BOOK CHAPTER | *"Freebies""*

Digital Forensic and Distributed Evidence

Emmanuel Kpakpo Brown
Digital Forensics & Cyber Security Graduate Programme
Department Of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mails: emmanuel.brown@st.gimpa.edu.gh
Phone: +233244976646

ABSTRACT

Digital Forensics investigation is the science and legal process of investigating computer/cybercrimes and digital media or objects to gather evidence. This new and fast evolving field encompasses computer forensics, network forensics, mobile forensics, cloud computing forensics, and IoT forensics; and for this reason have digital evidence distributed widely when the need arises for crime prosecution. Digital evidence must be authentic, accurate, complete, and convincing to the jury for legal admissibility at the court of law. In many instances due to the distributed nature of digital forensic evidence and the legal procedures to be adhered to in evidence gathering at a digital crime scene, presenting at the law courts have proven to be challenging and in some instances inadmissible. Following legal procedures in evidence gathering at a digital crime scene is critical for admissibility and prosecution. This paper aims to discuss digital forensics investigations jurisprudence in relation to distributed digital evidence. For the study to be relevant to policy and practice, forensic tools and frameworks, legal and ethical obligations, and digital evidence handling and admissibility are highlighted. This paper does not follow any forensic investigations process; but rather discusses the need for development and implementation of unique frameworks that could be utilised to gather distributed digital evidence required for admissibility in court.

Keywords - Digital forensics investigations; Digital evidence; Jurisprudence

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Emmanuel Kpakpo Brown (2022): Digital Forensic and Distributed Evidence
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 357-362
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P57

1. INTRODUCTION

Joseph (2018) defines digital forensics as the application of scientifically established methods in preserving, collecting, validating, identifying, analysing, interpreting and presenting digital evidence to the court of law after obtaining the evidence from reconstruction of events if possible. In the late 1990s and early 2000s when computer based crime started growing with the increasing usage of computers and the Internet.

Digital forensics developed as an independent field (Sriram Raghavan, n.d.). The field is made up of computer forensics, network forensics, mobile forensics, cloud computing forensics, and IoT forensics.

The varied branches of the field largely explain the distributed nature of evidence to be collected when a computer/cybercrime is reported or suspected to have been perpetrated. In evidence law, digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial. According to Ryan (n.d.) for evidence to be admissible in court, it must be relevant, material and competent, and its probative value must outweigh any prejudicial effect. This paper gives a comprehensive review of digital forensic and distributed evidence. It focuses on the frameworks for gathering distributed digital evidence that can meet the techno-legal requirements for admissibility in the courts of law. The rest of this paper is organized as follows - section 2 presents a background to the study; section 3 discusses the related literature; section 4 touches on research gaps/findings; section 5 concludes the study; section 6 makes recommendation for policy and practice, and section 7 provides directions for future works.

1.1 Background To The Study

Digital forensics is most closely defined by legal requirements, and its growth and evolution is informed and guided by case law, regulatory changes, and the ability of cyber-lawyers and digital forensics experts to take the products of forensic tools and processes to court (Ryan, n.d.).
In tradition forensics, the evidence is something tangible that could identify the criminal, such as blood, fingerprint, and hair, but these evidences cannot be found at digital forensics (Khanafseh & Qatawneh, 2019). The law courts resort to digital evidence have increased in the past few decades.

They have allowed the use of e-mails, digital photographs, ATM transaction logs, word processing documents, instant message histories, internet browser histories, databases, digital printouts, Global Positioning System tracks, logs from a hotel's electronic door locks, and digital video or audio files found on digital devices such as computers, external hard drives, flash drives, routers, smartphones, tablets, cameras, smart televisions, Internet-enabled home appliances; and communication service providers business records; and cloud storage providers records of user activity and content. With the rise and use of several electronic means of transfer of documents and information, the commission of especially a cybercrime transcends national and continental boundaries; hence distributing evidence and making the gathering process a herculean task. This study is largely focused on what the current challenges of gathering distributed digital forensic evidence are; the available harmonization frameworks for admissibility of the evidence by the Courts for prosecution.

2. RELATED LITERATURE

A literature review was adopted as a research methodology in order to locate existing relevant literature based on prior formulated research questions and to evaluate their respective contributions to the field. The literature found was used to map emerging issues related to digital forensic and distributed evidence as follows.

Forensic Tools and Frameworks

The various branches of digital forensics should have unique tools for gathering evidence and upon practice and perfecting each, should be harmonised to facilitate digital forensics jurisprudence. Recently Patil & Devane (2022) have proposed a network forensics protocol that ensures tracking up to the true source of digital evidence by collecting beforehand forensically sound evidence and the protocol can collect target data from the device in the form of a device fingerprint. Joseph (2018) began an implementation of a digital forensic framework that could be used with standalone systems as well as in distributed environments, including cloud systems. It is oriented towards combining concepts of cyber forensics and security frameworks in operating systems. Khanafseh & Qatawneh (2019) conducted a survey of various frameworks and solutions in all branches of Digital Forensics with a focus on Cloud Forensics that concluded that a solution to improve many key issues such as security, accuracy, performance and privacy in the framework must be considered.

Cyber offenders spread their influence as fast as the Internet and cloud computing develop; therefore it aggravates the challenges in collecting and analyzing digital evidence in a cybercrime investigation. Establishing timeline information using date-time stamps is recommended for law enforcement agents in investigating cloud-related crime (Kao, 2016). Additionally, a model for digital evidence admissibility assessment Antwi-Boasiako and Venter (2017) - the *Harmonized Model for Digital Evidence Admissibility Assessment (HM-DEAA)* encapsulates the essential techno-legal requirements that determine evidence admissibility in the court.

Legal and Ethical Obligations

The existence of some forensic tools and frameworks is laudable, but there is always the need to assess the legal rudiments of utilizing these frameworks in gathering and harmonising distributed evidence to facilitate admissibility for the administration of justice in the courts of law. Apau & Koranteng, (2020) assesses the effectiveness of the legal infrastructure for digital forensics investigations in Ghana and concludes that, existing legislations are scattered and cumbersome whereas mandated institutions lack the requisite capacity.

When a case is identified to have evidence distributed across geographical boundaries - legal frameworks and human rights information about jurisdictions come into play. It therefore becomes imperative to identify country-specific laws and cultural norms that may affect the investigative process and also determine whether additional subject-matter or local professionals will be needed (International, n.d.). Many applications, websites, and digital devices utilize cloud storage services; distributing users' data in fragments by many different cloud service providers in servers in multiple locations (Practices & Acquisitions, 2018). Retrieving data from these providers is quite challenging and therefore the need to resort to International Cooperation against Cybercrime framework.

Digital Evidence Handling and Admissibility

How distributed forensic evidence is handled is a paramount determinant for use in jurisprudence. Digital evidence is volatile and fragile and the improper handling of the evidence can alter it. The four phases (Standard & Last, 2018) involved in the initial handling of digital evidence: identification, collection, acquisition, and preservation must be adhered to. In the course of handling digital evidence, certain legal and technical requirements must be met to ensure the admissibility of the evidence in a court of law (Antwi-boasiako et al., 2018).

Ay & Akoto (2020) asserts that for digital evidence to appear at court to be legally admissible, the evidence must be authentic, accurate, complete, and convincing to the jury. Antwi-boasiako et al., (2018) further states that for admissibility, the court examines the legal authorization to conduct searches and seizures of information and communication technology and related data, and the relevance, authenticity, integrity, and reliability of the digital evidence.

3. IMPLICATIONS FOR CYBER SAFETY IN AFRICA

Cyber safety has globally become one of the most critical issues to all who are active in cyber space. In most African countries no coordinated activities are taking place, even though many children are already active on cyber space. There is less education on cyber safety principles and the admissibility of cyber forensic evidence in the court of law when a crime is suspected to have been committed. The issue becomes more scarier now that almost all the IT infrastructure in many African countries are connected to the Internet and making digital evidence spread across vast geographic distances and several sovereign jurisdictions (Mahfouz & Adjei-quaye, 2017).

Modern day computers come with or can be augmented to provide huge amounts of data storage. Seizing and freezing can no longer be accomplished simply by burning a single CDROM (Ryan, n.d.). The problem of locating relevant evidence within massive amounts of data is a daunting task especially when a digital forensic investigator has to look beyond a single computer. In modern distributed computer architectures, the digital evidence we may need for the Courts may reside on many different servers and clients within an organization's IT infrastructure. The distributed nature of digital evidence makes it more difficult for Africa that is deficient in the technical expertise and resources required to properly investigate cybercrimes to bring sanity into its cyberspace.

4. RESEARCH GAPS/FINDINGS

Interestingly, despite the valuable reviews, the various studies did a generalized distributed digital evidence framework assessment except Khanafseh & Qatawneh (2019) that surveyed available frameworks and focused specifically on cloud computing framework; and the Joseph (2018) implementation of digital forensic framework that could be used with standalone systems as well as in distributed environments, including cloud systems and solutions of cloud forensics - both of which are at the experimental stage. The effectiveness of the Antwi-boasiako et al., (2018) HM-DEAA have not been assessed or attested to by players in the criminal prosecutions circles locally in Ghana and internationally.

The focus of developing frameworks for gathering distributed digital evidence have largely been general frameworks, apart from the cloud computing forensics branch that have received some attention. All the other branches - computer forensics, network forensics, mobile forensics and IoT forensics have been left to be gathered with *one-size-fits-all* frameworks.

5. CONCLUSION

A standardized and harmonized framework or solution that comprehensively captures the techno-legal requirements of DFI is an indispensable tool for computer/cybercrime investigators and digital forensics experts to handle and/or otherwise process distributed digital evidence expeditiously for admissibility in the law courts.

6. RECOMMENDATION FOR POLICY AND PRACTICES

There is first of all, the need to streamline existing laws and implement existing policies, technical and legal requirements for evidence admissibility. Standard procedures that are coherent and ensure harmony between lawyers, judges, forensic experts, law enforcement agencies, corporations, individuals, and the court must be adhered to. Secondly, the harmonization of cybercrime investigation and digital forensics practices across borders is essential for investigations which often times involve more than one legal jurisdiction. Furthermore, heavy investments must be made to boost the capacities of the relevant institutions engaged in both digital evidence gathering and prosecution.

7. DIRECTION FOR FUTURE WORKS

While this work discovered that the available literature is mainly geared towards general framework for digital forensics; only a few studied a specific branch of digital forensics such as cloud computing. Future works could explore unique frameworks designed and implemented for the other branches of digital forensics - computer forensics, network forensics, mobile forensics, and IoT forensics for gathering distributed digital evidence for jurisprudence. Issues such as security, accuracy, performance and privacy with any of the frameworks could also be considered.

The above apart, a study into the unique and relevant legal requirements for digital evidence gathering and admissibility for different jurisdictions (cross-border) could be explored and recommendations for harmonization made. Additionally, a future study could focus on comparing and contrasting the different digital forensic investigation processes for the various digital devices and propose a process that is compatible with all devices and environments. The last but the least, a study could also be conducted into digital forensic technical mechanisms, the availability of capacity building programs, organisational infrastructure as well as the existence of cooperation mechanisms.

REFERENCES

1. Antwi-boasiako, A., Venter, H., Antwi-boasiako, A., Venter, H., Model, A., Evidence, D., & Assessment, A. (2018). *A Model for Digital Evidence Admissibility Assessment To cite this version : HAL Id : hal-01716394*.
2. Apau, R., & Koranteng, F. N. (2020). Forensic Science International : Synergy An overview of the digital forensic investigation infrastructure of Ghana. *Forensic Science International: Synergy*, *2*, 299–309. https://doi.org/10.1016/j.fsisyn.2020.10.002
3. Ay, O., & Akoto, D. (2020). *Digital Forensics Investigation Jurisprudence : Issues of Admissibility of Digital Evidence*. https://doi.org/10.24966/FLIS-733X/100045
4. International, K. (n.d.). *Cross-border investigations: Are you prepared for the challenge?*

5. Joseph, A. (2018). *Digital Forensics in Distributed Environment*. *April*. https://doi.org/10.4018/978-1-5225-4100-4.ch013
6. Kao, D. (2016). *Cybercrime investigation countermeasure using created- accessed-modified model in cloud computing environments*. *September 2015*.
7. Khanafseh, M., & Qatawneh, M. (2019). *A Survey of Various Frameworks and Solutions in all Branches of Digital Forensics with a Focus on Cloud Forensics*. *September*. https://doi.org/10.14569/IJACSA.2019.0100880
8. Mahfouz, M., & Adjei-quaye, A. (2017). *Computer & Cyber Forensics : A Case Study of Ghana Computer & Cyber Forensics : A Case Study of Ghana*. *January*.
9. Patil, R. Y., & Devane, S. R. (2022). Network Forensic Investigation Protocol to Identify True Origin of Cyber Crime. *Journal of King Saud University - Computer and Information Sciences*, *34*(5), 2031–2044. https://doi.org/10.1016/j.jksuci.2019.11.016
10. Practices, S. B., & Acquisitions, C. F. (2018). *Scientific Working Group on Digital Evidence Scientific Working Group on Digital Evidence*. *0*, 1–11.
11. Ryan, D. J. (n.d.). *Legal Aspects of Digital Forensics*.
12. Sriram Raghavan. (n.d.). *Digital forensic research: current state of the art*.
13. Standard, T., & Last, W. A. S. (2018). *THIS VERSION REMAINS CURRENT .*