IJournals: International Journal of Software & Hardware Research in Engineering
ISSN-2347-4890
Volume 4 Issue 10 October, 2016

Digital Forensic Investigation of Facebook on Windows 10

Ming Sang Chang

Department of Information Management, Central Police University, Taiwan.

mschang@mail.cpu.edu.tw

ABSTRACT

Facebook 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 Facebook application on Windows 10 platform and presents evidence gathering of Facebook application. It proves beneficial for forensic analysts and practitioners as it assists them in course of mapping and locating digital evidences of Facebook on Windows 10 PC.

Keywords:Social Networking, Facebook, 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 Facebook, LinkedIn, Twitter, and Instagram [1]. 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].

Facebook is an online social networking service. Its website was launched in February 2004. As of the second quarter of 2016, Facebook had 1.71 billion monthly active users [5]. After registering to use the site, users can create a user profile, connect with friends, share information and thoughts, post status updates and photos, post comments, share videos, and engage in real-time instant messaging and chat rooms. Furthermore, users may join interest groups, organize events, and create fans pages for a workplace, or even a brand product. However, it is unavoidable that this platform may also provide incentives for criminals to carry out illegal activities such as bullying and stalking.

Facebook also recommends the publication of personal data, such as age, gender, contact information, relationship status, and work experience. The personal information uploaded to the websites makes it possible for cyber criminals to commit criminal acts. Cyber criminals also can commit other abusive activities such as uploading illegal material, defaming, and stalking. Digital forensics in social networks becomes important because the number of criminal acts rise in social networking services. It is a great assistance in investigating a criminal case if we can retrieve electronic evidences from social networking activities on a suspect's computer. The electronic evidences can be incriminating or proving the innocence of a suspect.

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 Facebook activities. We conduct research into the data remnants of a

user using Facebook in a variety of ways on a Windows 10 operating system. We use three different browsers to access Facebook. There are Google Chrome, Internet Explorer, and Mozilla Firefox.

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 [6]. 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 [7].

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 [8], Yahoo Messenger [9], and AOL Instant Messenger [10]. In 2013 Mahajan et al., [11] performed forensic analysis of Whatsapp and Viber on five android phones using UFED and manual analysis. CosimoAnglano [12] carried out Whatsapp forensics on Android in 2014 using YouWave virtualization platform. Levendoski et al. [13] concluded that artifacts of the Yahoo Messenger client produced a different directory structure on Windows Vista and 7. Wong et al. [14] and Al Mutawa et al. [15] demonstrated that artifacts of the Facebook web-application could be recovered from memory dumps and web browsing cache. Chu et al. [16] 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. Iqbal et al. [17] 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. [18] investigated Facebook and other IM applications, it was determined that only BlackBerry Bold 9700 and iPhone 3G/3GS provided evidence of Facebook unencrypted. Sgaras et al. [19] 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. Walnycky et al. [20] added that artifacts of the Facebook Messenger could vary depending on user settings, OS version, and manufacturer. Azfar A. et al. [21] 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. Parsons [22] 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 Facebook. It is often useful to corroborate evidence from different sources. It may confirm evidence from Facebook 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 Facebook 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 Facebook. A variety of virtual machines were created. It was decided to examine a variety of circumstances of a user using Facebook, and also to examine any differences when using different browsers. Multiple scenarios were explored. Each scenario made use of Facebook with a different browser. They are Google Chrome (GC), Internet Explorer (IE), and Mozilla Firefox (FF). Forty-two Virtual Machines (VMs) were created for each browser to replicate different circumstance of usage, as shown in Table 1.

Virtual Machine were created using VMware Workstation (V10.0.0). For each scenario, a base image was created, and Windows 10 32-bit build9841 was installed on a 15 GB virtual hard drive with 2 GB RAM. The Base-VM files were used as control media to determine the files created when user activity was undertaken in each scenario. The different actions undertaken were as follows.

1. The first step was to install the browser software into separate Base-VM's for each browser; Google Chrome v39.0.2171.71m, Mozilla Firefox v33.0.2, and Internet Explorer v11.0.98410.0 for Windows 10.

2. Next was to make copies of the Base-VM for each browser. These nine VMs were labeled GC, FF, IE Post-VM, and were used to post text, image, and video file on Facebook using each installed browser.

3. Additional copies of the Base-VM for each browser were made. These six VMs were labeled GC, FF, IE Reply-VM, and were used to reply message with text and image to Facebook using each installed browser.

4. Copies were made of the three Base-VMs. These three VMs were labeled GC, FF, IE Upload-VM, and each installed browser was used to upload a file for sharing with a group.

Table 1 All virtual machines files

Virtual PCs		Activities
GC, FF, IE (Base-VM)		Windows10 (build9841), 2 GB RAM, 15 GB Hard Disk Drive. Browser for each test installed; Microsoft Internet Explorer (IE), Mozilla Firefox (FF), Google Chrome (GC).
GC, FF, IE (Post-VM)	text	Test account accessed. Post different type of sample data to the Facebook account.
	image	
	video	
GC, FF, IE (Reply-VM)	text	Test account accessed. Reply different type of sample data to the Facebook account.
	image	
GC, FF, IE (Upload-VM)		Browser used to access the Facebook website. Post and share with a group. Upload a file.
GC, FF, IE (Download-VM)		Browser used to access the Facebook website. Post and share with a group. Download a file.
GC, FF, IE (Send_Msg-VM)	text	Using chat function, send different type of sample data to friend.
	image	
	file	
GC, FF, IE (Rcv_Msg-VM)	text	Using chat function, receive different type of sample data from friend.
	image	
	file	

5. Copies were made of the three Base-VMs. These three VMs were labeled GC, FF, IE Download-VM, and each installed browser was used to download a file from a sharing group.

6. Copies were made of the three Download-VMs. These nine VMs were labeled Send_msg-VM, and were used to send different type of sample data to friend using chat function on Facebook.

7. Copies were made of the three Download-VMs. These nine VMs were labeled Rcv_msg-VM, and were used to receive different type of sample data from friend using chat function on Facebook.

4. RESULT AND ANALYSIS

In this section we will describe the findings of the use of Google+.

4.1 Post-VM

(1) GC browser: We find the remnants of posting message in memory as Figure 1. The locations of remnant of posting message are on C:\Users\[UserName]\ntuser.dat.LOG2, and C:\Users\[UserName]\AppData\Roaming\Microsoft\Windows\Recent\IMG_10087.lnk.

Figure 1 the remnants of posting message with GC

(2) IEbrowser: We find the remnants of posting message in memory. The locations of remnant of posting message are on C:\Users\[UserName]\ntuser.dat.LOG2, and C:\Users\[UserName]\AppData\Roaming\Microsoft\Windows\Recent\IMG_0265.lnk.

(3) FF browser: We find the remnants of posting message in memory. The locations of remnant of posting message are on C:\Users\[UserName]\ntuser.dat.LOG2, and C:\Users\[UserName]\AppData\Roaming\Microsoft\Windows\Recent\IMG_10087.lnk

4.2 Reply-VM

(1) GC browser: We find the time stamp, user ID, and replying text as shown in Figure 2. The locations of remnant of replying message are on C:\Users\[UserName]\AppData\Roaming\Microsoft\Windows\Recent\IMG_0265.lnk, and C:\Users\[UserName]\ntuser.dat.LOG2.

(2) IE browser: We find the time stamp, user ID, and replying message. The locations of remnant of replying message are on C:\Users\[UserName]\ntuser.dat.LOG2, and C:\Users\[UserName]\AppData\Roaming\Microsoft\Windows\Recent\IMG_0265.lnk.

(3) FF browser: We find the time stamp, user ID, and replying message. The locations of remnant of replying message are on C:\Users\[UserName]\ntuser.dat.LOG2, and C:\Users\[UserName]\AppData\Roaming\Microsoft\Windows\Recent\IMG_0265.lnk.

Figure 2 The remnants of replying message with GC

4.3 Upload-VM

(1) GC browser: We find the uploading file as Figure 3. The locations of remnant of uploading file are on C:\Users\[UserName]\AppData\Local\Google\Chrome\User,C:\$LogFile, Data\Default\History, and C:\$Extend\$UsnJml $j.

(2) IEbrowser: We find the uploading file in memory. The locations of remnant of uploading file are on C:\Users\[UserName]\ntuser.dat.LOG1, C:\$Extend\$UsnJml$j, and C:\$LogFile.

(3) FF browser: We find the uploading file in memory. The locations of remnant of uploading file are on C:\Users\[UserName]\ntuser.dat.LOG1, C:\$Extend\$UsnJml $j, and C:\$LogFile.

Figure 3The remnants of uploading file with GC

4.4 Download-VM

(1) GC browser: We find the downloading file as Figure 4. The locations of remnant of

downloading file are on C:\Users\[UserName]\AppData\Local\Google\Chrome\User Data\Default\History,and C:\$Extend\$UsnJml $j.

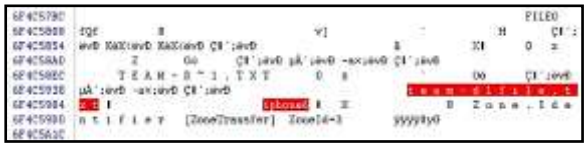

Figure 4 The remnants of downloading file with GC

(2) IEbrowser: We find the downloading file in memory. The locations of remnant of downloading file are on C:\$LogFile, C:\Unallocated Clusters, and C:\Users\[UserName]\AppData\Local\Microsoft\Windows\WebCache\V01.log.

(3) FF browser: We find the downloading file in memory. The locations of remnant of downloading file are on C:\$LogFile, C:\Unallocated Clusters, and C:\$Extend\$UsnJml $j.

4.5 Send_Msg-VM

(1) GC browser: We find the user's name, time stamp, and sending message as shown in Figure 5. The locations of remnant of sending message are on C:\$MFT, and C:\Users\[UserName]\AppData\Roaming\Microsoft\Windows\Recent\IMG_0499.lnk.

Figure 5 The remnants of sending message with GC

(2) IEbrowser: We find the user's name, time stamp, and sending message in memory. The locations of remnant of sending message are on C:\$MFT, and C:\Users\[UserName]\AppData\Roaming\Microsoft\Windows\Recent\IMG_0499.lnk.

(3) FF browser: We find the user's name, time stamp, and sending message in memory. The locations of remnant of sending message are on C:\$MFT, and C:\Users\[UserName]\AppData\Roaming\Microsoft\Windows\Recent\IMG_0499.lnk.

4.6 Rcv_Msg-VM

(1) GC browser: We find the receiving message in memory. The locations of remnant of receiving message are on C:\Users\[UserName]\AppData\Local\Google\Chrome\User Data\Default\Cache\data_1, C:\Users\[UserName]\Downloads\movie.txt, C:\$MFT.

(2) IEbrowser: We find the user's name, time stamp, and receiving message in memory. The locations of remnant of sending message are on C:\$LogFile, C:\$Extend\$UsnJml $j, C:\Users\[UserName]\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat, and C:\$MFT.

(3) FF browser: We find the user's name, time stamp, and receiving message in memory. The locations of remnant of sending message are on C:\$LogFile, C:\$Extend\$UsnJml $j, C:\Unallocated Clusters, and C:\$MFT.

5. DISCUSSIONS

In this research, we identified artifacts for Facebook application. We focus on both the volatile memory and hard drive artifacts. Our experiments showed that the Facebook 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 Facebook application activities remain some artifacts in different locations. This indicated that when a user has used the Facebook apps, there will be records remaining in the application folder.

We will explain the analysis of the internal memory and hard drive of a Windows 10 PC to determine data remnants after performing login, sending message, and receiving message on Facebook application. The analysis was performed to identify the file types, search for related Facebook activities data, and determine the location of stored artifacts.

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.

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 Facebook application with Windows 10. The results indicated that use of the Facebook 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.

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]. Number of monthly active Facebook users worldwide http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ [last accessed 05.08.16].

[6]. 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].

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

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

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

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

[11]. 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.

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

[13]. 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.

[14]. 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]

[15]. 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.

[16]. 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.

[17]. 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.

[18]. 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.

[19]. 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.

[20]. 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.

[21]. 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.

[22]. 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]

