BOOK CHAPTER | *"Catching The Thief – What Works Best"*

Mobile Device's Digital Forensic Process Model

Bismark Boateng
Digital Forensics & Cyber Security Graduate Programme
Department Of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: bismark.boateng@st.gimpa.edu.gh
Phone: +233244637788

ABSTRACT

The primary goal is to compare various digital forensics process models, particularly mobile devices. One must conduct investigations forensically to prosecute digital offenders, with the resulting evidence acknowledged in a court of law. Digital forensic process models outline the necessary procedures that one must follow to ensure a successful enquiry.

Keywords: Mobile Devices, Digital Devices, Digital Evidence and Smartphone

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

Citation: Bismark Boateng (2022): Mobile Device's Digital Forensic Process Model
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 267-272
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P43

1. INTRODUCTION

Modern-age businesses rely heavily on digital devices, and they are increasingly turning to mobile devices like PDAs, smartphones, and tablets to run and improve their operations. Such organizations rely on digital devices to handle, store, and restore data. Mobile devices acquire and distribute a vast amount of processed information. Due to advancements in semiconductor technologies and computational power, mobile gadgets are becoming more functional despite their small size that can fit in a pocket. Cell phones are best suited for fact-finding with their fast hardware and software changes.

1.1 Background to the Study

It is essential to understand the basic operation of cellular networks and the locations of any potential evidence. A cellular network is made up of individual cells. Smartphones are mobile phones that run on a mobile operating system and have more advanced computer and communication capabilities, such as wireless, Bluetooth, and AirDrop. Users make and receive phone calls, browse the Internet, chat, send and receive text and multimedia messages, make video calls, record video calls, and view and edit PDF, Excel, and PowerPoint files using these modern phones. Because of the vast activities of mobile devices, they have become vulnerable to crime omissions and thus very important in evidence proving before the law court.

As a result, forensic investigators discovered that mobile devices had become a potential source of digital evidence in criminal investigations, which can be crucial in capturing key information to charge a suspect who compromises a digital device. This study aims to provide an overview of digital forensic investigation process models, particularly for mobile devices, to highlight the need for the digital forensic community to agree with the pursuit of an identical fundamental approach that is adaptable to new emerging technologies and device types.

2. LITERATURE REVIEW

Digital evidence and its characteristics: According to the Scientific Working Group on Digital Evidence (SWGDE), "digital evidence" is "information of probative value that is stored or transmitted in the binary form". Based on this definition, digital evidence includes evidence on any digital device such as portable media players, digital cameras, or telecommunication devices. It is not merely limited to those found on computers. Furthermore, digital evidence has been expanded to include any crime where digital evidence can be found and used as proof in a court of law; it is no longer limited to traditional computer crimes such as hacking and intrusion (Ghosh, 2004). Digital evidence covers digital data that confirms a crime or provides a link between a crime and its victim or between a crime and its executor. In general, digital evidence is a sequence of binary digit numbers on transmission information files stored on the electronic device.

The digital evidence file formats include digital images, text, audio, video, etc. (SWGDE, 2006). The International Organization on Computer Evidence (IOCE) (2002) defines digital evidence as "any information in digital form with an appropriate attestation or liberating value or value of reasonable doubt, and it is stored or transmitted in digital form." Digital evidence may be copied in infinite variations, easily modified. It cannot be understood directly without a technical process. Original resources of such evidence are challenging as well. There are five properties the evidence must have to be helpful: admissibility, authenticity, completeness, reliability, and believability. Missed, dialed, and received calls; SMS; MMs; phonebook contacts; calendars; photos, videos, and notes are all examples of digital evidence from a Smartphone.

As smartphones have internet connection capability, they may contain web browser history. The NIST categorization of smartphone digital evidence class Digital evidence Memory card for smartphones: device ID number, date and language settings, address book, pictures, email, browser history, SMS, media SIM card PIN code, PUK code, IMEI, IMSI Deleted videos, photos, files emails, social networking contacts, messages, and vocational information. Digital evidence of a mobile device can be retrieved from the SIM (Subscriber Identity Modules) card, mobile internal flash memory, or SD (Secure Digital) card. The National Institute of Standards and Technology (NIST) divides digital evidence of smartphones into three parts based on their storage location: SIM card, smartphone memory, and SD card memory, as shown in Table 1 (Lin et al., 2011). In mobile device forensics, evidence is divided into several categories based on the type of mobile device and the services it provides to the user (Spalevicet al., 2012). The classes are as follows: User ID is utilized by network providers for mobile phones as the user's authentication tool and verification of the types of services available for users.

An international number identifies mobile devices identify mobile devices (IMEI). The SIM card contains:

- An "international number for user identification" (IMSI) is used for system registration.
- A secret code for verification.
- Other information.

IMEI and IMSI numbers are independent, which provides users mobility. A SIM card can be protected from unauthorized access by a personal identification number, PIN, or password. The diaries of mobile devices often contain timely-arranged lists of incoming, missed, replied, and selected numbers, GPS information, connection moments on appropriate network cells, and moments of connection termination with network cells. This information can lead to an exact user location at a specific moment. Contacts, which may contain photos, email addresses, physical addresses, alternative phone numbers, and other helpful information on individuals, can be considered a list of potential witnesses, victims, or accomplices. Text messages contain segments of evidence and time indicators, which are very valuable in an investigation. Modern forensic methods allow the reconstruction and tracing of damaged or deleted messages. The user's calendar can indicate the user's movement, commitments, or individuals they have contacted. Electronic mail provides information on the internet communication of the suspect. Instant messages are exchanged in real-time and may contain complete conversations and time indicators.

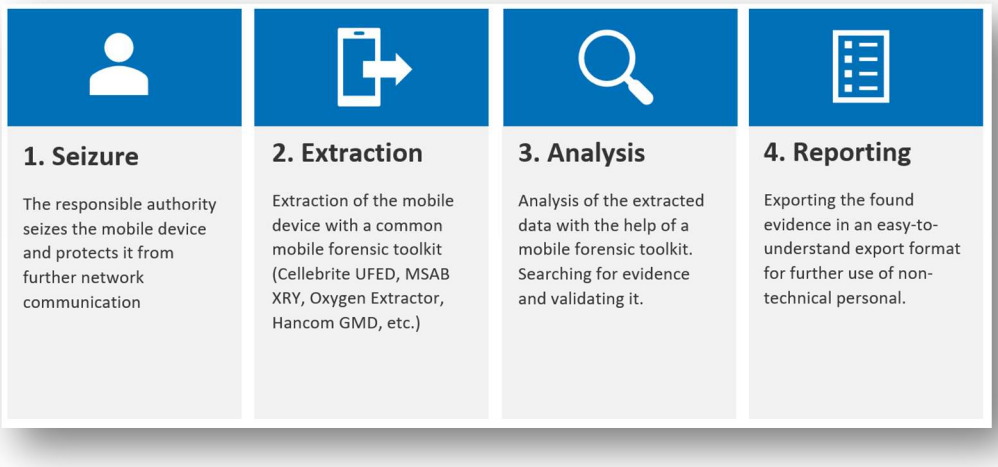

Figure 1 is the typical mobile device investigation process
Source : https://www.t3k.ai/allgemein/10-challenges-in-mobile-forensics/

3. RESEARCH GAPS/FINDINGS

There are a variety of digital forensic process models developed by various organizations around the world. Still, there is no agreement among forensic investigation and legislative delegation on which procedures to follow, particularly with mobile devices that use cutting-edge technology. Other issues peculiar to mobile forensics include data deleting or resetting by accident (intentional wiping or resetting by a suspect, even from a remote location). Investigators must comprehend and navigate various hardware and software systems and devices.

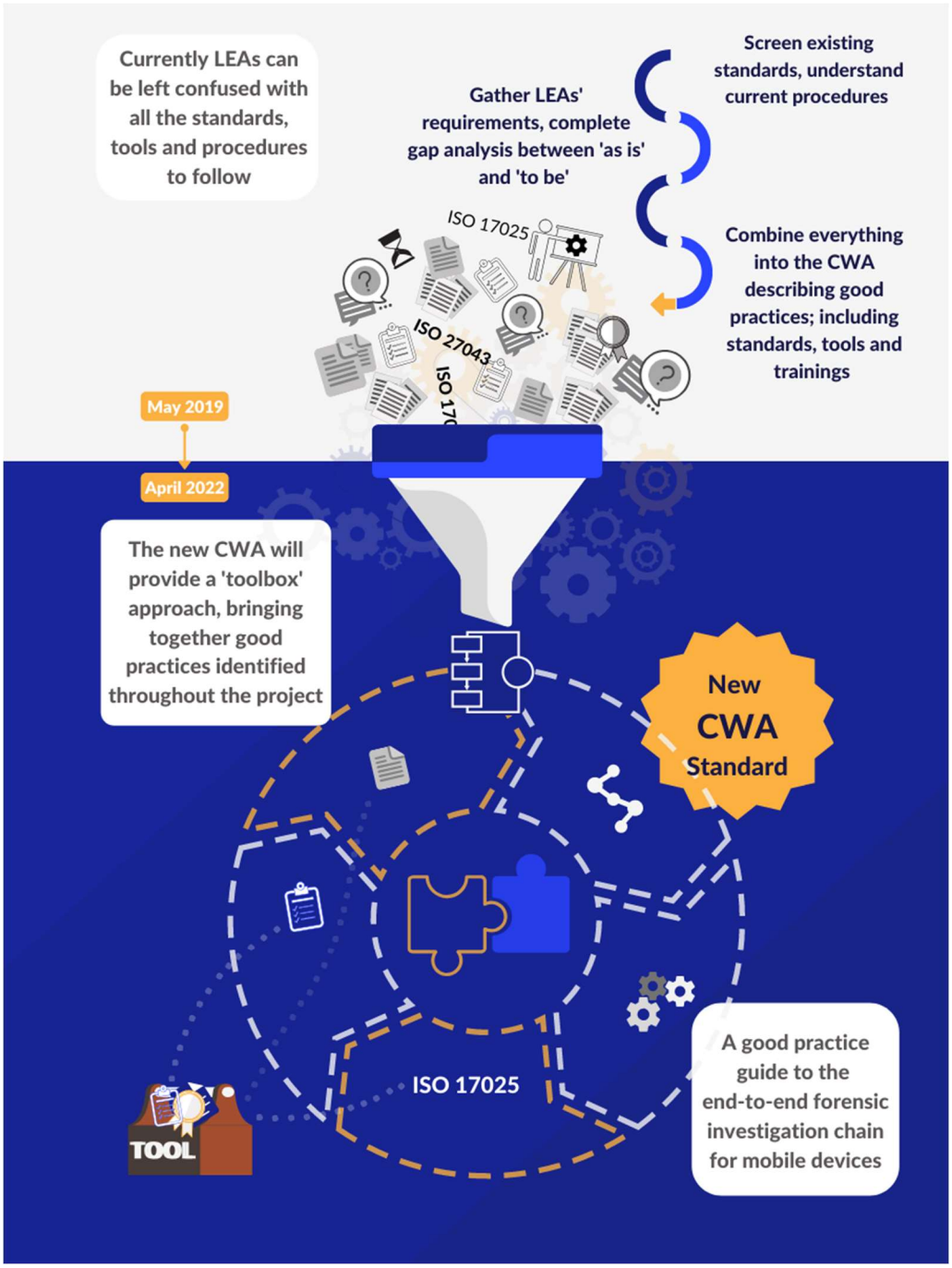

Fig 1: FORMOBILE Project - Current Standards and Practices in Mobile Forensics
Source: https://formobile-project.eu/news/31-current-standards-and-practices-in-mobile-forensics

Another obstacle that forensic professionals must overcome is mobile apps' proliferation and ever-changing landscape. Make a list of all installed apps. Some applications archive and backup data. This is critical because cell phones and other mobile devices are ubiquitous, and the users usually don't know how important the data on their devices carries.

4. CONCLUSION

The technology employed in mobile devices' digital forensic process model keeps advancing. This paves the way for forensic examiners to upgrade themselves to the latest cutting-edge technology. Generally, it has been accepted that to make a claim in the law court, a trusted process must be used during a digital forensic investigation, and a proven digital forensic investigation process model should adhere to. As a result, the authors argue that the primary methodologies for evidence processing should stay consistent to ensure the thoroughness and consistency of forensic procedures. At the same time, forensics process models should be updated on a regular basis to account for high-tech evidence.

5. RECOMMENDATIONS

In acquisition processes, the forensic examiner should employ SIM Card imagining, which is a method that makes a replica image of the SIM Card content. Like other reproductions, original evidence is preserved while the replica image is analyzed. One must hash image files to ensure that data remains correct and unmodified. To obtain and analyze data from the machine, the examiner may need to employ various forensic tools. Because of the wide variety of mobile devices, there is no one-size-fits-all solution for mobile forensic tools. As a result, it is best to employ more than one tool for examination. Popular forensic software solutions with analytic capabilities include AccessData, Sleuthkit, XRY, and EnCase. Depending on the type and model of mobile device, the best tool(s) are selected. Mobile device under seizure process must remain on and out of network connectivity till investigation is being conducted to avoid network intrusion.

6. IMPLICATIONS FOR CYBER SAFTY, PRACTICE, RESEARCH AND POLICIES IN AFRICA

Cybersecurity is a crucial because it safeguards all the types of data against theft and harm. A successful cyber-attack can be devasting to a company. It can have an impact on financial line, as well as a company’s reputation and customer trust. Breach of data privacy compromises the integrity of the company, and the consequences is huge. Cyber Safety must be given the needed attention in Africa due to the rate of internet crime increase in today’s world. Education must be introduced to create awareness on how to limit the risk involve in using technology.IT security measures must be put in place to regulate and to signal users when approaching a threat. Because cyberattacks and data breaches can be costly, cybersecurity rules are essential. There should be rules for using email encryption, Steps for accessing work applications remotely, Guidelines for creating and safeguarding passwords and Rules on use of social media.

7. DIRECTIONS FOR FUTURE WORK

Analytical techniques, Physical techniques and software-based techniques advancement help smooth the fact funding in mobile devices forensics.

REFERENCES

1. Ademu, I.O., C.O. Imafidon, and D.S. Preston, 2011. A new approach to the digital forensic model for digital forensic investigation
2. Adv. Comput. Sci. Appl., 2(12), pp. 175–178.Ali, A., 2014. A review of different comparative studies on mobile operating systems
3. 7(12), pp. 2578–2582.Casey, E., 2009. Handbook of Digital Forensics and Investigation Forensic Analysis: Online Access via Elsevier
4. Cohen, F.B., 2010. Fundamentals of digital forensic evidence P.P. Stavroulakis and M. Stamp (Eds.), Handbook of Information and Communication Security, 1st Edition, Springer, pp. 789–808, 10.1007/978-1-84882-684-7.
5. Cohen, F.B., J. Lowrie, and C. Preston, 2011. The state of the science of digital evidence examination
6. Ankit, G. Megha, G. Saurabh, and C. Gupta. "Systematic digital forensic investigation model" [Jan. 15, 2012].
7. Ayers, W. Jansen, N. Cilleros, & R. Daniellou. "Cell Phone Forensic Tools: An Overview and Analysis." 2007. http://csrc.nist.gov/publications/nistir/nistir-7250.pdf[21 January 2012]