IJournals: International Journal of Software & Hardware Research in Engineering
ISSN-2347-4890
Volume 4 Issue 9 September, 2016

Evidence Gathering of LinkedIn on Windows10

Ming Sang Chang[1]; Chih Yen Chang[2]

[1]Department of Information Management, Central Police University,Taiwan.

[2]Graduate Institute of Communication Engineering, National Taiwan University, Taiwan.

[1]mschang@mail.cpu.edu.tw; [2]gsmmcc@gmail.com

ABSTRACT

Social networking has changed the way people communicate with each other. It is used by a wide range of age groups. Social networking applications like LinkedIn, Facebook, Twitter, and Google+ which facilitate users to send and receive messages, upload posts and comments via various end devices. Its extensive use in everyday life provides unique opportunities but means that it can also be used to commit crime such as cyber stalking and cyber bullying. 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 LinkedIn application with Windows 10 and presents evidence gathering of LinkedIn application. It proves beneficial for forensic analysts and practitioners as it assists them in course of mapping and locating digital evidences of LinkedIn on Windows 10 PC.

Keywords:Social networking, LinkedIn, Investigation, Digital forensics.

1. INTRODUCTION

A social networking service is an online platform that is used by people to build social networks with other people. They share similar personal interests, activities, or real-life connections [1]. Social networking sites allow users to share ideas, digital photos and videos, posts, activities, events, and interests with people in their network. Depending on the social media platform, members may be able to contact any other member. Over the past years, social networks have become the largest and fastest growing websites on the Internet. There are some popular social networking sites such as Facebook, YouTube, Twitter, LinkedIn, and Google+ [2]. Various types of personal information are shared on social networking platforms such as name, email addresses, phone numbers, photos, and date of birth. Social networking sites contain sensitive and personal data of billions of people [3].

LinkedIn is a business-oriented social networking service. It is mainly used for professional networking. LinkedIn launched on May 5, 2003 [4]. As of March 2016, LinkedIn has more than 433 million accounts, and more than 106 million active users [5]. The basic functionality of LinkedIn allows users to create profiles and connect to each other in an online social network. Users can invite anyone to become a connection. The list of connections can be used in a number of ways such as finding jobs, listing jobs, obtaining introductions to the connections, following different companies, etc. LinkedIn also can post photos and update status, send an instant messaging, tag your contacts, etc. LinkedIn is a cross platform application for Windows, MAC, iOS, Android, etc. It is a widely used application. As the use of LinkedIn 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, cyber bullying, etc. 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 [6-8].

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. It challenges to forensic examiners for recovering digital evidences of a conversation under investigation. 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 LinkedIn on windows 10 operating system. Our purpose is to identify various data remnants in LinkedIn on the Windows 10 platform. It proves beneficial for forensic analysts and practitioners as it assists them in course of mapping and locating digital evidences of LinkedIn on Windows 10 PC.

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 networking. They are hard drive, memory, and network. Some social networking services have the ability to log information on the user's hard drive [9]. To use a social networking, an account must be established to create a screen name provided with user information. Some instant messenger providers might assist the investigation with information of the account owner.

Evidence can be found in various internet file caches used by Internet Explorer for volatile social networking and each cache holds different pieces of data. Apart from the normal files, files left by instant messenger on a hard 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 [10].

Artifacts of instant messaging 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 [11], Yahoo Messenger [12], and AOL Instant Messenger [13]. In 2013 Mahajan et al., [14] performed forensic analysis of Whatsapp and Viber on five android phones using UFED and manual analysis. CosimoAnglano [15] carried out Whatsapp forensics on Android in 2014 using YouWave virtualization platform. Levendoski et al. [16] concluded that artifacts of the Yahoo Messenger client produced a different directory structure on Windows Vista and 7. Wong et al. [17] and Al Mutawa et al. [18] demonstrated that artifacts of the Facebook web-application could be recovered from memory dumps and web browsing cache.

Said et al. [19] investigated Facebook and other social networking applications, it was determined that only BlackBerry Bold 9700 and iPhone 3G/3GS provided evidence of Facebook unencrypted. Sgaras et al. [20] 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. [21] added that artifacts of the Facebook Messenger could vary depending on user settings, OS version, and manufacturer. Azfar A. et al. [22] 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. Chu et al. [23] 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. [24] studied the artifacts left by the ChatON instant messaging application. The analysis was conducted on an iPhone running iOS6 and a Samsung Galaxy Note running Android 4.1.

To our knowledge, no detailed analysis of LinkedIn artifacts on Windows 10 has been undertaken, hence this research aims to fill the gap and provide a road map of LinkedIn forensic artifacts.

3. METHODOLOGY

In our research, we use virtual machines with a standard installation of Windows 10 build 10240. The Internet Explorer 11.0.10240 and Google Chrome 44.0.2403 were installed on Windows 10. We set up 32 different configurations. We don't re-configure and copy physical hard disk drives. This allowed us to examine a variety of test in several configurations and to facilitate forensic analysis of LinkedIn. When conducting analysis with message exchange of using LinkedIn, one of the main issues is to identify where potential data remnants resides. We focus on identifying data remnants of the activities of LinkedIn on a Windows 10 PC. This is undertaken to determine the remnants an examiner should search for when LinkedIn is suspected. Our research also includes the circumstances of using anti-forensic methodology to hide evidence, and whether remnants remain to identify the use of LinkedIn.

This research focuses on what data remnants on Windows 10 PC after a user log in, post message, and send message of the use of LinkedIn. We want to find username, password, text, and files. In addition, we also create circumstances to simulate a user running CCleaner V1.13.50 to remove evidences.

There are 32 virtual machines which replicate different circumstance of activities to gather the data in relation to the use of LinkedIn on Windows 10. We make multiple scenarios to explore the use of LinkedIn. The virtual machines were created for each different circumstance of LinkedIn 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 V10.0.0. For each experiment, Windows 10 was installed on every virtual machine. 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 17.4, SQLite V2.0.1, AccessData FTK Imager V3.1.1.8, MANDIANT Memoryze V3.0, and Social Password Decryptor V6.5.

According to the activities of LinkedIn, we create eight sub-experiment systems. They are Login-VM, PostText-VM, ReplyText-VM, DeleteText-VM, PostImage-VM, DeleteImage-VM, SendMessage-VM, and DeleteMessage-VM. There are four environments in each sub-experiment system. They include two different browser modes of Internet Explorer and Google Chrome. The activities of default browser mode and private browser mode of Internet Explorer are in different virtual machines that are different scenarios. Google Chrome also has default browser mode and incognito browser mode that are different scenarios. In all experiments, there are 32 virtual machines to gather the data in relation to the activities of LinkedIn.

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

1. The first case was to install Internet Explorer (IE) and Google Chrome (GC) into different base virtual machine with Windows 10.

2.The second case was to make four copies of the base virtual PC with IE and GC for each scenario. An account of LinkedIn was created for these experiments. We use email address to sign in LinkedIn on four different virtual PCs. We do nothing and sign out. Then we use SQLite Database Browser, WinHex, and Social Password Decryptor to find the data remnants of the account and password.

3.The third case was to make four copies of the base virtual PC with IE and GC for each scenario. There are four scenarios for posting text. After posting text we sign out and find the data remnants on Virtual PC.

4.The forth case was to make four copies of the base virtual PC with IE and GC for each scenario. There are four scenarios for uploading reply comments. After uploading replying text we sign out and find the data remnants on Virtual PC.

5. The fifth case was to make four copies of the base virtual PC with IE and GC for each scenario. There are four scenarios for deleting uploading text. After deleting text we sign out and find the data remnants on Virtual PC.

6.The sixth case was to make four copies of the base virtual PC with IE and GC for each scenario. There are four scenarios for posting image. After posting image we sign out and find the data remnants on Virtual PC.

7.The seventh case was to make four copies of the base virtual PC with IE and GC for each scenario. There are four scenarios for deleting uploading image. After deleting image we sign out and find the data remnants on Virtual PC.

8.The eighth case was to make four copies of the base virtual PC with IE and GC for each scenario. There are four scenarios for sending text message. After sending text message we sign out and find the data remnants on Virtual PC.

9.The ninth case was to make four copies of the base virtual PC with IE and GC for each scenario. There are four scenarios for deleting sending text. After deleting text we sign out and find the data remnants on Virtual PC.

4. RESULT AND ANALYSIS

In this section we will describe the remnants of the use of LinkedIn.

4.1 Login-VM

(1) IE default browser mode: We find the login email address (nwx9c@yahoo.com.tw) but can't find the password as shown in Figure 1. The time stamp also can be found. We believe the password with a secure encryption method so that we can't find it. After CCleaner was run to delete temporary, history, cookies, recycle bin, memory dumps, log files, etc. The remnants can be found as before.

Figure 1 the remnants of login with IE

(2) IE private browser mode: We find the login email address. In this experiment, a search for the login password produced no matches in the forensic image and memory dump. After running CCleaner the remnants can be found as before.

Figure 2 The remnants of login with GC

(3) GC default browser mode: We find the login email address and the password as shown in Figure 2. After running CCleaner the remnants can be found as before.

(4) GC incognito browser mode: We find the login email address and register telephone number but can't find the password. After running CCleaner all the remnants can't be found.

In these four experiments we can find some data remnants. In IE the password can't be found but it can be found in GC. In GC the password was encrypted in some area of memory. We use Chrome Password Decryptor V7.0 to decrypt it and find the password.

4.2 PostText-VM

(1) IE default browser mode: We find the user's name (young sun), time stamp (1449497564542), and uploading text (long time no see) as shown in Figure 3. After running CCleaner the user's name, time stamp, and text can also be found.

Figure 3 The remnants of posting text with IE

(2) IE private browser mode: We find the user's name and uploading text. After CCleaner was run to delete temporary, history, cookies, recycle bin, memory dumps, log files, etc. The user's name and text can also be found.

(3) GC default browser mode: We find the user's email address, time stamp, and uploading text. After running CCleaner the remnants can be found as before.

(4) GC incognito browser mode: We find the time stamp and uploading text. After running CCleaner the remnants can be found as before.

In these four experiments we can find some data remnants such as user's name,time stamp, and posting text.

4.3 ReplyText-VM

(1) IE default browser mode: We find the user's name, time stamp, and uploading reply text as shown in Figure 4. After running CCleaner the remnants can be found as before.

(2) IE private browser mode: We find the user's name, time stamp, and uploading reply text. After running CCleaner the remnants can be found as before.

(3) GC default browser mode: We find the time stamp and reply text. After running CCleaner the user's email address and user's ID can only be found.

Figure 4 The remnants of replying text with IE

(4) GC incognito browser mode: We find the time stamp and reply text. After running CCleaner the user's email address and user's ID can only be found.

4.4 DeleteText-VM

(1) IE default browser mode: We find the user's name, time stamp, and post text. After running CCleaner the remnants can be found as before.

(2) IE private browser mode:the remnants are the same as **IE default browser mode**.

(3) GC default browser mode: We find the time stamp and text. After running CCleaner the remnants can be found as before.

(4) GC incognito browser mode: We find the time stamp and text. After running CCleaner the remnants can be found as before.

4.5 PostImage-VM

(1) IE default browser mode: We find the user's name, time stamp, and image filename as shown in Figure 5. The remnants are also on c:\users\joe\desktop\8561.jpg. After CCleaner was run to delete temporary, history, cookies, recycle bin, memory dumps, log files, etc. The remnant can also be found on c:\users\joe\desktop\8561.jpg.

(2) IE private browser mode: We find the user's name and image file. After running CCleaner the image file name can be found.

(3) GC default browser mode: We find the time stamp, image filename and local disk location of image file. After running CCleaner the image filename, time stamp, and local disk location of image file can be found.

(4) GC incognito browser mode: We find the time stamp, image filename and local disk location of image file. After running CCleaner the image filename, time stamp, and local disk location of image file can be found.

Figure 5 The remnants of posting image with IE

4.6 DeleteImage-VM

(1) IE default browser mode: We find the image file on memory and hard drive. After running CCleaner the local disk location of image file also can be found.

(2) IE private browser mode:the remnants are the same as**IE default browser mode**.

(3) GC default browser mode: We find the image file, local disk location of image file, and time stamp. After running CCleaner the image file, time stamp, and local disk location of image file can only be found.

(4) GC incognito browser mode: We find the image file, local disk location of image file, and time stamp. After running CCleaner the image file, time stamp, and local disk location of image file can only be found

4.7 SendMessage-VM

(1) IE default browser mode: We find the sender username, receiver username, and sending message as shown in Figure 6. After running CCleaner the user's name and text can also be found.

(2) IE private browser mode: We find the sender username and sending message. After running CCleaner the sending message can also be found.

(3) GC default browser mode: We find the sender user name, receiver user name, time stamp, and sending message. After running CCleaner the receiver user name, time stamp, and sending message can be found.

(4) GC incognito browser mode: We find the sender user name, receiver user name, time stamp, and sending message. After running CCleaner the receiver user name, time stamp, and sending message can be found.

Figure 6 The remnants of sending message with IE

4.8 DeleteMessage-VM

(1) IE default browser mode: We find the sender username and sending message. After running CCleaner the sender username and sending message can also be found.

(2) IE private browser mode: We find the sending message. After running CCleaner the sending message can also be found.

(3) GC default browser mode: We find the sender user name, receiver user name, time stamp, and sending message. After running CCleaner the receiver user name, time stamp, and sending message can be found.

(4) GC incognito browser mode: We find the sender user name, receiver user name, time stamp, and sending message. After running CCleaner the sending message can be found.

5. DISCUSSIONS

In this research, we identified artifacts for LinkedIn. We focus on both the volatile memory and hard drive artifacts. Our experiments showed that the LinkedIn 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 LinkedIn activities remain some artifacts. This indicated that when a user has used the LinkedIn, 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, uploading posts, uploading comments, and sending messages activities in LinkedIn applications.

(1) Login information

Logging in to the LinkedIn would leave the username and email address in internal memory which can be detected by searching with the keywords such as username or email address.However, no trace of the user password could be detected in the internal memory of IE scenarios. In GC the user password could be detected in the internal memoryby searching with the keyword password.

(2)Uploading posts

The investigation revealed that posts uploaded using the LinkedIn, and their corresponding timestamps, are detectable in the internal storage in plain text and can be recovered by searching with the keywords text, time, and name.

(3)Uploading comments

The LinkedIn stores comments uploaded on the internal storage in plain text, along with the upload time. These artifacts contain the information of the person who has uploaded the comment and the content of the comment itself. It can be recovered from the internal storage by searching with the keywords text, time, and comment.

(4)Messaging

The examination of the LinkedIn revealed instant messages sent by the user. These artifacts remain in the internal storage in plain text, and can be retrieved from the internal storage by searching with the keywords text, time, and recipient.

It should be noted that the significance and location of artifacts could be investigated. In our research, it was determined that: (1) LinkedIn maintain directories in the application folders. (2) The LinkedIn caches copies of the upload and sending message.

6. CONCLUSIONS

Social networking is increasingly popular among individuals and business organizations. Applications such as LinkedIn, Facebook, and Twitterare some of the commonly used applications. 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 LinkedIn application with Windows 10.The results indicated that use of the LinkedIn for 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]. Buettner, R. Getting a Job via Career-oriented Social Networking Sites: The Weakness of Ties. 49th Annual Hawaii International Conference on System Sciences, January 5-8, 2016. DOI: 10.13140/RG.2.1.3249.2241.

[2]. Top 15 Most Popular Social Networking Sites, August 2016. http://www.ebizmba.com/articles/social-networking-websites [last accessed 16.08.2016]

[3]. Number of monthly active Facebook users worldwide as of 2nd quarter 2016. http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ [last accessed 20.08.2016]

[4]. "LinkedIn - About". LinkedIn Corporation. 2015. Retrieved March 5, 2015.

[5]. "LinkedIn Announces First Quarter 2016 Results". LinkedIn Newsroom.

[6]. 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

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

[8]. 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]

[9]. 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 05.07.2016].

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

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

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

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

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

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

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

[17]. 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/faceboo

k_forensics-finalized.pdf [last accessed 01.08.2016]

[18]. 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), pp. 771–776., 2011.

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

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

[21]. 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.

[22]. 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.

[23]. 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, 29(7):1368–1376., 2011.

[24]. 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), pp. 1-6., 2013.