BOOK CHAPTER | *"Chasing Shadows"*

Libforensics For Developing Digital Forensics Applications.

James Hebidzi Senanu
Digital Forensics & Cyber Security Graduate Programme
Department Of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mails: james.senanu@st.gimpa.edu.gh/senasonlove@gmail.com
Phone: +233242837723

ABSTRACT

The evolution of computers, increase in cybercrime and the demand by law requirements for the production of admissible forensic reports require the application of digital/computer technologies and require the development of a methodology to systematically search digital devices for significant evidence. Cyber and computer fraud are growing by the passing of the day with less than two percent of the reported cases resulting in confidence leading to securing justice and or convictions. This study explores the digital forensic applications and ease of integration of the existing forensic applications. It was the view of the researcher that there exists a gap of monolithic in forensic applications and the cyber universe. One requires different applications to conduct a forensic investigation into a crime revolving around different digital universes. The study proposed research into the development of a single enterprise digital forensic application capable of examining all aspects of the universe regardless and producing an admissible report in the court of law

Keywords: Forensic, Cybercrime, Monolithic, Digital universe, Cyberspace, Cyber ecosystem

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

Citation: James Hebidzi Senanu (2022): Libforensics For Developing Digital Forensics Applications. Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 335-338
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P53

1. INTRODUCTION

The act and process of establishing evidence, cause of action and proof of a crime in the space of computers or digital artifacts is kwon or termed digital forensics. Digital forensics is a specialized area of discipline, the practice relies on technology, scientific tools, and systems. The critical component of digital forensics is forensic application. Forensic applications are digital analytic tools used to collect, analyze, interpret, document, and produce admissible evidence in a court of law. Sriram R., 2014 [1] states that the subject – of digital forensic spans the acquisition, examination, analysis, documentation, and presentation of digital evidence in a court of law.

This paper seeks to peruse existing literature on digital forensic applications, challenges and gaps identified, make projections into the future of the cybercrime landscape, and forensic applications and provide useful guidelines for developers to improve the consolidation of forensic applications. The heterogeneous nature of digital evidence poses a lot of challenges to forensic examiners

1.1 Background to the study

The ever-increasing innovation in technology and the adoption and application of IoTs to our daily life and business activities opened the door to cyber threats and attacks. Law enforcement and criminal justice regimes, child pornography, cyberwarfare, Man-in-the-Middle (MitM) attacks, malware attacks, denial-of-service (DOS) attacks, SQL Injections, Cross-scripting, and many other cyberattack strategies have become critical to individuals, governments, businesses, and the world at large. The crime rate in the cyberspace stood at 4.7 million in 2020, according to embroker.com, 2022, cybercrime costs the global economy USD 3.3 million in the year 2015 and it is estimated to cost over USD 10.5 trillion to the global economy by 2025, across the cyber spectrum, https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025 [2].

Crimes committed in cyberspace, in most cases are left untended and the perpetrators are left off the hook due to a lack of evidence to establish the facts relating to the crime. The international community and the global e-commerce have become vulnerable to cyberattacks in recent times and are expected to increase in the coming years due to the vulnerabilities and appetite for crime, and the capacity to execute the same. Investigation into computers and their related crimes began in the late 1970s in relation to the requirement of law enforcement. In barely 45 years, the subject/science has seen a tremendous hike due to an increase in cybercrime and related digital crimes.

2. RELATED LITERATURE

Salamh, F.E., Mirza, M.M. et al 2021 [3], in their work identified: the identification, preservation, examination, documentation, and reporting of evidence; source of evidence, and multiple components that operate in the unmanned area vehicles (UAVs; discovery of personally identifiable information, test and evaluation of currently available forensic software tools, data storage mechanism and evidence structure as some of the several challenges caused with UAV applications eg. Phantom 4 and Matrice 210), three-dimensional (3D) visualization software. Gyamfi, N.K., Bensah, L.E. et al [4], concluded that the identification of the location of the cybercrime offenders remains a major problem in Ghana and proposed the law enforcement agencies be empowered with the requisite tools which include digital forensic applications to get the locations of the perpetrators.

According to Prasanthi, B.V., 2016 [5], the investigation of material on digital media and networks is one of these actions. Cyber Forensic Investigation includes the Capture & Analysis of digital data either to prove or disprove whether the internet related theft has been committed or not. Earlier Computer are used only for storing large volumes of data & perform many operations on it, but nowadays it has expanded & occupied a prior role in Crime Investigation. To solve these cyber-related problems, the selection & usage of forensic tools is very important. In the face of rapid technological advancements, we are increasingly confronted with a diverse

set of digital evidence and being able to identify a particular tool for conducting a specific analysis is an essential task, Raghavan, S. and Raghavan, S.V., 2013 [6].
Raghavan, S., 2014 [7], in his article – A Framework for Identifying Associations in Digital Evidence Using Metadata identified the growing volumes of digital evidence; and the technological diversity in storage of data in different file formats and representations. Education in the digital forensic eco-system was considered a challenge or an opportunity to improve the study and development of forensic application in the area of virtualization technology which can be used to create realistic learning environments for digital forensics that reduce cost and space requirements while saving students and instructors time cost, Hay, B., 2010 [8].

3. RESEARCH GAPS/FINDINGS

The gap in the findings of existing digital forensic analytic tools has been the monolithic nature of the computer universe requiring different analytic results which means that a single digital forensic application cannot be used to extract, analyze, document and report on all the cyber forensic universe. The Integration and or inter-operability of digital forensic applications with each other due to their specialized nature remains a challenge for developers in the domain.

4. IMPLICATIONS FOR ONLINE SAFETY IN AFRICA

The implications of Africa's online safety in the context of digital forensic analytic tools can be viewed in soo many ways including the complexity of the cybercrime universe, monolithic forensic tools, and more especially lack of regulation in our cyber economic space relative to information technology. With the advent of cloud computing, distributed databases management systems (DDBMS), IoTs, mobile applications, and telecommunications with the hosts stationed offshore poses a lot of challenges and have implication for African's online safety and cyber integrity due to access to data for forensic and analysis, documentation and report and submission for prosecution.

5. CONCLUSION

The gap of disjointed forensic application for the various digital forensics coupled with the widening scope of cybercrime and the legal regime for amicability of findings of forensic outcomes requires a holistic development of an enterprise digital forensic application to encompass all the monolithic aspects of the digital forensic universe, incorporate legal requirements into the development of future forensic applications.

6. RECOMMENDATION FOR POLICY AND PRACTICES

Regulation from law-making bodies must take into account the monolithic nature of the digital forensic universe in formulating laws to adequately capture all aspects that the criminals do not escape justice due to inadequate laws to aid in the evidence gathering for successful prosecution. The law enforcement agencies, and justice delivery systems – local and internal must be abreast with the changing trends in the cybercrime landscape, and the diverse scope of the forensic universe in enforcing the law and delivering justice. In the same vein, the digital forensic space is an evolving and fast-changing endeavor hence constant research and learning into the deep space of the digital forensic ecology is required from practitioners.

7. DIRECTION FOR FUTURE WORKS

Research into the possibility of integration of all the monolithic digital forensic applications into a simple enterprise digital forensic application building on the available or existing applications. Draw inspiration and insight from the existing works of groups like the Computer Analysis and Response Team (CART), the Scientific Working Group on Digital Evidence (SWGDE), the Technical Working Group on Digital Evidence (TWGDE), and the National Institute of Justice (NIJ) have since been formed in order to discuss the computer forensic science as a discipline including the need for a standardized approach to examinations.

REFERENCES

1. Salamh, F.E., Mirza, M.M. and Karabiyik, U., 2021. UAV Forensic Analysis and Software Tools
2. https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
3. Assessment: DJI Phantom 4 and Matrice 210 as Case Studies. *Electronics*, *10*(6), p.733.
4. Gyamfi, N.K., Bensah, L.E., Nyamadi, M. And Aggrey, R., Instrument And Technology For Computer Forensic: Research In Ghana
5. Prasanthi, B.V., 2016. Cyber forensic tools: a review. *International Journal of Engineering Trends and Technology (IJETT)*, *41*(5), pp.266-271.
6. Raghavan, S. and Raghavan, S.V., 2013, November. A study of forensic & analysis tools. In *2013 8th International Workshop on Systematic Approaches to Digital Forensics Engineering (SADFE)* (pp. 1-5). IEEE.
7. Raghavan, S., 2014. *A framework for identifying associations in digital evidence using metadata* (Doctoral dissertation, Queensland University of Technology).
8. Hay, B., 2010, January. Applications of virtualization to digital forensics education. In *2010 43rd Hawaii International Conference on System Sciences* (pp. 1-7). IEEE.