Forensic Analysis of Cloud Storage on Android Volatile Memory

Long Chen[1], Honghua Zhao[2]

***Abstract*—**With the popularity of smart phones, criminal activity involving smart phones has become a common phenomenon, especially committing a crime with Cloud Data Storage . i . e . Cloud Storage aids in the manipulating of illicit data, and avoid the scrutiny of law enforcement and national security agencies. This paper attempts to investigate the identification and acquisition of data in the volatile memory of smart phone compared to traditional combination of computer technology and network technology. First of all, we will make an experiment between Baidu Cloud and 360 Cloud that are both Cloud storage application software embedded in Android phones. Secondly, some information associated with Cloud Storage applications that are remained in the Android volatile memory and their regularity and characteristic are recognized through our analysis. Finally, a new automatic Cloud Storage forensic tool through volatile memory of Android phone was designed by us. This tool is able to assist forensic investigators retrieve cloud storage application related evidence from memory dump.

***Keywords*—**Cloud storage forensic; Characteristics; related evidence； volatile memory

I. Introduction

Cloud Computing offers a wide range of efficient and secure services available for users. However, it also poses huge risks to digital forensics because of its sophisticated framework, even if criminal activities are committed by several criminals on this platform. An increasing number of users have access to Cloud Storage service according to mobile terminal, which leads to more forensic objects and challenges for forensic investigators. Traditionally, there are two aspects of Cloud forensics data acquisition. The first aspect is subscriber terminal is able to extract data generated from Cloud services and conduct user behavior analysis. The other aspect is examining user behavior through the information originated from Cloud service terminal interface.

With the development of mobile internet, the private data of user are stored in non-volatile memory of mobile phone, which enables forensics investigators to obtain evidence from its thirty-party software application. However, the data investigators acquired mainly are encrypted and not all of the program data is saved in the non-volatile memory as the encryption function is widely utilized by general public. Therefore, more difficulties are being presented for investigators. Speritzenbarth and Müller [1] extract disk encryption key based on Android volatile memory and analyze its data. Zhou [2] recovered Wechat chat record information stored in the volatile memory dump of Android mobile phone. The acquisition and analysis methodology of computing volatile memory forensics are very mature as its research has been established for several years. Reversely, having access to data from volatile memory of mobile phone has been concentrated on the initial stage, and it requires further research.

At present, most of the research and analysis of mobile phone forensics are focused on the non-volatile memory [3]. However, the research in volatile memory of Android mobile phone is at the initial stage. Especially, so far there is no research on extraction and analysis of Cloud storage relevant data from volatile memory of mobile phone. So this paper will concentrates on discovering cloud storage application related information in the volatile memory of the mobile phone. Furthermore, we will analyze the characteristic value and structure of data storage to realize the automatic analysis and extraction of the information.

In this paper, we choose Android mobile as a research emphases, because Android is currently popular mobile operating system, and two Chinese mainstream Android cloud applications—Baidu Cloud and 360 Cloud as cloud client to the experimental test. Our main work of this paper includes:

1) Examine each investigated cloud client application to discover cloud storage related information in the volatile memory of the Android mobile phone.

2) Identifying and summarizing the regularities and characteristics of the cloud storage related information are stored in the memory dump of the Android mobile phone.

3) According to the regularities and characteristics, we developed a tool that can automatically extract and analyze cloud storage related information from the memory dump.

In the rest of the paper, Section II illustrates the background information of the research. Section III introduces the related work of the volatile memory of the mobile phone. Section IV describes methods for the acquisition of volatile memory of mobile phone and the experiments. Section V displays the detail of experiments result . Finally, the conclusion and future work are given in the Section VI.

Long Chen[1] is with the Institute of Computer Forensic, Chongqing University of Post and Telecommunications, Chongqing 400065, China (corresponding author's phone:13648443661;(e-mail: chenlong@cqupt.edu.cn).

Honghua Zhao[2], was with the Institute of Computer Forensic, Chongqing University of Post and Telecommunications, Chongqing 400065, China (e-mail: younzhh123@163.com).

https://doi.org/10.15242/IIE.E0517012

II. Background

A. Android Operating System

Android is a mobile operating system, and its primary service is based on the Linux Kernel 2.6 including security, storage administration, process administration and protocol stack. Android Executes its application with the assistance of an integral virtual machine (Dalvik), who plays a key role in process isolation and thread management. In addition, there is a virtual machine for every Android application.

A wide range of data are stored in memory of Android system, such as photos, messages and web-browers , etc. There are two basic memory in Android.

1)Non-volatile memory: It includes its original flash memory and additional SD card. For instance, users are likely to be accessible to data with restart after the power is turned off, and retrieve data owing to system bug, which are both attributed to non-volatile memory's outstanding advantage.

2)Volatile memory (RAM): Data being stored in memory will disappear when rebooting the system, whose role is identical with computer RAM memory. A variety of valuable information are being preserved in volatile memory with the operation of system, such as user name, password, encryption code and data from application software.

In order to protect private data of user and security, Android enables the function of disk encryption applied to electronic device of user from Android 4.0 [4]. Besides, data recovery in volatile memory has become a significant field that results from the unencrypted feature of volatile memory compared to encrypted data in non-volatile memory.

B. The Features of Cloud Service

NIST defines: Cloud Computing consists of five essential characteristics, three service models and four deployment models. In terms of five essential characteristics, it is made of measured service, rapid elasticity, on-demand self-service, broad network access and resource pooling. As for three service models, it includes SaaS, PaaS and IaaS. What is more, public cloud, private cloud, hybrid cloud, community cloud are models for Cloud Computing deployment. Client is likely to interact with the combination of local servers and Cloud services. By taking advantage of data storage, it is able to support manipulation of user, which is defined as file operation. As shown in Table I, we can analysis and reconstruct behavior of client according to the attribute of Cloud files.

The attribute of cloud file is the important part for analyzing user behavior, contains the user to create the file name, file content, file time. Especially the value of transmitter_type represents the user operation behavior. Through the analysis of the correlation between the attribute values reconstruct the behavior of clients.

The current scholars on cloud forensics research primarily concentrated in two aspects.

1)Through analyzing the suspicious data from client's machine to reconstruct the behavior of user.

2)Through designing scheme on cloud server that record user information and obtain process, network, and access logs via the API on the server, collect the user information to analyze the activities of user.

TABLE I
Attribute Of Cloud Files

Attribute value	Attribute Description
File_name	It describes the name of file that users operated.
File_md5	Indicates that each cloud file has a unique hash value.
File_size	It describes that each file containing different content, so size is different.
Server_ctime	It describes the time that the cloud server accept the file.
Client_ctime	Written to the file, change the rights to the owner, or a link set along with the content changes of nodes, the file status for the last time is the time to change.
Client_mtime	Written to the file along with the change of the file content changes, is refers to the time of the last time the file content is modified.
Transmitter_type	It describes the user's operation documents, like uploading documents.
Remote_url	It represents each file remote address in the cloud.
File_category	It describes that each file has its own corresponding format.

III. Related Work

At present, most of the research and analysis of mobile phone forensics are focused on the non-volatile memory. However, the research in volatile memory of Android mobile phone is at the initial stage. With the improvement of mobile phone security, acquiring the non-volatile memory is limited. Data in RAM is generally not encrypted, the research of Android volatile memory forensics is valuable. It mainly includes memory acquisition and memory analysis.

A. Android volatile memory acquisition

Memory forensic in volatile memory has been a research theme for several years, but mostly focusing on x86 system like Linux and Windows, only little on Android. Because of the limited method that dumped the volatile memory, Researchers have been researched to acquire complete memory from Android phone for a long time. Yen [5] and Urrea [6] focus on Linux memory, Urrea[6] developed a tool named "dd" to obtain physical memory at runtime from /proc/mem. Thing [7] firstly proposed that the volatile memory of the mobile phone is important role in forensic investigation process, they developed a forensic tool named "memgrab" to dump a specific process memory for Android. However, It cannot acquire the complete volatile memory from Android phone. Leppert [8] described another way for Android memory analysis by using the DDMS tool, but it just acquired and analyzed the heap of specific, running applications. Memory Dumpstr(DMD) or Linux Extraction Memory(LiME) is an open source tool for dumping volatile memory from Android phone developed by Sylve [9], it is the unique tool that acquire complete memory from Android phone. Not only that, LiMe provided the function that

dumps the volatile memory directly to sd card or via the network. In addition, LiME can minimizes interaction between the kernel land and user land when acquiring the memory process. Although the limitations of using the LiME is that we should root the Android devices, it has become the best legal effect way to dump the volatile memory of Android devices.

B. Android volatile memory analysis

Researchers have researched server methods to analyze volatile memory. Researcher use Winhex to find string in the volatile memory, then finding the regularity and characteristic. Because the Android system is based on the Linux kernel operating system, so researcher utilize an open source investigation framework called Volatility [11] to analyze Android memory dump. Volatility contains support for extract running processes, opened network sockets, memory for each process and kernel modules, but the application data such as deleted message, char history that is not provide by Volatility. Because of the limitations with Winhex and Volatility, proposed a new way using python scripts to analyze memory and developed automatic tool to analyze related data in Android memory. In the last few years, there are some analysis researches on Android volatile memory. Ntantogian [12] has proved that it is possible to extract authentication credentials of user like user username and password of mobile application from the volatile memory of rooted Android devices. Andersen [13] propose a method to retrieve the encryption key of Luks from the volatile memory of Android mobile phone. Zhou recovered the Wechat chat record information that are encrypted or unrecoverable after deleting from the Android volatile memory by using the python script. Speritzenbarth and Müller [1] exploited cold boot attacks theory and developed a tool named FROST(Forensic Recovery of Scrambled Telephones) to analyze the android devices with full encrypted disk. They reconstructed the encrypted key and personal information including messages, photos, password. However this tool in some configurations is deployed to break disk encryption, encrypted user partitions are usually wiped during a cold boot attack. In addition, the defect of the method is that need to unplug the battery briefly, many smart phone cannot open it up, or disassemble the battery.

IV. Experiments

A. Acquisition volatile memory with LiMe

By comparing the several methods that acquired the Android volatile memory, we finally decided to employ an open source and free tool called Linux Memory Extractor(LiME) to acquire the volatile memory. we know that LiME is a loadable kernel module, so far it is the only tool that dump the complete volatile memory of Android mobile phone [14]. Loading the kernel module into the Android OS kernel needs the root permissions of the Android mobile. Although loading codes in the kernel module requires to break through Android security mechanism, according to the latest results of survey, a large number of users root their smart phones for different purpose [15]. To successfully acquire the Android mobile volatile memory, we must firstly rooted the mobile before performing the LiME, secondly It needs to download the kernel source code of the Android mobile phone that was used in our experiments on google official website. Thirdly in order to ensure successful cross-compiling the source code of LiME and generate lime.ko, it must modify lime configuration file that the value of the variables in our experiments. Finally, we excuted the pull command to copy the lime.ko module to the Android SD card of mobile by using the Android Debug Bridge(ADB) [16], and then executed insmod command to mount it. After waiting a few minutes, the acquisition process was completed successfully and the volatile memory was stored in the SD card. So we copy the dump to the PC by the Android Debug Bridge(ADB). In this paper, the Android mobile phone has been rooted in all experiment.

B. Development Environment and Condition

To acquire the Android mobile memory successfully with LiME in this paper, we require the additional preparations. We make use of a rooted Nexus Galaxy(I9250) that runs Android version 4.04, also known as is the third smartphone in the Google Nexus series. Moreover, through the investigation and analysis the amount of user at Cloud storage application market in china, we select the Baidu Cloud and 360 Cloud that the most popular Cloud storage application as cloud client to perform experimental tests. Both cloud storage applications have their own cloud services, so their structure and characteristics are also different. In each experiment, we mainly analyze and extract the cloud storage related information in the volatile memory of the android mobile under six various mobile usage scenarios(as shown in Table II). To ensure the accuracy of the experimental data, we respectively investigate two cloud client applications for experiment. After finishing the test of BaiduYun-related scenarios, the battery must be unplugged straightway and plugged in a few day to wipe the data that stored in the volatile memory of Android phone, then we will implement the test of 360 cloud client.

TABLE II
SUMMARY OF EXPERIMENTAL SCENARIOS

Scenarios	Step description
Scenario#1	Login BaiduCloud, use(including browse, upload, download file ,etc.) it, let the application run in the background, and then acquire the memory dump with LIME.
Scenario#2	Login BaiduCloud, use(including browse, upload, download file ,etc.) it, logout the application and then acquire the memory dump with LIME.
Scenario#3	Login BaiduCloud, use(including browse, upload, download file ,etc.)it, reboot the phone and then acquire the memory dump with LIME.
Scenario#4	Login 360Yunpan, use(including browse, upload,download file ,etc.)it, let the application run in the background, and then acquire the memory dump with LIME.
Scenario#5	Login 360Yunpan, use(including browse, upload, download file ,etc.)it, logout the application and then acquire the memory dump with LIME.
Scenario#6	Login 360Yunpan, use(including browse, upload, download file ,etc.)it, reboot the phone and then acquire the memory dump with LIME.

V. Experimental Results

A. Analysis of cloud disk data in volatile memory

Through the above six different experimental scenarios analysis, we could successfully acquire the volatile memory of the Android mobile phone, and also obtained cloud disk data of user from Android volatile memory. The following is a detailed analysis of our result.

1) The relevant information of cloud disk user

According on the experimental analysis and observation in the regularity and characteristic of user information in volatile memory of Android phone, we could find user information in the memory dump. Under scenario 1 and scenario 2, user information in volatile memory of the Android phone could be positioned by searching keyword , as shown in Fig. 1 and Fig. 2. And then extract and parse username, login time and a unique ID number as shown in table III. The user ID is the only ID for user which provide by cloud server. Similarly, in scenario 4 and 5 experimental conditions, we discover the user information in Fig. 3. Table III shows the information that was acquired user ID and final login time of user. However, we can not find user login password by these experiments, it means that user password is encrypted or hidden.

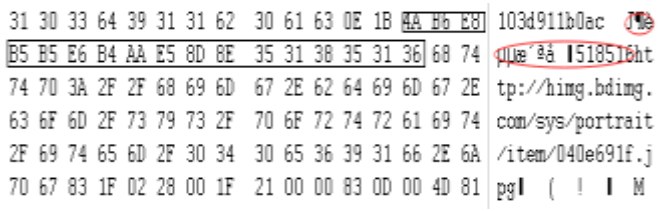

Fig.1 Username of the Baidu Cloud

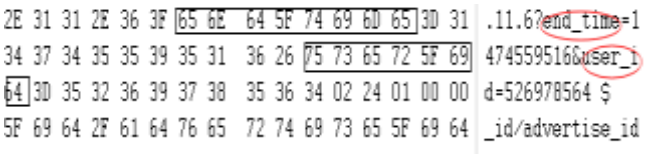

Fig. 2 User Account and login time of Baidu Cloud

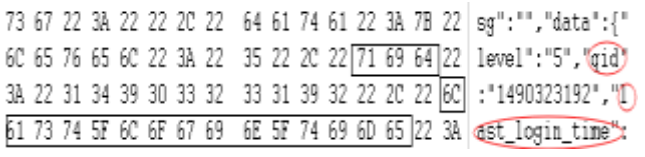

Fig. 3 User Account and login time of 360Yun

2) The relevant information of Cloud client

By acquiring Android volatile memory from scenario 1 and scenario 2 , we could acquire some details about cloud client information. By analyzing Fig. 4, we could know Baidu cloud client version is 7.11.6. By analyzing the experimental scenarios 4 and 5, we use keyword search and correlation methods to analyze the presence of information in the memory of the Android phone. As shown in table IV and Fig. 5, we can obtain many information in the memory dump of the Android phone, such as mobile login IP, the size of the cloud disk has been used and username. But we have not acquired software version number in the memory dump. The information reveals user client-side message in detail, and also provide valuable information for forensic investigators.

TABLE III
The Filed Value Of User Information

Field name	Field Description
user_name	Through analyzing keyword information in the Fig.1, the user name is found.
end_time	It describes the last login time, the time that is found after "end_time=" keyword in Fig. 2.
user_id	The user_id value represents the unique user in Baidu Cloud, through analyzing the id in Fig. 2, it is found after a keyword "user_id=".
qid	qid as same as the user_id, merely is defined by 360Yun server.
last_login_time	It means that the last login time user, to search the keyword, locating the position of login time in Fig. 3.

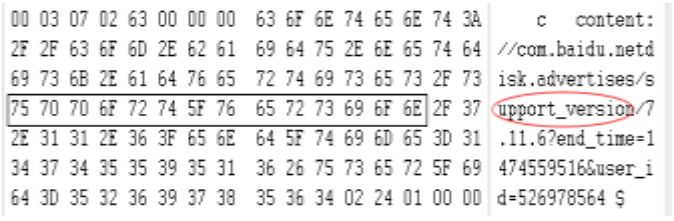

Fig. 4 Baidu Cloud Client Information

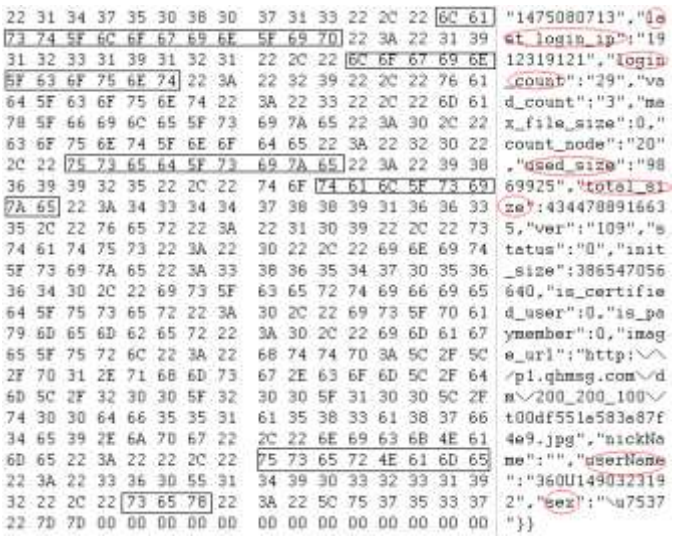

Fig. 5 360 Cloud Client Information

3) The relevant information of user operation file

A significant step before analyzing user behavior is that we need to know the user's operating cloud file. There are many important information files in cloud: filename, created time, upload time and file content, etc. We define the user behavior on the document to oper= {operation time, filename, operation type, hash value}. By analyzing scenario 1 and 2, we could analyze the behavior of Baidu cloud from volatile memory of the Android phone, as shown in Fig. 6 and 7.we acquire the related information, which include filename, created time, upload time and file content. Besides, By finding out the characteristics and rules of the file in the volatile memory, we

analyze the user's operating events, the information obtained is shown in Table V. Through the classification and analysis of these data, we reconstruct the user behavior of the file.

TABLE IV
THE FILED VALUE OF CLIENT CLOUD INFORMATION

Field name	Field Description
login_count	Through analyzing the keyword "login_count" in fig 5. We find it record the user login times.
used_size	It indicates that the user employ the disk size of 360 cloud, through analyzing.
total_size	It means that the Cloud server assigns the user's cloud size, through analyzing the size to evaluate the level.
last_login_ip	After user used the 360Yun cloud,the client record the login_ip. Through analyzing the login_ip in fig 5, we can get the Android mobile phone ip.

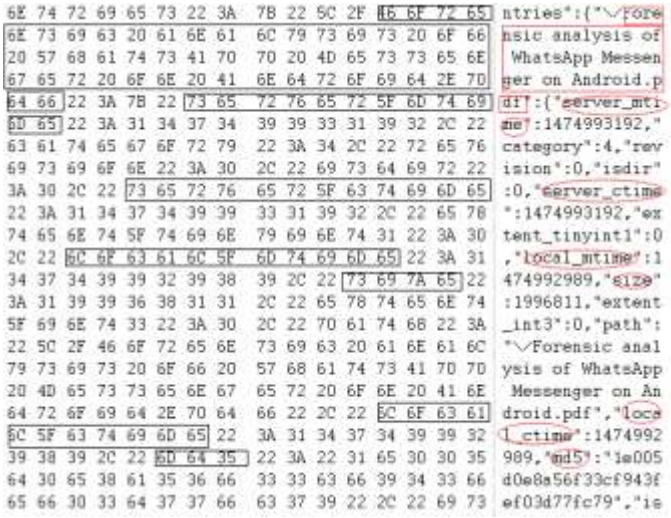

Fig. 6 The information of user operation files(Baidu Cloud)

Through the scenario 4 and 5，we could acquire 360 cloud disk memory dump, and analyze 360 cloud user operating files from volatile memory of the Android phone. As shown in Fig. 8 and Fig. 9, we find the characteristic and the rule of the data in the memory dump, and analyze the user's operation, we could discover the hash value of the corresponding document as well as the type of document operation, the name of the document, and the time attribute value of the document, especially there is a long string behind the file. The string is divided into three parts; The first part is that 1 to 20 characters represent document creation time; The second part of a character from 21 to 26 on behalf of the document size; And the last part is the file hash value, which shows in Table VI.

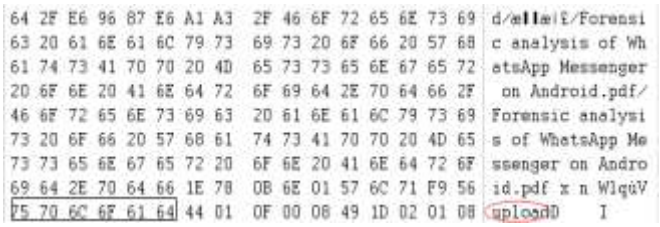

Fig.7 The information of user operation files(Baidu Cloud)

In order to verify the comprehensiveness of experiment accurately, we also make experiments such as scenario 3 and 6. For acquiring Android volatile memory, we removed the battery, and then restarted the Android mobile phone. Scenario 3 shows that we could only obtain Baidu cloud user filename, except the operation time of the file. Similarly, under scenario 6, we could only acquire filename but not operation time of the fil

TABLE V
ANALYSIS THE INFORMATION OF FILE IN BAIDU CLOUD

Field name	Field Description
server_ctime	Through analyzing the keyword "login_count" in Fig. 5. We find it record the user login times.
local_ctime	It describes the time that the local file was created . after a key word "local_ctime" ,we found the time is "1474992989" that was unix timestamp format in Fig. 6.
md5	To ensure the file correctly ,each file uploaded to the server, there is a corresponding md5 value in Fig. 6.
size	It describes the size of the file in cloud server.
File format	Each user operate different file, and that file owns different format, liking pdf, doc, picture.

4) The other relevant information

We also find all the filename that are stored in the user cloud disk from the volatile memory of Android phone, this can provide more useful information for forensic investigators. Besides acquiring the information in the cloud storage, we can also acquire the user phone information in the memory dump (such as mobile device models, mobile phone operating system version, etc.) as well as social software information.

TABLE VI
ANALYSIS THE INFORMATION OF FILE IN 360 CLOUD

Field name	Field Description
comstring	After the string "docx", the comstring is divided into three parts in Fig. 8.
size	It describes the size of the file in cloud server.we found the file size was "893859byte" after the keyword "size=" .
upload	It represents the user upload the file .
local	The hash value was found after a keyword "local=", composed with forty strings.

5) User behavior analysis

We can analyze the related information in the cloud disk through the six scenarios above. Identifying and summarizing the regularities and characteristics of the cloud storage related information are stored in the memory dump of the Android mobile phone. And then, we can obtain the customers operating information, analyze the cloud files and its related properties, reconstruct the user operating action time-line, and finally analyze the behavior of users.

B. Extract the cloud disk information from the memory dump

The experimental results proved that we can acquire a lot of

cloud disk related information in the volatile memory of Android mobile phone. Furthermore, by analyzing the structure and characteristics of the user's cloud disk files in the memory dump, we located the position of the relevant information. By long standing experiment test and various software version test, we found that the structure and characteristics of the different cloud storage software are different in the volatile memory, so we have to determine their characteristics and structure in the memory dump. Finally, we develop the automatic tools to extract and analyze cloud storage related information from the memory dump.

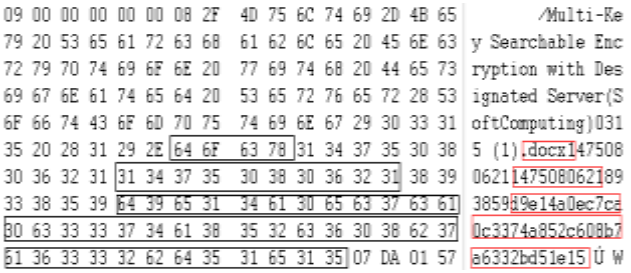

Fig. 8 The information of user operation files(360 Cloud)

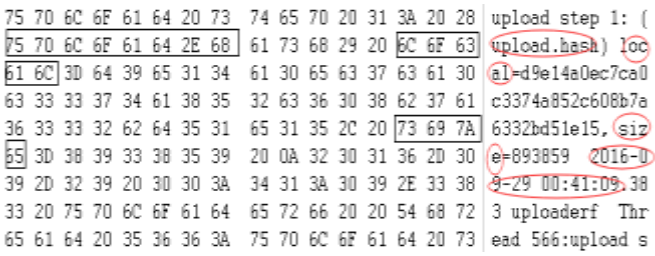

Fig. 9 The information of user operation files(360 Cloud)

1) Extract baidu cloud related information

Through searching the keyword "user_id" "end_time" in the memory dump, Baidu cloud user information can be located by logging the Baidu cloud client, include Baidu cloud username, login time, user id, support version, these information are shown in Fig. 10. In order to obtain the users log file information, we analyze the users operating event, search keyword to find the location of users operating files, extract the users operating file information. Moreover, we can also analyze the timestamp information to reconstruct the users behavior and analyze the files operation , shown in Fig. 11.

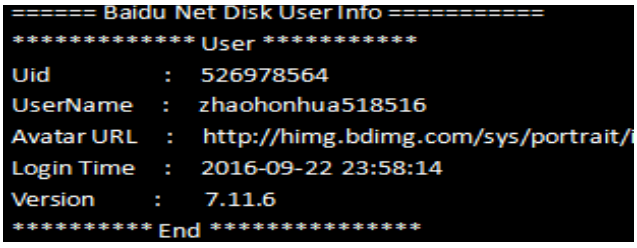

Fig. 10 Account Information of Baidu Cloud Client

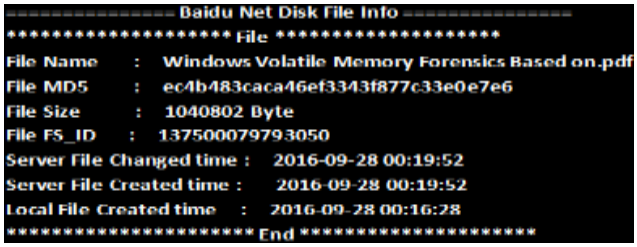

Fig. 11 Files Information of Baidu Cloud user operator

2) Extract 360 cloud information

Through searching the location of keyword in the memory dump, we obtain the users login information, which include user login time, login IP number, login-times, storage size of cloud, shown in Fig. 12. Moreover, through searching keywords and correlation analysis to locate user operating files in the memory dump, we discover the user operating files name, files time, files creating time, files size, as shown in Fig. 13. Finally, we classify the files through users operating time to reconstruct users behavior.

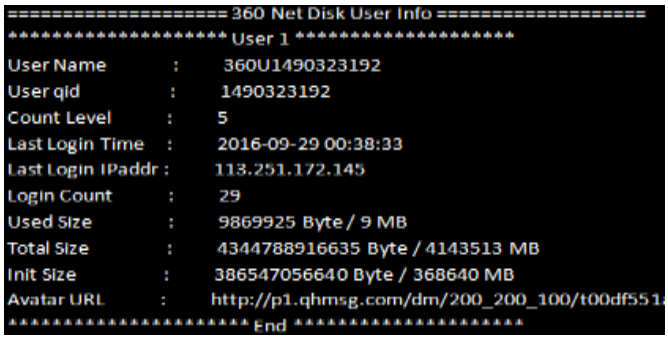

Fig.12 Account Information of 360 Cloud Client

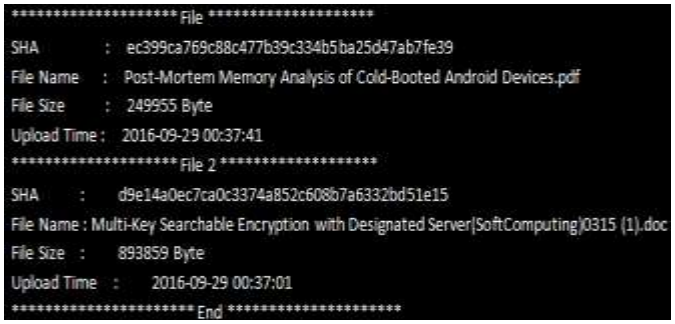

Fig. 13 Files Information of 360 Cloud user operator

VI. Conclusion

In this paper, we concentrates on discovering cloud storage application related information in the volatile memory of the Android mobile phone. Specifically, we choose two Chinese mainstream Android cloud applications—Baidu Cloud and 360Yunpan as cloud client to carry out the experimental test. The experimental results display that a lot of related information of cloud application stored in the volatile memory of the mobile phone, including the information of user file in the cloud application(such as the name of file, the creation time of file, operation time, operation event), user client information from memory(such as the version number, the use size of cloud disk size, total cloud disk size), network information （e.g.,

WiFi hotspots, telecom operators etc.） and the devices information. Through analyzing the memory dump under the six categories of tests, we identify and summarize the regularities and characteristics of the cloud storage related information are stored in the memory dump of the Android mobile phone. Moreover, according to the regularities and characteristics, we develop a tool that can automatically extract and analyze cloud storage related information from the memory dump. And then, we classify the information and reconstruct the behavior of user. Furthermore we can discover that even restart the phone after shut down a period of time; we can also recover the information from the memory dump. The work of this paper can provide a strategy for forensic investigators, this tool in this paper can be used as a forensic tool on Android phones to assist forensic investigators extract email-related evidence from memory dump.

Acquiring and analyzing the volatile memory of mobile phone is valuable to research. But owing to different manufacturer production of mobile phones and the fragmentation is a serious problem in Android investigation, it is a great challenge for researchers to extract all the information from different mobile phones. In the future, the main work is to acquire and analyze information from popular application software in memory dump of Android mobile phone, and establish a unified system to classify the information in volatile memory of Android mobile phone. It is more conductive for forensics investigators to take the evidence. With the improvement of the security of the mobile phone, obtaining the encryption key in volatile memory of Android mobile phone is also a main work in the future.

ACKNOWLEDGMENT

The authors would like to thank the reviewers for their detailed reviews and constructive comments. This work was supported by the National Social Science Committee of China (No. 14BFX156) and partially sponsored by New Direction Cultivation Program of Chongqing University of Posts and Telecommunications (No. A2015-45).

REFERENCES

[1] Müller T, Spreitzenbarth M. Frost[C]//International Conference on Applied Cryptography and Network Security. Springer Berlin Heidelberg, 2013: 373-388.

[2] Zhou F, Yang Y, Ding Z, et al. Dump and analysis of android volatile memory on wechat[C]//Communications (ICC), 2015 IEEE International Conference on. IEEE, 2015: 7151-7156.

[3] Heriyanto, Andri P. "Procedures and tools for acquisition and analysis of volatile memory on android smartphones." (2013).

[4] Google. "Ice Cream Sandwich," 14-April-2016; http://developer.android.com/about/versions/android-4.0-highlights.html#UserFeatures.

[5] Yen P H, Yang C H, Ahn T N. Design and implementation of a live-analysis digital forensic system[C]//Proceedings of the 2009 international conference on hybrid information technology. ACM, 2009: 239-243.

[6] J. M. Urrea, "An Analysis of Linux RAM Forensics," Master's thesis, Naval Postgraduate School, Monterey California, 2006.

[7] Thing, Vrizlynn LL, Kian-Yong Ng, and Ee-Chien Chang. "Live memory forensics of mobile phones." digital investigation 7 (2010): S74-S82.

[8] Leppert, Simon. "Android memory dump analysis." Student Research Paper, Chair of Computer Science 1 (2012).

[9] Sylve, Joe, et al. "Acquisition and analysis of volatile memory from android devices." Digital Investigation 8.3 (2012): 175-184.

[10] Wachter, Philipp, and Michael Gruhn. "Practicability study of android volatile memory forensic research." Information Forensics and Security (WIFS), 2015 IEEE International Workshop on. IEEE, 2015.

[11] Andrew Case. "Volatility Foundation" 14-April-2016; https://github.com/volatilityfoundation.

[12] Ntantogian, Christoforos, et al. "Evaluating the privacy of Android mobile applications under forensic analysis." Computers & Security 42 (2014): 66-76.

[13] David R. Andersen. "Cracking LUKS on Android Phones," 14-April-2016; https://dx.eng.uiowa.edu/dave/luks.php.

[14] G. R. Faulhaber, "Design of service systems with priority reservation," in Conf. Rec. 1995 IEEE Int. Conf. Communications, pp. 3–8.

[15] China Internet Watch, "80% China's Mobile Users Rooted Smartphones in 2014," 14-April-2016; http://www.chinainternetwatch.com/12926/80-china-smartphone-users-rooted/.

[16] Google, "Android Debug Bridge," 14-April-2016; http://developer.android.com/tools/help/adb.html.

Long Chen is a professor and an associate director of the Center for Information Security Technology Engineering, Chongqing University of Post and Communications. He is an intelligent digital security professional committee of the China Association for artificial intelligence, the editor of international journal, the appraiser of computer judicial. His main researched directions include network security, computer forensic, intelligent digital security, published papers in the authoritative journal, such as the Journal of Computer Science, Journal of Software, Electronic Journal. In all, he has published more than 30 paper in the domestic and foreign important journal or conference.