

# Logical Image Acquisition and Analysis of Android Smartphones

Nursel Yalçın<sup>1</sup>, Tayfun Yıldırım<sup>2\*</sup>

<sup>1</sup>Department of Computer and Instructional Technologies Education, Faculty of Education, Gazi University, Ankara, Türkiye

<sup>2</sup>Department of Computer Forensics, Institute of Informatics, Gazi University, Ankara, Türkiye

Email: nyalcin@gazi.edu.tr, \*av.tayfunyildirim@gmail.com

**How to cite this paper:** Yalçın, N. and Yıldırım, T. (2024) Logical Image Acquisition and Analysis of Android Smartphones. *Journal of Computer and Communications*, 12, 139-152.

<https://doi.org/10.4236/jcc.2024.124011>

**Received:** February 29, 2024

**Accepted:** April 21, 2024

**Published:** April 24, 2024

Copyright © 2024 by author(s) and Scientific Research Publishing Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

## Abstract

Android smartphones largely dominate the smartphone market. For this reason, it is very important to examine these smartphones in terms of digital forensics since they are often used as evidence in trials. It is possible to acquire a physical or logical image of these devices. Acquiring physical and logical images has advantages and disadvantages compared to each other. Creating the logical image is done at the file system level. Analysis can be made on this logical image. Both logical image acquisition and analysis of the image can be done by software tools. In this study, the differences between logical image and physical image acquisition in Android smartphones, their advantages and disadvantages compared to each other, the difficulties that may be encountered in obtaining physical images, which type of image contributes to obtaining more useful and effective data, which one should be preferred for different conditions, and the benefits of having root authority are discussed. The practice of getting the logical image of the Android smartphones and making an analysis on the image is also included. Although root privileges are not required for logical image acquisition, it has been observed that very limited data will be obtained with the logical image created without root privileges. Nevertheless, logical image acquisition has advantages too against physical image acquisition.

## Keywords

Android Smartphone Forensics, Data Acquisition, Data Analysis, Root Privileges, Digital Forensics

## 1. Introduction

Android smartphones dominate the global smartphone market by 71% in 2021.

Therefore, the rate of these devices being evidence in trials is high [1]. A vast quantity of data can be stored on Android smartphones [2]. The information available on an Android phone encompasses fundamental details, data from various applications, multimedia content, call histories, contact details, images, sent and received messages, as well as the chat applications database like WhatsApp database [3]. It is foreseen that artificial intelligence can be used to detect crime-related data among this vast amount of data [4]. Additionally, mobile devices can be targeted in cybercrimes.

In 2023, Internet of Things (IoT) gadgets were the primary focus of outside cyber assaults, with 33 percent of such devices experiencing cyber-attacks. Following closely behind were employee and company-owned mobile devices, which accounted for 28 percent of the attacks [5].

With the integration of technological developments, the widespread use of mobile phones around the world has provided many benefits to humanity in terms of the dissemination of information. However, because of this great technical capacity development, the possibility of social harm has increased as well as allowing for new risks, abuse, and crime opportunities for users. While digital forensics, which started in the early 1990s, is a rapidly growing discipline in the field of forensic science, mobile forensics has started as a department of digital forensics since the early 2000s. Due to the widespread use of smartphones and their development with new technologies, users rely more on these devices. For this reason, smartphones have a significant importance. The volume and importance of personal data stored on a smartphone are beginning to be similar to that stored on laptops and computers [6]. In 2021 there were 7.1 billion smartphone users worldwide, and in 2025 this number is expected to be 7.49 billion [7].

Mobile forensics is the legal and accepted method of obtaining digital evidence from a cell phone, and a branch of digital forensics. Digital forensics is a set of specialized techniques, processes and procedures that are used to preserve electronic evidence, extracting, analyzing, and presenting the data in this evidence. It is also the methodology of techniques in computer forensic and analysis used to identify potential legal evidence. This methodology involves the process of extracting data and evaluating their meaning, usually from files on computers or other digital devices [8].

There are three different methods that can be applied when obtaining data from Android smartphones. These are manual data acquisition, logical image acquisition and physical image acquisition [9]. Manual data acquisition is the collection of data on the device by using the device directly, and it cannot be considered as creating an image.

In this study, how to get the logical image with the tool called Android Triage and how to analyze the image with the tool called ALEAPP will be discussed by explaining the concepts of logical image and physical image. At the same time, how much useful data and which data will be obtained with the logical image, how to quickly analyze the data with the tool called ALEAPP, and the difficulties

encountered while doing all these are explained.

Due to the developing technology and differentiating types of crime, forensic experts should also be constantly in search of new methods and software for investigating digital evidence. Because Computer Forensics is not a department that has completed its development in all countries, this department of science, which aims to establish justice, constantly renews itself and seeks answers to emerging problems that caused by technical developments [10]. The field of mobile forensics faces challenges due to the frequent release of new mobile device models by providers, which can occasionally pose challenges for forensic investigators in collecting information [11].

Since this study deals with the difficulties encountered during logical image acquisition and analysis, and issues related to maintaining data integrity and accuracy. This study was aimed to develop legal and effective new methods by experts in terms of investigating Android smartphones in computer forensics.

In the second part of the study, the concepts of logical and physical image acquisition are explained. In the 2.1 section, the acquisition of the logical image and in the 2.2 section the analysis of the logical image are discussed.

## 2. Logical and Physical Image Acquisition

Creating an image is of critical importance as it defines the state of the evidence that will be the basis for analysis. Analyses will be carried out on the data in the image acquired from the target device, and the interpretation of the data will be presented. All operations performed after acquiring the image and preserving the image should be reported. Thus, the possibility of voluntary or involuntary changes on the evidence should be reduced. The reporting process, which starts with the acquisition of evidence in this way, is called the chain of custody [12].

Obtaining data in computer forensics is the first step after identifying and determining digital devices that may be of legal relevance. This process involves making a forensically accurate copy of the targeted media. This step is usually accomplished by acquiring a bitstream image of the actual data. This activity is necessary to perform forensic examination on the copied data instead of the original data, ensuring that the original data on the target device and the copy are exactly the same [13].

Logical image or physical image acquisition methods can be used to obtain this copy.

Acquiring a logical image is obtaining the data and file system in the allocated space on the disk of the target device. On the other hand, acquiring a physical image means getting the data in all areas, including unallocated space and free disk space on the disk. Therefore, by acquiring physical image of target device, it will be possible to obtain disk spaces that have not yet been processed with new data after data deletion. As a matter of fact, these deleted data will have residual traces on the disk, apart from the existing file system [9]. In this way while creating the physical image, each of the binary data on the disk is completely

obtained without skipping; on the other hand, only the binary data of the files and directories are obtained in the logical image that was created. The difference between the two lies in this distinction: data that can be seen by using operating system tools forms logical image, whereas the data can be seen in an unprocessed raw state with processor and other hardware parts forms the physical image [8].

However, taking the physical image is getting more and more difficult due to the constant updating of android smartphones and increasing security measures. To create physical image, target device must be rooted. For this reason, if it is desired to create a physical image of the device that does not have root privileges before, it will be necessary to gain root privileges [14]. Process of gaining root privileges threatens the security of android smartphone and data integrity.

Also, if the data is encrypted, creating a physical image won't be beneficial because the image itself will also be encrypted. In such situations, you'll need to create a logical image instead [15]. Besides, logical image acquisition is commonly employed too when copying an entire drive or network is impractical due to its size [16].

Although preferring the logical image instead of the physical image on Android smartphones causes less data to be accessed; since it will cause a lower level of change in the device, it creates a more convenient way in terms of computer forensics. Therefore, it is preferable to examine through logical images to protect the data integrity of the device. Even though it is more limited than the rooted devices, the process of creating the logical image can also be performed on non-rooted devices [17].

Whereas on Android 6 and higher versions, the bootloader must be unlocked to gain root privileges on devices. Since this means resetting the device to factory settings in most cases, even if root privileges are gained afterwards; it will not be possible to obtain suitable data from the device, and data loss will occur probably. Therefore, trying to gain root authority during the examination of the seized device, especially in the latest versions of Android, poses a great danger in terms of data integrity [18].

Out of the Android Authority readers surveyed, only 19.7% of them reported that their phones had been rooted. Their reasoning included advantages such as ad-blocking, using call recording software, installing custom ROMs, and enjoying enhanced backup support [19]. Given that the individuals participating in this survey are passionate about Android devices, the proportion of rooted Android phones among all devices is expected to be relatively small. In this regard, the significance of acquiring a logical image is evident.

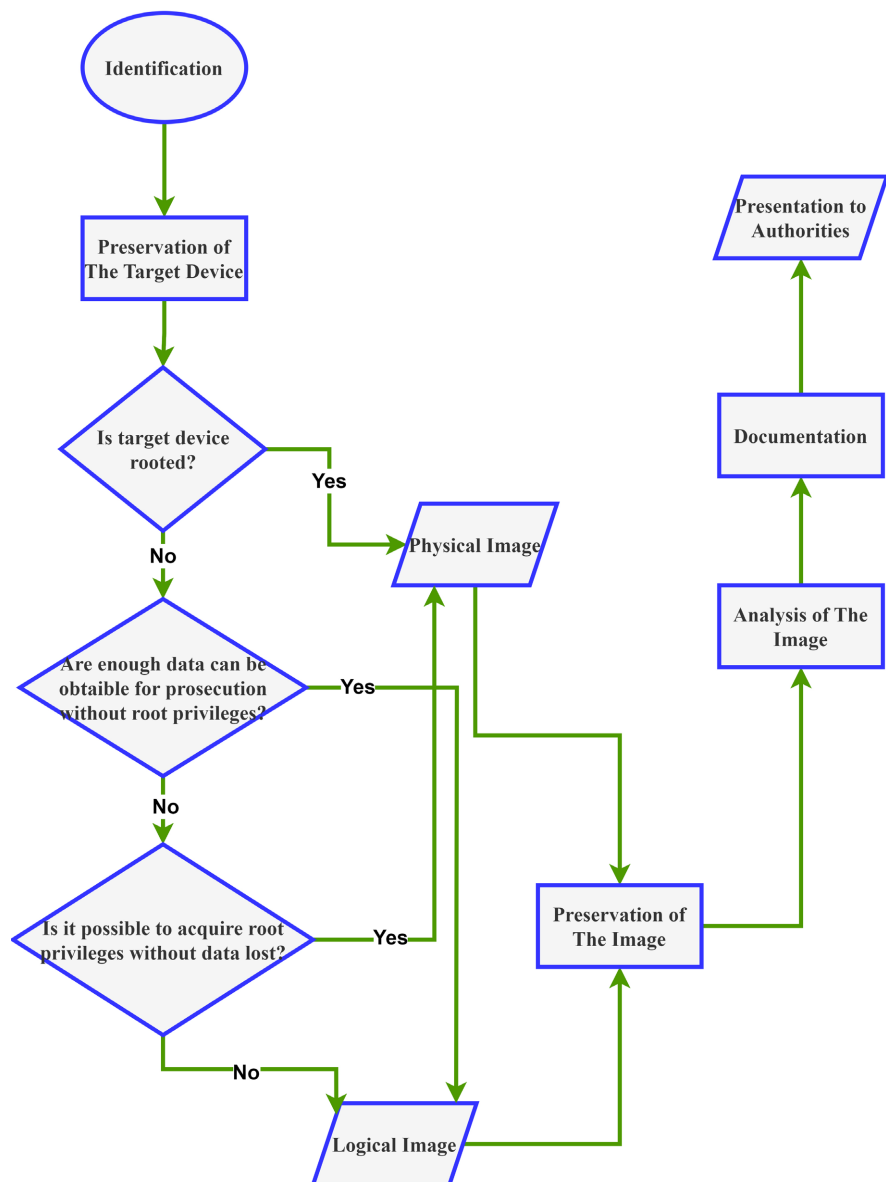
There is a deep divergence among mobile forensic examiners. While some of the investigators argue that only limited data should be obtained by not making any changes on the device with the traditional approach, the other part advocates taking a radical step to collect valuable data at the maximum level from the target device by making minimal possible changes. Although the second ap-

proach is controversial in terms of computer forensics; the limitations of the traditional approach and the need for valuable evidence in modern smartphones negate the arguments to the contrary. However, these changes are permissible as long as the relevance and effect of the changes are explained [20].

The methodology that can be applied is shown for deciding which image to acquire in **Figure 1**.

## 2.1. Practice of Logical Image Acquisition

Creating a logical image of android devices is possible with various tools. One of these tools is Android Triage, which performs the logical image acquisition process in a comprehensive way [21].



**Figure 1.** Methodology to decide which image will be acquired, and steps of Android smartphone forensics.

The target device should be running while acquiring logical image. Therefore, it is important to preserve device integrity as much as possible by turning airplane mode on or putting the device inside faraday bag [22].

The tool named Android Triage runs on Linux Operating Systems. This tool is installed in the Linux Operating System distribution named Tsurugi [23]. It is designed to preserve the integrity of the evidence at the highest level if the order specified in the tool interface is used.

Android Triage performs operations via ADB (Android Debug Bridge). ADB is part of the Android Software Developers Kit (SDK) that connects Android devices and computers to access and control files on Android-based smartphones from computers [24].

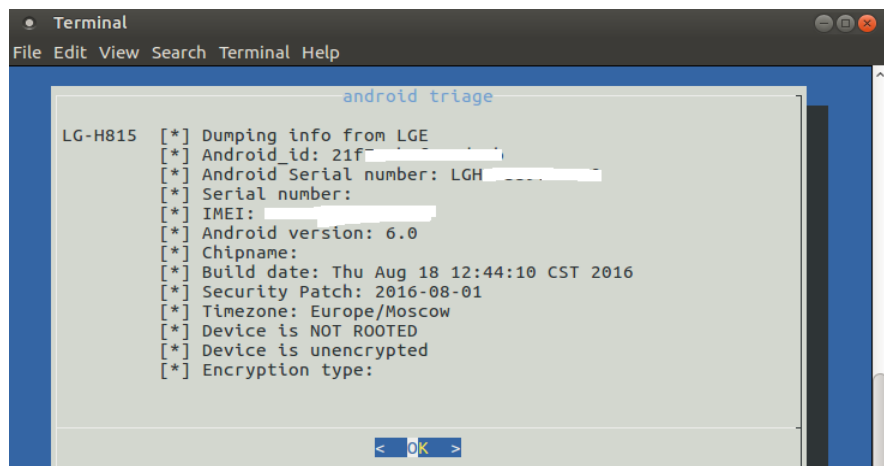
By running the Tsurugi Linux system distribution with the help of a virtual machine in the Windows operating system, the logical image of a physical LG Brand G-4 Model phone with the Android Triage tool was carried out as follows.

First, USB debugging mode is turned on before the Android smartphone is connected to the computer. Then, the terminal screen was opened in the Linux Tsurugi distribution and the *adb devices* command was entered directly. After this command is entered, the phrase “*unauthorized*” appears next to the device’s information. Afterwards, when USB debugging is allowed on the screen of the android device so that the computer can access the android device, the phrase “*unauthorized*” is replaced with the phrase “*device*”, thus creating the necessary conditions for to run the tool called Android Triage, which can use adb commands effectively.

First, general information about the phone was obtained by using the tool (Figure 2).

After doing this, a folder is created in the Linux operating system with the information in the *Android\_id* section and the files obtained in the next logical image operation options are pulled into this folder.

Afterwards, logical image acquisition operations were performed sequentially in the application interface shown in Figure 3.



```

Terminal
File Edit View Search Terminal Help

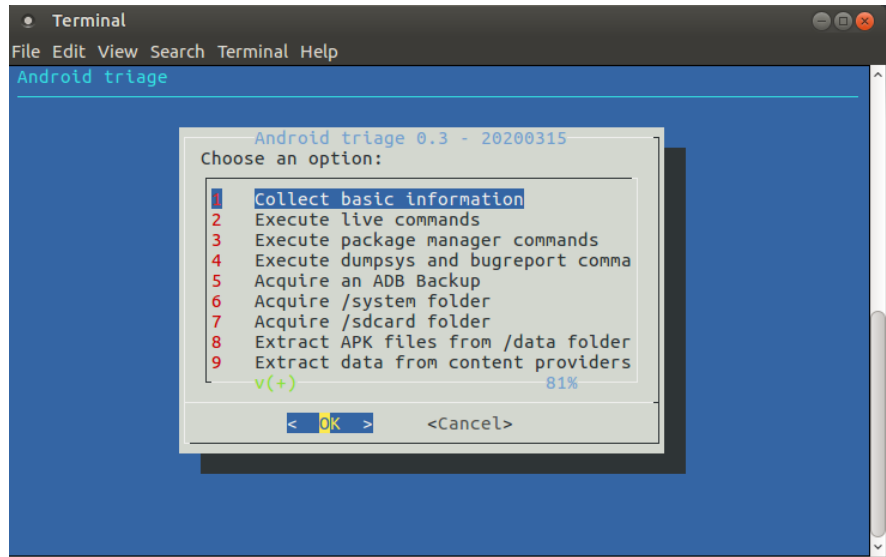
android triage

LG-H815 [*] Dumping info from LGE
[*] Android_id: 21f[REDACTED]
[*] Android Serial number: LGH[REDACTED]
[*] Serial number:
[*] IMEI: [REDACTED]
[*] Android version: 6.0
[*] Chipname:
[*] Build date: Thu Aug 18 12:44:10 CST 2016
[*] Security Patch: 2016-08-01
[*] Timezone: Europe/Moscow
[*] Device is NOT ROOTED
[*] Device is unencrypted
[*] Encryption type:
  
```

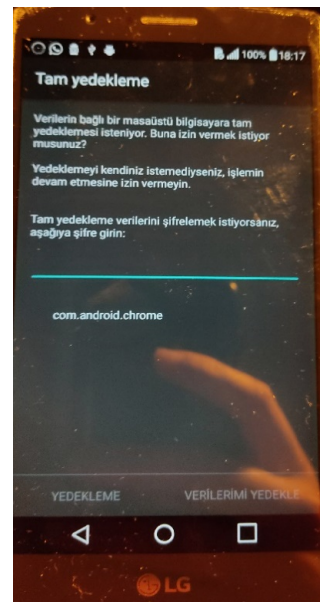
Figure 2. General information about the android smartphone.

From these processes, it took much longer to get the logical images by selecting options ADB Backup #5, /system folder #6, APK files from /data folder #8.

While it is not necessary to get any permission from the smart phone, where options 6 and 8 are performed; while performing the ADB Backup process which option 5, it was necessary to obtain permission from the smartphone as in **Figure 4**. In this way, while to backup is allowed on the phone, it is possible to encrypt the backup by entering a password on the phone. Since there is no SD card inserted in the device, option number 7 was not performed.



**Figure 3.** Interface that shows the logical image acquisition options of the Android Triage tool.



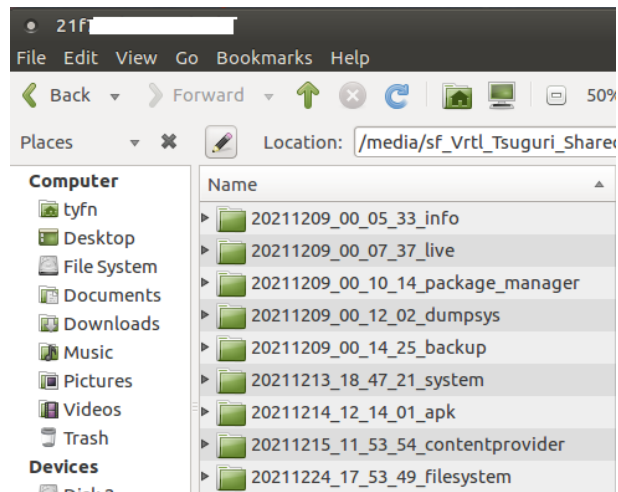
**Figure 4.** Permission to be given from the phone to perform ADB Backup (In Turkish “verilerimiyedekle” means backup my data, “yedekleme” means not to backup. Line that appears green color is the space where the password can be given for encryption).

As a result of these logical image acquisition processes, subfolders as in **Figure 5** were created in the folder created with *Android\_idof* of the phone in the *home* folder of the Linux operating system with Tsurugi distribution.

With the Android Triage tool, it will be enough data to get started; browser searches and history, contact information saved on the phone, Bluetooth devices, calendar events and login information. As a matter of fact, the data of the websites visited in the browser that was built into the android system can be accessed in a .txt file (**Figure 6**).

## 2.2. Analysis of Logical Image

It is not possible to directly examine the data obtained and preserved by the court. For this reason, forensic experts should analyze the data collected with the help of tools. Analysis is to interpret the obtained data by extracting it and processing it [25].



**Figure 5.** Subfolders created after logical image acquisition of Android smartphone.



**Figure 6.** Browser history data obtained from Android smartphone with Android Triage tool.



Indeed, many of the digital evidence that have a specific meaning (e.g. deleted files, free disk space) is required to be analyzed because their meaning remains hidden in their primary form [26].

Although general data can be accessed with the Android Triage tool, a more detailed analysis is also possible. In this context, the logical image of the Android smartphone taken with the file system dump option in the tool named Android Triage can be examined with the tool called ALEAPP [27]. To run the ALEAPP, python must be installed in the operating system of the workstation where the computer forensics investigation is performed. Afterwards, the library required for the tool to work must be installed with the code “*pip install -r|requirements.txt*” by opening a command prompt in the folder where the ALEAPP tool is located.

By running the file named aleappGUI.py in the folder where the tool was located, it is possible to select the location where the logical image and the report will be created with the help of the graphical interface and to generate a report about the logical image (Figure 7).

When we analyzed the file system image of LG G-4 Model device created by Android Triage with ALEAPP, no suitable data could be obtained. The reason for this is that this smartphone does not have root authority. Because of this the data obtained from */data* and */system* folders has been limited. As a matter of fact, during the logical image acquisition using the file system dump option that comes with the Android Triage 1.1 version, the tool could not continue the operations at some points, it was necessary to proceed to the next operation even though some previous operations were not completed.

Because on android devices, valuable data in terms of forensics is in the */data* folder, within this folder are many different directories, usually beginning with the word “.com”. There is data for all applications installed on the smartphone, including dependencies such as databases and configuration files. Some of these

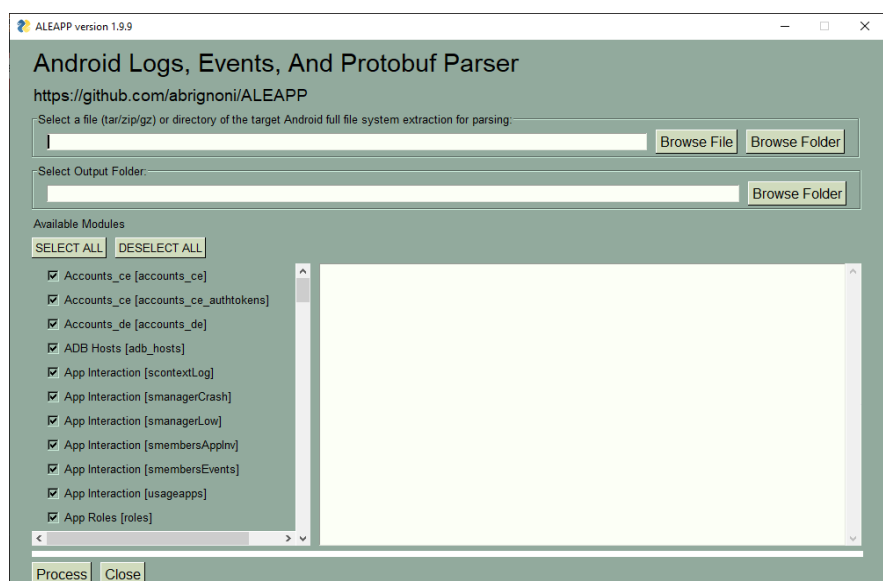


Figure 7. Graphic Interface of ALEAPP.

directories use sensitive databases of how the app was created, some use sensitive databases such as usernames and passwords, or keep logs such as Facebook, messages, call logs and status updates on apps [28].

Because ADB daemon running on non-rooted devices works with shell permissions, for this reason, files with the maximum level of evidence cannot be accessed. However, the *adb pull* command can still access unencrypted applications, the majority of tmpfs file systems such as browser history containing user data, and system information as showed **Figure 5** above. However, with root privileges, the analysis of files containing important data can be done on the computer in the workstation [29].

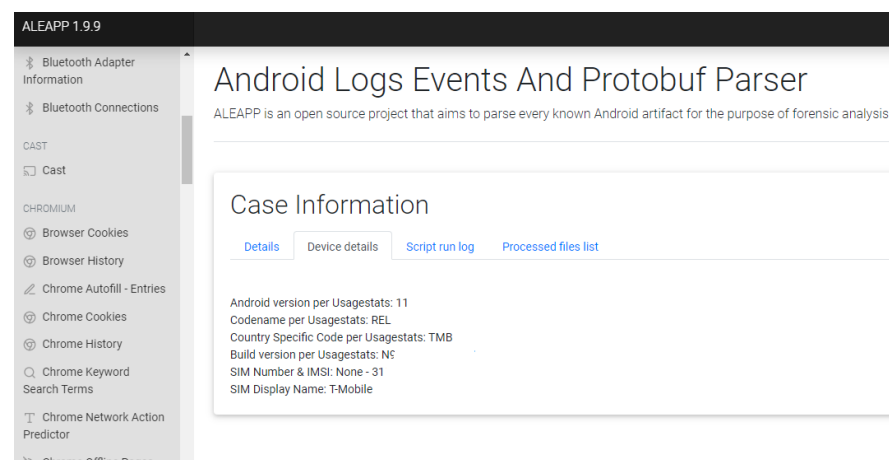
However, in analyzing the logical image of a rooted device with ALEAPP, many useful data about the device were obtained [30].

In this way, the device's Bluetooth adapter, Bluetooth connections; cast; browser history, cookies, autofill, searched keywords, offline pages; sim card; Gmail; Google duo contacts; Google now and quick search; Google photos cache and local media; Google Play recent searches; WhatsApp contacts, messages and user profile; SMS, MMS information; Many data such as operating system and developer number of the device were obtained. In the script run log and processed files list tabs of the generated report, there are also records of which files were analyzed and the operations performed (**Figure 8**).

ALEAPP enabled the creation of a report suitable for analysis on the logical image in less than a minute. Thus, it was possible to obtain a general analysis data about the device quickly.

### 3. Results and Discussion

The data on Android smartphones can be physically or logically obtained. It will be possible to obtain more data by creating a physical image, since the physical image can also contain deleted data due to the unallocated areas on the disk and the empty disk partition. However, the prerequisite for obtaining a physical image



**Figure 8.** The report was created as a result of the analysis made on the file system of the device with ALEAPP.

is the ability to have root privileges on the Android device. For this reason, it may not always be possible to apply the method of acquiring a physical image. As a matter of fact, in Android 6 and higher versions, it will not be convenient as the bootloader will need to be unlocked to root the device, and this will often cause the data on the device to be lost.

If the logical image is created, it will be at the file system level, so the deleted data will not be present in the logical image. However, creating the logical image is preferable from to point of that it does not require root privileges and makes much fewer changes to the target device. But it should not be forgotten that, if a logical image is acquired from a rooted device, it will be possible to obtain more data from the device. As a matter of fact, the */data* folder on the device can only be accessed with root authority, and there may be many data in this folder that are suitable for illuminating the investigation or prosecution.

Logical image acquisition can be done with the tool called Android Triage. With this tool it is possible to obtain a lot of useful data for the entry level. While creating the image with the file system dump option without root privileges, many steps had to be skipped. A tool called ALEAPP can be used for more detailed analysis. However, for the tool to analyze effectively, it is necessary to acquire a logical image of a rooted device, including the */data* folder.

It was also seen in this study that it is necessary to develop new methods to effectively examine smartphones with up-to-date Android operating systems in terms of forensic informatics. As a matter of fact, with the Android 6.0 version, it has become difficult to gain root authority over Android devices or even if it can be gained, the data on the target device can be deleted permanently. Although gaining root authority causes changes on the target device, if the operations performed during the acquisition of root authority are reported correctly, the way to gain root privileges of the target device can be preferred. Thus, it will be more possible to obtain data from the targeted device that will provide insight into the investigation or prosecution. Although the method of gaining root privileges should not be preferred unless it is necessary, it may be necessary to resort to this route, especially if the investigation and prosecution are of great importance in terms of public interest.

However, there is not any practical research that shows how to acquire physical images or vast amounts of data by acquiring logical images from an Android phone that has no root privileges in the first place. This research finds that there will be very limited data obtainable for digital forensics from unrooted smartphones, especially the ones which have newer versions of Android.

This study explained what steps to take before acquiring the image, how to get the logical image without gaining root authority, differences between logical images taken with and without root privileges, the methodology to decide which image should be obtained, and how to analyze the obtained logical image; it has offered a solution to obtain data swiftly by a tool called Android Triage that will be sufficient for the initial stage in the examination of digital evidence. Android

Triage tool is used on unrooted Android smartphones, and which data can be obtainable with this tool from unrooted target Android smartphones is shown. Also, the ALEAPP tool is used on a logical image taken from a rooted Android smartphone for logical image analysis. This way, an obtainable amount of data differentiation with or without root privileges is demonstrated.

## Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

## References

- [1] Curry, D. (2022) Android Statistics (2021). Business of Apps. <https://www.businessofapps.com/data/android-statistics/>
- [2] AlHidaifi, S. (2018) Mobile Forensics: Android Platforms and WhatsApp Extraction Tools. *International Journal of Computer Applications*, **179**, 25-29. <https://doi.org/10.5120/ijca2018917264>
- [3] Ashawa, M. and Ogwuche, I. (2017) Forensic Data Extraction and Analysis of Left Artifacts on Emulated Android Phones: A Case Study of Instant Messaging Applications. *Seizure*, **19**, 8-16. <https://doi.org/10.22632/ccs-2017-252-67>
- [4] Jeffay, J. (2024) Smartphone Is the Key to Solving Crime with AI. NoCamels. <https://nocamels.com/2023/02/smartphone-is-the-key-to-solving-crime-with-ai/>
- [5] Petrosyan, A. (2024) Targets of External Attacks Global 2023. Statista. <https://www.statista.com/statistics/1451097/targets-of-external-attacks-worldwide/>
- [6] Tajuddin, T.B. and Manaf, A.A. (2015) Forensic Investigation and Analysis on Digital Evidence Discovery through Physical Acquisition on Smartphone. 2015 *World Congress on Internet Security (WorldCIS)*, Dublin, 19-21 October 2015, 132-138. <https://doi.org/10.1109/WorldCIS.2015.7359429>
- [7] Taylor, P. (2024) Forecast Number of Mobile Users Worldwide 2020-2025. Statista. <https://www.statista.com/statistics/218984/number-of-global-mobile-users-since-2010/>
- [8] Daware, S., Dahake, S. and Thakare, V.M. (2012) Mobile Forensics: Overview of Digital Forensic, Computer Forensics vs. Mobile Forensics and Tools. *International Journal of Computer Applications*, **2012**, 7-8.
- [9] Srivastava, H. and Tapaswi, S. (2015) Logical Acquisition and Analysis of Data from Android Mobile Devices. *Information and Computer Security*, **23**, 450-475. <https://doi.org/10.1108/ICS-02-2014-0013>
- [10] Çakır, H. and Kiliç, M.S. (2013) An Overview of Methods of Obtaining Evidence on Cyber Crimes (Bilişim suçlarına ilişkin delil elde etme yöntemlerine genel bir bakış). *Polis Bilimleri Dergisi*, **15**, 23-44.
- [11] Harding, S. (2024) Why Mobile Digital Forensics Is a Growing Field. <https://studyonline.port.ac.uk/blog/mobile-forensics>
- [12] Freiling, F., Groß, T., Latzo, T., Müller, T. and Palutke, R. (2018) Advances in Forensic Data Acquisition. *IEEE Design & Test*, **35**, 63-74. <https://doi.org/10.1109/MDAT.2018.2862366>
- [13] Kessler, G.C. and Carlton, G.H. (2014) A Study of Forensic Imaging in the Absence of Write-Blockers. *Journal of Digital Forensics, Security and Law*, **9**, Article 4. <https://doi.org/10.15394/jdfsl.2014.1187>
- [14] Feng, P., Li, Q., Zhang, P. and Chen, Z. (2018) Logical Acquisition Method Based

- on Data Migration for Android Mobile Devices. *Digital Investigation*, **26**, 55-62. <https://doi.org/10.1016/j.diin.2018.05.003>
- [15] Kävrestad, J. (2020) Collecting Data. In: Kävrestad, J., Ed., *Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications*, Springer International Publishing, Cham, 101-113. [https://doi.org/10.1007/978-3-030-38954-3\\_11](https://doi.org/10.1007/978-3-030-38954-3_11)
- [16] EC-Council (2024) How to Handle Data Acquisition in Digital Forensics. Cybersecurity Exchange. <https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/data-acquisition-digital-forensics/>
- [17] Lukito, N.Y.P., Yulianto, F.A. and Jadied, E. (2016) Comparison of Data Acquisition Technique Using Logical Extraction Method on Unrooted Android Device. 2016 *4th International Conference on Information and Communication Technology (ICoICT)*, Bandung, 25-27 May 2016, 1-6. <https://doi.org/10.1109/ICoICT.2016.7571934>
- [18] (2021) Questions about Rooting without Unlocking Bootloader? General Questions and Answers. <https://forum.xda-developers.com/t/questions-about-rooting-without-unlocking-bootloader.4281491/>
- [19] Android Authority (2024) We Asked, You Told Us: Your Android Phone Definitely Isn't Rooted. <https://www.androidauthority.com/android-phone-rooted-poll-results-3225345/>
- [20] Akarawita, I., Perera, A. and Atukorale, A. (2015) ANDROPHSY—Forensic Framework for Android. 2015 *Fifteenth International Conference on Advances in ICT for Emerging Regions (ICTer)*, Colombo, 24-26 August 2015, 250-258. <https://doi.org/10.1109/ICTER.2015.7377696>
- [21] Reality Net (2021) Android\_Triage. [https://github.com/RealityNet/android\\_triage](https://github.com/RealityNet/android_triage)
- [22] Da Silveira, C.M., et al. (2020) Methodology for Forensics Data Reconstruction on Mobile Devices with Android Operating System Applying In-System Programming and Combination Firmware. *Applied Sciences*, **10**, Article 4231. <https://doi.org/10.3390/app10124231>
- [23] Backtrack and Deft Linux Experts (2022) Tsurugi Linux. <https://tsurugi-linux.org/index.php>
- [24] Aji, M., Hariyadi, D. and Rochmadi, T. (2020) Logical Acquisition in the Forensic Investigation Process of Android Smartphones Based on Agent Using Open Source Software. *IOP Conference Series: Materials Science and Engineering*, **771**, Article ID: 012024. <https://doi.org/10.1088/1757-899X/771/1/012024>
- [25] Zhang, H., Chen, L. and Liu, Q. (2018) Digital Forensic Analysis of Instant Messaging Applications on Android Smartphones. 2018 *International Conference on Computing, Networking and Communications (ICNC)*, Maui, 5-8 March 2018, 647-651. <https://doi.org/10.1109/ICNC.2018.8390330>
- [26] Yalçın, N. and Kılıç, B. (2019) Digital Evidences According to ISO/IEC 27035-2, ISO/IEC 27037, ISO/IEC 27041, ISO/IEC 27042 and ISO/IEC 27043 Standards. *SETSCI-Conference Proceedings*, **9**, 444-449. <https://doi.org/10.36287/setsci.4.6.118>
- [27] Alexis, B. (2021) ALEAPP-Master. <https://github.com/abrignoni/ALEAPP>
- [28] Racioppo, C. and Murthy, N. (2012) Android Forensics: A Case Study of the 'HTC Incredible' Phone. *Proceedings of Student-Faculty Research Day*, New York, May 2012, 8.

- [29] Sathe, S.C. and Dongre, N.M. (2018) Data Acquisition Techniques in Mobile Forensics. 2018 *2nd International Conference on Inventive Systems and Control (ICISC)*, Coimbatore, 19-20 January 2018, 280-286.  
<https://doi.org/10.1109/ICISC.2018.8399079>
- [30] DFIR Science (2022) Logical Image Created with Root Authority.  
[https://www.youtube.com/watch?v=\\_cm1n0stVrA](https://www.youtube.com/watch?v=_cm1n0stVrA)