Forensic Analysis of Social Networks Based on Instagram

Ming Sang Chang and Chih Ping Yen
(Corresponding author: Chih Ping Yen)

Department of Information Management, Central Police University
Taoyuan 33304, Taiwan
(Email: peter@mail.cpu.edu.tw)

(Received Feb. 23, 2018; Revised and Accepted Oct. 18, 2018; First Online June 15, 2019)

Abstract

The trend in social networking is changing people's life style. Since both the smart phone and computers are connected to the same tools, the newly developed applications must serve both ends to please the users. Although the previous flourishing social networks such as Facebook, Google+, and LinkedIn, among the other social network sites, still have a high number of users, but their growth rates have gradually flattened. They have been replaced by emerging social networking sites such as Instagram. Therefore, the modes of cybercrime have also changed in accordance with the users' activities. In order to identify crimes, it is basically necessary to use appropriate forensic techniques to retrieve these traces and evidence. This study considers the social network, Instagram, as the research subject. Analyze the artifacts left on the Instagram application and shows evidence of gathering such as posting pictures, tagging others, leaving comments and liking on Windows 10 and Android platform, respectively. Besides, this study uses an anti-forensic process to explore the differences between the traces that are left on different browsers, browsing environments, and operating systems. Finally, forensic analysis found that different browsers, due to the differences in privacy control, can lead to the discrepancies in recording the user behaviors on the same social network. It proves to be helpful to forensic analysts and practitioners because it assists them in mapping and finding digital evidences of Instagram on Windows 10 PC and Android smart phone.

Keywords: CyberCrime; Digital Forensics; Instagram; Social Network

1 Introduction

Social networking websites provide a virtual exchange space on the internet for people with common interests, hobbies, and activities to easily share, discuss, and exchange their views without any limitation of space and time. Therefore, social networking websites continue to accumulate a large number of users. According to the Metcalfe's law, the value of a telecommunications network is proportional to the square of the number of connected users of the system [2].

As a result, social networking has become a great force in today's society. However, this has also brought about endless criminal activities on social networks, such as cyberbullying, social engineering, and identity theft, among the other issues. Due to the following characteristics, the detecting cybercrime on social networks is different in comparison to other cybercrime [7]. Therefore, to assist the investigators in improving their efficiency of solving crimes, researches focusing on these upcoming technologies are needed [13].

- Anonymity: Users are often unaware of the true identity of their counterpart in a social network because they are dealing with a fake account. Therefore, in the case of a social network cybercrime, it is difficult to extract the suspect's information and make arrests immediately [3].

- Diffuseness: Any news published on the social network will be forwarded or shared immediately, which generates the diffusion effect [15]. Therefore, if a social network crime is not responded to immediately, it may cause the victim to suffer some serious damage.

- Cross-Regional feature: Due to the nature of internet, the location of the cybercrime is not necessarily the place where the criminal suspects are located. A bottleneck is formed during the crime investigation due to the difficulty in locating the suspects [9].

- Vulnerability of Evidence: The evidences obtained on social networks are in the form of digital data. In addition to the highly volatile nature of the digital evidences in the processing program from collection to storage, it is easy to change, delete, lose, or contaminate the digital evidences due to the anti-forensics

operation of the suspects or negligence of the investigators [10].

According to the eBizMBA statistics [5], the major social networking websites in the world include Facebook, YouTube, Twitter, Instagram, LinkedIn, Pinterest, Google Plus, Tumblr, and Reddit, among others. Although Facebook has the highest number (2.07 billion for Q3 2017) of the monthly visitors on the social networking websites, a large number of users do not contribute toward a high growth rate and a high usage rate.

There may not be too many active accounts, one person may have several accounts, or the website may not attract the youth. So, to understand the future development of a social network, we must examine the growth rate at a deeper level. Ever since breaking into the top 15 website with most users in 2014, Instagram has maintained its 7th ranking until it made a significant jump to the 4th place in July 2017, the Dreamgrow latest statistics and then jumped to 3rd place in January 2018 [4]. In 2016, it had 110 million users in a single month and the number grew to 275 million in 2017, creating the highest growth rate of 150% and taking the first place in the growth rate. According to the statistics of Statista, the number of active users on Instagram was 600 million in December 2016 and 800 million in September 2017, which ranked Instagram as the first website with a growth rate of up to 33.3%.

Globally speaking, Instagram is most popular with teens and young Millennials, 41 percent of users are 24 years of age or younger in the United States, beating out Twitter and Facebook [16]. Besides, Matthew Pittman proposed that image-based platforms (e.g. Instagram) may be worth more than text-based platforms (e.g. Twitter) [12]. Instagram also proved to be a particularly useful platform for health and smart city of the application [8, 14]. Therefore, we can say that Instagram will be the most popular among the social networking application in the near future.

This study considers the social network, Instagram, as the study subject. User activities are performed through internet webpages, virtual smart phones, and smart phones. Forensic analysis is conducted to understand what type of user behavior leaves digital evidence on Windows 10 and Android. We also use an anti-forensic process to explore the differences between the traces that are left on different browsers, browsing environments, and operating systems. The results will be served as a reference for the future researchers in social network cybercrime investigation or digital forensics.

The rest of this paper is organized as follows. In the next section, we present our related work. In Section 3, we present our methodology. In Section 4, we present the results and findings of computer forensics on Instagram. Finally, we summarize our conclusions.

2 Overview of Instagram and Social Networking Forensics

2.1 Instagram

Instagram, established in October 2010, is a social networking application which allows the users to share their pictures online for free. Users on Instagram can capture a picture with a smartphone, add different filter effects to the picture, and share it on Facebook, Twitter, Tumblr, and Flickr or on the Instagram. The web version of Instagram was launched toward the end of 2012, which allowed the users to browse pictures directly on their computers and perform some user actions on their own Instagram page. Although the mobile application has more functions, the PC version is still expanding its functionalities [19].

Instagram is mainly used for uploading pictures, following user accounts, adding tags (# and text), comments, and forwarding photos to other social networks, among others. It should be noted that Instagram does not have the "Add Friends" feature; the users browse pictures shared by other people's accounts by directly "following" them. Since the web-based version of Instagram has not yet provided the option to upload and image, the open software Gramblr is used to support such functions on the web version of Instagram. In addition to the photo uploading and posting service, it is yet to provide services such as sharing photos on other social networks, reposting the links shared by others, sending photo emails, and GPS function.

2.2 Social Networking Forensics

Presently, various researches focusing on the forensic analysis of social networking are being conducted. William Glisson explored the effectiveness of different forensic tools and techniques for extracting evidences on mobile devices [6]. In 2014, Christoforos Ntantogian made a privacy assessment of Android mobile devices and their APPs for forensic analysis and found some security concerns in certain Android apps [11]. In 2015, Nikos Virvilis presented studies based on the security of web browsers and reported the shortcomings and vulnerabilities of browsers operated on desktop and mobile devices. It was found that some browsers using secure browsing protocols had actually limited their own protection level [18]. Nor Zarina Abidin published a forensic analysis study of Instagram on iPhone and reported the integrity and address of some material evidences of user behaviors extracted [1]. Jia-Rong Sun proposed the viewpoints of cybercrime investigation and forensic procedures for the research of investigation and forensic procedures [17]. In 2017, Yusoff report the results of investigation and analysis of three social media services (Facebook, Twitter, and Google +) as well as three instant messaging services (Telegram, OpenWapp, and Line) for forensic investigators to examine residual remnants of forensics value in

Firefox OS [21]. Song-Yang Wu describes several forensic examinations of Android WeChat and provides corresponding technical methods [20].

This paper investigated the user behaviors by logging into Instagram for uploading images, comments, and browsing other people's accounts. We conducted forensics and anti-forensics, and explored and compared the type of user behavior that leaves digital evidence on the device. The results will be served as a reference for the future researchers in social network cybercrime investigation or digital forensics.

3 Methodology

3.1 Research Goal

This paper studies the user behaviors including logging into Instagram, uploading images, exchanging information, and browsing other accounts through different browsers (Chrome, Internet Explorer, and Firefox) under a PC Window 10 environment and the APPs under an Android environment of virtual mobiles and physical mobiles. The study also explored and compared the type of user behavior that leaves digital evidence on the device, and how these evidences can be searched. Finally, cleaning software was used to simulate the elimination of the evidence and restoration software was used to restore the evidence. Finally, we checked the changes and discrepancies in the residual digital data and relevant material evidence on the computer.

3.2 Experimental Environment

This study is built on two operating system environments: the first is Windows 10 that uses VMware virtual machine software on PCs for cost considerations. It generates multiple VMware virtual machines, and each is equipped with its industrial version 64-bit Windows 10 operating system. The second is Android 5.0/6.0, installed on a phone and a Bluestacks virtual mobile device, respectively. The Bluestacks virtual mobile device operated in Windows 10 environment of VMware virtual computer, and then the Android 6.0 operating system is chosen after installing the Bluestacks virtual mobile device software.

Subsequently, three versions of browsers, *i.e.*, Google Chrome, internet Explorer, and Firefox were installed in the Windows 10 operating environment. Each browser had a normal browsing mode and a private browsing mode for browsing the Instagram social network page. Under the Android 5.0/6.0 operating environment, the Instagram social networking application was installed to run the Instagram features directly. The abovementioned hardware and software are detailed in Table 1.

3.3 Forensics and Anti-forensics Tools

This study used different forensics and anti-forensics software and tools for different experimental situations. For the post-experiment results of the web version, a forensic analysis was done using WinHex on VMDK file and VMEM file of the VM virtual machine; and the db files of VM virtual machine were read and analyzed using DB Browser for SQLite.

An access analysis was done using SQLite Editor on db files of Bluestacks virtual mobile devices to simulate the post-experiment results of the mobile version. ES File Explorer was used to view the files on the Bluestacks virtual mobile device and Free Opener was used to view the VM virtual machine files on the Bluestacks virtual mobile device. Finally, WinHex was used for forensic analysis of associated files.

The physical smart phone uses SQLite Editor to read and analyze the db files on mobile devices. The built-in file manager V2.0.0.333_161109 was used to view the files on the mobile device.

To carry out anti-forensic studies after the web version experiment, the information in the folder was completely removed using the Eraser Portable software. A final thorough cleaning of the environment, including cookies, index.dat, Windows log files, history records, internet cache, network temporary files, system temporary files, and memory dump, was accomplished using the CCleaner software. Then, a forensic analysis was done using WinHex and DB Browser for SQLite. The abovementioned software tools are listed in Table 2.

3.4 Experiment Elaboration

We separated the experiments into following five scenarios according to the different browsers or Instagram App to ensure the integrity of digital evidence and avoid the interference between digital evidences. Based on the experimental environment designed in the previous section, we run the Instagram features, including logging in, uploading pictures, comments, liking a post, following, and browsing. Finally, the relevant evidence on each device was extracted and analyzed using forensic and anti-forensic tools.

1) Scenario 1: Google chrome. In the environment of VM virtual machine installed on Google Chrome, we logged into the Instagram webpage for running various features using the normal browsing mode and private browsing mode to identify and analyze the VMDK file and VMEM file of the VM virtual machine as well as to search for any material evidence left by the users.

2) Scenario 2: Internet explorer. We used Internet Explorer as the browser, and the experimental environment and steps are the same as in Scenario 1.

3) Scenario 3: Mozilla firefox. In this scenario, Mozilla Firefox was used as the browser, and the experimental environment and steps are also the same as in Scenario 1.

Table 1: List of hardware and software used for analysis

Devices/Tools	Introduction	Specification/Versions
ASUS M32AD-US032S	Desktop PC	Intel Core i7-4790 (3.60 GHz), 16 GB DDR3, 2 TB HDD
ASUS Zenfone 5	Android smart phone	T00P, Android 5.0, CPU 1.2GHz, Memory 16G
VMware Workstation	Virtual machine software	Version 12.5.0 build-4352439
Windows 10	Microsoft operation system	Version Enterprise (64-bit)
BlueStacks	Android emulators for PC	Version 3.0.0.82, Android 6.0
Google Chrome	Browser	Version 51.0.2704.103
Internet Explorer	Browser	Version 48.0.2
Mozilla Firefox	Browser	Version 2.7.3 (64-bit)
Gramblr	Upload photos and post content to Instagram from PC	Version 8.0 (for Windows 10)
Instagram	Social networking media for sharing photos and videos	Version 8.4.0 (for Android)

Table 2: List of software tools used for analysis

Devices/Tools	Introduction	Specification/Versions
WinHex	Universal hexadecimal editor	Version 18.9
DB Browser for SQLite	GUI editor for SQLite databases	Version 3.9.0
SQLite Editor	edit SQLite database on smartphone	Version 2.1.1
ES File Explorer	browsing files on Android devices	Version 4.1.2.4
Free Opener	A versatile file viewer supporting Office documents and multimedia formats	Version 2.2.0.0
Eraser Portable	Data removal tool	Version 5.8.8.1
CCleaner	Delete temporary or potentially unwanted files	Version 5.19.5633
Recuva Portable	Restore accidentally deleted files	Version 1.52.1086

4) Scenario 4: Bluestacks virtual device. In the environment of VM virtual machine installed on virtual device using Bluestacks, we logged into the Instagram app for running various features to identify and analyze the VMDK file and VMEM file of the VM virtual machine as well as to search for virtual device left by the users.

5) Scenario 5: Android smartphone. In the smartphone installed on Android 5.0 version, we logged into the Instagram app for running various features to search for any material evidence left by the users.

4 Result and Findings

4.1 Findings: Scenario 1: Google Chrome

Normal browsing mode:

1) For VMDK file from the hard disk of the computer, we used WinHex to search for the keyword "www.instagram.com/", and the name of the experiment account (pomeloojiayi) and its nickname "pomelo" on Instagram were found, as shown in Figure 1. Then we searched the keyword "Gramblr", and the photos uploaded to Instagram were found in the path "C:\Program Data\Gramblr\pomeloojiayi", including the original images and the modified image files, as shown in Figure 2.

When we searched using the keyword "/? Taken-by=", the URL for uploading the photos could be found. The URL of these photos has a fixed format "https://www.instagram.com/p/Photo Coding/? taken-by = photo account." If the photo account displayed after the equal sign is an experimental account, it indicates that there has been some uploading or browsing behaviors. Otherwise, it belongs to others. The evidence shown in Figure 3 indicates that the experimental account has some uploading or browsing behaviors. A search by keyword "gramblr.db" will display the database location where Gramblr resides on a computer, in the path "C:\Program Data\Gramblr\gramblr.db." This file can be viewed using DB Browser for SQLite, and the experimental account and the password can be found, as shown in Figure 4.

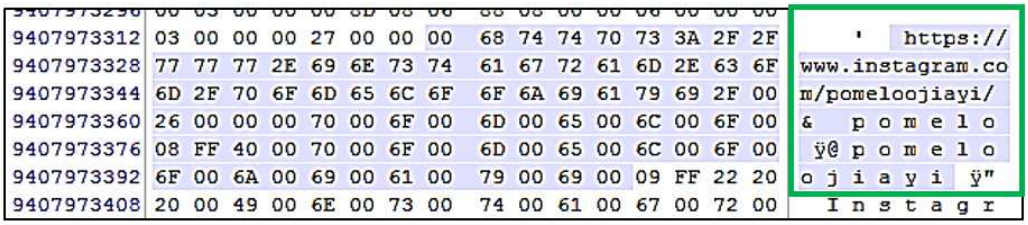

Figure 1: Search results of the keyword "www.instagram.com/" using WinHex

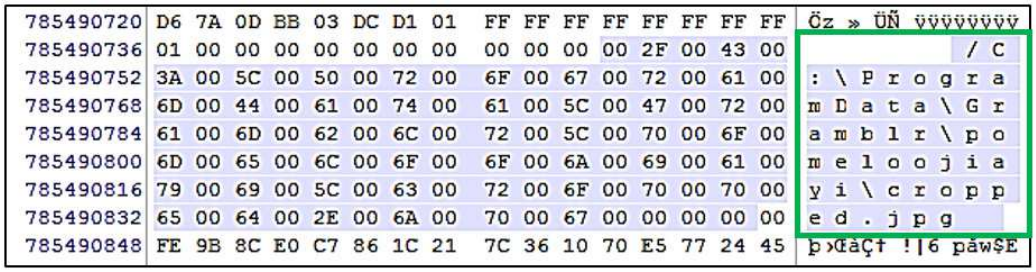

Figure 2: Search results of the keyword "Gramblr" using WinHex

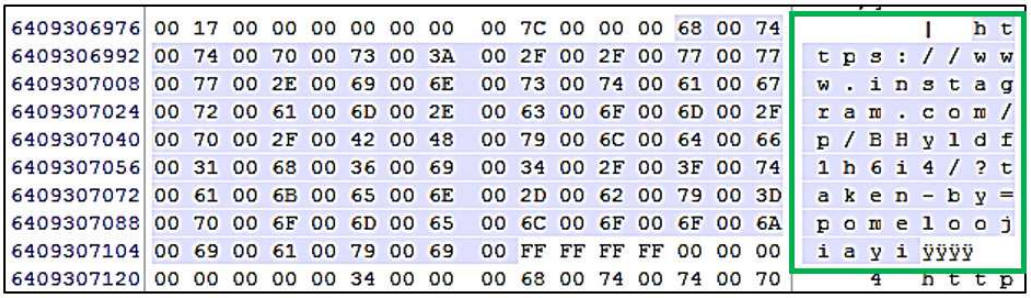

Figure 3: Search results of the keyword "/? Taken-by=" using WinHex

A search by the keyword "text" revealed the traces of comments left by the account on the pictures of the other user's account, while Figure 5 show the comment "TEESTT" left by the experimental account. In addition, it is impossible to find the evidence through the time of uploading photos and posting, posted content, and the user behaviors such as tagging others, adding tags, following other user's account if WinHex is used to search by the following keywords: time, timestamp, tag, follower, like, label, and other's account.

2) For VMEM file, *i.e.*, the memory of the computer for forensics, we performed the same forensics as described in 1) above and found the same evidence as the VMDK file. However, if the search were made with the keyword "like", the evidence and the time stamp of "liking" by the experiment account could be found, as shown in Figure 6.

3) In the LIVE deleted data for anti-forensics, all the files in the pomeloojiayi folder of the experimental account under the Gramblr path were erased with Eraser Portable; and Gramblr was then removed completely from the control panel. In addition, CCleaner was used to perform a thorough cleaning of data such as cookies, index.dat, Windows log files, history records, internet cache, network temporary files, system temporary files, and memory dump, among other information. Next, the same forensics as described in 1) and 2) above were performed. The results showed that there was a substantial decrease in the number of evidence. However, the hard disk retained the nickname (pomelo) and the website of the uploaded pictures. The memory generally kept the paths of the originally uploaded picture files and modified picture files, but the pictures themselves were deleted and the original contents could no longer be accessed. Finally, Recuva Portable was used to recover the deleted data and files, and the forensic analysis was repeated. The results showed that the deleted evidence could no longer be retrieved from the hard disk and the memory.

4) After the device was shut down and restarted, the forensics of the hard disk showed that the remnant evidence indicated the Instagram account, nickname, and the paths of the original

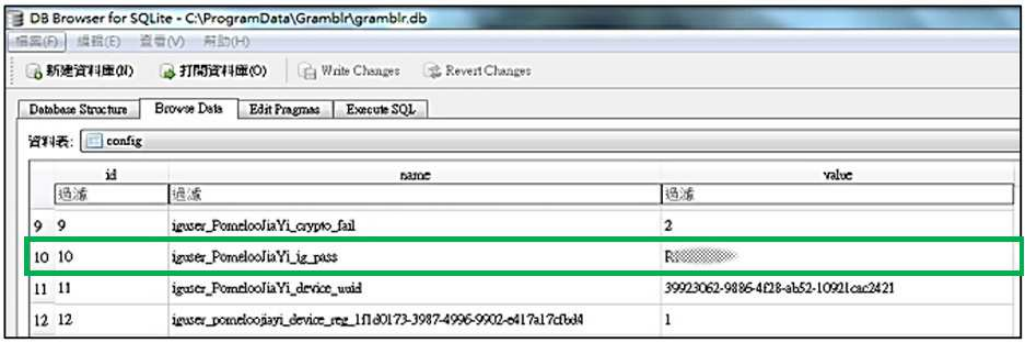

Figure 4: Viewing gramblr.db with DB Browser for SQLite to reveal the experimental account and password

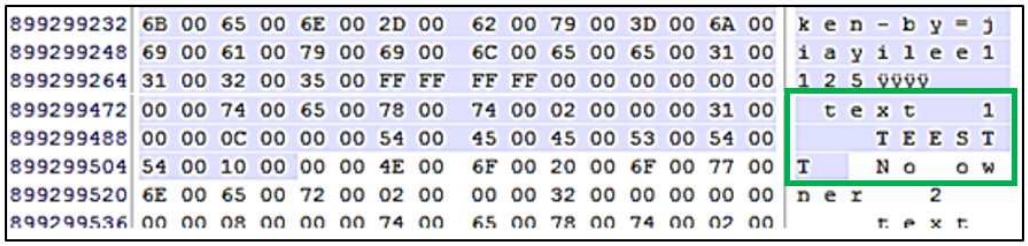

Figure 5: Research result of the keyword "text" using WinHex

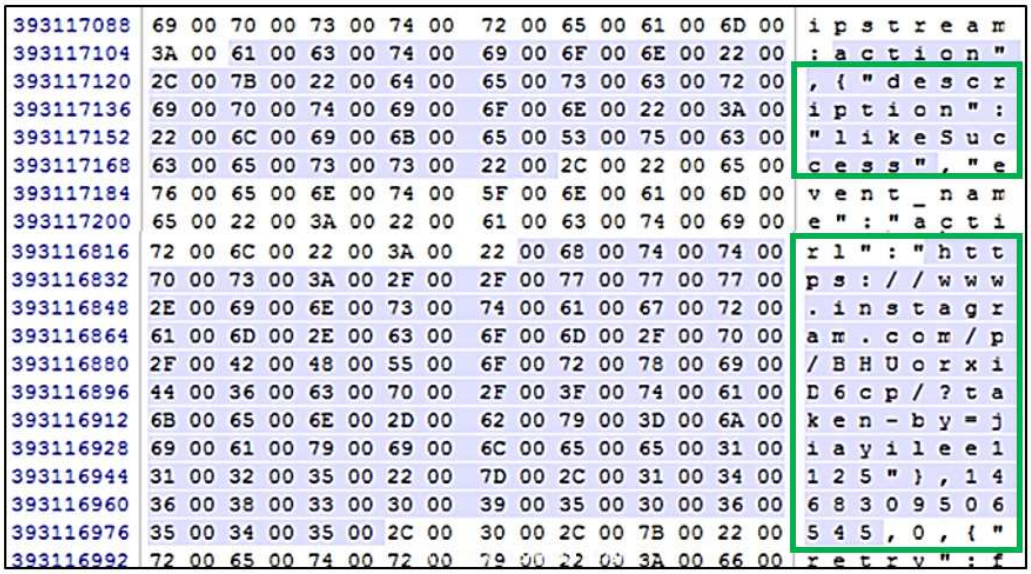

Figure 6: Search results of the keyword "like" using WinHex

and modified uploaded picture files. The forensics of the memory showed the same remnant evidence, except that the nickname pomelo was no longer there. This was followed by a data delete action, as described in 3) above. The forensics of the hard disk still showed the experiment account, but the nickname has been deleted. The websites of the uploaded pictures were still there, but the pictures had been cleared, and the original contents can no longer be accessed. As for the memory, the forensic results were the same as in 3). Finally, Recuva Portable was used to restore the deleted data and files; however, the nickname can no longer be found on the hard disk.

Private browsing mode:

1) After the experiment was made in the private browsing mode, the forensics of the hard disk showed that the contents existed in the normal browsing mode, had all disappeared. However, the evidence for posting content and # tags were retained, as shown in Figures 7. The other evidences were the same in both the normal and the private browsing modes.

2) In the memory, the posting content and # tags can only be found in the private browsing mode,

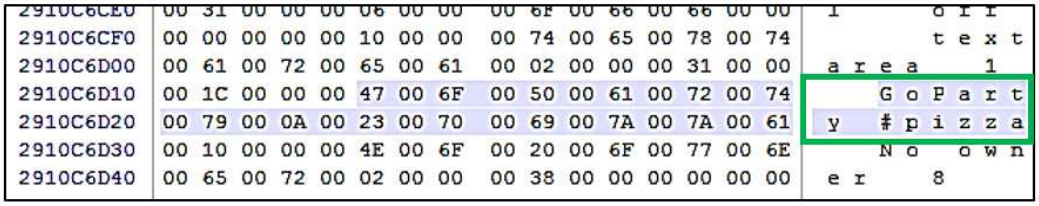

Figure 7: Text and # tags found in VMDK file

and not in the normal browsing mode. The evidence of the nickname of the experimental account, which was present previously in the normal browsing mode, disappeared in the private browsing mode. The other remaining evidences include the experimental account, the web addresses of text and pictures, the contents of text and pictures, # tags, the paths of uploaded photos, the browsing traces, and the comment contents.

3) In terms of LIVE deleted data for anti-forensics, after performing the deletion steps in the general browsing mode described above, the forensic analysis showed that the hard disk contained only the evidence of posting content and # tags. The memory only contained the paths of the original and the modified uploaded photo files. The other evidences, such as the experiment account, posting content, # tags, the websites of the uploaded photos and texts, and the comments, had all been deleted. Finally, Recuva Portable was used to recover the deleted data and files, and the repeated forensic analysis showed that the deleted evidences can no longer be retrieved from the hard disk and the memory.

4) After the device was shut down and restart, the evidence of the posting content and # tags are still present on the hard disk, but all evidences have removed from the memory. After going through the deletion process, neither the hard disk nor the memory contains any evidence. The deleted evidence cannot be retrieved by the recovery process.

4.2 Findings: Scenario 2: Internet Explorer

Normal browsing mode:

1) For the VMDK file, *i.e.*, the hard disk of the computer for forensics, keyword searches using WinHex can reveal the same evidences as Google Chrome. This browser could find more information regarding the post in comparison with Google Chrome. The search using the keyword "text" could not find any evidence of the comments. Similarly, searches using keywords "timestamp", "like", "tag", and "label" cannot find the evidences of the other user behaviors.

2) For the VMEM file, *i.e.*, the memory of the computer for forensics, in addition to the same evidence as in the hard disk, an additional tag of "#TRAIN" and name of the user who sent the picture or message can also be obtained. A search using the keyword "like" can reveal which user accounts liked the experimental account. A search using the keyword "text" can find the comments that are left on the experimental account and the evidence of the comments posted on the picture of the experimental account. Such evidence includes the comments, timestamps (a Unix timestamp "1469518609" represents the time "2016/07/26 15:36:49"), and the ID and name of the person who left a comment.

3) In terms of the LIVE deleted data for anti-forensics, Eraser Portable and CCleaner were used for clearing the data. After the forensic analysis, both the hard disk and memory were found to contain the remnants of Instagram account, nickname, browsing traces and URL of uploaded pictures, but the memory also retained the paths for the original and revised uploaded picture files. The picture has been deleted and its original content would not be known. Finally, Recuva Portable was used to recover the deleted data and files. The analysis results showed that the deleted evidence can no longer be retrieved.

4) After shutting down and restarting, the evidences as in 1) are still exist. The forensics of the memory showed that it contained the same remnant evidences, except that the nickname no longer exists. This is followed by a data deletion action as mentioned in 3). The forensics of the hard disk showed that the experiment account, nickname, website, and text of the uploaded pictures could still be found, but the pictures had been deleted and its original content could not be known. There is no sign of any evidence in the memory. Finally, Recuva Portable was used to restore the deleted data and files, but the results showed no traces of browsing in the hard disk and the experimental account could be no longer found in the memory.

Private browsing mode:

1) After the experiment was performed in the private browsing mode, the forensics found that both the hard disk and memory shared the information regarding the residual experimental account, nickname, website, and browsing traces of uploaded photo; but unlike the hard disk, memory also contained evidences of the experimental account ID, paths of the original and the revised uploaded photo files, content of the posting, # tags, and comment contents. The evidence of the message included the comments, timestamp of the comment, author ID associated with the message, and author's name associated with the author ID.
2) In terms of the LIVE deleted data of anti-forensic, the hard disk revealed the experimental account, nickname, and website and browsing trace of uploaded photos. The memory revealed the experiment account, nickname, paths of the original and revised uploaded photo files, and the website and browsing trace of uploaded photos. The evidences of the originally existing experimental account ID, text contents, # tags, and comments left by the other user at the experiment account or by the experiment account itself had all been deleted. After Recuva Portable was used to recover the deleted data and files, the forensic analysis showed that the deleted evidence could no longer be retrieved.
3) After shutting down and restarting, the hard disk only contained the evidence of the website and browsing traces of the uploaded photos, while the evidence in the memory has all evaporated. After the LIVE deletion process, the result is the same as before. The deleted evidence cannot be retrieved through the recovery procedure cannot retrieve the deleted evidence.

4.3 Findings: Scenario 3: Mozilla Firefox

Normal browsing mode:

1) For the hard disk, the same evidences as Google Chrome, and the added tag # PARK could be found. In addition, based on the data behind the equal sign, the evidence can determine whether you uploaded your photo or you browsed other's photo. From the viewpoint of the password of the experimental account, time of uploading photo or posting texts, content of the text, and the user behaviors such as tagging others, leaving comments, liking, and following of other's accounts could be searched by WinHex using the following keywords: "time, timestamp, tag, text, like, follower, and account number of others." These searches cannot find the presence of any evidence, and no evidence of leaving comments, liking, and following in the experiment account by any other account could be left.
2) For the memory, in addition to the same evidence that can be found on the hard disk, it also contains the extra message to click "Like" button on other users' posting. In addition, when the "L/p/Photo Encoding sequence/? Taken-by = Experiment Account" has any specific description, it means that the uploaded photo in the experiment account has been liked by itself.
3) In terms of the anti-forensic LIVE deleted data, the hard disk and memory only retained Instagram account number and nickname, but the hard disk also retains the browsing trace. The final Recuva Portable recovery action also found it impossible to retrieve the deleted evidence.
4) After shutting down and restarting, the remnant evidence on the hard disk and the memory contains Instagram account number, nickname, paths of uploaded photo files, and # tags. After cleaning with Eraser Portable and CCleaner, we found that the abovementioned evidence still existed. This shows that if the user deletes the uploaded photos on a smart phone or other devices or software, the computer still retains the photos information, but the contents of the photos are unknown. The recovery action of Recuva Portable actually made it impossible to find the nickname in the hard disk and the memory.

Private browsing mode:

1) Only the memory contains the posting content and the paths of the original and the revised picture files that were uploaded; the hard disk is totally devoid of evidence.
2) In terms of the anti-forensic LIVE deleted data, only the memory contains the text content and the paths of the original and the revised uploaded photo files; the hard disk is totally devoid of evidence. The deleted evidence cannot be retrieved through the recovery procedure.
3) After shutting down and restarting, the evidence in the memory has removed totally and hard disk itself had no evidence at all, so there is no need for the LIVE deletion and recovery procedures.

4.4 Findings: Scenario 4: Bluestacks Virtual Device

In the environment of VM virtual machine installed on virtual device using Bluestacks, we logged into the Instagram app for running various features to identify and

Table 3: The comparison of findings between 5 scenarios for normal browsing mode

	Google Chrome		Internet Explorer		Mozilla Firefox		Virtual Mobil Device	ASUS _T00P
	Hard Disk	Memory	Hard Disk	Memory	Hard Disk	Memory		
Account	O	O	O	O	O	O	O	—
Password	—	—	—	—	—	—	—	—
Nickname	O	O	O	O	O	O	—	—
Last login time	—	—	—	—	—	—	O	—
The path of the uploaded photo files	O	O	O	O	O	O	O	—
Uploading the photos and posting timestamp	—	—	—	—	—	—	—	—
Posted content	—	—	O	O	—	O	—	—
# tags	—	—	—	O	O	O	—	—
Tag other users	—	—	—	—	—	—	—	—
The URL for uploading the photos	O	O	O	O	O	O	—	—
Clicking "Like" button on other users' posting	—	O	—	—	—	O	—	—
Making comments on other users' posting	O	O	—	O	—	—	—	—
Following other user's account	—	—	—	—	—	—	—	—
Other users click "Like" button on my posting	—	—	—	O	—	—	—	—
Other users make comments on my posting	—	—	—	O	—	—	—	—
Other users following experimental account	—	—	—	—	—	—	—	—
Browsing trace	O	O	O	O	O	O	—	—

O: Found —: None

analyze the VMDK file and VMEM file of the VM virtual machine as well as to search for virtual device left by the users.

1) The "Cookies" and "Web Data" database files were found in the path `"/data/data/com.instagram.android/app\_webview/''`. Both files can be viewed using SQLite Editor, and the experimental account, the password and Android version number can be found in the "Cookies" file, whereas there is no sign of any evidence in the "Web Data" file.

2) After deleting the uploaded photos to Instagram, the computer still retains the photos content in the path "sdcard/Pictures/Instagram/." Besides, the "clean" and "journal" files were found in the path " sdcard/Android/data/com.instagram.android/cache/", neither file contains any evidence.

3) After copying Bluestacks and Instagram related files from virtual machine, these files were placed in another computerized environment for analysis. The "apps.json" file was found in the path "Bluestacks/UserData/Gadget", it contains experimental account, the password and Android version number.

We speculated that Instagram user behavioral evidence from the abovementioned analysis, most of the stored in the server, the client has little evidence.

4.5 Findings: Scenario 5: Android Smartphone

The "Cookies" and "Web Data" database files were found in the path `"/data/data/com.instagram.android/app\_webview/''`. Both files can be viewed also using SQLite Editor, and there is no sign of any evidence inside files. As we judge from the above, Instagram privacy protection, more rigorous.

4.6 Experiment Comparison

As there is a higher demand of digital forensics in normal browsing mode for investigators, we drew a table to clearly comparing the difference between them. Watch the three browsers in Table 3, the account and nickname can be found via the keyword "www.instagram.com". Although the password trace cannot be found, but found a nickname followed by a bunch of garbled, it is speculated that the most likely the password. We can find the path and URL of the uploaded photo files through the keywords "Gramblr" and "/? Taken-by=", as for the evidences of timestamp and tag other users which cannot be found. Besides, IE and Firefox can be found the evidences of posted content and adding tags more than Chrome. For any browser can be found browsing traces, but none can be found the last login time.

Except for Firefox browser, the comments could be searched on other users' posting by the keyword "text" and "/? Taken-by=". For "Like" information to click on other users' posting, Chrome can be found by the keyword

"like"; Firefox can be found through "L/P/"; IE cannot be found it. All three browsers cannot be found anyone following to other users' account. Only IE browser can be found the evidences of "Other users make comments on my posting" and "Other users click Like button on my posting", the rest cannot be found. All three browsers cannot be found anyone following message for other users following experimental account.

For Virtual Mobile Device, we can find the following three evidences, including "Account", "Last login time", "The path of the uploaded photo files", and for Android Smartphone, then none.

5 Conclusions

In this paper, we investigated the web version and the APP version of Instagram to conduct a forensic analysis of the user behaviors in Windows 10 and Android environments. The study found that different browsers, due to the differences in privacy control, can lead to the discrepancies in recording the user behaviors on the same social network. In terms of protecting user data, Mozilla Firefox provides the highest protection, followed by Google Chrome, and Internet Explorer provides the lowest protection. In addition, the forensic evidences of Instagram application are almost identical on virtual and physical smart phones. In addition to the differences in the evidence storage capacity caused by in the different framework space, the reason for the minute differences is the structural integrity of physical smart phones running in their operating environment.

While investigating cybercrime on Instagram, we recommend that the first goal should be finding the account number, nickname, and password of the criminal suspect. Using the account number and nickname, the operational behaviors of the criminal suspect on the social network can be searched, such as, uploading pictures, posting, comments, timestamps, added tags, and browsing traces. Then, based on the contents of the operation, the possible criminal activity or victimization practice can be deduced or estimated. At the same time, using the additional account numbers that are possibly discovered during the evidence gathering phase, the scope of the investigation can be expanded to find the possible accomplices or other victims. The full evidence scenario obtained in a step-by-step and layer-by-layer outward expansion will be the key to solving the case.

References

[1] N. Z. B. Z. Abidin, "Forensic analysis of third party applications: Instagram," *Forensic Focus*, Nov. 2015. (https://articles.forensicfocus.com/2015/11/06/forensic-analysis-of-third-party-application-instagram/\#respond)

[2] M. Bob, "Metcalfe's law after 40 years of ethernet," *IEEE Computer Society*, vol. 46, no. 12, pp. 26–31, 2013.

[3] D. Correa, L. A. Silva, and M. Mondal, *et al.*, "The many shades of anonymity: Characterizing anonymous social media content," in *Proceedings of the Ninth International Conference on Web and Social Media (ICWSM'15)*, pp. 71–80, 2015.

[4] Dreamgrow, "Top 15 most popular social networking sites and apps," *DreamGrow*, Jan. 2018. (https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/)

[5] eBizMBA, "Top 15 most popular social networking sites," *eBizMBA*, 2017. (http://www.ebizmba.com/articles/social-networking-websites)

[6] W. B. Glisson, T. Storer, and J. Buchanan-Wollaston, "An empirical comparison of data recovered from mobile forensic toolkits," *Digital Investigation*, vol. 10, no. 1, pp. 44–55, 2013.

[7] J. Golbeck, *Introduction to Social Media Investigation*, Netherlands: Elsevier, Amsterdam, pp. 273–278, 2015.

[8] J. Guidry, Y. Jin, and C. Orr, *et al.*, "Ebola on Instagram and Twitter: How health organizations address the health crisis in their social media engagement," *Public Relations Review*, vol. 43, no. 3, pp. 477–486, 2017.

[9] E. Martellozzo and E. A. Jane, Cybercrime and its victims," *Routledge*, 2017. (https://www.routledge.com/Cybercrime-and-its-victims/Martellozzo-Jane/p/book/9781138639447)

[10] Doris Karina Oropeza Mendoza, "The vulnerability of cyberspace-the cyber crime," *Journal of Forensic Sciences & Criminal Investigation*, vol. 2, no. 1, pp. 273–278, Feb. 2017.

[11] C. Ntantogian, D. Apostolopoulos, and G. Marinakis, *et al.*, "Evaluating the privacy of Android mobile applications under forensic analysis," *Computers & Security*, vol. 42, pp. 66–76, 2014.

[12] M. Pittman and B. Reich, "Social media and loneliness: Why an Instagram picture may be worth more than a thousand Twitter words," *Computers in Human Behavior*, vol. 62, pp. 155–167, 2016.

[13] D. Quick and K. K. Choo, "Pervasive social networking forensics: Intelligence and evidence from mobile device extracts," *Journal of Network and Computer Applications*, vol. 86, pp. 24–33, May 2017.

[14] D. R. Rodríguez, R. D. Redondo, and A. F. Vilas, *et al.*, "Sensing the city with Instagram: Clustering geolocated data for outlier detection," *Expert Systems with Applications*, vol. 78, pp. 319–333, 2017.

[15] P. Shakarian, A. Bhatnagar, and A. Aleali, *et al.*, "Diffusion in social networks," *Computer Science*, 2015. (https://www.springer.com/gb/book/9783319231044)

[16] Statista, *Number of monthly active Instagram users from January 2013 to September 2017*, Sep. 2017. (http://mediakix.com/wp-content/uploads/2017/03/How-Many-People-Use-Instagram.pdf)

[17] J. R. Sun, M. L. Shih, and M. S. Hwang, "A survey of digital evidences forensic and cybercrime investigation procedure," *International Journal Network Security*, vol. 17, no. 5, pp. 497–509, 2015.

[18] N. Virvilis, A. Mylonas, and N. Tsalis, *et al.*, "Security busters: Web browser security vs. Rogue sites," *Computers & Security*, vol. 52, pp. 90–105, 2015.

[19] Wikipedia, *Instagram*, Feb. 2018. (`https://en.wikipedia.org/wiki/Instagram`)

[20] S. Y. Wu, Y. Zhang, and X. Wang, *et al.*, "Forensic analysis of WeChat on Android smartphones," *Digital Investigation*, vol. 21, pp. 3–10, Jun. 2017.

[21] M. N. Yusoff, A. Dehghantanha, and R. Mahmod, "Chapter 4 – Forensic investigation of social media and instant messaging services in Firefox OS: Facebook, Twitter, Google+, Telegram, OpenWapp, and Line as case studies," in *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*, pp. 41–62, 2017.

Biography

Ming Sang Chang received the Ph.D. degree from National Chiao Tung University, Taiwan, in 1999. In 2001 he joined the faculty of the Department of Information Management, Central Police University, where he is now a Professor. His research interest includes Computer Networking, Network Security, Digital Investigation, and Social Networks.

Chih Ping Yen is an Associate Professor, Department of Information Management, Central Police University. Received his Ph.D. degree from Department of Computer Science and Information Engineering, National Central University, Taiwan, in 2014. His research interest includes Digital Investigation, Artificial Intelligence & Pattern Recognition, Image Processing, and Management Information Systems.