BOOK CHAPTER | *"Beyond Mobile Signals"*

Current and Future Trends In Mobile Device Forensics

Godwin Anyomi
Digital Forensics & Cyber Security Graduate Programme
Department Of Information Systems And Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: anyocot2005@yahoo.com
Phone: +233268906000

ABSTRACT

The contemporary nature of Mobile Devices has brought about evolution process making computational algorithm and networking capabilities to keep up to pace with its constantly growing workload requirements in it usage. This has allowed devices such as smartphones, tablets, and Personal Digital Assistants (PDAs) to perform increasingly complex activities making it more efficient enough to replace the traditional options like desktop computers and notebooks. However, due to their portability and size, these devices are more prone to theft, to become compromised, or to be exploited for attacks and other malicious activity. The need for investigation of the aforementioned incidents resulted in the creation of the Mobile Forensics (MF) discipline. MF, a sub-domain of digital forensics, is specialized in extracting and processing evidence from mobile devices in such a way that attacking entities and actions are identified and traced. Apart from the MF being used for extraction and processing evidence from mobile devices, the MF has recently expanded its scope to encompass the organized and advanced evidence representation and analysis of future malicious entity behavior. The activity of mobile device in crime also falls under the classification of cybercrime as sophisticated devices such as smartphones can be used by hackers on the move. Nonetheless, data acquisition still remains its focus. While the field is under continuous research activity, new concepts such as the involvement of Cloud Computing in the MF ecosystem and the evolution of enterprise mobile solutions – particularly Mobile Device Management (MDM) and Bring Your Own Device (BYOD) – bring new opportunities and issues to the discipline. The current paper presents the research conducted with the MF ecosystem during the last 7 years (Konstantia Barmpatsalou, Tiago Cruz, Edmundo Monteiro, and Paulo Simoes. 2018. Current and Future Trends in Mobile Device Forensics), identifies the gaps, and highlights the impact or implication in different jurisdiction. There is a need to have well defined research programmes to constantly search into the behaviors and flaws of institution on cyber safety and challenges that behalf governance on decision making.

Keywords: Mobile Forensics, Cybersecurity, Device Management, smartphones, Politics, Trust

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

Citation: Godwin Anyomi (2022): Current and Future Trends In Mobile Device Forensics
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 215-220
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P35

1. INTRODUCTION

Criminal activities has gone beyond the traditional way of theft, to digital and to the little less considered medium to be used as a breeding ground of these activities, which the activist having in mind not to be caught due to the gadget being used. The Mobile device as a medium for committing crime, has made then traditional challenge of committing crimes easier in terms of space, time and opportunity to commit the crimes very high, since what is needed is having a performing mobile device to have inter device connection or internet accessibility.

The acquisition of data from the Mobile Device that is used to commit a crime became a challenge since most of these handheld computers can be damaged by the perpetuators and makes it difficult for crime investigators to even mimic the act in order to reproduce the action. In such situations, made it now necessary to have a device or system beyond normal human reasoning to be able to put out crime facts through vigorous data exposition by means of built machine language program to be able to interpret data and compare fact findings from images, text, and video and voice data. Over the years, scientist through research have established methods and processes to extract evidence data from mobile devices in a forensically sound manner (Barmpatsalou et al., 2013; Reedy, 2020).

The use of digital forensics to ascertain mobile device crime through proper data acquisition and its representation will help both government and Telco services to standardized, that is, Telco services with profit orientation to operate standardization with the agreed legal frame work of the state for both parties.

1.1 Background of the study

The background of the current state-of-the-art in Mobile Forensic (MF) in more developed countries has greatly impacted the effectiveness of mobile forensic techniques. The concept of this study is to observe current methodology and possible an advance standardized data acquisition through legally agreed process between a state and the operators or manufactures of the mobile device, since the state actually needs the Telco service that also has impact on the national economy since it has become one of the fastest growing business tools in our daily lives, especially when most transaction entities are done through digital means as the world has become a global centre for doing business that wouldn't require physical movement.

2. RELATED LITERATURE

The use of advanced technology to aid in mobile device forensics has been a concern to both developed and developing countries. The use of Mobile Device has cut across all sphere of profession as it can be used in activities such as voice and video, text and imagery. The ability to retrieve data through complex scientific methods from dead or compromised phones, mimicking to system to reconstruct or replay the activities by recreating of the policies. The methodology approach to investigate crime committed through Mobile Device has evolved due to the new trend in Mobile crimes that seems to outage the traditional or the supposed new of investigation processes. Due to several factors, the forensics acquisition method landscape is constantly expanding towards new directions and changing overtime. The increased in live forensic techniques is such an example, as they provide a way to overcome the limitations of post-mortem forensics, enabling the acquisition of volatile elements. The use of modern services such as Cloud services in Mobile Device has also introduce another level of forensic perspective.

As much as Mobile devices has similar functionalities, they cannot be handled during investigation the same way. There are differences in terms of hardware, software, power consumption and overall mobility makes them unsuitable for classification under computers. The differences in these functionalities helped in the formulation of the Mobile Forensic (MF) to incorporate the criminal investigation of different types of mobile devices. The methods that is involved in Mobile device forensic data acquisition mainly includes, Post-Mortem Forensics, Live Forensics and Non-intrusive forensics. The inability of this acquisition methods occurs if it is unable to perform most difficult task such as bitwise memory image or part of file system extraction fails with respect to the rules of forensic soundness (Vomel 2013), the rest of the extraction procedure cannot be completed.

3. RESEARCH GAPS/FINDINGS

The introduction of smartphones and other android base operating systems has made some of the used methodology becoming a challenge since such mini devices turn to have high processing storage from a complicated technology. As much as there are equally high level investigation tools, there seems to be a challenge when a data integrity is tempered making it difficult for some of the higher scientific tools find it difficult to reproduce data representation either through voice and video, text etc. The research couldn't focus on the technology platform standardization globally, as there seems to be different adaptation to mobile device base on each jurisdiction and once such device is relocated, it is difficult for that jurisdiction to identify the complexity of the technology used making it difficult to acquire data when that device is involve in any crime and even if they do, it takes more time and resource or it is left without investigation completed.

4. CONCLUSION

The subject of Mobile Device Forensics is beyond borders that will require a corporate effort across all jurisdiction. The current technology diversity clearly shows it is difficult for mobile forensic to see it success as having fore advantage through data acquisition. The issue of cybercrime is constantly a threat to safety and trust in both governance and business

5. IMPLICATIONS OF CYBER SAFETY IN AFRICA

The issue of cyber safety has become a thing of functional security but no more of displaying beauty of ego as in what one possess. Most developed world have/or are still beefing up cybersecurity measures through strict rules in order to tackle the increasing threat posed by cyber-attacks as well as to take advantage of the opportunities of the new digital age such as Cybersecurity Act which was adopted by the EU council on April 2019, which introduces a system of EU-wide certification schemes (https://www.consilium.europa.eu/en/policies/cybersecurity) .The establishment of properly instituted commissions such The European Cybersecurity Organisation (ECSO) to serve as a counterpart in a contractual public-private partnership. In view of this, the majority of its members belong to either the cybersecurity industry or to research and academic institutions in the field,

Through The Digital Europe programme for cybersecurity, which is responsible for having an ambitious programme plan within a particular period or scope into cybersecurity capacity increment and the wide deployment of cybersecurity infrastructures and tools across the EU for public administrations, businesses and individuals, as most of these institutions are becoming increasingly dependent on digital technologies to run their core business.

Fig 1: Most Cyber Dependent Sectors
Source: Consilium.europa.eu- European Union

Addressing same for Africa as a continent, having organization bodies such as Africa Union (AU), Economic Community of West African States (ECOWAS), there is no continental policy that bound each member state or commission states to have strict laws about internet security as we are equally involved in sectors such as the Health, Transport, Energy and Finance that are equally exposed to cybercrime. As one of the fastest developing areas globally, having most business striving on internet usage, the failure to address cybercrime issue becomes failure to having serene ecosystem of dwelling for all level of societal strata. Many Africa countries face enormous challenges having sufficient laws to prevent cybercrime since it is very expensive and these countries most solely relies on donor countries for development and hence finds it difficult to even improve or have in place current security measures from the outdated or weaker ones in place (Symantec report: https://docs.broadcom.com/doc/cyber-security-trends-report-africa-interactive-en).

The cyber safety laws not in place turns to make perpetuators have crimes committed without any trace or complete data for legal prosecution and this turns to impact business growth as it turns to put fear among both businesses and individuals to engage in digital transactions and it has hindered growth as people prefer human mobility than doing things online for fast response or result. From the Symantec report, out of 29 African countries only nine (9) have active data protection laws and this hinders continental growth as one cannot trade or do business with countries that do not have strong cybersecurity law in place and this is known to cyber perpetuators such as hackers, fraudsters, terrorist taking advantage of the situation (https://www.itnewsafrica.com/2020/10/the-state-of-cybersecurity-in-africa). As quoted by the Former International Telecommunications Union (ITU) Secretary-General, Hamadoun Toure, "At the moment, cybercriminals see Africa as a safe haven to operate illegally with impunity" (https://www.policycenter.ma/opinion/misunderstood-world-cybersecurity-africa)

6. RECOMMENDATION FOR POLICY AND PRACTICES

Crime through mobile device can be committed anywhere not necessarily being at the location physically. It is a global fight and would need to have a unique standardized policy in terms of mobile device manufacturing and also agreed legal operation standardization between the state and the Telco service, since the Telco plays key role in crime investigation. On the part of Africa countries, there is a need to create a viable risk plan, followed by the correct laws and cybersecurity policies, as well as proper recovery plan in times of surging situations. There should be a proper institutions in place that will be responsible for monitoring and tracking current trend of cyber theft and have a programme to counter as done by the, The Digital programme for cybersecurity by the Europe Councils since it is skilled intensive and this will turn into a cyber-resilience strategy after being able to fetch out their operational activities.

7. DIRECTION FOR FUTURE WORKS

Crimes are committed everywhere in the world but the only common thing is the device and telco system used but the human geographical approach to these crimes differs. It will be best if the global technology institution through state legality have knowledge shared to assist on the people reasoning, which will indirectly translate in finding a good methodology and approach in curb this crimes. African countries should rather go for infrastructure development in cybersecurity from donor countries, that is, they building and training than handing over the donated funds to government to do it themselves, as this translating into what it is meant for will be difficult to achieve.

REFERENCES

1. Konstantia Barmpatsalou, Tiago Cruz, Edmundo Monteiro, and Paulo Simoes. 2018. Current and Future Trends in Mobile Device Forensics.
2. Eoghan Casey. 2013. Smartphone forensics and mobile malware analysis. Retrieved February 4, 2015, from http://www.caseite.com/content/smartphone-forensics-and-malware-analysis.
3. Barmpatsalou et al., 2013.
4. Vomel, 2013.
5. https://www.itnewsafrica.com/2020/10/the-state-of-cybersecurity-in-africa
6. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies
7. https://www.consilium.europa.eu/en/policies/cybersecurity
8. https://docs.broadcom.com/doc/cyber-security-trends-report-africa-interactive-en
9. https://www.policycenter.ma/opinion/misunderstood-world-cybersecurity-africa
10. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies).