Evidence Gathering of Instagram on Windows 10

Ming Sang Chang

Department of Information Management, Central Police University, Taoyuan City, 33304, Taiwan (R.O.C.)

Abstract

Social networking has changed the way people communicate with each other. There are many social networks such as Instagram, Facebook, LinkedIn, and Twitter. Instagram activities have grown in popularity along with its social networking site. Its extensive use in everyday that means it can also be used to commit crime such as cyber stalking, cyber bullying, hacking, and copyright infringement. In order to identify crimes, it is essentially required to retrieve these traces and evidences by using appropriate forensic technique. This paper studies the artifacts left by Instagram application on Windows 10 platform and presents evidence gathering of Instagram application. It proves beneficial for forensic analysts and practitioners as it assists them in course of mapping and locating digital evidences of Instagram on Windows 10 PC.

Keywords: *Social Networking, Instagram, Investigation, Digital Forensics.*

1. Introduction

Over the past years, social networks have become the largest and fastest growing websites on the Internet. There are many social networks such as Instagram, Facebook, LinkedIn, and Twitter [1]. A social networking service is an online platform that is used by people to build social networks with other people. Social networking sites allow users to share ideas, photos and videos, posts, activities, and events in their network. They contain sensitive and personal data of hundreds of millions of people. Many researches have acknowledged the importance of these websites. We also can find a number of publications have focused on security issues that are associated with social networks. They highlight challenges to security and privacy of social network users and their data [2-4].

Instagram is an online social networking service that enables its users to take pictures and videos, and share them either publicly or privately. Instagram launched in October 2010. The service rapidly gained popularity, with over 100 million active users as of April 2012 [5-6] and over 500 million as of June 2016 [7]. In 2015, there were approximately more than 77.6 million active Instagram users in the United States. Instagram is most popular with teens and young Millennials. In the United States where more than half of Instagram’s user base is between 18 and 29 years old. Instagram is the preferred social network of teens in the United States, beating out Twitter and Facebook.

Instagram users can upload photographs and short videos, follow other users' feeds and geotag images with longitude and latitude coordinates, or the name of a location. Users can connect their Instagram account to other social networking sites, enabling them to share uploaded photos to those sites [8]. As of June 2013, users can connect their Instagram accounts to Facebook, Twitter, Tumblr, and Flickr. In 2016, Instagram announced new tools for business accounts, including new business profiles, analytics and the ability to turn Instagram posts into ads directly from the Instagram app itself [9]. As the use of Instagram is increasing, it is important to take measures in advance from forensic standpoint forecasting the potential use of it in cybercrimes such as hacking, copyright infringement, cyber stalking, and cyber bullying. To solve social networking cybercrimes, investigator need to perform forensic analysis of suspect device to find digital evidences.

User devices and social networking applications may hold the data that can provide evidence of the activities carried out through them. The use environment of the social networking applications can provide evidences. These evidences can be used to profile the behavior of its user and may even allow the investigator to anticipate the users’ actions [10-12]. Each device and application has its own acquisition requirements and potential sets of evidence. Many of the activities are logged on the hard disk and memory of the device from which access is made. The remnants may reveal details about private connections and the user activities. Due to increased usage of Windows OS on desktop investigating Windows behavior has become imperative for forensic investigators. In this work, we study and report the forensic analysis of Instagram on windows 10 operating system.

Our research is to try various tools on searching and extracting footprints from the memory and other locations such as volatile memory, browser cache file, and virtual machine snapshot files. If we can determine activities conducted through these applications were stored on, the amount, significance, and locations of data that could be found and retrieved from the logical image of each device were determined. In this paper, we attempt to identify footprints for the Instagram activities. We conduct research into the data remnants of a user using Instagram in a variety of ways on a Windows 10 operating system. We use Gramblr and two different browsers to access Instagram. The browsers are Google Chrome and Internet Explorer.

The rest of the paper is organized as follows: In section 2 introduces the related works. In section 3, we outline the research methodology. In section 4, results and analysis are described. In section 5, we discuss our research findings. Finally, section 6 is a conclusion.

2. Related Works

The evidences were stored on three principle areas by using social network. They are hard drive, memory, and network. Some social network services have the ability to log information on the user’s hard drive [13]. To use a social network, an account must be established to create a screen name provided with user information. Evidences can be found in various internet file caches used by Internet Explorer for volatile instant messaging and each cache holds different pieces of data. Apart from the normal files, files left by social networking application on a hard disk drive can be in temp file format and will generally be deleted could be very difficult to retrieve once the machine is power down. An operating system generally stores information of all the installed and uninstalled applications in the system. The uninstalled application also leaves evidence. If a user has deleted an instant messenger application, there is a chance that a record can be found in the registry to prove that the instant messenger has once installed onto the system. Information is also stored within the memory. Since every application requires memory to execute, it is logical to think that there evidence could be left behind in the system’s memory. The analysis on live memory has allows us to extend the possibility in providing additional contextual information for any cases. For any Windows based operating system, it is important evidence can usually be found beneath the physical memory, hibernation file and pagefile [14].

Artifacts of social networking have been of interest in many different digital forensic studies. Early work focused on artifacts left behind by many instant messaging applications, such as MSN Messenger [15], Yahoo Messenger [16], and AOL Instant Messenger [17]. In 2013 Mahajan et al., [18] performed forensic analysis of Whatsapp and Viber on five android phones using UFED and manual analysis. Cosimo Anglano [19] carried out Whatsapp forensics on Android in 2014 using YouWave virtualization platform. Iqbal et al. [20] studied the artifacts left by the ChatON IM application. The analysis was conducted on an iPhone running iOS6 and a Samsung Galaxy Note running Android 4.1. Said et al. [21] investigated Facebook and other IM applications, it was determined that only BlackBerry Bold 9700 and iPhone 3G/3GS provided evidence of Facebook unencrypted. Wong et al. [22] and Al Mutawa et al. [23] demonstrated that artifacts of the Facebook web-application could be recovered from memory dumps and web browsing cache. Sgaras et al. [24] analyzed Skype and several other VoIP applications for iOS and Android platforms. It was concluded that the Android apps store far less artifacts than of the iOS apps. Azfar A. et al. [25] adapt a widely used adversary model from the cryptographic literature to formally capture a forensic investigator's capabilities during the collection and analysis of evidentiary materials from mobile devices. Walnycky et al. [26] added that artifacts of the Facebook Messenger could vary depending on user settings, OS version, and manufacturer. Levendoski et al. [27] concluded that artifacts of the Yahoo Messenger client produced a different directory structure on Windows Vista and 7. Chu et al. [28] focused on live data acquisition from personal computer and was able to identify distinct strings that will assist forensic practitioners with reconstruction of the previous Facebook sessions. Parsons [29] concludes that over half of the core artifacts have changed from Windows 8.1 to Windows 10.

3. Methodology

The main purpose of our study is to determine whether activities performed through personal computer installed windows 10 are stored on the internal memory and disk of these devices and whether these data can be recovered. We can use these high evidentiary value data to assist in the investigation of criminal, civil, or other types of cases. The goal of this study was achieved by conducting experiments on a number of virtual machines installed by windows 10. Manual forensic examinations and analyses were performed on a social networking which is Instagram. It is often useful to corroborate evidence from different sources. It may confirm evidence from Instagram provider or from the personal computer. In a real investigation, it is difficult to confirm evidence from the social networking providers. We conduct research into the data remnants of a user using Instagram in a variety of ways.

It may be critical to know whether particular social networking activities took place on a particular PC for the investigation of criminal. We conduct many experiments to extract evidences from PC. The experiments were conducted using forensically approaches and under forensically acceptable conditions. They are to preserve the integrity of the original data and to prevent it from any contamination that would interfere with their acceptance in court. The test and examination procedure was derived from the Computer Forensics Tool Testing program guidelines established by the National Institute of Standards and Technology. It can ensure the quality of the testing methods and the reliability and validity of the results.

This process is applied to the use of Instagram. A variety of virtual machines were created. It was decided to examine a variety of circumstances of a user using Instagram, and also to examine any differences when using different browsers. Multiple scenarios were explored. Each scenario made use of Instagram with a different browser. They are Google Chrome (GC) V51.0.2704 and Internet Explorer (IE) V11.0.10586. This research focuses on what data remnants on Windows 10 PC after a user log in, uploading photographs, post message, tagging, and doing comments and likes of the use of Instagram. We want to find username, password, photographs, messages, etc. In addition, we also create circumstances to simulate a user running Eraser Portable V5.8.8.1 and CCleaner V5.19.5633 to remove evidences. There are many virtual machines which replicate different circumstance of activities to gather the data in relation to the use of Instagram on Windows 10. We make multiple scenarios to explore the use of Instagram. The virtual machines were created for each different circumstance of Instagram activities. This represents different physical computer systems available for analysis, with different circumstances and data remnants available for analysis on each VM. The virtual machines reduce the costs of the study, since neither many real personal computers are necessary to carry out the experiments.

Our experimental test-bed consists of a set of virtual machines. That is VMware Workstation V12.0.0. For each experiment, Windows 10 was installed on every virtual machine. Gramblr application V2.7.3 was installed on Windows 10 to upload pictures or videos on Instagram. In each experiment, we assign a role to each virtual device. We use it to carry out the corresponding activities. At the end of the experiment, we suspend the virtual device. We parse the file implementing the corresponding internal memory and hard drive by means of WinHex 18.9, SQLite V3.9.0.

According to the activities of Instagram, we create four experiment systems. Each experiment includes the activities of login, uploading photographs, posting message, tagging, liking, following, comments, and label photographs. They include two different browser named Internet Explorer and Google Chrome.

The different actions undertaken are as follows. We divide them in ten cases.

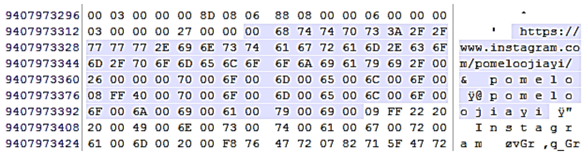
1. The first step was to install Gramblr application, Internet Explorer (IE), and Google Chrome (GC) into different base virtual machine with Windows 10.
2. The second step was to make two copies of the base virtual PC with IE and GC for each scenario. An account of Instagram was created for these experiments. We log in Instagram on two different virtual PCs. We do nothing and log out. Then we use SQLite Database Browser, WinHex to find the data remnants of the account and password.
3. The third step was to make two copies of the base virtual PC with IE and GC for each scenario. There are two scenarios for posting text. After posting text we sign out and find the data remnants on Virtual PC.
4. The forth step was to make two copies of the base virtual PC with IE and GC for each scenario. There are two scenarios for uploading comments. After uploading comments we sign out and find the data remnants on Virtual PC.
5. The fifth step was to make two copies of the base virtual PC with IE and GC for each scenario. There are two scenarios for uploading photographs. After uploading photographs we sign out and find the data remnants on Virtual PC.
6. The sixth step was to make two copies of the base virtual PC with IE and GC for each scenario. There are two scenarios for tagging. After tagging we sign out and find the data remnants on Virtual PC.
7. The seventh step was to make two copies of the base virtual PC with IE and GC for each scenario. There are two scenarios for liking. After liking we sign out and find the data remnants on Virtual PC.
8. The eighth step was to make two copies of the base virtual PC with IE and GC for each scenario. There are two scenarios for labeling. After labeling we sign out and find the data remnants on Virtual PC.
9. The ninth step was to make two copies of the base virtual PC with IE and GC for each scenario. There are two scenarios for following. After following we sign out and find the data remnants on Virtual PC.
10. The tenth step was to make two copies of all above actions of virtual PC with IE and GC for each scenario. There are two scenarios for erasing and deleting. After erasing and deleting we find the data remnants on Virtual PC.

4. Result and Analysis

In this section we will describe the findings of the use of Instagram.

4.1 Google Chrome Environments

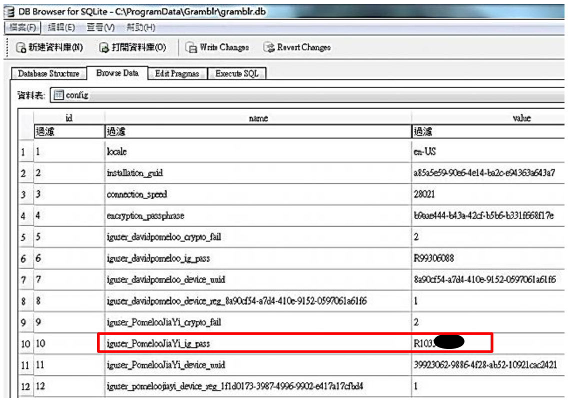
(1) Hard Drive: We use the keyword, www.instagram.com/, to find the remnants of user account and password. The account (pomeloojiayi) and nickname (pomelo) could be found as Figure 1.



```
9407973296 00 03 00 00 00 8D 08 06  88 08 00 00 06 00 00 00         ˆ
9407973312 03 00 00 00 27 00 00 00  68 74 74 70 73 3A 2F 2F     '   https://
9407973328 77 77 77 2E 69 6E 73 74  61 67 72 61 6D 2E 63 6F www.instagram.co
9407973344 6D 2F 70 6F 6D 65 6C 6F  6F 6A 69 61 79 69 2F 00 m/pomeloojiayi/
9407973360 26 00 00 00 70 00 6F 00  6D 00 65 00 6C 00 6F 00 &   p o m e l o
9407973376 08 FF 40 00 70 00 6F 00  6D 00 65 00 6C 00 6F 00  ÿ@ p o m e l o
9407973392 6F 00 6A 00 69 00 61 00  79 00 69 00 09 FF 22 20 o j i a y i  ÿ"
9407973408 20 00 49 00 6E 00 73 00  74 00 61 00 67 00 72 00   I n s t a g r
9407973424 61 00 6D 00 20 00 F8 76  47 72 07 82 71 5F 47 72 a m   øvGr ‚q_Gr
```

Figure 1 The remnants of account with GC

We use the keyword, gramblr.db, to find the remnants of locations of Gramblr application. The Gramblr database file was located on C\Program Data\Gramblr\gramblr.db. The account and password are found on config table of gramblr.db as Figure 2.



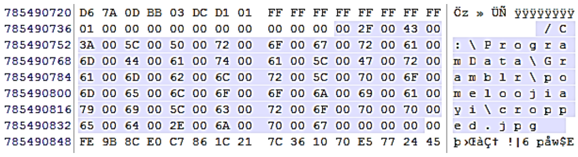
DB Browser for SQLite - C:\ProgramData\Gramblr\gramblr.db

資料表: config

	id	name	value
	過濾	過濾	過濾
1	1	locale	en-US
2	2	installation_guid	a85a5e59-90e6-4e14-ba2c-e94363a643a7
3	3	connection_speed	28021
4	4	encryption_passphrase	b9aae444-b43a-42cf-b5b6-b331f668f17e
5	5	iguser_davidpomeloo_crypto_fail	2
6	6	iguser_davidpomeloo_ig_pass	R99306088
7	7	iguser_davidpomeloo_device_uuid	8a90cf54-a7d4-410e-9152-0597061a61f6
8	8	iguser_davidpomeloo_device_reg_8a90cf54-a7d4-410e-9152-0597061a61f6	1
9	9	iguser_PomelooJiaYi_crypto_fail	2
10	10	iguser_PomelooJiaYi_ig_pass	R103[redacted]
11	11	iguser_PomelooJiaYi_device_uuid	39923062-9886-4f28-ab52-10921cac2421
12	12	iguser_pomeloojiayi_device_reg_1f1d0173-3987-4996-9902-e417a17cfbd4	1

Figure 2 The remnants of gramblr.db

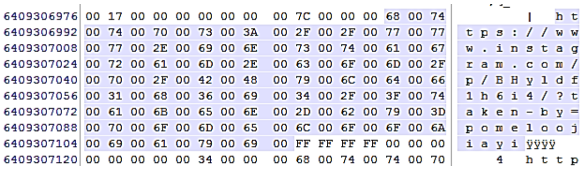
We use the keyword, gramblr, to find the remnants of photographs on C\Program Data\Gramblr\pomeloojiayi as Figure 3.



```
785490720 D6 7A 0D BB 03 DC D1 01  FF FF FF FF FF FF FF FF Öz » ÜÑ ÿÿÿÿÿÿÿÿ
785490736 01 00 00 00 00 00 00 00  00 00 00 00 2F 00 43 00              / C
785490752 3A 00 5C 00 50 00 72 00  6F 00 67 00 72 00 61 00 : \ P r o g r a
785490768 6D 00 44 00 61 00 74 00  61 00 5C 00 47 00 72 00 m D a t a \ G r
785490784 61 00 6D 00 62 00 6C 00  72 00 5C 00 70 00 6F 00 a m b l r \ p o
785490800 6D 00 65 00 6C 00 6F 00  6F 00 6A 00 69 00 61 00 m e l o o j i a
785490816 79 00 69 00 5C 00 63 00  72 00 6F 00 70 00 70 00 y i \ c r o p p
785490832 65 00 64 00 2E 00 6A 00  70 00 67 00 00 00 00 00 e d . j p g
785490848 FE 9B 8C E0 C7 86 1C 21  7C 36 10 70 E5 77 24 45 þ›ŒàÇ† !|6 påw$E
```

Figure 3 The remnants of location of photographs

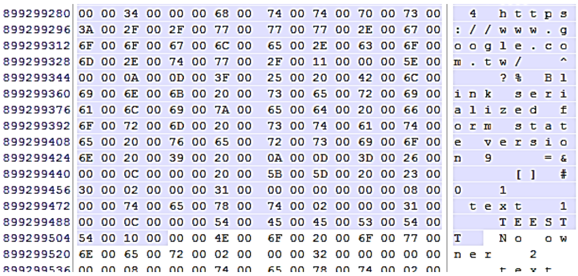
The photograph can be found by the keyword "/？taken-by=" as Figure 4.



```
6409306976 00 17 00 00 00 00 00 00  00 7C 00 00 00 68 00 74          |   h t
6409306992 00 74 00 70 00 73 00 3A  00 2F 00 2F 00 77 00 77  t p s : / / w w
6409307008 00 77 00 2E 00 69 00 6E  00 73 00 74 00 61 00 67  w . i n s t a g
6409307024 00 72 00 61 00 6D 00 2E  00 63 00 6F 00 6D 00 2F  r a m . c o m /
6409307040 00 70 00 2F 00 42 00 48  00 79 00 6C 00 64 00 66  p / B H y l d f
6409307056 00 31 00 68 00 36 00 69  00 34 00 2F 00 3F 00 74  1 h 6 i 4 / ? t
6409307072 00 61 00 6B 00 65 00 6E  00 2D 00 62 00 79 00 3D  a k e n - b y =
6409307088 00 70 00 6F 00 6D 00 65  00 6C 00 6F 00 6F 00 6A  p o m e l o o j
6409307104 00 69 00 61 00 79 00 69  00 FF FF FF FF 00 00 00  i a y i ÿÿÿÿ
6409307120 00 00 00 00 00 34 00 00  00 68 00 74 00 74 00 70      4   h t t p
```

Figure 4 The remnants of URL of photographs

We use the keyword, text, to find the remnants of posting text (TEESTT) as Figure 5.

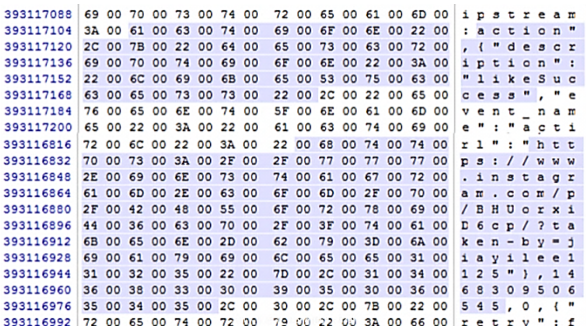


```
899299280 00 00 34 00 00 00 68 00  74 00 74 00 70 00 73 00   4   h t t p s
899299296 3A 00 2F 00 2F 00 77 00  77 00 77 00 2E 00 67 00 : / / w w w . g
899299312 6F 00 6F 00 67 00 6C 00  65 00 2E 00 63 00 6F 00 o o g l e . c o
899299328 6D 00 2E 00 74 00 77 00  2F 00 11 00 00 00 5E 00 m . t w /       ^
899299344 00 00 0A 00 0D 00 3F 00  25 00 20 00 42 00 6C 00       ? %   B l
899299360 69 00 6E 00 6B 00 20 00  73 00 65 00 72 00 69 00 i n k   s e r i
899299376 61 00 6C 00 69 00 7A 00  65 00 64 00 20 00 66 00 a l i z e d   f
899299392 6F 00 72 00 6D 00 20 00  73 00 74 00 61 00 74 00 o r m   s t a t
899299408 65 00 20 00 76 00 65 00  72 00 73 00 69 00 6F 00 e   v e r s i o
899299424 6E 00 20 00 39 00 20 00  0A 00 0D 00 3D 00 26 00 n   9       = &
899299440 00 00 0C 00 00 00 20 00  5B 00 5D 00 20 00 23 00         [ ]   #
899299456 30 00 02 00 00 00 31 00  00 00 00 00 00 00 08 00 0     1
899299472 00 00 74 00 65 00 78 00  74 00 02 00 00 00 31 00   t e x t     1
899299488 00 00 0C 00 00 00 54 00  45 00 45 00 53 00 54 00       T E E S T
899299504 54 00 10 00 00 00 4E 00  6F 00 20 00 6F 00 77 00 T     N o   o w
899299520 6E 00 65 00 72 00 02 00  00 00 32 00 00 00 00 00 n e r     2
899299536 00 00 08 00 00 00 74 00  65 00 78 00 74 00 02 00       t e x t
```

Figure 5 The remnants of URL of posting text

We also use different keywords such as time, time stamp, tag, follower, like, label, etc. to find the remnants. The remnants could not be found with such keywords.

(2) Memory: The remnants of memory are almost like hard drive. In memory, the URL of photographs can't be found. But the account can be found with *like* keyword as Figure 6.



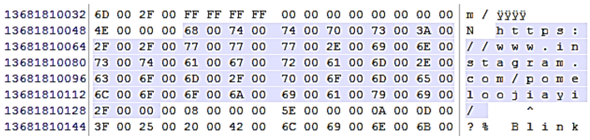
```
393117088 69 00 70 00 73 00 74 00  72 00 65 00 61 00 6D 00 i p s t r e a m
393117104 3A 00 61 00 63 00 74 00  69 00 6F 00 6E 00 22 00 : a c t i o n "
393117120 2C 00 7B 00 22 00 64 00  65 00 73 00 63 00 72 00 , { " d e s c r
393117136 69 00 70 00 74 00 69 00  6F 00 6E 00 22 00 3A 00 i p t i o n " :
393117152 22 00 6C 00 69 00 6B 00  65 00 53 00 75 00 63 00 " l i k e S u c
393117168 63 00 65 00 73 00 73 00  22 00 2C 00 22 00 65 00 c e s s " , " e
393117184 76 00 65 00 6E 00 74 00  5F 00 6E 00 61 00 6D 00 v e n t _ n a m
393117200 65 00 22 00 3A 00 22 00  61 00 63 00 74 00 69 00 e " : " a c t i
393116816 72 00 6C 00 22 00 3A 00  22 00 68 00 74 00 74 00 r l " : " h t t
393116832 70 00 73 00 3A 00 2F 00  2F 00 77 00 77 00 77 00 p s : / / w w w
393116848 2E 00 69 00 6E 00 73 00  74 00 61 00 67 00 72 00 . i n s t a g r
393116864 61 00 6D 00 2E 00 63 00  6F 00 6D 00 2F 00 70 00 a m . c o m / p
393116880 2F 00 42 00 48 00 55 00  6F 00 72 00 78 00 69 00 / B H U o r x i
393116896 44 00 36 00 63 00 70 00  2F 00 3F 00 74 00 61 00 D 6 c p / ? t a
393116912 6B 00 65 00 6E 00 2D 00  62 00 79 00 3D 00 6A 00 k e n - b y = j
393116928 69 00 61 00 79 00 69 00  6C 00 65 00 65 00 31 00 i a y i l e e 1
393116944 31 00 32 00 35 00 22 00  7D 00 2C 00 31 00 34 00 1 2 5 " } , 1 4
393116960 36 00 38 00 33 00 30 00  39 00 35 00 30 00 36 00 6 8 3 0 9 5 0 6
393116976 35 00 34 00 35 00 2C 00  30 00 2C 00 7B 00 22 00 5 4 5 , 0 , { "
393116992 72 00 65 00 74 00 72 00  79 00 22 00 3A 00 66 00 r e t r y " : f
```

Figure 6 The remnants in memory with *like* keyword

4.2 Google Chrome with Eraser and CCleaner

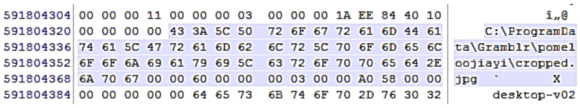
We restart the virtual machine and log in Instagram. The uploading photographs, posting text, and other actions are deleted. The data of Gramblr application are deleted with Eraser Portable. Then Gramblr application was removed from Windows 10. We run CCleaner to delete browser data remnants such as password, cookies, cache, history, etc. We also delete the history of the Windows Explorer such as most recently used files list, image cache, Recycle

Bin, Scrapbook, etc. The same keywords as section 4.1 are used to find the remnants. The remnants are found with *www.instagram.com* keyword as Figure 7 and with *gramblr* keyword as Figure 8.



```
13681810032 6D 00 2F 00 FF FF FF FF  00 00 00 00 00 00 00 00  m / ÿÿÿÿ
13681810048 4E 00 00 00 68 00 74 00  74 00 70 00 73 00 3A 00  N   h t t p s :
13681810064 2F 00 2F 00 77 00 77 00  77 00 2E 00 69 00 6E 00  / / w w w . i n
13681810080 73 00 74 00 61 00 67 00  72 00 61 00 6D 00 2E 00  s t a g r a m .
13681810096 63 00 6F 00 6D 00 2F 00  70 00 6F 00 6D 00 65 00  c o m / p o m e
13681810112 6C 00 6F 00 6F 00 6A 00  69 00 61 00 79 00 69 00  l o o j i a y i
13681810128 2F 00 00 00 08 00 00 00  5E 00 00 00 0A 00 0D 00  /       ^
13681810144 3F 00 25 00 20 00 42 00  6C 00 69 00 6E 00 6B 00  ? %   B l i n k
```

Figure 7 The remnants of account after deleting

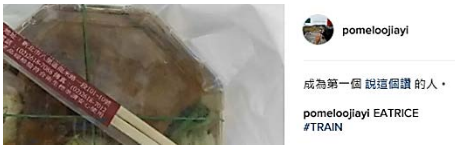


```
591804304 00 00 00 11 00 00 00 03  00 00 00 1A EE 84 40 10              î„@
591804320 00 00 00 00 43 3A 5C 50  72 6F 67 72 61 6D 44 61      C:\ProgramDa
591804336 74 61 5C 47 72 61 6D 62  6C 72 5C 70 6F 6D 65 6C  ta\Gramblr\pomel
591804352 6F 6F 6A 69 61 79 69 5C  63 72 6F 70 70 65 64 2E  oojiayi\cropped.
591804368 6A 70 67 00 00 60 00 00  00 03 00 00 A0 58 00 00  jpg  `        X
591804384 00 00 00 00 00 64 65 73  6B 74 6F 70 2D 76 30 32       desktop-v02
```

Figure 8 The remnants of location of photograph after deleting

4.3 Internet Explorer Environments

(1) Hard Drive: We use the keyword as section 4.1 to find remnants. The data remnants can be found as section 4.1. In addition, the content of label can be found as Figure 9 and 10.

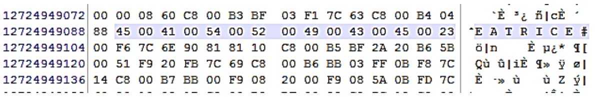


pomeloojiayi

成為第一個 說這個讚 的人。

pomeloojiayi EATRICE
#TRAIN

Figure 9 The remnants of label

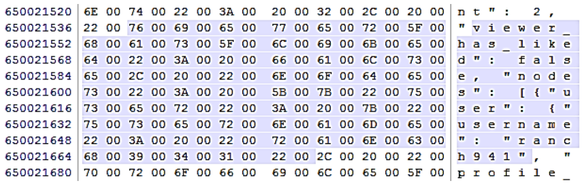


```
12724949072 00 00 08 60 C8 00 B3 BF  03 F1 7C 63 C8 00 B4 04    `È ³¿ ñ|cÈ ´
12724949088 88 45 00 41 00 54 00 52  00 49 00 43 00 45 00 23  ˆE A T R I C E #
12724949104 00 F6 7C 6E 90 81 81 10  C8 00 B5 BF 2A 20 B6 5B   ö|n    È µ¿* ¶[
12724949120 00 51 F9 20 FB 7C 69 C8  00 B6 BB 03 FF 0B F8 7C   Qù û|iÈ ¶» ÿ ø|
12724949136 14 C8 00 B7 BB 00 F9 08  20 00 F9 08 5A 0B FD 7C   È ·» ù   ù Z ý|
```

Figure 10 The remnants of label

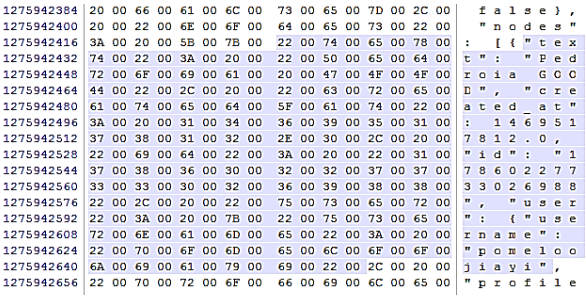
We also use different keywords such as time, time stamp, tag, follower, like, label, etc. to find the remnants. The remnants could not be found with such keywords.

(2) Memory: The remnants of hard drive can almost be found in memory with exception of URL of uploading photograph. The remnant of label (#TRAIN) can be found with *pomeloojiayi* key word. Which accounts do the *like* actions can be found with the keyword *like* as Figure 11.
The posting text and time stamp can be found with keyword *text* as Figure 12.



```
650021520 6E 00 74 00 22 00 3A 00  20 00 32 00 2C 00 20 00  n t " :   2 ,
650021536 22 00 76 00 69 00 65 00  77 00 65 00 72 00 5F 00  " v i e w e r _
650021552 68 00 61 00 73 00 5F 00  6C 00 69 00 6B 00 65 00  h a s _ l i k e
650021568 64 00 22 00 3A 00 20 00  66 00 61 00 6C 00 73 00  d " :   f a l s
650021584 65 00 2C 00 20 00 22 00  6E 00 6F 00 64 00 65 00  e ,   " n o d e
650021600 73 00 22 00 3A 00 20 00  5B 00 7B 00 22 00 75 00  s " :   [ { " u
650021616 73 00 65 00 72 00 22 00  3A 00 20 00 7B 00 22 00  s e r " :   { "
650021632 75 00 73 00 65 00 72 00  6E 00 61 00 6D 00 65 00  u s e r n a m e
650021648 22 00 3A 00 20 00 22 00  72 00 61 00 6E 00 63 00  " :   " r a n c
650021664 68 00 39 00 34 00 31 00  22 00 2C 00 20 00 22 00  h 9 4 1 " ,   "
650021680 70 00 72 00 6F 00 66 00  69 00 6C 00 65 00 5F 00  p r o f i l e _
```

Figure 11 The remnants of accounts do the *like* action



```
1275942384 20 00 66 00 61 00 6C 00  73 00 65 00 7D 00 2C 00    f a l s e } ,
1275942400 20 00 22 00 6E 00 6F 00  64 00 65 00 73 00 22 00    " n o d e s "
1275942416 3A 00 20 00 5B 00 7B 00  22 00 74 00 65 00 78 00  :   [ { " t e x
1275942432 74 00 22 00 3A 00 20 00  22 00 50 00 65 00 64 00  t " :   " P e d
1275942448 72 00 6F 00 69 00 61 00  20 00 47 00 4F 00 4F 00  r o i a   G O O
1275942464 44 00 22 00 2C 00 20 00  22 00 63 00 72 00 65 00  D " ,   " c r e
1275942480 61 00 74 00 65 00 64 00  5F 00 61 00 74 00 22 00  a t e d _ a t "
1275942496 3A 00 20 00 31 00 34 00  36 00 39 00 35 00 31 00  :   1 4 6 9 5 1
1275942512 37 00 38 00 31 00 32 00  2E 00 30 00 2C 00 20 00  7 8 1 2 . 0 ,
1275942528 22 00 69 00 64 00 22 00  3A 00 20 00 22 00 31 00  " i d " :   " 1
1275942544 37 00 38 00 36 00 30 00  32 00 32 00 37 00 37 00  7 8 6 0 2 2 7 7
1275942560 33 00 33 00 30 00 32 00  36 00 39 00 38 00 38 00  3 3 0 2 6 9 8 8
1275942576 22 00 2C 00 20 00 22 00  75 00 73 00 65 00 72 00  " ,   " u s e r
1275942592 22 00 3A 00 20 00 7B 00  22 00 75 00 73 00 65 00  " :   { " u s e
1275942608 72 00 6E 00 61 00 6D 00  65 00 22 00 3A 00 20 00  r n a m e " :
1275942624 22 00 70 00 6F 00 6D 00  65 00 6C 00 6F 00 6F 00  " p o m e l o o
1275942640 6A 00 69 00 61 00 79 00  69 00 22 00 2C 00 20 00  j i a y i " ,
1275942656 22 00 70 00 72 00 6F 00  66 00 69 00 6C 00 65 00  " p r o f i l e
```

Figure 12 The remnants with *text* keyword

4.4 Internet Explorer with Eraser and CCleaner

We restart the virtual machine and log in Instagram. The uploading photographs, posting text, and other actions are deleted. The data of Gramblr application are deleted with Eraser Portable. Then Gramblr application was removed from Windows 10. We run CCleaner to delete browser data remnants such as password, cookies, cache, history, etc. We also delete the history of the Windows Explorer such as most recently used files list, image cache, Recycle Bin, Scrapbook, etc. The same keywords as section 4.1 are used to find the remnants. The account and nickname are found with *www.instagram.com* keyword. The location of uploading photograph can be found with *gramblr* keyword but the file can't be found.

5. Discussions

In this research, we identified artifacts for Instagram application. We focus on both the volatile memory and hard drive artifacts. Our experiments showed that the Instagram application on volatile memory has proved that critical application data is present in the RAM and it can be extracted for further analysis. Our hard drive analysis has shown that Instagram application activities remain some artifacts in different locations. This indicated that when a user has used the Instagram apps, there will be records remaining in the application folder.

Our examinations of the physical memory captures indicated that the memory dumps can recover the application caches in plain text. We performed all our research inside a virtual machine which gave us an advantage to download or run executable files without having to worry about any executable affecting the host machine. Other than that all our forensic data was not leaked to the outside world and a separate environment was provided to hold all our files in one place.

The summary of findings is shown as Table1.

Table 1 The summary of research findings

Category Actions	Google Chrome		Internet Explorer	
	Hard Drive	Memory	Hard Drive	Memory
Password	X	X	X	X
Account	V	V	V	V
Nickname	V	V	V	V
Location of uploading photograph	V	V	V	V
Posting text	X	X	V	V
#Label	X	X	X	V
Tag	X	X	X	X
URL of uploading photograph	V	X	V	X
comments	V	V	X	V
Like	X	V	X	X

V：found X：None

6. Conclusions

Social network is increasingly popular among individuals and business organizations. With the tremendous use of such applications, it may be used to commit crimes. It is important to identify the forensic artifacts left by these application. In this paper we have presented the findings from our forensic examination of Instagram application with Windows 10. The results indicated that use of the Instagram with Windows 10 leave useful evidential material on the hard drive and memory dumps. The implementation may vary between different end devices. Possible work can be done to identify its artifacts that are left on other devices. The research findings prove beneficial for forensic analysts and practitioners as it assists them in course of mapping and locating digital evidences of Instagram on Windows 10 PC.

References

[1] Top 15 Most Popular Social Networking Sites http://www.ebizmba.com/articles/social-networking-websites

[2] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Zhao. Detecting and characterizing social spam campaigns. In Proceedings of the 10th annual conference on Internet measurement, pages 35–47. ACM, 2010.

[3] M. Huber, M. Mulazzani, E. Weippl, G. Kitzler, and S. Goluch. Friend-in-the-middle attacks: Exploiting social networking sites for spam. Internet Computing, 2011.

[4] Markus Huber, et al. Social Snapshots: Digital Forensics for Online Social Networks. Proceedings of the 27th Annual Computer Security Applications Conference. 2011, pp113-122.

[5] "Press Center • Instagram". https://www.instagram.com/press/.

[6] DesMarais, Christina "Facebook's Instagram says it has 90 million monthly active users". PC World, 2013.

[7] Number of monthly active Instagram users from January 2013 to June 2016 https://www.statista.com/statistics/253577/number-of-monthly-active-instagram-users/

[8] Buck, Stephanie. "The Beginner's Guide to Instagram – Yahoo! News", 2012, News.yahoo.com.

[9] Sarah Perez. "Instagram officially announces its new business tools". The Guardian UK, 2016.

[10] Orebaugh, A., Allnutt, J. Data Mining Instant Messaging Communications to Perform Author Identification for Cybercrime Investigations, In Book: Digital Forensics and Cyber Crime, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010; pp. 99-110

[11] Iqbal, Asif, Al Obaidli, H., Marrington, A., & Jones, A. Windows Surface RT tablet forensics. Digital Investigation 2014; 11, S87-S93.

[12] The United Nations Office on Drugs and Crime, "Comprehensive study on Cybercrime," Technical Report. United Nations; 2013. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [last accessed 06.08.2016]

[13] Alberto R. Gonzales, Regina B. Schofield, David W. Hagy. Investigations Involving the Internet and Computer Networks. Washington, DC: National Institute of Justice, 2007. https://www.ncjrs.gov/pdffiles1/nij/210798.pdf [last accessed 05.07.16].

[14] Gao, Y., & Cao, T. Memory forensics for QQ from a live system. Journal of computers 2010; 5(4):541-548.

[15] Dickson M. An examination into MSN Messenger 7.5 contact identification. Digital Investigation. 2006; 3(2):79–83.

[16] Dickson M. An examination into Yahoo Messenger 7.0 contact identification. Digital Investigation. 2006; 3(3):159–165

[17] Reust, J. Case study: AOL instant messenger trace evidence. Digital Investigation 2006; 3(4):238–243.

[18] Mahajan, A., Dahiya, M. S., Sanghvi, H. P. Forensic Analysis of Instant Messenger Applications on Android Devices. International Journal of Computer Applications 2013; 68(8):38-44.

[19] Anglano C., Forensic analysis of WhatsApp Messenger on Android smartphones. Digital Investigation 2014; 11:201-213.

[20] Iqbal, Asif, Andrew Marrington, and Ibrahim Baggili. Forensic artifacts of the ChatON Instant Messaging application. 2013 Eighth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE), 2013; pp. 1-6.

[21] Said H, Yousif A, Humaid H. IPhone forensics techniques and crime investigation. International Conference and Workshop on Current Trends in Information Technology, 2011; pp. 120–125.

[22] Wong K, Lai ACT, Yeung JCK, Lee WL, Chan PH. Facebook Forensics. Valkyrie-X Security Research Group, 2011. https://www.fbiic.gov/public/2011/jul/facebook_forensics-finalized.pdf [last accessed 11.08.16]

[23] Al Mutawa N, Al Awadhi I, Baggili I, Marrington A. Forensic artifacts of Facebook's instant messaging service. International Conference for Internet Technology and Secured Transactions (ICITST), 2011; pp. 771–776.

[24] Sgaras C, Kechadi M-T, Le-Khac N-A. Forensics Acquisition and Analysis of Instant Messaging and VoIP Applications. Computational Forensics. Springer International Publishing; 2015. pp. 188–199.

[25] Azfar A, Choo K-KR, Liu L., An Android Social App Forensics Adversary Model, In Proceedings of Annual Hawaii International Conference on System Sciences (HICSS 2016), pp.5597 – 5606., 2016

[26] Walnycky D, Baggili I, Marrington A, Moore J, Breitinger F., "Network and device forensic analysis of Android social-messaging applications," Digital Investigation, Vol. 14, Supplement 1: S77–84., 2015.

[27] Levendoski M, Datar T, Rogers M. Yahoo! Messenger Forensics on Windows Vista and Windows 7. Digital Forensics and Cyber Crime, Volume 88. Berlin, Heidelberg: Springer Berlin Heidelberg; 2012; pp. 172–179.

[28] Chu H-C, Deng D-J, Park JH. Live Data Mining Concerning Social Networking Forensics Based on a Facebook Session Through Aggregation of Social Data. IEEE Journal on Selected Areas in Communications, 2011; 29(7):1368–1376.

[29] Parsons, A. Windows 10 Forensics: Conclusion - Computer & Digital Forensics Blog, 2015, April 30. http://computerforensicsblog.champlain.edu/2015/04/30/windows-10-forensics-conclusion/ [last accessed 21.08.16]