Mobile and Forensics
Vol. 4, No. 2, September 2022, pp. 102-114
ISSN: 2714-6685 (online), 2656-6257 (print)
DOI: 10.12928/mf.v4i2.6355

Comparative Forensic Analysis of Android based Social Media Applications

Naveed Naeem Abbas[a,1,*], Adeel Ahmed Zeerak[a,2],
Mohammad Awais Javaid[a,3], Mehdi Hussain[a,4]
[a]School of Electrical Engineering and Computer Science, National University of Sciences and Technology (NUST), Islamabad - Pakistan.
[1]nabbas.phdcs21seecs@seecs.edu.pk, [2*]azeerak.msis21seecs@seecs.edu.pk,
[3]mjavaid.msis21seecs@seecs.edu.pk, [4]mehdi.hussain@seecs.edu.pk
[*]Corresponding email

Abstract

Smartphones are increasing worldwide rapidly. It works as a personal assistant that helps us master our everyday life. This is the reason why forensic experts always try to get the most crucial evidence from smartphones. While doing a forensic analysis of smartphones there is a need to identify the programs/files containing malicious actions or activity. Most of the users' information resides inside the digital device and should be extracted carefully as it is needed for further users' entity and behavior analytics. In this study, we used the most famous forensic tools MOBILedit and Autopsy for efficient extraction of potential evidence from the Android file system. The file system images from different android devices (rooted and unrooted) are extracted on multiple analyses (type-based, size-based). Additionally, a timeline of the log files has also been made, which can assist the investigator in locating any log files that were updated or altered at the scene of the crime by suspects or victims.

Keywords: Mobile Forensic, Android Forensic, Image Analysis, Social Application Analysis.

INTRODUCTION

Smartphones are increasing worldwide rapidly. According to the report, the number of smartphone users in the world is 6.648 billion, which translates to 83.72% of the world's population owning a smartphone [1]. It works as a personal assistant that helps us master our everyday life. On the other side, the applications that are installed on smartphones for communication purpose contains logs or user records. For this purpose, all logs related to user data are recorded inside the mobile, mostly people are using banking applications or e-commerce applications that consist of various financial transactions. The aim of this study is to perform a comprehensive analysis of both (published on google play store and third-party) applications (Table 4) on the android device for the extraction of relevant evidence.

The field of mobile forensics is growing continuously even after the emergence of IoT devices and their integration with smartphones. With the development of information and communication technology, the emergence of devices can be seen. However, forensic investigators try to deal with some difficulties during the examination, 1) ROM of smartphones is increasing rapidly, which makes investigator difficult to analyze huge amounts of data and identify specific data related to crimes [2]. 2) Enough time and money are required for user behavior analytics [3]. 3) There is a

Article History: *Received July 08, 2022; Revised August 17, 2022; Accepted August 19, 2022*

possibility of an unpublished application to be installed on mobile when it is involved in a crime scene and the forensic investigator won't be able to analyze that critical application and much-needed evidence can be skipped.

D. Kim et al. [5] approach, was based on three phases: 1) Grouping of potential evidence 2) Identification of potential evidence and 3) Taxonomy of Android data and management of acquired evidence but they failed to overcome the analyzing the application's data through user's entire timeline. To avoid the difficulties, in this study, we have used multiple techniques to investigate smartphones equipped with the open-source Android operating system. In the proposed approach, we succeed in grouping the data based on application type, size and have successfully identified the potential evidence, and how to retrieve user-related information from the application logs.

Table 1 presents the general criteria for examining any evidence.

D. Kim et al. [5] approach, was based on three phases: 1) Grouping of potential evidence 2) Identification of potential evidence and 3) Taxonomy of Android data and management of acquired evidence but they failed to overcome the analyzing the application's data through user's entire timeline. To avoid the difficulties, in this study, we have used multiple techniques to investigate smartphones equipped with the open-source Android operating system. In the proposed approach, we succeed in grouping the data based on application type, size and have successfully identified the potential evidence, and how to retrieve user-related information from the application logs.

Table 1. Criteria for validating the integrity of digital evidence [4]

Criteria	Relevant Questions	Process Implementation
Transparency	Is it possible to examine digital evidence independently?	Uses consistently reproducible method
Meaning	Is the semantics of digital evidence did not alter the process of digital forensics?	Using hashing preserves the initial structure of evidence
Errors	Have all errors been reasonably identified?	Accounts for and reports errors.
Experience	Does the individual have relative experience in the field of digital forensics?	Professional entities are required

The rest of the chapter is structured as follows. Section 2 discusses the literature review. Section 3, and Section 4 present the proposed methodology and implementation. Section 5 contains the experimental result. In the end, Section 6 concludes.

LITERATURE REVIEW

There is growing concern about the ever-increasing amount of data on how digital forensics can enable analysis timely [6]. Predictions show that smartphone storage capacity will increase by an average of 70GB by the end of 2019, and the world is witnessing the latest launch of the Samsung Galaxy S10 Plus with 1.1TB of storage. Investigators and investigators consider mobile devices to be the most important component in conducting important forensic investigations, as they contain a lot of important personal information. [7]. Recent research shows that the increase in data which was a way significant makes it difficult for investigators to properly observe and identify crime-related data from the vast amount of data collected by mobile devices.

In the last decade, research related to mobile forensics focuses on technology collection, and in latest years the focus has turned around to evaluating applications that people used mostly. R. Ahmed et al. [8] examines the information obtained from mobile phones in detail which can later be used as potential evidence. The emerging technologies have also been discussed concerning on the evidence-based on mobile phones. F. Marturana et al. [9] introduced the latest way to classify phone's usage based on prediction. The above facts derived from research were discussed it details with the cybercrime specialists of Italy. It was all done to look for a more appropriate set of methods to find out the evidence that a smartphone is used to perform the specific crime and that can be very relevant when dealing with the cases like pedophilia. A detailed review of the digital forensics techniques and have discussed multiple opportunities which much be seen to introduce new and workable methodologies which will lead to a solution in upcoming days [10]. M. M. Cruz-Cunha et al. [11] demonstrated the extensive review of the literature and the main topics were related to forensics especially mobile forensics was based on methodology of PRISMA, the intent was to uplift and amplify the investigation process of mobile forensics and permit for a powerful knowledge which is not old and is completely up to date by working the available tactics and techniques. V. Fernando et al. [12] introduced a study on how we can select the appropriate or suitable forensic tool for cybercrime, it has been seen that in many previous studies researchers have not selected the suitable tool related to crime that alternate or destroy the evidence. A. Al-Sabaawi et al. [13] demonstrated the work that was based on challenges related to android forensics i.e., android application complexity, various methods and techniques to get the data, problems which were faced in setting up hardware, and using the tools for acquiring the data which are commercial and have a very high cost but in the end, the tools also failed to extract out the data from an image which was acquires using a physical acquisition of data. J. Grover et al. [14] developed a corporate level monitoring system for smartphones based on android which collects a dataset of incidents without root privileges. It was a latest strategy designed to be used for multiple components which are very useful in the monitoring of platforms which are based on android. H. H. B. Bhushan et al. [15] mainly focuses on the issues related to the anti-forensic technique that how it is handled in android-based smartphones and how there can be an improvement in the field of smartphone forensics and acquisition of data. It is also briefed in the research how to acquire the files during the investigation process, what type of techniques time perform a role of aid to tamper the evidence found, and how one can differentiate between the data which is tampered with or not. S. Hu et al. [16] illustrated the scheme for data of mobile phone which was based on blockchain and is known as a trusted scheme of forensics for smartphones. In this research uses the mechanism of access control to realize the authorization of police investigators and experts of forensics to their evidence. A. Ahmad et al. [1] worked on identifying stored artifacts on the mobile devices left behind by the android video streaming applications. M. R. Arshad et al. [17] analyze the storage, registry, and memory of Windows 10 devices and the memory, logs, storage, and Zram of Android 10 devices for three possible scenarios i.e. before, during, and after use of the Tor browser. A. Afzal et al. [18] give a network forensic technique to find the potential artifacts from the encrypted network traffic of the famous social messenger applications. After that, the forensic experts analyzed the potential evidence and generated a detailed evaluation report related to that. Table 2 includes an analysis of existing studies and their approach.

Table 2. Analysis of Existing Research

Reference	Platform	Methodology	Target artifacts	Tools	Limitation of work
H. H. Lwin et al. [19] (2020)	Android	The acquisition methods i.e. the logical methods and physical methods have been used to acquire images of android devices and then later analyzed the image to get data	Different tools are used for logical and physical acquisition to acquire android artifacts	Belkasoft, Magnet Acquire	Did not applicable to commercial and open-sourapplicationsion.
S. C. Sathe et al. [20] (2018)	Android	Multiple techniques to acquire digital evidence were there but the most appropriate technique to be selected	Used logical and physical acquisition to acquire android artifacts	Cellebrite UFED, MOBILedit, Oxygen Forensics, and XRY	Did not extract from unpublished applications
T. Almehmadi et al. [21] (2019)	Android	One technique to acquire a mobile image is to root the device but this paper discusses the alternatives to rooting and validates the forensic soundness of rooting	Mobile applications artifacts	Belkasoft Evidence Center v9.2, FileAlyzer v2.0	The device must be rooted.
P. Feng et al. [22] (2019)	Android	The private data acquisition method (PASM) is used in the migration of data at the system level which is a build-in functionality provided by manufacturers of android to transfer the application's private data and load them into a new device	Private data	Dumpit, Volatility	The device must be rooted.
C. Anglano et al. [23] (2019)	Android	To analyze the applications of android, the activities related to automation were carried out to validate the acquired image by presenting the latest implementation, design	WhatsApp, SMS, Call logs, MMS, images, videos	AnForA	Did not extract from unpublished applications
C. M. da Silveira et al. [24] (2020)	Android	This underlying methodology permits to view of the usage of a technique i.e. In-System Programming (ISP). Firmware	Artifacts from encrypted devices	UFED Touch 2, UFED Physical Analyzer	Cannot bypass the android devices secure boot mechanism

Reference	Platform	Methodology	Target artifacts	Tools	Limitation of work
		combination is its main usage which has been aligned with a special process of analysis and collection			
R. Zhang et al. [25] (2022)	Android	Presented a forensic system for smartphones based on android i.e., a forensic system that can be controlled remotely. It allows the investigators effectively acquire a huge number of artifacts that are forensically sound and scale them to top-level	Wide range of social media applications artifacts	RAFT, GRR, MOBILedit, XRY Forensic Examiner's Kit	Different OS compatibilities issue as the number of applications is increased
J. A. M. Jeyaseeli et al. [26] (2021)	Android	Acquiring an image of operating system based on Android OS and extracting the data of applications like GSM Calls, Short Message Service, Videos and Pictures, WhatsApp related contents which are saved anywhere in devices	WhatsApp, SMS, Call logs, MMS, images, videos	Android Debug Bridge, Aspeaksoft Android toolkit	Did not extract from unpublished applications

METHODS

The algorithm presented in the [5] divides into three major sub-problems discussed below:

Grouping of potential evidence

Firstly, they organize the immense number of files from an Android phone application and use attribute information from each group to indicate a classification that need to be analyzed and what kind of illegal activity is reported. By taking the data of android and to make abstract from it and later need to be explored, they have discovered a way to smartly handle the artifacts and directories which are to be investigated i.e., Files->Groups -> Potential Evidence Groups.

Extraction of application attributes

Android's security design gives every application a separate unique identifier and sandboxes it so they can access only its own authorized data. Some applications require you to use system services, data from other programs, or data generation in the SD card area. Android allows these relevant permissions in manifest xml file which is located in the APK file. These files can be used to extract permissions and other attributes of the applications.

Data grouping based on app

Files connected to individual applications are dispersed multiple locations in the file system and detecting and correlating all the associated files that may analyze mutual relationships, and date every isolated file.

Identification of potential evidence groups

After successful grouping of data, it is then organized recognized and classed as Potential Evidence Groups (PEGs). The ones which are identified now need to be investigated based on crime type.

Identification of potential evidence

In this section, the files are classified and analyzed and included within PEGs to find the artifacts within the file that are associated with crime. The abstracted data is then provided to Potential Evidence Groups -> Potential Evidence Sets to manage potential evidence. The overall technique is depicted in Figure 1.

Signature-based classification of file format

System files and other ones are categorized based on their signature to correctly select the files to inspect.

Identification of app logs containing user information

The data types in application logs on tested mobiles are examined & used to discover valuable information about user as well as a timestamp. By detecting and retrieving the information of users left in the logs of application, the files required for User Behavior and Analysis were investigated.

Management of potential evidence and Android data taxonomy

This section elaborates on how to organize the potential evidence that was finally picked in the previous two sections, as well as classification of application logs by the sorting out information of user contained in it. That is, Android data is abstracted into Potential Evidence Groups -> Potential Evidence Sets -> AFXML to manage potential evidence.

Management of potential evidence

Files within the same PEG can be produced or modified by the user's particular actions, they must be cross analyzed. As a result, we propose selecting potential evidence from the PEG files that need to be investigated and managing it as a Potential Evidence Set (PES). To organize all PESs (Potential Evidence Groups -> Potential Evidence Sets), a format called Android Forensics XML (AFXML) was created.

Android data taxonomy

Using the algorithm discussed above, we can categorize practically all Android Image files based on the app's qualities and the type and characteristics of user information provided in the file. We suggest this as a new Android data taxonomy since it may be used to properly identify app logs that are vital for studying user activity, especially in genuine forensic investigations.

IMPLEMENTATION

The given paper uses around 33 android devices for the testing of the proposed algorithm but due to limitations of availability of resources and public implementation of the algorithm, we have simulated the algorithm using Autopsy and MOBILedit tools.

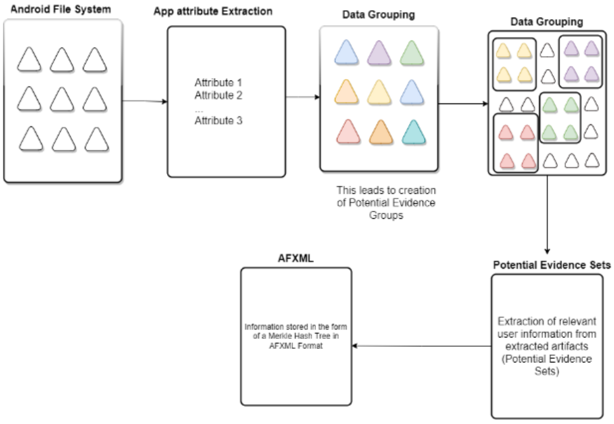

Android File System
App attribute Extraction
Attribute 1
Attribute 2
...
Attribute 3
Data Grouping
This leads to creation of Potential Evidence Groups
Data Grouping
Potential Evidence Sets
Extraction of relevant user information from extracted artifacts (Potential Evidence Sets)
AFXML
Information stored in the form of a Merkle Hash Tree in AFXML Format

Figure 1. Potential Evidence Extraction

Table 3. Android Devices Details

Sr #	Device Name	Android Version	RAM	ROM	Rooted
1	Infinix X521	7.1.2	3 GB	16 GB	No
2	Nox Emulator	7.1.2	3.4 GB	120 GB	Yes
3	Huawei T1 701U	4.4.2	1 GB	16 GB	Yes

Table 4 represents the applications and their versions for analyzing android file system.

Table 4. Applications used for Analysis

Sr.	Application	Version	Status
1	Gmail	2022.05.01.44951655	Published
2	Facebook	340.0.0.27.113	Published
3	Instagram	235.0.0.21.107	Published
4	Viber	17.5.0.6	Published
5	Mico	7.0.4.1	Published
6	Meetme	14.40.1.3500	Published
7	Tango	7.13.1631519493	Published
8	Snapchat	11.79.0.34	Published
9	Photo Editor	1.0	Third-party

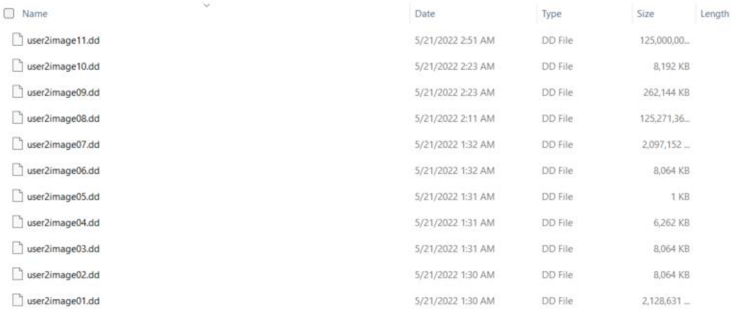
The applications on both devices are used to communicate with each other, which creates log files to analyze.

Creating android Image

To create an image of the android emulator devices, we have used following process:

- Root the device by installing KingoRoot and BusyBox
- Once the device is rooted, we can use adb, ncat and adb to create raw image of the android filesystem.

It can be seen in Figure 2 a total of 11 images are created for each device. Each image file created represents a single partition of the storage disk of the android devices which results in multiple files of different sizes.



Name	Date	Type	Size	Length
user2image11.dd	5/21/2022 2:51 AM	DD File	125,000,00...	
user2image10.dd	5/21/2022 2:23 AM	DD File	8,192 KB	
user2image09.dd	5/21/2022 2:23 AM	DD File	262,144 KB	
user2image08.dd	5/21/2022 2:11 AM	DD File	125,271,36...	
user2image07.dd	5/21/2022 1:32 AM	DD File	2,097,152 ...	
user2image06.dd	5/21/2022 1:32 AM	DD File	8,064 KB	
user2image05.dd	5/21/2022 1:31 AM	DD File	1 KB	
user2image04.dd	5/21/2022 1:31 AM	DD File	6,262 KB	
user2image03.dd	5/21/2022 1:31 AM	DD File	8,064 KB	
user2image02.dd	5/21/2022 1:30 AM	DD File	8,064 KB	
user2image01.dd	5/21/2022 1:30 AM	DD File	2,128,631 ...	

Figure 2. Android File System Images

Analyzing Android Images

Autopsy

Autopsy allows us to group data based on multiple factors (filetypes, Data Artifacts, File Size, Time, etc.). The android file system images are analyzed based on multiple factors which are discussed below:

Timeline

Figure 3 represents a timeline of events generated in the android devices which can help us narrow down PEG by selecting events around the time of crime. See.

File Type

It is also possible to search for specific file types across the android file system relating to our case. An example of search of image files on the image is shown in Figure 4.

Data Artifacts

The specific type of artifacts like calls, messages, can also be filtered. e.g., contacts can be seen in Figure 5.

MOBILedit

MOBILedit provides us with multiple levels of analysis of the android device image. We have conducted following analysis for android device images

Specific Selection (Search through android file system for specific keywords)

Specific Selection Analysis can be done to filter files/applications based on specific keyword that could form our potential evidence group. Specific Search for 'user' across all applications. See Figure 6.

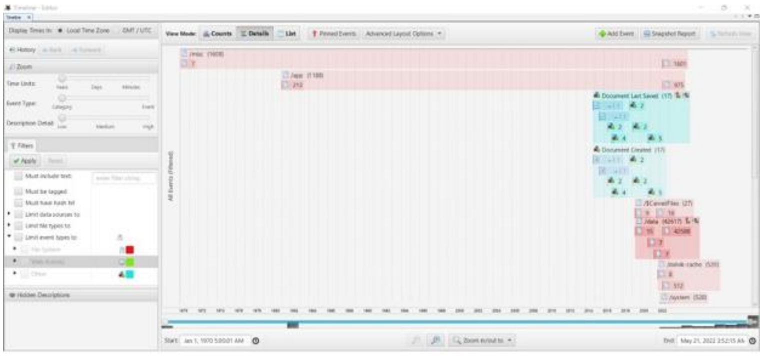
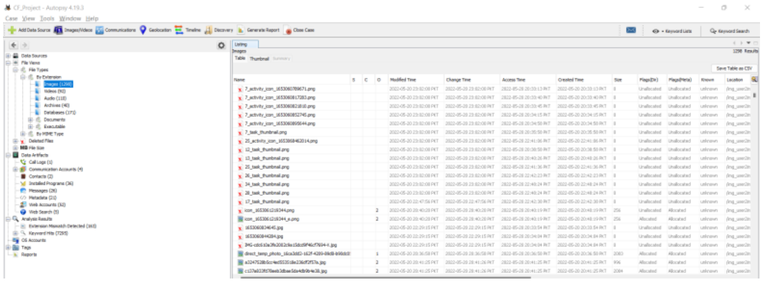
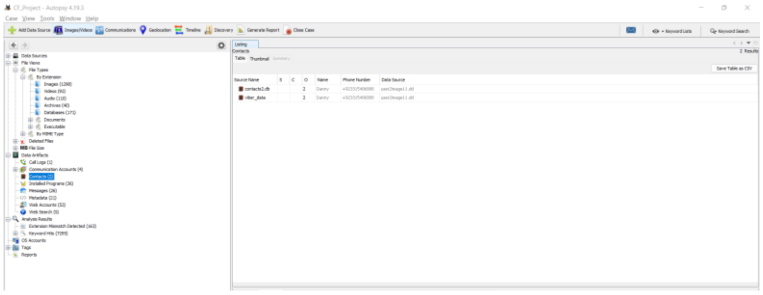


Figure 3. Temporal Analysis



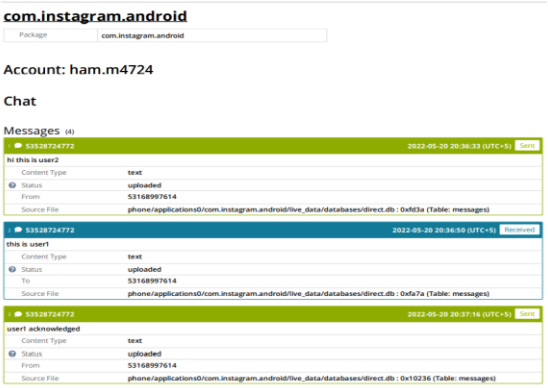
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
7_activity_icon_1653060789671.png				2022-05-20 23:02:08 PKT	2022-05-20 23:02:08 PKT	2022-05-20 20:33:13 PKT	2022-05-20 20:33:13 PKT	0	Unallocated	Unallocated	unknown	/img_user2in
7_activity_icon_1653060817283.png				2022-05-20 23:02:08 PKT	2022-05-20 23:02:08 PKT	2022-05-20 20:33:40 PKT	2022-05-20 20:33:40 PKT	0	Unallocated	Unallocated	unknown	/img_user2in
7_activity_icon_1653060821818.png				2022-05-20 23:02:08 PKT	2022-05-20 23:02:08 PKT	2022-05-20 20:33:45 PKT	2022-05-20 20:33:45 PKT	0	Unallocated	Unallocated	unknown	/img_user2in
7_activity_icon_1653060852745.png				2022-05-20 23:02:08 PKT	2022-05-20 23:02:08 PKT	2022-05-20 20:34:15 PKT	2022-05-20 20:34:15 PKT	0	Unallocated	Unallocated	unknown	/img_user2in
7_activity_icon_1653060895644.png				2022-05-20 23:02:08 PKT	2022-05-20 23:02:08 PKT	2022-05-20 20:34:50 PKT	2022-05-20 20:34:50 PKT	0	Unallocated	Unallocated	unknown	/img_user2in
7_task_thumbnail.png				2022-05-20 23:02:08 PKT	2022-05-20 23:02:08 PKT	2022-05-20 20:35:50 PKT	2022-05-20 20:35:50 PKT	0	Unallocated	Unallocated	unknown	/img_user2in
25_activity_icon_1653068462014.png				2022-05-20 23:02:08 PKT	2022-05-20 23:02:08 PKT	2022-05-20 22:41:06 PKT	2022-05-20 22:41:06 PKT	0	Unallocated	Unallocated	unknown	/img_user2in
12_task_thumbnail.png				2022-05-20 23:02:08 PKT	2022-05-20 23:02:08 PKT	2022-05-20 20:38:50 PKT	2022-05-20 20:38:50 PKT	0	Unallocated	Unallocated	unknown	/img_user2in
13_task_thumbnail.png				2022-05-20 23:02:08 PKT	2022-05-20 23:02:08 PKT	2022-05-20 20:40:26 PKT	2022-05-20 20:40:26 PKT	0	Unallocated	Unallocated	unknown	/img_user2in
25_task_thumbnail.png				2022-05-20 23:02:08 PKT	2022-05-20 23:02:08 PKT	2022-05-20 22:41:36 PKT	2022-05-20 22:41:36 PKT	0	Unallocated	Unallocated	unknown	/img_user2in
26_task_thumbnail.png				2022-05-20 23:02:08 PKT	2022-05-20 23:02:08 PKT	2022-05-20 22:42:23 PKT	2022-05-20 22:42:23 PKT	0	Unallocated	Unallocated	unknown	/img_user2in
34_task_thumbnail.png				2022-05-20 23:02:08 PKT	2022-05-20 23:02:08 PKT	2022-05-20 22:48:24 PKT	2022-05-20 22:48:24 PKT	0	Unallocated	Unallocated	unknown	/img_user2in
28_task_thumbnail.png				2022-05-20 23:02:08 PKT	2022-05-20 23:02:08 PKT	2022-05-20 22:48:24 PKT	2022-05-20 22:48:24 PKT	0	Unallocated	Unallocated	unknown	/img_user2in
17_task_thumbnail.png				2022-05-20 22:47:56 PKT	2022-05-20 22:47:56 PKT	2022-05-20 22:42:30 PKT	2022-05-20 22:42:30 PKT	0	Unallocated	Unallocated	unknown	/img_user2in
icon_1653061216344.png			2	2022-05-20 20:40:20 PKT	2022-05-20 20:40:20 PKT	2022-05-20 20:40:19 PKT	2022-05-20 20:40:19 PKT	256	Unallocated	Allocated	unknown	/img_user2in
icon_1653061216344_e.png			2	2022-05-20 20:40:20 PKT	2022-05-20 20:40:20 PKT	2022-05-20 20:40:19 PKT	2022-05-20 20:40:19 PKT	256	Allocated	Allocated	unknown	/img_user2in
1653060834645.jpg				2022-05-20 22:29:15 PKT	2022-05-20 22:29:15 PKT	2022-05-20 20:33:54 PKT	2022-05-20 20:33:54 PKT	0	Unallocated	Unallocated	unknown	/img_user2in
1653060844284.jpg				2022-05-20 22:29:15 PKT	2022-05-20 22:29:15 PKT	2022-05-20 20:34:04 PKT	2022-05-20 20:34:04 PKT	0	Unallocated	Unallocated	unknown	/img_user2in
IMG-cdc610a3fe2082c9a15dcd9f46cf7694-V.jpg				2022-05-20 22:29:15 PKT	2022-05-20 22:29:15 PKT	2022-05-20 20:34:04 PKT	2022-05-20 20:34:04 PKT	0	Unallocated	Unallocated	unknown	/img_user2in
direct_temp_photo_16ca3dd2-162f-4289-89d8-b98dc0			1	2022-05-20 20:36:58 PKT	2022-05-20 20:36:58 PKT	2022-05-20 20:36:50 PKT	2022-05-20 20:36:50 PKT	2083	Allocated	Allocated	unknown	/img_user2in
a32475280b5cc4ed5535b8e236df2f57a.jpg			2	2022-05-20 20:41:25 PKT	2022-05-20 20:41:26 PKT	2022-05-20 20:41:25 PKT	2022-05-20 20:41:25 PKT	996	Allocated	Allocated	unknown	/img_user2in
c137a033ffd76eeb3dbae5da4db9b4e38.jpg			2	2022-05-20 20:41:25 PKT	2022-05-20 20:41:26 PKT	2022-05-20 20:41:25 PKT	2022-05-20 20:41:25 PKT	2084	Allocated	Allocated	unknown	/img_user2in

Figure 4. Grouping based on file type



Source Name	S	C	O	Name	Phone Number	Data Source
contacts2.db			2	Danny	+923335466688	user2image11.dd
viber_data			2	Danny	+923335466688	user2image11.dd

Figure 5. Grouping based on data artifacts



com.instagram.android

Package	com.instagram.android

Account: ham.m4724

Chat

Messages (4)

1 53528724772 2022-05-20 20:36:33 (UTC+5) Sent

hi this is user2

Content Type	text
Status	uploaded
From	53168997614
Source File	phone/applications0/com.instagram.android/live_data/databases/direct.db : 0xfd3a (Table: messages)

2 53528724772 2022-05-20 20:36:50 (UTC+5) Received

this is user1

Content Type	text
Status	uploaded
To	53168997614
Source File	phone/applications0/com.instagram.android/live_data/databases/direct.db : 0xfa7a (Table: messages)

3 53528724772 2022-05-20 20:37:16 (UTC+5) Sent

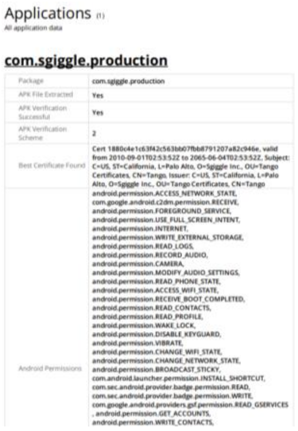
user1 acknowledged

Content Type	text
Status	uploaded
From	53168997614
Source File	phone/applications0/com.instagram.android/live_data/databases/direct.db : 0x10236 (Table: messages)

Figure 6. Keyword "User" searching

Application Analysis (Details about a single application)

Specific Application Analysis can be done to analyze a single application. Specific Application for Tango across all applications is represented in Figure 7.



Applications (1)
All application data

com.sgiggle.production

Package	com.sgiggle.production
APK File Extracted	Yes
APK Verification Successful	Yes
APK Verification Scheme	2
Best Certificate Found	Cert 1880c4e1c63f42c563bb07fbb8791207a82c946e, valid from 2010-09-01T02:53:52Z to 2065-06-04T02:53:52Z, Subject: C=US, ST=California, L=Palo Alto, O=Sgiggle Inc., OU=Tango Certificates, CN=Tango, Issuer: C=US, ST=California, L=Palo Alto, O=Sgiggle Inc., OU=Tango Certificates, CN=Tango
Android Permissions	android.permission.ACCESS_NETWORK_STATE, com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_SERVICE, android.permission.USE_FULL_SCREEN_INTENT, android.permission.INTERNET, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_LOGS, android.permission.RECORD_AUDIO, android.permission.CAMERA, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.READ_PHONE_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.READ_CONTACTS, android.permission.READ_PROFILE, android.permission.WAKE_LOCK, android.permission.DISABLE_KEYGUARD, android.permission.VIBRATE, android.permission.CHANGE_WIFI_STATE, android.permission.CHANGE_NETWORK_STATE, android.permission.BROADCAST_STICKY, com.android.launcher.permission.INSTALL_SHORTCUT, com.sec.android.provider.badge.permission.READ, com.sec.android.provider.badge.permission.WRITE, com.google.android.providers.gsf.permission.READ_GSERVICES , android.permission.GET_ACCOUNTS, android.permission.WRITE_CONTACTS,

Figure 7. Application Analysis

Experimental Results:

Table 5 presents the results that have been achieved through Autopsy and MOBILedit applications. The file system analysis is conducted to extract and analyze the artifacts that provide the relevant information related to the application being tested. Additionally, the application details along with the relevant artifacts were also successfully extracted for unpublished and custom applications Also, the relevant artifacts were successfully retrieved from the unrooted device which is a limitation of much existing research work. The following additional analyses are performed for efficient results which are summarized in Table 5.

- Type-baseded Grouping
- Size-baseded Grouping
- Data Artifacts
- Temporal (Timeline) Analysis

Table 5. Android Application Analysis Results

Sr. #	Application	Attributes Extracted			
		Permissions	Log Files	Data	Media
1	Gmail	No	Yes	Yes	Yes
2	Facebook	No	Yes	Yes	Yes
3	Instagram	Yes	Yes	Yes	Yes
4	Viber	No	Yes	Yes	Yes
5	Mico	No	Yes	Yes	Yes
6	Meetme	No	Yes	Yes	Yes
7	Tango	No	Yes	Yes	Yes
8	Snapchat	No	Yes	Yes	No
9	PhotoEditor	Yes	Yes	Yes	Yes

CONCLUSION

The primary objective of the research paper was efficiently extraction of crime-related evidence from the Android file system. The proposed approach is simulated which was inspired by (Kim and Lee 2020) method. We employed the Autopsy and MOBILedit tools. In experimentation, application data is extracted and analyzed with the above tools. Moreover, we have also performed File-based analysis, application level e.g. Table 5 enlists all the artifacts extracted from different applications. A total of 9 applications (Table 4) were analyzed and information regarding the permissions, logs, data, and media files were obtained. The actual media files were also extracted along with the information. It helped in narrowing down the potential evidence areas in the Android file system. Lastly, a timeline is extracted from the log files which helped an investigator to identify the modified or altered log file at the time of crime by suspects or victims.

REFERENCES

[1] A. Ahmad, Mehdi Hussain, "A Forensic Analysis of Video Streaming Activities on Android Applications," *Mob. Forensics*, vol. 4, no. 1, pp. 44–52, 2022, doi: https://doi.org/10.12928/mf.v4i1.5762.

[2] B. Thesis, D. Patapas, "Investigation of Digital Forensic Methods for Mobile Devices," 2021.

[3] H. M. McGee, B. J. Crowley-Koch, "Performance Assessment of Organizations," *J. Organ. Behav. Manage.*, vol. 41, no. 3, pp. 255–285, 2021, doi: 10.1080/01608061.2021.1909687.

[4] F. Amato, A. Castiglione, G. Cozzolino, F. Narducci, "A semantic-based methodology for digital forensics analysis," *J. Parallel Distrib. Comput.*, vol. 138, pp. 172–177, 2020, doi: 10.1016/j.jpdc.2019.12.017.

[5] D. Kim, S. Lee, "Study of identifying and managing the potential evidence for effective Android forensics," *Forensic Sci. Int. Digit. Investig.*, vol. 33, p. 200897, 2020, doi: 10.1016/j.fsidi.2019.200897.

[6] D. Quick and K. K. R. Choo, "Impacts of increasing volume of digital forensic data: A survey and future research challenges," *Digit. Investig.*, vol. 11, no. 4, pp. 273–294, 2014, doi: 10.1016/j.diin.2014.09.002.

[7] K. Barmpatsalou, T. Cruz, E. Monteiro, and P. Simoes, "Current and future trends in mobile device forensics: A survey," *ACM Comput. Surv.*, vol. 51, no. 3, 2018, doi: 10.1145/3177847.

[8] R. Ahmed, R.V. Dharaskar, Mobile forensics: an overview, tools, future trends and challenges from law enforcement perspective. In *6th international conference on e-governance, iceg, emerging technologies in e-government, m-government*, pp. 312-23, 2008.

[9] F. Marturana, G. Me, R. Bertè, and S. Tacconi, "A quantitative approach to triaging in mobile forensics," *Proc. 10th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2011, 8th IEEE Int. Conf. Embed. Softw. Syst. ICESS 2011, 6th Int. Conf. FCST 2011*, pp. 582–588, 2011, doi: 10.1109/TrustCom.2011.75.

[10] G. Gogolin, "Mobile forensics," *Digit. Forensics Explain.*, pp. 55–68, 2012, doi: 10.1201/b13689-10.

[11] M. M. Cruz-Cunha, N. R. Mateus-Coelho, IGI Global, *Handbook of research on cyber crime and information privacy*, vol. I, 2020.

[12] V. Fernando, "Cyber Forensics Tools: A Review on Mechanism and Emerging Challenges," *2021 11th IFIP Int. Conf. New Technol. Mobil. Secur. NTMS 2021*, 2021, doi: 10.1109/NTMS49979.2021.9432641.

[13] A. Al-Sabaawi, E. Foo, and E. Au, "A Comparison Study of Android Mobile Forensics for Retrieving Files System Handprint Recognition Technique Based in Image Segmentation for Recognize View project A Comparison Study of Android Mobile Forensics for Retrieving Files System," *Int. J. Comput. Sci. Secur.*, no. 13, pp. 2019–148, 2019.

[14] J. Grover, "Android forensics: Automated data collection and reporting from a mobile device," *Proc. Digit. Forensic Res. Conf. DFRWS 2013 USA*, vol. 10, pp. S12–S20, 2013, doi: 10.1016/j.diin.2013.06.002.

[15] H. H. B. Bhushan, S. M. Florance, "An Overview on Handling Anti Forensic Issues in Android Devices Using Forensic Automator Tool," 2022.

[16] S. Hu, S. Zhang, and K. Fu, "TFChain:Blockchain-based Trusted Forensics Scheme for Mobile Phone Data Whole Process," pp. 155–165, 2022, doi: 10.1109/itoec53115.2022.9734408.

[17] M. R. Arshad, M. Hussain, H. Tahir, S. Qadir, F. I. Ahmed Memon, and Y. Javed, "Forensic Analysis of Tor Browser on Windows 10 and Android 10 Operating Systems," *IEEE Access*, vol. 9, pp. 141273–141294, 2021, doi: 10.1109/ACCESS.2021.3119724.

[18] A. Afzal, M. Hussain, S. Saleem, M. K. Shahzad, A. T. S. Ho, and K. H. Jung, "Encrypted network traffic analysis of secure instant messaging application: A case study of signal messenger app," *Appl. Sci.*, vol. 11, no. 17, 2021, doi: 10.3390/app11177789.

[19] H. H. Lwin, W. P. Aung, and K. K. Lin, "Comparative Analysis of Android Mobile Forensics Tools," *2020 IEEE Conf. Comput. Appl. ICCA 2020*, 2020, doi: 10.1109/ICCA49400.2020.9022838.

[20] S. C. Sathe, N. M. Dongre, "Data acquisition techniques in mobile forensics," *Proc. 2nd Int. Conf. Inven. Syst. Control. ICISC 2018*, no. Icisc, pp. 280–286, 2018, doi: 10.1109/ICISC.2018.8399079.

[21] T. Almehmadi, O. Batarfi, "Impact of Android Phone Rooting on User Data Integrity in Mobile Forensics," *2nd Int. Conf. Comput. Appl. Inf. Secur. ICCAIS 2019*, 2019, doi: 10.1109/CAIS.2019.8769520.

[22] P. Feng, Q. Li, P. Zhang, and Z. Chen, "Private Data Acquisition Method Based on System-Level Data Migration and Volatile Memory Forensics for Android Applications," *IEEE Access*, vol. 7, pp. 16695–16703, 2019, doi: 10.1109/ACCESS.2019.2894643.

[23] C. Anglano, M. Canonico, and M. Guazzone, "The Android Forensics Automator (AnForA): A tool for the Automated Forensic Analysis of Android Applications," *Comput. Secur.*, vol. 88, 2020, doi: 10.1016/j.cose.2019.101650.

[24] C. M. da Silveira *et al.*, "Methodology for forensics data reconstruction on mobile devices with android operating system applying in-system programming and combination firmware," *Appl. Sci.*, vol. 10, no. 12, pp. 1–29, 2020, doi: 10.3390/app10124231.

[25] R. Zhang, M. Xie, and J. Bian, "ReLF: Scalable Remote Live Forensics for Android," pp. 822–831, 2022, doi: 10.1109/trustcom53373.2021.00117.

[26] J. A. M. Jeyaseeli and C. Shanthi, "Physical Data Extraction from Android mobile using Apeaksoft Android toolkit and Android Debug Bridge," vol. 8, no. 5, pp. 1913–1922, 2021.