Comparative Analysis of Android Mobile Forensics Tools

Htar Htar Lwin
Faculty of Computer Systems and Technologies
University of Computer Studies,Yangon
htarhtarlwin@ucsy.edu.mm

Wai Phyo Aung
Department of Automation Control System
Moscow Automobile and Road Construction State Technical University
Russia
myfamily46123@gmail.com

Kyaw Kyaw Lin
Department of Computer Technology
Defence Services Academy
Pyin Oo Lwin
kklin1500@gmail.com

Abstract

This paper performs a comparative analysis of Android mobile forensics tools which are used for acquisition and analyzing of Android mobile devices. The major challenges of Android forensics investigation are manufacturing of Android devices with various operating system versions and there is no single tool which can be used for all sorts of Android devices. Aiming to overcome these challenges and increase more accuracy and integrity in Android forensic investigation, we made comparative analysis on both open source tools and one commercial tool. Logical and physical acquisition methods were utilized to acquire data from Android devices. Android Debug Bridge backup, Linux Data Duplicator utility tool, Magnet Acquire and Belkasoft Acquisition tools were used for acquisition. Two popular analyzing tools such as Autopsy and Belkasoft Evidence Center were utilized to analyze acquired data. The results show that using multiple tools can get more accuracy and integrity of artifacts which is forensically sound.

Keywords: *android forensics, logical acquisition, physical acquisition, forensics investigation*

I. INTRODUCTION

Digital forensics is an exciting, fast-paced field that can have a powerful impact on a variety of situations including internal corporate investigations, civil litigation, criminal investigations, intelligence gathering, and matters involving national security. While the interesting part of Android forensics involves the acquisition and analysis of data from devices, it is important to have a broad understanding of both the platform and the tools that will be used throughout the investigation. A thorough understanding will assist a forensic examiner or security engineer through the successful investigation and analysis of an Android device [1].

An investigator needs to observe about forensics tools in order to select suitable tool based on each scenario. In some cases, investigators use only certain and important data while in other cases full extraction of the physical memory and/or the embedded file system of the mobile is desirable for the potential recovery of deleted data and a full forensic examination. Therefore, the development of guidelines and processes for the extraction and collecting of data from Android mobiles is especially important, and researchers must periodically review and improve those processes according to Android technology development [2].

It is important for an examiner to understand how a forensic tool acquires and analyzes data to ensure nothing is missed and that the data is being decoded correctly. While manual extraction and analysis is useful, a forensic examiner may need the help of tools to accomplish the tasks involved in mobile device forensics. Forensic tools not only save time, but also make the process a lot easier [3]. We need to perform comparative analysis of important tools that are widely used during forensic acquisition and the analysis of Android devices.

As the use of mobile device continues to increase, it is important to efficiently acquire as much information as possible from those devices. In this work, we analyzed Android mobile forensics tools which are used for acquisition and analyzing. We focused on both open source tools and one commercial tool. The rest of this paper is organized as follows. In section 2 we reviewed some papers related with our work. Section 3 presents Android forensic methods. In section 4 we describe our experiment in detail. Comparison of forensic tools are presented in Section 5. We discuss and conclude our work in Section 6. In section 7, we plan our future works.

II. RELATED WORK

In [4], a comparative study of the Android forensic field in terms of Android forensic process for acquiring and analyzing an Android disk image was presented. The challenges of Android forensics, including the complexity of the Android applications, different procedures and tools for obtaining data, difficulties with hardware set up, using expensive commercial tools for acquiring logical data that fail to retrieve physical data acquisition were described. To solve these challenges and achieve high accuracy and integrity in Android forensic processes, a new open source technique was investigated. Manual, Logical and physical acquisition techniques were used to acquire data from an Android mobile device. Following the manual acquisition, logical acquisition was conducted using the AFLogical application in the ViaExtract tool installed on a Santoku Linux Virtual Machine. The image file is then created using the AccessData FTK imager tool for physical acquisition. Four tools were utilized to analyze recovered data: one using ViaExtract on a Santoku Linux Virtual Machine, two using the AccessData FTK Imager, and one using file carving in Autopsy on a Kali Linux Virtual Machine. The results of the analysis demonstrated that the technique can retrieve Contacts, Photos, Videos, Call Logs, and SMSs. Also, the EaseUS Data Recovery Wizard Free tool was used for the recovery of files from the LOST.DIR on external memory.

The paper [5] gives an overview of forensic software tools for Personal Digital Assistants (PDA). A set of generic scenarios was devised to simulate evidentiary situations and applied to a set of target devices to gauge how selected tools react under various situations. The paper summarized those results, giving a snapshot of the capabilities and limitations of present day tools, and also provided background information on PDA hardware and software.

In [6] the author highlighted various techniques available in the market in terms of logical acquisition, physical acquisition and analysis. They deals with the survey of various Android forensics techniques and tools. Forensics methods were discussed with respect to logical and physical acquisition process. They discussed about various tools in both the categories by studying the functionalities existing in the tools and drawbacks. Major tools are capable to provide required results for cybercrime investigation and the evidence and analysis results are acceptable in the court of law. Using these tools the tests are repeatable until unless the evidences are not tampered.

III. ANDROID FORENSIC METHODS

In forensic process, there are five phases such as identification, preservation, acquisition, analyzing and reporting. Identification is determining which device will be processed. The main purpose of the preservation is to maintain the data integrity of the device. We focus on acquisition and analyzing phases in the following sections. After analyzing phases, reporting is imperative.

A. Forensics Acquisition

Forensic acquisition is imaging or extracting data from digital devices. There are three types of acquisition methods: manual, logical and physical. The amount and sort of data that can be acquired may be different based on the type of acquisition method being utilized. Forensic acquisition tools we used in our experiment is shown in Table 1.

TABLE I. FORENSIC ACQUISITION TOOLS

Tools	Logical	Physical
Android Debug Bridge (ADB) Backup	√	
Disk Duplicator (DD)		√
Magnet Acquire	√	√
Belkasoft Acquisition	√	√

Logical acquisition is extracting allocated (non-deleted) data and it accesses the Android file system. Logical acquisition relies on Content Providers to acquire forensically sound data with effective manner. This technique can get only a fraction part of the whole Android file system.

For data acquisition, we need to use Universal Serial Bus (USB) cable to connect the mobile device to forensic workstation. After connecting, the workstation sends command to the device. These commands are interpreted by the device processor. Finally requested data is received from the device's non-volatile memory and sent back to the forensic workstation. This technique writes some data to the mobile device and may change the integrity of the evidence. With logical acquisition tools, deleted data is never accessible.

Physical acquisition is not concerned to the file system. The main advantage of this technique is it can acquire significant amounts of deleted data. When a user delete a file, it is not permanently removed by the Android system. File system only marks data as deleted, and does not actually erase the storage medium as long as there is no need more storage space in the system. As physical forensic methods directly access the storage medium, both the allocated and the unallocated data can be obtained. Physical acquisition is generally difficult and takes long times. Wrong procedure in some steps could lead the device broken.

B. Forensic Analysis

In analyzing step, we need to extract data from acquired image file and analyze using various tools. There is no single tool which can be used for all sorts of Android device and scenario. We need to use multiple tools in order not to lost valuable information. Analysis tools we used in our experiment are listed in Table 2.

TABLE II. FORENSIC ANALYSIS TOOLS

Tools	Open Source	Commercial
Autopsy	√	
Belkasoft Evidence Center		√

IV. EXPERIMENT

The specifications of tested Android mobile devices which we used in our experiment are shown in Table 3. Samsung device has been used since 2015 and Oppo device has been used since 2018. These device are owned by one of the authors.

Table III. Specification of Tested Android Devices

Brand	Samsung	Oppo
Device Name/Model number	Galaxy Note 4/SM-N910H	Oppo A83/CPH1729
Android Version	6.0.1	7.1.1
Baseband version	N910HXXU1DPD2	M_V3_10
Kernel Version	3.10.9-7284779	4.4.22-G2019111
Build Number	MMB29K.N910HXXS2DQH5	
Micro SD Card	16 GB	16 GB

Before the acquisition is started, we isolated the Android devices from networks such as Wi-Fi, Data and Cellular to prevent changing data on the devices. And then we prepared forensics workstation installing forensics tools on a laptop computer with these specifications— Dell Intel (R) Core i7 (2.70 GHz) CPU, 8.0 GB RAM. In our experiment, after identifying the tested devices and configuring forensic workstation, we performed rooting, acquisition and analyzing using various forensic tools.

A. Rooting

On un-rooted devices, data from /data/data directory could not be accessed. Therefore, the tested Android phones were first rooted utilizing Odin3 (version 3.10.6) to upload the root-kit (CF-Auto-Root).

Installing a root-kit enables the user to gain privilege access the Android Operating System, permitting examiners to bypass a few restrictions that the manufacturers put on the device. A rooted Android phone enables the user to access protected directories on the system that hold user data (e.g., /data/data directory) and the entirety of the files in these directories. These data files can hold a lot of that may support an ongoing investigation.

B. Acquisition

We need to maintain the integrity of data by write blocking and calculating cryptographic hash value on the data. Therefore, write blocking and, Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1) were used to calculate hash values and check integrity of the data.

ADB Backup. In order to acquire logical data, we used three tools such as ADB Backup, Belkasoft Acquisition and Magnetic Acquire tools. For physical acquisition, Linux DD, Belkasoft Evidence Center and Magnetic Acquire tools were used. Belkasoft Evidence Center and Magnetic Acquire can be used for both logical acquisition and physical acquisition.

To get the logical data of the device, we used the ‘adb backup’ command and also unpacked into ‘.tar’ as follow.

```
adb backup -f e:/backup.ab –shared –all
java –jar abe.jar unpack backup.ab backup.tar
```

DD tool. We used the following commands to get physical image of the tested phones. Firstly, we need to know which partition holds the data. So we used ‘mount’ command in first command window to take a look at the location of our desire data partition.

```
adb –d shell
su
mount
```

From output of ‘mount’, we knew that data is located in partition ‘mmcblk0p21’. In second command window, we did TCP port forwarding in order to transfer extracted data image to the forensics work station.

```
adb forward tcp:8888 tcp:8888
```

In first command window again, we used ‘dd’ command to get image of data partition.

```
dd if=/dev/block/ mmcblk0p21 | busybox nc -l -p 8888
```

In second command window, we used netcat.exe to transfer acquired image file to the forensics work station. Our image files were named as dd_data.dd and O_dd_data.dd, respectively.

```
C:\netcat\nc64 127.0.0.1 8888 > dd.dd
```

Following is alternative to transfer image file to the work station instead of TCP traffic.

```
dd if=/dev/block/mmcblk0p21 of=/sdcard/dd.img
bs=512 conv=notrunc, noerror,sync
adb pull /sdcard/dd.img
```

We calculated SHA1 hash values and checked integrity of acquired image using these hash values.

Magnet Acquire. By using several different methods of extraction, Magnet Acquire can retrieve as much data as possible, given the enhanced security on Android. Magnet Acquire can also capture images from common storage drives. In order to obtain logical and physical images of device, we also used Magnet Acquire. It calculated MD5 and SHA1 hash values. Finally we checked integrity of acquired image using these hash values. Acquisition information of Magnet is listed in Table 4 and 5.

TABLE IV. ACQUISITION INFORMATION WITH MAGNET (SAMSUNG)

	Logical	**Physical**
File name	Magnet.tar	.raw (MMCBLK0) .raw (MMCBLK1)
Size	15.0 GB	29.1 GB (MMCBLK0) 14.8 GB (MMCBLK0)
Time taken	01:00:0	3:46:07

TABLE V. ACQUISITION INFORMATION OF MAGNET (OPPO)

	Logical	**Physical**
File name	O_Magnet.ab	.raw (MMCBLK0) .raw (MMCBLK1)
Size	5.0 GB	9.7 GB (MMCBLK0) 4.9 GB (MMCBLK0)
Time taken	00:20:0	1:15:03

Belkasoft. This tool can be used for ADB backup, Agent backup, DD backup, Odin RAM image and MTP backup. ADB backup is a method of acquiring data from an Android device that utilizes pre-installed ADB-services. Agent backup is a method for data acquisition from Android devices by collecting user data with a custom Agent-application. DD backup is a method of acquiring data from an Android device that creates a complete physical copy of its permanent. Odin RAM-imaging acquisition method is based on Odin commands utilization. We used ADB backup for logical and DD backup for physical in our experiment. Acquisition information of Belkasoft is listed in Table 6 and 7.

TABLE VI. ACQUISITION INFORMATION WITH BELKASOFT (SAMSUNG)

	Logical	**Physical**
File name	Blks.ab	Blks.dd
Size	1.41 GB	25.1 GB
Time taken (hh:mm:ss)	00:11:00	02:02:02

Table VII. Acquisition Information with Belkasoft (oppo)

	Logical	**Physical**
File name	O_Blks.ab	O_Blks.dd
Size	1.6 GB	8.3 GB
Time taken (hh:mm:ss)	00:12:00	00:40:00

C. Analysis

For analysis of acquired data from previous acquisition methods, we used Autopsy and Belkasoft Evidence Center tools. We selected ‘Magnet.tar’ obtained from Magnet Acquire tool for logical data analyzing because the size of this file is maximum comparing to other files. It may contain more information. We also selected ‘Blks.ab’ as a logical file to be analyzed. As a physical image we choose ‘dd.dd’ getting form DD utility.

Autopsy. Autopsy is a free and open source analysis tool. Autopsy can analyze most common Android file systems. Ingest Modules are tools built into Autopsy that can be run when the case is started, or at any point afterward. There are the 17 ingest modules in Autopsy version 4.13.0. We used 15 modules in the experiment. Even though the case is still being loaded and Ingest Modules being run, we can begin analyzing the case. In our experiment, we found nothing artifacts on ‘Blks.ab’. Artifacts we have got from ‘Magnet.tar’ and ‘dd.dd’ by analyzing Autopsy tool are shown in Table 8 and 9, respectively.

TABLE VIII. ARTIFACTS OF MAGNET.TAR WITH AUTOPSY

Artifacts of Magnet.tar	**Amount (Samsung)**	**Amount (Oppo)**
Accounts	871	1161
Archives	178	59
Audio	1152	384
Contacts	615	820
Databases	653	217
Documents	1274	424
Encryption Suspected	4	5
Executable	62	20
EXIF Metadata	479	159
Extension Mismatch Detected	2115	705
Images	7872	2624
Install Applications	48	64

Keyword Hits	9782	3260
Videos	8	10

TABLE IX. ARTIFACTS OF PHYSICAL IMAGE WITH AUTOPSY

Artifacts of dd.dd	Amount (Samsung)	Amount (Oppp)
Accounts	40	53
Archives	907	302
Audio	2331	777
Call Logs	1000	333
Contacts	1023	1364
Databases	669	223
Deleted Files	37964	12654
Documents	1171	390
Download Source	79	105
Encryption Suspected	4	5
Executable	65	21
EXIF Metadata	1	1
Extension Mismatch Detected	2115	705
Images	16053	10702
Install Applications	111	148
Messages	283	377
OS Information	1	1
Videos	21	28
Web Bookmarks	10	13
Web Cookies	3213	1071
Web Downloads	152	304
Web Form Autofill	754	1006
Web History	291	388

Belkasoft. Belkasoft Evidence Center is flagship digital forensic suite. The product makes it easy for an investigator to perform all steps of modern digital investigation such as: Data acquisition from various devices and clouds, artifact extraction and recovery, analysis of extracted data, reporting, and sharing evidence. Artifacts we have got from analyzing with Belkasoft are shown in Table 10, 11 and 12, respectively.

TABLE X. ARTIFACTS OF BLKS.AB WITH BELKASOFT

Artifacts of Blks.ab	Amount (Samsung)	Amount (Oppo)
Audio	3	9
Cache	52	69
Calendar	32	42
Contacts	10	13
Cookies	1908	636
Documents	715	953
Downloads	584	778
Encrypted files	4	5
Favorites	20	6
Form values	764	254
Geo location data	4	8
Installed applications	269	358
Most visited sites	2	2
Passwords	70	23
Pictures	2515	3353
URLs	846	282

TABLE XI. ARTIFACTS OF MAGNET.TAR WITH BELKASOFT

Artifacts of Magnet.tar	Amount (Samsung)	Amount (Oppo)
Audio	4	12
Cache	204	68
Calendar	32	42
Calls	4289	1429
Chats	25642	8547
Cloud Services	232	77
Contacts	8281	11041
Cookies	3781	1260
Documents	1688	562
Downloads	581	193
Encrypted files	63	21
Favorites	24	32
File transfers	2750	916
Form values	767	255
Geo location data	54	72
Herrevad	208	69
Installed applications	272	362
Instant messengers	28720	14360
Mailboxes	967	1289
Network connections	208	277
Other files	248	82
Passwords	70	23
Pictures	22142	7380
Sessions	1	1
SMS	4821	2410
Thumbnails	18	6
URLs	780	260
Videos	35	11
Voice mail	28	56
Wi-Fi connections	47	62
Wpa_supplicant.config	47	62

TABLE XII. ARTIFACTS OF DD.DD WITH BELKASOFT

Artifacts of dd.dd	Amount (Samsung)	Amount (Oppo)
Audio	4	12
Cache	218	72
Calendar	33	42
Calls	3875	1291
Chats	25055	8351
Cloud Services	232	77
Contacts	8292	11041
Cookies	3739	1246
Documents	6250	2083
Downloads	583	193
Encrypted files	243	21
Favorites	24	32
File transfers	2687	895
Form values	767	255
Geo location data	53	72
Herrevad	208	69
Installed applications	253	337
Instant messengers	27996	13998
Mailboxes	1006	1289
Network connections	208	277
Other files	250	82
Passwords	70	23
Pictures	22332	7444
Sessions	1	1
SMS	4902	2410
Thumbnails	30	6
URLs	984	260
Videos	10	11
Voice mail	28	56
Wi-Fi connections	46	62
Wpa_supplicant.config	46	62

V. COMPARISON OF FORENSICS TOOLS

According to experiment results, we performed comparative analysis on both acquisition and analyzing tools.

A. Acquisition Tools

As ADB Backup is command line tool, forensic examiners need to familiar with commands. Android Software Development Kit (SDK) is needed to be downloaded and located in forensic workstation because ADB Backup tool is included in SDK. Acquisition time is exactly 3 hours in Samsung and 1 hour in Oppo. It took longer time than other tools.

As Magnet and Belkasoft are GUI tools, they are user friendly and easy to use. Magnet can be used per request to their team. Magnet took exactly one hour in Samsung and 20 minutes in Oppo for logical acquisition.

Belkasoft is commercial tool. We used trial version requesting to their team. For Samsung, acquisition time is just 10 minutes. Acquired size of data is only 1.41 GB. The size of data is same with one which we tried second times to be sure the size of data. Comparison of logical acquisition tools is listed in Table 13 and 14, respectively.

TABLE XIII. COMPARISON OF LOGICAL ACQUISITION TOOLS (SAMSUNG)

	ADB Backup	Magnet	Belkasoft
Type	.ab./.tar	.tar	.ab
Size	11.6 GB	15.0 GB	1.41 GB
Time (hh:mm:ss)	03:00:00	01:00:00	00:10:00
GUI	No	Yes	Yes
Cost	Free	Request	Trial

TABLE XIV. COMPARISON OF LOGICAL ACQUISITION TOOLS (OPPO)

	ADB Backup	Magnet	Belkasoft
Type	.ab./.tar	.tar	.ab
Size	3.8 GB	5.0 GB	1.6 GB
Time (hh:mm:ss)	01:00:00	00:20:00	00:12:00
GUI	No	Yes	Yes
Cost	Free	Request	Trial

DD is Linux utility tool and can be used free of charge. Examiners need to understand commands to use it. It took longer time than other tools. We can choose which partition we want to be acquired.

With Magnet tool, there is no option to choose data partition. All data of device is imaged. It divided the image file into two files: MMCBLK0.raw and MMCBLK1.raw. MMCBLK0.raw contains data from user data partition. Therefore we focused on this file. Size of the files are much larger than other tools because it imaged all data of the whole device.

Belkasoft image size is the same with DD image but time taken is only half of it. We can also choose desire partition such as user data partition. Comparison of physical acquisition tools is listed in Table 15 and 16, respectively.

TABLE XV. COMPARISON OF PHYSICAL ACQUISITION TOOLS (SAMSUNG)

	DD	Magnet	Belkasoft
Type	.dd/.img	.raw (2 files)	.dd
Size	25.1 GB	29.1 GB 14.8 GB	25.1 GB
Time (hh:mm:ss)	05:00:00	03:46:07	02:02:02
GUI	No	Yes	Yes
Cost	Free	Request	Trial

TABLE XVI. COMPARISON OF PHYSICAL ACQUISITION TOOLS (OPPO)

	DD	Magnet	Belkasoft
Type	.dd/.img	.raw (2 files)	.dd
Size	8.3 GB	9.7 GB 4.9 GB	8.3 GB
Time (hh:mm:ss)	01:40:00	01:15:03	00:40:00
GUI	No	Yes	Yes
Cost	Free	Request	Trial

B. Analyzing Tools

In analysis of logical image, 14 categories of artifacts was found by Autopsy. Belkasoft found 31 categories. In the findings of Belkasoft, there are voice mail and Instant Messages such as Viper, Facebook and Hangout. Although Belkasoft found encrypted passwords, Autopsy could not do it. Comparison of analysis tools for logical data is listed in Table 17 and 18, respectively.

TABLE XVII. COMPARISON FOR LOGICAL DATA (SAMSUNG)

	Autopsy	Belkasoft
Categories	14	31
Artifacts	25113	107004
Report	Yes	Yes
Time (hh:mm:ss)	00:39:00	00:40:00
GUI	Yes	Yes
Cost	Open source	Trial

TABLE XVIII. COMPARISON FOR LOGICAL DATA (OPPO)

	Autopsy	Belkasoft
Categories	14	31
Artifacts	9912	51237
Report	Yes	Yes
Time (hh:mm:ss)	00:15:00	00:20:00
GUI	Yes	Yes
Cost	Open source	Trial

In analysis of physical image, 23 categories of artifacts were found by Autopsy. Belkasoft found 31 categories. Although Belkasoft found encrypted passwords, Autopsy could not do it. Comparison of analysis tools for physical image is listed in Table 19 and 20, respectively.

TABLE XIX. COMPARISON FOR PHYSICAL IMAGE (SAMSUNG)

	Autopsy	Belkasoft
Categories	23	31
Artifacts	68258	110425
Report	Yes	Yes
Time (hh:mm:ss)	01:49:00	00:45:00
GUI	Yes	Yes
Cost	Open source	Trial

TABLE XX. COMPARISON FOR PHYSICAL IMAGE (OPPO)

	Autopsy	Belkasoft
Categories	23	31
Artifacts	30971	52070
Report	Yes	Yes
Time (hh:mm:ss)	00:49:00	00:30:00
GUI	Yes	Yes
Cost	Open source	Trial

VI. DISSCUSSION AND CONCLUSION

We used various free and commercial mobile forensics tools focusing on Android devices. Because of there are large number of models and manufacturer specific mobile devices, tools do not provide and have for same procedure for digital investigation process. Each tool has own procedure to acquire and analyze the data in forensically sound manner.

In acquisition process, we used ADB Backup, DD and Manget Acquire tools which are open source tools and, Belkasoft which is commercial tool. ADB Backup and DD is totally free for all users but Manget Acquire is free for only members of forensics community. Therefore, we need to request by giving our information to use Manget Acquire. For testing purpose, Belkasoft can be used for one month requesting their team. Because of ADB Backup and DD are command utilities, they are not user friendly compare to Magnet Acquire and Belkasoft which are GUI tools. ADB Backup can be used for only logical acquisition but Magnet Acquire and Belkasoft can be used for both logical and physical acquisition. ADB Backup and DD took more time than Magnet Acquire and Belkasoft for acquisition on same device. In analysis process, we used Autopsy open source tool and Belkasoft Evidence Center commercial tool. Autopsy was built with features available in commercial tools. However, Autopsy cannot extract encrypted passwords like Belkasoft can. Compare to open source tools, we can see that commercial tools can save time and, get more data and more accurate results.

According to the results of Analyzing tools, we can conclude that there are different artifacts we found based on utilized tools. Amount of data are also different. In here, we'd like to recommend Magnet Acquire for logical acquisition because it is open source and obtained much more data than Belkasoft. For physical acquisition, DD tool is more preferable because it is open source tool and can acquire data exactly like a Belkasoft commercial tool. As an analyzing tool, Belkasoft is suitable. In trial version, even though its generated reports contain only random 50% of extracted data, we have found comparable artifacts with other tools. However, there is no single tool which can get and analyze all sort of data. We'd better use multiple tools to get integrity and accurate result.

VII. FURTHER WORK

Our group will perform with other acquisition and analyzing open source and commercial tools in future.

ACKNOWLEDGMENT

Our special thanks are due to Maria Khripun, Marketing Manager, Belkasoft, and Magnet Forensics Team for supporting their tools.

REFERENCES

[1] Andrew Hoog and John McCash, "Android Forensics (Investigation, Analysis and Mobile Security for Google Android)", Elsevier.

[2] L. Xue, C. Qian, H. Zhou, X. Luo, Y. Zhou, Y. Shao, and A.T. Chan. "NDroid: Toward tracking information flows across multiple Android contexts." IEEE Transactions on Information Forensics and Security, 14(3), 2018, pp. 814-828.

[3] Satish Bommisetty, Rohit Tamms and Heather Mahalik, "Practical Mobile Forensic", Packt Publishing Ltd, July 2014.

[4] Aiman Al-Sabaawi, Brisbane, and Australia "A Comparison Study of Android Mobile Forensics for Retrieving Files System", August 2019.

[5] Wayne Jansen and Rick Ayers, "An Overview and Analysis of PDA Forensic Tools"

[6] Venkateswara Rao V. and Chakravarthy, "Survey on Android Forensic Tools and Methodologies", International Journal of Computer Applications (0975 – 8887) Volume 154 – No.8, November 2016