iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** X **Month of publication:** October 2023

DOI: https://doi.org/10.22214/ijraset.2023.56106

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue X Oct 2023- Available at www.ijraset.com

Android Smart Phone Forensics using Open Source Tools

Austin Makate[1], Martin Muduva[2], Ronald Chiwariro[3], Animesh Kumar Agrawal[4], Pallavi Khatri[5]
[1]*University of Zimbabwe,* [2]*Midlands State University,* [3]*Department of Computer Science and Engineering, Jain University, Bangalore, India,* [4,5]*National Forensics Science University, Gujarat, India.*

Abstract: ***Mobile Smart Phone Technology (MSPT) is one of the greatest civilizations in history, but, unfortunately, the same is being taken advantage of and unseemly conduct is inevitable. Android Technology is fast evolving and dominating over its competitors because of its features, open-source architecture and ease of customization. In addition, Android Apps often use Self-Signed certificates unlike Apple Apps bound by Certificate Authority. To overcome the challenges of security in the newer versions of Android, the concept of a Virtual Android phone using a Genymotion Emulator is adopted. This approach will help in analyzing the latest phones through open-source tools without the need to physically procure them. The virtual phone interface is the same as the physical phone but it obviates the need to root/bypass the phone security, thereby allowing the researcher to concentrate on developing techniques for extracting forensic artifacts. Open source tools are used to carry out the research and a comparative analysis is done so that a combination of tools can be used to extract the maximum artifacts from the phone.***

Keywords: Android Forensics, Smartphone Forensics, Open Source Tools.

I. INTRODUCTION

Law enforcement agents consider any MSPT to be a significant source of evidence when a crime has been committed. According to [1], the comprehensive review of mobile device versus desktop usage reflected that mobile devices successfully compete for user's attention and globally, 68.1% of all website visits in 2020 came from mobile devices. MSTPs are slowly replacing their desktop counterparts in human-to-computer interactions and automatically have become large digital storage vaults that store personal and professional secrets. It is therefore pertinent to invest more time towards finding efficient techniques in extracting and analyzing data on MSPTs particularly biased towards Android Technology because it has the largest market share the world over. In the recent publication by [2], Android OS had the largest market share of 71.74%, Fig. 2 is indicative.

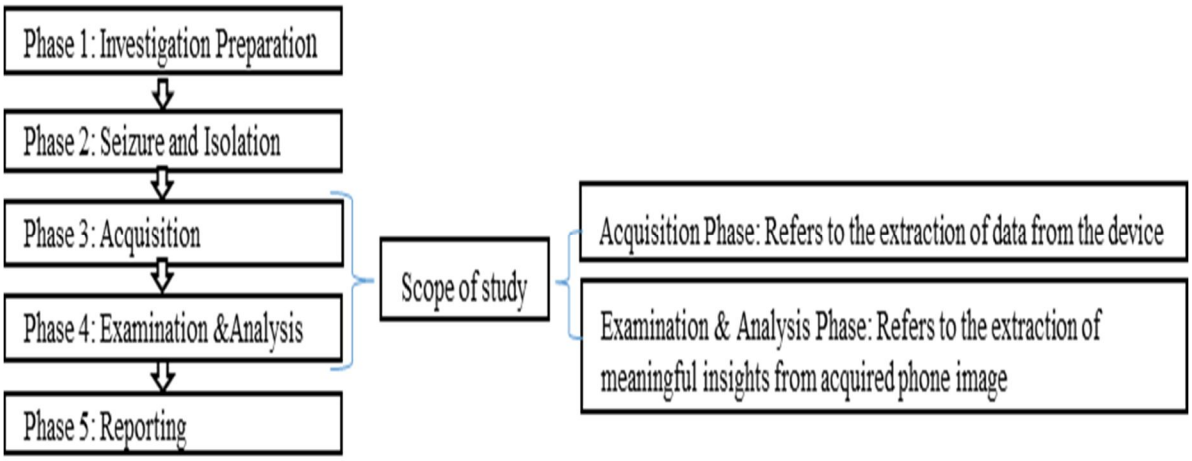


Fig. 1 Mobile Forensic Phases

According to [3], mobile device forensics is a branch of digital forensics which deals with extracting, recovering and analyzing digital evidence or data from a mobile device under forensically sound conditions. There are generally five phases of mobile forensics as shown in Fig. 1. In this study, the researcher discusses the potential forensic process related to only the acquisition and examination & analysis as the other phases were not relevant to the study in particular.

©IJRASET: All Rights are Reserved

Fig. 2 Mobile OS Market Share Worldwide. Source Statcounter [2]

II. THEORETICAL BACKGROUND

A lot of scholars and Cyber Security specialists have been researching Android Smartphone forensics using open-source tools and research in the subject area is still ongoing. This effort has gone a long way towards availing economic solutions within the android forensics fraternity. According to [4] [5], several different types of data extractions determine how much data is obtained from the device. They state that Physical acquisition contains most data followed by File System acquisition, Logical Acquisition and Photographic documentation respectively. The extraction of data can be affected by three things are Type of Mobile Device, the Diversity of Forensic Tools and the Physical State of Devices. In their study, [6] worked on finding the best method to produce more evidential artefacts from android technology. The research was performed on Alcatel One Touch 6012x (4.2.2). Various open source tools were used including manual extraction through adb pull and dd command. The analysis concluded that a proper step-by-step combination of tools is effective in getting meaningful insights. The best solution for extracting data from various Android mobile devices was delved into by [7]. A comparative study of UFED, Paraben, XRY and Mobiledit was done on four various Android phones. It turned out that commercial tools were a critical solution for data acquisition in cases where Android devices are not rooted.

However, the logical acquisition was deemed a good alternative in the absence of expensive commercial tools. The paper by [8] sought to find a convenient way to bypass rooting by use of custom recovery. Team Win Recovery Project (TWRP) was utilized to unlock the bootloader and put a custom ROM in order to access root privilege and extract a disk dump via dd command. This method successfully facilitated forensics to take place and was further recommended for trial with emerging Android Technologies. The same concept was discussed by [9] in their study and stock ROM and custom ROM ware explained on how they can facilitate a step-by-step rooting procedure. In their research paper, [10] explored on various acquisition techniques in which a comparative study was done to come up with a better approach. Commercial tools offered a better solution than open-source tools in which software-based acquisition was found more feasible than hardware besides it posing a risk of compromising the integrity of the original image. The research concluded that no one tool does it all.

A comparison between Paraben E3:DS and Autopsy was carried out by [11] to analyze a logical image that had been acquired on Nexus 6P (V7.1.2) using the Titanium backup application. The research focused on the extraction of evidential artefacts from applications in which Paraben E3:DS produced the best results. The study concluded that more artefacts can still be extracted provided the rightful forensic tools are identified. The effectiveness of rooting in the recovery from anti-forensics was done by [12]. The approach taken was to compare results from Logical and Physical images of Samsung Note 4 (6.0.1). It was discovered that even after factory resetting the phone, the physical image was able to recover both existing and deleted data but the logical image recovered only existing data. According to [13] [14], adb pull particularly serves the purpose of transferring the files from the mobile device under investigation to the forensic station workstation. Because many partitions require root permission to be accessed, it is therefore pertinent to first root the mobile device before pulling logical files. Conferring from [15] [16], Android Debug Bridge (ADB) is a tool by Android Software Developers Kit (SDK) and is utilized to facilitate a smooth connection between an Android device and a computer in order to extract various images from a mobile device. The prerequisite for using adb is to first enable the USB debugging mode on the Android device. As stated by [17] [18], rooting allows an examiner to access elevated privileges on a mobile device which would otherwise not have been accessed in normal mode. It can be used legally or illegitimately.

It is clear from this review of literature that Android Technology is fast evolving and more research needs to be conducted. In all the papers reviewed, the highest version of Android worked with was 7.1.2 yet according to [19], the latest release of Android is version 12. From this gap, the researchers derived the following Hypothesis: Open Source mobile forensic tools are somehow relevant to preceding Android Technologies and can still be relevant to emerging Android Technologies. This assumption was the centre of the investigation and was tested for proof throughout the study with a set of selected open-source tools.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

III. PROPOSED WORK AND METHODOLOGY

The proposed methodology sought to provide a systematic step by step procedure of testing the set Hypotheses throughout the investigation. Fig. 3 shows the flow chart of proposed work.

Step by step Methodology

Step 1: Create a Santoku virtual forensic workstation on Oracle VM VirtualBox.
Step 2: Create two emerging Android phones with Genymotion Emulator.
Step 3: Populate the known data set in the Virtual phone.
Step 4: Random selection of open-source tools and techniques to be used

Scenario 1: Perform Logical Acquisition on Rooted Phone

Step 5: Perform Photographic Documentation/ manual extraction.
Step 6: Perform logical acquisition using open-source tools.
Step 7: Analyze logical the image with open-source analytical tools.
Step 8: Draw a conclusion for scenario 1.

Scenario 2: Perform Physical Acquisition on Rooted Phone

Step 9: Perform physical acquisition using open-source tools.
Step 10: Analyze Physically acquired the image with open-source tools.
Step 11: Draw a conclusion for Scenario 2.

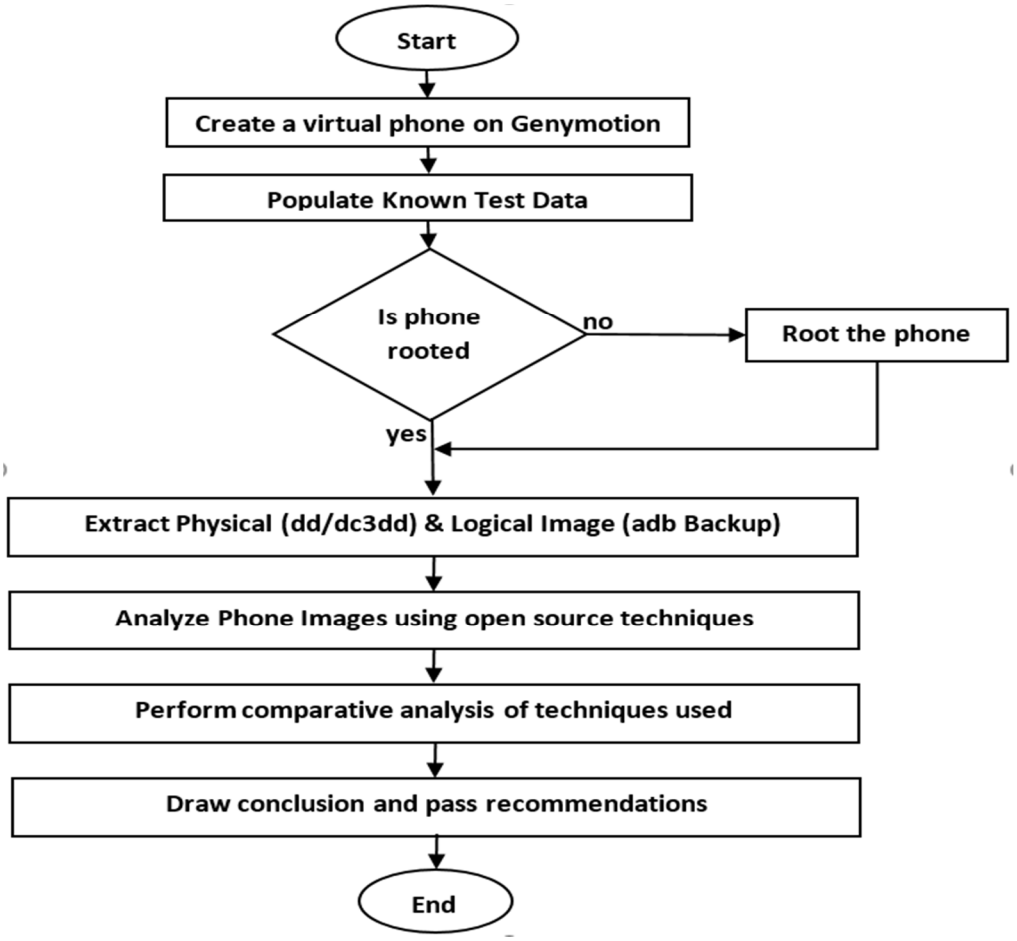


Fig. 3: Flow chart of the proposed work

IV. PRELIMINARY WORK

The preliminary work covered the assessment done towards selecting the open source tools considered for data extraction and examination & analysis. Tables 1, 2 and 3 demonstrates the comparative analysis on the open source tools considered for Logical acquisition, Physical acquisition and Examination and analysis respectively.

Table 1: Comparative Analysis for Logical Acquisition Tools

Items	Logical Acquisition Tools and Techniques Considered		
	adb pull	adb backup	AFLogical-OSE
Rooting	Need Rooting	Need Rooting	Need Rooting
Data Access	adb daemon	adb daemon	Content provider
Integrity	Partially preserve	Partially preserve	Partially preserve
Compatibility	Compatible	Partially compatible	Not compatible

Table 2: Comparative Analysis for Physical Acquisition Tools

Items	Physical Acquisition Tools and Techniques Considered		
	dd command	dd command+Busy Box	FTK Imager
Rooting	Need Rooting	Need Rooting	No need
Integrity	Partially preserve	Partially preserve	Partially Preserve
Compatibility	Compatible	Compatible	Not compatible

Table 3: Comparative Study for Examination and Analysis Tools

Image format	Physical Acquisition Tools and Techniques Considered			
	Autopsy	FTK Imager	DB Browser SQLite	SIFT
.db compatibility	Yes	Yes	Yes	No
.dd compatibility	Yes	Yes	No	Yes
.ab compatibility	Yes	Yes	No	Yes

V. EXPERIMENTAL SETUP

A. Lab Setup

Initially, an Acer Aspire A515-56 11th Gen Intel® Core i5-1135G7 @ 2.4GHz, with 8 Logical Processors, Memory 20GB DDR4 and 512GB SSD was set up. Oracle VM VirtualBox, Santoku Mobile Forensic workstation, and Genymotion were installed and Samsung Galaxy S8 (8.1) and Xiaomi Redmi Note 7 (9) virtual phones were setup. Thereafter, population of known test data was done on the two phones.

B. Logical Acquisition with adb pull

The file hierarchy of both phones was studied and the target partition hosting pertinent logical data was identified as **/data/media/0.** After enabling the USB debugging, this directory was successfully pulled using the following command:

adb pull /data/media/0

The directory contained all logical images and databases from various applications.

C. Physical Acquisition with dd command + BusyBox

The command ran on the shell terminal of the Android device was:

dd if=/dev/block/sdb3 | busybox nc –l –p 8888

The commands ran on Santoku forensic workstation shell terminal receiving the .dd were:

adb forward tcp:8888 tcp:8888
nc 127.0.0.1 8888 > image2.dd

D. Examination & Analysis of Logical files

By design, the adb pull command extract logical files which are in a format ready to view in GUI mode of various desktop OS. Fig 4 shows some of the artefacts recovered from Samsung Galaxy S8 and these include Pictures taken by Camera, downloaded files and all WhatsApp generated artefacts. Logical artefacts which were in form of databases were further analyzed using DB Browser SQLite. Figs 5, 6 and 7 below show evidential artefacts of Call logs, Contacts and SMS found in the Samsung Galaxy S8 respectively.

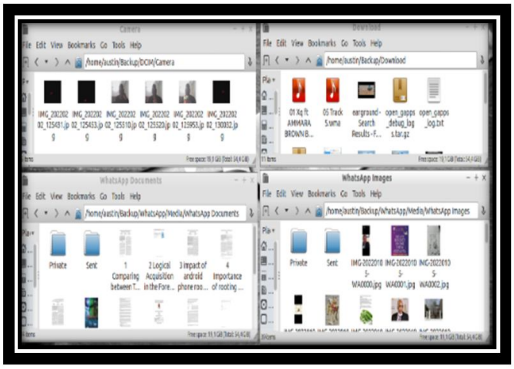


Fig 4 Logical Artefact in GUI for WhatsApp

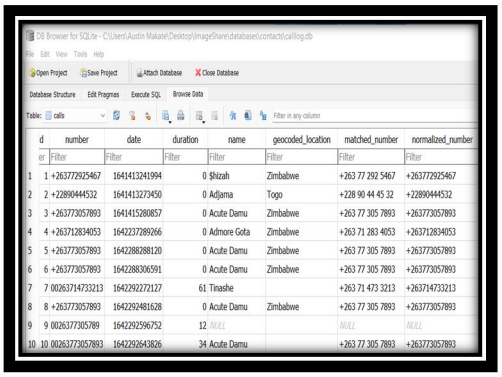


Fig 5: Call log

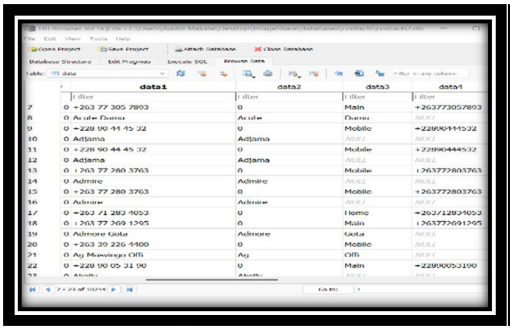


Fig 6 Contacts in phone

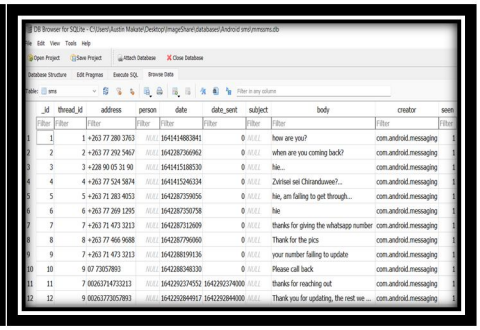


Fig 7 SMS Log

E. Examination & Analysis of Hex Dumps

The open source tools used to perform analysis of extracted Hex Dumps were Autopsy, FTK Imager and SIFT. As can be seen from Fig 8 and 9, Autopsy failed to parse raw data into meaningful insights hence no evidential artifacts were realized from this tool. With the aid of FTK Imager, image2.dd was converted into image2.vmdk and s8.E01 formats in an effort to access the best format in which Autopsy would handle. Despite having various image format, according to this study, not much evidential artifacts came out from Autopsy, instead it only picked much of the application installed on the Samsung Galaxy S8 but failed to parse properly the user data that was associated with the applications. Lately Autopsy had been effectively parsing much of the raw data into meaningful insights on preceding Android Technologies but from this study not much came out. It is the researcher's strong belief that the technology associated with image files examined was a bit complex to be handled with Autopsy.

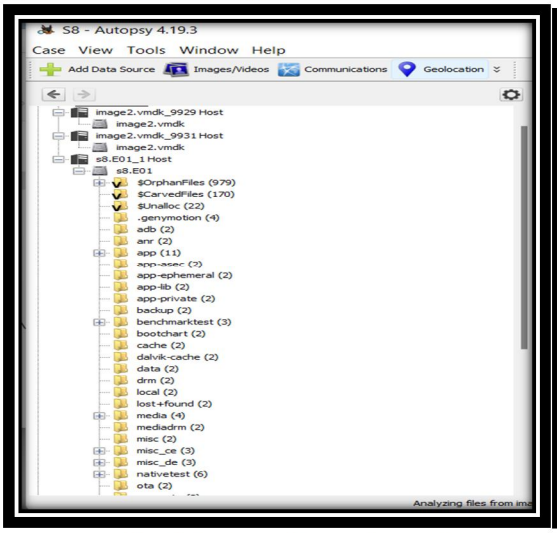


Fig. 8 Autopsy General output

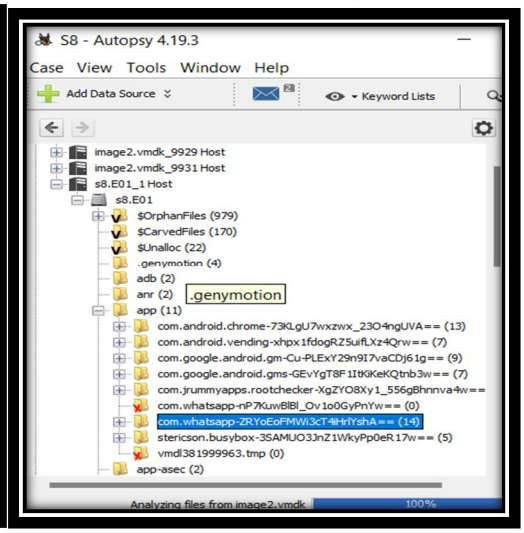


Fig. 9 Installed Apps

Analysis made by SIFT using the ewfmount method is brought out as depicted in Fig. 10. This method failed and gave an error, this error normally happens when SIFT fails to support a particular file system format. FTK was used to convert the image into other file formats like (.E01), (.vmdk) and (.001) but still to no avail.

Fig. 11 shows the second method of SIFT failing to mount the physical image of Samsung Galaxy S8 despite it being converted to .001 format. Both the two methods demonstrated were repeated in the same order to analyze the physical image of the Xiaomi Redmi Note 7 and again no results were obtained.

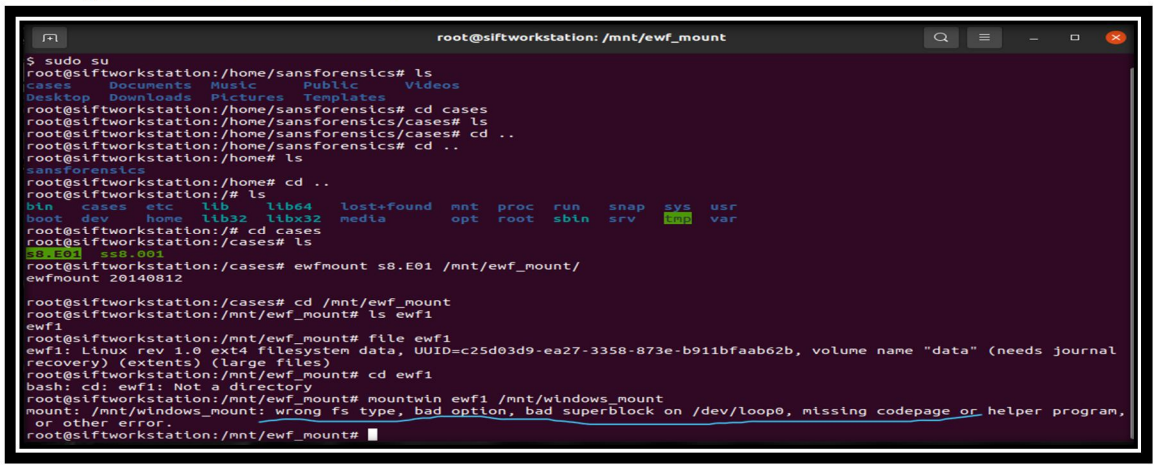


Fig. 10 First Method: (ewfmount)

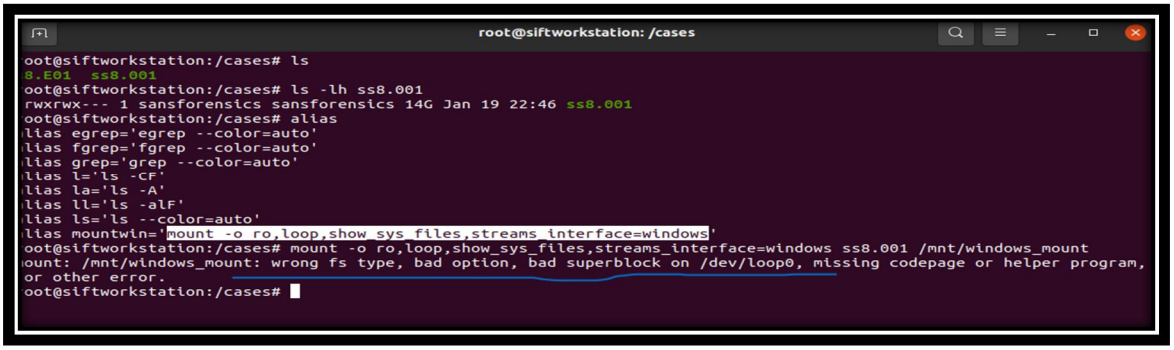


Fig. 11 Second Method: (mount -o ro,loop,show_sys_files,streams_interface=windows)

Just like Autopsy, FTK imager was able to recognize much of the applications installed on devices being examined yet it failed to parse much of the raw data into meaningful insights. Fig. 12 illustrates an error in continuation in the examination of image2.dd from Samsung Galaxy S8. After several attempts in running the same process, the same error was incurred yet this same tool used to handle well physical images of preceding Android Technologies. In view to this, the researcher concluded that there could be some antiforensic complexity associated with physical images from emerging Android Technologies which FTK Imager is currently failing to handle.

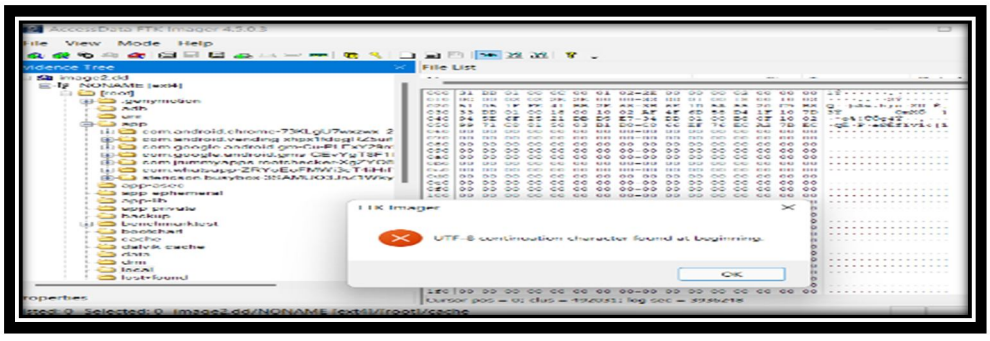


Fig. 12 image2.dd Analyzed by FTK

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue X Oct 2023- Available at www.ijraset.com

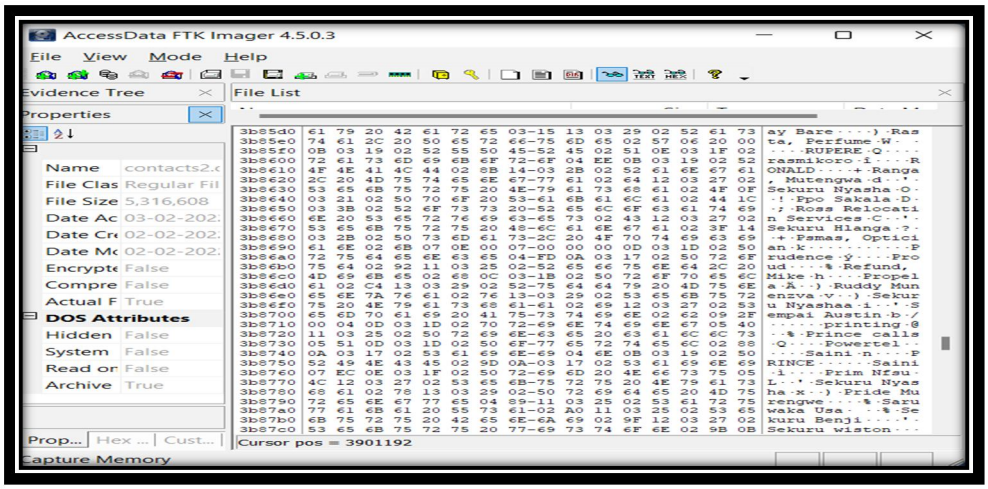


Fig. 13 SMS Captured by FTK

Fig. 13 shows some of the SMS artefacts picked by FTK Imager after examining a physical image from the Samsung Galaxy S8. To some extent this result confirms the notion that FTK had some challenges in parsing some of raw data of emerging Android Technologies into meaningful insights. Had FTK imager been much more relevant, it could have come up with more meaningful insights from the image2.dd file after the examination.

VI. RESULTS

Results are drawn from experimental setup in which each and every tool considered for this study was tested for its relevance to emerging Android Technology. Two virtual phones i.e. Samsung Galaxy S8 (V8.1) and Xiaomi Redmi Note 7 (V9.0) were particularly setup to emulate emerging Android technologies. Table 4 is a reflection of summary results noted after data acquisition and Analysis was done on the two phones in question. Each tool that has a green tick underneath it is somehow relevant to emerging Android Technologies. The green tick with a gray background shows that the tool is relevant through a combination with another tool. For example, DB Browser SQLite produces a call log list after analyzing a call log database which is a product of adb pull technique. The black X shows absolute failure by a tool to extract a desired evidential item. An X with a gray background reflects failure by a tool because of compatibility issues with the virtual platform.

Table 4 Summary of Results

ITEM	Tools being tested for relevance with emerging Android Technology								
	Data Acquisition Tools				Examination & Analysis Tools				
	adb pull	adb backup	dd cmd	Busybox + dd cmd	AFLogical	FTK	Autopsy	SIFT	SQLite
Logical image	✓	✗	✗	✗	✗	✗	✗	✗	✗
Physical image	✗	✗	✗	✓	✗	✗	✗	✗	✗
Call logs	✓	✗	✗	✗	✗	✗	✗	✗	✓
Sms chats	✓	✗	✗	✓	✗	✓	✗	✗	✓
Pictures	✓	✗	✗	✗	✗	✗	✗	✗	✗
Videos	✓	✗	✗	✗	✗	✗	✗	✗	✗
Audio	✓	✗	✗	✗	✗	✗	✗	✗	✗
Contacts	✓	✗	✗	✓	✗	✓	✗	✗	✓

©IJRASET: All Rights are Reserved

KEY

✗	The tool was not relevant because of compatibility issues
✗	The tool was absolutely not relevant
✓	The tool was relevant by combination with another tool
✓	Absolute relevance

VII. LIMITATIONS

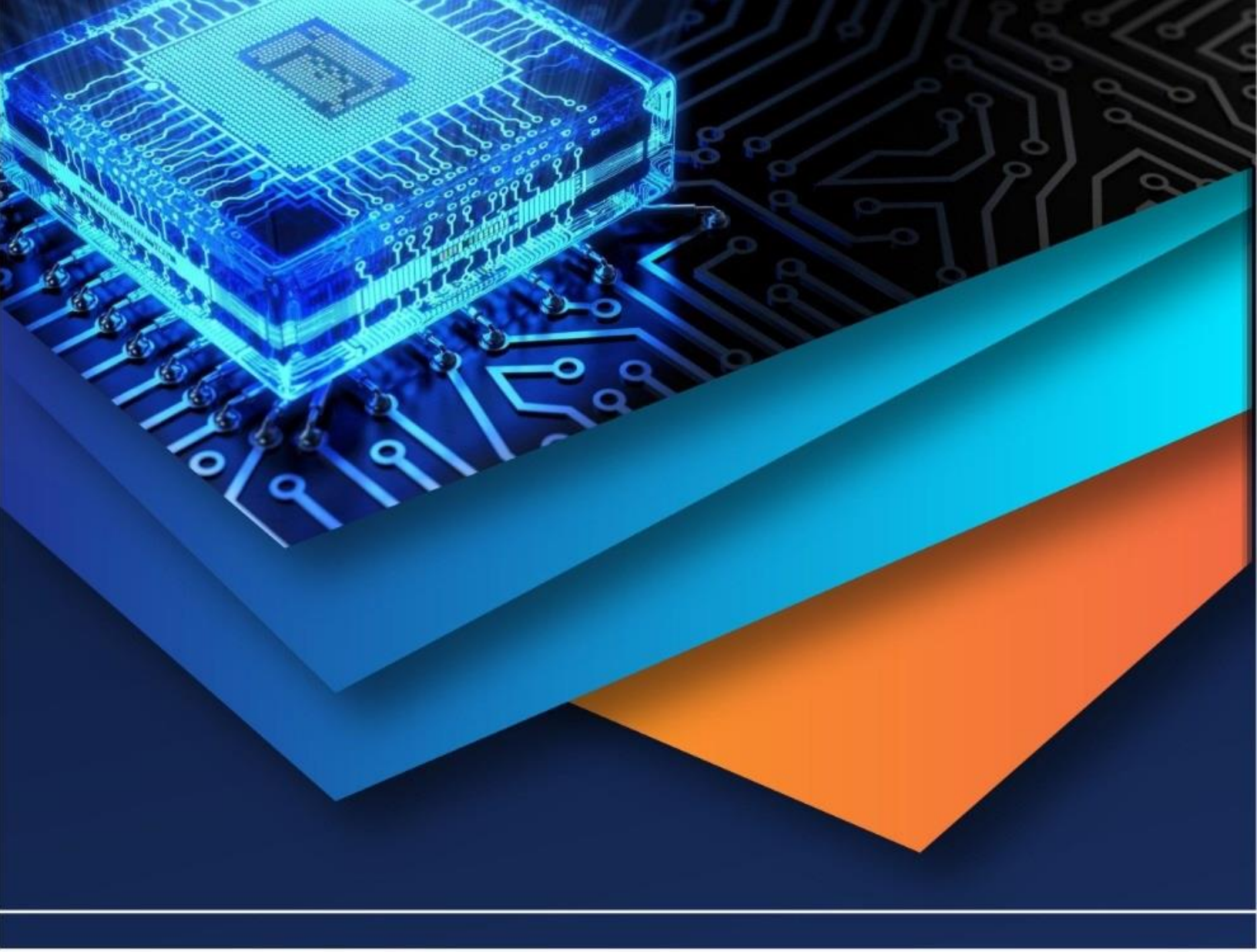
Though the virtual environment provisioned a free-of-cost base for the research, it had its own limitations. The virtual environment did not allow for a complete practical performance as other aspects of it were assumed and preconfigured. Also, the Genymotion virtual devices could not support applications which are not from the Google Play Store despite being rooted, therefore, other open-source tools could not be tested for their relevance yet this could have been achieved if it were a real phone. Another major drawback of the virtual environment was the unexpected crushing of Genymotion devices but this was later overcome by taking snapshots. Regardless of the stated limitations, the research study was successfully carried out with compatible open-source tools and a comparative study was done to bring a conclusion to the study as shown in Table 4. Though some of the tools proved irrelevant, some were relevant and can actually be used in the forensics of emerging Android Technologies.

VIII. CONCLUSION AND FUTURE WORK

From this study, it can be easily deduced that some of the tools and techniques used are still relevant or partially relevant whilst others are not. It is also pertinent to note from this research that not one tool does it all, a good combination of tools can be much more relevant in providing solutions than depending on one tool. In this research, a combination of tools managed to provide some good forensic results. It should be noted that the findings of this research are not conclusive as the study was performed on a virtual plartform which omitted some of the critical aspects faced in a real physical environment. For instance, Genymotion virtual phones come by default rooted which is not always the case in real situations. To some extent there is an oversight to other challenges of antiforensics posed by the Original Equipment Manufacturers (OEMs) in an effort to ensure user data privacy. Despite the stated limitations, the researchers believe the study will contribute in knowledge acquisition of performing forensics on emerging android Technology. The researcher recommends that the same study be conducted on physical devices for further exploration.

REFERENCES

[1] https://gs.statcounter.com/os-market-share/mobile/worldwide#
[2] https://www.perficient.com/insights/research-hub/mobile-vs-desktop-usage, last accessed 2021/11/27.
[3] Tamma Rohit and Tindall Donnie 2015 Learning Android Forensics page 4
[4] Afonin Oleg and Katalov Vladimir 2016 Mobile Forensics-Advanced Investigative strategies page 22
[5] Scrivens, Nathan & Lin, Xiaodong. (2017). Android digital forensics: data, extraction and analysis. 26. 10.1145/3063955.3063981.
[6] MRKAIĆ, I. (2016). Android forensic using some open source tools. In The Eighth International Conference on Business Information Security (BISEC-2016), Belgrade, Serbia, 15th October.
[7] Agrawal A.K., Khatri P., Sinha S.R. (2018) Comparative Study of Mobile Forensic Tools. In: Kolhe M., Trivedi M., Tiwari S., Singh V. (eds) Advances in Data and Information Sciences. Lecture Notes in Networks and Systems, vol 38. Springer, Singapore. https://doi.org/10.1007/978-981-10-8360-0_4
[8] Agrawal A.K., Sharma A, Sinha S.R and Khatri P International Journal of Electronic Security and Digital Forensics, 2020 Vol.12 No.1, pp.118 – 137
[9] Kamble, J. (2015) 'Digital forensic investigation procedure', International Journal for Advance Research Science and Engineering, Vol. 4, pp.157–168.
[10] S. C. Sathe and N. M. Dongre, "Data acquisition techniques in mobile forensics," 2018 2nd International Conference on Inventive Systems and Control (ICISC), 2018, pp. 280-286, doi: 10.1109/ICISC.2018.8399079.
[11] M. Raji, H. Wimmer and R. J. Haddad, "Analyzing data from an android smartphone while comparing between two forensic tools", SoutheastCon 2018, pp. 1-6, 2018.
[12] M. Boueiz, "Importance of rooting in an Android data acquisition," 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 2020, pp. 1-4, doi: 10.1109/ISDFS49300.2020.9116445.
[13] Andrew Hoog, Android Forensics: Investigation, Analysis and Mobile Security for Google Android 1st Edition, Syngress, 2011, page 218.
[14] https://developer.android.com/studio/commandline/adb.html, last accessed 2022/01/15
[15] S. J. Yang, J. H. Choi, K. B. Kim, and T. Chang, "New acquisition method based on firmware update protocols for Android smartphones," Digit. Investig., vol. 14, no. S1, pp. S68–S76, 2015
[16] D. Quick and M. Alzaabi, "Forensic analysis of the Android file system Yaffs2," Proc. 9th Aust. Digit. Forensics Conf., no. December, 2011.
[17] J. Grover, "Android forensics: Automated data collection and reporting from a mobile device," Digital Investigation, vol. 10, pp. S12–S20, 2013.
[18] M. -R. Boueiz, "Importance of rooting in an Android data acquisition," 2020 8th International Symposium on Digital Forensics and Security (ISDFS), Beirut, Lebanon, 2020, pp. 1-4, doi: 10.1109/ISDFS49300.2020.9116445.
[19] https://www.techradar.com/in/news/android-12-news, last accessed 2022/01/01.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)