Digital Forensic Investigation of Cloud Storage Client in Android

Huixiang Zhang^{1, a}, Yanan Wang^{1, b}, Chunlei Chen^{2, c}

¹School of Automation, Northwest Polytechnical University, Xi'an, 710072, China

²School of Computer Engineering, Weifang University, Weifang, 261061, China

^aemail:

zhanghuixiang@nwpu.edu.cn, ^bemail:kingdou725@mail.nwpu.edu.cn, ^cemail:chunlei.chen@wfu.edu.cn

Keywords: Digital Forensic; Cloud Storage Client; Android; OneDrive

Abstract. Cloud storage services sometimes descend into criminal tools. It is very necessary to investigate on digital Forensic of cloud storage services to obtain sworn evidence. The digital forensic investigation of the OneDrive Android client application is conducted in this paper. By imitating users' behavior, thirty-two images were acquired for forensic analysis. The analysis results show that legacy data always remain in the usage traces of the cloud storage service client device. These traces can be used as digital evidence for criminal cases.

Introduction

The cloud storage service allows users to store their data such as documents, images, and music files into the Internet [1]. Usually, users can access their data using cloud storage client application installed on their PCs or smart phones. These access are available as long as there is an Internet connection.

As the popularity of cloud storage service, some criminals engage in illegal activities through cloud storage services [2]. However, collecting the digital forensic evidence is not a trivial work [3]. The cloud storage service preserves users' data in a distributed manner [4]. The data of interest may be divided into several fragmentation and preserved in different data centers. The law enforcement cannot acquire the complete files of interest in a timely fashion. Moreover, the cloud storage service providers are averse to offer information about cloud servers for the sake of users' personal privacy information [5].

Nevertheless, we can obtain the digital evidences from criminals' client device other than the cloud storage servers. When criminals use the cloud storage client applications to access their data, legacy data always remain in usage traces on the client device. These traces consists of not only the using logs, but also some buffered complete files. By analyzing these traces, we can learn how the criminals use their cloud storage service and obtain forensic evidences.

The Android OS has become the most popular mobile operating system [6]. The cloud storage service always provide client applications for Android smart phones. Moreover, OneDrive [7] is a popular and widespread cloud storage service provided by Microsoft. In this paper, we conduct research on cloud storage service forensics on the client side. The OneDrive client application in Android is used as an example to perform the digital forensic research.

Procedure for Cloud Storage Client Forensic

The procedure for OneDrive client forensic is depicted in figure 1. The process is divided into five major steps. There are several defined activities to mimic the user's behaviors of using the OneDrive client. To avoid mutual interference among these activities, the procedure is performed individually for each activity in a loop.

A smart phone of Samsung Galaxy Note 2 with Android OS 4.1.1 installed has been selected to carry out forensic investigation. The smart phone is of 16G internal memory and no external memory card. The test phone is initially rooted via rootkit tool KingRoot. Rooted android phones provide the owner with full rights to access the application's data which is essential to the forensic

examination [8].

Fig.1. The forensic procedure

Each step is elaborated as follows.

Preparing Evidence Files on a PC. A pre-defined evidence data set is created which consist of 15 files in common used format. These files cover document (1.doc, 2.docx, 3.pdf and 4.txt), image (5.jpeg, 6.png, 7.gif and 8.bmp), video (9.mp4, 10.avi, 11.flv, 12.mov and 13.swf) and audio (14.mp3 and 15.wma). An OneDrive account is applied on a PC first, and these files are uploaded to the cloud storage as the account's data files.

Resetting the Smart Phone. Since the procedure is repeated for every activity, the smart phone is reset every time. The smart phone is restored to the default factory settings. After those steps, any previous data stored on the devices is removed. At last, the OneDrive client application is installed in the phone.

Performing Defined Activities. There are four defined activities which are applied to the evidence files. These include:

- 1) doing nothing, just log into the cloud storage service on the smart phone using the applied account;
- 2) the evidence files are viewed or played online;
- 3) the evidence files are downloaded from cloud storage service for offline access;
- 4) the evidence files are deleted online.

Creating Forensic Image. After perform a defined activity, the snap shot of the phone is acquired by using dd tool as the first initial image. Then, one of the following actions are manipulated on the phone to mimic various scenarios during an investigation:

- 1) logout from the OneDrive client application;
- 2) clear cache using the function in OneDrive client application;
- 3) login using the other OneDrive account;
- 4) reboot the smart phone;
- 5) uninstall the OneDrive client application;
- 6) clear cache using the function in Android OS;
- 7) restore default factory setting.

After each manipulation, an image is created to capture the status of the smart phone. Thus, there are 8 images for every activity and 32 images totally.

Conducting Forensic Analysis. For every acquired image, the forensic analysis is conducted using three forensic analysis tools in subsequently. These are:

- 1) Forensics Master [9]. This tool is used to retrieve and classify files in the image. The forensic investigator would check whether the evidence files exist in the files list by the tool.
- 2) R-Studio [10]. If some evidence files cannot be found by the Forensics Master, R-Studio is used to restore deleted files in that image. The forensic investigator would try to find those evidence files deleted by the user or smart phone.
- 3) WinHex [11]. If there are still can't find the evidence files, the hexadecimal search is perform in the image by the tool.

The Forensic Results

The analysis results by Forensics Master are shown in Table 1. All 32 image are encoded in two numbers. The first number represents the four defined activities described in the above section. The second number represents the seven actions listed in the above section, and number 0 is the first

initial image. Take image code “11” as an example, it is the captured image after performing activity 1 (“doing nothing”) and manipulation 1 (“logout”). We find that there remains many thumbnails of the evidence files in the phone. Moreover, the complete file of the 15 evidence files are always restored together if anyone can be found. The number 1 in the result cells denotes this kind of file can be found, otherwise 0 means cannot.

Table 1. The analysis results by Forensics Master

Image code	Thumbnails															Files
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
10	1	1	1	0	1	1	1	1	1	0	0	1	0	1	0	0
11	1	1	1	0	1	1	1	1	1	0	0	1	0	1	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	1	1	1	0	1	1	1	1	1	0	0	1	0	1	0	0
14	1	1	1	0	1	1	1	1	1	0	0	1	0	1	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	1	1	1	0	1	1	1	1	1	0	0	1	0	1	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	1	1	1	0	1	1	1	1	1	0	0	1	0	1	0	0
21	1	1	1	0	1	1	1	1	1	0	0	1	0	1	0	0
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
23	1	1	1	0	1	1	1	1	1	0	0	1	0	1	0	0
24	1	1	1	0	1	1	1	1	1	0	0	1	0	1	0	0
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26	1	1	1	0	1	1	1	1	1	0	0	1	0	1	0	0
27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
30	1	1	1	0	1	1	1	1	1	0	0	1	0	1	0	1
31	1	1	1	0	1	1	1	1	1	0	0	1	0	1	0	1
32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
33	1	1	1	0	1	1	1	1	1	0	0	1	0	1	0	1
34	1	1	1	0	1	1	1	1	1	0	0	1	0	1	0	1
35	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
36	1	1	1	0	1	1	1	1	1	0	0	1	0	1	0	1
37	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
40	1	1	1	0	1	1	1	1	1	0	0	1	0	1	0	0
41	1	1	1	0	1	1	1	1	1	0	0	1	0	1	0	0
42	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
43	1	1	1	0	1	1	1	1	1	0	0	1	0	1	0	0
44	1	1	1	0	1	1	1	1	1	0	0	1	0	1	0	0
45	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
46	1	1	1	0	1	1	1	1	1	0	0	1	0	1	0	0
47	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

As can be seen in the table 1, most of the evidence files (except 4.txt, 10.avi, 11.flv, 13.swf, 15.wma) always remain its thumbnails in the phone. And if the phone is restored to default factory setting (image code 17, 27, 37, 47), these thumbnails disappear. When the evidence file is downloaded from the cloud storage, the complete evidence files can be found (image code 30-36). Moreover, the actions of 2, 5 and 7 can remove the thumbnail traces in the phone. Thus, the R-Studio is used to restore these files. The analysis results by R-Studio are shown in Table 2.

Table 2. The analysis results by R-Studio

Image code	Restore the thumbnails or not?	Restore the files or not?
12	Yes, but damaged.	No.
15	No.	No.
17	Yes, but damaged.	No.
22	Yes.	Yes, but damaged.
25	Yes.	Yes, but damaged.
27	Yes.	Yes.
37	No.	No.
42	Yes, but damaged.	No.
45	Yes, but damaged.	No.
47	Yes.	No.

As seen in the table 2, part of the traces can be restored by R-Studio. For the image 27, even the complete files are restored. Some recovered files are damaged and can't be open again. At last, the WinHex is used to recover the deleted files for the image 12, 15, 17, 37, 42 and 45. There are no effective trace files in these image. Part of data in hexadecimal format of the evidence file 5-15 are

used to search in the images. The search results are illustrated in table 3.

Table 3. The search results by WinHex

Image code	Files										
	5	6	7	8	9	10	11	12	13	14	15
12	1	1	0	0	1	0	0	0	0	0	0
15	1	1	0	0	1	0	0	0	0	0	0
17	0	0	0	0	1	0	0	0	0	0	0
37	1	1	1	1	1	1	1	1	1	1	1
42	1	1	0	0	1	0	0	0	0	0	0
45	1	1	0	0	1	0	0	0	0	0	0

As shown in table 3, some of the hexadecimal data still remain in the phone. If the evidence files are downloaded from the cloud storage service, the files data can be find in the phone even if the phone is restored to the default factory setting.

Conclusion

A digital forensic investigation of cloud storage client in Android is conducted in this paper. Four activities of using cloud storage service and eight manipulation in the smart phone are considered in the experiments. The OneDrive cloud storage service client is adopted as instance for the investigation. The forensic analysis results show that legacy data always remain in usage traces of the cloud storage service client device. These traces can be used as digital forensic evidences.

Acknowledgement

This work is financially supported by the Fundamental Research Funds for the Central Universities (Project NO.3102016JKBJJGZ07), the Science and Technology Development Program of Weifang (No. 2015GX008), and the Doctoral Program of Weifang University (2016BS03).

References

- [1] Enrico Bocchi, Idilio Drago, Marco Mellia. Personal Cloud Storage Benchmarks and Comparison [J]. IEEE Transactions on Cloud Computing, 2015 (99) 1-14.
- [2] Quang Do, Ben Martini, Kim-Kwang Raymond Choo. A Cloud-Focused Mobile Forensics Methodology [J]. IEEE Cloud Computing, 2015 (4) 60-65.
- [3] Normaziah A. Aziz, Fakhrulrazi Mokti, Mohd Nadhar M. NozriMobile. Device Forensics: Extracting and Analysing Data from an Android-based Smartphone [C]. Proceedings 2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic, 2015.
- [4] Matthew B. Hancock, Carlos A. Varela. Augmenting Performance For Distributed Cloud Storage [C]. Proceedings 2015 15th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), 2015.
- [5] George Grispos, William Bradley Glisson, Tim Storer. Using Smartphones as a Proxy for Forensic Evidence Contained in Cloud Storage Services [C]. Proceedings 2013 46th Hawaii International Conference on System Sciences (HICSS), 2013.
- [6] Huixiang Zhang, Chunlei Chen, Jinghua Li and Yi Luo. Study on Minimal Feature Selection for Android Malware Detection [J]. ICIC Express Letters, Part B: Applications, 2016 (7) 1505-1510.
- [7] OneDrive. <https://onedrive.live.com>.
- [8] Fazeel Ali Awan. Forensic Examination of Social Networking Applications on Smartphones [C]. Proceedings 2015 Conference on Information Assurance and Cyber Security (CIACS), 2015.
- [9] Forensics Master. <http://www.meiyapico.com/>
- [10] R-Studio. <https://www.r-studio.com/>

[11] WinHex. <https://www.rstudio.com/>