. The maturity level has scale-up due to the tactical influences that have consistently help the development arising from technology advancements, creation of commercial tools, and integrating with other professions [1]. On the other side, even though the number of strategic impacts may be a little less, the alignment to forensic science and the subsequent development of principles, methodology, and strategies to follow, have resulted in standardization and formality in the structure of digital forensics.

II. COMPUTER FORENSICS

The word "forensics" itself derives from the Latin forensis, which means "public" [3]. According to its implied definition, the word "forensics" refers to a public discussion that typically relates to a legal action. The fact that a court proceeding is a type of public discourse gives the phrase a connection to legal issues. When completing investigations on information technology crimes, forensics is used in a wide range of technical and legal contexts [4]. Modern companies are almost always using computers, therefore computer use in criminal activity is inevitable. These actions may involve child pornography, threatening letters, theft, fraud, and intellectual property, all of which are crimes that may leave evidence. When this machine is being looked at, the investigation is based on suspicions of commission, and the study entails searching through the enormous amounts of data for specific keywords while also looking through the log files to determine the precise frequency of the incidents. This could lead to presenting proof of what a certain individual must have done in violation of the law while demonstrating that another person has not done so. An unlawful act committed using a computer cannot be covered as there are always digital tracks [5]. Computer forensics is the retrieval, analysis, and use of digital evidence in a civil or criminal investigation. The investigation of information technology crimes is not limited to computer, so computer forensics is not restricted to computers alone as there could be other areas evidence can be the source. Digital files can be saved in any medium which becomes a readily available source for computer forensics investigation. Obviously, these include devices such as network servers, smartphones, pagers and laptops. As a result, the scope of computer forensics has expanded to include devices such as cell phones, routers, tablets, global positioning system (GPS) devices, among others. Meanwhile, the misconception with the application of computer forensics is that it focuses mainly to resolve computer crime, that is cybercrime.

Although, this is accurate computer forensics is extended to complement the investigation of other crimes such as murder, financial corruptions, and corporate espionage. In the meantime, a common misunderstanding regarding the application of computer forensics is that it primarily focuses on resolving computer crime, or cybercrime. Despite the fact that this is true, computer forensics has been expanded to support the investigation of other crimes like murder, financial fraud, and corporate espionage. As stated by [5], Seung-Hui Cho committed suicide after killing 32 people and injuring many more on the Virginia Polytechnic campus on April 16, 2007. But, in order to retrace the sequence of events leading up to the murder investigation, the detectives examined Cho's computer, covering every aspect of Cho's actions and his contacts in great detail. So, computer forensics is immensely widened in terms of scope of study when information technology crimes take place. The Enron case investigation uncovered how the employees shredded large quantities of documents, thereby seeking computer forensics experts to retrieve evidence from the employee's computers hard drives as there is always digital tracks of event perform computers [5]. The primary objectives of computer forensics are to retrieve and analyze files with computer forensics hardware and software, utilizing a scientific methodology that is acceptable in a court of law. Contrary to the perception computer forensics can only retrieve deleted files, but files that cannot readily accessible are equally possible to be extracted using computer forensics technology tools.

Furthermore, because it concentrated on hard drives and storage devices, systems forensics was initially known as computer forensics [6]. Also known as digital forensic, the name doesn't really matter; what counts is the outcome. In other words, all forensics specialties use similar procedures for conducting investigations. These procedures include thoroughly examining computer media, network components, software, and memory as sources of evidence. When conducting an inquiry into a crime, computer forensics avoids making assumptions. The evidence is analyzed in all of the devices' peripherals since it helps us understand the crime [5].

All of the domains of a typical I.T. infrastructure, including the user domain, remote access domain, wide area network domain, and internet domain, are covered by system forensics. Everyone is aware of information technology crimes, and they have quickly spread to all fields. As an illustration, the FBI looked into a single case of computer crime in 1985. Yet in 2008, they looked at 52,000 cyber offenses. The amount of computer offenses handled by the FBI has grown significantly as their staff has grown to thousands of people [4].

While disks are more visible and computers are smaller, the fundamental forensic methodology doesn't change. And the basic method includes the following:

- The evidence cannot be changed;
- The recovered evidence must match the original; and
- Analysis must be done on the data without modifying it.

The evidence must not be altered: The proof cannot be changed: When conducting an investigation to find digital trails that will serve as evidence, computer forensics experts are inevitably faced with doubt. Depending on how they happened, cybercrimes receive varying levels of treatment. For instance, in circumstances involving internet invasions, the system's RAM may include the relevant evidence. The danger of tampering with the evidence exists when the power source is disconnected from the system. It is crucial to carefully consider how evidence is extracted [4]. To avoid having to worry about backing up and restoring the evidence on your analysis workstation, each computer that needs to be analyzed may be powered off, booted from a floppy disk, and possibly even have its hard drives mirrored. On the other side, the investigators occasionally encounter difficulties they are unfamiliar with and sometimes nothing happens as planned. The capacity to justify and explain the investigative model is a requirement for computer forensics investigators. There is continuous discussion regarding the appropriate way to begin analyzing a computer for a forensics inquiry; some investigators believe that the power connector should stay attached to the power source, while others believe that it should not be taken out of the computer's back. The investigator will be held accountable for any mistakes it makes during the investigation [4]. The easiest way to evaluate a system and keep the most convincing evidence is to freeze it and look at a copy of the original data. There are disadvantages to this as well, and some businesses might not think that this is the best and most appropriate way to shut down their systems—most importantly, no one knows how long the equipment will stay in that state. Because a computer with malware running on it and the information connected to it will be lost when the system is shut down, many computer forensics professionals did not agree with this strategy [4]. Carefully maintaining the chain of custody has the dual purpose of safeguarding the integrity of your evidence and making it challenging for a defense lawyer to prove that the evidence was tampered with while it was in your possession. The chain of custody is crucial to the entire process of gathering evidence and to the forensics investigation's ability to respond to follow-up queries.

- Who collected the evidence?
- What was process and which location was it at?
- Who accepted the evidence or possession of it?
- How was the evidence stored and protected?
- Who took the evidence from the store location?

Evidence possession must be established by a recorded process that includes the identification of the evidence, the dates and times it was taken and returned, and the justifications for doing so. Keep in mind that a defense attorney will thoroughly go over any document relating to the evidence, cross-reference them, and look for any inconsistencies that might be used to undermine the evidence in their clients' favour. Everyone who had access to the evidence must have tampered with it, the defense attorney likes to assert. Their goal is to demonstrate that the evidence was not properly protected, and when the jury agrees with them, they claim that the evidence may have been altered. This will render the evidence unacceptable.

Retrieval Number: 100.1/ijese.G25520611723
DOI: 10.35940/ijese.G2552.0611723
Journal Website: www.ijese.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

A crucial component of the journey to establish the proof is making sure that the source is not compromised during the collection of the evidence. Nothing should be left behind when gathering evidence, and everything must be done legally because the investigators might come across some of the items when they go back to the crime scene. When visiting an ISP for a computer forensics examination, keep in mind that the computer logs are only kept on the system for a certain period of time before being erased by a cron job. So, the forensics investigators must move quickly and efficiently. If not, investigators might request that the logs be retained so they won't be overwritten while working on other tasks that are important to obtaining evidence. Every piece of evidence collected at the crime scene must be labeled. According to [4], an individual is designated by a law enforcement agency to be the evidence custodian at the scene of a large-scale investigation. This regulation forbids a situation where more than one person is in charge of gathering evidence and designates one person as the responsible party. Yet, conducting a forensics investigation for a major corporation requires that the evidence be well preserved, the evidence custodian adhere to tight guidelines, and that every item be labeled with a serial number and registered correctly with the owner's name. Also, moving the evidence should be done with caution in order to avoid damage from improper handling. Like hard drives and laptops, some of the items are delicate. Always use packaging that is static-free; pink bubble wrap is frequently static-free and the greyish plastic is because it has been treated with graphite dust. Evidence should be packaged and sealed in a container with a sign stating that it has been opened by the authorized person as per accepted practice. Any investigational task requiring the opening of the seal must be recorded with a narration outlining precisely what was done and by whom. The evidence needs to be repackaged and secured in a safety locker before being resealed in the container with a fresh label. The evidence needs to be kept in a cold, dry area designed to prevent damages. Also, unauthorized persons must be prevented from entering this site by controlling access. By restricting access, the evidence is protected from public access and every forensics investigator is required to record the inquiry. Finding and recording evidence might be difficult at times s o, it is advisable to solicit someone's assistance in documenting while the investigator looks for additional proof. The documentation phase should follow best practices to enable detailed reports with all the facts, including versioning the document with the appropriate numbers. It is necessary to document additional elements, including collection instruments and the model used to gather and analyze the evidence.

Confirm the Authenticity of the Evidence: It can be hard to determine whether a piece of evidence is authentic as the evidence might have been compromised by environmental factors. Therefore, the investigators must show that the evidence is unaltered. The condition of the things before the crime was committed may be the only indication of change [4]. The chain of custody and other regulations for managing evidence provide the jury with assurance that no random errors were made as a result of digital wear and tear. A digital track and a link to the source are present in all data and images found in a computer. Yet, the evidence has a time stamp that gives the appearance that it was created at a specific moment and that it was amended at the same time because the system leaves a trace when a piece of data has been altered. In some cases, it might have been taken from the computer. All of this is done to validate the evidence by authenticating the verifiers. The capacity of technology to enable the authentication of evidence, such as MD5 and SHA, allows for the creation of hashes of both the entire disk and individual files within the system.

Perform analysis on the data without modifying it: The evidence must not be changed throughout the analysis phase. Before beginning the analysis, this precaution should be taken to protect the original copy. As you retrieve and return the initial evidence to the proper storage place, you should keep a record of the analysis in your reports and chain of custody records. In the past, it was only individuals who could readily travel through and recollect commands that were previously executed were able to undertake analysis on the command-line interface. Yet, as technology has advanced, operating systems with user-friendly graphical interfaces have made it easier for all forensics experts to analyze the data. No forensics specialist should be confined to a particular software and must become conversant with various contexts. There are several quick disk image copying tools that are suitable for forensics examination. It is always required to create a bit-for-bit clone of the original drive copy as a forensics backup. If hard disk sectors need to be examined, the operating system's default method of making backup copies won't transfer erased files as well. Hard drives are important components in the forensics process when examining crimes involving information technology. Before beginning the analysis and if more jobs are needed for the inspection, hard disk images created using MD5 hash should be used to ensure a full investigation. Before beginning further analysis, the MD5 hash process must be successfully finished. The hash values should be obtained, recorded, and then the analysis can start.

III. DIGITAL FORENSICS

Cybercrime's methodology is constantly changing and never stays the same. The attackers' technical proficiency, advanced technological capabilities, and the potential financial rewards make this conceivable [7]. Today's cybercriminals carry out sophisticated attacks that simultaneously take advantage of a wide range of endpoints and massive digital networks, leading to data breaches and disclosure. With technology at its top standard, thorough forensics investigation procedures are essential. Digital traces are constantly left after information technology crimes. Otherwise put, [5] define digital forensics as the recovery, examination, and use of digital evidence in a civil or criminal investigation. Yet, the forensics technique used to investigate crimes does not only use computers as sources of evidence [8]. In addition to laptops and desktop computers, mobile devices, networks, and cloud systems are also included in the subject of digital forensics.

Hence, the main sources of evidence for the forensics method of investigation are any objects that contain digital data. In a nutshell, the method used for gathering, analyzing, and accepting the evidence in a court of law makes digital forensics a science. The technologies used to retrieve and analyze digital evidence have been put through years of rigorous testing, according to [5].

Digital forensics techniques are constantly evolving along with the digital space. The effectiveness and efficiency of a digital forensics investigation are challenged by the rise in technology adaptability. Regardless of how digital crimes have evolved, the procedures for generating digital evidence should be carefully organized and free of any gaps that can compromise the process' integrity [9]. Digital evidence is information that has been compiled and processed in a way that makes it pertinent to an inquiry and supports a particular conclusion or finding. Also, the evidence must have a clear chain of custody to ensure that it hasn't been tampered with, according to [9]. The continuity of control over the evidence, known as the chain of custody, allows for an unaltered account to be given in court. Investigators must provide testimony that the chain of custody was maintained during the investigation; otherwise, the court may reject the evidence [1]. Businesses will be better equipped to gather and handle digital evidence in accordance with legal criteria for prosecuting digital intruders if they have a solid understanding of the technical needs for practicing digital forensics. The execution of digital forensics will be compromised in the absence of sufficient technological expertise without the investigators' knowledge. On the other side, this organization might not be using standard forensics principles and methodologies, and it might be portraying itself in the market as lacking the necessary expertise to conduct a digital forensic investigation.

IV. DIGITAL FORENSICS INVESTIGATION TYPES

Performing digital forensics is primarily done to find out information technology offenses. Also, it depends on the type of establishment that investigates computer crimes [2]. A federal, state, or local law enforcement entity may ask the laboratory to conduct an investigation that covers the full spectrum of criminal crimes. There is a lot of variety since diverse technologies are increasingly being used in areas of human life other than only the more traditional computer-based crimes. Yet, a digital forensics investigation is typically a course of activity related to an incident with the aim of determining the underlying factors that contributed to the crime. And to do this, the evidence must be retrieved from many technological systems linked to the main malicious device [1]. Since the 1980s, when computer forensics was first introduced, the application of forensics science has grown into a fundamental building block that has enabled the integration of the consistent principles that underpin repeatable methodologies and techniques across a number of other information security disciplines. An appropriate level of confidence that re-validate and verified processes are adopted to secure digital data is provided by enterprises embracing digital forensics science to uncover concealed evidence.

V. DIGITAL FORENSICS PROCESSES

The study of digital evidence from any devices, such as a laptop used to commit cybercrime, is done using a framework called "digital forensics"[7]. The method is universal in that it may be utilized for any type of digital crime or incident investigation, including those involving computer forensics, mobile forensics, Internet forensics, and emerging digital technologies. The methods used by those who commit crimes in other categories, such as murderers and robbers, differ[6]. The methodology used to process digital evidence must be fully understood by digital forensic. The methodology includes a significant quantity of evidence-processing documentation and a step-by-step chain of custody system. The processes can be split into multiple steps, though there may be both more and fewer steps that are similar. The authenticity of the evidence they produce is what matters most.

Yet, digital forensics procedures can be used in both business and, on occasion, private investigations as well as all types of criminal investigations. Every forensic investigator needs to develop a method that will allow them to carry out an effective forensic investigation, according to [10]. In addition, the forensic expert must have a thorough understanding of the tools employed, the procedures, and the outcome of the evidence. Technology-based tools are used to aid the process, and critical thinking should be applied throughout the procedure to make sure the evidence is not weakened.

In some circumstances, a forensics investigation may reveal similarities, and this will call for more strategic thinking in order to be productive or yield results. At this point, the investigator needs to be flexible because one approach could not work for all situations involving multiple operating systems, various logical and physical network architectures, criminal elements, and prospective suspects, among others.

However, below are the procedures for uncovering any forensics investigation in order to provide evidence that won't raise any questions.

Search Authority: The first forensic procedure is search authority. Without the right to search and without any evidence being produced, the act will still be illegal. There are numerous ways to exercise the search authority [11]. A search warrant, subpoena, or permission may be sufficient in a criminal prosecution. Parties to civil lawsuits may agree to a search that the court has authorized. In a legal context, this first process is therefore applicable.

Identification: This step involves finding the precise location of the data sources, and it starts primarily by making a list of the devices that appear to be the sources of the evidence. When a crime has been committed, this should ideally be the first stage of the digital forensics investigation [7]. An hypothesis about what might have happened is formed when an incident or crime is identified. As a result, the event that started the investigation will be used to support the hypothesis, which will determine which device to employ to launch the inquiry and perhaps gather evidence.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

While conducting analysis on a laptop, the first step in the identification phase is determining which files on a volume are accessible, active, or deleted from the computer. Planning and the use of technological tools will support all forensic procedures and result in strong evidence rather than unsatisfactory findings. In order to effectively plan and prepare before beginning an investigation into a crime incidence, all investigators—including those from law enforcement agencies, digital forensic experts, and business investigators—must pay attention to this [7]. Beside fingerprint analysis and DNA profiling, preparing at a physical crime scene also includes taking notes about the environment's layout. Nonetheless, setting up and installing digital forensics tools, such as software and hardware, may be necessary in cases of information technology crime to ease the preparation before the investigation begins. The standard identification procedure should be followed after the investigators are happy with the level of preparation; this involves recordkeeping and safeguarding the integrity of the evidence. Also, when identifying evidence, investigators must use the principles of evidence integrity. The integrity of the exercise will be impacted if the investigator touches the laptop, disconnects it from the cords, or removes it from the docking station after seizing it for examination. Only significant tasks that can be justified in retrospect and do not compromise the integrity of the evidence should be undertaken with prudence.

A clear chain of custody is also essential to protecting the validity of the evidence. In the case of a computer crime, the chain of custody aids in preventing any sort of indiscipline in the evidence collection process [11]. That is, from the time the things are gathered until the evidence is presented in court, someone is responsible for all of the evidence. Before beginning the process of looking for evidence when examining a computer storage device, the raw data must first be extracted from the device. To avoid tampering with the data while carrying out this activity, care must be taken not to change the data contained on the device throughout the copying process. The transferred data must be a perfect duplicate of the original. The outcome of assessing the copy at this time must be consistent with the original's content. To comply with the custody requirements, all of these actions must be documented [7]. A crucial step in the digital forensics process is the chain of custody. The evidence might be excluded from a case if the chain of custody is not followed exactly as it should be.

Evidence Collection: [12] state that the methods used to acquire digital evidence must guarantee the preservation of the evidence's integrity and provide justification where necessary. Evidence gathering in a computer forensics investigation refers to data capture. A device, such as a laptop, with raw content that has been determined to be pertinent to the inquiry may be examined by a forensic specialist [7]. [13] assert that the correct management and security of evidence are essential; as a result, mistakes made during the collecting of the evidence may cause it to be tainted and, as a result, not forensically sound. Experts in forensics must understand very well that actions performed during cross-examination of the evidence should not change the initial evidence.

Also, evidence collection can be done as live data most importantly in response to the incident [14]. The primary purpose of the collection is to preserve volatile evidence that will further the investigation. In reality, more information is collected faster, such as logs file and file listing. Investigators must exercise caution because the methods they take to gather evidence may alter certain portions of it. As a result, when forensics investigators are conducting their normal investigative procedures, suitable documentation techniques should be used with justification [13]. The saying "If you didn't write it down, it didn't happen" is a recurrent one in law enforcement. Every action made while running the processes must be recorded in some form as part of forensics investigations. This includes thorough notes and diagrams[13]. If the validity of the evidence is ever questioned, thorough documentation enables examiners to retrace the sequence of events. Real - time data data collection and analysis make it easier to handle feedback concerns and reduce the likelihood that data will be lost in the course of the occurrence. Yet collecting and analyzing live data carries a certain amount of risk. This should be kept in mind to limit system modifications performed while data gathering is taking place. The manual approach chosen may bring excessive and unneeded changes to the system, disrupt business, destroy evidence, cause systems to crash, and make the environment exposed to easy exploration by attackers. An automated process would be the most preferable choice.

According to [14], there are five essential factors to be considered when deciding if a live response is appropriate in handling forensics investigation.

- What is the reason to believe volatile data contains information critical to the investigation that is not present elsewhere?
- Is there an alternative to running the live response such as in an ideal manner, that would have minimal impact on the target system?
- Is the number of affected systems large, making it infeasible to perform forensic duplications on all of them?
- Is there any risk that forensic duplications will take an excessive amount of time, or potentially fail?
- Are there any legal reasons why it would be advisable to keep as much data as possible?

One must constantly assess the tools and processes to ensure they are appropriate as computer forensics evolves. Both free and paid programs are available that offer the capability needed to complete the task[14]. The information gathered throughout an investigation is continually assessed based on how well it will help address concerns related to the research.

Evidence Examination Phase: This involves gathering prospective evidence from numerous data sources and preparing it for use. To support the whole chain of custody process, it is crucial for digital forensics professionals to record actions and the manner the data is handled[7]. In order to make the data more organized and intelligible and to facilitate the examination of the evidence, the analyst should employ forensic tools and techniques to extract crucial information at the outset, before beginning the inquiry.

Also, the forensic tool can perform this, eliminating the need for a manual process that might perhaps lead to errors and raise serious questions about the authenticity of the content. Moore's rule is used in forensics procedures to hasten the identification of essential data. When there is a limited amount of time and resources available to carry out a forensic investigation, Moore’s law is employed to help manage the situation. The use of the event type to highlight regions of data interest is another strategy to expedite the investigation phase.

One illustration is carrying out malicious tasks. In actuality, web activity includes things like email messages, website caching, bookmarked pages, and cookies. The definition and organization of the data for the forensics expert's seamless analysis of the actual content of the evidence are other steps in the examination phase's structure. The report generated by the use of the forensics tools during the examination phase must reflect the evidence related to the incident under investigation and include as much extra information as feasible in the format of the copied data [7]. The ability to store information in different digital formats has different effects on the results of the investigation, particularly the raw data format, which is used to extract data directly from data sources. EnCase, Smart, AFF, and Prodiscover are some of the expanded storage formats.

Moreover, all digital devices are designed to hold information securely and accessible when there is a need for forensics activity. But, technology has made it possible to recover data from any type of storage after deletion as long as it is not overwritten. Besides, data filtering is another mechanism that makes reducing the data volume to an acceptable quantity to ease active digital forensics investigations. Conventional filtering techniques embedded on a database with cryptographic hash values known as files [7]. Multiple files in the computer are owned by the operating system, software, and few applications, but this file doesn't have much information to aid in forensics investigation. However, the use of the file database in combination with digital forensic tools, which makes it possible to improve the understanding of files that are known to be useful to filter them out if considered useless. In forensics investigations, the internal clock known as the system timestamps plays a significant role. Also, the time can be changed to synchronize with the back-end components so that they are all located in the same region.

Analysis Phase: [7] define this as the processing of information that addresses the investigation's objective to determine the facts surrounding an event, the importance of the evidence, and the perpetrator. The preparation of the acquired data for analysis is the result of the examination phase. The following statistical approaches, manual analysis techniques, protocols understanding methods, and data formats links are all included in the analysis process. This approach is primarily iterative and begins by identifying data-related hypotheses that are likely supported by strong evidence. However, as the analysis advances, it generates new hypotheses that might call for the collection of additional data objects. The investigators continue the analysis until the results are sufficient to successfully complete the investigation; otherwise, the case might be deemed to be infeasible.

When conducting forensics investigation on systems uncovered by the evidence, it is discovered that data seen by the application is not the same as what the operating system sees. What is stored in the storage are bits and bytes format of the storage. The deleted data from a hard drive can be recovered regardless of the layers of the sectors. Every crime has its evidence and so crimes committed through digital devices, the evidence is located within that device. Potential evidence is the source from an email from a particular email address. They are making it possible to link the mail, multiple people. Forensics investigation leveraging collaboration tools like email can lead to identifying evidence faster compare another criminal case. Defining the hypothesis before the investigation begins is made simple by the case. To help with the forensics analysis, strings and keywords can occasionally be used. It is possible to extract more evidence connected to the crime after the evidence has been recognized based on the case by using the right string and keyword combinations. In addition to using forensic techniques, this approach can be automated. Similar to how evidence can be tracked in a criminal case, pattern matching techniques can be used, however it depends on the theories formed from the case. One example is the theft of a credit card, where the evidence may be tracked thanks to the card numbers.

The Presentation Phase: The presentation will follow once the analysis is complete. At a legally recognized court, the investigation's final paperwork and presentation will be made during this period. Based on the evaluation of the data, the final report is based on impartial conclusions with sufficient assurance. In a nutshell, the presentation step is the method by which the examiner communicates to the interested party the findings from the analysis phase in the form of reports, as per [7]. The final report represents the complete forensics process, chain of custody, and integrity evidence based on meticulous documenting of each process taken from beginning to end, with time of the actions. In conclusion, the report provides context for the work that has been done, the investigator, and the hypotheses that were examined.

VI. NETWORK FORENSICS

[15] define network forensics as the collection, recording, and analysis of network events to identify the source of security attacks or other problematic instances. It is a branch of digital forensics whose main objective is to look into computer crimes. Before presenting the case in court, network forensics gather evidence to show how the crime was committed and who was guilty by watching and capturing real-time network traffic and other relevant data from network devices. Investigators in the field of forensics should consider the network environment rather than just the data stored on hard drives and operating systems [16]. A network forensics investigator can go to the network itself to gather data about an attack that is currently underway or search through historical data that may be available after a company has experienced a security breach with someone trying to move in permanently, someone who has the ability to observe and put what they see into context.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

It is important to note that the following material is provided for informational purposes only and is not intended to be used for any other purpose. The network is a crucial component of the investigation that cannot be overlooked because it has a record of every transmission that has gone through it. The expert needs to be aware of the network's boundaries before beginning a forensics examination. The ports' perimeter ranges from 0 to 65,535. As forensics investigators, you are expected to understand that particular ports indicate particular kinds of traffic, according to [17]. So, it is crucial that each investigator become familiar with and proficient in all of the ports. The forensics expert needs to be aware that 1,024 of the 65,535 ports are well-known and primarily used by programs in order to limit the number of ports to memorize. Also, the application's associated port numbers range from 25 to 50; you must be aware of this (Muniz, Joseph, & Aamir, 2018). Although it is standard practice to presume that recognized services are connected to particular ports when examining networks, applications don't have to operate over commonly related ports in order to save time [18]. In network forensics, you must identify a wide range of packets in order to create a clear picture of the investigation. The result is helpful when analyzing packet captures from compromised servers since it shows which files were accessed as well as which components were involved in handling a certain request. Also, it expedites the process of determining if the imposed controls are operational and fulfilling their main goals. When a malicious request is received, which occurs in every business, the protective controls typically return a 404 (NOT FOUND) or 403 (FORBIDDEN) response code rather than a 200 signaling everything is normal.

At the same time, forensics experts must become familiar with the fundamental network logs format and the technical terms needed to carry out a network forensics process. And the areas that follow will shed light on the forensics processes:

- Inter-networking refresher
- Exposure to various types of logs
- Case studies on records and packet structures

The following forensics tools such as as Apache Log viewer, Sawmill, Kali Linux, and Wireshark will complement the process. When a program is deployed within a company's infrastructure to communicate with the outside world, it passes through numerous layers and leaves evidence of its transmission as logs on various devices. All of these components could be firewalls, proxy servers, routers, switches, f5 load balancers, and application servers. On the other hand, it is crucial that the network forensics expert have a basic knowledge of the various kinds of logs created at different endpoints during data transmission [18]. When the scenarios don't include network captures, these logs come in very handy because they allow the investigators to draw conclusions about the forensics investigation and arrive at a definitive conclusion. The devices have the intelligence to analyze the logs, but occasionally it's necessary to have different results for comparison, so a third-party log parser is required for the log generated. The network forensics expert also needs to be familiar with the process for handling evidence identities. However, network forensics is a subset of digital forensics. Its approach differs from the regular forensics investigations. Unlike other focus areas of forensics investigation, network forensics focus areas are to manage volatile and dynamic information. The study of network forensically must pre-arrange inorder t capture and store network traffic [15]. Without obtaining a duplicate of it, such as CCTV footage for a specific occurrence, it is never possible to examine what happened within a network. Investigators can reconstruct the full footage once it is made available, which makes it easier to identify the criminal.

VII. MOBILE FORENSICS

Because of improvements in their capabilities, such as the fact that they are arguably more essential than a personal computer, mobile device forensics has gained greater attention recently and is now regarded as a significant topic of research. The capacity to constantly record movement, activities, and offer insight into human behaviour is impressive. They surpass the personal computer family as a means of communication (Arnes & Andre, 2017). The specific techniques, rules, and best practices for investigation frequently change along with mobile phones as an embedded system [5].

It hasn't always been common to take cellphone forensics seriously. If you asked a law enforcement official about a cellphone investigation in 2008, you were likely to hear that no one worked on cellphone investigations in the lab or that smartphones didn't contain anything of value. Yet, the equipment needed for forensic purposes is also lacking and is probably quite expensive for the vast majority of law enforcement officers [19]. Statistically, the examination of mobile device data should be proportionally similar to computer examinations, but unfortunately, this is not the case. In reality, computer evidence is more welcome and acceptable as criminal evidence, but mobile device evidence is gradually drawing attention but still at a low rate [19]. Participants in the law enforcement survey have categorically stated that demands for the analysis of data from mobile devices are more common than requests for any other kind of electronic evidence [20]. Mobile devices have unquestionably incorporated into our life. They have revolutionized how tasks are carried out, and as a result, the method has given rise to the emergence of mobile phone forensics. The method is now a massive repository that contains private and sensitive data about its owner.

However, while the number of people using mobile phones increases exponentially around the world, more people are switching from personal computers to mobile phones. The transition is mostly being felt because of the soaring demand for smart phones [20]. Global mobile data traffic increased by a compound annual growth rate of 42% from 8.8 exabytes in 2017 to 71 exabytes per month in 2022, according to a report by Ericsson. Smartphones are thought to be the most convenient way to transmit data and track movement. The stored data on the device subsequently became a key source of evidence for forensics investigations addressing computer crimes, civil crimes, and high-profile cases due to the increased usage of mobile phones in both daily life and criminal activity [19].

With the rise in global population and the people's growing reliance on technology, as well as the fact that mobile devices contain a lot more information than desktop computers do, the proliferation of mobile devices will only continue to rise. In other words, mobile device, forensics investigators now have a very important need for this unprecedented volume of information on mobile phones. The procedure for gathering mobile devices, examining the evidence obtained on them, and communicating their findings must be completely understood by the forensics investigators. Holistically speaking, the technical strategy for gathering and analyzing evidence should not be the only focus of the mobile device forensics paradigm. Instead, it ought to concentrate on forensically examining the legal aspects of the device.

In the meanwhile, the same way that evidence from computers is used for inquiry, so too is evidence from mobile devices. The distinction is that in typical machines, evidence is kept on a hard drive with a normal interface for low-level access. Mobile devices, in contrast, don't have immediate, low-level access to the data they store on flash memory. Hence, the forensic investigator must comprehend the various approaches to gather the evidence without modifying the content of the data [7]. The chain of custody and maintaining the integrity of the evidence are two essential forensic investigative procedures. According to[5], investigators shouldn't make any changes to digital device storage material that could later be used as evidence in court. Since there are so many portable devices on the market from so many different suppliers, it might be difficult for forensic experts to understand the device design even if each mobile device has a unique design in terms of how each component of the underlying board is inserted. Strict attention must be paid to the lack of a uniform model that all manufacturers of mobile devices might use. The routine of forensics experts to locate criminal evidence will be less difficult once there is a generally accepted standard design [5]. A major issue arises with cellphone forensics. Due to the typically low onboard memory capacity of smartphones, memory utilization and compression are crucial. This takes into account the network-connected devices, and as a result, the data's content is continuously changing. When the gadget is being cross-examined, evidence extraction may be altered. Nonetheless, best practices must be followed in order to protect the user's data. Moreover, only properly documented procedures will allow for admissible evidence.

According to [20], mobile phones are dynamic embedded systems associated with multiple challenges concerning evidence extraction and for analyzing purpose. The exponential increas in the numbers of different mobile devices flooding the market from various manufactures makes it challenging to adopt a single process as well as a tool to perform a forensics examination on the device. Beyond that, the technology of portable mobile devices is continuously evolving with emerging technology introduced into the industry. Also, the devices are designed with a variety of operating systems running in them. Therefore forensics experts need to acquire special skills to extract evidence and analyze the data presented as evidence. Forensic investigation of mobile devices comes with unique challenges compared to computer forensics. As a result, law enforcement and forensics experts debate how digital evidence should be extracted from mobile devices. Outlined below are the reasons:

- **Hardware disparity**: Many manufacturers have saturated the market with several brands of mobile devices on a global scale. To execute a practical examination on the device so that the evidence produced is admissible in court, the forensics experts must struggle in order to comprehend this distinction.
- **Mobile Operating Systems**: In contrast to personal computers, which are known to run a small number of operating systems like Windows, which has taken over the industry and is found in every home, mobile devices employ a variety of operating systems. Redhat is renowned for its dependability and other Unix variants like AIX, Solarise, and HP-Unix. With such a wide range of mobile device operating systems, the job of the forensic expert becomes increasingly challenging.
- **Mobile Devive platform security features:** Mobile device designs include incorporated security features to protect user data and privacy. A forensics specialist will find it challenging to retrieve evidence from the analysis due to this security feature.
- **Avoidance of data modification**: Data extraction from any device should be done carefully by forensics examiners. Nonetheless, it can be difficult to follow these guidelines with all mobile devices because it is uncommon to examine a gadget without turning it on. But, turning the device on is likely to change the information stored inside. Even when the device appears to be in an inactive mode, some processes and programs are still active. Hence, when a mobile device's state is changed to a new one, the data may be modified or lost altogether.
- **Anti-forensic approach**: Anti-forensic practices including data masking, data obfuscation, data forging, and protected wiping can tend to make forensic tasks very challenging.
- **Passcode recovery:** Although users of mobile devices secure their vital information as well as maintain their privacy passcodes on their mobile device, forensics experts face challenges with this practice when trying to access them. Though the use some known techniques, these techniques sometimes don't work with all the multiple versions of operating systems running on the device.
- **Absence of resources**: Resources needed by the examiners may not be available, thereby making it impossible to start the forensic processes.
- **Dynamic nature of the evidence**: The forensics procedure prohibited changing the evidence while conducting the inquiry. Although sometimes there is unintentional evidence manipulation, this is exceedingly difficult to follow.
- **Accidental reset**: This could happen if you investigate using a mobile device as your only choice, however it will cause data loss.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

- **Malicious programs**: It's possible that malware on some of the mobile devices being examined has spread to every aspect of the device, presenting a problem for the examiner.
- **Legal Challenges**: Criminal activity sometimes transcends boundaries of place. The forensics investigator must be knowledgeable about the crime and the local laws governing the crime's location.

A. Applying Forensics Processes and Procedures

The International Association of Computer Investigative Specialist (IACIS) and the International Society of Forensic Computer Examiners both acknowledge the forensics procedure applied to mobile devices (ISFCE). Both groups impose restrictions on the forensics industry [19]. The process and procedure documentation in forensics and technology investigation in general should only be used as a reference. There are variables in every investigation situation, including the usage of software tools, hardware devices, and the sort of investigation the evidence from mobile devices supports. The examiner can be linked to proper processes by adopting a clearly defined forensic approach early on. Also, the procedure needs to start with scientific methodologies, which will provide it a solid base and meticulous processing. When an examiner testifies regarding the investigation's report, assurance is created by the basis and process. The forensic process for mobile devices is not unique from the forensic process for personal computers, but the ways in which each phase of the process is carried out vary due to the nature of the devices. The standard procedure is outlined below:

- Acquisition of evidence
- Analysis / Examination of the evidence.
  - Define and understand objectives
  - Obtain relevant data.
  - Inspect the data content.
  - Perform any necessary conversion or normalization.
  - Select a method
  - Perform analysis
  - Evaluate the result.
- Presentation of the evidence.
- Generation of a final report

VIII. FORENSICS TECHNOLOGY TOOLS

The field of digital forensics has experienced tremendous advancement over the last decade; all the known best practices in years past are no longer applicable [21]. Things we just could not do with what was available ten years ago are now conceivable thanks to emerging technologies and techniques. And also, [21] because digital forensics is a science, we must follow the scientific methods with our job. A wide range of forensics tools, many of which are available for free download in the open-source community, are flooding the market specifically for use in digital forensics investigations. Knowing what each tool can and cannot perform is crucial for the expert while inspecting the majority of the tools. The investigators must have a similar understanding of how the tools work and how the background process operates while the analysis phase is underway [22]. Let's use an airline pilot as an example to explain why it is crucial that forensics investigators understand the background investigation procedure.

An airline pilot operating a commercial jet makes use of numerous systems, including hydraulic, electrical, and navigational. Most of the time, those systems work without issue, and frequently, the computer manages them automatically. When a system aboard a plane malfunctions, the pilot must understand how it works so that he or she can either fix the issue or find a manual solution. This should also apply in the case for digital forensic investigators and the tools they use.

Although necessary to the investigation, the technology tools employed by forensics professionals are not used to testify in court [4]. Before using any program for forensics, one should first check that the software accomplishes what it's meant to do. To determine if and how to use these tools, it is important to verify the results of the deployment of forensics technology tools [23]. There are many different kinds of tools that can be used, but one place to start looking at the market for tools is the computer forensics tool testing program run by the American National Institute of Justice under the direction of NIST. The website www.cftt.nist.gov is a database of forensics tools that have been evaluated for their ability to carry out fundamental forensic tasks like imaging drives and extracting data, as well as for their performance on these tasks as well as for their actual testing specifications, testing software, and methodology.

IX. MOBILE DEVICES FORENSICS TOOLS

The evolution of technology has made it impossible to have a particular tool mapped to mobile devices. There are a variety of portable devices flooding the market from different manufactures as well as vast numbers of forensic software tools. And sometimes, these tools may not provide the required capability to perform extensive analysis on the device[19]. Mobile device forensics in today's world does not involve merely attaching a cable, clicking a Go button, and waiting for completion. This requires a comprehensive examination of the mobile devices when it matters most to comprehend the tool profession continuum. Moreover, according to [19]. There are various ways that mobile forensics are different from computer forensics, and one important distinction has to do with how the devices are handled while being examined. Taking into account the structural layout of mobile devices, adopting a specific instrument for the forensic investigation and evidence extraction might be quite risky. Unlike computer forensics, the professional can execute the complete process using a single tool. The cost associated with purchasing these tools influences which tools are used. Whilst software tools from open sources can be downloaded, there is a restriction because not all mobile forensics solutions are available there, and no one tool can enable thorough process investigation and mobile device analysis. However, performing analysis on multiple mobile devices for the extraction of evidence is not possible with mobile forensic tools.

Retrieval Number: 100.1/ijese.G25520611723
DOI: 10.35940/ijese.G2552.0611723
Journal Website: www.ijese.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

In this case, the forensic expert resorts to using computer forensic tools for in-depth analysis [19]. Many digital devices will be used in a single event under investigation, so it would be advantageous to be able to examine all of the data gathered on a single platform. Verification and validation are crucial after purchasing forensic tools to make sure they can be applied to a specific set of knowns [19]. International organization for standard (ISO) 9000:2005 outlines quality management system standards and defines both verification and validation separately. Also, in both definitions, objective evidence is used, which ISO 9000:2005 defines as data supporting the existence of a variety of something.

Listed below are mobile forensic tools

- Paraben Project a Phone ICD8ooo and Paraben Project a Phone Flex: This is camera setup provide both H.D. video and 8-megapixel pictures.
- Fernico ZRT3: This tool has a combination of camera and H.D. camera along with materials to hold the device and camera in place.
- Teel Technologies: Eclipse 3 Pro: This tool like ZRT3 combines camera, mount, and platform as well as software solution capable of capturing the images and document extraction.
- Flasher Boxes: This is a mobile forensic tool generally used by mobile device technicians to resolve to nonresponsive mobile devices, like for unlocking a device for unrestricted access with any telecoms provider. It facilitates flashing a new version of the device firmware, ROM, O.S., and setting.
- JTAG (Joint European Test Action Group): This tool was developed in 1985 as a conventional boundary-scan testing tool. Use to scan mobile devices to confirm connections on the printed circuit board to debug the equipment without physical access to the flash.
- TCK (Test Clock): This test establishes the synchronization of the internal state of the device between components. Portable device design has multiple parts using the various form of timing.
- TMS (Test Mode Select): This tool controls the TAP controller and depends on the test clock to determine the state of the process.
- TDI (Test Data In): This tool work by accepting data from a software diagnostic and forward to its target.
- TDO (Test Data Out): This tool work by accepting data from the target and sends it to the diagnostic software.

A. Operating Systems / Computer Forensic Tools

Forensic tools make excavation of evidence from a computer possible. As a result, the forensic expert must ensure that the real tools needed to begin the investigation are available and that the following conditions have been met, such as an appropriately completed license that has been accepted and confirmed for usage by a laboratory employee [4]. In order to conduct a computer forensics investigation, software tools and peripherals are needed. Computer forensics entails the identification, extraction, preservation, and documentation of computer data. When purchasing a forensic tool, be sure that it offers additional programs in addition to those that it uses for forensics. Many tools have a single purpose, and if achieving set objectives is the goal, they apply to do so. But, when needs span many services, this may not be beneficial. Instead, acquiring forensic software packages with a range of capabilities is necessary in order to complete any task.

Outlined below are the computers and operating systems forensics Tools.

- **Data Collection Tool**: DFF (Digital Forensics Framework): is an open-source tool that has many useful resources built into it.
- **Slowloris DDOS Tool**: This is an attack tool that serves as a denial of service tool that allows an attacker to disrupt services of another computer and enterprise network with negligible effort and bandwidth.
- **Cuckoo Sandbox** is a malware analysis sandbox: This is needed when building a digital forensics lab.
- **Cisco Snort**: This is a free open source tool that works as a network intrusion detection system. Snort detects vulnerabilities and other possible attacks.
- **FTK Imager**: This is a popular tool used by forensic investigators for data ingestion, analysis, and reporting.
- **FireEye Redline** is a data collection tool for extracting storage-based images, FireEye Redline is by forensic computer specialist for collecting memory dumps. And its applicable only window base operating system and dedicated mainly for memory forensics.
- **P2Explorer data analysis tool**: Primarily to view disk image files and explore their contents. The interface is user friendly.
- plain sight data collection tool; Primarily for beginner forensic investigators in collecting and viewing information.
- **WebUtil Data Collection Tool**: This is a client-side tool for collecting java-based events. Other security tools mainly use them to extracting events that can be helpful in later analysis. Due to the java plugins, it considers better of then another clients-side tool.
- **IBM QRadar** is a data collection tool, refer to as the SIEM that is popular in large enterprise environments.
- **Prodiscover Basics:** This is a hard drive imaging and analysis tool.
- **Splunk** is a data collection platform to generate, collect, and search for machine-generated data. The data source can be logs, trends, and other data sources.
- **RSA Security Analytics**: This is a data analysis tool. It is a suite of software and hardware which collects a vast quantity of network data and provides machine-learning-based insight into the data, specifically around threats and data breaches.
- **WinHex Data** analysis tool that is a windows hex viewer and editor.

X. FORENSIC READINESS

The importance of carefully carrying out a forensic procedure, such as evidence extraction, evidence preservation, and presentation of the digital proof, is thought to be the main factor in reducing the negative effects of digital crime, disputes, and incidents on organizational companies. Therefore, it becomes an essential for a digital forensic readiness model to be adopted as part of the enterprise business strategy and goals. The forensic examination must be conducted in response to a forensic crime according to the framework of forensic investigations. Also, experts are needed to carry out the investigation process that results in the gathering of evidence and the presentation of that evidence in a way that makes it admissible in court. However, it is sometimes difficult to have reliable evidence because it may not be available at the time of the investigation[1]. Compared to the capacity to gather evidence in a law enforcement setting, the possibility to proactively obtain digital evidence is more common in the enterprise operational environment. So, the lack of digital evidence in the early stages of the investigation raises the possibility that it won't be accessible afterwards. As a result, it is crucial that businesses make use of technology to close any gaps in information security and digital forensics. Enterprises must understand that capturing digital evidence is a crucial part of identifying illegal activity inside the company and reducing the risk involved [1]. The capacity of an organization to proactively maximize the use of electronically stored information in order to lower the expense of digital forensic investigations is known as digital forensic readiness.

Individuals and organizations have taken use of technology's exponential growth to stay fiercely competitive in their respective markets. Also, cybercriminals are getting more chances to perpetrate crimes [1]. As a result, hackers have redirected their efforts to capitalize on the vast amounts of digital information produced by regular human interaction, making an effective and efficient information security program crucial. The risk of losing important business information data and assets has been addressed by businesses struggling to implement systems such information security programs, robust architectural designs, and a well-articulated strategy in accordance with the company goals. Regardless of compliance, it is important to make sure that the working environment is secure to prevent any unanticipated incidents from negatively damaging the organization. . Knowing the underlying reasons of the event, the organization must take proactive measures to reduce its impact and resume normal business operations. Businesses all over the world run their technological operations by implementing best practices to secure vital assets and customer data. Digital evidence is frequently difficult to recover since there is a good chance that it has been corrupted or overlooked.

According to [1], in 2001, John Tan released a paper that presented the idea of a digital forensic preparedness program. The program was expected to assist the company in taking a precise and informed stance regarding its business risks and the need of gathering digital forensic evidence. Implementing the digital forensic readiness paradigm offers every firm two important advantages.

- Widen the intelligence to retrieve trustworthy digital evidence.
- Curtail the cost of forensics investigations when the digital crime takes place.

In addition, the digital forensic readiness model focuses on what and how companies can effectively retrieve digital evidence when a crime incidence occurs rather than only on how the incident is resolved. To facilitate the forensic process with conclusive digital forensic evidence that will not spark a disagreement, it is best practice for all parties involved to play a significant role in the investigation.

A. Financial Benefit Associated with Digital Forensics Readiness Model

The financial costs associated with adopting the digital forensics readiness model practice will increase if the businesses' current information security program has flaws and doesn't cover every part of the business. The security program may be strong and have high coverage in some cases, but it may not always be widely used to align the program's content with the operational element of the organization. Doing a digital forensic program is less expensive when its information is applied to improving an organization's security posture. Finally, prior to the program being implemented, management permission is requested (Sachowski & Jason, 2016). Organizations must be able to compare the program's tangible and intangible components on an apples-to-apples basis in order to make an educated and informed decision about whether establishing a digital forensic readiness program is feasible. Once the organization's management has given the notion their approval, the next step is to synchronize all security measures with the forensic program so that both processes can operate simultaneously.

B. Digital Forensics Readiness Model

Based on the concept that digital crimes can occur anyway, a thorough evaluation to identify hazards and determine the amount of effect from a cybersecurity controls viewpoint is considered to be of lower risk and poses no significant harm to the enterprise's security posture. Notwithstanding the risk category, businesses must nonetheless implement additional layers of security measures in order to methodically gather evidence in the event that cybercrimes occur (Sachowski & Jason, 2016). When enterprises realize the need for specific investigative intelligence, the next step is to mitigate this need through efficient and competent capabilities. Outlined below are the articulated benefits of the forensic readiness model.

- **Minimizes financial implications**: Based on the presumption that digital crimes may occur, the business will minimize the amount of disturbance to the performance of the business function and concentrate on forensic investigative processes that are less cost-effective in producing final admissible digital evidence.
- **Controls Expansion:** Security measures should be expanded to include notice, containment, and remediation as well as all other facets of the organizational ecosystems. To identify and counteract a wide range of cyber risks before they emerge as an incident and cause harm, proactive real-time monitoring must be implemented and used.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

- **Digital Crime Obstacle**s: Detecting malicious behavior is one advantage of real-time data collection and monitoring. Real-time data collection is used to warm up potential cybercriminals who have been apprehended.
- **Governance and Regulatory Compliance**: Businesses that have strong governance frameworks are in a better position to respond quickly to incidents before they interrupt operations. Additionally, adhering to legal regulations ensures a secure environment that offers customers and other stakeholders protection for their data and assets.
- **Law enforcement**: A platform for collaboration to address forensics investigations collectively is provided by operating in compliance with all regulatory regulations. In the case of an incident, law enforcement and the local team of investigators will collaborate to produce digital evidence both before and after the incident occurs.

C. Digital Forensic Challenges

As technology develops, the market is being overrun by a variety of technological products. for instance, computers, networks, portable mobile devices, and embedded systems. Attackers have also created sophisticated methods to undermine technology and compromise data integrity during the progression (Arnes & Andre, 2017). The enormous amount of unstructured data and the inherent ambiguities and faults that it includes present the major challenges for digital forensics. Despite that, it takes an extremely long time to finish an inquiry. There are not enough technological tools available to support forensic processes, and those that are, cannot be used when large amounts of evidence must be extracted and processed. The introduction of computational forensics methodology can be used to address the technological challenges. Investigating data amounts that have grown exponentially over time, the complexity of technology infrastructure, the growth of interconnection across many social networks, and the quality of the evidence produced are all made possible. It may not always be admissible as evidence in a legal proceeding. According to [7], computational forensics is the hypothesis-driven investigation of a specific forensic problem using computers, with the primary goal of discovery and advancement of forensic knowledge. Applying computational forensics method to the processes of the investigation will attract the following benefits.

- **Extensive Forensic Investigation**: Most significantly, the impact of a crime depends on how far it spreads across the company. Additionally, the data breach becomes concerning as a result of the crime. To successfully complete the forensic process from beginning to end with convincing evidence, the computational forensic technique is necessary. Given that the organization has a widespread malware infection on more than three thousand computers, and all of the machines have an internet connection either directly or indirectly, it is possible to automatically identify the digital traces of illicit activity introduced through malware attacks [7]. Large-scale network traffic analysis in digital forensic investigations provides the foundation for research using neurofuzzy (N.F.) approaches. The results of subsequent research reveal a pathway for known hostile activities in network traffic within businesses, which is made possible by algorithms built to handle large amounts of datasets with poor categorization.
- **Automation:** Forensic processes are traditionally driven by a standard approach in conjunction with a checklist in order not to skip any step. This model will not meet expectations as there could be possible errors in the final evidence generated. However, introducing automation to run the entire process will eliminate mistakes and reduce human intervention leading to production of quality forensic process, according to [7]. To easily carry out a repeatable forensic reconstruction experience, the researchers use a virtual environment. Automating I.P. address geolocation using triangulation based on several, geographically separated measurements is another study to show how useful automation may speed up the forensic process. This study made strides toward confirming the value of conducting automated digital forensic investigations.
- **Analysis:** Computational techniques must be used to simplify the analytical stage of conducting digital forensics investigations. Despite the fact that the regular process contains abnormalities, they are recognized thanks to years of experience. The computational technique will still solve the following issues with timeframes, link analysis, and outcome forecasting. In the end, computational methods will make it simple for forensic investigators to accurately forecast the outcome of the evidence in a brief amount of time. When computing techniques are used to quickly identify and extract cryptographic keys from volatile memory in portable laptop and computer devices, this is an example of a forensic investigation analysis. The forensic analysis step is accelerated by the computational technique since it presents an interrogative strategy that can be used. The results demonstrate that there is a good chance of finding forensic keys. The results of numerous studies conducted by individuals to show the effectiveness of using a computational method to undertake forensic analysis demonstrated that this phase is quicker regardless of the type of investigation [7]. The usefulness of intrusion detection by correlation feature selection, to automatically get a feature set for network traffic without involving expert knowledge, was explored in Nguyen's study work in 2010. The study's findings showed that it is possible to eliminate redundant features while maintaining classification accuracy, which leads to better performance when compared to alternative approaches.
- **Forensic Integrity:** What matters most is the integrity of the entire process and outcome, which is the admissibility of the evidence, regardless of the methodology used for the forensic processes. To facilitate the forensics process without errors, the computational model's new dimensions must guarantee that the evidence produced carries the weight of integrity and has the chain of custody embedded into the computational methods [7]. Forensic tool testing ought to be carried out at all levels, much like automated testing for software quality assurance.

Retrieval Number: 100.1/ijese.G25520611723
DOI: 10.35940/ijese.G2552.0611723
Journal Website: www.ijese.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

XI. RESTRAINT WITH COMPUTATIONAL FORENSICS METHODOLOGY

The development of computational forensics methodology goes beyond the extraction of digital evidence and encompasses the entire forensics process flow, as seen below:

- **Signal and Image processing:** Using computational technology, the signal and images obtained during forensic collection are accurately processed for both human and machine analysis.
- **Computer Vision:** Recognition of items in computer-generated images and videos is simplified by the computational forensics methodology.
- **Statistical pattern recognition**: It involves using statistics to help gather evidence and distinguish between that which is based on known facts and that which is based on probability.
- **Machine Learning**: This makes it easier to comprehend forensics from the viewpoint of a learner.
- **Data mining:** This speeds up processing huge data volumes for forensic investigation and evidence gathering.
- **Robotics:** Robotics in computational forensics enables machines to mimic human movement. Reconstructing forensic testing is one example.

XII. CONCLUSION

In conclusion, the branch of the science of digital forensics known as computer forensics deals with the retrieval of evidence found in computer devices using digital traces. Regardless of the exact sectors where forensics is used, there are numerous difficulties. The gathering of digital evidence is where the core issues lie. This difficulty manifests in a variety of ways, including data access, restrictions on search and seizure, and the ease with which evidence can be tampered with or manipulated. The dynamics of having the actual evidence with the complete chain of custody present and documented is essential for the admissibility of the evidence. The forensics technique needs to be in line with changes in all the devices for the investigators to be effective and efficient in the investigative process, which is tough given how quickly technology is advancing.

In the meantime, the advent of computer technology in 1980 increased the use of the devices by everyone, which prompted their acceptance as a tool for criminal activity. Governments were prompted to establish commissions or agencies with the assistance of their laws in order to adopt laws that would support the commission's main goal and purpose as the crime rate increased tremendously with each passing year. The Federal Bureau of Intelligence's computer analysis and response team was created as a result (FBI).

The digital forensic technique requires an understanding of the criminal environment. Following forensic processes and using technology tools to support important aspects of evidence extractions are essential for conducting forensically correct investigations. Additionally, because of the worldwide digitization affecting every element of the sector and the accessibility of the internet to both law enforcement and cyber-actors, it is challenging to identify digital footprints at the site of the crime and on the devices utilized. As well as non-digital crimes including civil crimes, homicide, and other cases, digital forensics now plays a vital part in identifying information technology crime. Criminals are less likely to alter the digital evidence if the forensics process is carried out meticulously and without compromising any investigations. Graduate degrees in computer science, criminal justice, law, mathematics, writing, and forensics science are just a few of the ways competent digital forensic investigators pick up their talents. On-the-job, practical, and certification programs are various ways to acquire the necessary expertise.

DECLARATION

Funding/ Grants/ Financial Support	No, I did not receive.
Conflicts of Interest/ Competing Interests	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material/ Data Access Statement	Not relevant.
Authors Contributions	I am only the sole author of the article.

REFERENCES

1. Sachowski and Jason, Implementing Digital Forensics Readiness, Rockland, Massachusetts : Syngress, 2016. [CrossRef]
2. Jones and C. V. Andrew, Buidling a Digital Forensic Laboratory, Hoboken, New Jersey: Syngress , 2011.
3. Messier and Ric, Operating System Forensics, Rockland, Massachusetts : Syngress , 2015. [CrossRef]
4. Heiser, K. Jay G and W. G, Computer Forensics: Incident Response Essentials, Boston: Addison-Wesley Professional , 2001 .
5. Hayes and D. R, A Practical Guide to Digital Forensics Investigation, 2nd Edition, New York City: Pearson IT Certification , 2020.
6. Vacca, J. R and R. R, System Forensics, Investigation, and Response, Massachusetts: Jones and Bartlett Learning, 2010.
7. Arnes and Andre, Digital Forensics, Hoboken, New Jersey : Wiley , 2017.
8. Sammons and John, Gigital Forensics, Massachusetts : Syngress, 2015. [CrossRef]
9. Easttom and Chuck, System Forensics, Investigation, and Response, 3rd Editon, Sudbury, Massachustts: Jones & Bartlett Learning , 2017.
10. Oettinger and William, Learn Computer Forensics, Birmingham, UK: Packt Publishing , 2020.
11. John and Sammons, The Basic of Digital Forensics, 2nd Editon, Massachusetts: Syngress , 2014. [CrossRef]
12. Sapronov, K. Shaaban and Ayman, Practical Windows Forensics, Birmingham, UK: Packt Publishing , 2016.
13. Johansen and Gerard, Digital Forensics and Incident Response - Second Edition, Birmingham, UK: Packt Publishing , 2020.
14. Mandia, L. Kevin, P. Jason and Mathew, Incident Response & Computer Forensics, Third Edition, New York City: McGraw-Hill , 2014.
15. Datt and Samir, Learning Network Forensics, Birmingham, UK: Packt Publishing , 2016.
16. Messier and Ric, Network Foreniscs, Hoboken, New Jersey : Wiley , 2017.
17. Muniz, L. Joseph and Aamir, Investigating the Cyber Breach: The Digital Forensics Guide for the Network Engineer, First Edition, United State: Cisco Press , 2018.
18. Jaswal and Nipun, Hands-On Network Forensics, Birmingham, UK: Packt Publishing , 2019 .

19. Reiber and Lee, Mobile Forensics Investigations: A Guide to Evidence Collection, Analysis, and Presentation, New York City : Mc-Graw-Hill , 2015.
20. Tamma, B. Rohit, M. Satish, S. Heather and Oleg, Practical Mobile Forensics - Fourth Edition, Birmingham, UK: Packt Publishing , 2020.
21. Grant, S. Nicholas and J. II, Unified Communications Forensics, Rockland, Massachusetts : Syngress , 2013.
22. Sheward and Mike, Hands-on Incident Response and Digital Forensics, Swindon, United Kingom: BCS Learning & Development Limited , 2018.
23. Johnson and Leighton, Computer Incident Response and Forensics Team Management, Rockland, Massachusetts : Syngress , 2013. [CrossRef]

AUTHOR PROFILE

Dr. Oghene Augustine, currently serves as technology recovery and operations management head for eProcess International, the technology hub for ECOBANK TRANSNATIONAL INTERNATIONAL. He joined eProcess in 2011 and has brought more than 22 years of technology industry leadership, enterprise architecture expertise, hands-on experience in information systems, information technologies architecture and infrastructure operations management into the role. He is very vast in cloud strategy, cybersecurity, and business continuity. As a Senior Information Technology professional, Dr. Augustine Oghene oversees technology recovery activities of critical services of ECOBANK TRANSNATIONAL INTERNATIONAL financial services in thirty-five countries. He is also responsible for leading service architecture and implementation of all operational and business support systems that the organization uses to operate and manage its business across thirty-five countries, as well as the design and development of digital platform. He is equally responsible for providing evolving enterprise architecture services to enhance customer’s experience.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.