Proposed Method for Mobile Forensics Investigation Analysis of Remnant Data on Google Drive Client

Gandeva Bayu Satrya, Soo Young Shin

IT Convergence Engineering, Kumoh National Institute of Technology, Republic of Korea
gbs@telkomuniversity.ac.id, wdragon@kumoh.ac.kr

Abstract

The best known software developers all offer cloud storage services. Microsoft offers Onedrive to its users, Apple offers iCloud Drive and Google offers Google Drive or GDrive. The battle between these software developers is ongoing and they will always strive to give the best services to their users. It is not only technology that is evolving, however, but also ways in which security can be breached and data abused. The security of information on the Internet is increasingly at risk and there are many threats to cloud storage platforms.

This research used the mobile forensics approach to help in identifying and analyzing user behavior that may occur while using GDrive application for cybercrime. The novelty of comparison and analyzing methods performed in this research can help to find remnant data from all activities performed by GDrive users in Android smartphones. Hence, this proposed method can assist investigators in finding remnant data on GDrive client and can provide knowledge for legal practitioners.

Keywords: Cloud storage, Mobile forensics, GDrive analysis, Remnant data, Cybercrime

1 Introduction

Cloud storage is a software service operated virtually, that allows users to store data online. It can be accessed from anywhere in the world by hosts connected to the Internet [1-3]. Based on the price, cloud storage services can be divided into two categories, paid services and free services [4-5]. Google Drive (GDrive) is the most widely used cloud storage service [4]. One of the conveniences provided by Google™ is a single-ID in which the user does not need to create a new account. By simply logging in to a Google account, Google Drive can be enjoyed with a free quota of up to 15GB [6]. GDrive can “use, host, store, reproduce, modify, create derivative works, communicate, publish, publicly perform, publicly display and distribute (user) content” [7-8].

From on-demand access to a shared pool of computing resources can be provided by cloud computing. It also can be provisioned on a scalable basis and has the potential for faster service delivery, more efficiently and with lower cost than custom-developed systems. Each of the seven agencies selected for audit by US Government Accountability Office has identified opportunities for implementing cloud computing in the future, from moving storage and help desk services to a cloud environment [9]. The positive sides of cloud storage are the conveniences; synchronization, sharing, collaboration, accessibility and disaster recovery. There is also a negative side to cloud storage services which is that there is no guarantee of a security service provided to fend off cybercrime activities [10]. Cybercrime is any kind of act using computers and networks that violates the law, or causes harm or threat to an individual or group [11-15]. All researchers and practitioners in network security work to provide solutions to these problems. This paper discusses digital forensics in GDrive cloud storage client to aid the process of finding remnant data from cybercrime activity.

Mobile forensics is a branch of digital forensic science conducting identification, preservation, analysis, and presentation with mobile devices as the media [16-19]. It is a little different from forensics on a personal computer (PC). Mobile devices have a file structure that is different between operating systems. As described later in the guidelines for mobile forensics, National Institute of Standards and Technology (NIST) mentions some focuses for analysis, which among others are Operating System (OS), PIM (personal information management), application, call, messaging and log history (chat, email, web, etc.) [2]. In this research, two devices from two separate vendors with different Android OSs were used as experimentation objects to test GDrive.

A concept of analyzing cloud-native digital artifacts-data object is introduced by McCulley and Roussev that maintain the persistent state of web/SaaS application [16, 20]. On the contrary with traditional application, web apps download the necessary state quickly without any trace in the local storage. While in traditional applications, the persistent state picks up the form of files in the local file system. Choo and Quick

[*] Corresponding Author: Soo Young Shin; E-mail: wdragon@kumoh.ac.kr

DOI: 10.3966/160792642018111906011

make a study of the process of collecting data from a cloud storage account using a browser and downloading files using client software [21]. Then, it is compared with the original files and an analysis is carried out of the resulting data. Furthermore, it is decided that there were no changes to the contents of the files during upload, storage and download to the three cloud storage services. The timestamp of the files were also examined in the relation to the files downloaded via browser and client software.

Similar to this study, Quick and Choo [22-23] have made a guide for forensic analysis of remnant data of Google Drive on different platforms, the PC and Apple iPhone3G. Also, Quick and Choo paid attention to the structures and preferences of GDrive, whereas this paper analyzed fourteen user activities. With the proposed method of comparing and analyzing the database contents before and after each user activity, remnant data was found that could be used as digital evidence in cyberlaw cases. In addition, this paper also contributes in providing a SOP (standard operating procedure) which could be used by investigators in writing analysis reports for GDrive cloud storage client.

A brief illustration of the mobile forensics procedures undertaken in this paper are as follows. Before experimentation of GDrive could proceed the Android smartphones were put through a rooting process. Open source software ADB, Busybox, and SQLite were used in the acquisition process and analysis. Following updated cyberlaw recommendations, the author used SHA-512 to check the hash values of the files that were acquired. This improves on previous research conducted by Quick and Choo which used MD5. Fourteen user activities were analyzed for data remnants.

Section 2 discusses the mobile forensics methods that were used in finding remnant data for digital evidence. In Section 3, the findings and analysis of the digital forensics process are detailed. Section 4 contains a discussion and summary of the analysis described in Section 3. Finally, Section 5, gives the overall conclusion from this research. Here, the SOP is also delivered by the authors for researchers, investigators, and legal practitioners who wish to study and learn more about digital mobile forensics on GDrive cloud storage client.

2 Investigating Steps for Android OS

Figure 1 above is a development of McKemmish and Quick & Choo's method of digital forensics where the most major difference lays in analysis and comparison step. In the method of digital forensic, Mckkemish describes four steps of investigation which are identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable [16]. While Quick & Choo develop methods of cloud forensics with eight investigation steps which are commence (scope), prepare and response, Identify and

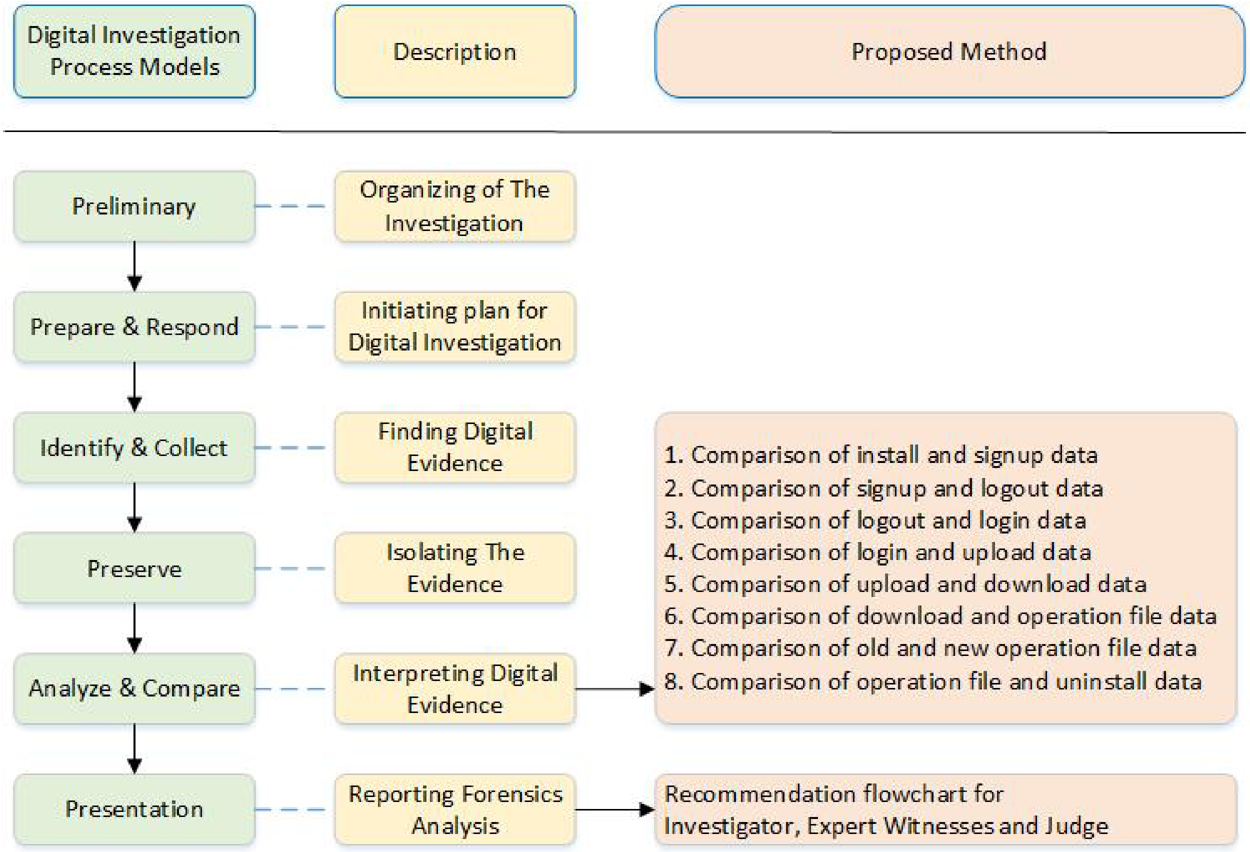

Digital Investigation Process Models
Description
Proposed Method
Preliminary
Organizing of The Investigation
Prepare & Respond
Initiating plan for Digital Investigation
Identify & Collect
Finding Digital Evidence
Preserve
Isolating The Evidence
Analyze & Compare
Interpreting Digital Evidence
Presentation
Reporting Forensics Analysis
1. Comparison of install and signup data
2. Comparison of signup and logout data
3. Comparison of logout and login data
4. Comparison of login and upload data
5. Comparison of upload and download data
6. Comparison of download and operation file data
7. Comparison of old and new operation file data
8. Comparison of operation file and uninstall data
Recommendation flowchart for Investigator, Expert Witnesses and Judge

Figure 1. Diagram of forensics process

collect, preserve (forensic copy), analyze, present, feedback, and complete or further task [22]. Furthermore, this research develops the method by combining [16] and [22] into six steps of investigation as can be seen in Figure 1.

2.1 Preliminary

A fundamental aim of digital forensics (mobile forensics, in this case) is to avoid any modifications to the device that is to be examined [11-12]. It is extremely difficult for the investigator to prevent some slight changes. Therefore, an investigator should be able to account for any modifications. To assist the investigation process, a methodology is required in performing mobile forensics [24-25]. At this preliminary stage, a global definition is given to the investigation process. Figure 1 below is the research method that was used in this research.

2.2 Prepare and Respond

There is a lot of software available on the Internet, both paid and free, for carrying out digital forensics. An investigator is free to choose which software / hardware to use. Experts in digital forensics suggest use of tools that are reputable and reliable [12, 23]. This study used the following software - Google drive client software v2.2.183.17.32 [7-8], Android Debug Bridge (ADB) v1.0.32 [26], SQLite Browser v3.8.0 [27], Hex Editor Neo v6.20.02.5651 [28], Busybox v4.1 [29], Root Browser v2.2.3 [30], Online Nandroid Backup v4.4.5 [31], Shark for Root v1.0.2, dex2jar v2.0, sha512sum (Linux Ubuntu 14.04) and Notepad++ v6.8.8.

2.3 Identify and Collect

To conduct an investigation, the investigator must identify and collect digital evidence for the case being handled. A sound procedure will greatly help the analysis process later. Based on the fingerprint (in this case, remnant data) left behind on the smartphone, a continuous track record can be formed and produce accurate analysis. Also at this stage, an investigator faces a challenge of how to find remnant data related to previous events of the case.

On the identification and collection stage, the smartphone will be checked whether it has been root or not. In this study the rooting process were done in both smartphone. In accordance with the principle of forensically sound, the processes done to obtain the evidence must be documented, and can be accounted for. The routing process is necessary in order to gain access to the highest structure on the Android OS. A normal Android smartphone does not allow you to access certain directories and files on the device. Once the smartphone in a state of root, the acquisition can be done online and offline.

2.4 Preserve

After all the digital evidence has been collected, preservation has to be done to maintain the integrity of the evidence. The purpose of this preserve stage is to make the exact duplication (bit by bit) of the original. By ensuring that the hash value (MD5 / SHA) for the original evidence and the image evidence is the same it was ensured that the copies were identical [14, 19]. In accordance with the rules of forensics, only the image can be worked upon. The following is an Algorithm 1 of shell scripts to perform the data acquisition process on GDrive application:

Algorithm 1 is used for the acquisition of all data on the smartphone that relate to GDrive. Once the database is found, then the database will be stored in the investigator's PC. This algorithm will be run every time the user has finished an activity.

Algorithm 1. GDrive Data Acquisition

```
initialize inputDB;
   ◀ from smartphone
initialize dataAcqusition;
   . for acquisition
inputDB ← search the database of “GoogleDrive”;
Save inputDB to our database
   ◀ save the file for analysis
Our db = query our database
   ◀ retrieve the data to our PC
repeatdataAcqusition ← Our db;
until the database is not empty
Print dataAcqusition
```

2.5 Analyze

The proposed method was analyzing and then comparing the contents of the databases related to certain user activities before and after those activities were carried out (also shown in Figure 1). This method is an effective and efficient way of finding remnant data to be used as evidence. When making correlations between the evidence obtained and the timestamp of events, the source logs obtained should also be considered. The correlations of each analysis were obtained manually by comparing the databases one by one. After that, strong evidence (acceptable by law) was attained. During the analysis process, investigators assess the evidence that has been obtained and build a theory of events that happened before (reconstruction). The end of the process is an interpretation of the evidence obtained in court. The following are the points of analysis compared in this study.

i. Comparison of install and signup data
ii. Comparison of signup and logout data
iii. Comparison of logout and login data
iv. Comparison of login and upload data
v. Comparison of upload and download data

vi. Comparison of download and operation file data
vii. Comparison of old and new operation file data
viii. Comparison of operation file and uninstall data

The following flowchart compares two results of data acquisition performed by the users. The most important thing here is to search for the hash values of all files obtained from the previous Algorithm 1. If there was a difference between hash values (SHA-512) found in (1) and (2), then it is assumed that the data has been altered as presented in Figure 2. The next step is analyses of those files/databases.

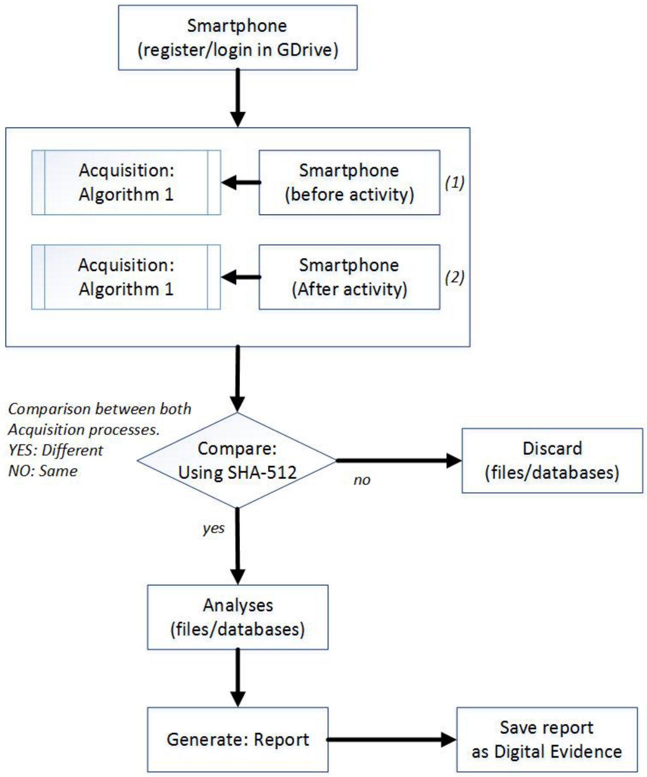

Smartphone (register/login in GDrive)
Acquisition: Algorithm 1
Smartphone (before activity)
(1)
Acquisition: Algorithm 1
Smartphone (After activity)
(2)
Comparison between both Acquisition processes.
YES: Different
NO: Same
Compare: Using SHA-512
no
Discard (files/databases)
yes
Analyses (files/databases)
Generate: Report
Save report as Digital Evidence

Figure 2. Flowchart for the comparison process

Our experimentation is based on the earlier mentioned version of GDrive, but as there is compatibility between all the versions of GDrive. So, our method can be applied to other versions of GDrive (with slight modifications or considering the additional features of newer versions).

2.6 Reporting

The reporting stage is where the investigator delivers the results that have been obtained from preparation to analysis. Reporting is the most important aspect of an investigation. Commercial forensic software can provide this feature, however reports must be understandable by the layman. Good reports should be understandable to non-technical people such as legal teams, managers, HR, judges, and juries, should be defensible in detail, and should be factual. If evidence from an investigation is insufficient then it should return to the initial step which is to prepare and respond.

3 Analyze The Google Drive

As have been stated in the Introduction, the methods used in this research are different in the comparison and analysis step. The main focus of mobile forensics in this research is the process of finding a different database after the user performed an activity. The main database on GDrive exist in the directory data/data/com.google. android.apps.docs/databases/DocList.db. Once the information in database is found then the analysis can be conducted on the remnant data. The following results detail the remnant data that were created when the user activities were performed.

3.1 Install Data Analysis

When installation of Google Drive was performed, some new files were formed. One that needs to be considered among other files was the file with path data/app/com.google.android.apps.docs-1.apk which is an .apk file. In total, there were eight files Table 1 obtained associated with the installation.

Table 1. Example of Install Activity

No	Path
1	data/app/com.google.android.apps.docs-1.apk
2	data/app-lib/com.google.android.apps.docs-1/ libwebp_android.so
3	data/app-lib/com.google.android.apps.docs-1/ libfileutils.so
4	data/app-lib/com.google.android.apps.docs-1/ libdocscanner_image.so
5	data/app-lib/com.google.android.apps.docs-1/ libbitmap_parcel.so
6	data/app-lib/com.google.android.apps.docs-1/ libdocsimageutils.so
7	data/app-lib/com.google.android.apps.docs-1/ librectifier.so
8	data/app-lib/com.google.android.apps.docs-1/ libfoxit.so

3.2 Signup Data Analysis

When the signup activity was carried out, there were several new files created by Google Drive application. One of the files that need to be considered was the file with path data/data/com.google.android.apps.docs/ databases/DocList.db that contains user signup information. By using software browser SQLite, the information related to the user could be viewed in detail as shown in Figure 3 below. There were six other supporting files Table 2 that could be found when the signup activity had been carried out. These seven files can be used as evidence by investigators that signup took place.

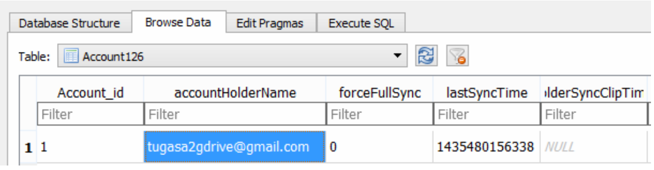


Table: Account126

	Account_id	accountHolderName	forceFullSync	lastSyncTime	ılderSyncClipTim
	Filter	Filter	Filter	Filter	Filter
1	1	tugasa2gdrive@gmail.com	0	1435480156338	NULL

Figure 3. Signup activity

Table 2. Example of Signup Activity

No	Path
1	data/data/com.google.android.apps.docs/shared_prefs /WarmWelcomePersister.xml
2	data/data/com.google.android.apps.docs/databases /CsiRequestQueue.db-journal
3	data/data/com.google.android.apps.docs/databases /CsiRequestQueue.db
4	data/data/com.google.android.apps.docs/databases /DocList.db-shm
5	data/data/com.google.android.apps.docs/databases /DocList.db-wal
6	data/data/com.google.android.apps.docs/databases /DocList.db
7	data/data/com.google.android.apps.docs/cache/com. android.opengl.shaders_cache

3.3 Login Data Analysis

From the login activity, data about user information made on the file with path data/data/com.google. android.apps.docs/databases/DocList.db was added to the **accounts** table. The information associated with the login activity is similar to that associated with the signup activity. The time synchronization of all activities can also be seen.

3.4 Logout Data Analysis

When the logout activity was undertaken, data about user information that was previously made on the file with path data/data/com.google.android.apps.docs/ databases/DocList.db was removed. If there is no information found regarding logout activity by using offline forensics, then the second way is to use online forensics. Live Log Android data is information that is only useful when the smartphone is still switched on. This is a big challenge for investigators. By using the command of *adb logcat -v threadtime*, all the information can be found in full from when the smartphone has been turned on. Remnant data that can be used as evidence of the logout activity here are *removePreferenceInt* and *SVC-Destroying service*. Both of these threads are codes that show the user has logged out on the timestamp seen in the log / logcat.

3.5 Upload Data Analysis

For the upload scenario, the user uploaded five files named **shell.docx**, **notepad.exe**, **LogoTelU.png**, **BusyBoxV27.apk**, and **accound.rtf** as shown in Figure 4. As shown on Table 3 below, the files that were uploaded could be seen directly without decryption. This could be used in an investigation to find any files that have been uploaded by a suspect.

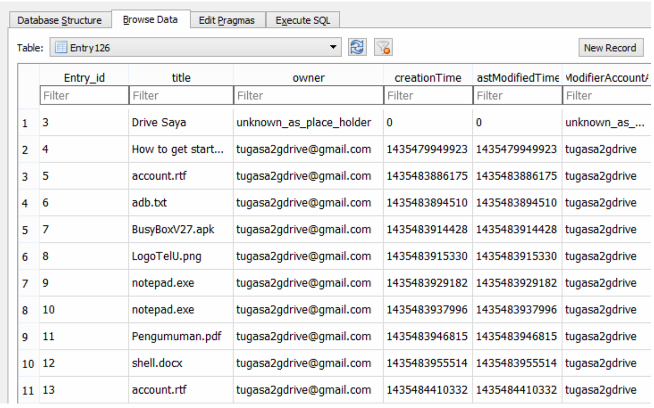


Table: Entry126

	Entry_id	title	owner	creationTime	astModifiedTime	ModifierAccount/
	Filter	Filter	Filter	Filter	Filter	Filter
1	3	Drive Saya	unknown_as_place_holder	0	0	unknown_as_...
2	4	How to get start...	tugasa2gdrive@gmail.com	1435479949923	1435479949923	tugasa2gdrive
3	5	account.rtf	tugasa2gdrive@gmail.com	1435483886175	1435483886175	tugasa2gdrive
4	6	adb.txt	tugasa2gdrive@gmail.com	1435483894510	1435483894510	tugasa2gdrive
5	7	BusyBoxV27.apk	tugasa2gdrive@gmail.com	1435483914428	1435483914428	tugasa2gdrive
6	8	LogoTelU.png	tugasa2gdrive@gmail.com	1435483915330	1435483915330	tugasa2gdrive
7	9	notepad.exe	tugasa2gdrive@gmail.com	1435483929182	1435483929182	tugasa2gdrive
8	10	notepad.exe	tugasa2gdrive@gmail.com	1435483937996	1435483937996	tugasa2gdrive
9	11	Pengumuman.pdf	tugasa2gdrive@gmail.com	1435483946815	1435483946815	tugasa2gdrive
10	12	shell.docx	tugasa2gdrive@gmail.com	1435483955514	1435483955514	tugasa2gdrive
11	13	account.rtf	tugasa2gdrive@gmail.com	1435484410332	1435484410332	tugasa2gdrive

Figure 4. Uploading activity

Table 3. Example of upload activity

No	Path
1	data/data/com.google.android.apps.docs/files/fileintern al/97c8a84d19ace3b2770f82f569c8cea4/shell.docx
2	data/data/com.google.android.apps.docs/files/fileintern al/ddabe5dd9409183474bf3936acdd6e20/notepad.exe
3	data/data/com.google.android.apps.docs/files/fileintern al/25152a139995b84d4fe5080ad65369d9/LogoTelU.p ng
4	data/data/com.google.android.apps.docs/files/fileintern al/50436a5cdca8f197901be32fab563eb3/BusyBoxV27. apk
5	data/data/com.google.android.apps.docs/files/fileintern al/51d9a8bf6f8c932ddb71d7fe7eee4b07/account.rtf

When the upload activity was performed, the uploaded files were copied to the directory data/data/com.google.android.apps.docs/files/fileintern al. Moreover, database data/data/com.google.android. apps.docs/databases/DocList.db was updated with data related to the files uploaded by the user. For example in the **htmlurl** field, the table document contains data about the user's URL documents that were uploaded.

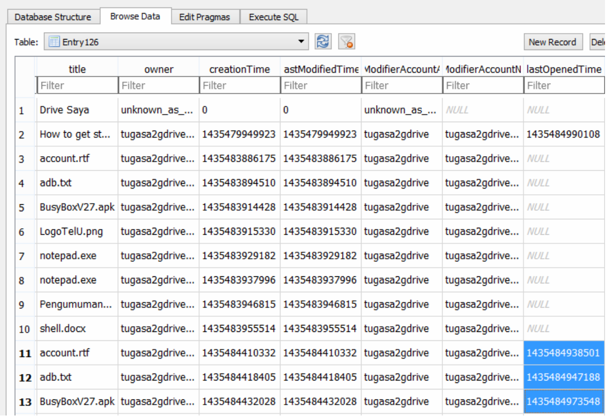
3.6 Download Data Analysis

By conducting an investigation on metadata **DocList.db**, information associated with the title of the downloaded files, the owner, creation time, last modified time and modifier account could be found. By simply using DB Browser for SQLite, this information could be found without encryption at all (as shown in Table 4).

The download process was performed by downloading some files that had been uploaded previously. When the download activity was done, the database file data/data/com.google.android.apps.docs/ databases/DocList.db was updated in the field **lastOpenedTime** table **Entry** as can be seen in Figure 5.

Table 4. Example of download activity

No	Path	
1	data/data/com.google.android.apps.docs/databases/DocList.db-shm	files/home/slave2/Downloads/TA/tmp/gdrive/drupload-all/DocList.db-shm /home/slave2/Downloads/TA/tmp/gdrive/drdownload-all/DocList.db-shmdiffer
2	data/data/com.google.android.apps.docs/databases/DocList.db-wal	files/home/slave2/Downloads/TA/tmp/gdrive/drupload-all/DocList.db-wal /home/slave2/Downloads/TA/tmp/gdrive/drdownload-all/DocList.db-waldiffer
3	data/data/com.google.android.apps.docs/databases/DocList.db	INSERT INTO Entry126VALUES(15,BusyBoxV27.apk,tugasa2gdrive@gmail.com,1435484432028,1435484432028,tugasa2gdrive,tugasa2gdrive@gmail.com,NULL,NULL,0,1435484432028,C0ECREVRGSt7ImBl,0B__DZniEtrg8Rzk0SkNXbV91Y2c,0,application/vnd.android.package-archive,NULL,file,1,0,0,0,0,0,0,0,2,110,2,0,0,1,NULL,NULL);|INSERTINTOEntry126VALUES(15,BusyBoxV27.apk,tugasa2gdrive@gmail.com,1435484432028,1435484432028,tugasa2gdrive,tugasa2gdrive@gmail.com,1435484973548,NULL,0,1435484432028,C0ECREVRGSt7ImBl,0B__DZniEtrg8Rzk0SkNXbV91Y2c,0,application/vnd.android.package-archive,NULL,file,1,0,0,0,0,0,1,0,2,158,2,0,0,1,NULL,NULL);



	title	owner	creationTime	astModifiedTime	ModifierAccount/	lodifierAccountN	lastOpenedTime
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	Drive Saya	unknown_as_...	0	0	unknown_as_...	NULL	NULL
2	How to get st...	tugasa2gdrive...	1435479949923	1435479949923	tugasa2gdrive	tugasa2gdrive...	1435484990108
3	account.rtf	tugasa2gdrive...	1435483886175	1435483886175	tugasa2gdrive	tugasa2gdrive...	NULL
4	adb.txt	tugasa2gdrive...	1435483894510	1435483894510	tugasa2gdrive	tugasa2gdrive...	NULL
5	BusyBoxV27.apk	tugasa2gdrive...	1435483914428	1435483914428	tugasa2gdrive	tugasa2gdrive...	NULL
6	LogoTelU.png	tugasa2gdrive...	1435483915330	1435483915330	tugasa2gdrive	tugasa2gdrive...	NULL
7	notepad.exe	tugasa2gdrive...	1435483929182	1435483929182	tugasa2gdrive	tugasa2gdrive...	NULL
8	notepad.exe	tugasa2gdrive...	1435483937996	1435483937996	tugasa2gdrive	tugasa2gdrive...	NULL
9	Pengumuman...	tugasa2gdrive...	1435483946815	1435483946815	tugasa2gdrive	tugasa2gdrive...	NULL
10	shell.docx	tugasa2gdrive...	1435483955514	1435483955514	tugasa2gdrive	tugasa2gdrive...	NULL
11	account.rtf	tugasa2gdrive...	1435484410332	1435484410332	tugasa2gdrive	tugasa2gdrive...	1435484938501
12	adb.txt	tugasa2gdrive...	1435484418405	1435484418405	tugasa2gdrive	tugasa2gdrive...	1435484947188
13	BusyBoxV27.apk	tugasa2gdrive...	1435484432028	1435484432028	tugasa2gdrive	tugasa2gdrive...	1435484973548

Figure 5. Downloading activity

3.7 Operation File Data (Open) Analysis

Two files that were updated when the open file activity was conducted are shown in Table 5 and Figure 6. When the open activity was carried out, thumbnails were formed for image files in the directory data/data/com.google.android.apps.docs/cache/diskCache/previewImageCacheDir/accountCache_1/ when the open process was done, the database file data/data/com.google.android.apps.docs/databases/DocList.db was updated in field **lastOpenedTime** of table **Entry**. In addition, on directory data/data/com.google.android.apps.docs/app_webview/Cache/ there were some file caches of the opened file.

Table 5. Example of open file data activity

No	Path	
1	data/data/com.google.android.apps.docs/shared_prefs/com.google.android.apps.docs_preferences.xml	> <int name=NumLaunches value=2/>
2	data/data/com.google.android.apps.docs/shared_prefs/HelpCard.xml	<int name=docListActivityVisitCount value=47/> | <int name=docListActivityVisitCount value=56/>
3	data/data/com.google.android.apps.docs/shared_prefs/accountFlagstugasa2gdrive@gmail.com.xml	<string name=startTimeLogKey>1435485032728</string> | <string name=startTimeLogKey>1435486401557</string>
4	data/data/com.google.android.apps.docs/databases/DocList.db-shm	Binary files/home/slave2/Downloads/TA/tmp/gdrive/drdownload-all/DocList.db-shm and/home/slave2/Downloads/TA/tmp/gdrive/dropen-all/DocList.db-shmdiffer
5	data/data/com.google.android.apps.docs/databases/DocList.db-wal	Binary files/home/slave2/Downloads/TA/tmp/gdrive/drdownload-all/DocList.db-wal and /home/slave2/Downloads/TA/tmp/gdrive/dropen-all/DocList.db-waldiffer
6	data/data/com.google.android.apps.docs/databases/DocList.db	INSERT INTO Entry126 VALUES(13,account.rtf,tugasa2gdrive@gmail.com,1435484410332,1435484410332,tugasa2gdrive,tugasa2gdrive@gmail.com,1435484938501,NULL,0,1435484410332,C0ECQw9PTit7ImBl,0B__DZniEtrg8STczdmVVUjFoR2c,0,text/rtf,NULL,file,1,0,0,0,0,0,1,0,2,155,2,0,0,1,NULL,NULL);|INSERT INTO Entry126VALUES(13,account.rtf,tugasa2gdrive@gmail.com,1435484410332,1435484410332,tugasa2gdrive,tugasa2gdrive@gmail.com,1435486350698,NULL,0,1435484410332,C0ECQw9PTit7ImBl,0B__DZniEtrg8STczdmVVUjFoR2c,0,text/rtf,NULL,file,1,0,0,0,0,0,1,0,2,167,2,0,0,1,NULL,NULL);

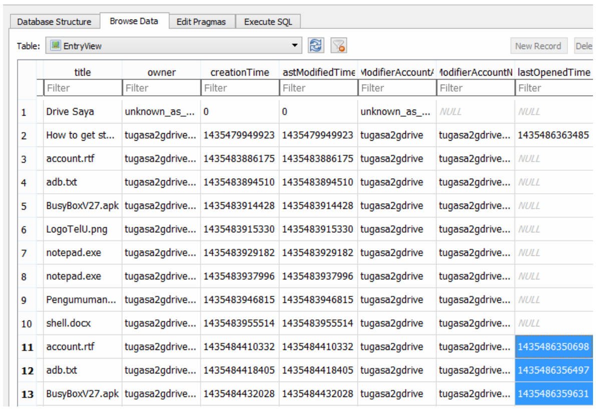


Table: EntryView

	title	owner	creationTime	astModifiedTime	ModifierAccount/	1odifierAccountN	lastOpenedTime
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	Drive Saya	unknown_as_...	0	0	unknown_as_...	NULL	NULL
2	How to get st...	tugasa2gdrive...	1435479949923	1435479949923	tugasa2gdrive	tugasa2gdrive...	1435486363485
3	account.rtf	tugasa2gdrive...	1435483886175	1435483886175	tugasa2gdrive	tugasa2gdrive...	NULL
4	adb.txt	tugasa2gdrive...	1435483894510	1435483894510	tugasa2gdrive	tugasa2gdrive...	NULL
5	BusyBoxV27.apk	tugasa2gdrive...	1435483914428	1435483914428	tugasa2gdrive	tugasa2gdrive...	NULL
6	LogoTelU.png	tugasa2gdrive...	1435483915330	1435483915330	tugasa2gdrive	tugasa2gdrive...	NULL
7	notepad.exe	tugasa2gdrive...	1435483929182	1435483929182	tugasa2gdrive	tugasa2gdrive...	NULL
8	notepad.exe	tugasa2gdrive...	1435483937996	1435483937996	tugasa2gdrive	tugasa2gdrive...	NULL
9	Pengumuman...	tugasa2gdrive...	1435483946815	1435483946815	tugasa2gdrive	tugasa2gdrive...	NULL
10	shell.docx	tugasa2gdrive...	1435483955514	1435483955514	tugasa2gdrive	tugasa2gdrive...	NULL
11	account.rtf	tugasa2gdrive...	1435484410332	1435484410332	tugasa2gdrive	tugasa2gdrive...	1435486350698
12	adb.txt	tugasa2gdrive...	1435484418405	1435484418405	tugasa2gdrive	tugasa2gdrive...	1435486356497
13	BusyBoxV27.apk	tugasa2gdrive...	1435484432028	1435484432028	tugasa2gdrive	tugasa2gdrive...	1435486359631

Figure 6. Opening files activity

3.8 Operation File Data (New Folder) Analysis

In this scenario, two new folders were created, namely **TA1** and **TA2** as can be observed in Figure 7. An investigator could find information related to those new folders in the **DocList.db** metadata. Information that could be submitted as evidence could include *folder title, owner, creation time, last modified time*, and *modifier account*. When the '*create new folder*' activity was done, the database file data/data/com.google.android.apps.docs/databases/DocList.db was updated and added with data related to the folder created.

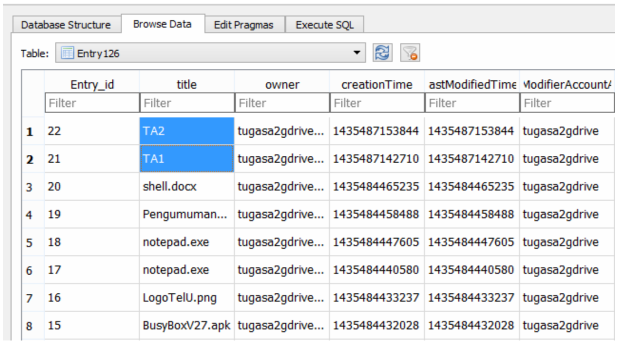


Table: Entry126

	Entry_id	title	owner	creationTime	astModifiedTime	ModifierAccount/
	Filter	Filter	Filter	Filter	Filter	Filter
1	22	TA2	tugasa2gdrive...	1435487153844	1435487153844	tugasa2gdrive
2	21	TA1	tugasa2gdrive...	1435487142710	1435487142710	tugasa2gdrive
3	20	shell.docx	tugasa2gdrive...	1435484465235	1435484465235	tugasa2gdrive
4	19	Pengumuman...	tugasa2gdrive...	1435484458488	1435484458488	tugasa2gdrive
5	18	notepad.exe	tugasa2gdrive...	1435484447605	1435484447605	tugasa2gdrive
6	17	notepad.exe	tugasa2gdrive...	1435484440580	1435484440580	tugasa2gdrive
7	16	LogoTelU.png	tugasa2gdrive...	1435484433237	1435484433237	tugasa2gdrive
8	15	BusyBoxV27.apk	tugasa2gdrive...	1435484432028	1435484432028	tugasa2gdrive

Figure 7. Creating new folder activity

3.9 Operation File Data (New File) Analysis

Similar to the new folder activity, in conducting the "*create new file*" activity, investigators could directly analyze the **DocList.db** metadata. All information related to the user is available in that database. When the "*create new file*" activity was undertaken, the database file data/data/com.google.android.apps.docs/databases/DocList.db in the "**Entry**" table was updated and added with data related to the file created.

3.10 Operation File Data (Rename) Analysis

In this scenario suppose the file's name was **account.rtf** and would be renamed as **akun.rtf**, then by using DB browser SQLite any files that have been renamed can be found along with complete information of the events. When the rename activity was undertaken, then the table entry on the database file data/data/com.google.android.apps.docs/databases/DocList.db was updated in accordance with the file that had been renamed. Figure 8 contains this illustration.

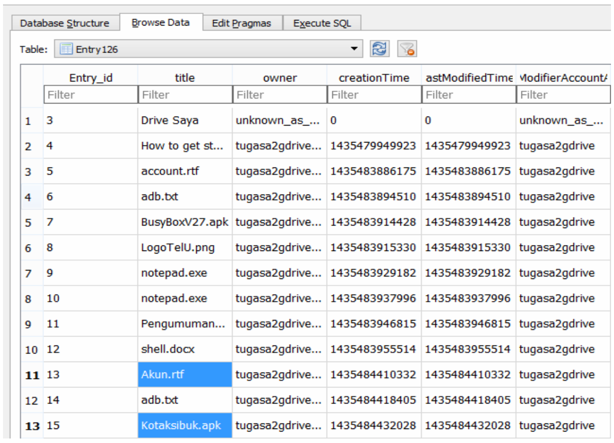


Table: Entry126

	Entry_id	title	owner	creationTime	astModifiedTime	ModifierAccount/
	Filter	Filter	Filter	Filter	Filter	Filter
1	3	Drive Saya	unknown_as_...	0	0	unknown_as_...
2	4	How to get st...	tugasa2gdrive...	1435479949923	1435479949923	tugasa2gdrive
3	5	account.rtf	tugasa2gdrive...	1435483886175	1435483886175	tugasa2gdrive
4	6	adb.txt	tugasa2gdrive...	1435483894510	1435483894510	tugasa2gdrive
5	7	BusyBoxV27.apk	tugasa2gdrive...	1435483914428	1435483914428	tugasa2gdrive
6	8	LogoTelU.png	tugasa2gdrive...	1435483915330	1435483915330	tugasa2gdrive
7	9	notepad.exe	tugasa2gdrive...	1435483929182	1435483929182	tugasa2gdrive
8	10	notepad.exe	tugasa2gdrive...	1435483937996	1435483937996	tugasa2gdrive
9	11	Pengumuman...	tugasa2gdrive...	1435483946815	1435483946815	tugasa2gdrive
10	12	shell.docx	tugasa2gdrive...	1435483955514	1435483955514	tugasa2gdrive
11	13	Akun.rtf	tugasa2gdrive...	1435484410332	1435484410332	tugasa2gdrive
12	14	adb.txt	tugasa2gdrive...	1435484418405	1435484418405	tugasa2gdrive
13	15	Kotaksibuk.apk	tugasa2gdrive...	1435484432028	1435484432028	tugasa2gdrive

Figure 8. Renaming files activity

3.11 Operation File Data (Move) Analysis

The scenario here used the folder created in the "*New Folder*" activity. The file named **LogoTelU.png** was moved from folder **/TA1** to folder **/TA2**. An investigator could directly open the **containsId94** table. On that table, is found the information on which folder that file had been moved to (based on the collection ID of the folder). When the move activity was carried out, the table **ContainsId** on database file data/data/com.google.android.apps.docs/databases/DocList.db was updated in accordance with the directory occupied by the files that were moved.

3.12 Operation File Data (Share) Analysis

The sharing scenario (full access) was sharing a folder (for instance, folder **/TA2**) between user-A and user-B. When this occurred in **DocList.db** of the database (user-A), a **shared** column was found as presented in Figure 9. This is only found if user-B has accepted that folder. A second column was the "*modified by time*" column which contains the last time the file was updated. When the share activity was undertaken, the table **Entry** on database file "data/data/com.google.android.apps.docs/databases/DocList.db" was updated in accordance with the file that was shared.

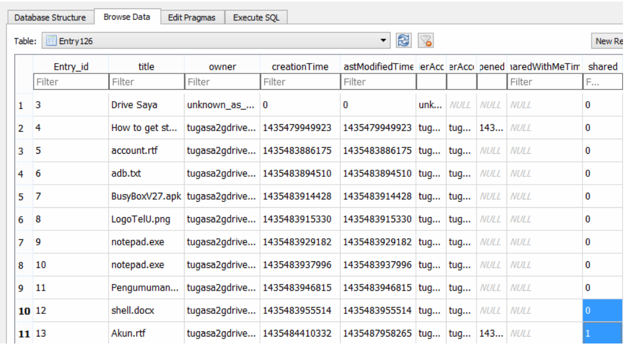


Table: Entry126

	Entry_id	title	owner	creationTime	astModifiedTime	ierAcc	erAcc	pened	iaredWithMeTim	shared
	Filter	Filter	Filter	Filter	Filter				Filter	F...
1	3	Drive Saya	unknown_as_...	0	0	unk...	NULL	NULL	NULL	0
2	4	How to get st...	tugasa2gdrive...	1435479949923	1435479949923	tug...	tug...	143...	NULL	0
3	5	account.rtf	tugasa2gdrive...	1435483886175	1435483886175	tug...	tug...	NULL	NULL	0
4	6	adb.txt	tugasa2gdrive...	1435483894510	1435483894510	tug...	tug...	NULL	NULL	0
5	7	BusyBoxV27.apk	tugasa2gdrive...	1435483914428	1435483914428	tug...	tug...	NULL	NULL	0
6	8	LogoTelU.png	tugasa2gdrive...	1435483915330	1435483915330	tug...	tug...	NULL	NULL	0
7	9	notepad.exe	tugasa2gdrive...	1435483929182	1435483929182	tug...	tug...	NULL	NULL	0
8	10	notepad.exe	tugasa2gdrive...	1435483937996	1435483937996	tug...	tug...	NULL	NULL	0
9	11	Pengumuman...	tugasa2gdrive...	1435483946815	1435483946815	tug...	tug...	NULL	NULL	0
10	12	shell.docx	tugasa2gdrive...	1435483955514	1435483955514	tug...	tug...	NULL	NULL	0
11	13	Akun.rtf	tugasa2gdrive...	1435484410332	1435487958265	tug...	tug...	143...	NULL	1

Figure 9. Sharing activity

3.13 Operation File Data (Delete) Analysis

For the delete scenario a file was deleted by user-A. The information about this deleted file was recorded in **DocList.db** of the database. An investigator could also check the table named **Entry126**. On that table, there is a column named **trashed** as shown in Figure 10. That is where the information of that deleted file was updated. The deleted file was still listed in the database “data/data/com.google.android.apps.docs/databases/DocList.db” in table **Entry**.

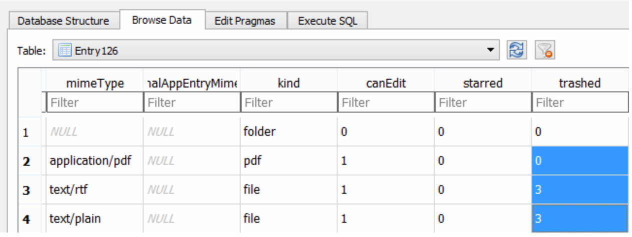


Table: Entry126

	mimeType	ıalAppEntryMime	kind	canEdit	starred	trashed
	Filter	Filter	Filter	Filter	Filter	Filter
1	NULL	NULL	folder	0	0	0
2	application/pdf	NULL	pdf	1	0	0
3	text/rtf	NULL	file	1	0	3
4	text/plain	NULL	file	1	0	3

Figure 10. Deleting a file activity

3.14 Uninstall Data Analysis

As mentioned in the logout analysis in subsection 3.4, if the remnant data cannot be found by using the offline method, then the online method is recommended. By using ADB tool, information about remnant data can be obtained relating to the uninstall activity complete with the date and time of the occurrence. The date and time format of ADB tool is already human readable so it does not need to be converted. There were five pieces of remnant data from the uninstall activity that could be used as a reference. These are *Killing 7133, START u0 (UninstallerActivity), Force stopping, Removing old permissions,* and *metrics were deleted (ACTION_PACKAGE_REMOVED*). This log / logcat can be used to analyze why the files and databases in the directory /com.google.android.apps/ are empty. Live log analysis can also be used as digital evidence in cyberlaw.

3.15 Reporting The Investigation

The analysis results obtained are presented in Table 6 below. To make sure the remnant data obtained was correct, it was necessary to check that the results from each scenario were not obtained by accident. To do this the steps were repeated on a second device, a Lenovo smartphone. This followed “*Reversal Burden of Proof* ” principles of the law [32], *reversal burden of proof* and ensured that the first test object (Samsung smartphone) was not imposed with the burden of proof.

Based on the analysis results above, a testing table was established containing a list of questions for the *reversal burden of proof* so that later the relationships between the files/paths from the analysis could be proven. Repeated results were rolled into one and incorporated into the list of questions on the testing table. Below is a table containing the results of the tests performed (Table 7 & Table 8).

Table 6. The results of GDrive analysis

No	Activity	Path	Information
1	Install data	data/app/com.google.android.apps.docs-1.apk	-
2	Sign up Data	data/data/com.google.android.apps.docs/ databases/DocList.db	Username used for sign in.
3	Logout Data	data/data/com.google.android.apps.docs/ databases/DocList.db	ADB logcat to find the information about Logout.
4	Login Data	data/data/com.google.android.apps.docs/ databases/DocList.db	Username used for login.
5	Upload Data	data/data/com.google.android.apps.docs/ files/fileinternal	List of files uploaded by the user with information of the date of upload.
6	Download Data	data/data/com.google.android.apps.docs/ databases/DocList.db	Files that have been downloaded by the user. This file can be accessed directly.
7	Operation File Data (Open)	data/data/com.google.android.apps.docs/ app_webview/Cache/	Files that have been previewed by the user. This file can be accessed directly.
8	Operation File Data (New Folder)	data/data/com.google.android.apps.docs/ databases/DocList.db	List of files made by the user with information of date of the file modification.
9	Operation File Data (New File)	data/data/com.google.android.apps.docs/ databases/DocList.db	List of files made by the user with information of date of the file modification.
10	Operation File Data (Rename)	data/data/com.google.android.apps.docs/ databases/DocList.db	List of files made by the user with information of date of the file modification.
11	Operation File Data (Move)	data/data/com.google.android.apps.docs/ databases/DocList.db	List of files made by the user with information of date of the file modification.
12	Operation File Data (Share)	data/data/com.google.android.apps.docs/ databases/DocList.db	List of files made by the user with information of date of the file modification.
13	Operation File Data (Delete)	data/data/com.google.android.apps.docs/ databases/DocList.db	List of files made by the user with information of date of the file modification.
14	Uninstall Data	*Using log live forensics*	ADB logcat to find the information about Logout

Table 7. GDrive test on the Lenovo K900 smartphone

No	Inquiry	Found (yes/no)	Description
1	Is there any file in data/app/com.google.android.apps.docs-1.apk?	yes	(install data)
2	Are there any files in directory data/data/com.google.android.apps.docs/databases/DocList.db?	yes	(signup data or login data)
3	Is the Entry table in the database data/data/com.google.android.apps.docs/databases/DocList.db, containing information about the new file in the directory data/data/com.google.android.apps.docs/files/fileinternal/?	yes	(upload data or operation file)
4	Is there any file in data/data/com.google.android.apps.docs/app _webview/Cache/?	yes	(operation file data - open)

Table 8. GDrive test on the Samsung Galaxy Young 2-G130H smartphone

No	Inquiry	Found (yes/no)	Description
1	Is there any file in data/app/com.google.android.apps.docs-1.apk?	yes	(install data)
2	Are there any files in directory data/data/com.google.android.apps. docs/databases/DocList.db?	yes	(signup data or login data)
3	Is the Entry table in the database data/data/com.google.android. apps.docs/databases/DocList.db, containing information about the new file in the directory data/data/com.google.android.apps. docs/files/fileinternal/?	yes	(upload data or operation file)
4	Is there any file in data/data/com.google.android.apps.docs/ app_webview/Cache/?	yes	(operation file data - open)

Based on the analysis results, testing and validation, instructions have been established for the analyze phase of the digital forensics analysis cycle in order for investigators to discover remnant data related to GDrive. The instructions for standard operating procedure (SOP) are shown in Table 9.

Table 9. SOP of analysis stage

No	Path
1	Google Drive has been installed on the smartphone
2	Google Drive has not been installed on the smartphone
3	Google Drive has been installed, signup or login has never been done
4	Google Drive has been installed, signup or login has been done
5	Google Drive has been installed, signup or login has been done, the upload process has never been done
6	Google Drive has been installed, signup or login has been done, the upload process has been done

For the cases with different circumstances, (for example, if there was only upload data or download data found on the application without any install data or uninstall data), the investigators would need to gather further evidence. GDrive analysis results on Table 7 can be used as a reference.

4 Discussion and Summary

When an investigation is being conducted, a digital forensic life cycle is very helpful. A chronological chain of custody will produce a good report. This research investigated GDrive cloud storage client application on Android smartphones, analyzing fourteen user scenarios which have been described in detail. Remnant data was obtained from twelve of these and could be used as evidence in an investigation of a criminal case. The twelve were install, signup, login, upload, download, open files, create new folders, create new files, rename files, move files, share files, and delete files.

For the activities logout and uninstall, no remnant data can be found using the method of comparative analysis. Information on remnant data for these activities could be obtained by analyzing live log forensics. With the help of ADB software, information can be found on when the user last conducted the log out and uninstall processes. A special requirement for such investigations is that the smartphone has to have remained switched on and not have been locked.

5 Conclusion

The proposed method of comparison and analysis has identified numerous data remnants on GDrive. Investigators and practitioners in cyberlaw can use the standard operating procedure, as a guideline to find remnant data on GDrive cloud storage client, that could be used as digital evidence in cyberlaw cases.

Future work could be conducted on other operating systems and on different smartphones such as iOS 9 on iPhone, Windows Phone 8.1 on Nokia Lumia 950, or Android Lollipop 5.0 on the Samsung Galaxy S6. Our method can be applied to other versions of GDrive as well (with slight modifications or considering the additional features of newer versions), which is also the future work of this research.

Acknowledgements

This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2017-2014-0-00639) supervised by the IITP (Institute for Information & communications Technology Promotion).

References

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stocia, M. Zaharia, A View of Cloub Computing, *Communications of the ACM*, Vol. 53, No. 4, pp. 50-58, April, 2010.

[2] P. Mell, T. Grance, *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology Special Publication 800-145, September, 2011.

[3] M. Taylor, J. Haggerty, D. Gresty, D. Lamb, Forensic Investigation of Cloud Computing Systems, *Network Security*, Vol. 2011, No. 3, pp. 4-10, March, 2011.

[4] S. Mitroff, OneDrive, Dropbox, *Google Drive and Box: Which Cloud Storage Service is Right for You?*, http://www.cnet.com/how-to/onedrive-dropbox-google-drive-and-box-which-cloud-storage-service-is-right-for-you/.

[5] J. Linder, *Cloud Storage Providers: Comparison of Features and Prices*, https://www.tomshardware.com/reviews/cloud-storage-provider-comparison,3905.html.

[6] Google, *My Drive*, https://drive.google.com.

[7] Google, *Google Terms of Service: Last Modified: October 25, 2017. URL*, https://www.google.com/policies/terms/.

[8] Google, *Google Drive Blog archive: October 28, 2008. 2008. URL*, https://drive.googleblog.com/2008/10/interesting-ways-to-use-docs-in.html.

[9] US Government Accountability Office, *Information Technology Reform: Progress Made but Future Cloud Computing Efforts Should be Better Planned*, GAO-12-756, July, 2012.

[10] M. Sato, T. Yamauchi, VMM-based Log-tampering and Loss Detection Scheme, *Journal of Internet Technology*, Vol. 13, No. 4, pp. 655-666, July, 2012.

[11] E. Casey, *Digital Evidence and Computer Crime: Forensic Science*, Computers, and the Internet, Academic Press, 2011.

[12] E. Casey, *Handbook of Computer Crime Investigation: Forensic Tools and Technology*, Academic Press, 2001.

[13] N. Bergman, M. Stanfield, J. Rouse, J. Scambray, S. Geethakumar, S. Deshmukh, S. Matsumoto, J. Steven, M. Price, *Hacking Exposed Mobile: Security Secrets & Solutions*, McGraw-Hill, 2013.

[14] G. B. Satrya, A. A. Nasrullah, S. Y. Shin, Identifying Artefact on Microsoft OneDrive Client to Support Android Forensics, *International Journal of Electronic Security and Digital Forensics*, Vol. 9, No. 3, pp. 269-291, June, 2017.

[15] H. C. Chu, W. D. Lin, *Live Information Discovery of the P2P Instant Messaging Based on Skype's Finger Printing, Journal of Internet Technology*, Vol. 11, No. 2, pp. 193-202, March, 2010.

[16] R. McKemmish, When is Digital Evidence Forensically Sound?, *IFIP International Conference on Digital Forensics, Kyoto*, Japan, 2008, pp. 3-15.

[17] A. Hoog, *Android Forensics: Investigation, Analysis and Mobile Security for Google Android*, Elsevier, 2011.

[18] D. Birk, C. Wegener, Technical Issues of Forensic Investigations in Cloud Computing Environments, *Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, Oakland, CA, 2011, pp. 1-10.

[19] G. B. Satrya, P. T. Daely, S. Y. Shin, Android Forensics Analysis: Private Chat on Social Messenger, *Eighth International Conference on Ubiquitous and Future Networks (ICUFN)*, Vienna, Austria, 2016, pp. 430-435.

[20] V. Roussev, S. McCulley, *Forensic Analysis of Cloud-native Artifacts, Digital Investigation*, Vol. 16, No. Supplement, pp. S104-S113, March, 2016.

[21] D. Quick, K.-K. R. Choo, Forensic Collection of Cloud Storage Data: Does the Act of Collection Result in Changes to the Data or Its Metadata?, *Digital Investigation*, Vol. 10, No. 3, pp. 266-277, October, 2013.

[22] D. Quick, K.-K. R. Choo, Google Drive: Forensic Analysis of Data Remnants, *Journal of Network and Computer Applications*, Vol. 40, pp. 179-193, April, 2014.

[23] D. Quick, B. Martini, K.-K. R. Choo, *Cloud Storage Forensics*, Syngress, 2013.

[24] G. Palmer, A Road Map for Digital Forensic Research, *First Digital Forensic Research Workshop*, Utica, NY, 2001, pp. 27-30.

[25] EC-Council, *Computer Forensics: Investigating Data and Image Files*, Cengage Learning, 2010.

[26] Android Studio, *Android Debug Bridge*, https://developer.android.com/studio/command-line/adb.html.

[27] Github, *DB Browser for SQLite 3.9.1*, https://github.com/sqlitebrowser/sqlitebrowser/releases.

[28] Hex Editor, *Editor Windows*, https://www.hhdsoftware.com/doc/hex-editor/editor-windows-editor-windows.html.

[29] Busybox, *Documentation*, https://busybox.net/downloads/BusyBox.html.

[30] Root Browser, *Root Browser*, http://rootbrowser.net/#.

[31] Forum Xda developers, *Online Nandroid / Nandroid Backup without re-booting*, http://forum.xda-developers.com/showthread.php?t=1620255.

[32] Kemenkumham, *Uudang Undang No. 8 Tahun 1981 Tentang: Kitab Undang Undang Hukum Acara Pidana (kuhap)*, https://www.kpk.go.id/images/pdf/Undang-undang/uu_8_1981.pdf.

Biographies

Gandeva Bayu Satrya is currently a Ph.D candidate of security communication in next generation networks, IT Convergence Engineering, School of Electronic Engineering, Kumoh National Institute of Technology, South Korea. He has been a lecturer and researcher at Telkom Applied Science School in Telkom University, Bandung, Indonesia since 2011.

Soo Young Shin received B.S., M.S., and Ph. D from Seoul National University. His research interests are wireless networks and next generation mobile wireless broadband networks (4G/5G). He is now an associate professor in School of Electronics in Kumoh National Institute of Technology since April 2017.