Analysis of Physical Image Acquisition Forensic Tools for Android Smartphones

Firdous Kausar† and Tadani Nasser Alyahya††

Computer Science Department, Al Imam Mohammad Ibn Saud Islamic University, Riyadh, KSA

Summary
Mobile phones play an important role in our lives, especially smartphones. With the tremendous growth of the mobile device market, the possibility of using them in criminal activity will continually increase. Android is one of the highly competitive platform in the market. Android used by many manufactures to run different models, causing a strong diversity. Thus, the difficulty of physical image acquisition of android based smartphones arises, especially, when the source code of latest Android version is released too late. As a consequence, the available smartphones with latest versions memory cannot be acquired using available smartphone forensic tools. This paper gives a comprehensive perspective of some of the mobile device forensic tools that offer physical acquisition. A comparative analysis of these tools is performed based on different parameters which includes: cost, integrity, data recovery, usability, ways to export data forensic phases support, and supporting generic android smartphones.

Key words:
physical image; physical acquisition; Android forensic; forensic tools

1. Introduction

The utilization of mobile devices has increased, especially smartphones, and at the same time digital crime has also increased. The advent of the smartphones has completely revolutionized the way people live, work and play. However, there is a dark side of using smartphones in committing crimes. Investigators use suspects smartphones to derive evidence and then use them in courtroom against them. The smartphone derived evidence should be reliable in order to be accepted in a courtroom as no different from other forms of evidence.

In the last few years, there has been a substantial amount of memory acquisition researches targeting Android smarphones. The acquisition aim is to extract and collect useful information including deleted data to be further analyzed and presented to courtroom. There are two main acquisition methods for mobile device forensic: physical and logical. Physical acquisition is a bit-by-bit copy from an entire physical storage including deleted data. Logical acquisition extracts logical storage such as portion of a file system. Data stored in smartphones are fragile, as the data can be overwritten or deleted. Therefore, the need to use physical acquisition instead of logical acquisition to extract and maintain deleted data [1].

Physical acquisition tools are classified into hardware-based and software-based tools. Hardware-based method is to bypass the operating system by means of a physical device. A dedicated communication port will be opened by a dedicated hardware to copy the internal memory [2]. In Android smarphones, JTAG test pins can be used to retrieve the internal memory of a device [3]. However, not all Android smarphones have JTAG test pins. Software-based method is the use or design a tool for acquiring the internal memory [2]. In Android smartphones, one option is to acquire data from /dev/mem devices [3]. Unfortunately, this method only works for smartphones with at most 896 MB RAM [4]. Kollar [5] developed a loadable kernel module named fmem, that crates /dev/mem device for acquisition purpose. However, it does not work for all Android smartphones [4].

To acquire data from Android smartphones physically, usually the smartphone is required to be booted in either custom bootloader, custom recovery mode, or normal mode with root access [6]. Then, execute code on the smartphone to send a copied data to hardware device or server (e.g., laptop or desktop) [6].

The process of physical acquisition can be time-intensive, due to smartphone processor speeds, cable types used, and the amount of data transferred. Sometimes it takes hours to complete the physical acquisition. Most commercial tools, such as UFED and Oxygen, send data over USB. However, the transmission rate of the copied data does not utilize the maximum transmission rate of the USB. For illustration, USB 2.0 has a maximum transmission rate of 480 Mbps but it receives at most 320 Mbps [7]. In 2016, the largest Android smartphones available on the market are 128 GB. As smartphones continue to grow in size, the times to physically acquire them will increase as well [6].

In this paper, we analyzed many different physical acquisition tools for Android smartphones and compared their cost, integrity, data recovery, usability, ways to export data forensic phases support, and supporting generic Android smartphones. This paper is organized as follows: Section 2 describes Android architecture, Section 3 shows different scenarios of data acquisition procedure, Section 4 discusses some of the available physical forensic

Manuscript received November 5, 2016
Manuscript revised November 20, 2016

tools, Section 5 provides comparative analysis of selected physical forensic acquisition tools, Section 6 concludes with summery and some proposed future work.

2. Android Architecture

Understanding Android internals and architecture is at most important in forensic investigation, due to the flexibility of Android. Android platform is changing over time with new versions. According to the differences between versions, so does the architecture differs. However, the main core components of Android architecture are the same. Android architecture has four main layers, as shown in Figure 1:

2.1 Linux Kernel

Understanding Linux kernel is the most important, as it is the basic of Android architecture [8]. It supports the core services, such as memory, network, and process management, and security. It also maintains various drivers for almost all of the hardware [8, 9].

2.2 Library and Android Runtime

Android includes a set of libraries written in C/C++ [8]. Libraries, such as Standard CSystem Library, Media Libraries, 3D Libraries, are used by the components of the system through the Application Framework layer [9].

The Android runtime section provides a key component called Dalvik Virtual Machine (DVM) which is a kind of Java Virtual Machine specially designed and optimized for Android [8]. It also provides as set of core libraries which enable developers to write Android applications using standard Java programming language [8]. A set of core libraries and DVM compose an Android runtime, where every running application holds its own instance of the DVM and executes in its own process [9].

2.3 Application Framework

This layer provides many higher-level services to Java applications that can be exploited [8, 9]. Application developers can consume and provide services through of a wide set of Application Programming Interfaces (APIs), always respecting the security constraints enforced by the framework [9].

2.4 Application

The highest layer includes a bundle of programs (e.g., contact manager, calendar, SMS program, web-browser, an email client) written in Java Programming Language [10].

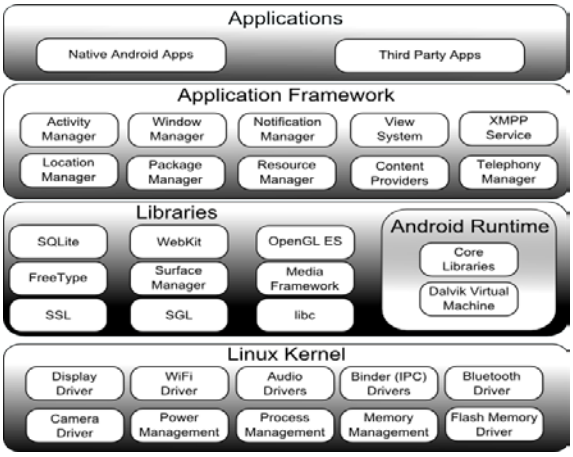

Fig 1. Android architecture.

3. Data Acquisition Procedure

Different scenarios of data acquisition process from Android smartphones which forensic examiners may adopt. By using the proper procedure, forensic examiners may retrieve maximum information from the smartphone, so that the acquired data can be further analyzed and documented in the safest and least intrusive manner as possible. The forensic examiner must follow the procedures in order to preserve the stored data on the target smartphone [11].

3.1 Data Preservation Procedures

The forensic examiner should check the status of the target smartphone, on or off. When the smartphone is powered off, the forensic investigator checks its memory card. If the memory card cannot be removed (i.e. internal memory), the data can be copied using standard USB card reader. If the memory card can be removed, then remove the memory card and copy it into a forensic memory card to ensure its preservation. The data can be copied using the same approach used with pen drives. Another, use forensic tools to copy the data and then generate hash values of the duplicate data. At the end of the procedure, the forensic memory card with the copied data should be returned to the smartphone.

3.2 Network and Connection Isolation Procedures

It is important to isolate the smartphone from the network to prevent any alteration of data. The smartphone can be isolated by using a room with physical insulation from electromagnetic signals, or simply set the smartphone to flight or offline mode. As the forensic examiner turns the smartphone on, he must immediately configure it to such connectionless mode, to avoid data transmission, receiving calls or SMS. Whenever the smartphone receives an information, such as incoming call, SMS, or email, the

examiner should document and describe it in the final report.

When the smartphone is isolated from telecommunication networks, the examiner should check if the smartphone has been configured to provide an authentication mechanism (e.g., password or pattern). After that, the examiner should complete the data acquisition procedures depending on the access control mechanism which is configured on the device.

3.3 Data Acquisition of Smartphone without Access Control Procedure

One situation, which is the simplest, is to have an unlocked smartphone with removable memory card. As mentioned earlier, the examiner should extract data from memory cards at first and then reinstall into the smartphone the forensic cards that have received the copies. The examiner should now check the status of super user privileges in Android smartphone. If it is enabled, the examiner can gain access to all stored data in the smartphone without any restriction by using USB debugging tool ADB and make a copy of its internal memory.

However, if the super user privileges are disabled in the smartphone, in this case some Android smartphones can be acquired using bootloader mode or recovery mode. The examiner should evaluate the possibility to apply those techniques on that kind of smartphone. Some of the available mobile device forensic tools that can be used by examiners do not use user privileges to acquire data, such as Cellebrit UFED and Oxygen. Instead Cellebrit UFED uses bootloader mode. It is up to the examiner to choose an efficient mobile device forensic tool to recover a complete copy of the internal memory.

3.4 Data Acquisition of Smartphone with Access Control Procedure

The Android runtime section provides a key component called Dalvik Virtual Machine (DVM) which is a kind of Java Virtual Machine specially designed and optimized for Android [8]. It also provides as set of core libraries which enable developers to write Android applications using standard Java programming language [8]. A set of core libraries and DVM compose an Android runtime, where every running application holds its own instance of the DVM and executes in its own process [9].

Android smartphone can be locked using access control, such as a password or pattern. According to NIST [12], there are three ways of gaining access to locked smartphones:

1. Investigative method, where the examiner seeks possible valid passwords.
2. Gain access via hardware, where the examiner should perform a non-destructive procedure to access the smartphone. This method request support from manufacturers and authorized service centres.
3. Software access methods, are usually the easiest way even though it depends on the handset model and Android version.

The examiner must use the least intrusive method to avoid compromising the evidence. If the password or the pattern has been obtained when the smartphone was seized, it should be tested. If the examiner not succeeded, he should check if the smartphone is configured to accept USB debugging connections using a ADB tool. If he succeeds, he attempts to gain super user access control privileges to resume the acquisition process, as mentioned earlier in the last section. Even when there are no privileges to super user access control to the smartphone, the examiner can install applications through the ADB tool to bypass the access control system. In case where it is not possible to bypass the access control system or USB debugging access is disabled, it is left to the examiner to acquire the data from the removable memory card that may be installed on the smartphone.

3.5 Acquisition Documentation

All the techniques and procedures that have been used must be documented by the examiner, in order to facilitate the analysis of the extracted data. The better documenting the data acquisition procedure, the more trust will be given to the examination results. The examiner should register the hash codes of data generated and extracted during the acquisition process carefully. He must also document any caveats that he faced during the acquisition process, such as receiving an e-mail or SMS before the smartphone have been isolated from telecommunication networks.

4. Physical Forensic Tools for Android

4.1 Linux Memory Extractor (LiME)

LiME tool was introduced in 2012 by J. Sylve et al. [4]. It is an open-source forensic tool for acquiring a complete volatile memory from devises powered by Linux, such as Android. LiME is based on a new loadable kernel module, named dmd, that is able to acquire the memory pages in a forensically sound manner. It supports dumping memory to either the SD on the smartphone or via the network. The dmd module works as follows: parsing the kernel structure for learning the ranges of the physical memory address of system RAM, translating physical addresses to virtual addresses on every memory page, reading all memory pages and writing them on SD of TCP socket. LiME tool offers significant features [13]: only dmd module is needed to transfer to target device for acquisition, very few kernel functions are required for memory dumping, loading of

dmd module requires a minimal footprint, and minimal interactions are required with userland. The authors showed that about 99.46% of pages correctly captured over TCP connection, and 99.15% of pages correctly captured to SD card. The proposed module supports all Android devises, but it is still not considered to be a generic module. Moreover, Wächter [14] concluded that LiME tool in not feasible for memory forensic in law enforcement for several reasons: identifying the model, identifying Android version, lock screen, root exploit, availability of sources, kernel configuration, and evidence erosion.

4.2 Android Physical Dump (APD)

APD was developed by S. Yang et al. [15] in 2015. The tool is based on analyzing the firmware update protocols of Android smartphones. Therefore, it acquires internal memory through the Android update protocols of Android devices' bootloader. It supports dumping both partition and entire memory. The format of the acquired data using APD is raw data that can be analyzed through smartphone forensic analysis tools. The authors proved that the proposed method guarantees the integrity of the acquired data. They showed that APD acquires the data at a high speed; it took about 30 min to acquire 32 GB memory, while UFED 4PC took 120 min on average. APD can be executed despite of the restriction due to screen lock; by turning off the phone and rebooting in the firmware update mode rather than normal boot mode. APD tool supports over 80 of the latest Android models. However, the main drawback of the method is that it requires to analyze the firmware update protocol whenever new Android smartphones are launched.

4.3 Hawkeye

Hawkeye was proposed for physical acquisition purposes in 2016, by Guido et al. [6]. The purpose of Hawkeye is focusing on reducing the amount of data, redundant data, that needs to be transferred during the physical acquisition. Thus, decreasing the overall acquisition time. Hawkeye runs Android smartphones on either custom bootloader or recovery mode in order to acquire physical images. The tool temporarily installs hawkeye agent into the target smartphone’s volatile storage. The agent is provided with a list of baseline hashes and partitions. The agent will then identify and send only necessary data blocks to the backend PMF architecture via USB. The authors chose PMF for several reasons: converting images into their raw format, writing back automatically. The agent can acquire a partition or full smartphone’s internal memory. Hawkeye could successfully acquire the internal memory on 16 GB memory in 7 min.

4.4 Android Memory Extractor (AMExtractor)

AMExtractor [3] is a tool for acquiring volatile memory from Android devices. AMExtractor uses the /dev/kmem device to execute code in kernel space. This will avoid the restriction of loadable kernel module and provide the ability to work on the latest stock ROMs without any modifications. AMExtractor does not need the source code of the target smartphone and it is compatible with most Android operating system versions. Unlike other tools, AMExtractor runs in kernel mode, which makes the tool forensically sound, as it has minimum impact on target smartphones. Furthermore, running the device on the kernel mode minimizes copying data and fines hidden data from user mode. H. Yang et al. [3] showed that the acquired data using AMExtractor is nearly the same as acquired data using LiME.

4.5 ANDROPHSY

ANDROPHSY is an open source tool that was developed in 2015 by I. Akarawita et al. [16]. It is the first open-source tool that supports the all phases of the digital forensic process. ANDROPHSY architecture consists of four major modules: case handling, acquisition, analysis support, and reporting module. In case handling module, case creation and backup archive functionalities for specific case are provided. In acquisition module, it provides physical and logical acquisition. In analysis module, a complete examination and analysis of the removed data. And last the reporting module, a report in PDF format is generated. In order to use this tool, a single .jar file and configuration script are need to be installed separately.

Focusing on physical acquisition in this tool, the authors used low level Linux and Android built-in forensic functionalities such as dd and Android Debug Bridge (adb) commands. The adb commands is used for connection and communication between Android smartphone and workstation over USB. The dd command is a built in command line utility used to recover raw image from physical drives. ANDROPHSY exploits kernel to gain root access, which minimizes data alteration. It provides user access control and case management for authentication and privacy. It does not use SD card as a collection target. Instead, the data are transferred over TCP connection.

4.6 Android Digital Autopsy (ADA)

ADA is an open source digital forensic tool that was developed in 2016 by R. Fasra et al. [17]. The tool performs physical, logical, and file system acquisition. The authors used a device with multimedia card (MMC) partition layout. The developed a script file to automate the physical acquisition process. The script file identifies the data blocks, then uses dd commands to acquire RAW images of the blocks after gaining root access. The

recovered data are then stored in an external storage card, i.e. SD card. Along with the proposed tool, the authors developed ADA Analysis Tool, but unfortunately it is only for logical acquisition

4.7 Cellebrite UFED

Cellebrite UFED [18] is a commercial forensic tool that performs physical, logical, file system, and password acquisition on wide range of devices and platform, such as Android. It also performs decoding, analysis, and reporting. UFED can acquire data from all Android OS versions.

4.8 Oxegen Forensic Suite

Oxygen Forensic Suite [19] is one of the leading forensic tools that supports wide range of smartphones. It is used by Law Enforcement, army, police department, and other government authorities, in more than 50 countries all over the world. It enables investigators to perform physical acquisition of Android smartphones, advanced examination, and analysis of raw data and of device images extracted from the smartphone. It allows a fully automated acquisition and analysis of supported smartphones. It can acquire a 16 GB smartphone in approximately 45 minutes. It offers a well-defined report for the examiner that summarizes smartphone activities.

4.9 XRY Physical

MSAB [20] provides products for extraction, analyzing, and reporting. XRY Physical tool supports extraction of internal memory and removable media without changing the target device. It also allows users to generate hash values of the memory image, as well as individually decoded file. XRY Physical recovers raw data from the target smartphone by bypassing the operating system and offers the chance to go deeper and recover deleted data from the target smartphone. The physical extraction is separated into two distinct stages: the initial dump stage, where raw data is recovered from the smartphone, and decoding stage, where the tool can automatically reconstruct the data into meaningful information. The extracted data can be viewed by XAMN Spotlight.

4.10 Device Seizure (DS)

DS [21] supports physical, logical, file system, and password extraction. It provides a complete analysis and report on all acquired data. It supports wide range of platforms and devices. By using DS physical acquisitions, most, but not all, deleted data can be recovered from smartphone. It supports physical acquisitions for Android up to 4.4.2 (except for version 3). DS has low minimum system requirements, so it can run on any device. It can search through a smartphone's memory dump for crucial evidence [22].

4.11 MOBILedit! Forensic

MOBILedit! Forensic [23] allows to retrieve, search, and view all data, including deleted data, stored on a smartphone with only few clicks. This tool is able to support all smartphones powered by Android and iOS. It is frequently updated and upgraded with new features to support more smartphones. The tool has changed the way this evidence is obtained and presented. It generates detailed forensic reports ready to be presented in courtroom. The report could be generated in any language.

4.12 ViaExtract

ViaExtract [24] is a physical and logical extraction tool created by ViaForensics. It offers a guided data acquisition, powerful analysis, and flexible reporting features for Android smartphones. ViaExtract uses device rooting wizard to gain root access of most smartphones with only click of a button. This tool allows examiners to crack passcode to extract data from internal and external storage. It provides a global search feature for greater speed and ease of use. This feature allows the examiner to search all the content types extracted in all the currently opened acquisitions at once. ViaExtract works on many of the most popular Android smartphones.

4.13 Mobile Phone Examiner Plus (MPE+)

MPE+ [25] is a mobile device investigation tool that includes enhanced smartphone acquisition and analysis capabilities It supports wide range of platforms and devices. It allows examiners to quickly collect, easily identify, and effectively obtain the data. Like DS, MPE+ can search through a smartphone's memory dump for crucial evidence [22]. The examiners can acquire more data from iOS and Android devices 30% faster than any other tool in the market. MPE+ includes a robust and superior analysis tools. To perform physical acquisition, an empty forensic SD card, holds temporarily MPE+'s agent, should be inserted in a target smartphone. Use a tool (e.g. SuperOneClick) to gain Shell Root, i.e. not full root.

5. Comparative Analysis

It is very hard to evaluate tool performance, as their capabilities varied. In this paper physical forensic tools are compared in terms of cost, user friendly, data recovery with screen lock, data integrity, partition data recovery, ways to export data, forensic phases support, and supporting generic Android smartphones. Table 1 illustrates the summery of the evaluated forensic tools.

5.1 Open Source

The most powerful mobile devices forensic tools, such as Oxygen, UFED, and MSAB XRY, are expensive and not

affordable, as they are intended for not personal use. Besides commercial tools, there are free open source mobile devices forensic tools, such as LiME, AMExtractor, ADA, and ANDROPHSY, that compete the commercial tools in many terms (e.g. supported devices, acquired data, integrity, friendliness) to achieve best results.

5.2 User Friendly

Almost all commercial tools provide users with easy-to-use interface for data extraction, analysis, and reporting. They are designed with a simple interface to navigate, along with a wizard to guide users through the entire process. Some of them supports multi-language user interface, such as Cellebrite UFED and Oxygen. ANDROPHSY is the only open source forensic tool that provides users with friendly interface.

5.3 Bypass Screen-Lock

All Android smartphones could be locked using either pattern or password, and delivered with USB debugging disabled for security reasons. Therefore, USB debugging should be enabled in order to apply existing acquisition methods. Most of the software based forensic tools, such as MOBILedit! Forensic, use the ADB protocol for physical acquisition. However, USB debugging must be enabled to use the ADB protocol and apply acquisition methods. ADB tool overcomes this problem by executing physical acquisition after turning off the smartphone and rebooting in the firmware update mode [15]. Regardless of whether USB debugging is enabled or if the device is in a rooted state, MPE+ can bypass screen locks and get physical images from Samsung Galaxy S II family powered by Android 2.3.4 or 2.3.5 [25]. ANDROPHSY, DS, and MSAB XRY support bypassing screen lock of Android smartphones [19, 20, 21]. UFED and viaExtract can bypass any kind of lock and acquires data only if USB Debugging is enabled [18, 24]. Oxygen can create physical images and bypass lock screen for some of Samsung Galaxy Note family smartphones [19].

5.4 Data Integrity

Integrity of evidence is a significant dimension in forensics, which describes the need of evidence to be integral and not altered during acquisition and analysis. Some of the mobile device forensic tools required a smartphone to be booted into normal mode for getting physical images, which inherently makes changes to a smartphone's storage. Other mobile device forensic tools ran in the smartphone's recovery mode or through the bootloader, which are more forensically sound. ADB tool preserved integrity by booting the target smartphone in the firmware update mode which guarantees the integrity of artefact even after physical acquisition multiple times [15]. Integrity can be verified through hash value checksum. DS, MOBILedit! Forensic, UFED, Oxygen, MSAB XRY, ADA, Hawkeye, and ANDROPHSY verify data integrity by calculating hash values (e.g., MD5, SHA-1, SHA-256, SHA-512) among images produced. MPE+ builds a Python Script that acts upon a copy of evidence rather than the original binary data, thus original data will not be altered [21, 25].

Table 1: Comparative analysis of Android forensic tool

Forensic Tool	*Open Source*	*Friendly*	*Recover Data With Screen Lock Smartphone*	*Integrity*	*Partition*	*Export Data*	*Support Forensic phases*	*Generic*
LiME	Yes	No	No Information	high	No	TCP SD card	No	No
AMExtractor	Yes	No	No	high	No	TCP	No	No
APD	No	No	Yes	Yes	Yes	No Information	No	No
Hawkeye	No	No	No	Yes	Yes	No Information	No	No
ANDROPHSY	Yes	Yes	Yes	Yes	Yes	TCP	Yes	Yes
ADA	Yes	No	No	Yes	No	SD card	No	No
UFED	No	Yes	Yes	Yes	No	SD card USB flash memory	Yes	No
Oxygen	No	Yes	Yes	Yes	No	USB connection Bluetooth	Yes	No
MSAB XRY/XACT	No	Yes	Yes	Yes	No	USB connection	Yes	No
DS	No	Yes	Yes	Yes	No	USB connection	Yes	No
MOBILedit! Forensic	No	Yes	No	Yes	No	USB cable TCP	Yes	No
ViaExtract	No	Yes	Yes	No Information	No	No Information	Yes	No
MPE+	No	Yes	Yes	No	No	Cables Infrared Bluetooth	Yes	No

5.5 Partition Data Recovery

Data recovery is the It is heart of any forensic tool. All physical acquisition tools focus on retrieving whole internal memory. Some of them (e.g. APD, Hawakye and ANDROFSY) allows part of the internal memory to be acquired physically

5.6 Export Data

Acquired data can be then exported by using different ways to be saved such as USB connection, Bluetooth, TCP socket and Infrared. Further, it can be saved directly by using SD card of USB flash memory. Table1 illustrates the tools and how data are exported.

5.7 Support Forensic Phases

The main mobile device forensic phases are: acquisition, analysis, and reporting. Few commercial tools support the entire mobile device forensic phases, such as Oxygen, Cellebrite UFED, MSAB XRY/XACT, MOBILedit! Forensic, ViaExtract, and MPE+. For free tools, ANDROPHSY is the only tool that supports the life cycle of mobile device forensic.

5.8 Generic

There is no general recovery image method that can be used on every Android smartphone, as in all android smartphones highly coupled with Android version, device model, kernel version, hardware profile, build version and firmware version specific. ANDROPHSY method pursued a modern approach by using low level Linux and Android built-in forensic functionalities such as dd and adb commands to fits any situation. DS supports physical acquisitions for Android up to 4.4.2 (excluding version 3). UFED and ViaExtract extracts data physically via USB debugging for all Android versions including Android 4.NO in the earlier one and Android version 2.2 or higher for the later one. Although, Oxygen, MSAB XRY, and MOBILedit! Forensic support wide range of Android smartphones, but still the former one cannot unlock every Android smartphones and the later ones cannot support all Android smartphones for physical acquisition.

6. Conclusion

With the increase in physical forensic tools and practical use of Android smartphones, this paper sets benchmarks for any researcher who wants to compare the new tools with the available tools. It also tends to supply investigators or practitioners a more efficient interactive, and convenient way of capturing physical images via choosing reliable and suitable physical forensics tools.

Commercial forensic tools, such as Oxygen and Cellebrite UFED, are reliable, easy to use, can be used on wide range of Android smartphones across many Android versions, and support all forensic phases. However, they are not applicable on every Android smartphone, especially when the target smartphone is locked. Moreover, it is not affordable for personal use. Opens source tools are often not user friendly, focus only on acquisition phase, can be used on limited version of Android smartphones, but still reliable. One interested open source tool, ANDROPHSY, can compete commercial forensic tools in its feature. It is designed to be used to acquire all Android smartphone with any version. It is the first open source tool that support the life cycle of mobile device forensic.

In the future we hope to include more physical forensic tools in this comparative analysis. Also providing physical forensic tools of different platform, such as iOS and Windows. For future research we will conduct a practical research for examining physical forensic tools on smartphones running iOS and Android.

References

[1] T. B. Tajuddin and A. A. Manaf, "Forensic investigation and analysis on digital evidence discovery through physical acquisition on smartphone," in 2015 World Congress on Internet Security (WorldCIS), Dublin, 2015

[2] L. Cai, J. Sha, and W. Qian, "Study on forensic analysis of physical memory," in Proc. of 2nd International Symposium on Computer, Communication, Control and Automation (3CA 2013), 2013.

[3] H. Yang, , J. Zhuge, H. Liu, and W. Liu,"A tool for volatile memory acquisition from Android devices," in Advances in Digital Forensics XII, New Delhi, Springer International Publishing, 2016, pp. 365-378.

[4] J. Sylve, A. Case, L. Marziale, and G.G. Richard, "Acquisition and analysis of volatile memory from android devices," Digital Investigation, vol. 8, no. 3, pp. 175-184, 2012.

[5] I. Kollár, "Forensic RAM dump image analyser," MCS thesis, Charles Univ., Prague, Czech Republic, 2010.

[6] M. Guido, J. Buttner, and J. Grover, "Rapid differential forensic imaging of mobile devices," Digital Investigation, vol. 18, pp. S46-S54, 2016.

[7] L. Spector, "USB 3.0 speed: real and imagined," PCWorld, 2014. [Online]. Available: http://www.pcworld.com/article/2360306/usb-3-0-speed-real-and-imagined.html. Accessed: Oct. 17, 2016.

[8] C. A. Jayasinghe, "Android smart phone contact analyzer", MSIS dessirtation, 2015.

[9] A. Distefano, G. Me, and F. Pace. "Android anti-forensics through a local paradigm," Digital Investigation: The International Journal of Digital Forensics & Incident, vol. 7, pp. S83-S94, 2010.

[10] X. Lee, C. Yang, S. Chen, and J. Wu, "Design and implementation of forensic system in Android smart phone," in Convergence and Hybrid Information Technology - 5th International Conference, Daejeon, 2009.

[11] A. Simao, F. Sicoli, L. Melo, F. Deus, and R. Sousa Junior, "Acquisition of digital evidence in android smartphones," in Proc. of 9th Australian Digital Forensics Conference, p. 116-124, 2011.
[12] W. Jansen, and R. P. Ayers, "SP 800-101. Guidelines on cell phone forensics," 2007.
[13] C. Ntantogian, D. Apostolopoulos, G. Marinakis, and C. Xenakis, "Evaluating the privacy of Android mobile applications under forensic analysis," Computers & Security, vol. 42, pp. 66-76, 2014.
[14] P. Wächter, "Practical infeasibility of Android smartphone live forensics,"Master thesis, Friedrich-Alexander Univ. Erlangen-Nürnberg, Erlangen and Nurnberg, Bavaria, 2015.
[15] S. J. Yang, J. H. Choi, K. B. Kim, and T. Chang, "New acquisition method based on firmware update protocols for Android smartphones," Digital Investigation, vol. 14, pp. S68-S76, 2015.
[16] I. U. Akarawita, A. B. Perera, and A. Atukorale, "ANDROPHSY-forensic framework for Android," in Proc. of 2015 Internatoinal Conferace on Advances in ICT for Emerging Regions (ICTer), pp. 250-258, 2015.
[17] R. Fasra, and A.R. Meeran, " Performing digital autopsy on an Android device: an “open aource” approach," International Journal of Computer Technology and Applications, vol. 9, no. 15, pp. 7111-7117, 2016.
[18] "Cellebrite UFED,". [Online]. Available: http://www.cellebrite.com/Mobile-Forensics. Accessed: Oct. 17, 2016.
[19] "Oxygen Forensic® analyst,". [Online]. Available: http://www.oxygen-forensics.com/en/. Accessed: Oct. 17, 2016.
[20] majo, "The pioneers of mobile forensics," MSAB, 2016. [Online]. Available: https://www.msab.com/. Accessed: Oct. 17, 2016.
[21] P. Corporation, "Device seizure," [Online]. Available: https://www.paraben.com/device-seizure.html. Accessed: Oct. 17, 2016.
[22] I. I. Yates, "Practical investigations of digital forensics tools for mobile devices," in Proc. of 2010 Information Security Curriculum Development Conference, pp. 156-162, 2010.
[23] C. Labs, "MOBILedit!," 2016. [Online]. Available: http://www.mobiledit.com/forensic. Accessed: Oct. 17, 2016.
[24] S. Goetsch, "Team," in Computer Security, NowSecure, 2016. [Online]. Available: https://www.nowsecure.com/solutions/mobile-app-security-testing/. Accessed: Oct. 17, 2016.
[25] AccessData, "Mobile phone examiner plus," AccessData, 2016. [Online]. Available: http://accessdata.com/solutions/digital-forensics/mpe. Accessed: Oct. 17, 2016.