Smartphone Forensic Challenges

Sundar Krishnan *skrishnan@shsu.edu*
Department of Computer Science
Sam Houston State University
Huntsville, USA

Bing Zhou *bxz003@shsu.edu*
Department of Computer Science
Sam Houston State University
Huntsville, USA

Min Kyung An *an@shsu.edu*
Department of Computer Science
Sam Houston State University
Huntsville, USA

Abstract

Globally, the extensive use of smartphone devices has led to an increase in storage and transmission of enormous volumes of data that could be potentially be used as digital evidence in a forensic investigation. Digital evidence can sometimes be difficult to extract from these devices given the various versions and models of smartphone devices in the market. Forensic analysis of smartphones to extract digital evidence can be carried out in many ways, however, prior knowledge of smartphone forensic tools is paramount to a successful forensic investigation. In this paper, the authors outline challenges, limitations and reliability issues faced when using smartphone device forensic tools and accompanied forensic techniques. The main objective of this paper is intended to be consciousness-raising than suggesting best practices to these forensic work challenges.

Keywords: Smartphone Forensics, Digital Forensics, Mobile Forensics, Mobile Security.

1. INTRODUCTION

Since the debut of the original iPhone in 2007, the evolution of smartphone features has been on a predictable trajectory with increasing processing speed, user friendliness, security, faster connectivity and a plethora of apps. With their increasing functionality and ever-growing data storage, smartphones have become pocket size computers. With advances in technology, device manufactures continue to add more features like privacy controls and bendable screens leading to new device models being released each week. Password protection and default device encryption are now the norm for many of these devices making it a struggle for law enforcement to find accurate ways for data extraction and analysis.

Device vendors and features of operating systems can vary widely, particularly with Android devices. The apps that they support also change keeping up with technology advancements. According to a recent IDC Research survey [1], the top five smartphone vendors by market share by the end of Q4 2018 were Samsung (18.7%), Apple (18.2%), Huawei (16.1%), Oppo (7.8%) and Xiaomi (7.6%). The same survey finds "other" device vendors making up 31.6% of the 2018 smartphone market. Devices from the "other" vendors often are the challenge when it comes to smartphone forensics as forensic product vendors often focus tuning their product compatibility with the high-use device models. With smartphones replacing conventional mobile phones and traditional home computer tasks, their use has been of forensic interest especially when part of the digital evidence of a crime or litigation.

Smartphone forensics covers the process of triage, extraction, recovery and analyzing data from the devices or smartphones. Commonly used smartphone forensic tools are Encase Mobile Investigator [2], Cellebrite [3], Magnet ACQUIRE [4], Paraben E3-DS [5] and Salvationdata SPF [6], etc. Smartphones are often targets of security attacks given their support for financial transactions and the residual private data that they may contain. For a long time, cheap pre-paid/post-paid (burner) smartphones have been a problem for law enforcement. Forensic support for such devices can be a challenge as forensic product vendors are often swamped with supporting various models in the market or just wait for a business/legal case to evolve around these devices. Due to these factors, most forensic product vendors offer a catalog of devices that are supported fully or partially. While forensic tools often aid investigators in digital forensic investigations, an unending challenge is for them to be compatible with various in the market. When working with these forensic tools, investigators can experience various challenges related to skill levels, forensic tool reliability and device-tool compatibility with the smartphone (forensic evidence). Targeting and carefully choosing automated solutions for novice investigators can improve the efficiency, speed and quality of investigations. In this paper, the authors discuss existing forensic smartphone acquisition methods and outline challenges with the implementation of smartphone forensic tools while identifying key areas of improvements.

The rest of the paper is organized as follows. Section 2 covers related works. Section 3 dives into smartphone forensics, file systems and forensic evidence management. Section 4 outlines various challenges and limitations. Section 5 provides a discussion on ways of improving overall smartphone forensics process. Lastly, Section 6 concludes with remarks.

2. RELATED WORK

Digital forensic tools continue to improve in technology and has also embraced Artificial Intelligence. Most forensic tools comprise of automation, analysis and reporting features. Mobile traffic continues to skyrocket across the world. According to a study in 2017, Americans used 15.7 trillion megabytes (MBs) of smartphone data in 2017, nearly quadrupling since 2014 and representing 40 times the volume of traffic in 2010 [7].

Henry et al. [8] conducted a survey of forensic examiners working in both private industry and government. Almost half (47%) of government personnel reported that smartphone devices are involved in more than 10% of their cases. Mobile forensic tools have become more user friendly over time and mask the complexities in automation by offering a push-button approach. Kovar [11] highlighted the value of push-button forensics, and discusses three main reasons for the acceptance of increased automation; non-expert market, speed-related financial interest from consumers and the growing volume of digital evidence resulting in case backlogs.

Given the various apps on a smartphone that individually connect to the cloud for data storage, Krishnan et al. [10] point to the legal challenges in accessing this data and the cloud provider's role. With cloud storage getting cheaper, analyzing large volumes of cloud data from a smartphone needs automation and machine learning. James and Gladyshev [12] highlight the challenges in forensic automation. In a survey done in 2016 by Harichandran et al. [9] on tools/technology needing improvement, North Americans were more focused on mobile forensics while the Europeans were most concerned with cloud forensics. This could be due to the new privacy laws like General Data Protection Regulation (GDPR) introduced in 2016 and their greater degree of severity than that of the United States.

Meanwhile Irons et al. [13] studied how to train competent digital investigators differentiate between practice and theory as well as skills and knowledge claiming that each area calls for development to ensure competency. Umale et al. [14] claimed that although forensics toolkits exist for the forensic investigator, the bulk of the tools do not offer full functionality for multiple devices. The National Institute for Standards and Technology (NIST) and the Scientific Group on Digital Evidence (SWGDE) provide an in-depth look at mobile forensics process, outlining the benefits and the challenges these devices present to Law enforcement [15], [16]. With ever

increasing makes and models of smartphones being rolled out each day, smartphone forensic tool vendors are ever keen on catering to these devices. Core forensic skills, such as data carving, Operating System knowledge and custom programs coupled with analytical thinking will continue to be necessary. Forensic practitioners need to know how to use forensic tools, but this is only complementary to a thorough understanding of the forensic process, operating systems, device applications and investigative skills.

There is a large body of literature that focuses on smartphone file system analysis, forensic methodology and techniques. A few studies have focused on the challenges faced by forensic practitioners, but these studies mostly covered smartphone forensic challenges in part coupled with surveys, security, etc. While the aforementioned works make important contributions, they do not undertake a fine-grained collection of challenges faced when using forensic tools. A literature gap was noticed in outlining these challenges faced during smartphone forensics coupled with forensic tool limitations. This paper overcomes the shortcomings.

3. MOBILE FORENSICS

The growth of mobile security and privacy features and their layers often work opposite to the ease of doing forensics. Some security features are activated by default by the Operating System (OS) and protects the user in the background, while others are obvious and seek user attention. For instance, with every operating system upgrade, Apple's iOS and Android OS seem to add another layer of security enhancement. For Apple devices, it started in 2013 with the introduction of Touch ID, a fingerprint sensor built into the iPhone 5S, and continued in iOS 8 with stronger encryption. Similarly, Android OS is also packed with powerful and practical security features starting with Android version 5.0 supporting encryption. The healthy completion between the two platforms have led to a myriad of security features that tend to increase the forensic challenges during device acquisitions.

Forensic data extracted from these devices can provide investigators and attorneys with the information they need to crack a case. As mobile devices become smaller and powerful, people sometimes carry their devices everywhere they go which means they can tell a story about who the user is communicating with, what they are communicating about, and where the user has been. The device make, country of origin, carrier, model and OS version are key to ascertain the security features that accompany the device. Table 1 lists the few security and filesystem features that can be of consideration for a forensic analyst. Sometimes, certain OS features with the same device make and model can vary based on the country that it was sold.

Mobile forensics is a branch of digital forensics that relates to methods of evidence extraction from the mobile devices like smartphones, tablets, wearables, PDAs, GPS units, etc. Mobile forensic tools acquire data from these devices and provide analysis. Smartphone devices present many challenges from a forensic perspective due to the ever-changing device models and apps being developed each day. It is extremely difficult to develop a single solution to cover all makes and models of devices. In this section, we describe various forensic processes and the file systems involved.

3.1 File System Overview

The Android operating system is a Linux-based operating system with a single root partition. Android devices feature a Linux file system structure with six main partitions on a device: boot, system, recovery, data, cache, and misc. Without root access, Android users only have access to the data partition which appears when connecting the device to a PC or browsing via a file manager app on the device. The microSD card, if applicable, will also appear mounted under this user accessible data partition. All drives and partitions are displayed as directories a tree like structure [17].

The iOS operating system is geared toward apps running on their own. Users of iOS devices do not have direct access to the file system and apps are generally prohibited from accessing or

creating files outside its container directories [21]. Most of the file-related interfaces in iOS are designed with concurrency in mind. As of iOS 10.3 (March 2017), Apple File System (APFS) is now the file system being used on Apple devices. Before iOS 10.3, HFS+ had been used.

TABLE 1: Few Smartphone Security and File-system Highlights [18], [19], [20].

	Android	**iOS**
System Security	• Linux kernel security features System Partition and Safe Mode Biometric authentication • Fingerprint • Device Administration APIs • Facial recognition scan • Verified boot (version 6.0 onwards) • System image signing • Strong passwords • Remote Wipe	• Secure boot chain • Secure enclave • Touch ID • FaceID • Activation lock • Strong passwords • Remote Wipe
Encryption and data protection	• Filesystem Encryption • Keychain • Cryptographic APIs • Security-Enhanced Linux (SELinux) Limited root usage • Full-disk encryption (Android 5.0 and above) • Full filesystem encryption at kernel level (Android 3.0 and later) • File-based encryption (Android 7.0 and later)	• Encryption by default • Two-step verification • Hardware security features • File data protection • Passcodes • Data protection classes • Keychain data protection (Keybags) • Per file encryption • Keys in separate HW module Erasure of data after 10 failed passcode attempts
App Security	• The Application Sandbox • Backdoor checks • Filesystem permissions	• App code signing • Runtime process security • App groups • Data protection in Apps • Secure notes • HealthKit • ReplayKit • SecureElement • iCloud Keychain • AppPay
Network Security	TLS, VPN, Wi-Fi, Bluetooth, Wi-Fi Password Sharing	TLS, VPN, Wi-Fi, Bluetooth, AirDrop, Wi-Fi Password Sharing
Access	Rooting, Recovery/Flashboot	Jailbreak, Boot exploit in old devices and application exploit in newer
Secondary Storage	Files on SD Card/cloud	iTunes backup
File System	(YAFFS), EXT4, FAT	HFSX
Files	SQLite, XML	SQLite, XML, Propriety List of ASCII or Binary

3.2 Mobile Forensic Evidence

Modern mobile devices like smartphones contain an abundance of information that could potentially be of evidentiary value. Much of this information is increasingly volatile and thus live forensics is often needed before working in isolation using traditional computer forensic approaches. Further forensic evidence can be gathered over the network in certain cases

depending on the operating condition of the device. Few examples of forensically interesting data during an on a smartphone device are listed below [22].

1. Incoming, outgoing, missed call history - Call detail records (“CDRs”)
2. Phonebook or contact lists
3. SMS text, application based, and multimedia messaging content
4. Pictures, videos, and audio files and sometimes voicemail messages
5. Internet browsing history, content, cookies, search history, analytics information
6. To-do lists, notes, calendar entries, ringtones, memos (notes)
7. Documents, spreadsheets, presentation files and other user-created data
8. Passwords, passcodes, swipe codes, user account credentials
9. Historical geolocation data, cell phone tower related location data, Wi-Fi connection information
10. User dictionary content
11. Data from various installed apps
12. System files, usage logs, error messages
13. Deleted data from all the above

In some cases, if proper authentication details are available, data from the cloud storage of apps can also be recovered. Other methodologies that can be used to find the geographical location of the device or its user are listed below [23].

1. GPS: The Global Positioning System (GPS) of satellites are used to pinpoint the location of a smartphone. [Note that Federal Communications Commission (FCC) E911 regulations require wireless carriers to be able to track 911 callers.]
2. Triangulation: Three cell phone towers in close proximity can be used to approximate the location of the smartphone.
3. Wi-Fi Networks: Even with the GPS turned off, a smartphone can record Wi-Fi network connections.
4. Ping: Ping by service provider for hardware associated with a smartphone number
5. Rogue tower (Stingray): Rouge devices that impersonate cell towers can trick smartphones into thinking they are the service provider.

Since smartphone usage has become ubiquitous in our daily life and at our workplaces, they play a critical role in the theft of intellectual property and other crimes. While computer forensics has almost become commonplace, smartphone forensics is still evolving and presents several challenges for digital forensic examiners.

3.3 Forensic Evidence Management

Smartphone devices once part of the evidence pile must be treated as an active digital device. Any change in power state or accidental transmission can cause evidence contamination. Below are few steps to manage smartphone device evidence [15], [24].

1. Evidence Box and Seizure: Digital forensics operates on the principles that evidence should always be adequately preserved, processed, documented and admissible in a court of law. Digital devices may contain latent, trace, or biological evidence. The forensic investigator should thoroughly document and preserve this potential evidence for processing before the digital evidence imaging is undertaken.

2. Phone Jammers and Faraday Bag: Smartphone devices are often seized switched on. Background apps are sometimes activated, and this could alter the state of the device. Active, apps can invoke services and can start to transmit data over the network. Thus, the best way to store and transport these devices is to attempt to keep them in a Faraday bag. A phone jammer is also recommended to be kept beside this evidence.

3. Device State: Smartphone devices should be charged, turned on and set to airplane mode to avoid a shutdown, which would inevitably alter file state. Disabling Wi-Fi and Hotspots is also recommended. If possible, the SIM card may be removed and preserved.

3.4 Data Acquisition Process and Approach

In NIST's Special Publication 800-101 Revision 1, Rick Ayers et al. [15] proposed a framework as in Figure 1 for forensic examiners to compare forensic extraction methods used by different tools to acquire data. A forensic examiner can easily classify and compare extraction methods thereby understanding the limitations of tools at each layer.

3.4.1 Manual Extraction

The Manual Extraction method involves viewing and recording the data content stored on a smartphone device. This method cannot recover deleted information but can provide a record of various screens and the user interface. This is a time-consuming process and depends on the device working condition.

FIGURE 1: Mobile Tools Classification System [15].

3.4.2 Logical Extraction

The Logical Extraction is possible when a connectivity between a smartphone device and a forensics workstation is achieved, where the connectivity can be made with a wired/wireless USB. Logical extraction tools send a series of commands over the established communication interface from the computer to the smartphone device. The smartphone device data collected is sent back to the workstation for further examination. The Logical extraction is often quick and results in collection of call history, SMS, photos, music etc. data. For Android 5.0+ devices, the user needs to trust the forensic workstation by accepting a RSA key.

The Android Debug Bridge (ADB) is a versatile command-line tool that lets the investigator communicate with a Android smartphone device. It is a client-server program that includes the client, a background process daemon and a server. ADB is included in the Android SDK Platform-Tools package. Android's ADB is free to use and can be downloaded along with the SDK Manager. ADB usually communicates with the device over USB but can also use Wi-Fi after some initial setup over the USB. Using ADB, all visible files can be obtained through the file system, which does not include deleted files or hidden partitions.

3.4.3 Physical Extraction

The Physical Extraction methods like Hex Dumping, Joint Test Action Group (JTAG), Chip-Off and Micro Read allow for a more direct access to the raw information stored on the smartphone device flash memory.

The Hex Dumping technique is commonly used to upload a modified boot loader into a protected area of memory (e.g., RAM) on a smartphone device using a flasher box [15]. A series of

commands is sent from the flasher box to the smartphone device to place it in a diagnostic mode. Once in diagnostic mode, the flasher box captures all (or sections) of the device's flash memory and sends it to the forensic workstation.

JTAG is used when forensic extractions cannot acquire a physical image or when a device is logically damaged or "bricked" [15]. Many device manufacturers support the JTAG standard. Forensic examiners can communicate with a JTAG-compliant component of a smartphone device by utilizing special purpose standalone programmer devices to probe defined JTAG test points. JTAG extractions are more advanced and invasive than HEX Dumping as the examiner must dismantle some (or most) of a smartphone device to obtain access to establish the wiring connections.

The Hex Dumping and JTAG extraction methods [15] require a connectivity between a smartphone device and a forensic workstation. These methods allow a more direct access to the raw information stored in smartphone device's flash memory. However, the ability of a given tool to parse and decode the captured data can be challenging. Sometimes, all data contained within a given flash memory chip may not be acquired as well.

The Chip-off Forensics involves physically removing the flash memory chip from the smartphone device and preparing it using balling techniques allowing for a chip reader to acquire the raw data residing on the chip [15]. This method provides examiners with the ability to create a binary image of the removed chip. While the chip reader is a required device for the extraction, a chip adapter may also be required depending on chip specifications. Unlike JTAG, the Chip-off is a destructive process, and the smartphone device may no longer function as before. Many examiners start with a non-destructive technique such as Logical, JTAG and HEX-dumping before opting for a Chip-off.

The Micro Read process records the physical observation of the gates on a NAND or NOR chip with the use of an electron microscope [15]. Skilled technical expertise coupled with almost no commercially available tools make such extractions a rarity. It is generally accepted that the Micro-Read technique is most forensically sound and most technical, while the manual extraction technique is the simplest. For a successful acquisition at this level, technical experts, necessary equipment, time and in-depth knowledge of proprietary information is required. Also, there are no known U.S. Law Enforcement agencies performing acquisitions at this level.

3.4.4 Smartphone Forensic Tool Classification and Complexity

There are many tools and techniques available in smartphone forensics thereby making the selection criteria dependent on the investigative requirement, type of device and its associated media. Smartphone forensic tools are usually categorized by vendors as separate products in their portfolio. This is probably due to targeted support for the smartphone forensics user community who often branched out from traditional computer forensics.

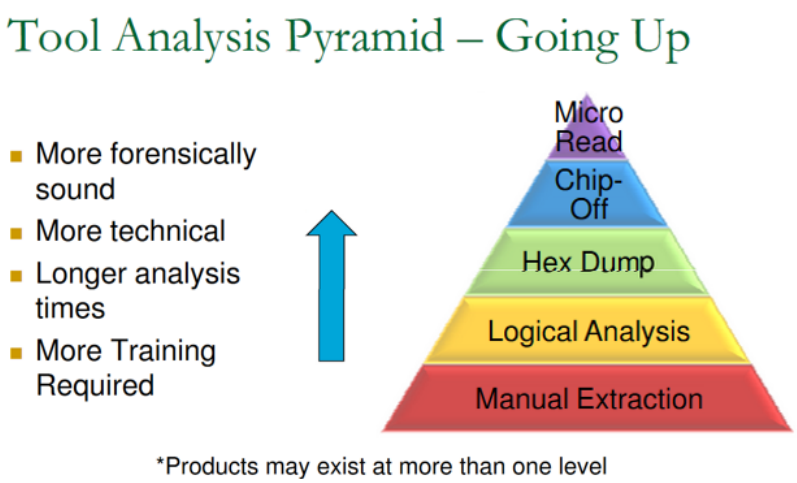

FIGURE 2: Mobile Tools Classification System [15].

In Figure 2, a general comparison of tool characteristics is shown. During investigations, it is also important for forensic analysts to consider different aspects beyond tools, such as methodologies, timelines, phases of the process and the complications inherent therein. For example, evidence acquisition or extraction process in an Android smartphone device require enabling of the "USB debugging" option on the device. If the terminal has any screen lock option configured, it is necessary to circumvent it by turning-on the "Stay awake" option disabling of any time-out screen lock option.

4. SMARTPHONE FORENSIC CHALLENGES AND TOOL LIMITATIONS

In this section, challenges for beginner or skilled smartphone forensic analysts are described during their use of smartphone forensic tools.

4.1 To Root or Not?

Out of security concerns, by default, the operating system in smartphones provide lower privileges for users, and thus gaining *root access* on a smartphone is akin to user privilege elevation. The process to privilege elevation is known as *rooting* of a device or *jailbreaking*. This allows users to attain administrative privileges (known as root access) on their smartphones and access operating system processes that are otherwise restricted to normal users. Rooting a smartphone device can void its manufacturer's warranty and is a security risk as the user then operates the device with full administrative level privileges. Nonetheless, tech savvy smartphone users continuously develop rooting methods, which vary depending on device.

A forensic examiner can expect to encounter such rooted phones as a part of evidence. Also, as rooting Android smartphone devices has become a common phenomenon because manufacturers and Android OS do not provide root access to device owners by default, forensic examiner may need to root devices to acquire data for forensic examination. However, common users seldom root their smartphone device unless an application from the app store needs such an access on their device for its functioning. Usually the device manufacturer and Android do not provide root access to the device owner by default. Meanwhile, Abalenkovs et al. [20] that a bit by bit extraction of data from iOS smartphone devices has become a moving target due to increasingly stronger protection mechanisms.

For the above reasons and the diverseness of makes and models of smartphone devices, forensic tools can be more challenging when rooting is required. The forensic examiner should decide on root level access and obtain necessary approvals before rooting the device. Once root access is granted, the forensic examiner is able to perform extensive data recovery and file carving which uncovers deleted evidence stored on the device (evidence).

Note that before forensic examiners root devices, risks of the rooting process must be ascertained to decide whether to accept a specific risk or take action to prevent or minimize it. In the following, the examples of risks to evaluate are listed:

1. Intrusiveness of the rooting process on device (evidence).
2. Use of commercially available root exploits that exploit vulnerabilities or unproven solutions off the Internet.
3. Evidence and data integrity change due to privilege escalation.
4. Availability of reliable root exploits for the particular smartphone.
5. Added privacy concerns due to the increased data visibility with root access.
6. Periodic vendor patching that can plug exploits used for rooting.
7. Flasher boxes use for dead exploits (mostly due to carrier locking).

4.2 Device Dependency, Limitations and Hardware Dynamics

Smartphone hardware manufacturers keep releasing new models almost monthly upgrading their hardware specifications regularly. These devices also seem to have a lesser life span with newer operating systems released annually. Users replace lost devices more regularly than a laptop or home computer. This also calls for special data, drivers and power cables for different makes and models of hardware. Due to such rapidly changing smartphone device environment, forensic tool vendors seldom guarantee that their tools operate on any type of makes and models of smartphones, and thus the vendors provide a list of smartphone devices that are compatible with their forensic products. Meanwhile, the forensic analyst should be aware that a forensic tool in use can fail or only be partially successful during device acquisitions.

4.3 Logical or Physical Acquisition

There are two main data acquisition types in smartphone forensics, namely – logical and physical. The logical acquisition involves leveraging APIs to copy all available files that are not deleted from the smartphone device's file system into a forensic case. The retrieved data is active user content (user accessible) from the memory storage like contacts, call logs, images, videos and music. Partial app data such as configuration files, app SQLite files etc. can also be obtained. Meanwhile, the physical acquisition process involves a bit-by-bit memory dump of an image of the smartphone device including deleted data. The physical acquisition dump contains both allocated and unallocated space. Note that such physically acquired data is in its raw format and needs additional parsing depending on the file systems.

When it comes to selecting the most suitable method, many aspects are considered: the level of thoroughness required, the available time for carrying out the process and what type of information it is necessary to obtain such as volatile information, previously deleted data, information from third party applications, etc. Figure 3 shows a forensic process flow useful to follow when making such a decision. It considers other aspects as well such as whether a USB debugging is activated, whether a terminal is locked with an access granted, etc.

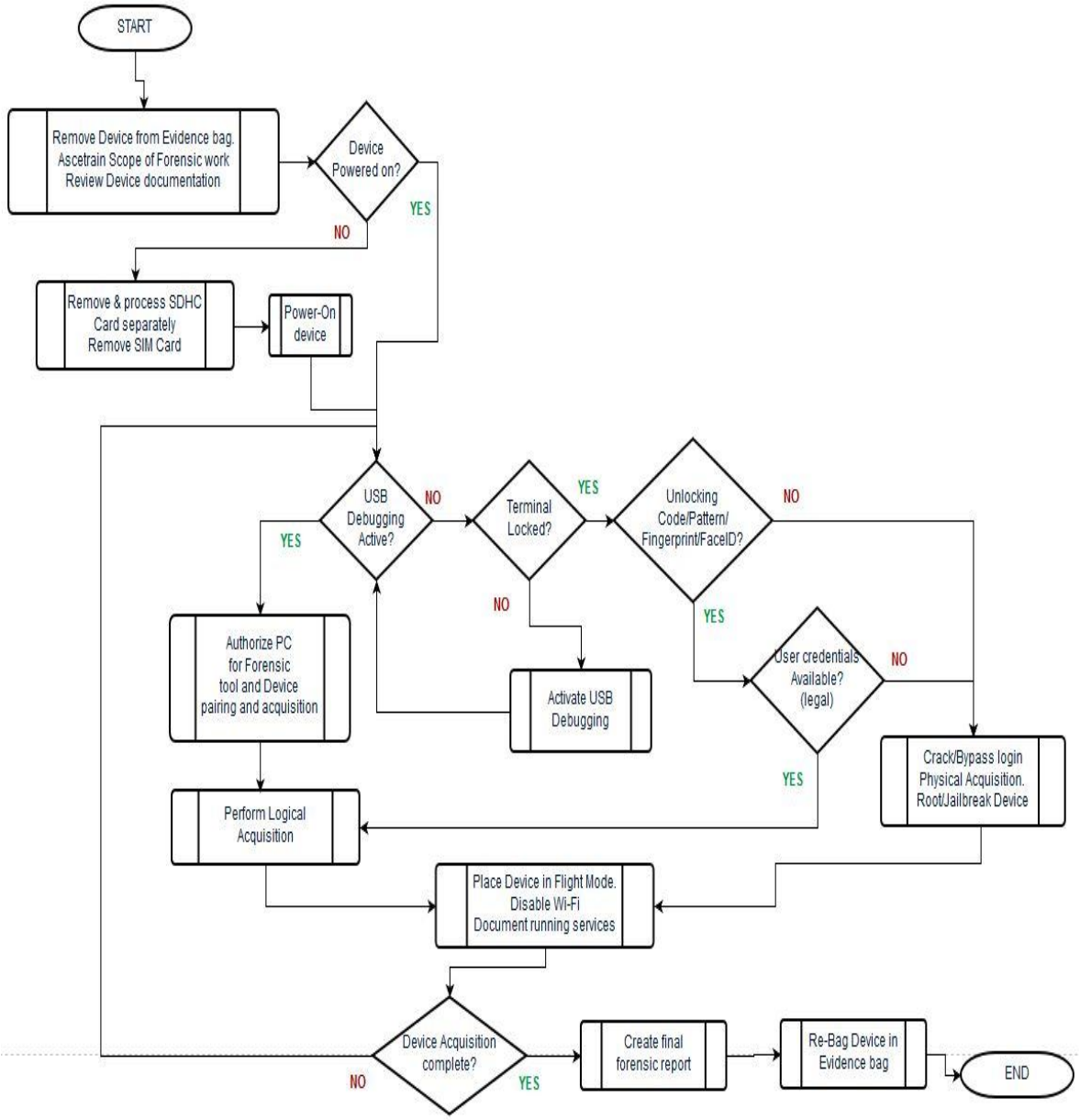

FIGURE 3: A General Smartphone Forensics Process Workflow.

4.4 Time Intensive

Smartphone forensics has become time intensive due to growing storage on smartphone devices which makes acquisition process hours to complete. Also, given the uncertainty of the forensic tool used during the acquisition process and rooting challenges, time should be suitably factored. Opening vendor communication and support channels for each case is thus suggested in case of unforeseen hurdles.

4.5 Forensic Tool Training

Training forensic analysts is essential so that they can have opportunities to develop requisite skills. Especially, product agnostic trainings on core smartphone forensic concepts, evidence handling and reporting are considered to be most essential. During a process of a forensic investigation, an analyst must bear in mind first and foremost the phases of acquisition and analysis of an evidence. It is necessary to understand a wide range of methods, techniques and

tools as well as the criteria necessary for being able to evaluate the suitability of using one tool versus another.

4.6 Tool Reliability

It is not always easy for forensics investigators to select right tools because of complexity and diverseness of both smartphone devices and forensics tools, and the volatile nature of digital evidence and legal threshold of admissibility.

Saleem et al. [26] performed a comparative evaluation of Margin of Error and Confidence Interval (CI) against two smartphone devices, Samsung HTC (Desire 300) and Galaxy (GT-S5300) using five trial versions of various smartphone forensic tools. In their conclusion, tools fared with mixed results highlighting the fact that selection of the appropriate tool is required per investigation. Meanwhile, Padmanabhan et al. [27] analyzed few smartphone forensic tools for reliability and accuracy. Their experimental results show that XRY 5.0 performed better than UFED Physical Pro1.1.3.8 in terms of reliability and accuracy. Osho et al. [28] claimed that finding a forensic tool or toolkit that is virtually applicable across all smartphone device platforms and operating systems is currently infeasible. Computer Forensics Tool Testing program (CFTT) [29] often reports on smartphone device acquisition tools (organized by publication date) and can be a useful source on tool reliability.

As the market floods with various device models, forensic product vendors have been trying their best to keep up device compatibility. Also, as the chances of rooting the smartphone device via forensic tools are getting more difficult, reliability of such tools for evidence acquisition and analysis has become more essential.

4.7 Vendor Support

Vendor support for smartphone forensic tools can vary overtime. Few vendors are niche players in the market and only work with federal and state buyers thus limiting their support to very specific clients. Vendor support channels should be pre-established before working on an evidence which could impact wait times. Vendor support staff should be able to quickly turnaround and fulfil the requirement on an identical device similar to the evidence in question. Usually vendors have dedicated R&D teams that issue new features and releases to meet customer needs depending on the terms service contract. However, not all vendors have a 24/7 service desk support and this service may need to be purchased separately. Penalties for turnaround time and failures can be addressed on service contracts.

4.8 Non-Standardization in Reporting

Since there is no standardization adopted by vendors on reporting structure and the odds of successful forensic acquisition on various tools, forensic analysts are advised to be prepared for reports in different formats from the tools.

4.9 Chip-off and JTAG Techniques

Nowadays, very few forensic tools use chip-off and JTAG techniques. This forensic method is of high risk of damage to the memory chips of smartphone devices. The chip-off techniques therefore should be used by experience personnel (investigators). This technique is based on Nand or eMMC memory chip extraction from the smartphone device requiring special hardware and adapter kits that are easily available though. One of the widely used tools for chip-off dumps analysis is UFED Physical Analyzer [30]. Forensic examiners also use other tools such as UP-828 [31], Z3x Easy Jtag [32], eMMC Pro Tool [33], Riff Box [33], etc., to read data directly from chip using adapters such as MOORC E-Mate Pro eMMC Tool. These techniques are the most difficult way to extract data apart from Micro Read.

JTAG forensics is another method of data acquisition, which utilizes Test Access Ports (TAPs) on a smartphone device instructing the smartphone processor to transfer the raw data stored on connected memory chips. When commercial forensic extraction options cannot acquire a

physical image or a device is logically damaged or “bricked”, the advanced method, jtagging, can extract a full physical image from devices.

4.10 Timestamps

Sometimes, timestamps such as file “creation time” reported by what tools are created based on acquisition timestamp.

Creation time	Last access time	Last modification time
7/3/2018 6:03:17 PM	7/2/2067 9:14:28 PM	12/31/1979 12:00:00 AM
7/3/2018 6:03:17 PM	7/2/2067 9:14:28 PM	12/31/1979 12:00:00 AM

FIGURE 4: Incorrect Timestamps Reported from Forensic Tools.

The Figure 4 shows an example of possible ambiguity in reported timestamps. Because of such ambiguity, few time formats conversions can result in creating incorrect data such as "last Modification time" reported as 12/31/1979 and "last access time" of files reported as 7/28/2067. Therefore, it would be helpful for forensic analysts to cross-verify metadata before reporting on findings involving timestamps.

4.11 Tool Standardization

There is still a lack of global standardization on forensic processes in industry. With the growing smartphone markets, forensics product vendors have started focusing on each country’s forensic needs and adapting their products towards local geographical markets. Currently, the “Smartphone Tool Specifications Standard” [32] developed by NIST is the only framework that lists requirements to be met by all forensic acquisition tools. Meanwhile, the Computer Forensic Tool Testing (CFTT) [29] project at NIST helps in establishing a methodology for testing computer forensic software tools by development of general tool specifications, test procedures, test criteria, test sets, and test hardware. NIST guidelines of smartphone forensics help organizations evolve appropriate policies and procedures to deal with these devices and to prepare forensic specialists to conduct forensically sound examinations [15]. The evaluation results from CFTT provide the information necessary for forensic product vendors to improve their forensic tools, for users to make informed choices about acquiring and using computer forensics tools, and for interested parties to understand the tools capabilities.

4.12 Overcoming Device Protections

Many paid forensic tools include mechanisms to bypass device access protections. Although this is not always guaranteed by such tools, if the process is going to be carried out manually on a smartphone device, one or more of the following actions should be performed [34].

1. If the device is rooted, remove the gesture.key or password.key file in accordance with the mode of protection established.
2. Install a personalized recovery tool such as ClockWorkMod or Team Win Recovery Project (TWRP) and then deactivate device access locking.
3. Using brute force to crack the device. (On a 4-digit pin, it has been demonstrated the pin can be cracked in a maximum period of 16 hours.)
4. Do a “Smudge Attack” [35], which involves obtaining the locking pattern from fingerprints on the device’s screen by using different-angled photographs.

4.13 Data Volatility

Smartphone forensics yields evidence mostly obtained via non-volatile physical memory dump and file system analysis. Volatile memory (often referred to as RAM memory) stores data created by installed apps that can be crucial for an investigation. Non-volatile memory known as flash or ROM memory stores data like phone contacts, pictures, emails, etc. which remains saved even when the device is powered off. In iOS smartphone devices, app-data such as usernames, passwords, encryption keys are erased as the device memory is full or when the device is re-booted. Apple encrypts this volatile user data using 256-bit encryption making it

difficult for physical acquisition or when the device is powered off. Jalibreaking an iOS smartphone involves restarting of the device thereby erasing the volatile memory.

4.14 Forensic Soundness

Forensically sound data extraction on a smartphone is a continuous challenge due to evolving technology. Boot loaders are considered the most forensically sound physical extraction method [35]. Temporary rooting is not as forensically sound as a boot loader because it does load the device's operating system, which may be logged within the device.

While forensic acquisition tools are executed on smartphone devices, they must be kept powered on throughout the process due to the volatile nature of data. These tools load client APIs to a device to be executed or install small boot-loader code into the device's RAM during boot. Thus, there will be no concept of a write blocker during acquisition that could potentially cause questioning of evidence integrity by the opposing counsel. However, during manual acquisition methods using advanced *dd* command (application), a write blocker is advised during file transfers.

4.15 Encryption

Personal smartphone devices are encrypted by default when sold with various methods such as password lock, bio-metric authentication, and use of encrypted memory cards thereby providing a user with additional means to protect data. Such data encryption capabilities on on-board or removable memory storage are offered as a standard feature in many smartphone devices or available through add-on applications. With the advanced encryptions, cracking passwords to unlock a device has been getting more difficult for all forensic tools. Also, data storage on devices have resulted in longer decryption time. Even though most mainstream forensic tools provide a password bypass and password recovery mechanism, decryption is still a challenge to these tools. Thus, Flasher box, JTAG, or chip-off extraction methods have become necessary when devices are locked by their service providers [36]. Meanwhile, many smartphone vendors and network carriers also have introduced advancements in anti-theft features such as "automatic device wipe" after a set of unsuccessful attempts which interfere with a legitimate forensic investigation.

4.16 Network Protocols

There are a number of network communication protocols used between the smartphone device and cell towers or wireless access points. Network protocols also govern communication between smartphone devices and other smart devices. While smartphones and related technology evolved in the past decades, multiple protocols has been introduced while others have retired. Few communication protocols [37], [38] supported by smartphones over the years are ANSI-41, GSM Mobile Application Part (MAP), Push Access Protocol (PAP), Push Over the Air (OTA), Sub-network Dependent Convergence Protocol (SNDCP), Base Station System GPRS Protocol (BSSGP), GPRS Tunneling Protocol (GTP), Mobile IP, Mobile Shell (mosh), Wireless Application Protocol (WAP), etc. These protocols coupled with multiplexing can easily overwhelm forensic analysts. Even though forensic analysts are not expected to be aware of each and every such protocol, they still should have a general understanding of the communication protocols in play for specific smartphone (evidence) device. A general list of supported network communication protocols can be ascertained from the device manuals.

5. IMPROVING SMARTPHONE FORENSICS PROCESS

Overcoming smartphone forensic challenges can help improve the overall forensic process and yield results that can be well accepted by the courts or investigative agencies. Below are a few ways discussed to overcome smartphone forensic challenges.

5.1 Time Management

Digital forensic investigations irrespective of the type of evidence can take time especially when encryption, cloud and privacy constraints are involved. Each investigative case is unique and

time spent can be a variable. The investigator's ability to link a suspect as the one who clicked the photos on the smartphone can take time and patience. Similarly, accessing and processing data from third-party servers or the cloud could take a lot of paperwork and coordination with external teams. Planning of such investigations and clear identification of roles and responsibilities of the team are highly recommended. Special handling may be required for some situations especially when dealing with evidence and suspect across geographical borders and jurisdictions. Thus, the forensic investigators should set realistic timelines and factor additional time for unknown tasks when updating management or reporting to authorities.

5.2 Cost Management

Cost of a smartphone forensic investigation can easily spiral when left unchecked. The more upfront information is known about the scope of work, the tighter the cost estimate can be. Failure to properly scope the work can lead to both time and cost overruns. There are many factors [39] that affect the cost of smartphone forensics like the type of investigation required, parties involved, forensic tools required, skills required, manpower needed, encryption levels, deadlines, the volume of data to investigate, smartphone age in the market, Operating Systems etc. Independent third-parties can prove expensive if State labs do not have the necessary expertise or tools. This was evident during the FBI's iPhone investigations concerning the massacre in San Bernardino, California [40], [41] during which assistance of private entities was requested to overcome the unlock attempt limit of the iPhone device. It cost the FBI roughly $900,000 to hack the locked iPhone. Smartphone forensic investigations conducted by State labs are usually constrained by manpower and budgets making timely cost estimates crucial when management approvals are necessary.

5.3 Training and Skills Management

A smartphone forensics investigator is a specially trained professional who works with law enforcement agencies, as well as private firms, to retrieve information from smartphones and associated data storage devices. Adequate training of these investigators can largely overcome many forensic challenges specified thus far. Training is a continuous activity and adequate funding should be set aside for keeping-up with the forensic tools and smartphones in the market. Attending conferences across the country and globe and interacting with other professionals can advance their knowledge base. The willingness to learn is a prerequisite in this field.

5.4 Process Capability, Reliability and Maturity

Forensic investigation process capability is the ability to do it right without any errors, while reliability is a measure of how capable the forensic investigative process is to deliver a specified outcome over many attempts. By applying a look down method, process reliability can help identify problems, allow significant cost reduction opportunities and allow for improvements. By applying process measurement and improvement steps, factors like process interruption causes, costs and process specific improvements can be targeted. The forensic laboratories or organization(s) conducting forensic work, may have to sacrifice some investigative process capability to improve the reliability of the process as a possible trade-off. Statistical tools may also be used to streamline the various investigative process involved thereby highlighting process areas where improvements are needed. Similarly, the use of a process capability maturity model can enable labs and organizations to evaluate the maturity of their digital forensics capabilities and identify roadmaps for improving by following industry best practices or regulatory requirements [43]. Also, a generic capability maturity models for process management can be used to tailor a more specific derived model for the laboratory or organization conducting digital forensic investigations.

5.5 Accreditation of Forensic Laboratory

Forensic investigators/examiners should provide acceptable, accurate, and complete answers to address concerns or questions regarding the admissibility of their testimony into legal proceedings. Depending upon the jurisdiction of the case, their testimony may also have to meet the requirements of Frye1 [44] or Daubert2 [45] standards. Laboratories or organizations

conducting routine digital forensics can benefit from accreditation against standards set by The American Society of Crime Laboratory Directors Laboratory Accreditation Board (ASCLD/LAB) [46], ISO/IEC 17020:2012 [47] or ISO/IEC 17025:2005 standards [48]. Through accreditation, a digital forensic laboratory demonstrates that its management, operations, personnel, procedures, equipment, and security, etc. meet recommendations outlined on international standards. A forensic laboratory accreditation can provide a standard or framework to ensure confidence in the results obtained from the forensic processes of digital evidence investigation. Similarly, adoption of a Quality Management System (QMS) to support training programs, periodic competency checks of examiners, policy documentation, use of standards, controls and recommended best-practices can help overcome work quality concerns while improving productivity.

6. CONCLUSION

In this paper, we studied various challenges faced by a forensic investigator when dealing with smartphone forensics and provided a comparative overview of these challenges. While smartphones provide a ton of valuable information, deterrents to their successful forensics can be a mix of their evolving technology, stronger security features, forensic tool limitations, communication protocols, customization by multiple device carriers, and the sheer number of models. Thus, an important consideration for the forensic investigators is to be fully aware of what data can and should be extracted from the devices in question, risks in the extraction process, and how much quality data can be retrieved and processed by the specific forensic tool at hand given the tool limitations. Future research will need to be undertaken to document workflows on tool options for an investigator when encountering these challenges. Development of a forensic tool picker software application would be helpful that could direct the investigator on forensic tool compatibility based upon smartphone device (evidence) specifications and supported devices from forensic tool vendor.

7. ACKNOWLEDGEMENT

The authors would like to thank the forensics lab at the Cyber Forensics Intelligence Center, Sam Houston State University, for providing necessary research facilities and access to digital forensic tools.

8. REFERENCES

[1] “Smartphone Market Share.”, Internet:.https://www.idc.com/promo/smartphone-market-share/vendor, 2018, [May 19, 2019].

[2] “EnCase Mobile Investigator - Mobile Forensics Investigation Solution.”, Internet: https://www.guidancesoftware.com/encase-mobile-investigator?cmpid=nav_r., [May 22, 2019].

[3] “Home - Cellebrite.”, Internet:https://www.cellebrite.com/en/home/, [May 22, 2019].

[4] “Magnet ACQUIRE - Magnet Forensics.”, Internet: https://www.magnetforensics.com/products/magnet-acquire/ , [May 22, 2019].

[5] “E3 DS for Mobile forensics, Smartphone Forensics, and IoT forensics - Paraben Corporation.”, Internet: https://paraben.com/mobile-forensics-software/ , [May 22, 2019].

[6] “SmartPhone Forensic System - Cell Phone Forensics Tools.”, Internet: http://www.salvationdata.com/spf-smartphone-forensic-system.html , [May 22, 2019].

[7] “Background on CTIA’s Wireless Industry Survey.”, Internet: https://api.ctia.org/wp-content/uploads/2018/07/CTIA_ToplineWirelessIndustrySurvey.pdf, 2018, [May 22, 2019].

[8] Henry P., 2013, “The SANS Survey of Digital Forensics and Incident Response.”, Internet: https://blogs.sans.org/computer-forensics/files/2013/07/sans_dfir_survey_2013.pdf, [May 22, 2019].

[9] Harichandran V. S., Breitinger F., Baggili I., and Marrington A., (2016, Mar) , “A cyber forensics needs analysis survey: Revisiting the domain’s needs a decade later,” [On-line], Comput. Secur., vol. 57, pp. 1–13, Available: https://www.sciencedirect.com/science/article/pii/S0167404815001595, [May 22, 2019].

[10] Krishnan S., Chen L., (2014), “Legal Concerns and Challenges in Cloud Computing,” in 2nd International Symposium on Digital Forensics and Security (ISDFS 2014), [On-line], Available: https://arxiv.org/abs/1905.10868 , [May 21, 2019].

[11] Kovar D., (2009), “Push button forensics – managing the downsides | Integriography: A Journal of Broken Locks, Ethics, and Computer Forensics,” Intergriography: A Journal of Broken Locks, Ethics, and Computer Forensics , [On-line], Internet: https://integriography.wordpress.com/2009/11/19/push-button-forensics-managing-the-downsides/, [May 18, 2019].

[12] James J. I. , Gladyshev P. (2013, Mar) , “Challenges with Automation in Digital Forensic Investigations,” Available: http://arxiv.org/abs/1303.4498, [May 18, 2019].

[13] Irons A. D., Stephens P., Ferguson R. I. (2009 Sept), “Digital Investigation as a distinct discipline: A pedagogic perspective,” Digit. Investig., vol. 6, no. 1–2, pp. 82–90, Internet: https://linkinghub.elsevier.com/retrieve/pii/S1742287609000309, [May 18, 2019].

[14] Umale M., Deshmukh A. B., Tambhakhe M. D., (2014) “Mobile phone forensics challenges and tools classification: A review”, [On-line], Internet: https://pdfs.semanticscholar.org/867c/098360eb7ed57bd991bf0bb99042799f2824.pdf, [May 18, 2019].

[15] Ayers R., Brothers S., Jansen W., (2007, May), “Guidelines on Mobile Device Forensics,” NIST Spec. Publ. 800-101 Revis. 1, Internet: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-101r1.pdf, [May 18, 2019].

[16] “SWGDE Best Practices for Mobile Phone Forensics.”, Internet: https://www.swgde.org/documents/CurrentDocuments/SWGDEBestPracticesforMobilePhoneForensics, 2013, [May 18, 2019].

[17] Steve, “Android File System and Directory Structure Explained,” Internet: http://www.stevesandroidguide.com/android-files/, 2017, [May 18, 2019].

[18] “iOS Security.”, Internet: https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf, 2019, [18-May-2019].

[19] “System and kernel security | Android Open Source Project.” Internet: https://source.android.com/security/overview/kernel-security, [May 20, 2019].

[20] Abalenkovs D, Bondarenko P, Pathapati V. K., Nordbø A., Piatkivskyi D., Rekdal J. E., Ruthven P. B., (2012), “Mobile forensics: Comparison of extraction and analyzing methods of ios and android”, [On-line], Available: https://andynor.net/static/fileupload/399/Mobile Forensics - Comparisonof extraction and analyzing methods of iOS and Android.pdf, [May 20, 2019].

[21] “File System Basics.”, Internet:

https://developer.apple.com/library/archive/documentation/FileManagement/Conceptual/FileSystemProgrammingGuide/FileSystemOverview/FileSystemOverview.html. [May 18, 2019].

[22] "What digital forensics artifacts can you find on a mobile phone?", Internet: https://www.gillware.com/digital-forensics/mobile-forensics/. [May 18, 2019].

[23] Cell Phone Science - Criminal Advocacy Program, Internet: http://capwayne.org/cap-archives/capwayne/handouts/2014/2014-10-10_SRR-Cell-Phone-Science.pdf, [May 16, 2019].

[24] Introduction: Importance of Mobile Forensics , Internet: https://resources.infosecinstitute.com/category/computerforensics/introduction/mobile-forensics/the-mobile-forensics-process-steps-types/#gref, [May 16, 2019].

[25] Lohiya R., John P., and Shah P. (2015, May), "Survey on Mobile Forensics," Int. J. Comput. Appl., vol. 118, no. 16, [On-line], pp. 6–11, Internet: http://research.ijcaonline.org/volume118/number16/pxc3903476.pdf, [May 17, 2019].

[26] Saleem S., Popov O., and Appiah-Kubi O. K., (2013, Oct), "Evaluating and Comparing Tools for Mobile Device Forensics Using Quantitative Analysis," Springer, Berlin, Heidelberg, [On-line], pp. 264–282, Available: http://link.springer.com/10.1007/978-3-642-39891-9_17, [May 17, 2019].

[27] Padmanabhan R., Lobo K., Ghelani M., Sujan D., and Shirole M. (2016, Aug), "Comparative analysis of commercial and open source mobile device forensic tools," Ninth International Conference on Contemporary Computing (IC3), 2016, pp. 1–6, Internet: http://ieeexplore.ieee.org/document/7880238/, [May 18, 2019].

[28] Osho, O., & Ohida, S. O. (2016), "Comparative evaluation of mobile forensic tools," mecs-press.net, Available:http://www.mecs-press.net/ijitcs/ijitcs-v8-n1/IJITCS-V8-N1-9.pdf, [May 18, 2019].

[29] "Mobile Device Acquisition | Homeland Security," DHS. [On-line]. Internet: https://www.dhs.gov/publication/mobile-device-acquisition, [May 18, 2019].

[30] Cellebrite - UFED Physical Analyzer, Internet: https://www.cellebrite.com/en/products/ufed-ultimate/, [June 12, 2019].

[31] Teel Technologies, Internet: http://www.teeltech.com/mobile-device-forensic-software/up-828-programmer/, [June 11, 2019].

[32] Easy JTAG, Internet: http://easy-jtag.com/, [June 10, 2019].

[33] eMMC Pro, Internet: https://www.emmc-pro.com/, [June 10, 2019].

[34] Ayers R. P., "Smart Phone Tool Specification | NIST.", (2010, Apr), Internet: https://www.nist.gov/publications/smart-phone-tool-specification, [May 18, 2019].

[35] Martínez A. (2016), "Tools for carrying out forensic analyses on mobile devices | INCIBE-CERT," INCIBE, Internet: https://www.incibe-cert.es/en/blog/mobile-forensic-analyses-tools. [May 18, 2019].

[36] Aviv A. J., Gibson K., Mossop E., Blaze M., and Smith J. M. (2010), "Smudge attacks on smartphone touch screens," Proceedings of the 4th USENIX conference on Offensive technologies. USENIX Association, [On-line], pp. 1–7, Internet:

https://dl.acm.org/citation.cfm?id=1925009, [May 19, 2019].

[37] Engler R. and Miller C. (2013), “Six Persistent Challenges with Smartphone Forensics,” Forensicmag, Internet: https://www.forensicmag.com/article/2013/02/6-persistent-challenges-smartphone-forensics. [May 19, 2019].

[38] Bhargavi S. (2006), “Implementation of microcontroller based mobile communication data acquisition and control system using nokia F bus protocol in real time environment”, [On-line], Internet: https://shodhganga.inflibnet.ac.in/handle/10603/64948, [Jun 10, 2019].

[39] Ghosh R. K. (2017), “Mobile OS and Application Protocols,” in Wireless Networking and Mobile Data Management, Singapore: Springer Singapore, [On-line], pp. 217–261. Internet: http://link.springer.com/10.1007/978-981-10-3941-6_8, [Jun 10, 2019].

[40] Mikalack B., The Vestige Team, How much does Digital Forensic Services Cost? Internet: https://www.vestigeltd.com/thought-leadership/digital-forensic-services-cost-guide-vestige-digital-investigations/ , [Sept 5, 2019].

[41] Grossman L (2016, Mar) , Inside Apple CEO Tim Cook’s Fight With the FBI, Internet: https://time.com/4262480/tim-cook-apple-fbi-2/, [Sept 5, 2019].

[42] Benner K., Lichtblau E., The New York Times, U.S. Says It Has Unlocked iPhone Without Apple, Internet: https://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html , [Sept 8, 2019].

[43] Novac M (2017), Gizmodo, The FBI Paid $900,000 to Unlock the San Bernardino Terrorist's iPhone, Internet: https://gizmodo.com/the-fbi-paid-900-000-to-unlock-the-san-bernardino-kill-1795010203 , [Sept 8, 2019].

[44] Al Hanaei, E. H., Rashid, A. (2014, May). DF-C2M2: a capability maturity model for digital forensics organisations. In 2014 IEEE Security and Privacy Workshops (pp. 57-60). IEEE. , [Sept 10, 2019].

[45] Frye v. United States, 293 F. 1013 (D.C. Cir. 1923) , Internet: https://www.law.ufl.edu/_pdf/faculty/little/topic8.pdf , [Sept 12, 2019].

[46] Daubert v. Merrell Dow Pharmaceuticals (92-102), 509 U.S. 579 (1993), Internet: https://www.law.cornell.edu/supct/html/92-102.ZS.html , [Sept 12, 2019].

[47] The American Society of Crime Laboratory Directors (ASCLD) , Internet: https://www.ascld.org/ , [Sept 12, 2019].

[48] Conformity assessment — Requirements for the operation of various types of bodies performing inspection, ISO/IEC 17020:2012 [-,IEC], Internet: https://www.iso.org/standard/52994.html , [Sept 9, 2019].

[49] General requirements for the competence of testing and calibration laboratories, ISO/IEC 17025:2005, Internet: https://www.iso.org/standard/39883.html, [Sept 8, 2019].