Nat. Volatiles & Essent. Oils, 2021; 8(5): 1913 - 1922

NVEO
Natural Volatiles &
Essential Oils

Physical Data Extraction from Android mobile using Apeaksoft Android toolkit and Android Debug Bridge

J.Annies Mary Jeyaseeli[1] and Dr.C.Shanthi[2,*]

[1]Research Scholar, Department of Computer Science, VISTAS, Chennai, Tamil Nadu, India
[2]Assistant Professor,Department of Computer Science,VISTAS, Chennai, Tamil Nadu, India
[1]annies.phd@velsuniv.ac.in, [2,]shanthi.scs@velsuniv.ac.in*

Abstract. Android plays a vital role in day-to-day life. Android acts like a mini brain in many human lives. Therefore, data stored in android is also very essential. Now a days it is mandatory to preserve the stored data or to extract the stored data and place it safely in any location. Data extraction plays a major role in mobile forensics also. Mobile forensics is a kind of digital forensics that deals with extracting, analyzing and generating reports. It extracts data such as WhatsApp, SMS, Call logs, MMS, images, videos, etc. that can be stored on devices. To extract data efficiently, many data extraction tools are available. In this paper, command line tool such as ADB (Android Debug Bridge) and fully automated tool, Aspeaksoft Android toolkit are taken into consideration for extracting data. Moreover, performance of both the tools for extracting physical data can also be compared.

Keywords: Android, ADB, Application framework, SQLite, Linux.

1 Introduction

Android is a Linux based operating system mainly designed for mobile devices by Google. Android is an open-source operating system, which provides a unique way for the developers to develop an application but the applications run on different devices. Many applications can run on Android and efficient data storage mechanisms are maintained in Android. Android is purely versatile and each one come out with new unique features. It supports programming languages such as java, C++, Kotlin etc., Storing data, managing data and preserving data becomes a great challenge for e day to day life. Performance of the mobile is poor when the storage becomes full, so it is necessary to move or extract data to the safer place. Moreover in the field of forensics data acquisition plays the major role.

Data Extraction:

Data extraction is a method of extracting data from various storage partitions in android mobile and later use for different purposes. Three types of data extraction techniques are available.

(1)Logical extraction

(2)File System extraction

(3)Physical Extraction

Logical data extraction is a technique in which data can be extracted from the storage objects. While extracting data logically by using tools, API's can be used to communicate with the operation system. Deleted files cannot be extracted by using using this method.

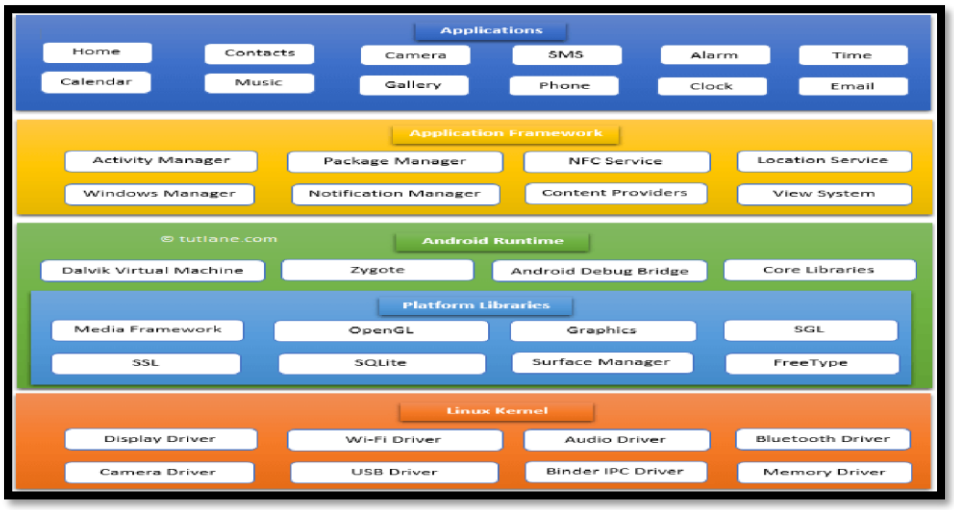
File System extraction method is same as that of Logical method, but it extracts the file directly on the internal storage rather than approaching API's.
Physical Data Extraction is a method in which deleted files can also be extracted. This paper focusses on physical data extraction.

2 Architecture of Android:

Android architecture is composed of five components

- Linux Kernel
- Platform libraries
- Android Runtime
- Application Framework
- Applications

Android architecture is a group of above five components, which can be arranged in the form of stack. It contains Linux kernel, which is the heart of an android, collection of libraries, which exhibited through android run time, application framework and applications.



3 Android Debug Bridge (ADB):

Android Debug Bridge (ADB) is a versatile command line tool. It is based on the Linux kernel and certain commands can be used to pull data. Even though it is Linux based, it supports other operating system such as Windows. ADB is also used for penetration testing. A penetration testing is a testing, which is used to check security level of applications. So, Forensic investigators also use ADB tools, to extract data simply by connecting the device through USB. ADB or Android Debug Bridge is a part of the Android SDK, which identifies the location, and the name of the files. There are many ways to get regular files from a mobile device to a computer, by using backup software, cloud services or even emailing the files. ADB is not a simple as those, but ADB can find and extract files not normally visible to the user.

4 Aspeaksoft Android Toolkit

Apeaksoft Android Toolkit 2.0.10 includes all the necessary files and uploaded program, which contains all latest and updated files, it is completely offline or standalone and following are some of the key features:

- To recover lost or deleted files including contacts, text messages, call history and documents from Android devices or SD card.
- To retrieve deleted or lost photos, music, videos and WhatsApp file and get them back from Android by using Aspeaksoft Android Toolkit.
- Managing data efficiently by storing backup on Windows or Mac easily with the USB cable.
- Recover deleted data, which may happen due to files deleting, system crashing, forgotten password, rooting error, etc.

5 Challenges of data extraction on Android devices:

The rate of increase in android usage is directly proportional to increase in data storage rate. Therefore maintaining stored data is very big challenge in the current trends. Sometimes minimum memory space forced the user to delete the stored data. In that situation, transferring data from android to some other devices become mandatory. To extract data, many tools are available and the great challenge is to use most appropriate tool to extract data [16,17] efficiently and securely. To extract physical data, tools namely Android Debug Bridge (ADB) and Aspeaksoft Android Toolkit are used.

- Experimental setup:
- Device name: Redmi
- Model number: Redmi 7
- Android version: 9 PKQ1.181021.001

6 Data Extraction using Android Debug Bridge (ADB):

Before extracting data, check the list of devices connected to PC. To check, type the following command in the command prompt, adb devices

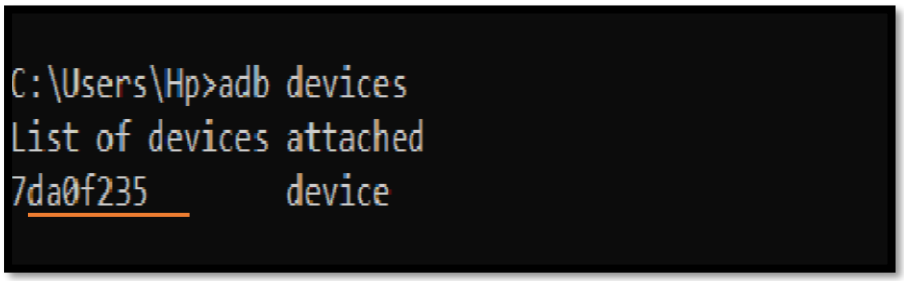


Figure 1 Connecting Android device to PC.

To insert data from PC to device, use adb push"path of file to be inserted"

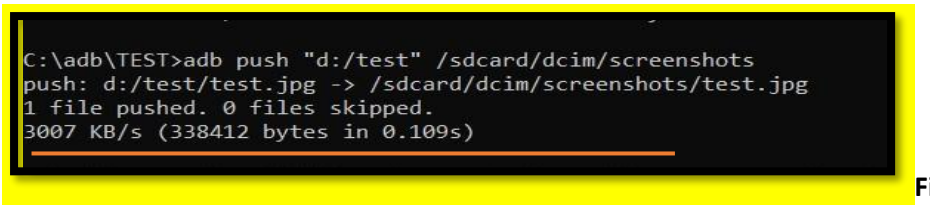


Figure 2 - Inserting files from PC to android

Figure 2 shows that the time taken to pull 338412 bytes from PC to android is 0.109s at the Rate of 3007 KB/s

To extract data from device, use adb pull "path of file data to be extracted"

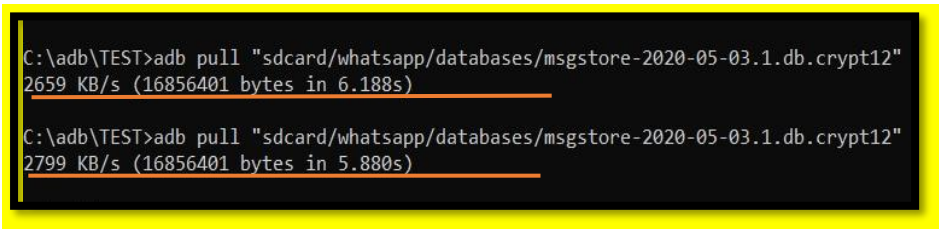


Figure 3 - Extraction of WhatsApp database

Figure 3 clearly shows that 16856401 bytes of data was extracted in 6.188s if the data rate is 2659 KB/s, or it takes 5.880s if the data rate is 2799 KB/s. It is highly secured because the extracted data is in encrypted form, to decrypt the database, respective decryption tool is used.

Figure 4 Extraction of screenshots from sdcard

Figure 4 clearly shows that the time taken to extract 4819155 bytes of data is 2.055s at the data rate of 2289 KB/s and it clearly denotes that no files were skipped.

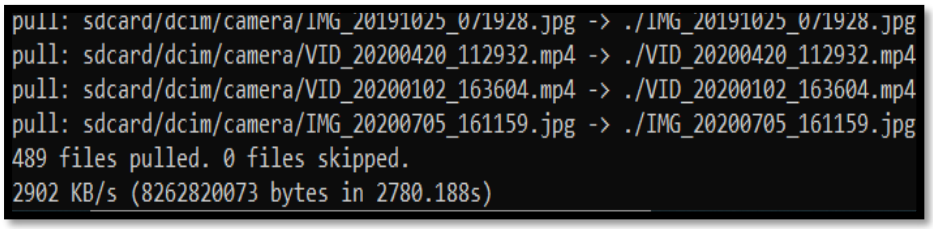


Figure 5 Extraction of data from Gallery

Figure 5 shows that the time taken to extract 8262820073 bytes of data in 2780.188s at the data rate of 2902 KB/s.

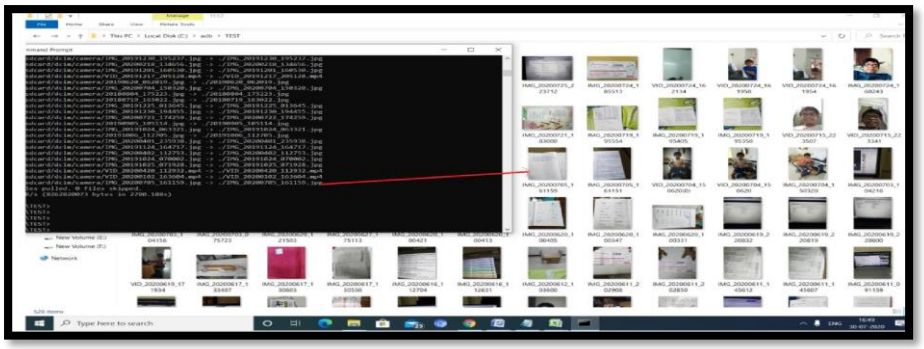


Figure 6 File transfer

The Figure 6 shows the name of the image and the extracted image in the respective file path.

Table: 1 Time taken to extract data using Android Debug Bridge (ADB):

Application	No.of Bytes	Time to extract(seconds)
Screenshots	4819155	2.055s
WhatsApp	16856401	5.880s
Camera(audio & video)	8262820073	2780.188s

Table1 clearly shows that the time taken to extract data is different for different file types. As per the data, minimal time period is required to transfer static images or text whereas more time is taken to extract video files.

Experimental Setup2:

System Requirements for Apeaksoft Android Toolkit 2.0.10:

- Operating System: Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows XP
- CPU: 1GHz Intel/AMD CPU or above
- RAM: 1GB RAM or more
- Hard Disk Space: 200 MB and above free space

Android mobile used is Redmi 7

7 Data extraction using Aspeaksoft Android Toolkit:

Download Aspeaksoft Android Toolkit on PC

Figure 7 Aspeaksoft Android Toolkit for data extraction

Connect the required android mobile to PC by enabling USB debugging on.

Figure 8

Displays the name of the device connected.

Figure 9

Displays the types of files to be extracted.

Figure 10 Extraction of Call log details

Figure10 displays information such as Name, phone no., date type of call such as incoming or outgoing, call duration etc.,

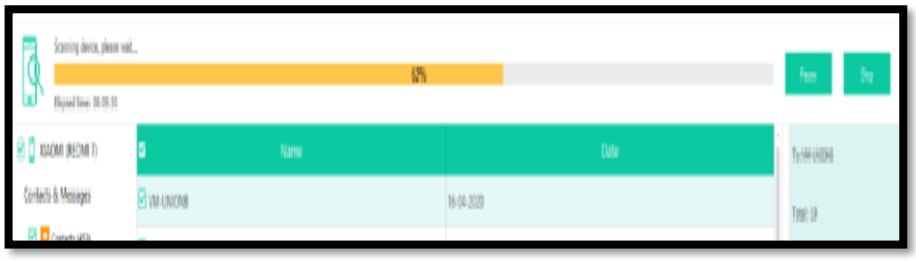


Figure11a Transferring Data

Figure 11b Time taken to transfer Data

Figure 11 shows the no. of items transferred from mobile gallery to PC and the time taken to transfer the data is also mentioned.

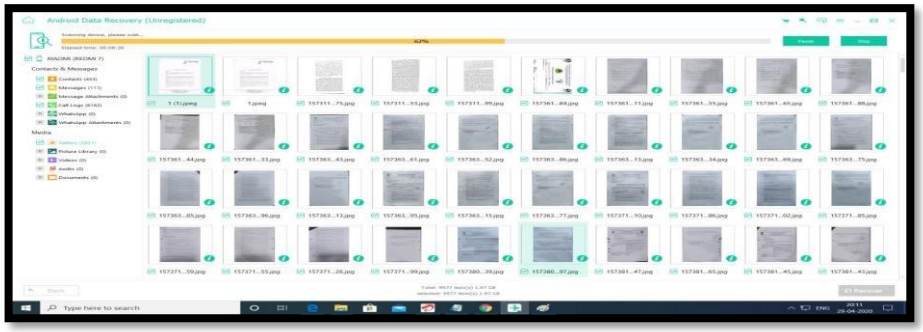


Figure 12 Extraction of Text Messages from Android to PC

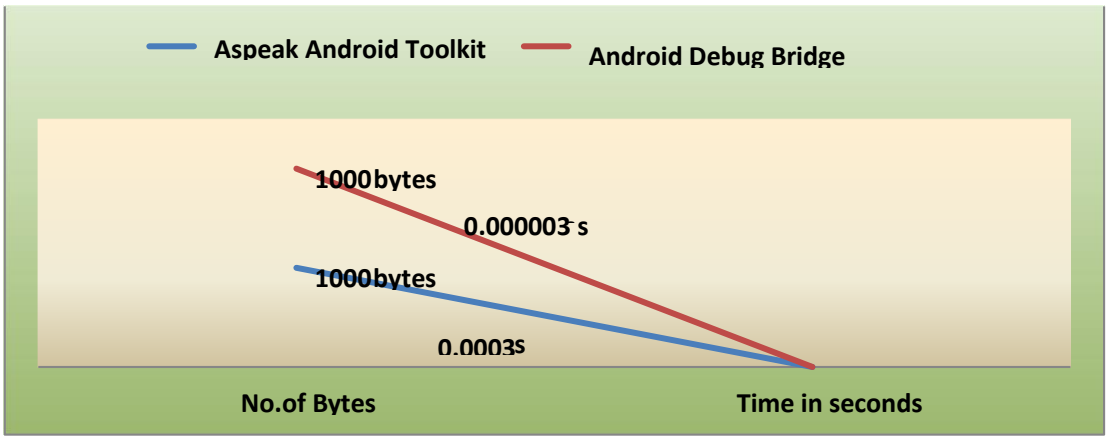
Figure 12 shows extracted messages from mobile to PC in which if any mobile number is selected then messages sent or received from that number is displayed simultaneously in date wise manner.

Table 2: **Time taken to extract data using Aspeaksoft Android Toolkit:**

Application	No.of Bytes	Time to extract(seconds)
Contacts	329150	3.45s
Mesaages	1970000000	9.30s
Gallery	1970000000	6.30s

Comparison of Table 1 and Table 2

Toolkit	No of bytes	Time in Seconds
Android Debug Bridge(ADB)	1000	0.0003 Sec
Aspeak Android Toolkit	1000	0.000003 Sec



Conclusion:

The above experimented tools are very effective for extracting data. Time taken to extract data from android to PC by using Android Debug Bridge (ADB) is somewhat more compared to Aspeaksoft Android Toolkit. Aspeaksoft Android Toolkit can be easily used by all users and extracted data can be viewed as it is in the form stored in the device whereas to use ADB tool, basic knowledge about ADB commands is required and extracted data is not visible to the others. Comparatively, extracting data using Android Debug Bridge (ADB) is secured because extracted

data can be directly moved to specified file path or in encrypted form. In future, deleted data and data from broken mobile can be extracted by using other data extraction tools.

References

1. Mentsiev, A. U., and M. T. Alams. "Mobile forensic tools and techniques: Android data security." Инженерный вестник Дона 2 (53) (2019).
2. Boueiz, Marie-Rose. "Importance of rooting in an Android data acquisition." 2020 8th International Symposium on Digital Forensics and Security (ISDFS). IEEE, 2020.
3. Kumar Agrawal, Animesh, Aman Sharma, and Pallavi Khatri. "Android Forensics: Tools and Techniques for Manual Data Extraction." In Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India. 2019.
4. Al-Sabaawi, Aiman, and Ernest Foo. "A Comparison Study of Android Mobile Forensics for Retrieving Files System." International Journal of Computer Science and Security (IJCSS) 13, no. 4 (2019): 148.
5. Anglano, Cosimo, Massimo Canonico, and Marco Guazzone. "The Android Forensics Automator (AnForA): A tool for the Automated Forensic Analysis of Android Applications." Computers & Security 88 (2020): 101650.
6. Alatawi, Hayam, Kholod Alenazi, Salehah Alshehri, Shahad Alshamakhi, Mohammed Mustafa, and Amer Aljaedi. "Mobile Forensics: A Review." In 2020 International Conference on Computing and Information Technology (ICCIT-1441), pp. 1-6. IEEE, 2020.
7. Easttom, Chuck, and Willie Sanders. "On the Efficacy of Using Android Debugging Bridge for Android Device Forensics." In 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pp. 0730-0735. IEEE, 2019.
8. Pieterse, Heloise. "Mobile Forensics: Beyond Traditional Sources of Digital Evidence." In ECCWS 2020 20th European Conference on Cyber Warfare and Security, p. 295. Academic Conferences and publishing limited, 2020.
9. Lwin, Htar Htar, Wai Phyo Aung, and Kyaw Kyaw Lin. "Comparative Analysis of Android Mobile Forensics Tools." In 2020 IEEE Conference on Computer Applications (ICCA), pp. 1-6. IEEE, 2020.
10. Kim, Dohyun, and Sangjin Lee. "Study of identifying and managing the potential evidence for effective Android forensics." Forensic Science International: Digital Investigation (2020): 200897.
11. Herrera, Lazaro A. "Challenges of acquiring mobile devices while minimizing the loss of usable forensics data." In 2020 8th International Symposium on Digital Forensics and Security (ISDFS), pp. 1-5. IEEE, 2020.
12. Aju, D., Anil Kumar Kakelli, Ashwin Suresh Varma, and Kishore Rajendiran. "A Comprehensive Perspective on Mobile Forensics: Process, Tools, and Future Trends." In Confluence of AI, Machine, and Deep Learning in Cyber Forensics, pp. 1-28. IGI Global, 2020.
13. Cantrell, Gary D., and Joan Runs Through. "Teaching Data Carving Using The Real World Problem of Text Message Extraction From Unstructured Mobile Device Data Dumps." Journal of Digital Forensics, Security and Law 14, no. 4 (2020): 4.
14. Mohammmed, Sheena, and R. Sridevi. "A Survey on Digital Forensics Phases, Tools and Challenges." In Proceedings of the Third International Conference on Computational Intelligence and Informatics, pp. 237-248. Springer, Singapore, 2020.

15. Yadav, Samarjeet, Satya Prakash, Neelam Dayal, and Vrijendra Singh. "Forensics Analysis of WhatsApp in Android Mobile Phone." Available at SSRN 3576379 (2020).
16. Garg H., Lal N. (2018) Data Analysis: Opinion Mining and Sentiment Analysis of Opinionated Unstructured Data. In: Singh M., Gupta P., Tyagi V., Flusser J., Ören T. (eds) Advances in Computing and Data Sciences. ICACDS 2018. Communications in Computer and Information Science, vol 906. Springer, Singapore. https://doi.org/10.1007/978-981-13-1813-9_25.
17. N. Lal, M. Singh, S. Pandey and A. Solanki, "A Proposed Ranked Clustering Approach for Unstructured Data from Dataspace using VSM," 2020 20th International Conference on Computational Science and Its Applications (ICCSA), Cagliari, Italy, 2020, pp. 80-86, doi: 10.1109/ICCSA50381.2020.00024.