BOOK CHAPTER | *"If you Know, You Know"*

Evidence Based Reconstruction for Digital Forensics

Ellen Akongwin Abanga
Digital Forensics and Cyber Security Graduate Programme
Department of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: ellen.abaga@st.gimpa.edu.gh
Phone: +233540337659

ABSTRACT

Evidence based reconstruction may often be even more illuminating than other traditional evidence gathering strategies, but it is also extremely delicate and unpredictable due to the fact that evidence may not always be conclusive. The integrity of digital evidence is therefore extremely important, particularly when it comes from allegedly unlawful, illegitimate, or harmful activity. Regardless of the good or bad consequences of the acts and activities that created the evidence, the capture and reconstruction of events are critical to the operation of the digital world. Owing to the lack of skill and knowledge of digital forensics in Ghana, it creates a susceptible environment for criminals to continue their operations while avoiding prosecution due to a lack of evidence to prosecute them. The reconstruction of occurrences based on evidence is considered an eminent need for Africa and for that matter Ghana. Hence, the need for well-defined and advanced knowledge in evidence based reconstruction in digital forensics investigation to bridge the gap currently existing. This paper reviews literature on the concept of evidence based reconstruction as a means to advance knowledge on its relevance to the Africa region and Ghana for that matter. This would help forensics investigators to better understand the need for focus on using digital tools for reconstruction and focusing on evidence driven activities in case of crime and investigations. Finally, this paper presents an elaborated view from a literature point of view over the evidence based reconstruction and also helps other fellow colleagues in their quest to further understand the concept.

Keywords: Evidence, Reconstruction, Digital evidence, Digital forensics, Investigation.

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

Citation: Ellen Akongwin Abanga (2022): 5G Cellular Network Forensics
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 185-190
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P30

1. INTRODUCTION

Evidence is defined as "any matter of fact, the effect, tendency or design of which is to produce in the mind a persuasion of the existence or non-existence of some other matter of fact" (Routledge, 2004). In gathering evidence for digital forensics and gaining a clear view of events and artefacts and activities that occur throughout time is a difficult task.

One of the most important and difficult challenges in digital forensics is reconstructing the chronology of events and activities, which allows digital investigators to grasp the history of digital crime and interpret the conclusion in the form of digital evidence (Bhandari & Jusas, 2019). Because of today's fast expansion of the internet, networked gadgets, and creative technologies, this difficult endeavor necessitates the processing of enormous volumes of data. What makes the task more difficult is the fact that, it requires hard core evidence to be able to establish a good case and be able to resolve any issues associated. Attribution, discovering a leak and analyzing the probable harm that happened following a breach are the most prevalent reasons for undertaking digital forensics (Bhandari & Jusas, 2019).

The event reconstruction step of a digital forensic inquiry is crucial in determining what transpired during the occurrence. The findings of this phase are used by the digital investigator to generate court reports. Because the outcomes must be repeatable and verified, the event reconstruction procedures must be thorough and evidence based. At the moment, information representation has solitary and fragmented properties. The source text information explaining data structures is broadly distributed in different information carriers, resulting in the emergence, development, and output of the information object not being displayed intuitively and systematically, and the information of other related information objects and their interrelationships being unavailable, so the reconstruction of information organization form is critical in today's era (Pan, Jingchang & Bo, 2020). However, with the growth in the need for hardcore evidence to be able to reconstruct an event and make available information reflect actual event occurrence, evidence based reconstruction approach seems best in most situations to enhance any adequate prevention and legal processes.

1.1. Background to the Study

The methodical process of putting together evidence and information obtained during an investigation in order to gain a clearer picture of what happened between the victim and the perpetrator during a crime is referred to as reconstruction. A critical capacity for digital forensics is reconstruction, which seeks to reconstruct a past execution of an attack delivery process. Existing methodologies, such as log-based forensics or record-and-replay techniques, are unsuitable for dealing with complicated and long-running current applications for cybercrime scene reconstruction and post mortem forensic analysis (Yonghwi, Weihang, Jinho, Hyung & Perdisci. 2021).

Log-based cyber forensics approaches, in particular, frequently lack inspection capabilities and do not give insights on how the assault unfolded. Evidence based reconstruction is gaining roots in digital forensics as these challenges keep being a major concern (Yonghwi, Weihang, Jinho, Hyung & Perdisci. 2021). Digital evidence is information that is saved or communicated in binary form and can be used in court (National Institute of Justice, 2021). It may be found on a computer hard disk, as well as a mobile phone. Electronic crime, or e-crime, such as credit card fraud, is frequently connected with digital proof. Digital evidence, however, is being utilized to prosecute all sorts of crimes, not only e-crime. Analysts in computer forensics seek to recover digital evidence from digital and cyber/physical equipment such as network devices, computers, smart and mobile sensors and devices, as well as drones and robots. Unfortunately, forensic investigations are becoming less successful as anti-forensics tactics become more prevalent (Yaacoub, Noura, Hassan & Ola, 2021).

In fact, contemporary forensics methodologies suffer from a variety of technological shortcomings as a result of anti-forensics technologies used to escape detection. Anti-forensics tactics are used to impede and distort forensics investigations by targeting forensics tools or removing, burying, or encrypting data. Some anti-forensics technologies, in particular, are employed to undermine the integrity of evidence (Yaacoub, Noura, Hassan & Ola, 2021). There are two basic approaches to dealing with a cybersecurity incident: recover swiftly or collect evidence (Cyber Security Coalition, 2015): The first strategy, recover rapidly, is focused with incident containment to minimize impact rather than data retention and/or collecting. Because of its emphasis on rapid reaction and recovery, valuable evidence may be lost.

The second method watches the cybersecurity event and focuses on digital forensic apps to collect evidence and information about the occurrence (Cyber Security Coalition, 2015). The significance of having an evidenced based reconstruction is dependent on useful evidence form forensic work. Forensic reconstruction becomes as good as the Evidence available. Reconstructing particular facts or elements of events without being able to recreate all of them (for different reasons) might give useful information for the investigation and subsequent prosecution of a case. In Africa, evidence gathering for reconstruction of events is highly still lacking. This paper therefore studies evidence based reconstruction as a way of enhancing digital forensics for adequate understanding of events and possible legal efficiency in this technology driven era.

2. RELATED LITERATURE

Buczak and Guven (2017) discovered that network evaluation, machine learning and data mining approaches used to enable reconstruction had a strong association. However, he also observed that network evaluation, machine learning, and data mining technologies for intrusion detection and reconstruction are vulnerable to security risks. He offered various solutions to the network dangers that the two techniques faced. However, his viewpoint is too hazy; he did not precisely identify the link between the two, nor did he offer particular solutions or remedies to the problems.

Chabot et al., (2014) defined a knowledge model for forensic timeline analysis. Several entities, including subject, object, event, and footprint, as well as their relationships, are officially specified initially. All of the aspects of the crime scene are identified this way. After that, a four-operator event reconstruction technique is described. The extraction operators find and extract useful data in footprints from a variety of sources. Subjects, objects, and events are created by the mapping operators and are related with the extracted footprints. The inference operators deduce new information about subjects, objects, and events using the knowledge provided by mapping operators. Finally, the analytical operators assist the investigator in identifying connections between events and highlighting pertinent data in the timeline.

Alrajeh et al., (2017) developed a formal framework for designing forensic-ready systems. The term "forensic ready" refers to the system's ability to assist digital forensic examinations of both known and unknown situations. To this goal, data that might be used as evidence in some instances is saved ahead of time. This formal technique defines the evidence preservation standards, which dictate the retention of the bare minimum of data relevant to a future digital forensic inquiry and reconstruction of events.

Jean-Paul et al., (2021), reviewed the different forensics and anti-forensics methods, tools, techniques, types, and challenges, while also discussing the rise of the anti-anti-forensics as a new forensics protection mechanism against anti-forensics activities. The author presents a fresh current forensics analytical perspective. A basic forensics backdrop was offered, which included the forensics investigation method, chain-of-custody, and the structure of cybercrimes, as well as the classification of digital data and types of digital investigators. The sub-domains of digital forensics were then covered, along with the various investigative forensics tools, methodologies, and approaches. Cyber-forensics issues were also discussed in length. Anti-forensics aspects and techniques were also discussed, as well as counter-forensics detection and prevention techniques. Machine learning techniques were used to improve detection rate and accuracy, while privacy-preserving techniques were used to prevent any evidence alteration, deletion, or modification.

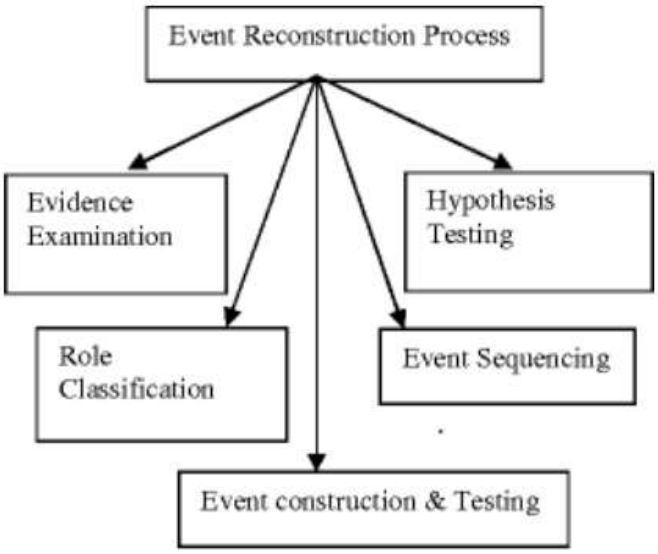

Figure 2.1. Event reconstruction phases
Source: Semantic Scholar

3. RESEARCH GAPS/FINDINGS

Throughout the study there was no research that exclusively detailed evidence based approach reconstruction in Africa or Ghana. Due to the enormous quantity and diversity of data, one of the key issues in digital forensics is reconstructing and analyzing the sequence of events and artifacts to interpret digital evidence. Various ways have been devised to figure it out, according to scientific and technical literature investigations, however the majority of them are unable of treating this issue accurately. The study uncovered forensics approaches, including computer, mobile, network, cloud, digital, malware, and e-mail forensics, as well as anti-forensics strategies and activities which help build evidence for reconstruction purposes.

4. IMPLICATION FOR CYBER SAFETY IN AFRICA

From the findings, the implication of evidence based reconstruction for Cyber Safety in Africa will mean that cyberspace attackers will be discouraged from committing cybercrimes because their steps can be traced using forensics approaches whiles cyberspace users will be encouraged and confident when using cyberspace without the fear of being attacked and not be able to ever find the perpetuators of the crime/attack. This will help reduce the number of cyberattacks in Africa

5. CONCLUSION

Gathering evidence from the system, reconstructing events using the data, and generating court reports are all part of a digital forensic investigation. The outcomes must be verified and repeatable, which involves the use of various methods and models for event reconstruction. Evidence gathered must be able to support the reconstruction in a coherent manner that give adequate account of occurrences.

6. RECOMMENDATION FOR POLICY AND PRACTICES

Digital forensic investigators will be encouraged in Africa if they are trained and are informed of evidence based reconstruction that enhance investigation techniques especially for the police. This will aid in the detection of perpetrators, which will prevent future cybercrime.
Better evidence based reconstruction will help combat cybercrime in Africa, therefore, policies that ensure investment in these areas must come to being. All available tools must be specialized in so that there will be growth and advancement in security.

7. DIRECTION FOR FUTURE WORKS

Further research is needed to ensure improved accuracy and detection rates by applying more evidence based methods in machine-learning-based techniques, as well as a variety of privacy-preserving solutions to prevent any evidence change caused by anti-forensics activities.

REFERENCES

1. Bhandari, Sandeepak & Jusas, Vacius. (2020) An Abstraction Based Approach for Reconstruction of TimeLine in Digital Forensics. Symmetry. 12. 104. 10.3390/sym12010104.
2. Buczak, A. & Guven, E. (2017) A survey of data mining and machine learning methods for cyber security intrusion detection, *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2017.
3. Chabot, Y., Bertaux, A., Nicolle, C., M-Tahar, K., (2014), A complete formalized knowledge representation model for advanced digital forensics timeline analysis. Digital Investigation. 2014; 11 (2): p. 95-105
4. Cyber Security Coalition, (2015) Handling of digital evidence. Cyber Security Incident Management Guide
5. Gaoyu, J, Bo, Z. (2019) ICBDR 2019: Proceedings of the 2019 3rd International Conference on Big Data Research November 2019 Pages 110–113https://doi.org/10.1145/3372454.3372456
6. Jean-Paul, A., Yaacoub, H., N. Noura, O., & Chehab (2021), Digital Forensics vs. Anti-Digital Forensics: Techniques, Limitations and Recommendations
7. Lrajeh, D, Pasquale, L., Nuseibeh, B. (2017) On Evidence Preservation Requirements for Forensic-Ready Systems. Proceedings of 2017 11th Joint Meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering; 2017; Paderborn, Germany
8. Nasereddin, H. (2017) (ARBSI): proposed algorithm association rules based on scanning itemsets, *International Journal of Current Research*, vol. 9, no. 2, pp. 46068–46073, 2017.
9. Pavel, L. & Ahmed, J. (2004). Finite state machine approach to digital event reconstruction. Digital Investigation. 2004; 1 (2): p. 130-149.
10. Routledge, (2004) Introduction, in Cavendish: Evidence Lawcards, 3rd ed., London: Routledge-Cavendish, 2004, pp. 1–8
11. Software Engineering Institute. (2016) Volatile Data Collection . Carnegie Mellon University. https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html
12. Yaacoub, A., Noura, J. P., Hassan, S., Ola, C. A, (2021) Digital Forensics vs. Anti-Digital Forensics: Techniques, Limitations and Recommendations.
13. Yonghwi, K., Weihang, W., Jinho, J., Hyung, L.,K. Perdisci, R. (2021) Cybercrime Scene Reconstruction for Post-mortem Forensic Analysis. Network and Distributed Systems Security (NDSS) Symposium 2021