Computing, Information Systems, Development Informatics & Allied Research Journal
Vol. 15 No. 1, 2024 - www.cisdijournal.net

Trends, Challenges and Opportunities of Engaging Digital Forensics for Cybercrime Investigations

Adams Terence Addey
School of Technology
Graduate Programme in Cyber Security & Digital Forensics
Ghana Institute for Management and Public Administration (GIMPA)
Green-Hills, Accra, Ghana
Email: addey.adams@police.gov.gh
Phone: +233248654959

ABSTRACT

The use of digital forensic tools and techniques has continued to evolve as the security community makes efforts to stay ahead and mitigate cyber crimes. These tools and techniques are assisting cybersecurity experts and law enforcement in identifying fraudsters and protecting data by utilizing techniques such as digital traces left by data processing and storage. This paper identifies the peculiarities of digital forensics as a field of study, explores trends, challenges and opportunities presented by digital forensic tools in investigating cyber crimes. We carried out a systematic literature review of applicable tools and techniques. Our research identified challenges affecting the use of digital forensics in investigating cybercrime, and capture comprehensively the pulse of the domain. Recommendations were made that digital forensics lack a unified formal representation of standardized procedures and knowledge for analyzing and gathering digital artifacts. This inevitably causes incompatibility and conflict within various digital forensics tools. This leads to errors in the interpretation and analysis of digital artifacts due to lack of standardized or formalized procedure for analyzing, preserving, and collecting digital evidence is absent.

Keywords: Cybercrimes, Police, Cyber Security, Challenges, Techniques

CISDI Journal Reference Format
Adams Terrence Addey (2024): Trends, Challenges and Opportunities of Engaging Digital Forensics for Cybercrime Investigations – A Review. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 15 No 1, Pp 1-.8. dx.doi.org/10.22624/AIMS/CISDI/V15N1P1x. Available online at www.isteams.net/cisdijournal

1. INTRODUCTION

Digital forensics (DF) is a relatively new discipline of information technology, according to Jawale (2010), DF has been and continues to be subjected to continuous technical advancements, which has resulted in increasingly distinct and difficult difficulties over time (Jones et al. 2009). For the first time in the 1980s, investigators used DF techniques to recover mistakenly lost data from extensively fragmented Database files, according to (Jawale 2010). Software tools with basic data recovery capabilities were generally available by the 1980s. Dedicated DF investigations were not done until the twenty-first century, according to (Pollitt, 2010).

The importance of preventing, investigating, and prosecuting cybercrime, as well as the rapid progress of DF investigation, had become clear at that time. Network monitoring, database forensics, and mobile device forensics are the three main specializations in DF currently, according to (Jawale et al., 2010).
Cybercriminals get more powerful as new technologies emerge, sophisticated instruments with which to commit crimes, putting increasing expectations on DF investigators to enhance their tools, tactics, and methodology, also wider range of specialty in DF sub-fields is also being developed. One of the most persistent challenges in DF is determining how to handle the expanding volume of digital evidence and cases processed using traditional DF investigation methods.

1.1 Digital Forensics (DF) Disciplines

Many digital forensic professions have emerged in recent years as a result of technical advancements. The digital forensic professionals are described as follows by Stoyanova et al. (2020) and Karie and Venter (2014).

1.1.1 Computer Forensics

It's a typical misnomer for digital forensics, and it refers to the study of digital data from sources like desktop, laptop, and server computers.

- **Software Forensics:** Investigating software to locate evidence is a source of concern.
- **Database Forensics: This** is concerned with the examination of data and metadata stored in a database.
- **Multimedia Forensics:** Images, videos, and audio recordings are used to verify the veracity of the information they convey.
- **Device Forensics:** With a focus on digital evidence collected from a variety of small to very large technologies.
- **IoT Forensics:** Where all evidential origins are more diverse than in device forensics, such as newborn or patient sensor devices, biomaterials in people and animals, in-vehicle infotainment (IVI) systems, traffic signals, and so on.
- **Network Forensics:** This is concerned with the approach of gathering and evaluating network data as well as tracking network traffic in order to determine the frequency of security issues.
- **Cloud Forensics:** This is also regarded as a subclass of network forensics that focuses on the virtualized environment (Zawoad & Hasan, 2013).

2. DIGITAL FORENSIC (DF) INVESTIGATION PROCESS

Several DF investigation models are in existence, however, none of them has developed to a level to be called the industry standard for DF investigation. However, the four essential characteristics described below are typically included in several proposed DF research models:

1. Getting or gathering information,
2. studying or identifying information,
3. Analyzing or assessing information, and
4. Presenting the information.

The process of keeping a copy of digital evidence is known as collection or gathering. (Baryamureeba et al., 2004). Examining is the process of searching for electronic evidence related to a suspected crime systematically and thoroughly. The phase by which an investigator measures and recreates data

fragments in order to make logistical decisions based on the evidence obtained is known as evaluation, (Horsman, 2020). In readiness for evidence entry, the procedure of presentation involves enumerating the findings and defining the conclusions. Given the restrictions of changing technologies, researchers developed models that blended methods and devices as DF examination improved. The DF investigation process can take hundreds of different forms, with each business developing its standards based on the investigation's technical requirements, (Apau & Koranteng, 2019). Due to the extensive scope of cybercrime, On a specific instance scenario, DF investigators will most likely choose the best framework, developing the technique regularly to satisfy case requirements, according to (Selamat and coworkers, 2008).

2.1 Digital Evidence

Digital gadgets play a significant role in the development of digital evidence (Vincze, 2016). Digital evidence can be found in practically every form of crime, and any gadget that carries digital information can be utilized in investigations (Cervantes Mori et al., 2021). Chinedu et al (2021) on the other hand, categorizes offenses into three groups:

a) **Offline Crimes with Digital Evidence**:(Ospina et al., n.d.) They are criminal offences which were perpetrated without the use of digital technology but may leave digital evidence. These traces may be useful in bringing the device's owner to justice.
b) **Cyber-aided crimes**: This form of crime was described by Grobler & Van Vuuren (2010) as "the old type of crimes through digital means." They are common criminal offences made much easier through the use of electronic devices and the internet.
c) **Cybercrimes**: Computer systems are sometimes used to commit crimes against other computer systems, such as denial-of-service attacks.

2.2 Devices that Generate Digital Evidence

Digital data can be obtained on a wide range of digital devices and in a variety of formats. The massive volume of digital data from digital devices can be retrieved, examined, and evaluated and can be presented to digital forensic experts as digital evidence by police agencies. The capability of such gadgets to generate and store digital data necessitates the development of a wide range of processes and tools to deal with the evaluation of large range of digital devices. According to the International Association of Chiefs of Police (IACP) (2015), the following gadgets can establish digital evidence:

1. Still and video cameras (including CCTV),
2. Mobile phones,
3. Desktop computers and laptops,
4. Portable Mobile devices,
5. Game consoles,
6. Extended storage devices (hard drive, thumb drive, optical and magneto-optical media, or data devices with similar functions),
7. Internet of Things devices,
8. Wearables,
9. Unmanned Aerial Systems (drones).

The above list is indeed not definitive, and any other device that performs comparable activities to the ones listed above can likewise store digital evidence.

3. THREATS FACED BY DIGITAL FORENSICS

3.1 Technical Challenges

Despite the fact that various digital forensic experts and researchers have been analyzing and studying numerous known digital forensic issues, it is still necessary to classify these challenges (Lallie, 2020). According to this account, digital forensic systems are vulnerable to technical challenges that jeopardize their integrity. Potential threats that can be addressed using existing operations, protocols, and expertise are referred to as technical challenges. Alghamdi, (2021) recognize that digital forensics necessitates the best combination of ethical behavior and technical abilities.

Encrypting large volumes of data, and incompatibility among various forensic tools are some of the major technical challenges associated with digital forensics (Park et al., 2020). Because of advancements in communication technology, sophisticated encryption products and services are now easily and widely available (Stoyanova et al., 2018). As a result, encryption algorithms and standards are becoming more complex, increasing the time and difficulty of performing cryptanalysis. This method combines encrypted files in order to extract meaningful information. Furthermore, encryption renders electronic data unreadable, allowing criminals to conceal their criminal activities Van Beek et al. (2020).

This can impede the investigation process of a digital forensic officer. It has been discovered that approximately 60% of cases involving some type of encryption go unprocessed because the investigator's ability to extract information from the evidence is significantly limited (Sommer, 2018). As a result, the ease of use, low cost, and widespread availability of encryption tools pose a significant threat to the integrity and credibility of the digital forensics process (Alghamdi, 2021). Aside from encryption, massive amounts of data stored in a variety of applications, such as enterprise resource planning, pose a significant threat to digital forensic operations. The significant increase in data volumes reduces legal systems' and forensic investigators' ability to keep up with digital threats. (Kshetri, 2019).

Similarly, with the advent of cloud computing, much IT-related hardware, such as network switches, racks, and servers, has been replaced with remote-on-demand, virtualized software that is configured based on business requirements. Furthermore, these services and data can be managed and hosted remotely by a third party or the user. As a result, the data and software may be physically stored in multiple geographic locations (Lillis et al., 2016). The distributive nature of data reduces forensic experts' control and visibility over digital forensic artifacts significantly (Kshetri, 2019). Similarly, the cost, complexity, and functionality of digital forensic tools and techniques vary widely. As a result, most digital forensic tools have disparate parts or elements, which makes them incompatible with one another (Park et al., 2020). Furthermore, some forensic tools are incapable of dealing with the ever-increasing storage capacity of target devices.(Dolliver et al., 2017). This means that large targets pose a significant technical challenge to digital forensic operations because they necessitate more complex analysis techniques (Alghamdi, 2021). As a result, it is confirmed that various technical challenges pose a significant threat to the performance and integrity of digital forensic operations.

3.2 Operational Challenges

It is a known fact that digital crimes are intentional in their scope of operation (Houck, 2020). Due to this, digital forensics is exposed to various operational challenges. Among such challenges, incidence

prevention, response, and detection have gained much attention (Chinedu et al., 2021). Traditional IT environments that have on-premises data processing have integrated internal incident management process for ensuring utmost security (Alghamdi, 2021).

This process utilizes intrusion detection systems, log file analysis, and monitoring, in addition to data loss prevention systems that identify and detect data loss, attackers, and intruders. For cloud users, these security incidents can often prove to be challenging. This is because, these security incidents compromise business and personal data and since they are equipped with anti-forensics technology, attackers can steal or destroy potential evidence (Grobler & Van Vuuren, 2010).

Likewise, the lack of standardized procedures and processes in digital forensics alarmingly endangers the evidence extraction and investigation process. It is established that currently, digital forensic models lack standardization that has further increased the complexity of the process. Besides, studies like (Owen & Thomas, 2011) argue that the lack of universal standards makes it quite tough to assess the competency of forensic experts.

The absence of standardized procedures was acceptable when digital forensics was considered a mysterious investigation process that enabled experts to discover hidden pieces of evidence and information that further provided useful insights regarding criminal behaviors (Cole, 2014). However, with the increase in the development of digital technologies, digital forensic investigation is no longer limited to small computer systems rather a virtualized environment that consists of non-standard interfaces and different storage devices.(Cătălin, 2019).

In addition to above-discussed threats, digital forensics is also exposed to forensics readiness problem. Forensic readiness can be understood as the capability of computer networks or computer systems to record data and activities in such a way that it can be perceived as authentic and are sufficient enough for forensics purposes (Scheidt & Adda, 2020). However, the rapid development in cloud computing has forced organizations to dynamically change how they enact, develop, and plan IT strategies. Besides, cloud computing lacks forensic readiness aspect, which further threatens digital forensic operations. Similarly, manual analysis and intervention of physical hard drives is another potential operational challenge that is faced by digital forensics.

Albeit, it is simple and straightforward in a single drive, or a single partition, the process becomes much more complicated when RAID configurations are involved (Cervantes Mori et al., 2021). Also, due to the complex nature of digital forensics, manual inspection of hard drive images can potentially risk the digital artifacts. Likewise, it is believed that forensic analysis should be valid, accurate, complete, and reliable (Sommer, 2011). However, balancing between user privacy and retrieving key digital evidence is a major threat to digital forensics. Due to the increase in the storage capacity, often a small portion of the information is used for investigation and a larger amount of information is discarded (Alghamdi, 2021). This can lead to a breach of the user's privacy, which poses an additional challenge to digital forensic operations. Thus, considering the evidence, it can be affirmed that operational challenges can notably endanger digital forensic analysis.

3.3 Personnel Related Challenges

Personnel related challenges endanger the integrity of digital evidence. Among various personnel-related challenges, lack of well-trained forensic staff is the most prominent one (Rogers & Seigfried,

2004) Despite the overwhelming significance of the digital forensics field because of cyber-crimes, the lack of qualified forensic officers threatens the process of digital forensics (Apau & Koranteng, 2020). The shortage of well-trained forensic investigators is due to the fierce competition in law enforcement as well as high requirements since digital forensics require technically proficient personnel that are certified and trained to deliver scientifically valid evidence (Ludik, 2020). Likewise, it cannot be denied that digital forensics has gained major importance among forensic practitioners, law enforcement agencies, and computer professionals. Unfortunately, the advancement in this field has encouraged an environment that is threatened by semantic disparities (Rogers & Seigfried, 2004).

Another potential personnel-related challenge is a chain of custody. Chain of custody refers to the location log that defines the collection point of the evidence. In digital forensic analysis, it is one of the most crucial issues because it requires physical control of the evidence that is not possible in a digital environment (Stoyanova et al., n.d.). In addition, due to proprietary technology, procedures, and multi-jurisdictional laws, effectively managing the chain of custody is a major challenge that is faced by digital forensics. Hence, it can be established that personnel-related challenges pose a great challenge to traditional forensic operations.

4. DIGITAL INVESTIGATION PROCESS

As stated by Baryamueeba and Tushaba, this is the most sophisticated model we've seen thus far (2004) By adding two phases to IDIP, the EDIP distanced the investigation from the computing equipment and the crime scene, reducing disputes (trackback and dynamite).

4.1 Investigation of Cybercrime Using the Extensive Model

According to Selamat and coworkers (2008), the DF investigation process can take hundreds of different forms, with each organization setting guidelines depending on the investigation's technology requirements. Due to the broad breadth of cybercrime, investigators are more likely to select the optimal a framework that is applied on a specific instance basis, modifying the technique as needed to meet the case's requirements. Awareness refers to raising awareness of the need for an investigation, authorization refers to gaining permission to conduct the DF investigation, and planning refers to the DF investigator arranging the required activities and assessing whether extra authorization is required. Following the search and identification phase, which includes the capture of photographs and evidence objects, comes the collecting stage.

The DF investigator transports the confiscated evidence items to the police station during the transport step throughout the storage step, before properly identifying and archiving them. The processes for discovering and interpreting significant information are covered in the inquiry phase. Considering the evidence items examined during the hypothesis phase, the DF investigator must build her claim regarding what happened. During the presentation step, the digital forensic examiners must offer the hypothesis to someone who is not one of the examiners, then test its validity and sustain it from any opposition or protest during the proof/defense phase. In the final stage, the investigational findings are revealed. This concept is intended to help investigators create rules, processes, and future obligations. Investigators can provide information in real-time or provide examiners with records demonstrating their abilities and experience, which they can refer to as needed.

Data Diversity

According to Anderson and his colleagues (2004), forensic investigators must work with a variety of data kinds, formats, and standards. DF investigators have access to databases, timestamps, program

logs, installation logs, transactions logs, files, excel sheets, configuration files, and a range of other file kinds and formats are among the file types and formats available.

Big Data

The Size of Digital Evidence, according to (Gogolin, 2010). The ever-increasing amount of forensic data has been dubbed "the digital tsunami" by some. Furthermore, the tremendous reduction in the price of storage drives has initiated a new challenge in digital forensics: investigative performance. Efficiency has a direct effect on the DF workflow, according to Leong (2006). Because of the time, it takes to forensically photograph and analyze all of the data in the report, the phenomenal increase in electronic data capacity has resulted in an extended waiting list. Many digital crime laboratories in Michigan have been closed for nearly two years due to delays, according to reports (Gogolin, 2010).

As a direct consequence of the wait times, forensic professionals are under increased pressure from stakeholders to do better, therefore they're resorting to automated "pushbutton forensics" to quickly evaluate enormous volumes of data, according to the report (James, Joshua, & Gladyshev, 2013). According to (Access Data, 2013; Guidance, 2014), FTK and Encase are two examples of digital investigation tools, include features that allow users to do simple and complex investigative tasks. Such approaches will erode the abilities of seasoned investigators over time, forcing forensic experts to limit their work to specific forensic instruments rather than pursuing other avenues, more sophisticated options. Creative solutions and tools are required by DF. As a result, forensic divisions must maintain a mix of push-button and manual forensics to preserve specialists' forensic experience.

4.2 Legal Requirements

According to the DF Examiners, the majority of their time is spent making sure the law, legal processes, and installation environment are all followed (Palmer, 2001; Quick & Choo, 2014). On working with digital evidence, ISO 27037 presents a list of legal concerns to consider. Brezinski and Killalea claim that, the DF investigator must guarantee that the digital evidence is admissible, authentic, complete, dependable, and credible (2002). As a result, completeness is a key factor in determining whether or not the evidence is accepted. True, completeness does not always require that all evidence items must be represented, but it does imply that the entire story, not just one point of view, must be communicated. As a result, any suggested solutions for expediting the DF investigation must also ensure that all legal requirements are met.

4.3 Information Visualization

The method focuses on data analysis and visualizations of abstract data using engaging and customized mapping tools. As a result, practitioners may be able to use information visualization techniques to help them deal with the influx of digital evidence data. When assessing evidence, such procedures can improve efficiency and extract data appearance. Intella is forensic investigators' open-source software that improves data presentation and social mapping. Intella displays data from devices utilizing clusters at multiple levels of abstraction, instead of the typical tree and table-based approach, which may make it easier to discover anomalies. This strategy, according to the organization, can increase staff productivity by reducing investigative costs and time. Intella, in theory, is an online platform that enables users to locate sampling phrases quickly by entering relevant keywords.

5. CONCLUDING REMARKS

In conclusion, apart from the challenges discussed it is undeniable that digital forensics lack a unified

formal representation of standardized procedures and knowledge for analyzing and gathering digital artifacts. This inevitably causes incompatibility and conflict within various digital forensics tools (Grobler & Van Vuuren, 2010). Errors in the interpretation and analysis of digital artifacts occur when the standardized or formalized procedure for analyzing, preserving, and collecting digital evidence is absent.

Likewise, when forensic experts manage a vast amount of data while simultaneously performing forensic investigation, they utilize specialized skills and digital technologies. However, these experts often fail to record their work, which further hampers training and external reviews (Alghamdi, 2021). Past knowledge and experience should be utilized to further train new digital forensic personnel while fostering knowledge sharing among detective communities. Unfortunately, digital forensic officers either fail to record their work or simply do not follow legal practices that further poses a great threat to digital forensic investigation.

BIBLIOGRAPHY :

1. Awadi et al. Alawadhi, J. C. Read, A. Marrington, and V. N. L. Franqueira. Factors influencing digital forensic investigations: Empirical evaluation of 12 years of Dubai police cases. Journal of Digital Forensics, Security and Law, 10(4):7-16, 2015.
2. E. Casey, G. Katz, and J. Lewthwaite. Honing digital forensic processes. Digital Investigation,
3. G. Gogolin. The digital crime tsunami. Digital Investigation, 7(12):3 - 8, 2010.
4. A. Irons and H. S. Lallie. Digital forensics to intelligent forensics. Future Internet, 6(3):584, 7 2014. ISSN: 19995903.
5. Overview of forensics science in Ghana https://police.gov.gh/en/index.php/forensic- science-laboratory-tel/
6. Digital forensics tools and their uses https://resources.infosecinstitute.com/topic/7- best-computer-forensics-tools/
7. Piriform. (2014). Recuva. from http://www.piriform.com/recuva Pollitt, M. “ComputerForensics (1995): an Approach to Evidence in Cyberspace”, (2001, October). Report on digital evidence. In 13th INTERPOL Forensic Science
8. Symposium. Pollitt, M. M. (2007, April). An ad hoc review of digital forensic models. In Systematic Approaches to Digital Forensic Engineering, 2007. SADFE 2007.
9. IEEE. Pollitt, Mark. "A history of Digital Forensics." IFIP International Conference on Digital Forensics.
10. Springer, Berlin, Heidelberg, 2010. Pooe, A. & Labuschagne, L. (2013). Digital Investigation, I I(4), 273-294. DOI DOI: http://dx.doi.org/10.1016/j.diin.2014.09.002 Quinn, P. M. (2002).
11. Saunders et a1., 2003; Robson, 2002; Research Methodology Guidance
12. Almarzooqi, 2016; Johansen & Perjons, 2014. after discussing the many types of research procedures.
13. History of the Ghana service https://police.gov.gh/en/index.php/cyber-crime/ Retrieved 14-April 2014, from http://www.easterniowanewsnow.com/2010/07/l2/child- porn-prosecutionsdel Reinard, J. (1998).

15. Criminal Investigation Department — CID — Ghana Police Service. (n.d.). Retrieved February 6, 2022, from https://police.gov.gh/en/index.php/criminal-investigation- department-cid/
16. Forensic science and the criminal justice system.- a blueprint for change. (n.d.). Retrieved

February 6, 2022, from http://www.parliament.uk/mps-1ords-and- offices/standards-and-interests/register-ot-lords-

17. Hansen, H. A., Andersen, S., Axelsson, S., & Hopland, S. (2017). Case Study: A New Method for Investigating Crimes Against Children. Annual ADFSL Conference on Digital Forensics, Security and Law, c,
18. Horsman, G., Laing, C., & Vickers, P. (2014).AC. https://doi.org/10.1016/j.dss.2014.01.007
19. Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016). Current Challenges and Future Research Areas for Digita Forensic Investigation. Ma y. https://doi.org/10.1314()/RG.2.2.34f›9f›.764f›9NIST to Digital Forensics Experts. Show Us What You Got NIST. (n.d.). Retrieved February 6, 2022, from https://www.nist.gov/news-events/news/2(J2(I/(If›/nist-digital- forensics-experts-show-us-what-You-cot
20. J. Beckmann (Eds.), Springer series in social psychology. Berlin: Springer.
21. Ajzen, I. (1991). The theory of planned behaviour. Organizational Behaviour and Human Decision Processes, 50(2), 179-211.
22. Angst, C. M., Agarwal, R., Sambamurthy, V., & Kelley, K. (2010). Social contagion and information technology diffusion: The adoption of electronic medical records in us hospitals.
23. Management Science, 56(8), 1219-1241. Austin, R. D., Sole, D., & Cotteleer, M. (2003). Harley Davidson motor company: enterprise software selection. Harvard Business School Case Study, 9-600-006.
24. Burns, T., & Stalker, G. M. (1962). The management of innovation. Chicago: Quadrangle Books.
25. Chau, P. Y. K., & Tann, K. Y. (1997). Factors affecting the adoption of open systems: An exploratory study. MIS Quarterly, 21(I), 1-24.
26. Collins, P. D., Hage, J., & Hull, F. M. (1988). Organizational and technological predictors of change in automaticity. Academy of Management Journal, 31(3), 512— 543.
27. Cooper, R. B., & Zmud, R. W. (1990). Information technology implementation research: A technological diffusion approach. Management Science, 36(2), 123-139.
28. Cyert, R. M., & March, J. G. (1963). A behavioural theory of the firm. Englewood Cliffs, NJ: Prentice-Hall. Daft, R. L., & Becker, S. W. (1978). The innovative organization: Innovation adoption in school organizations. New York: Elsevier.
29. Damanpour, F., & Evan, W. M. (1984). Organizational innovation and performance: The problem of “organizational lag”. Administrative Science Quarterly, 29(3), 392W09.
30. Beebe and Clark (2005) Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319—339
31. Schlepphorst, S., & Choo, K. R. (2020). C yber and Digital Forensic Investigations (Vol. 74). http://1ink.sprineer.com/10.1007/978-3-030-47131-6
32. Vincze, E. A. (2016). Challenges in digital forensics. Police Practice and Research, 17(2), 183—194. https://doi.org/1().1tJf›()/15614263.2()15.1128163
33. Walsh, S. 1. (2018). Australian Journal of Forensic Sciences Australasian forensic science summit 201d. the external future context and the case for change. https://doi.org/1().1tJf›()/()()45()618.2()17.1383572
34. National Institute of Standards and Technology (NIST) https://www.nist.gov/digital- evidence

35. 2021 Population and https://catalog.ihsn.org/index.php/catalog/378Housing Census report
37. Arshad, H., Jantan, A. B., & Abiodun, O. I. (2018). Digital Forensics: Review of Issues in

Scientific Validation of Digital Evidence. Journal of Information Processing Systems, Vol.14, No.2, pp. 346-376. https://doi.org/10.3745/HPS.03.0095.

38. Beebe N. (2009). Digital Forensic Research: The Good, the Bad and the Unaddressed. In: Peterson G., & Shenoi S. (Eds.), Advances in Digital Forensics V, IFIP Advances in Information and Communication Technology, vol 306, pp. 17-36. Springer. https://doi.org/10.1007/978-3-642- 04155-6 2.
39. Beebe, N. & Clark, J. (2005). A hierarchical, objectives-based framework for the digital investigations process. Digital Investigation, vol 2(2), pp. 147-167. https://doi.on/10.101 6/j.diin.2005.04.002.
40. Braun, V. & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3:2, pp. 77-101. https://doi.oi‘u/ 10. 1191/1478088706qp063oa.
41. Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., & Khalil, M. (2007). Lessons from applying the systematic literature review process within the software engineering domain. Journal of Systems and Software, 80(4), pp. 571-583. https://doi.org/1().1 tJ16/j.jss.2()()6.tJ7.()()9.
42. Bujra J. (2006). Lost in Translation? The Use of Interpreters in the Fieldwork. In: Desai, V., & Potter, R. B. (Eds.), Doing development research. Sage Publications. ISBN10 1 4129 02843.
43. Casey, E. (2019). The chequered past and risky future of digital forensics. Australian Journalof Forensic Sciences, 51(6), pp. 649 664. https://doi.org/1().1 tJf›()/()()45()61I›.2()1I›.1554()9().
44. Creswell, J., & Poth, C. (2018). Qualitative inquiry and research design: choosing among five approaches (4th ed.). Sage Publications. ISBN 978-1-5063-3020-4.
45. Fink, A., (2019). Conducting research literature reviews, from the Internet to paper (5th ed.). Sage Publications. ISBN 978-1-4833-0103-7.
46. Higgins, J.P.T., Thomas, J., Chandler, J., Cumpston, M., Li, T., Page, M.J., & Welch, V.A. (Eds.). (2019). Cochrane handbook for systematic reviews of interventions (2nd ed.). John Wiley & Sons. ISBN 9781119536611.
47. International Association of Chiefs of Police (IACP) (2015). COMMON ELECTRONIC DEVICES THAT GENERATE DIGITAL EVIDENCE. [Online]. Retrieved June 5, 2022, from https:l/www.iacpcvbercenter.org/officers/cyber-crime- investieations/common-electronicdevices- that-generate-digital-evidence/.
48. International Organization for Standardization (2012). Information technology — Security techniques— Guidelines for identification, collection, acquisition and preservation of digital evidence (ISO/IEC Standard No. 27037:20I2). Retrieved January 6, 2021, from https:llwww.iso.org/standard/44381 .html.
49. Israel, M., & Hay, I. (2006). Research ethics for social scientists: Between ethical conduct and regulatory compliance. Sage Publications. ISBN 13 978 1 4129 0389 9.
50. Karie, N. M., & Venter, H. S. (2014). Toward a General Ontology for Digital Forensic Disciplines. Journal of Forensic Sciences, 59(5), pp. 1231-1241. https://doi.org/1().1111/1556-4tJ29.12511.
51. History of Forensic Science in Ghana-Overview, https://scientect.org/2tJ16/()2/tel/49/
52. Forensic Science International: Synergy journal homepage: https://www.joui niils.elseviei .cont/1or ensic-science- i ntei nat itaniil-syne i y/
53. Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response (NIST SP 800-86; 0 ed., p. NIST SP 800-86). National Institute of Standards and Technology. https://doi.ore/10.6028/NIST.SP.800-86

54. Alghamdi, M. I. (2021). Digital Forensics in Cyber Security—Recent Trends, Threats, and Opportunities. Cybersecurity Threats with New Perspectives. https://doi.org/10.5772/INTECHOPEN.94452
55. Casey, E. (2019). Australian Journal of Forensic Sciences The chequered past and risky future of digital forensics The chequered past and risky future of digital forensics. https://doi.org/10.1080/00450618.2018.1554090
56. Cătălin, A. (2019). Digital Forensics – A Literature Review. The Annals of "Dunarea de Jos" University of Galati. Fascicle III, Electrotechnics, Electronics, Automatic Control and Informatics, 42(1), 23–27. https://doi.org/10.35219/eeaci.2019.1.05
57. Cervantes Mori, M. D., Kävrestad, J., & Nohlberg, M. (2021). Success factors and challenges in digital forensics for law enforcement in Sweden. CEUR Workshop Proceedings, 3016, 100–116.
58. Chinedu, P. U., Nwankwo, W., Masajuwa, F. U., & Imoisi, S. (2021). Cybercrime Detection and Prevention Efforts in the Last Decade: An Overview of the Possibilities of Machine Learning Models. Review of International Geographical Education Online, 11(7), 956–974. https://doi.org/10.48047/RIGEO.11.07.92
59. Cole, S. A. (2014). History of Forensic Science in Policing. Encyclopedia of Criminology and Criminal Justice, February 2016, 2153–2158. https://doi.org/10.1007/978-1-4614-5690-2_462
60. Cybercrime_Module_4_image_3.PNG (536×180). (n.d.). Retrieved July 23, 2022, from https://www.unodc.org/images/e4j/Cybercrime/Cybercrime_Module_4_image_3.PNG
61. Dolliver, D. S., Collins, C., & Sams, B. (2017). Hybrid approaches to digital forensic investigations: A comparative analysis in an institutional context. Digital Investigation, 23, 124–137. https://doi.org/10.1016/j.diin.2017.10.005
62. Forensic Science Laboratory – FSL – Ghana Police Service. (n.d.). Retrieved August 17, 2021, from https://police.gov.gh/en/index.php/forensic-science-laboratory-fsl/
63. Grobler, M., & Van Vuuren, J. J. (2010). Broadband broadens scope for cyber crime in Africa. Proceedings of the 2010 Information Security for South Africa Conference, ISSA 2010. https://doi.org/10.1109/ISSA.2010.5588287
64. Gyau, W. O. (2020). THE IMPACT OF DIGITAL FORENSICS ON CYBERCRIME IN GHANA THESIS B.Sc. Management Information Systems.
65. Horsman, G. (2020). ACPO principles for digital evidence: Time for an update? Forensic Science International: Reports, 2, 100076. https://doi.org/10.1016/j.fsir.2020.100076
66. Houck, M. M. (2020). Backlogs are a dynamic system, not a warehousing problem. Forensic Science International: Synergy, 2, 317–324. https://doi.org/10.1016/j.fsisyn.2020.10.003
67. Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. Journal of Global Information Technology Management, 22(2), 77–81. https://doi.org/10.1080/1097198X.2019.1603527
68. Lallie, H. S. (2012). An overview of the digital forensic investigation infrastructure of India. Digital Investigation, 9(1), 3–7. https://doi.org/10.1016/j.diin.2012.02.002
69. Lallie, H. S. (2020). Dashcam forensics: A preliminary analysis of 7 dashcam devices. Forensic Science International: Digital Investigation, 33. https://doi.org/10.1016/j.fsidi.2020.200910
70. Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016). Current Challenges and Future Research Areas for Digital Forensic Investigation. May. https://doi.org/10.13140/RG.2.2.34898.76489
71. Ludik, P. S. (2020). Interpol review papers special edition preface. Forensic Science International: Synergy, 2, 351. https://doi.org/10.1016/j.fsisyn.2020.01.006

72. Ospina, M., Harstall, C., Dennett, L., & Institute of Health Economics. (n.d.). Sexual exploitation of children and youth over the Internet : information paper.
73. Owen, P., & Thomas, P. (2011). An analysis of digital forensic examinations: Mobile devices versus hard disk drives utilising ACPO & NIST guidelines. Digital Investigation, 8(2), 135–140. https://doi.org/10.1016/j.diin.2011.03.002
74. Park, M., Yi, O., & Kim, J. (2020). A methodology for the decryption of encrypted smartphone backup data on android platform: A case study on the latest samsung smartphone backup system. Forensic Science International: Digital Investigation, 35, 301026. https://doi.org/10.1016/J.FSIDI.2020.301026
75. Prayudi, Y., & Sn, A. (2015). Digital Chain of Custody: State of The Art. International Journal of Computer Applications, 114, 975–8887. https://doi.org/10.5120/19971-1856
76. Rogers, M. K., & Seigfried, K. (2004). The future of computer forensics: a needs analysis survey. Computers & Security, 23(1), 12–16. https://doi.org/10.1016/J.COSE.2004.01.003
77. Scheidt, N., & Adda, M. (2020). Framework of confidence values during digital forensic investigation processes. WSEAS Transactions on Systems and Control, 15, 228–234. https://doi.org/10.37394/23203.2020.15.24
78. Schlepphorst, S., & Choo, K. R. (2020). Cyber and Digital Forensic Investigations (Vol. 74). http://link.springer.com/10.1007/978-3-030-47131-6
79. Sommer, P. (2011). Certification, registration and assessment of digital forensic experts: The UK experience. Digital Investigation, 8(2), 98–105. https://doi.org/10.1016/j.diin.2011.06.001
80. Sommer, P. (2018). Accrediting digital forensics: What are the choices? Digital Investigation, 25, 116–120. https://doi.org/10.1016/j.diin.2018.04.004
81. Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (n.d.). A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, 22(2). https://doi.org/10.1109/COMST.2019.2962586
82. Vincze, E. A. (2016). Challenges in digital forensics. Police Practice and Research, 17(2), 183–194. https://doi.org/10.1080/15614263.2015.1128163