J Inf Process Syst, Vol.14, No.3, pp.680~693, June 2018
https://doi.org/10.3745/JIPS.03.0097

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Analysis of a Third-Party Application for Mobile Forensic Investigation

Jung Hyun Ryu*, Nam Yong Kim*, Byoung Wook Kwon*, Sang Ki Suk*,
Jin Ho Park**, and Jong Hyuk Park*

Abstract

Nowadays, third-party applications form an important part of the mobile environment, and social networking applications in particular can leave a variety of user footprints compared to other applications. Digital forensics of mobile third-party applications can provide important evidence to forensics investigators. However, most mobile operating systems are now updated on a frequent basis, and developers are constantly releasing new versions of them. For these reasons, forensic investigators experience difficulties in finding the locations and meanings of data during digital investigations. Therefore, this paper presents scenario-based methods of forensic analysis for a specific third-party social networking service application on a specific mobile device. When applied to certain third-party applications, digital forensics can provide forensic investigators with useful data for the investigation process. The main purpose of the forensic analysis proposed in the present paper is to determine whether the general use of third-party applications leaves data in the mobile internal storage of mobile devices and whether such data are meaningful for forensic purposes.

Keywords

Digital Investigation, Mobile, Forensics, Third-Party Applications

1. Introduction

The deep human desire to communicate more effectively and conveniently has led to the development of the wireless communication technology that we know and use today. In 2011, the number of mobile phones sold surpassed the number of PCs sold around the world; while in 2013, the number of users who wanted to use the Internet through mobile phones increased by nearly 60% to 800 million. In addition, the number of users who access social networking services has increased by about 200%, leading to a revolution in the modern way of life. However, according to a report released by a smartphone application analyst firm, the average number of applications used by each user per month was about 38, while the total usage time of the global benchmark application was about 900 billion hours [1,2]. Also, the volume of application downloads and sales at Apple's App Store and Google's Play Store are growing every year [3], thus indicating that a great deal of users' smartphone activities are being handled by third-party applications.

Manuscript received April 16, 2018; accepted May 21, 2018.
Corresponding Author: Jong Hyuk Park (jhpark1@seoultech.ac.kr)
* Dept. of Computer Science and Engineering, Seoul National University of Science and Technology (SeoulTech), Seoul, Korea ({jh.ryu, nykim, rnjsqud123, sksuk}@seoultech.ac.kr)
**Dept. of Computer Science, School of Software, Soongsil University, Seoul, Korea (j.park@ssu.ac.kr)

Given the statistics cited above, it is clear that the percentage of social networking applications in the mobile environment is enormous. In other words, in terms of digital forensics, users are more likely to leave traces of social networks, which is a difficult reality for mobile devices and applications. This is because mobile operating systems are frequently updated and numerous applications are released on a continuous basis. For example, Apple, the manufacturer of the iPhone, uses iOS as the operating system of the device, and has released a total of ten versions, averaging about 7 different detailed versions per version. The average interval between the releases of each new detailed version was approximately 1.5 months. These frequent updates and new releases can confuse forensic investigators in the field, making them uncomfortable, unlike the user's stance.

In addition, each application depends on whether or not the developer intends to leave the data on the device's internal storage. Therefore, if digital investigators perform digital forensic analysis with common mobile forensic tools and frameworks, some elements of digital evidence can be missed [4]. Nevertheless, no guidelines, tools or frameworks for digital forensics analysis of specific third-party applications have been established as yet. Furthermore, a simple forensic analysis of mobile devices could be rendered meaningless if the smartphone used to solve a cybercrime is mostly made up of third-party applications [5]. The main purpose of the mobile forensic analysis presented in this paper is to investigate the forensics issues raised by certain social networking services in iOS, Apple's mobile device, and to assist in the digital forensic investigation process.

In this paper, we provided the location and meaning of the data left by a third-party application, Instagram, on the internal file system of iPhones. To contribute to the investigation, we conducted examinations of the latest versions of iOS and various applications in order to resolve the difficulties faced by forensic investigators in the ever-changing mobile phone environment. The analysis presented in this paper could help with such investigations. Jung Hyun Ryu wrote most of this paper and presented the main concept of the scenario. Nam Yong Kim, Byoung Wook Kwon and Jin Ho Park assisted with the writing and the development of the main idea. Finally, Jong Hyuk Park reviewed the paper entirely as the corresponding author.

Section 2 presents a discussion of the related works about mobile forensics and a problem statement, as well as a simple definition of a third-party application; Section 3 describes the proposed method; Section 4 presents the results of the data analysis by the proposed method for each mean of data, findings, and changes; and Section 5 includes a discussion of the results for some generic issues of third-party application forensics, and the conclusion.

2. Related Works

Currently, the number of mobile devices worldwide has already surpassed that of PCs, and the potential for cybercrime using mobile devices has greatly increased. However, digital forensics is focused on the computer operating system, with which investigators are also familiar. The frequent updates and releases of diverse applications pose a considerable challenge to forensic investigators [6]. Mobile operating systems generally have a more closed policy than computer operating systems, and manufacturers and developers intentionally hide most of their codes. In addition, forensic workstation developers are hesitant about releasing their internal codes. If we look at the environment of mobile devices from the viewpoint of digital forensics, the characteristics of mobile technology, the various

types of firmware, and the different types of hardware and software issued by manufacturers cause forensic investigators a lot of problems. These new technologies and updates of mobile operating systems are often distributed and result in a short cycle of production [7].

In contrast, the development and updating of forensic workstations is relatively slow, creating a gap between the new technologies of mobile devices and those of forensic technologies. For this reason, the present paper focuses on new mobile devices, operating systems and applications, and that forensics analysis should be applied to other devices, operating systems, and third-party applications [8].

2.1 Third-Party Applications

In the current context of mobile phones, the term "third-party application" refers to an application creator or company, excluding manufacturers and mobile carriers. Because third-party applications can provide a better user experience than first- and second-party apps, most of the smartphone environment is made up of third-party applications. Third-party applications are very important in terms of forensics, because they are so diverse that they are likely to contain information about an individual's calls, messages, photos and personal information.

However, because they store different types of information, the same forensic analysis can lose information, making it necessary to consider forensics countermeasures for each third-party application.

2.2 Existing Research

In the field of digital forensics, mobile forensics is currently one of the most important areas of investigation. In particular, the forensic analysis of iOS devices raises many challenges compared to other operating systems and platforms. Research on the forensic analysis of Apple's mobile phone, the iPhone, is less common than research on other devices and platforms of operating systems.

The main research related to this paper presented a forensic analysis technique that used the backup function of the iPhone [11]. In their paper, the study is done through the iTunes backup utility for the forensic analysis process. This approach adhered to legally sound methods of forensic acquisition and did not break the file system of the device. The methodology was performed according to NIST's Computer Forensics Tool Test program guidelines. The experimental process consisted of the experiment requirements, the experimental plan and test cases, the acquisition and examination tools, the examination environment setup, and the test procedures and results.

Meanwhile, Tso et al. [12] presented an analysis of social network applications using the iTunes backup utility. Their study involved a forensic analysis of iOS version 4.3.5 of iPhone 4. They also analyzed Facebook, Skype, Viber and many other applications on Windows and other operating systems. Their study provided a specific file name containing the contents of each application in the backup data. In addition, their analysis of the backup data showed that analysis process can extract the key-record of all interactive contents and text messages. These results suggest that it could be used by investigators as digital evidence.

In addition, Zdziarski [13] discussed the overall structure of the iPhone's internal and file systems, and presented a wide range of vulnerabilities and security issues relating to the iPhone. Notably, this paper introduced a brute-force attack using the Sogeti tool to unlock the iPhone's device and decrypt the internal keychain, and then used it to encrypt all of the iTunes backup data. However, this

procedure does not work with the current versions of iOS 10.

Ahmed and Dharaskar [14] discussed the potential for emerging digital evidence in the mobile environment. It also discussed the differences between traditional computer forensics and the weaknesses of mobile forensic tools. In particular, they discussed the limitations of law enforcement in mobile forensic investigations and mentioned the need for differentiation.

In another paper, Raghav and Saxena [15] discussed the guidelines, challenges, and data preservation and acquisition in mobile forensics. They have been working to prepare for the growth of mobile cybercrime due to the ever-increasing use of mobile devices. Their study focused on data preservation and acquisition throughout the many stages of a mobile forensic investigation. The forensic process is subdivided according to the type of device on data preservation and acquisition. The guidelines on data preservation and acquisition proposed in their paper can be applied to various devices.

The study by Stirparo and Kounelis [16] focused on where data is stored and where data can be found in the mobile environment. They proposed a forensic methodology for assessing the privacy of mobile devices. The state of the data was categorized according to where the data was located and used for their MobiLeak project. They analyzed the data status of twelve third-party applications and the data type of a particular mobile operating system. They also discussed the privacy assessment by providing the results of a data analysis of various third-party applications [16].

Muraina et al. [17] proposed a framework for preserving data integrity in mobile device forensics. The main purpose of this study was to help mobile forensic investigations in Open Source Software (OSS) environments. Their framework uses three levels of authentication to preserve the integrity of data.

The iPhone backup function is one of the ways of acquiring the logical image of a mobile device. This method uses the iTunes program provided by Apple Computer to iPhone users, which is used to restore a mobile phone by copying the current mobile status bit by bit and storing it on iCloud or a PC.

3. Analysis Method

Access to the target device analysis is based on forensic analysis using Apple's iTunes backup utility [11, 12]. However, the procedures, logical data acquisition, and data analysis were slightly modified to suit the main purpose of this paper. The environment, software, and forensic workstations used in the analysis process are all free versions, but a more detailed analysis of the data will be conducted using a professional forensic analysis workstation.

3.1 Hypothetical Scenario

Before the forensic analysis, there are somethings to prepare such as installing the target application, Instagram, on the mobile device in the App Store and planning the hypothetical activities and making a dataset via specific activities through a fictitious account created by the suspect for forensic analysis.

Fig. 1 is an overview of the scenario performed by hypothetical suspects.

The first spreader, suspect A, posts a defamation or canard using the photo filter utility inside Instagram, while B checks A's post in the main feed, i.e., 'following' and 'like' A. Then, C 'follows' A and posts the same post as A.

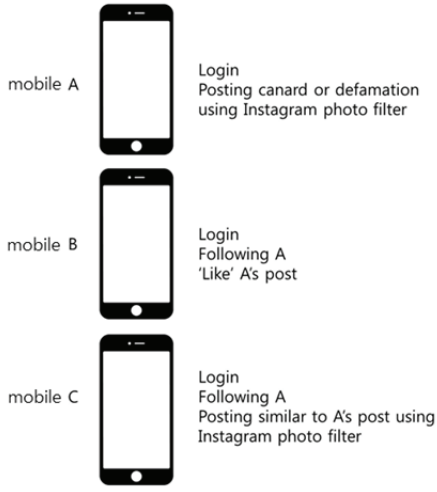


Fig. 1. Overview of hypothetical scenario.

3.2 Data Acquisition and Experimental Environment

The process of obtaining a logical image of a device's internal storage is carried out via the process of using iTunes to copy the directory and other types of files from the iPhone file system to bits [9]. This method of acquisition is a type of imaging because it copies the device's file system to bits. After performing the specific hypothetical activities described above, mobile must be set the mobile device flight mode to block all networks and connection with iTunes to perform backup of the device. We determined which target device and free software would be suitable for the experiment.

The target device, application and software set for the forensic analysis are shown in Table 1.

Table 1. Devices and software used in the experiment

	Devices and software
Target device	iPhone 6s (iOS 10.3.0)
App	Instagram (v.10.17)
PC OS	Windows 7
Software	EditPlus3 Plist editor for windows Apple iTunes iBackupBot iPhone Backup Extractor iBackup Viewer iPhone Tracker DB browser for SQLite

3.3 Analysis Process

In this paper, the backup of the iPhone using iTunes was made up of PCs. The main purpose of this analysis process was to focus on specific applications, rather than the entire file system of the iPhone, in order to help investigate a limited environment.

The backup process creates a folder named Unique Device Identifier (UDID), which is an identifier for the iPhone. In Windows 7, the default directory for the backup folder is C:\Users\'UserName' \AppData\Roaming\AppleComputer\MobileSync\Backup\'UDID'.

The created backup folder contains a file with a plist extension and a number of files consisting of database files and random hexadecimal digits. The random hexadecimal digits are the hashed value of the file system's domain and the path information of the iPhone via SHA-1. In previous papers and research reports, the files in hash values are all listed in the backup folder, but in the current version of the iOS, they are grouped into a folder based on the first two digits of the hash values. The plist files in the backup folder can be easily checked by a specific plist file viewer or editor; database files can be checked by SQLite; and images and videos can be checked by a common media player or a photo viewer. Files with hashed filenames had intuitive headers when checked through a particular plist file viewer or editor. The task of classifying these files consisted in writing a simple Python script code and classifying it, and then checking it again through the plist file viewer or editor to ensure that there were no lost files. The extensions were divided into various kinds of plist, sqlite, and image and video including the jfif type. However, only those files with plist and sqlite extensions were analyzed for the purposes of this paper. If the extension of a file was verified as a plist or sqlite, it was classified and analyzed whether the file was related to the target third-party application, i.e. Instagram.

The analysis process was performed by the plist file viewer and database browser for sqlite, and then checked by the backup file analysis software again. The reason for this dual analysis is that the backup file analysis software is not designed for forensic analysis, so it was assumed that data would be lost.

An overview of the analysis process is shown in Fig. 2.

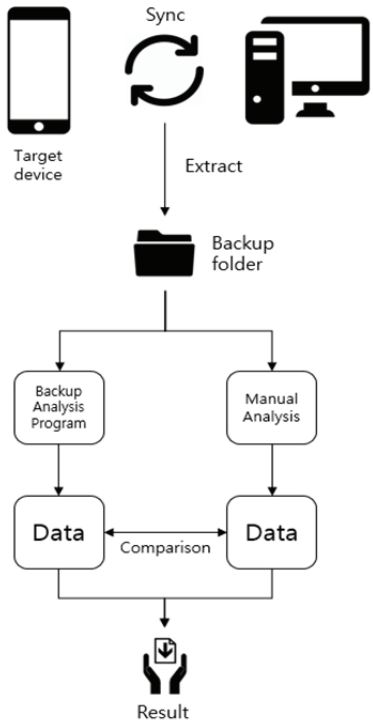


Fig. 2. Workflow of the analysis process.

4. Data Analysis

As a result of the analysis procedure described above, it was possible to obtain some meaningful data. Three files were found to contain information about the user's activities, using the plist editor and viewer, iBackupBot of VOW software, and iBackup Viewer of iMacTools. The file names are as follows:

- 72b88e49ac4f48605284907191d53d474397100f
- 83bcb5a9e2e253fcdc549d8d33a2a8dd7476f5e0
- 317bdcc8c07fcc4f7078e7d567cd58a474a30de4

The path of first file is 'com.burbn.instagram.plist' in the iPhone. This file contains such information as the last time the device attempted to log in as a real type, the last time the application approached the device internal photo album, the user name of the last login, the date and time of the user's last login, the date and time of installation of the application, and the date and time that the user last received the main feed.

The path of second file is 'Library/Cookies/Cookies.binarycookies' in the iPhone file system. This file contains information about the automatic login session, which makes it possible to view such information as the username, user ID, and session ID that attempted automatic login.

The path of third file is 'group.com.burbn.instagram' in the iPhone file system. This file contains more meaningful data than the two files mentioned above, including the list of the user's following information, and the searched hashtag and user ID by suspect. Especially, the user ID can present originality of each user. This can easily be changed to the user name if one uses Instagram's internal API. The data on search history includes the user ID and the hashtag, and the latter can be easily identified because it is exposed as the value of the search.

Figs. 3 and 4 are lists of data that can be verified by iBackupBot of the VOW software.

Fig. 3. Following user ID list.

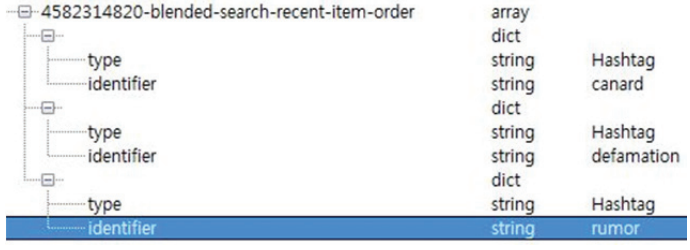


Fig. 4. Searched keywords list.

The user ID list of following, search history of user ID, and hashtags of the data analysis results are helpful in understanding the behavior of a suspected cybercriminal. This information can provide forensic investigators with clues or ideas about what the suspect may be thinking. For example, if this information is focused on cybercrimes such as defamation, canard, or electoral violations, it will be helpful in proving the crimes of a suspect that traces of hashtags searched for the purpose of defaming a

particular candidate, and traces of the fact that voters voted for a particular candidate during an election. The hashtag searched for purpose of adding photograph and videos when the suspect posts it. However, it should be noted that the history of searched hashtags is not searched using the internal searching function of an application. On the other hand, SQLite database files containing captions and information about the location of a posted photograph, and information about a direct message sent to a particular user in performed activities were not found.

The details of the contents of each file are shown in Table 2.

In this study, software and hardware write-block devices were not used in the process of acquiring logical data. Other studies have found that the images of backup files can be modified without using the Write-blocker, so other research and forensic investigations must use the Write-blocker in the process of acquiring data from backup files [4].

Table 2. Details of files and data

Filename	Path	Information
72b88e49ac4f48605284907191d53d474397100f	com.burbn.instagram.plist	Last device log time Inline gallery last interaction time Last logged in username Application installation date Last main feed fetch date
83bcb5a9e2e253fcdc549d8d33a2a8dd7476f5e0	Cookies.binarycookies	Instagram.com.csrftoken, Instagram.com.ds_user_id, Instagram.com.igfl, Instagram.com.sessionid
317bdcc8c07fcc4f7078e7d567cd58a474a30de4	group.com.burbn.instagram	Following user's code Blended search recent item order

4.1 Findings in the files

Some meaningful facts can be found when checking the data left by the devices used by suspects A, B, and C because of the hypothetical scenario. In the scenario, suspect A posted postings that included defamation and canard, and searched some hashtags. Suspect A used a photo filter inside Instagram when posting, which created a folder named 'Instagram' in the iPhone's internal photo album. Figs. 5–7 show analyses of the backup files of the mobile device used by suspect A.

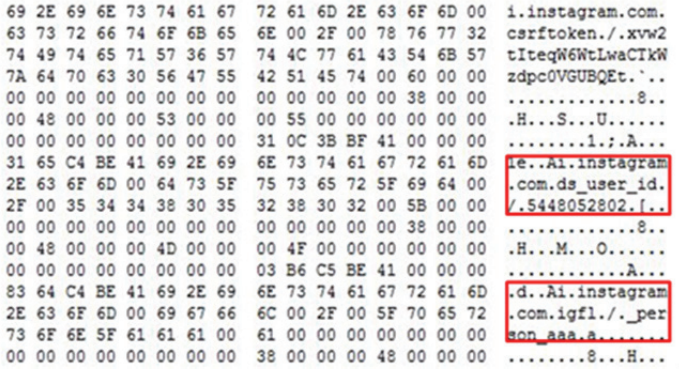
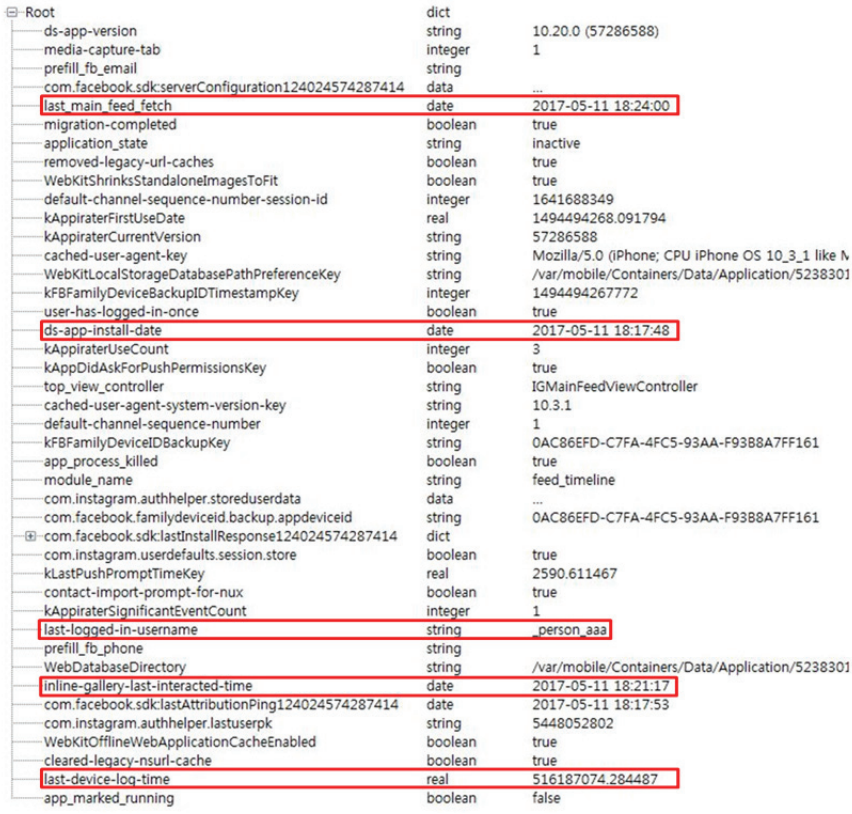
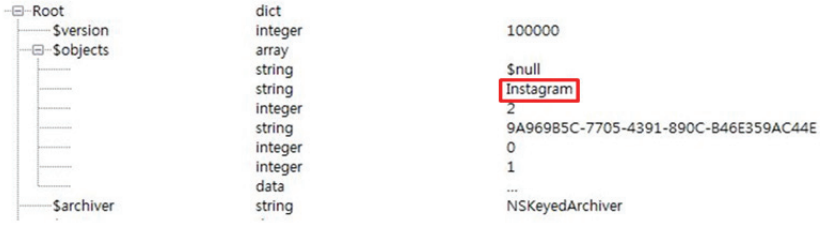


Fig. 5. Session information of cookie file.



Root	dict	
ds-app-version	string	10.20.0 (57286588)
media-capture-tab	integer	1
prefill_fb_email	string	
com.facebook.sdk:serverConfiguration124024574287414	data	...
last_main_feed_fetch	date	2017-05-11 18:24:00
migration-completed	boolean	true
application_state	string	inactive
removed-legacy-url-caches	boolean	true
WebKitShrinksStandaloneImagesToFit	boolean	true
default-channel-sequence-number-session-id	integer	1641688349
kAppiraterFirstUseDate	real	1494494268.091794
kAppiraterCurrentVersion	string	57286588
cached-user-agent-key	string	Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_1 like M
WebKitLocalStorageDatabasePathPreferenceKey	string	/var/mobile/Containers/Data/Application/5238301
kFBFamilyDeviceBackupIDTimestampKey	integer	1494494267772
user-has-logged-in-once	boolean	true
ds-app-install-date	date	2017-05-11 18:17:48
kAppiraterUseCount	integer	3
kAppDidAskForPushPermissionsKey	boolean	true
top_view_controller	string	IGMainFeedViewController
cached-user-agent-system-version-key	string	10.3.1
default-channel-sequence-number	integer	1
kFBFamilyDeviceIDBackupKey	string	0AC86EFD-C7FA-4FC5-93AA-F93B8A7FF161
app_process_killed	boolean	true
module_name	string	feed_timeline
com.instagram.authhelper.storeduserdata	data	...
com.facebook.familydeviceid.backup.appdeviceid	string	0AC86EFD-C7FA-4FC5-93AA-F93B8A7FF161
com.facebook.sdk:lastInstallResponse124024574287414	dict	
com.instagram.userdefaults.session.store	boolean	true
kLastPushPromptTimeKey	real	2590.611467
contact-import-prompt-for-nux	boolean	true
kAppiraterSignificantEventCount	integer	1
last-logged-in-username	string	_person_aaa
prefill_fb_phone	string	
WebDatabaseDirectory	string	/var/mobile/Containers/Data/Application/5238301
inline-gallery-last-interacted-time	date	2017-05-11 18:21:17
com.facebook.sdk:lastAttributionPing124024574287414	date	2017-05-11 18:17:53
com.instagram.authhelper.lastuserpk	string	5448052802
WebKitOfflineWebApplicationCacheEnabled	boolean	true
cleared-legacy-nsurl-cache	boolean	true
last-device-log-time	real	516187074.284487
app_marked_running	boolean	false

Fig. 6. Information of the plist file.



Root	dict	
$version	integer	100000
$objects	array	
	string	$null
	string	Instagram
	integer	2
	string	9A969B5C-7705-4391-890C-B46E359AC44E
	integer	0
	integer	1
	data	...
$archiver	string	NSKeyedArchiver

Fig. 7. Device internal album data in file system.

We can intuitively know the last 'mainfeed' fetch time, application installation date, last logged username, last gallery interaction time, last device log time, whether to create an Instagram folder in a device album, and the automatic login user ID and username. In the former version, the list of following users was known, but it was modified in the latest version. This is covered in the next chapter. In the case of suspects B and C, the following user was intuitively confirmed as suspect A.

4.2 Changes by Versions

The analysis of the case study described above was done in Instagram version 10.18. In the updated Instagram version 10.21, some of the data left behind as the iTunes backup utility were changed. In the previous version, the user's following list was easy to find, but this was impossible in the latest version.

These frequent updates and changes of data constitute a challenge for digital forensic investigators [10]. Fig. 8 shows the changes.

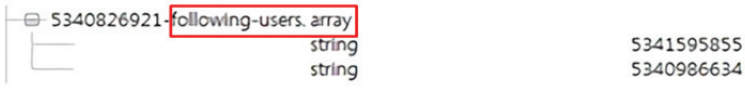


Fig. 8. Following user list of the previous version.

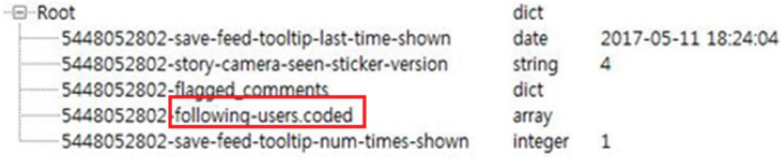


Fig. 9. Following user list of the latest version.

As explained above, the following user list was easily found in the old version, but it is coded in the latest version and could not be confirmed with any backup file viewer. Fig. 9 shows that the way in which Instagram stores data in the backup file has changed.

4.3 Comparison

This section presents a comparison with existing research based on an approach consisting of File System, Methodology, Examination, Specific Application, and Scenario. For this paper, we analyzed a specific social network application, Instagram, on the iPhone using a deeper approach than that applied by other papers to specific applications based on a hypothetical scenario. A comparison of the approaches is shown in Table 3.

Table 3. Approach comparison

Authors	File system	Examination	Specific app	Scenario-based
Bader and Baggili [4]	○	△	X	X
Tso et al. [5]	△	△	△	△
Raghav and Saxena [8]	X	X	X	X
Stirparo and Kounelis [9]	△	△	△	△
Proposed method	△	○	○	○

○=strong, △=medium, X=weak.

In the case of an approach involving the file system, Bader and Baggili [11] categorized extensions like SQLite and plist, and specified the name and content of the iPhone backup file. They also analyzed the role of each detailed file and its forensic significance. Tso et al. [12] partially approached the file system, and analyzed the five top-ranked applications in the App Store, but did not cover the entire file system. Meanwhile, Raghav and Saxena [15] did not attempt any approach to the file system of mobile devices in their research, whereas Stirparo and Kounelis [16] approached the file system of mobile devices for twelve different applications. They acquired data such as user information for each application in their privacy assessment of the mobile application. In this paper, we briefly analyzed the

file system of the backup files on iPhone mobile devices and discussed the specific social network application in detail.

In the case of an approach involving an examination, Bader and Baggili [11] experimented with analyzing almost every file system on the iPhone. Their examination covered the details about logical backup files and databases, including keychain, address book, call history, and calendar. Tso et al. [12] studied five target applications, discussed variation records and integration of application backup files, and extended the tests for each application. They provided relatively detailed information about the examination process. As for Raghav and Saxena [15], they provided forensic guidelines for various mobile devices, but did not perform an examination. In [16], the authors addressed the forensic view of the largest number of applications, but their examination was confined to privacy leakage. In this paper, we discuss a methodological approach and detailed experiments of forensic analysis.

In the case of an approach involving a specific application, Bader and Baggili's [11] forensic analysis mainly includes a database of pre-installed applications. Exceptionally, they discussed the database of Facebook, a typical social network application, but did not provide a detailed analysis. In [12], Tso et al. conducted a forensic analysis of Facebook, Viber, Skype, Windows Live Messenger, and WhatsApp. They provided an integration of each application backup file in the experiment and focused on the conversation content. In [15], the authors did not discuss any specific applications. In [16], the authors discussed the forensic aspects of twelve applications, including such applications as Box and Dropbox, but focused on privacy leakage. In this paper, we adopted an approach to one specific application and content that can help in the digital investigation of the various cybercrimes that can occur in this application.

In the case of an approach involving a specific application, the use of a scenario was not discussed in [11, 15, 16]. In [12], the authors discussed a scenario about fraud in the section on case description, but they performed no scenario-based examination. In this paper, we discuss a scenario-based examination that included violations of electoral laws, defamation, and the dissemination of false facts.

In the analysis presented by this paper, we present a scenario based on violations of political laws. Today, social networking applications can easily reveal individual opinions to an unspecified number of people. The scenario-based mobile forensic analysis methodology presented in this paper could be helpful for an investigation of an attempt by a malicious user to spread false facts or commit acts of defamation. A forensic analysis based on a specific scenario of a cybercrime situation has never been presented before in another research paper.

5. Conclusion

In this paper, we explain how specific data generated by performing activities are stored in the internal memory of a mobile device, and their significance. This process gave us a partial view of the location and meaning of data left by a specific third-party application. We hope that this paper will provide useful information to digital forensic investigators, as well as presenting an overview of the data we have covered so that we can assist with such investigations. The forensic analysis process covered in this research includes a hypothetical scenario, logical data acquisition, and data analysis. We found that the backup files on the iPhone can provide meaningful data for third-party applications, such as user information, activity history, and application settings. Following on from previous studies, there is a need for additional research on different types of third-party applications, other operating systems, and

mobile devices. The manufacturers and developers of mobile operating systems and applications need to consider potential forensic solutions in the face of increasing cybercrime, and develop the related forensic tools.

In addition, it is necessary to deal with the issues left by the Write-blocker, and the performed methodology could include missing data because there are some parts that have been directly accessed by reading the files [9]. If someone were to use a professional forensic analysis tool to resolve this issue, it may be possible to acquire other data. The mobile device and third-party application discussed in this paper have a large number of users all over the world including Korea. Especially by focusing on the characteristics of the social network service, suspects are likely to exploit the fact that information can be easily spread to an unspecified number of people. As a result, the application is likely to be exploited for cybercrime based on political activities, including violations of electoral laws, defamation of public statements, and canarding of certain persons. If an investigator uses the abovementioned process of analysis to investigate a cybercrime, we believe it will provide useful data for such an investigation.

Acknowledgement

This study was supported by the Research Program funded by Seoul National University of Science and Technology.

References

[1] App Annie, “App Annie 2015 retrospective: monetization open new frontiers,” 2016 [Online]. Available https://www.appannie.com/en/insights/market-data/app-annie-2015-retrospective/.

[2] E. Thompson, “App Annie 2016 retrospective: mobile’s continued momentum,” 2017 [Online]. Available https://www.appannie.com/en/insights/market-data/app-annie-2015-retrospective/.

[3] F. Marturana, G. Me, R. Berte, and S. Tacconi, “A quantitative approach to triaging in mobile forensics,” in Proceedings of 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Changsha, China, 2011, pp. 582-588.

[4] H. Kaur and K. R. Choudhary, “Digital forensics: implementation and analysis for google android framework,” in Information Fusion for Cyber-Security Analytics. Cham: Springer International Publishing, 2017, pp. 307-331.

[5] S. Rajendran and N. P. Gopalan, “Mobile Forensic Investigation (MFI) life cycle process for digital data discovery (DDD),” in Proceedings of the International Conference on Soft Computing Systems. New Delhi: Springer, 2016, pp. 393-403.

[6] E. Benkhelifa, B. E. Thomas, and Y. Jararweh, “Framework for mobile devices analysis,” Procedia Computer Science, vol. 83, pp. 1188-1193, 2016.

[7] R. Al Mushcab and P. Gladyshev, “Forensic analysis of Instagram and path on an iPhone 5S mobile device,” in Proceedings of 2015 IEEE Symposium on Computers and Communication, Larnaca, Cyprus, 2015, pp. 146-151.

[8] C. Carpene, “Looking to iPhone backup files for evidence extraction,” 2011 [Online]. Available: Https://doi.org/10.4225/75/57b2b9e540ce9.

[9] P. Gubian, “Exploring the iPhone backup made by iTunes,” The Journal of Digital Forensics, Security and Law, vol. 6, no. 3, pp. 31-62, 2011.

[10] T. Hone and R. Creutzburg, "iPhone forensics based on Macintosh open source and freeware tools," in Proceedings of SPIE 7881, Multimedia on Mobile Devices 2011. Bellingham, WA: International Society for Optics and Photonics, 2011.

[11] M. Bader and I. Baggili, "iPhone 3GS forensics: logical analysis using apple iTunes backup utility," Small Scale Digital Device Forensics Journal, vol. 4, no. 1, pp. 1-15. 2010. 4

[12] Y. C. Tso, S. J. Wang, C. T. Huang, and W. J. Wang, "iPhone social networking for evidence investigations using iTunes forensics," in Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication, Kuala Lumpur, Malaysia, 2012.5

[13] J. Zdziarski, Hacking and Securing iOS Applications: Stealing Data, Hijacking Software, and How to Prevent It. Sebastopol, CA: O'Reolly, 2012. 6

[14] R. Ahmed and R. V. Dharaskar, "Mobile forensics: an overview, tools, future trends and challenges from law enforcement perspective," in Proceedings of the 6th International Conference on E-Governance (ICEG), New Delhi, India, 2008, pp. 312-323. 7

[15] S. Raghav and A. K. Saxena, "Mobile forensics: guidelines and challenges in data preservation and acquisition," in Proceedings of 2009 IEEE Student Conference on Research and Development (SCOReD), Serdang, Malaysia, 2009, pp. 5-8. 8

[16] P. Stirparo and I. Kounelis, "The mobileak project: forensics methodology for mobile application privacy assessment," in Proceedings of 2012 International Conference for Internet Technology and Secured Transactions, London, UK, 2012, pp. 297-303. 9

[17] I. D. Muraina, M. M. Alobaedy, and H. H. Ibrahim, "A framework for preserving data integrity during mobile device forensic in open source software environment," in Proceedings of the Free and Open Source Software Conference (FOSSC), Muscat, Oman, 2017, pp. 22-26. 10

Jung Hyun Ryu https://orcid.org/0000-0002-0873-8398

He received B.S. in Department of Computer Science and Engineering, Seoul National University of Science and Technology (SeoulTech) in 2017. Since September 2017, he is with the Department of Computer Science and Engineering, SeoulTech as Master Course.

Nam Yong Kim https://orcid.org/0000-0003-0667-6872

He is a M.S. student in the Department of Computer Science at Seoul National University of Science and Technology (SeoulTech.), Seoul, South Korea. Currently, he is working in Ubiquitous Computing Security (UCS) Lab under the supervision of Prof. Jong Hyuk Park. His broadly research interest includes information and cyber security, cloud computing, IoT, network security, artificial intelligence. Before joining M.S. at SeoulTech, he received his B.Tech. In Computer Engineering from Dongguk University Lifelong Education Institute, Seoul, Korea.

Byoung Wook Kwon https://orcid.org/0000-0002-7730-5713

He received B.S. in Department of Computer Science and Engineering, Dongseo University in 2017. Since March 2017, he is with the Department of Computer Science and Engineering, Seoul National University of Science and Technology (SeoulTech) as Master Course.

Sang Ki Suk https://orcid.org/0000-0001-5948-4423

He obtained his Bachelor's degree in Computer Engineering at Hongik University, and Master's and Ph.D. degrees in Computer Engineering at Hongik University. He is currently serving as a professor in the Department of Computer Science and Engineering at Seoul National University of Science and Technology, and the areas of main interests include database architecture, distributed/objective computing, and so on.

Jin Ho Park https://orcid.org/0000-0003-1961-6983

He obtained his Bachelor's degree in Software Engineering at Soongsil University, and Master's and Ph.D. degrees in Software Engineering at Soongsil University. He is currently serving as a professor in the department of software at Soongsil University, and the areas of main interests include SW safety/quality/testing, SW fusion/soft power, Internet of Things, military ISR, IT service, IT technology commercialization/ start-up.

James J. (Jong Hyuk) Park https://orcid.org/0000-0003-1831-0309

Dr. James J. (Jong Hyuk) Park received Ph.D. degrees in Graduate School of Information Security from Korea University, Korea and Graduate School of Human Sciences from Waseda University, Japan. From December, 2002 to July, 2007, Dr. Park had been a research scientist of R&D Institute, Hanwha S&C Co. Ltd., Korea. From September, 2007 to August, 2009, He had been a professor at the Department of Computer Science and Engineering, Kyungnam University, Korea. He is now a professor at the Department of Computer Science and Engineering and Department of Interdisciplinary Bio IT Materials, Seoul National University of Science and Technology (SeoulTech), Korea. Dr. Park has published about 200 research papers in international journals and conferences. He has been serving as chair, program committee, or organizing committee chair for many international conferences and workshops. He is a steering chair of international conferences – MUE, FutureTech, CSA, CUTE, UCAWSN, World IT Congress-Jeju. He is editor-in-chief of *Human-centric Computing and Information Sciences* (HCIS) by Springer, *The Journal of Information Processing Systems* (JIPS) by KIPS, and *Journal of Convergence* (JoC) by KIPS CSWRG. He is Associate Editor / Editor of 14 international journals including JoS, JNCA, SCN, CJ, and so on. In addition, he has been serving as a Guest Editor for international journals by some publishers: Springer, Elsevier, John Wiley, Oxford Univ. press, Emerald, Inderscience, MDPI. He got the best paper awards from ISA-08 and ITCS-11 conferences and the outstanding leadership awards from IEEE HPCC-09, ICA3PP-10, IEE ISPA-11, PDCAT-11, IEEE AINA-15. Furthermore, he got the outstanding research awards from the SeoulTech, 2014. His research interests include IoT, Human-centric Ubiquitous Computing, Information Security, Digital Forensics, Vehicular Cloud Computing, Multimedia Computing, etc. He is a member of the IEEE, IEEE Computer Society, KIPS, and KMMS.