The Growing Attention on the Growth of Digital Forensics

Thowg Alrasheed
Student at Cybersecurity, College of Computer and information Sciences, Jouf University
Sakaka Jouf, Saudi Arabia
401205534@ju.edu.sa

***Abstract*—The current modern society highly depends on information technology (IT), communication networks, information and communication technologies (ICT), and the internet of things (IoT). In the same way, there has also been an increasing attention on the Cyber-physical systems and technologies and cloud-based services in undertaking the same. To increase their efficiency, companies and other business organisations are resorting to cutting-edge information and communication technologies in building their competitive edge in the industry. A focus on the value of these new approaches has seen a rapid growth in commercial activities in different industries, businesses, and a transformation of people's live. However, amidst these positive benefits, there have been a growing fair share of challenges emanating from these developments. As an amicable solution, the growth of digital forensics has proved beneficial in aiding in investigations and prosecuting of criminal elements disrupting individuals and corporates in handling their personal and commercial activities. While digital forensics is considered effective in dealing with the present tech-based challenges, it also faces certain challenges in its execution. Though these technologies have brought immense ease and convenience, the advancement in new technological paradigms has motivated cybercriminals to violate laws and conduct cybercrime, electronic crime, and computer crime. A management of these technical and legal challenges could offer the much-needed reprieve in increasing the level of efficiency and effectiveness of digital forensics. Therefore, there is a need for a novel solution that can be used to investigate and prevent cybercriminal activities. For this purpose, digital forensics has gained tremendous attention. However, it has been discovered that digital forensic investigation is exposed to various challenges. Thus, the current research has identified key challenges while highlighting the significance of the forensic investigation.**

Keywords*—*digital forensics; forensic tools; forensic investigators; cybercrime; review

I. Introduction

The rapid development of information technology (IT) and the introduction of web 2.0 has made digital forensics a critical tool for the identification of computer-assisted and computer-based crime. People, nowadays, are increasingly engaged in web-based interactions, where they share their projects and information over the networks. This aspect has resulted in increasing cyber security concerns [1]. Besides, the evolution of digital technologies has not only facilitated the users but has also enabled the cybercriminals to compartmentalize their behavior; hence, greatly increasing the complexity of their cyber-criminal endeavors. By taking advantage of modern information and communication technologies (ICT) features, business transactions, commercial activities, and government services have significantly grown but have led to the proliferation of new cybersecurity issues and threats, such as cyberbullying, identity, and data leakage [2]. To counter this emerging threat, forensics officers have been focusing on the development of tools and techniques that can potentially help in the digital forensics' investigation. Unfortunately, tracking cybercrimes often requires sophisticated investigations that can be either subjected to different legal systems and jurisdiction or span international borders [3]. This problem, in addition to complex modern software/hardware frameworks, the richness of information, and highly heterogeneous ICT technologies, raises new challenges in the digital hemisphere. Therefore, this study is geared towards identifying major challenges that can hinder digital forensics investigation.

Currently, advances in information and technology has seen a growth in the usage of mobile phones. While this is important in aiding faster communication, there are malpractices done with mobile phones that requires forensic investigations. Mobile forensics is categorized into three; there is seizure, acquisition, and the last one is examination. Firstly, this process is not always smooth, investigators always face certain challenges in seizing mobile phones from the alleged perpetrators of crime. Usually, when the device is found at the scene of crime and powered off, it is recommended that the investigating offers places it in a faraday bag to prevent any changes that can be made to it when it's finally powered on. In their development, the faraday bags are made specifically to prevent phones from accessing any network. If the investigators collect a phone at the scene of crime that is powered on, there are also several concerns to it. First, there is the issue of whether the phone is locked by a PIN, password, or simply encrypted. If all or any of these are available, it would be prudent for the investigator to find a way of bypassing these locks in accessing the device.

Mobile phones are always highly networked gadgets. Here, they are able to receive data from multiple sources such as through the Bluetooth, Wi-Fi access point, and telecommunication. In the case of a crime, it is possible for the criminal to access the phone and erase any evidence that could link them to the actions. This is possible when the phone is in a running state. Therefore, it is important to secure the phone in a faraday bag whenever it is found powered on. Where possible, the investigating officer should ensure the phone is disconnected from network before securing it in this bag. After doing this process, it is important for the examiner to use the relevant tools in acquiring and analyzing data stored in the phone.

II. RESEARCH METHODOLOGY

Data collection is highly essential in getting the information needed for a research project. In every piece of research work, the approaches chosen for data collection vary. There is always the need to have a careful consideration of the search terms, choice of research resources, and the methods to be used in the search process. It also requires a careful reflection on the results found in the process. Whenever one searches for literature in a systematic way, there is always the chance of avoiding selection biases and disparities that can affect the quality of the research findings. In this research, an observation of these consideration plays a major role in minimizing any risks associated with a reproduction of the already existing research.

In this research, there are two main areas of concern in the data collection process. First, there are technical challenges identified to affect the effectiveness of digital forensics. In the data collection process, the researchers will concentrate on the establishment of facts around these challenges. There will be a systematic literature review, focusing on the research studies that have been done in the past by scientists on this matter. A careful examination of the research findings will be vital in ensuring that the findings found are able to address some of the technical challenges affecting. The same approach will also be taken in examining literature around legal challenges affecting digital forensics. So far, there are incidences of cybercrimes that have been reported in different jurisdictions. In some of these cases, digital forensics have been considered as able to help in finding evidence and other material resources that aid the process of making informed judgments on cases. In this regard, the researchers will be keen in undertaking a process that provides the right information for this research study. All these processes will be handled under the proper research ethics guiding data collection and analysis.

III. TECHNICAL CHALLENGES

The last decade has seen a vast development of computer technologies. In this development, the use of the computer has been considered to be both good and bad in equal measure. While some people and organisations use technology in making innovations and inventions that bring benefits, there are some who use rely on the same technology to invent ideas that affect others. When investigating these cases, there are certain technical challenges that always emerge in the process. It is worth remembering that compared to many other sources of evidence, it is not always easy to delete or modify digital evidence. Technical challenges can be understood as the ones that can be solved using existing operations, expertise, and protocols. Knowing that digital forensics entail a well-balanced combination of ethical conduct and technical expertise, some of the identified digital forensics technical challenges are explained below.

A. Vast Volumes of Data

Due to the rapid adoption of ICT, there has been an immense increment in the volume of disk storage – persistent storage – that is used in both corporate and personal systems. The vast volumes of data that exist within different applications, such as enterprise resource planning (ERP), pose a great threat to the digital forensic investigation. In addition, as discussed in [4], the richness of information and large data volumes have certain implications - which are not only associated with the procedures as well as the techniques used for imaging and data acquisition but also for the methods that are used for examining the data. More importantly, the substantial increase in the data also lowers the capability of forensic investigators and legal systems to counter digital threats because the distributed nature of data storage reduces the visibility and control of forensic investigators over digital forensic artefacts [5]. Thus, the evidence-rich sheer volume of data causes prolonged processing time, because of which forensic experts may be left waiting for extended periods to follow a lead that might assist in their investigation. While vast data volumes are a major digital forensic challenge, studies like [6] have introduced database-driven, deduplicated data technique to counter this problem (see Figure 1). This technique uses a centralized storage system to perform checks by comparing cryptographic hash value. According to the study, this system has various benefits, including reduced storage requirements, reduced bandwidth, and simultaneous processing and data acquisition.

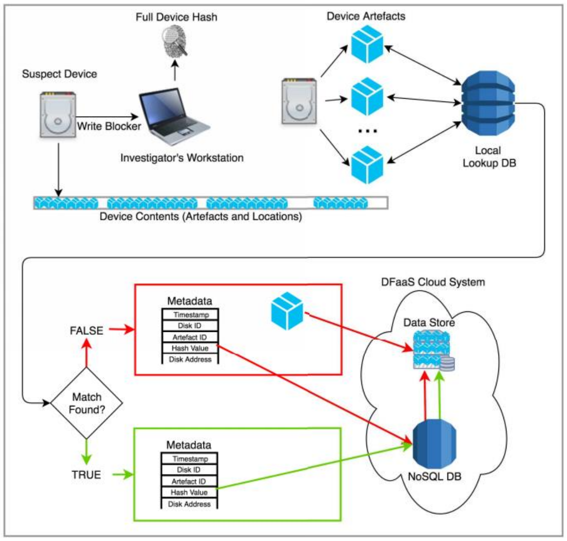

Figure 1: Database-driven, Deduplicated Data Technique [6].

B. *The Volatility of Digital Evidence*

It has been established that digital evidence is fragile. Any activity carried out on a digital device, whether intentionally or inadvertently - like shutting down or powering up a system - can either destroy or alter potential digital evidence [7]. Moreover, rough handling, extreme variations in temperature, exposure to light, magnetic field, and even loss of power in portable devices' battery can cause data loss. Therefore, obtaining volatile data presents a serious challenge that can hinder the performance of digital forensic investigation, as a little mishap can either change the content of the memory or the entire state of the system. To counter the issue associated with volatile data acquisition, for forensic investigation, various researchers have proposed different solutions. For example, the study of [8] used a digital evidence management framework (DEMF) to confirm the integrity of data (see Figure 2). The model divides the volatile data into fixed blocks of memory and then use hash functions to check the integrity of data. Likewise, in the research work of [9], the authors integrated Belkasoft RAM Capturer, OSForensics, Helix3(dd), Nigilant32, Pro Discover, and FTK Imager for the successful acquisition of volatile memory. According to the results of the study, the tested tools displayed 95% efficiency in extracting volatile data. This indicates that with the right tool and technique, the integrity of digital evidence can be maintained.

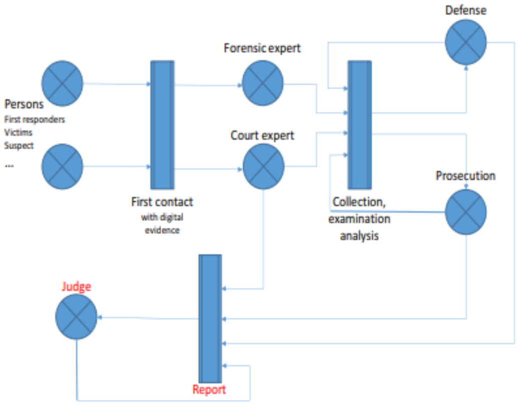

Figure 2: DEMF Model [8].

C. *The Complexity of Digital Crimes*

The rising complexity of digital crimes poses tremendous security challenges to digital forensic investigators and digital investigation. As discussed in the research work of [5], since digital evidence is obtained in raw binary form, understanding its content is challenging for humans, which further leads to higher complexity problems. Moreover, due to the rapid increase in the adoption of technologies, investigators are forced to adopt highly sophisticated data encryption techniques, along with latest malicious software and hacking tools that can jeopardize the security and integrity of the digital evidence [7]. What is more alarming is that cybercriminals are now taking advantage of anti-forensic techniques to bypass digital security. These techniques are capable of increasing the time of digital investigation by holding back scientific analysis, diminishing cyber footprints, and tampering the hidden data [10]. Although criminals use malicious tools, software, and methodologies to inflict damage to private and public networks, forensic investigators have started adopting state-of-the-art techniques to counter this emerging problem. The study of [11] proposed a similar technique that uses PCI hardware introspection and direct page table manipulation to counter anti-forensic attacks. The technique does not depend on the operating system (OS) facilities, but it independently enumerates memory and maps physical pages to increase the overall effectiveness. Thus, the increase in the complexity of cyberattacks provides opportunities to forensic experts to devise new methods to counter the ever-growing cyber problems.

D. *Bandwidth Restrictions*

Another major challenge - faced by digital forensic experts - is the bandwidth limitations. As discussed in [12], the network's bandwidth restrictions can either slow or limit the process of acquiring digital evidence. In particular, the forensic experts need connecting with the digital forensic agent that is installed on the machine through the network. More importantly, copying the information - as potential digital evidence from the questionable system to the forensic workstation - can reduce the bandwidth, particularly if multiple users are using the bandwidth at the same time [13]. Besides, significant remote digital evidence acquisition might have to be carried out for accommodating the limited bandwidth capacities; thereby, causing a delay in the investigations. While bandwidth restriction is a pressing challenge, various studies have proposed solutions to cater to this problem. For example, the study of [14] discovered that the log-based model and log-management architecture could significantly help in reducing the complexity of forensic evidence, which can further assist in bandwidth restriction. Likewise, in [15], the authors developed a distributed management architecture for forensic investigation. The authors proclaim that their system is capable of reducing time and load of log transmission in cloud digital forensic investigation. This indicates that albeit bandwidth restriction is a notable problem, recent advancements in technology have provided commendable tools and techniques to counter this issue.

E. *Emerging Cloud Forensic Challenges*

Cloud computing is a modern, cutting-edge platform, which is widely being adopted by the companies of cost-effectiveness, ubiquity, and elasticity. It has also emerged as a potential efficient solution to accomplish business objectives while fulfilling businesses' computing needs [7]. Unfortunately, hackers have started using these characteristics for victimizing users and conducting criminal activities (See Figure 3). Moreover, with emerging cloud forensic challenges, such as cloud heterogeneity and jurisdiction, organizations have become hesitant in shifting to cloud-based services. In addition to these challenges, the study of [16] discovered data protection, safeguarding data security, user authentication, managing the contractual relationship, and data breach contingency to be one of the few problems that need to be addressed. For this purpose, the research of [17] analyzed different solutions, such as secure-logging-as-service (SecLaas), and log-based model for cloud forensics. Likewise, the authors in [18] proposed a technique that centralizes all logging activities within the cloud before a forensic investigation. The findings of the study show that the proposed model is capable of improving the efficiency of acquisition of evidential data; hence, enabling forensic investigators to conduct examination and analysis immediately. Thus, the proposed techniques are powerful enough to counter emerging cloud forensic challenges.

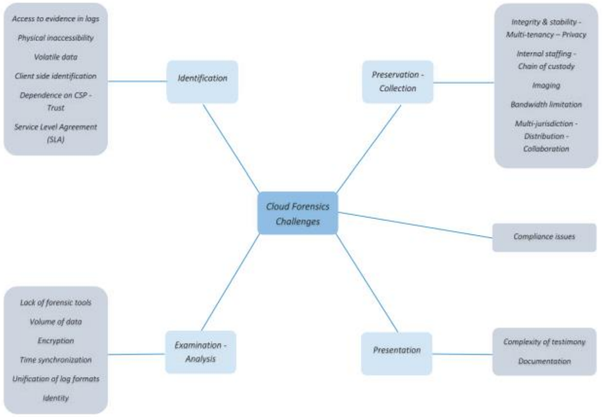
Access to evidence in logs
Physical inaccessibility
Volatile data
Client side identification
Dependence on CSP - Trust
Service Level Agreement (SLA)
Identification
Preservation - Collection
Integrity & stability - Multi-tenancy – Privacy
Internal staffing - Chain of custody
Imaging
Bandwidth limitation
Multi-jurisdiction - Distribution - Collaboration
Cloud Forensics Challenges
Compliance issues
Lack of forensic tools
Volume of data
Encryption
Time synchronization
Unification of log formats
Identity
Examination - Analysis
Presentation
Complexity of testimony
Documentation

Figure 3: Challenges Faced by Cloud Forensics [17].

F. *Encription*

In digital forensics, encryption of data is highly essential. According to [32], encryption can be described as the idea behind scrambling of information in a manner that can only be understood and decoded by an individual that has a proper decoding key. In digital forensics, encryption is important in hiding all evidence that can be discovered and tampered with by a compromised system [32]. While the digital forensic experts have been on the forefront in the development of effective data encryption strategies. Attackers tend to use various encryption methods in making data usable. Investors are expected to understand the decryption and encryption approaches to keep their evidence safe and secure. However, there are instances where the encrypted data cannot be decrypted [32]. Here, this understanding places an emphasis on the forensic experts to understand how the entire encryption and decryption process is done. If this development is done, there is a glimpse of a positive future in the tech-industry.

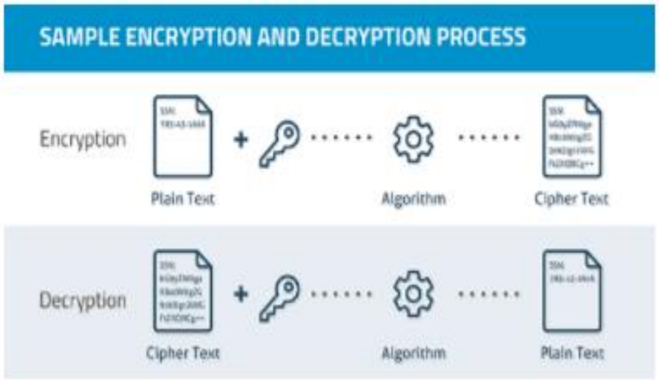

Fig 4: The data encryption process [32]

The schematic diagram above indicates the general approach that is always applied in encrypting data. By managing the challenges associated with this process, it is easy to improve the data forensic process in keeping individuals and organisations from unnecessary attacks from unscrupulous IT experts that have an ulterior motive.

G. *Covert Channels*

One of the things that happen with attackers is the development of a secret communication link between the compromised system and theirs. This is an area that prevails a major channel when digital forensic investigations is being undertaken. This channel is referred to as the covert channel. The covert channel protocols are credited with allowing attackers the liberty to hide their data over the network in a manner that allows a bypassing of the intrusion detection strategies [33]. At the time of developing this network, a network protocol has to be chosen carefully and its header modified for purposes of leaking messages between attackers. This is something that allows attackers to have undisrupted access to important data and other relevant information that is prohibited to unauthorized users. Forensic experts need to understand that in the current times, attackers have been using covert channels for developing and maintaining hidden connections between the attackers and the compromised systems [33]. This mode of communication is indicated below;

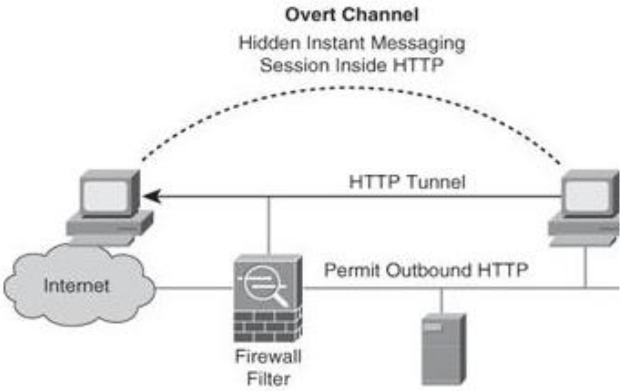

Fig 5: the Covert Channel

By knowing these developments, it is easy to improve the face of digital forensics and increase the level of efficiency in this process. Going forward a lot of commitment needs to be done in ensuring additional resources are diverted towards knowing how these covert channels are developed and implemented to secure information and business systems in different industries.

H. Steganography

Data protection remains as one of the goals of IT security. Steganography comes in to enahance the cryptographic process, thus adding an extra secure layer on a data protocol. Steganography is simply a special encryption strategy that is used alongside cryptography in making an extra-secure layer in protecting data [34]. This method is important in ensuring that all dta within a file carrier is safely secured without the need of modifying its apearance. For attackers, using this process is considered a secure process in transporting their hidden files, also referred to as payloads away from the compromised system. In the process of investigating a criminal undertaking digital forensic experts have the responsibility of identifying these hidden files.

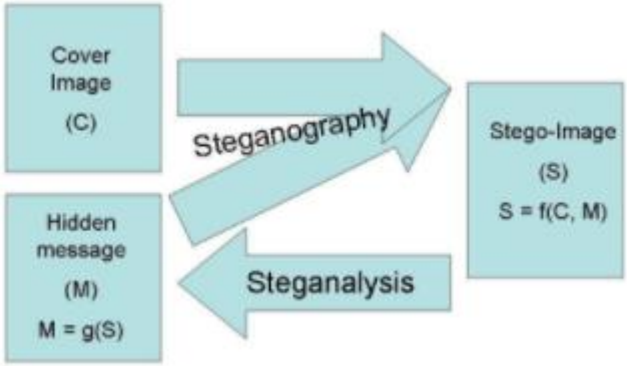

Fig 6: Steganography [34]

Identifying the hidden files plays a major role in revealing information that attackers could be making away with. Therefore, digital forensic experts have the task of knowing all these routes and the purpose they are developed for by the attackers.

Finally, the advancement in digital technology has provided various opportunities; however, it has caused the digital forensic domain to face additional challenges. In this account, it has been identified that digital forensic systems are exposed to technical challenges that can jeopardize the integrity and reliability of these systems [7]. These challenges include emerging technologies, incompatibility among heterogenous forensic tools, limited opportunity for the collection of potential evidence, and encryption. According to the study of [29], the advancement in ICT has allowed easy access to complex encryption services and products. As a result, encryption standards and algorithms are becoming increasingly sophisticated that further increases the difficulty and time of conducting cryptanalysis. Likewise, the distributive nature of the cloud environment and heterogeneous elements - present in digital forensic tools - can increase the incompatibility of these devices [17]. Additionally, most of the digital forensic tools are incapable of analyzing the ever-increasing number of target devices. This means huge targets restricts the ability of forensic tools and techniques to work harmoniously; hence, minimizing the efficiency of forensic investigation. While incompatibility is a notable challenge, various practitioners and researchers attempted to design harmonized digital forensic frameworks. For example, the research work of [30] introduced a harmonized digital forensic model that works on the principle of parallel actions. The authors proclaim that their model is not only comprehensive but can harmonize modern and sophisticated forensic investigation frameworks. Thus, it can be established that despite suffering from multiple technical challenges, digital forensic is an interesting research domain that is constantly evolving.

IV. LEGAL CHALLENGES

The increase in the number of cybercrimes has created a need to increase awareness in the legal community. However, unsatisfactory presentation of evidence or procedures in court can lead to unsuccessful prosecutions. To gain in-depth insights, following law enforcement or legal system challenges are discussed that are faced by digital forensics.

A. Jurisdiction

With the introduction of web 2.0 technologies, the sophistication of conventional cybercrimes and the adoption of cloud computing has made detection of cybercrimes a difficult task. The prominent advantage of cloud computing that enables anyone to use publicly accessible software for the processing of data - stored in a digital or virtual space - could be potentially used by cybercriminals to hide digital evidence on a server that is beyond the jurisdiction of the courts of that particular country [17]. This makes obtaining the hardware – containing relevant evidences and data - a significant challenge since the data is stored on a distributed system which is located at different places. Moreover, even with effective legislation, enforcement of the law in cyberspace creates distinct problems. It is mainly because since the internet is a medium that can be accessed by anyone, at any time, a potential criminal might not be within the jurisdiction where the attack was conducted [19]. Therefore, to avoid jurisdictional issues, network administrators and forensic officers have to become familiar with the jurisdiction of the particular state as well as the applicable laws before starting an investigation.

B. *Privacy*

The stability of evidence and integrity preservation are crucial in digital forensic investigation. However, in some cases, the forensic officer might be forced to compromise or share the victim's privacy to get to the actual truth [7]. This can cause distrust in the forensic team, which can further hinder the investigation performance. Moreover, due to the rapid increase in the adoption of internet of things (IoT), deployment of objects that sense private information of people, such as health data, pose an additional threat to the privacy of individuals [20]. Unlike conventional scenarios where users can take certain actions like posting some data, to jeopardize their privacy, IoT devices collect private data of users without letting them know about it. As a result, the adversary can disclose this information to the public or internet community through direct or indirect means, which can be considered as a violation of privacy policies [21]. Therefore, private information should be kept confidential by any forensic investigator to avoid the violation of forensic policies. This is also supported by the study of [22] that established a crucial foundation for privacy-respecting digital investigation. The study stated that it is important to investigate understand both local and federal laws while acquiring a digital investigation warrant before collecting, processing, and storing private user data to avoid privacy violations.

In digital forensics, the matter of privacy is always held in high esteem. Information is always and has to be held under the highest standards of security. However, in the case of undertaking investigations, forensic experts can be required by the law to share some information which is helpful in undertaking the investigations at hand. Often, there is always the likelihood of the investigator, who can be an individual or a company to reveal a lot of private information in their duty. Therefore, placing a requirement on the investigator to reveal this information has the probability of risking their privacy. In the past, issues of privacy have raised legal suits in the course of investigations. An example was in 2000, at the time of investigating the notorious online Wonderland Club [35]. In the case, Grant made an argument that all evidence that had been found in his custody were to be suppressed because the investigating officers had failed in linking him as the core perpetrator of the illegal online activities in question. However, on their part, the prosecutor presented a lot of evidence that linked Grant to the activities as the chief organizer and executor of the same.

Examining this case presents some interesting facts. First, it is a big challenge when the investigator is not able to use some useful information for the case on grounds of having violated the privacy of the accused person. Whenever this happens, it impacts of the quality of the case, leaving the criminal with the liberty they need to commit more harm to other individuals and companies. Based on the case, it is important for investing officers to keep in mind the need to keep to the ethical guidelines of their investigations.

The ability to arrest and prosecute a criminal in the course of law lies on the quality of the evidence collected. This evidence, in the course of picking it should adhere to all the laws including privacy. Often, digital forensics has the ability of amassing a wealth of information that can be highly reliable in nailing criminals involved in online fraud and other related atrocities. In securing the integrity of the data collected, investigators have the responsibility of storing this information carefully within the required legal parameters. This should be done in consideration of the privacy of the victims and the suspects. For this objective to be achieved, it is important for the investigating officers to have a perfect understanding of the legal expectations in different jurisdictions. As pointed out, the legal framework regarding electronic evidence collection and storage varies from one country to another. Since electronic fraud happens across nations, it is prudent for investigating officers to acquaint with both the international and country requirements for digital forensics.

It is always expected that digital forensic experts have the highest standards of professionalism. For this reason, they should always stick to this expectation and achieve the best in their investigations. It is the success of these processes that present a bright future for the technology world to individuals and corporate enterprises.

C. *Ethical Issues*

Another major challenge faced by digital forensic investigations is associated with ethical issues. The prominent and rising ethical concerns are related to maintaining the confidentiality of private data, which is unrelated to the on-going case [23]. With this, the question of what to do with the obtained information, even if it is irrelevant, arises. The general ethical code dictates that such information should not be made public and ignored because of its irrelevance to the case [7]. However, ignoring such information is harder than it seems and any secret that might be uncovered during an investigation can put a tremendous psychological burden in the mind of a forensic expert. Further, the study of [24] argued that digital forensic officers are inevitably going to come across ethical dilemmas, such acknowledgement of errors on evidence (data) and maintaining responsibility and control for forensic equipment, and bias during an investigation. Therefore, to solve ethical issues, various researchers, such as [25] and [26] derived a set of ethical guidelines and integrated them onto digital forensics investigation framework. These guidelines, by providing credibility and prestige, can eliminate unfair competition and errors while fostering fruitful cooperation among professionals.

D. *Admissibility of Digital Forensics Techniques and Tools*

Given data volumes that is being managed by digital forensic experts, the acceptability of digital forensic techniques and tools - used for obtaining and examining data - is becoming a great hassle. According to [27], the quality of the electronic or digital record is directly proportional to the respective digital record's evidentiary value. This means that digital forensic tools ought to meet basic scientific and evidentiary standards so that they can be allowed to use as evidence or forensic equipment during the legal proceedings. This also indicates that the procedures, processes, techniques, and tools should prove to be authentic via empirical testing. In a digital forensic context, this means that the procedures, processes, techniques, and tools used in the analysis and collection of digital evidence should be approximately validated for meeting all ethical and scientific standards [28]. Therefore, the admissibility of digital evidence is vital and can significantly influence the weight and reliability of the evidence in question.

V. ADDITIONAL CHALLENGES

A. Operational Challenges

Due to the nature of digital crimes, digital forensic is exposed to multiple operational challenges. These include the absence of standardized procedures and processes, poor incidence detection, prevention and response, and manual intervention [7]. Among these problems, the lack of standardized procedures significantly affects the investigation process. There is an absence of a standardized digital forensic model that can be used for retrieving potential digital evidence. Interestingly, the authors in [21] proclaim that the number of existing forensic investigation models have increased the overall complexity of the investigation process. In addition, the lack of universal standards adds another layer of problems when assessing the competency of forensic investigators. Therefore, there is a need to understand that the development of digital technologies has transformed traditional computer systems to a virtualized environment that requires proper incidence prevention and detection systems and standardized procedures.

B. Resource Challenges

In many jurisdictions, the level of technological advancement differs considerably. This understanding implies that the resources developed for digital forensics is different as well. Based on the prevailing scenarios to be investigated, the volume of data can be quite voluminous. Here, investigators have to go through a series of the data they collect in gathering criminating evidence in prosecuting the alleged offenses. Sometimes, this process takes a long time, which can be a limiting factor to investigators. This is one of the major challenges in digital forensics.

Often, the case of volatile memory forensics presents certain challenges. The data kept in this memory is always ephemeral; therefore, user activities tend to suffer as they are usually overwritten in thus memory. For the investigators, this observation leaves them with recent information to be analyzed, which is kept in the volatile memory. In the end, this process reduces the value of data available for investigation. At the time of collecting information from investigators, it is important for the investigator to ensure that the data is safely modified to increase its security. Whenever the investigation officers do not have all these resource capabilities, it is possible to compromise the quality of investigations.

In ensuring proper investigations are done, it is important to keep the data sources as secure as possible. Often, it is problematic whenever the investigator realizes that valuable information that is no longer usable. Therefore, before any investigations are done, it is paramount to ensure all the needed resources are in place to keep the information and evidence under investigation as safe as possible for the investigators. For investigation authorities, seeking expert opinion on the resources needed to undertake a digital forensic is considered relevant in ensuring the success of the entire process is achieved. This is due to the fact that every investigation offers has the goal of achieving the highest level of success in the entire process.

In addition to the challenges mentioned above, there is a need for well-trained staff, having exceptional expertise in using digital forensic tools. As discussed in [1], despite becoming an important research domain, there is only a handful of trained forensic personnel that are capable of conducting a forensic investigation. Moreover, digital forensic is gaining immense popularity among forensic practitioners, law enforcement agencies, and computer professionals; however, they must always cooperate in obtaining optimal results. Unfortunately, because of this, digital forensic investigation is exposed to semantic disparity issue, which means that there is a lack of coordination among forensic professionals. Another potential challenge is the absence of a knowledge base and records of previous investigations [1] [7]. Often, when forensic experts utilize digital technologies and specialized skills to obtain potential evidence, they fail to record their work, which limits the growth of future forensic officers. Thus, it can be affirmed that digital forensic investigation is exposed to various personnel-related challenges, and if not addressed, they can hamper the training and efficiency of future digital forensic investigations.

VI. MOBILE FORENSICS

For digital forensic expert, mobile phones always present a major challenge to investigators. It is not always easy for examiners to seize, acquire and obtain information to be used as digital evidence against criminal perpetrators. First, the ever increasing number of different mobile brands is a challenge in itself. This observation makes it hard for investigating officers to find a single strategy for investigating mobile phones as sources of evidence. Mobile phones are some of the highly evolving technologies as new ideas and technological inventions are developed. As a result, it is possible to see that every phone has its specific embedded operating systems that are secure. This understanding implies there is a set of skills and expertise that is needed in undertaking mobile forensics to study and analyse devices.

Mobile phones are dynamic systems that present a lot of challenges to the examiner in extracting and analyzing digital evidence. The rapid increase in the number of different kinds of mobile phones from different manufacturers makes it difficult to develop a single process or tool to examine all types of devices. Mobile phones are continuously evolving as existing technologies progress and new technologies are introduced. Furthermore, each mobile is designed with a variety of embedded operating systems. Hence, special knowledge and skills are required from forensic experts to acquire and analyze mobile devices.one of the biggest challenges with investigating phones is the fact that it is easy to access, store, and synchronize data across many devices. Data in mobile phones is considered to be highly volatile. Therefore, an alleged criminal can easily transform and delete it remotely. Whenever this happens, more effort is needed in accessing and collecting the needed information. Some of the specific challenges that investigators encounter during this process include the following

A. Hardware Challenges

First, the mobile phone market is and continues to flood with different brands of mobile phones. Forensic examiners can always come from different kinds of mobile network brands, which always appear in different features such as hardware, operating systems, and sizes. Since mobiles phones have a short product development cycle, the rate at which they are evolving in the market is quite high. With these rapid development, it is important for the forensic examiners to ensure they keep adapting to the various challenges and remaining updated at all times. The failure to address these devices has the ability of making criminal perpetrators prefer committing their atrocities via mobile phones.

B. Mobile Operating Systems

Compared to computers where the operating systems are les and well known, mobile phones have varied operating systems that power them. Different mobile phone companies, in securing their products put different security systems that make data usage and storage as secure as possible. For investigating officers, this observation presents a challenge that need to be addressed to enhance the effectiveness of mobile forensics. At the same time, the law, in many jurisdictions does not allow investigators to have free access to individual information due to privacy concerns. In the end, it is possible for the investigating offers to get good information which may not accepted in courts of law due to infringement on privacy.

Mobile forensics is not as easy as that of computers. Therefore, besides keeping abreast of the technological evolutions in developing mobile phones, it is important for investigating officers to also familiarize with the law. It is only the law that can provide the best avenues to be followed in undertaking mobile forensics. The failure to achieve this objective can be a precursor for weak legal avenues to protect individuals and corporate organisations from criminals.

VII. CONCLUSION

Digital forensic is an interesting area of research that has gained significant attention. The introduction of advanced technologies and the developments in IT has notably influenced the legal and technical requirements of digital evidence. Besides its obvious benefits, the sophistication of digital forensic investigation offers shelter to cybercriminals for conducting different types of criminal activities. Besides, malicious tools and techniques are continually being designed and integrated every day that threatens the integrity of digital evidence.

At the same, the increase in the number of people using mobile phones has also brought in a new dimensions of digital forensics. There are several atrocities committed though mobile phones and need to be investigated perfectly. However, from the foregone discussion, the evolving nature of mobile phones has meant a huge challenge to investigating offers as far as collecting evidence is concerned. The different operating systems in mobile phones, coupled with differences in the accompanying security features places a demand on the investigating authorities to find the information they need. Investigating officers need to keep learning and acquainting with these new developments to remain competitive in their work.Therefore, the present research has thoroughly investigated key challenges faced by digital forensic officers in hope to understand the importance of this field. Since modern digital societies are vulnerable to fraud and malicious activities, there is a need to develop digital forensic tools that offer scalability, preserves privacy, and support the heterogeneous forensic investigation.

REFERENCES

[1] E. Vincze, "Challenges in digital forensics", Police Practice and Research, vol. 17, no. 2, pp. 183-194, 2016. Available: 10.1080/15614263.2015.1128163 [Accessed 2 October 2020].J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] M. Al Fahdi, N. L. Clarke and S. M. Furnell, "Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions," 2013 Information Security for South Africa, Johannesburg, 2013, pp. 1-8, doi: 10.1109/ISSA.2013.6641058.

[3] L. Caviglione, S. Wendzel and W. Mazurczyk, "The Future of Digital Forensics: Challenges and the Road Ahead," in IEEE Security & Privacy, vol. 15, no. 6, pp. 12-17, November/December 2017, doi: 10.1109/MSP.2017.4251117.

[4] G. Mohay, "Technical challenges and directions for digital forensics," First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05), Taipei, Taiwan, 2005, pp. 155-161, doi: 10.1109/SADFE.2005.24.

[5] S. Raghavan, "Digital forensic research: current state of the art", CSI Transactions on ICT, vol. 1, no. 1, pp. 91-114, 2012. Available: 10.1007/s40012-012-0008-7 [Accessed 2 October 2020].

[6] M. Scanlon, "Battling the digital forensic backlog through data deduplication," 2016 Sixth International Conference on Innovative Computing Technology (INTECH), Dublin, 2016, pp. 10-14, doi: 10.1109/INTECH.2016.7845139.

[7] N. Karie and H. Venter, "Taxonomy of Challenges for Digital Forensics", Journal of Forensic Sciences, vol. 60, no. 4, pp. 885-893, 2015. Available: 10.1111/1556-4029.12809 [Accessed 2 October 2020].

[8] M. Bača, J. Ćosić and P. Grd, "Using DEMF in process of collecting volatile digital evidence," 2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, 2016, pp. 1442-1446, doi: 10.1109/MIPRO.2016.7522366.

[9] K. M. A. Kamal, M. Alfadel and M. S. Munia, "Memory forensics tools: Comparing processing time and left artifacts on volatile memory," 2016 International Workshop on Computational Intelligence (IWCI), Dhaka, 2016, pp. 84-90, doi: 10.1109/IWCI.2016.7860344.

[10] D. Das, U. Shaw and S. Priya Medhi, "REALIZING DIGITAL FORENSICS AS A BIG DATA CHALLENGE", In 4th International Conference on "Computing for Sustainable Global Development, 2017. [Accessed 2 October 2020].

[11] J. Stüttgen and M. Cohen, "Anti-forensic resilient memory acquisition", Digital Investigation, vol. 10, pp. S105-S115, 2013. Available: 10.1016/j.diin.2013.06.012 [Accessed 2 October 2020].

[12] B. Taute, M. Grobler and S. Nare, "Forensic challenges for handling incidents and crime in cyberspace", 2009.

Available: https://www.researchgate.net/publication/38958329_Forensic_challenges_for_handling_incidents_and_crime_in_cyberspace. [Accessed 2 October 2020].

[13] D. Lillis, B. Becker, T. O'Sullivan and M. Scanlon, "Current Challenges and Future Research Areas for Digital Forensic Investigation", arXiv preprint arXiv:1604.03850, 2016. Available: https://arxiv.org/abs/1604.03850. [Accessed 2 October 2020].

[14] S. Simou, C. Kalloniatis, E. Kavakli and S. Gritzalis, "Cloud Forensics Solutions: A Review", Lecture Notes in Business Information Processing, pp. 299-309, 2014. Available: 10.1007/978-3-319-07869-4_28 [Accessed 2 October 2020].

[15] C. Jiang, I. Liu, C. Liu, Y. Chen and J. Li, "Distributed Log System in Cloud Digital Forensics," 2016 International Computer Symposium (ICS), Chiayi, 2016, pp. 258-263, doi: 10.1109/ICS.2016.0059.

[16] S. Ali, S. Memon and F. Sahito, "Challenges and Solutions in Cloud Forensics", Proceedings of the 2018 2nd International Conference on Cloud and Big Data Computing - ICCBDC'18, 2018. Available: 10.1145/3264560.3264565 [Accessed 2 October 2020].

[17] S. Simou, C. Kalloniatis, S. Gritzalis and H. Mouratidis, "A survey on cloud forensics challenges and solutions", Security and Communication Networks, vol. 9, no. 18, pp. 6285-6314, 2016. Available: 10.1002/sec.1688 [Accessed 2 October 2020].

[18] P. M. Trenwith and H. S. Venter, "Digital forensic readiness in the cloud," 2013 Information Security for South Africa, Johannesburg, 2013, pp. 1-5, doi: 10.1109/ISSA.2013.6641055.

[19] M. Chawki, A. Darwish, M. Khan and S. Tyagi, "Cybercrime, Digital Forensics and Jurisdiction", Studies in Computational Intelligence, 2015. Available: 10.1007/978-3-319-15150-2 [Accessed 2 October 2020].

[20] M. Conti, A. Dehghantanha, K. Franke and S. Watson, "Internet of Things security and forensics: Challenges and opportunities", Future Generation Computer Systems, vol. 78, pp. 544-546, 2018. Available: 10.1016/j.future.2017.07.060 [Accessed 2 October 2020].

[21] H. Arshad, A. Jantan and O. Isaac Abiodun, "Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence", Journal of Information Processing Systems, vol. 14, no. 2, 2018. Available: https://www.researchgate.net/publication/327644306_Digital_Forensics_Review_of_Issues_in_Scientific_Validation_of_Digital_Evidence. [Accessed 2 October 2020].

[22] A. Dehghantanha and K. Franke, "Privacy-respecting digital investigation," 2014 Twelfth Annual International Conference on Privacy, Security and Trust, Toronto, ON, 2014, pp. 129-138, doi: 10.1109/PST.2014.6890932.

[23] V. Broucek and P. Turner, "Technical, legal and ethical dilemmas: distinguishing risks arising from malware and cyber-attack tools in the 'cloud'—a forensic computing perspective", Journal of Computer Virology and Hacking Techniques, vol. 9, no. 1, pp. 27-33, 2012. Available: 10.1007/s11416-012-0173-0 [Accessed 2 October 2020].

[24] K. Seigfried-Spellar, M. Rogers and D. Crimmins, "Development of A Professional Code of Ethics in Digital Forensics", 2017. Available: https://commons.erau.edu/adfsl/2017/papers/12/. [Accessed 2 October 2020].

[25] R. Ferguson, K. Renaud, S. Wilford and A. Irons, "PRECEPT: a framework for ethical digital forensics investigations", Journal of Intellectual Capital, vol. 21, no. 2, pp. 257-290, 2020. Available: 10.1108/jic-05-2019-0097 [Accessed 2 October 2020].

[26] S. Harrington, "Professional ethics in the digital forensics discipline: Part 1", Forensic Magazine, 2014. [Accessed 2 October 2020].

[27] D. Yadav, M. Mishra and S. Prakash, "Mobile Forensics Challenges and Admissibility of Electronic Evidences in India," 2013 5th International Conference and Computational Intelligence and Communication Networks, Mathura, 2013, pp. 237-242, doi: 10.1109/CICN.2013.57.

[28] A. Antwi-Boasiako and H. Venter, "A Model for Digital Evidence Admissibility Assessment", Advances in Digital Forensics XIII, pp. 23-38, 2017. Available: 10.1007/978-3-319-67208-3_2 [Accessed 2 October 2020].

[29] A. M. Balogun and S. Y. Zhu, "Privacy impacts of data encryption on the efficiency of digital forensics technology.," arXiv preprint arXiv:1312.3183., (2013).

[30] A. Valjarevic and H. S. Venter, "Harmonized digital forensic investigation process model," 2012 Information Security for South Africa, Johannesburg, Gauteng, 2012, pp. 1-10, doi: 10.1109/ISSA.2012.6320441.

[31] N. M. Karie and H. Venter, "Significance of Semantic Reconciliation in Digital Forensics", 2013. Available: https://commons.erau.edu/adfsl/2013/tuesday/8/. [Accessed 2 October 2020].

[32] TechTerms. Encryption. [ONLINE] Available at: http://www.techterms.com/definition/encryption. [Accessed 06/22/2017. 2014].

[33] S. Rekhis, and N, Boudriga, Formal Digital Investigation of Anti-forensic Attacks. 2010. Available from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5491959 [Accessed 06/22/2017].

[34] C. Janssen. Steganography. 2014. Available at: http://www.techopedia.com/definition/4131/steganography. [Accessed 06/22/2017].

[35] E. Casey. *Digital Evidence and Computer Crime*. 3rd ed. USA: Elsevier. 2011