Digital forensics investigation jurisprudence: issues of admissibility of digital evidence

Yeboah-Ofori A and Brown AD, J Forensic Leg Investig Sci 2020, 6: 045
DOI: 10.24966/FLIS-733X/100045

HSOA Journal of Forensic, Legal & Investigative Sciences

Research Article

Digital Forensics Investigation Jurisprudence: Issues of Admissibility of Digital Evidence

Yeboah-Ofori A* and Brown AD

Department of Computing and Engineering, University of East London, UK

Abstract

Digital Forensics investigations represent the science and legal process of investigating cybercrimes and digital media or objects to gather evidence. The digital evidence must prove that it has been used to commit a crime or used to gain unauthorized access. Digital Forensics investigations jurisprudence is the theory and philosophy of the study of law and the principles upon which a law is based. For digital evidence to appear at court and be legally admissible, the evidence must be authentic, accurate, complete, and convincing to the jury. Presenting digital forensic evidence at court has proved to be challenging, due to factors such as inadequate chain of custody, not maintaining legal procedures and inadequate evidential integrity. Following legal procedures in evidence gathering at a digital crime scene is critical for admissibility and prosecution. However, inadequate evidence gathering and maintaining accuracy, authenticity, completeness has prevented many cases to be inadmissible at court. This paper aims to discuss digital forensics investigations jurisprudence and the issues of authentic, accurate, complete, and convincing evidence leading to inadmissibility at court. To achieve the applicability of the study, we highlight the legal and technical factors required to harmonize these issues and how it could be addressed. This paper does not follow any forensic investigations process. Rather, it discusses how digital evidence could be admissible irrespective of the process implemented. The observations and outcomes of these legal criteria will contribute to the improvement of the evolving nature of digital evidence gathering phases.

Keywords: Cyber jurisprudence; Cyber science; Digital forensics investigations; Digital evidence; Jurisprudence

***Corresponding author:** Yeboah-Ofori A, Department of Computing and Engineering, University of East London, UK, Tel: +44 20 82233000; E-mail: u0118547@uel.ac.uk

Citation: Yeboah-Ofori A, Brown AD (2020) Digital Forensics Investigation Jurisprudence: Issues of Admissibility of Digital Evidence. Forensic Leg Investig Sci 6: 045.

Received: April 20, 2020; **Accepted:** May 22, 2020; **Published:** May 29, 2020

Introduction

Digital forensic investigation jurisprudence considers the legal system used in a court of law to administer justice in the event of cyber-attacks and cybercrimes. Cyber jurisprudence is the science and philosophy or theory of Law [1]. It considers the legal ramifications and the evolving nature of cyber technical and digital objects. Digital forensics investigations must be authentic, accurate, complete, and convincing to juries and in conformity with jurisdictional law and legislative rules to be admissible at court [2]. To ensure digital evidence meet these criteria and be admissible at court has been a challenge in evidence gathering procedures. Digital evidence in forensic investigations is legally binding and is normally intended to be admissible at court. Identify standards that justify the need to bridge the barriers between technological advancement and the legislations in digital forensics investigations to examine digital media in a forensically comprehensive method [3]. Following a proper chain of custody consistently and methodically has been challenging due to the dynamic nature of digital evidence. The phenomenon surrounding digital evidence is that cyber-attacks, and cybercrimes are evolving, and the invincibility nature of the attacks makes it difficult in evidence gatherings. However, investigators are required to adapt to the changing crime scenes and the digital media that has been used to commit the crimes. Hence, it has become imperative that standard procedures that are coherent and ensures harmony between the lawyers, judges, forensic experts, law enforcement agencies, corporations, individuals, and the court be implemented. The ACPO (2012) in its effort to combat cybercrime brought together the expertise in policing across the UK, the capability and best practice within the industry, support of Government and the criminal justice system [4]. Convention on Electronic Evidence (2016) raised concerns regarding the profound changes brought about by machine and software code (collectively digital systems) have altered how evidence is authenticated [5]. In that the medium and the content are no longer bound together as with paper, and that the rules established for paper do not always apply to evidence in electronic form. The factors leading to the inadequate evidence gathering, and maintaining evidential integrity includes the inability to ensure accuracy, authenticity, completeness to make the evidence convincing to the juror. Recognizing the need to facilitate the cooperation between forensic investigators, judges, lawyers, expert witnesses, and individuals regarding the proper evidence gathering, handling and authentication of electronic evidence is significant. These have prevented many cases to be inadmissible at court.

This paper aims to discuss digital forensics investigations jurisprudence and the factors leading to the issues of inadmissibility at court. The paper contributes to improving the four key criteria required to improve digital forensic investigation jurisprudence in line with various standards. Further, it will assist in resolving the legal and technical challenges that are impacting on digital evidence gathering. The paper does not follow any digital forensic investigations process. Rather, it discusses how digital evidence could be admissible at court in line with the various standards irrespective of the investigation process adopted in evidence gathering.

Related Works

This section discusses the state of the art of digital forensics investigations jurisprudence and the related works in digital evidence gathering. The dynamic nature of cyber-attacks and cybercrimes makes if challenging to interpret the same law to implement a coherent legal framework that could harmonize the legal and technical aspects of cyber law. Stephenson (2017) defined cyber law as the legislation, legality and practice of lawful, just and ethical protocol involving the internet as well as the alternative networking and information technologies. There is no single investigation that would support or refute digital evidence without a hypothesis. Postulates that digital forensics investigation is a new science with additional guidelines and practices designed to create a legal cyber audit trail [6], posits that cyber science is concerned with the study of the phenomenon caused or generated by the cyber world and the cyber-physical, cyber-social and cyber-mental worlds, as well as their complex intertwined integrations [7]. Jurisprudence in digital forensics investigations provides a platform to consider the legal complexities in a more practical and realistic approach to assist in improves investigation processes. UNODC (2013) report highlighted that forensic expert and law enforcement agencies are increasingly faced with the question of what it means to ensure accuracy, authenticity, completeness and convincing (AACC) evidence [8]. The issues of mutual legal assistance and admissibility arise when a formal request from one judicial from a country request another judicial authority to gather digital forensic gatherings on behalf of the other country [9]. Proposed that a harmonized framework for assessing digital evidence admissibility is required to provide a scientific basis for digital evidence to be admissible and to ensure the cross-jurisdictional acceptance and usability of digital evidence [10]. NIST SP800-86 proposes four basic phases for digital forensics process and guidelines, including collection, examination, analysis, and examination digital evidence [11]. Convention on Electronic Evidence (CEE) (2016) provides concepts of electronic evidence, covering civil and criminal proceedings, investigations and examination of evidence in electronic form. ISO 27037 provides guidelines for identification, collection, acquisition, and preserving digital evidence and digital devices systematically and impartially while preserving its integrity and authenticity. ISO/IEC 27043:2015 provides guidelines for incident investigations and legal principles and processes from pre-incident to post- incident preparations that ensure admissibility of evidence. It highlighted the standard legal requirement that could be adopted in terms of the legal issues pertaining to jurisdiction and the need for other expert investigators to be able to use the process to arrive the same result [12]. International Laboratory Accreditation Cooperation (ILAC) (2014), highlights the challenges faced by investigators as there are no clear guidelines and appropriate approach in forensic practices between investigation processes at the crime scene and that of the forensic Lab. ILAC provides accreditations that are consistent with ISO/IEC 17020 and 17025 guidelines [13]. The ACPO proposed a digital base evidence guide that attempts to encompass the digital world and assist in investigating cyber security incidents four. The approach combines the various industries, law enforcement and agencies hard work to unite them into single effort to gather intelligence, enforcement capabilities and create the right framework of policy and doctrine to tackle major issues identified. The Convention on Electronic Evidence (2016) proposes a few preambles considering that aim of the drafting committee is to encourage judges and lawyers to appreciate the concepts of evidence in electronic form. The recognition that evidence in electronic form has unique characteristics that are significantly different from paper and other objects which raises complex questions about the reliability and integrity of data in electronic form. Electronic discovery refers to the electronic evidence discovered on digital objects that could be used in a legal proceeding such as litigation and others where evidence is in electronic format [14].

Digital forensics investigations evidence of cybercrime cases

There are several existing cybercrime cases that digital forensics investigations evidence has been used successfully to prosecute criminals. We highlight a few of such cases as follows:

- **Joseph E Duncan III**

A spreadsheet recovered from Duncan's computer contained evidence that showed him planning his crimes. Prosecutors used this to show premeditation and secure the death penalty [15].

- **BTK Killer:** Beat Torture Kill

Dennis Rader was convicted of a string of serial killings that occurred over a period of sixteen years. Towards the end of this period, Rader sent letters to the police on a floppy disk. Metadata within the documents implicated an author named "Dennis" at "Christ Lutheran Church"; this evidence helped lead to Rader's arrest.

- **Sharon Lopatka**

Hundreds of emails on Lopatka's computer lead investigators to her killer, Robert Glass. Lopatka started an internet business from a kit she purchased from an Arizona company. Using the Internet, Lopatka searched for a man who would torture and kill her. After contacting several people who turned out not to be serious, she finally found someone willing to fulfill her request. Glass and Lopatka exchanged many e- mails until they met in North Carolina where Glass strangled Lopatka using a nylon cord after torturing her for several days.

- **Corcoran Group**

Einstein vrs 357 lLC and Corcoran Group. This case confirmed parties' duties to preserve digital evidence when litigation has commenced or is reasonably anticipated. Hard drives were analyzed by a computer forensics expert, who could not find relevant e-mails the Defendants should have had. Though the expert found no evidence of deletion on the hard drives initially, evidence came out that the defendants were found to have intentionally destroyed emails, misled and failed to disclose material facts to the plaintiffs and the court.

- **Dr Conrad Murray –vrs- M Jackson**

Dr Conrad Murray, the doctor of the deceased Michael Jackson, was convicted partially by digital evidence found on his computer. The evidence included medical documentation showing lethal amounts of propofol a drug used for patients going for heart bypass operation.

- **Neil Entwistle**

Neil Entwistle was sentenced to life in prison for killing his wife and baby daughter. Internet history on his computer included a Google search "how to kill with a knife".

- **Robert Durall**

Prosecutors upgraded the charge against Robert Durall from second degree to first-degree murder based on Internet searches found on his computer with keywords including "kill + spouse," "accidental + deaths," "smothering," and "murder".

- **William Guthrie**

William Guthrie was convicted in 2000 and sentenced to life in prison for killing his wife, who was found, drowned in a bathtub with a toxic level of the prescription drug Temazepam in her body. Guthrie lost multiple appeals to exclude Internet searches for "household accidents," "bathtub accidents," and various prescription drugs, including Temazepam.

The nature of digital evidence requires us to use technology during an investigation, so the main difference between a digital investigation and a digital forensic investigation is the introduction of legal requirements. Hence, the theory of jurisprudence is relevant in digital evidence gathering.

Pre-search and Post seizure warrant challenges

Pre-search and post-seizure warrant are two major factors in digital forensic investigations processes that are posing many challenges to how digital evidence are gathered and are made admissible at court. In seizure and examination of any digital device, the pre-search warrant is a legal document that is given out to law enforcement agencies and digital forensics investigators by the court before they appear at the cybercrime scene to gather evidence for the investigation. The post-seizure warrant is a document that requires investigators to tick a checkbox of all activities they have carried out post investigations. The procedure follows a reverse order to ensure due diligence and chain of custody [16]. In the digital crime scene, the investigators are dealing with both physical device evidence and digital evidence. In DFI, we have live analysis and dead analysis. Live analysis environment occurs when investigators are using the operating system and web browsers of other system resources under-investigated to gather evidence. A dead analysis is where the systems are shut down, and investigators may use trusted application tools to find digital evidence. In 2012, the (EOCO), a DFI unit went to the Ghana Football Association offices and seized their computers. A case in question was when the Economic and Organized Crime Office (EOCO) invaded the Ghana football association (GFA) and seized their computer and other media for investigations [17]. The EOCO unit was ordered by the court to return all the seized evidence to the GFA as they did not follow procedures including requesting for a pre-search warrant after EOCO went and seized their computers. [18]. Post- seizure warrant ensures due diligent are followed after DFI procedures.

- **Technical challenges**: Factors such as Network, laptops, (BYOD) might be out of synch with security updates or might already be compromised. Lack of expertise, technically competent and certified investigator are major factors. Similarly, the challenge of using obsolete tools and lack of update procedures. Further, lack of reporting platforms and information sharing platforms to create awareness of the threat landscape, vulnerabilities, risks, and impact [19].

- **Legal challenges:** Digital evidence admissibility at court requires that the evidence is authentic, accurate, complete and convincing to the juror. However, the challenges of bridging the gap between the judiciary, law enforcement agencies, forensic investigators, and expert witnesses have been a major issue due to a lack of robust cybercrime legal framework. Additionally, the issues of implementing, enforcing the laws and the applying rule of law is also a major determinant in ensuring legal proceedings. Acquiring a pre- search and post-seizure warrant that meet the required legal objectives has been challenging due to a lack of formalized procedures and stakeholder involvement.

Approach

The cyber threat landscape is continuously evolving, and it is impacting greatly on how digital forensics investigations processes are carried out. The next section discusses the approach used by forensic examiners how the concepts of authentic, accurate, complete and convincing impact on the investigation approach and admissibility of evidence. Forensic investigation analysis approach involves an objective and critical assessment of digital evidence to gain an understanding of the nature of the attacks and to arrive at conclusions. The digital forensic crime scene is either in a dead state or live state. The dead state is where the crime has occurred, and the investigators have been called in to gather the digital evidence for lab investigation. The live state is where the cybercrime in ongoing and requires the investigator to determine the source and nature of attacks. The forensic investigator must pose certain basic skills such as perception skills, logical reasoning, analytical reason, critical thinking, and research skills required of a subjective expert. Cyber-attack and cybercrimes are discussed briefly and their relevance to digital forensic jurisprudence. DFI process includes understanding cyber-attack, cybercrimes and the cyber security control mechanisms. For instance, cyber security controls such as confidentiality, integrity, availability, accountability, auditability and nonrepudiation provide background knowledge of cyber security issues relevant when caring out digital forensic investigation process. Figure 1 depicts the relationships between cyber securities on digital forensics investigations.

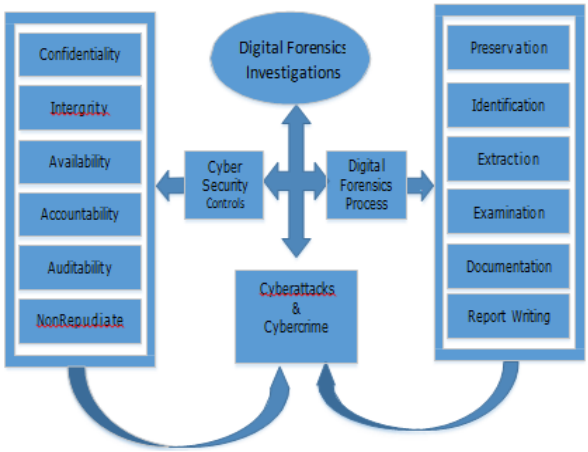

Figure 1: Cyber security on digital forensics investigations relationships.

Cyber-attack and cybercrime

The digital forensic examiners are required to have extensive knowledge of the motives, methods, and intents of perpetrators as

well as the difference between cyber-attacks, cybercrimes and the threat landscape. Cyber-attacks are (Penetration), and Cybercrimes are (Manipulations). Cyber-attacks are considered as the initial penetrations which can be randomly initiated attacks to gain access. Cybercrimes are considered as the various manipulations that could be deployed to exploit the systems after the penetration and the cascading impact of attacks. Examples of cyber-attacks include Malware, Spyware, Ransom ware and, Remote Access Trojan (RAT), Cross Site Scripting, SQL Injection, Session Hijacking, Cross Site Request Forgery. Cybercrime offences range from criminal activity against data to content and copyright infringement [20]. Examples of cybercrimes include software modifications, manipulations, alteration of delivery channels, ID theft, Intellectual property theft, Industrial espionage, advanced persistent threats (APTs), commands and controls (C&C) and other compromises. Cyber-attacks lead to cybercrimes and another system compromise [21,22]. Further, AACC concepts are discussed in relevance to digital forensic investigation process in the next section. Figure 2 categorizes the various cyber-attacks and cybercrimes in digital forensic investigations from a cyber-security perspective.

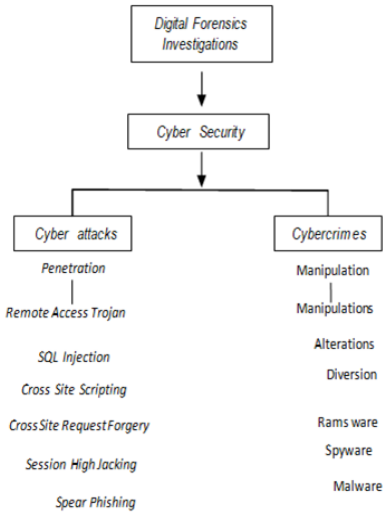

Figure 2: Categorizing cyber-attack and cybercrime.

Implementation

This section discusses the challenges faced by digital forensic investigators when implementing the investigation processes and how the challenges impact on admissibility at court. We look at the issues of inadmissibility that arise when digital evidence is not authentic, accurate, complete and convincing to the jury.

Authentic

Authentic in digital evidence gathering is to ensure that the evidence on digital objects gathered at the crime scene are the exact evidence and comes from the right source post preservation. That is crucial in the preservation phase as the authenticity of the evidence will determine whether the case may support or refute the hypothesis. There must be a pre-seizure and post- seizure legal document that specifies what the investigators are to do and procedures to follow when they appear at the crime scene. However, there have been instances where the investigator has appeared at the crime without a warrant and gather evidence without following due diligence. These digital objects include the digital device, digital media, and digital data such as e Discovery, industrial espionage, intellectual property, child pornography. Figure 3 provides an understanding of the taxonomy of the digital objects and background knowledge of the scene of the digital crimes, and how to gather evidence that ensures the evidence is accurate, complete, and convincing.

- The digital devices include computers, mobile phones, laptops, tablets, PDAs and smart screens
- The digital media includes the USB, Memory cards, printers, cameras, floppy disk and CD, routers and game consoles
- The digital data includes data stored on the digital device or the digital media employee fraud data, financial corruption, embezzlement, extortion, identity theft, bribery, theft of intellectual property or trade secrets, or pornography (Figure 3)

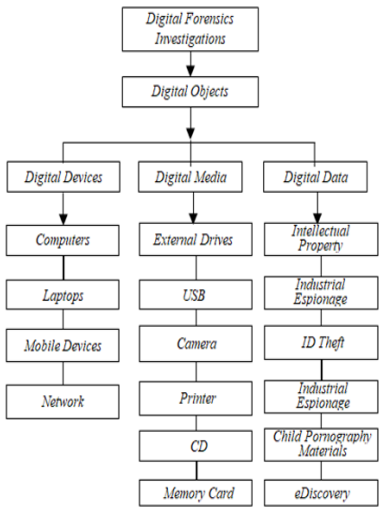

Figure 3: Digital objects in digital forensic investigations.

In digital forensics investigation, ensuring the digital evidence is usable as evidence and admissible at court, it is essential that none of the objects is tampered with and the procedure used to gather the evidence follow due diligence. For instance, digital data may be at rest, active, deleted, hidden, encrypted, overwritten or partially overwritten. All this evidence may be necessary for litigation purposes and evidential integrity and admissibility at court. In the event of uncertainties all the evidence that is overwriting to or partially written to may be used to assure accurate, reliable, verifiable, and repeatable findings based on the judicial system.

Accurate

Accurate in digital forensic investigations is to ensure that the evidence gathered is consistent and followed the legally correct chain of custody from pre-seizure through to post-seizure. The investigator must be able to account for all the evidence gathered from the time of arrival at the crime scene, from how evidence was gathered originally and to how it was preserved and where it was kept. The scientific principles related to the digital evidence gathering, processing, and

analysis must be applied to ensure both a proper chain of custody and accurate analysis. The challenge of maintaining accurate digital evidence of what happened to the exhibit between the initial appearance at the crime scene, first evidence collected and its appearance at court unaltered has caused lots of digital forensic evidence gathered to be inadmissible at court. Maintaining accuracy in evidence gathering requires good record keeping of all activities and logs of names, date, time, questions, findings, and assumptions that may prove hypothetical. The preservation of digital crime scene for identification for legal, business, and operational processes requires a different approach to that of the preservation of digital media at the forensic lab. Although digital evidence may be invincible, forensic examiners are required to use legal approaches, techniques, and tools for discovering digital data that resides on various media. Maintaining an accurate record of all activities in both preservation processes and ensuring the evidence is authentic could lead to uncertainties and inadmissibility. For instance, in a life analysis, the legal requirements procedure is that the digital device or media is unplugged from the hub during investigations before a mirror image is done to the data. However, unplugging the device could lead to the system shut down, and eventually change the time stamp in situations where the data was not hashed. While the dead analysis is carried out at the forensic lab and evidence could be tampered with in transit and could lead to inaccuracies in data extraction and analysis with that of initial evidence.

Complete

Complete: Process requires that all the digital evidence gathering must follow a consistent chain of custody from start to finish to that the evidence is authentic and accurate. The legal requirement for completeness demands that all exhibit numbers must be documented and ensure they are consistent from the initial crime scene preservation phase to the final report. These include the investigation procedures, materials, techniques, tools, and hypothesis used to arrive at the results. Further, the procedures used, and findings should be peer reviewed using expert witnesses to verify the legality of the evidence. The expert witness must arrive at the same result with that of the investigator without any legal disputes. The forensic investigator is required to explain the investigation process used to arrive at a conclusion. That includes the process used to identify the type of evidence, whether it is dead or live at the crime scene. How the evidence was preserved at the crime scene and supposed it was analysis, how was the evidence preserved at the forensic lab? The issues of digital evidence acquisition and extractions approach have been one of the challenging factors that are impacting on how evidence is considered complete. For instance, the investigator must be able to identify all the trails of the digital footprints that were established when the digital device was connected to the router including the timestamps, access logs, IP address, MAC address and activity logs. An adversary may use MAC address changer tool or IP address changer tool to change the MAC or IP address, commit cybercrimes and revert to the first MAC or IP address after the attack. The question is how the investigator will authenticate these artifacts and the time of the crime to an event is critical in prosecution. Further, the challenges of extracting evidence from Random Access Memory (RAM) and Random Only Memory (ROM) may impact on the examination of the digital evidence. Evidence on RAM may be volatile and requires the digital device to have electric power to keep the evidence. Whiles ROM is non- volatile and stores the evidence on the hard drive.

Convincing

The convincing aspects in the issues of evidence gathering and consider how the digital evidence must meet a certain level of acceptability from pre-handling of the evidence to post handling. For digital evidence to be convincing to the juror, there should not be any interference or contamination and must not cast any shadow of doubt in the jury's mind. Applying due diligence in digital forensics investigation process addresses the issues of authentic, accurate, completeness of the evidence. The admissibility of the evidence gathered must meet certain legal requirements and standards. The jury may come from different academic backgrounds; hence the evidence must not be too technical. Digital evidence answers questions raised regarding digital events and how the hypotheses were developed and tested throughout the investigation process. The forensic investigators use the scientific methods (legal Procedures) to develop a hypothesis from the evidence that was found at the digital crime scene. The hypothesis is tested by looking for additional evidence that shows the hypothesis is impossible or refutable. For instance, prosecutors upgraded the charge against Robert Durall from second degree to first-degree murder based on Internet searches found on his computer with keywords including "kill + spouse," "accidental + deaths," "smothering," and "murder" . Neil Entwistle was sentenced to life in prison for killing his wife and baby daughter. Internet history on his computer included a Google search "how to kill with a knife". Admissibility of digital evidence at court rises questions of what legal procedures used during the internet search for evidence are considered. Such as, what was the search criteria used to gather evidence? How was the evidence trail maintained during the evidence gatherings? What are the digital forensic tools that were used to gather evidence at the extraction phase? Are the forensic tools updated? What is the level of expertise of the investigators? What standards were used to validate the level of acceptability of the evidence? These questions and many more must be address in the cause of the investigation for the digital evidence to be admissible and convincing to the jury.

Discussion

This section discusses the challenges impacting of digital forensic investigation jurisprudence. Presenting digital forensic evidence at court has proved to be challenging due to the invincibility nature of cybercrimes, the evolving nature of business processes, the changing threat landscape and the phenomenon surrounding cyber-attacks. In digital forensic jurisprudence, while jurisprudence considers the philosophy and theory of law, cyber jurisprudence considers the science and philosophy or theory of Law in relations to cyber incidence. Whereas, digital forensic investigation jurisprudence considers the legal implications, the legal ramifications of digital evidence gathering and its admissibility at court. Admissibility of evidence at court does not necessarily mean the evidence is convincing to the jury. It considers the legal ramifications and the evolving nature of digital devices and digital media in the event of cyber-attacks and cybercrimes. Digital forensics investigations approach requires an evaluation of the source of digital devices at the digital crime scene; explore various file formats to extract usable evidence information. The analyst must develop timelines to identify sequences and patterns in time of events, especially in the dead analysis. Further, performing a functional analysis of the information extracted to ascertain what penetrations and manipulations were possible and impossible. Furthermore, perform relational analysis on the hypothesis to determine the relationships

and interaction between cyber-attack and cybercrime components. The theory behind digital evidence searching process involves two phase. First the forensic examiner must define the general characteristics of the digital object under investigation which is being searched for. Secondly, look for the digital object in a collection of the extracted data. The issues arise when the evidence are in different file formats but are not obvious especially JPG files hidden in images that are in steganography. Different web browser habits vary depending on the evidence search being searched for. Different web browser could be used to commit a cybercrime from one jurisdiction to another in different time frames. Hence, gathering data to support or refute a hypothesis could prove challenging as the evidence may not be static and could impact on the accuracy of the digital evidence. For instance, when investigating web browser habits, we look for the cyber trail such as the web browser cache, history, bookmarks, logs, cookies, pop ups, favorites and temp files. Mozilla, Google Chrome, Safari, and Microsoft Edge may all behave differently.

Standards Used for Digital Forensic Investigation Process

There are existing standards that provide comprehensive guidelines, collaborative support, and idealized models and processes for digital forensic investigations and electronic evidence. Convention on Electronic Evidence (CEE) 2016, the treaty provides general guidance on the recognition and admissibility of electronic evidence from foreign jurisdictions and encourages judges and lawyers to appreciate the concepts admissibility of digital evidence. ISO/IEC27043 provides guidelines for pre- incident to post-incident preparations that encapsulate idealized models across various scenarios in order that investigations can are repeated across every scenario and may obtain the same result. ISO/IEC 27037, is designed for incident responses. To maintain the integrity and authenticity of digital evidence and provides guidelines for specific activities in preserving and handling potential digital evidence [20]. ISO/IEC 27041, provides assurance that incident management, evidence handling, storage and methods used in the investigative process are appropriate for the incident under investigation and the required results [23]. ISO/IEC 27042, provides a comprehensive guide to ensure that tools, techniques, and methods used guide for on the conduct of the analysis and interpretation in order to identify and evaluate digital evidence to aid understanding of an incident in relation to ISO 27037 [24]. The digital forensic standards and processes include identification, collection, acquisition, and preservation and can expedite investigations. However, maintaining chain of custody and ensuring that the digital evidence is authentic, accurate, complete and convincing to the juror in line with standards irrespective of the process adopted could ensure digital forensic investigation jurisprudence.

Conclusion

This paper has discussed the challenges that are impacting on digital forensic jurisprudence and admissibility of evidence at court. Gathering and analyzing digital evidence that ensures that the digital evidence is authentic, accurate, complete and convincing to the juror does not depends solely on the process adopted but, on a sound, forensic discipline. Other factors impacting on the admissibility of evidence at court are due to factors such as inadequate chain of custody, illegal procedures, and deficiencies in evidential integrity. Lack of expertise in the field has further exacerbated the issues of inadmissibility of evidence as it impacts on due diligence and due process of jurisprudence. Digital forensic investigation standards, tools and techniques may gather all digital evidence for admissibility. However, they may not be convincing to jury until the evidence are authentic, accurate and complete in following proper chain of custody and due diligence were applied. The challenges of maintaining authenticity in digital evidence gathering are more than just finding, collecting, and analyzing the data, generating a report and testifying in court. Further research is required in harmonization digital forensic investigations and the legal framework due to the evolving nature of organizations goals, technological advancement and the evolving threat landscape.

References

1. Robertson PT (2017) Defining A Cyber Jurisprudence: Towards Evolving the Philosophy and Theory of Cyber Law: A Foundational Treatise.
2. Ofori YA, Boateng Y, Yankson HG (2019) Relativism Digital Forensic Investigations Model. IEEE Xplore.
3. Davies G, Smith k (2019) The Feasibility of Creating a Universal Digital Forensics Framework. Forensic Leg Investig Sci. 5: 1-9.
4. Association of Chief Police Officers: ACPO (2012) Good Practice Guide for Digital Evidence.
5. Mason S (2016) Draft Convention on Electronic Evidence. Digital Evidence and Electronic Signature Law Review 13: 1-11.
6. Vacca JR (2005) Computer Forensics-Computer Crime Scene Investigation.
7. Ma L, Choo KR, Hsu H, Zhou X (2016) Perspectives on Cyber Science and Technology for Cyberization and Cyber-Enabled Worlds. IEEE.
8. United Nation Office on Drugs and Crime (UNODC) (2013) A Comprehensive Study on Cybercrime: Harmonizing of National Frameworks.
9. UNODC The Doha Declaration (2018) Promoting a Culture of Lawfulness: Mutual Legal Assistance.
10. Boasiako A, Venter H (2017) A Model for Digital Evidence Admissibility Assessment. Advances in Digital Forensics 511: 23-38.
11. Kent K, Chevalier S, Grance T, Dang D (2006) Guide to Integrated Techniques into Incident Response. NIST, Computer Security Division, IT Laboratory.
12. ISO\IEC27043 (2016) Information Technology Security Techniques, Incident Investigation Principles, and Processes.
13. International Laboratory Accreditation Cooperation (ILAC), (2014).
14. Casey E (2009) Handbook of Digital Forensics and Investigation. Academic Press Pg no: 567.
15. Haynes N (2018) Cyber Crimes. Ed-Tech Press Pg no: 58.
16. Orin SK (2005) Search Warrant in An Era of Digital Evidence. Mississippi Law Journal 85: 1-61.
17. Economic and Organized Crime Office (2015) Court: EOCO raid on GFA illegal.
18. Economic and Organized Crime Office raid GFA office (2010).
19. Ofori AY, Islam S (2019) Cyber Security Threat Modelling for Supply Chain Organizational Environments MDPI Future Internet 11: 1-63.

20. ISO\IEC27037 (2012) Information Technology Security Techniques, Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence.

21. Ofori AY, Abdulai JD, Katsriku F (2018) Cybercrime and Risk for Cyber Physical Systems: A Review. IJCSDF 8: 43-57.

22. CAPEC-437: Supply Chain. Common Attack Pattern Enumeration and Classification: Domain of Attack.

23. ISO\IEC27041 (2015) Information Technology Security Techniques, Guidelines on Assurance Suitability and Adequacy of Incident Investigative Method.

24. ISO\IEC27042 (2015) Information Technology Security Techniques, Guidelines for the Analysis and Interpretation of Digital Evidence.

Advances In Industrial Biotechnology | ISSN: 2639-5665

Advances In Microbiology Research | ISSN: 2689-694X

Archives Of Surgery And Surgical Education | ISSN: 2689-3126

Archives Of Urology

Archives Of Zoological Studies | ISSN: 2640-7779

Current Trends Medical And Biological Engineering

International Journal Of Case Reports And Therapeutic Studies | ISSN: 2689-310X

Journal Of Addiction & Addictive Disorders | ISSN: 2578-7276

Journal Of Agronomy & Agricultural Science | ISSN: 2689-8292

Journal Of AIDS Clinical Research & STDs | ISSN: 2572-7370

Journal Of Alcoholism Drug Abuse & Substance Dependence | ISSN: 2572-9594

Journal Of Allergy Disorders & Therapy | ISSN: 2470-749X

Journal Of Alternative Complementary & Integrative Medicine | ISSN: 2470-7562

Journal Of Alzheimers & Neurodegenerative Diseases | ISSN: 2572-9608

Journal Of Anesthesia & Clinical Care | ISSN: 2378-8879

Journal Of Angiology & Vascular Surgery | ISSN: 2572-7397

Journal Of Animal Research & Veterinary Science | ISSN: 2639-3751

Journal Of Aquaculture & Fisheries | ISSN: 2576-5523

Journal Of Atmospheric & Earth Sciences | ISSN: 2689-8780

Journal Of Biotech Research & Biochemistry

Journal Of Brain & Neuroscience Research

Journal Of Cancer Biology & Treatment | ISSN: 2470-7546

Journal Of Cardiology Study & Research | ISSN: 2640-768X

Journal Of Cell Biology & Cell Metabolism | ISSN: 2381-1943

Journal Of Clinical Dermatology & Therapy | ISSN: 2378-8771

Journal Of Clinical Immunology & Immunotherapy | ISSN: 2378-8844

Journal Of Clinical Studies & Medical Case Reports | ISSN: 2378-8801

Journal Of Community Medicine & Public Health Care | ISSN: 2381-1978

Journal Of Cytology & Tissue Biology | ISSN: 2378-9107

Journal Of Dairy Research & Technology | ISSN: 2688-9315

Journal Of Dentistry Oral Health & Cosmesis | ISSN: 2473-6783

Journal Of Diabetes & Metabolic Disorders | ISSN: 2381-201X

Journal Of Emergency Medicine Trauma & Surgical Care | ISSN: 2378-8798

Journal Of Environmental Science Current Research | ISSN: 2643-5020

Journal Of Food Science & Nutrition | ISSN: 2470-1076

Journal Of Forensic Legal & Investigative Sciences | ISSN: 2473-733X

Journal Of Gastroenterology & Hepatology Research | ISSN: 2574-2566

Journal Of Genetics & Genomic Sciences | ISSN: 2574-2485

Journal Of Gerontology & Geriatric Medicine | ISSN: 2381-8662

Journal Of Hematology Blood Transfusion & Disorders | ISSN: 2572-2999

Journal Of Hospice & Palliative Medical Care

Journal Of Human Endocrinology | ISSN: 2572-9640

Journal Of Infectious & Non Infectious Diseases | ISSN: 2381-8654

Journal Of Internal Medicine & Primary Healthcare | ISSN: 2574-2493

Journal Of Light & Laser Current Trends

Journal Of Medicine Study & Research | ISSN: 2639-5657

Journal Of Modern Chemical Sciences

Journal Of Nanotechnology Nanomedicine & Nanobiotechnology | ISSN: 2381-2044

Journal Of Neonatology & Clinical Pediatrics | ISSN: 2378-878X

Journal Of Nephrology & Renal Therapy | ISSN: 2473-7313

Journal Of Non Invasive Vascular Investigation | ISSN: 2572-7400

Journal Of Nuclear Medicine Radiology & Radiation Therapy | ISSN: 2572-7419

Journal Of Obesity & Weight Loss | ISSN: 2473-7372

Journal Of Ophthalmology & Clinical Research | ISSN: 2378-8887

Journal Of Orthopedic Research & Physiotherapy | ISSN: 2381-2052

Journal Of Otolaryngology Head & Neck Surgery | ISSN: 2573-010X

Journal Of Pathology Clinical & Medical Research

Journal Of Pharmacology Pharmaceutics & Pharmacovigilance | ISSN: 2639-5649

Journal Of Physical Medicine Rehabilitation & Disabilities | ISSN: 2381-8670

Journal Of Plant Science Current Research | ISSN: 2639-3743

Journal Of Practical & Professional Nursing | ISSN: 2639-5681

Journal Of Protein Research & Bioinformatics

Journal Of Psychiatry Depression & Anxiety | ISSN: 2573-0150

Journal Of Pulmonary Medicine & Respiratory Research | ISSN: 2573-0177

Journal Of Reproductive Medicine Gynaecology & Obstetrics | ISSN: 2574-2574

Journal Of Stem Cells Research Development & Therapy | ISSN: 2381-2060

Journal Of Surgery Current Trends & Innovations | ISSN: 2578-7284

Journal Of Toxicology Current Research | ISSN: 2639-3735

Journal Of Translational Science And Research

Journal Of Vaccines Research & Vaccination | ISSN: 2573-0193

Journal Of Virology & Antivirals

Sports Medicine And Injury Care Journal | ISSN: 2689-8829

Trends In Anatomy & Physiology | ISSN: 2640-7752

Herald Scholarly Open Access, 2561 Cornelia Rd, #205, Herndon, VA 20171, USA.
Tel: +1 202-499-9679; E-mail: info@heraldsopenaccess.us
http://www.heraldopenaccess.us/