LinkedIn Social Media Forensics on Windows 10

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 Mar. 12, 2019; Revised and Accepted Sept. 3, 2019; First Online Sept. 16, 2019)

Abstract

Many people have gradually changed their way of living habits on account of the great popularity progression of social networking sites. There are varied kinds of social networking sites coming out in recent years, for example, Facebook, Twitter, Instagram, LinkedIn. Furthermore, social networking sites have already made people more convenient to make friends and communicate with each other much easier than before. However, there are some problems we should concern. Owing to the cyberworlds are flourishing, there are several kinds of crimes emerge in endlessly in recent years. This paper focuses on the digital forensics of LinkedIn by running on three different browsers, including Google Chrome, Mozilla Firefox, and Microsoft Edge. They are running respectively under windows 10 operating system. In our work, we strive to find digital evidences that user has been done on the computers. We make use of authoritative digital forensic tools to obtain significant evidences and analyze the correlation between these evidences in detail. Besides, we will find out which behaviors of the suspect will leave what kind of evidences on the computer. These findings could be important references for the law enforcement agency to investigate digital crime.

Keywords: Crime Investigation; Digital Forensics; LinkedIn; Social Media

1 Introduction

In recent years, the popularity of social networking sites has given rise to the number of social networking users for recreation and business purposes. A social network is a community where people across the globe world online that can develop a network with different individuals for a specific purpose [1]. Besides, the prevalence of these social networking websites has changed the living habits of many people. These people usually browse social networking sites to relieve their working pressure or any other kinds of pressures in their daily life.

People can make use of social networking sites to build up their profile. A profile is a list of identifying information that can portray users' online identity, including photographs, name, birthday, hometown, personal interest and so on [9]. Furthermore, social networking sites can connect people and maintain relationships from all parts of their lives [6]. They can share everything with their friends on the websites. There is no doubt that people have incorporated social networking sites into their lives and made using social networking sites as frequent daily activities.

Due to the advance of technology, the type of crime is getting much more complex than before. At present, traditional crime is on the decrease. In other words, high technology crime is increasing nowadays. There are a lot of perpetrators using social networking sites to commit the cybercrime because of its convenience and anonymity characteristics. Therefore, the traditional crimes such as killing people, domestic violence, stealing and robbing are decreasing nowadays. On the contrary, computer crime and cybercrime have already become the mainstream of all the crimes. Cybercrime refers to a perpetrator that abused or destroyed a computer to commit a crime. Therefore, cybercrime is definitely different from traditional crime. The following shows the characteristics of cybercrime [7]:

- Making use of the computer characteristics to commit the crime.
- The high dark figure of crime.
- The time and dimension features between crime behaviors and crime results.
- Take a computer as a crime scene.
- Take a computer as a target.

Over the past 10 years, the terrorists use the Internet have become of great concern. The gang of terrorist has successfully used the Internet to enlarge their memberships [11]. This will cause widespread harm to Internet victims.

According to the survey of National Police Agency, Ministry of the Interior Republic of China, the statistics show the cybercrimes happened in Taiwan between

January and June in 2017, there are 6,567 cybercrime cases occurred. The cybercrime ratio increases 4.39 percentages relative to the same period of last year. However, the perpetrators who are at the age of 18 to 23 called adolescents are increasing 28.07 percentages relative to the same period of last year. The victims who are more than 50 years old are increasing 43.54 percentages relative to the same period of last year [15]. Over the past few years, various kinds of cybercriminals have emerged endlessly due to the anonymity characteristic of the Internet. Therefore, anonymity is largely tied to the cybercrime nowadays. Moreover, it is also claimed that the anonymity characteristic allows perpetrators to use the Internet without the possibility of detection. Catherine D. Marcum, *et al.* categorized different types of social networking criminality, for instance, texting, identity theft, cyberbullying, digital piracy, sexual violence, and so forth [13]. Therefore, we can realize that social networking websites have seriously become a hotbed of cybercrimes based on these significant literatures. According to the survey of eBizMBA [10], popular social networking sites are prevalent nowadays, such as Facebook, YouTube, Twitter, Instagram, LinkedIn and so on. Many of them have over than 100 million members, a quite large number for the time.

This paper focuses on the digital forensics of LinkedIn by running on three different browsers, including Google Chrome, Mozilla Firefox and Microsoft Edge. They are running respectively under windows 10 operating system. In our work, we strive to find digital evidences that user has been done on the computers. 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 the related works. In Section 3, we introduce our investigation methodologies. In Section 4, we present results and findings of digital forensics on LinkedIn. Finally, we summarize the conclusions.

2 Related Works

2.1 LinkedIn Social Networking Site

LinkedIn is a business and employment-oriented service that operates via websites and mobile applications. It founded on December 28 in 2002 and launched on May 5 in 2003.

LinkedIn [19] is mainly used for professional networking, including employers posting jobs and job seekers posting their curriculum vitae. According to the survey of Alexa [2], LinkedIn was ranked 31st relative to other social networking websites in the world. As of April 2017, LinkedIn had 500 million members in 200 countries, out of which more than 106 million members are activities [12]. LinkedIn allows members to create profiles and connections to each other in an online social network that may represent real-world professional relationships. Members can invite anyone to become a connection [17].

Such dissemination of confidential information is possibly more likely concerning social networking applications such as LinkedIn where users may be actively looking for employment or maybe in contact with individuals from competitor organizations.

However, there are many kinds of literature focus on the forensic analysis of social networking sites nowadays. Azfar *et al.* [5] proposed the utility model for the evidence extraction of five social networking applications, including Twitter, POF Dating, Snapchat, Fling and Pinterest.

Neha [16] focused on the forensic analysis of WhatsApp application on storage devices and volatile memory. Mutawa *et al.* [14] focused on the forensic analysis of three popular social networking sites, including Facebook, Twitter, and Myspace. Dezfouli, *et al.* [8] examined four well-known social networking applications, Facebook, Twitter, LinkedIn, and Google+. They were able to recover artefacts, such as usernames, passwords, login information, personal information, posts, messages and comments from these social networking sites. However, they only focus on the mobile phone forensics for these four applications. They didn't perform computer forensics which refers to browser forensics for these four applications. As a result, we take the LinkedIn application as one of our experiment targets.

This paper studies the behavior of a user who log into LinkedIn from different browsers. We strive to extract the evidence of posts creation, making comments, chatting records, browsing behaviors, adding friends and so forth. All of these behaviors are conducted under Windows 10 operating system. Furthermore, this paper analyzes correlations between these evidences and discusses how these evidences can help law enforcement agencies to investigate a crime.

2.2 Tools

Due to the high dynamics and heterogeneity of social media, digital forensics can use different and complex software tools to conduct effective and legal evidence collection [3]. There are many forensic tools on the market today. The mainstream of digital forensic products such as Autopsy, Forensic Toolkit and EnCase forensic have support digital forensics. The study described in this paper has been executed by a series of processes. In the experiments, the hard disk and memory were examined to extract and analyze the data generated by LinkedIn website. With the advanced development of forensic tools, the forensic tools and techniques should keep investigators ahead of the criminals [18].

Arthur *et al.* [4] conducted an investigation into some of the forensic tools, including PC Inspector File Recovery, EnCase, Forensic Toolkit and FTK Imager. However, the main function of FTK Imager is to view and to image storage devices. In light of these advantages, we adopt AccessData FTK Imager V4.1.1 to create an image file for the hard disk. Forensic Toolkit is a computer forensics software made by AccessData. It scans a hard disk

searching for various types of information. The toolkit comprises a standalone disk imaging program called FTK Imager. The FTK Imager is a simple tool that saves an image of a hard disk in a file. The result is an image file that can be saved in several formats.

On the other hand, there are many kinds of tools used for memory forensics nowadays. The manipulation of these memory forensic tools is roughly different, but the theorem concepts are the same. The goal of these tools is to read physical memory for the sake of achieving memory forensics. Therefore, this paper adopts the MANDIANT tool to create an image file for the memory. MANDIANT is an open source tool that can be downloaded on the Internet. There are a few basic functions describe as follows:

- MemoryDD.bat: This batch file is used to create an image file for volatile memory.
- Process.bat: This batch file is used to list all the running processes.
- DriverSearch.bat: This batch file is used to list which SYS file is loading on the computer.
- HookDetection.bat: This batch file is used to list which hooks file is executing on the computer.

In the experiment, in order not to influence the integrity of digital evidence, this paper makes use of MemoryDD.bat file to dump the memory for the sake of creating image files. Finally, this paper makes use of AccessData FTK Imager V4.1.1 to analyze all the image files which were generated by the previous processes. However, the most important of all is that we take another clean computer to analyze these image files.

In this paper, all the experiments were conducted on the real computer system. The computer system was installed Windows 10 professional 64-bit operating system. The central processing unit is Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz. The memory size is 8 Gigabytes. This paper selects two common browsers, including Google Chrome V59.0.3071.115 and Microsoft Edge V 40.15063.0.0.

3 Methodology

3.1 Research Goal

The research described in this paper is done by a series of processes, each involving a specific scenario. In the experiment, we log into LinkedIn websites via three different browsers. All of these operations are executed under Windows 10 operating system. After login, we do a series of same behaviors, such as login account, adding friends, chatting with friends, writing posts, making comments, clicking the "Like" button. Afterward, we make use of Forensic Toolkit Imager to extract digital evidence of these behaviors left. Finally, we analyze and compare the difference between these digital evidences.

3.2 Experiment Elaboration

In order to ensure the integrity of digital evidence and avoid the interference between digital evidences, we separate the experiments into three scenarios according to the different browsers. We chose three clean computers and each of them was installed Windows 10 professional operating system. We did these three scenarios in different computer environments. They were not placed on the same computer system. Afterward, we performed a series of behaviors on the LinkedIn. The following shows the details for these three scenarios.

3.2.1 Scenario 1: Google Chrome

In scenario 1, all the operations were conducted via Google Chrome browser. We entered the personal account and password to log into the LinkedIn website. After log into the LinkedIn website, we created posts and uploaded the pictures. Moreover, we did a lot of users common activities, for example, adding friends, chatting with friends, making comments, clicking the "Like" button and so forth. After we did these user common activities, we didn't do anything anymore. We created image files for the hard disk and memory respectively. Thereafter, we adopted Forensic Toolkit Imager to extract and analyze the digital evidence.

3.2.2 Scenario 2: Mozilla Firefox

In scenario 2, all the operations were conducted via the Mozilla Firefox browser. We entered the personal account and password to log into the LinkedIn website. After login, we created posts and uploaded the pictures. Moreover, we did a lot of users common activities, for example, adding friends, chatting with friends, making comments, clicking the "Like" button and so forth. After we did these user common activities, we didn't do anything anymore. We created image files for the hard disk and memory respectively. Thereafter, we adopted Forensic Toolkit Imager to extract and analyze the digital evidence.

3.2.3 Scenario 3: Microsoft Edge

In scenario 3, all the operations were conducted via the Microsoft Edge browser. We entered the personal account and password to log into the LinkedIn website. After login, we created posts and uploaded the pictures. Moreover, we did a lot of users common activities, for example, adding friends, chatting with friends, making comments, clicking the "Like" button and so forth. After we did these user common activities, we didn't do anything anymore. We created image files for the hard disk and memory respectively. Thereafter, we adopted the Forensic Toolkit Imager to extract and analyze the digital evidence.

4 Results and Findings

We log into the LinkedIn website by entering the email account and password on the computer. Afterward, we execute a series of processes, such as creating posts, chatting with friends, making comments, adding friends. After executing these user common activities, we create image files for the hard disk and the memory. We separate analysis procedure into two parts, hard disk and memory. We make use of one practical function of FTK Imager to execute a quick search for the keyword. The following are our analyses and description of forensic results.

4.1 Findings: Scenario 1: Google Chrome

4.1.1 Account and Password

In the hard disk, there are various kinds of evidence we can extract. First, we can find out user account information by searching the key string "www.linkedin.com", as shown in Figure 1. We can find two keywords in the context, there are "session_key" and "session_password". These two keywords reveal important information about the e-mail login account and password. However, we can't find password information because the text of password was garbled. We can't comprehend its meaning by our first intuition. Therefore, we infer that the password may be encrypted.

In the part of memory, we can only find an e-mail login account, but the password was garbled as well.

4.1.2 Posting Evidence

Every posting has it's unique post ID. Post ID is a string of numbers. When a user writes a post on the feed, the system will automatically assign a unique ID to the posting, for example, "https:// www.linkedin.com/feed/update/urn:li:activity:6378505126512074752/". We can easily realize the post ID is 6378505126512074752. Therefore, the posting network address is often built in the form of "https://www.linkedin.com/feed/update/urn:li:activity: Post ID". In the hard disk, by searching the key string "https://www.linkedin.com/feed/update/urn:li:activity:", we can find creating evidence of posting, as shown in Figure 2. Therefore, we can match the post ID we found in the image file and the network address. If both of them are the same, we can definitely infer that they must have posted that article on the LinkedIn website in the past. Moreover, we also found post contents by searching the key string, as shown in Figure 3.

In the part of memory, we can also find creating evidence and posting contents by searching the key strings.

4.1.3 Making Comment Evidence

LinkedIn allows any people to make any comments on any articles. In the hard disk, by searching the keyword "comment", we can find comment evidence that we made on the other user's posting, as shown in Figure 4. On the other hand, by reverse searching the key string, we can find comment content, as shown in Figure 5.

In the part of memory, the situation is the same as in the hard disk, we can also find comment evidence and its content by searching the keyword and the key string.

4.1.4 Chatting Records

In the hard disk, we can extract chatting record evidence. When a user chatted with friends, the system will automatically record chat ID. Moreover, the network address of chatting page would show friend's chat ID, for example, "https://www.linkedin.com/messaging/thread/63784999 18738399232". Therefore, we can easily realize that the majority of the chatting record network address is often built in the form of "https://www.linkedin.com/messaging/thread/Chat-ID". By searching the key string "https://www.linkedin.com/messaging/thread/", we can easily find the chatting record evidence, as shown in Figure 6. Furthermore, we can also find chatting content evidence by searching the key string in reverse, as shown in Figure 7.

In the part of memory, we can also find chatting record evidence by searching the key string "https://www.linkedin.com/messaging/thread/", and find chatting content evidence by searching the key string in reverse.

4.1.5 Clicking "Like" Button Evidence

There is a function on the LinkedIn website called "Like". If people like a post, they may click the "Like" button on that post. In the part of hard disk, we can find clicking "Like" evidence by searching the keyword "likes".

In the part of memory, we can also find clicking "Like" evidence by searching the keyword "likes". As a result, by analyzing the clicking "Like" evidence, the investigator can easily realize the preference of a perpetrator.

4.1.6 Friend List and Friend Request

In the hard, we can find friends request evidence. When we search the keyword "invite-sent", we can see that there is a key string, for example, "https://www.linkedin.com/mynetwork/invite-sent/jing-you-lin-a9017b15b/?isSendInvite=true", as shown in Figure 8. The string "jing-you-lin-a9017b15b" is friend's personal ID. The string "?isSendInvite=true" represents that the user must have sent a friend request to other LinkedIn members in the past. Therefore, we can easily realize that the majority of friend-request format is often built in the form of "https://www.linkedin.com/mynetwork/invite-sent/Personal-ID/?isSendInvite=true". By searching the key string "https://www.linkedin.com/mynetwork/invite-sent/", we could easily understand whether the user had sent a friend request to other LinkedIn members or not. However, when we searched the key

string "https://www.linkedin.com/mynetwork/invite-connect/connections/" in the hard disk, we cannot find out the friend list.

In the part of memory, we can also find friend request evidence by searching the key string "https://www.linkedin.com/mynetwork/invite-sent/". However, we cannot find out friend list by searching the key string "https://www.linkedin.com/mynetwork/invite-connect/connections/" as well.

To sum up, the evidence we found in the memory is quite the same in the hard disk. In the memory, we also found login information, the evidence of writing a post, making comments, chatting with friends, clicking "Like" records and so on. Therefore, there is no difference between in the hard disk and in the memory that evidences we found on the Google Chrome browser.

4.2 Findings: Scenario 2: Mozilla Firefox

In scenario 2, we also aim to the hard disk and memory forensics. We did the same thing as the previous scenario did. However, the forensic target in this scenario is different from the previous scenario. In scenario 2, we did the experiment on the Mozilla Firefox browser.

4.2.1 Account and Password

In the Mozilla Firefox, we can find user account information by searching the key string "www.linkedin.com". We can also easily realize that the user must have been used this computer to perform LinkedIn activities. On the other hand, when we conduct a search for the password, we can find out password information by typing a user's password string directly.

In the part of memory, the situation is the same as in the hard disk. We can find login account and password information by searching the account string and password string directly.

4.2.2 Posting Evidence

As the same to the previous scenario, every posting has it's unique post ID. Post ID is a string of numbers. When a user writes a post on the feed, the system will automatically assign a unique ID to the posting. The posting network address is often built in the form of "https://www.linkedin.com/feed/update/urn:li:activity: Post ID". In the hard disk, by searching the key string "https://www.linkedin.com/feed/update/urn:li:activity:", we can find the evidence of post creation. Therefore, we can match the post ID we found in the image file and the network address. If both of them are the same, we can definitely infer that they must have posted that article on the LinkedIn website in the past.

In the part of memory, we can also find out the evidence of post creation by searching the key strings.

4.2.3 Making Comment Evidence

As the same to the previous scenario, LinkedIn allows any people to make any comments on any articles. In the hard disk, by searching the keyword "comment", we can find out comment evidence that we made on the other user's posting.

In the part of memory, the situation is the same as in the hard disk, we can also find comment evidence and its content by searching the keyword "comment".

4.2.4 Chatting Records

As the same to the previous scenario, the majority of chatting record network address is often built in the form of "https://www.linkedin.com/messaging/thread/Chat-ID". Therefore, by searching the key string "https://www.linkedin.com/messaging/thread/", we can easily find out the chatting record evidence as well. Furthermore, we can also find out chatting content evidence by looking for the key string in reverse searching.

In the part of memory, we can also find out chatting record evidence by searching the key string "https://www.linkedin.com/messaging/thread/", and find chatting content evidence by looking for the key string in reverse searching.

4.2.5 Clicking "Like" Button Evidence

As the same to the previous scenario, we can find out clicking "Like" evidence by searching the keyword "likes" in the hard disk.

In the part of memory, we can also find out clicking "Like" evidence by searching the keyword "likes". As a result, by analyzing the clicking "Like" evidence, the investigator can easily realize the preference of a perpetrator.

4.2.6 Friend List and Friend Request

As the same to the previous scenario, we can find out friend request evidence in the hard disk. The majority of friend-request format is often built in the form of "https://www.linkedin.com/mynetwork/invite-sent/Personal-ID/?isSendInvite=true". By searching the key string "https://www.linkedin.com/mynetwork/invite-sent/", we could easily understand whether the user had sent a friend request to other LinkedIn members or not. However, when we searched the key string "https://www.linkedin.com/mynetwork/invite-connect/connections/" in the hard disk, we cannot find out the friend list as well.

In the part of memory, we can also find out friend request evidence by searching the key string "https://www.linkedin.com/mynetwork/invite-sent/". However, we cannot find out friend list by searching the key string "https://www.linkedin.com/mynetwork/invite-connect/connections/" as well.

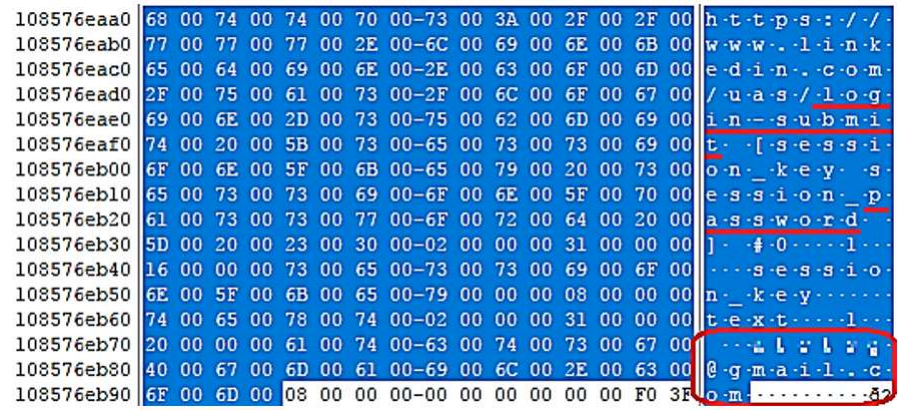

Figure 1: The result of searching login information

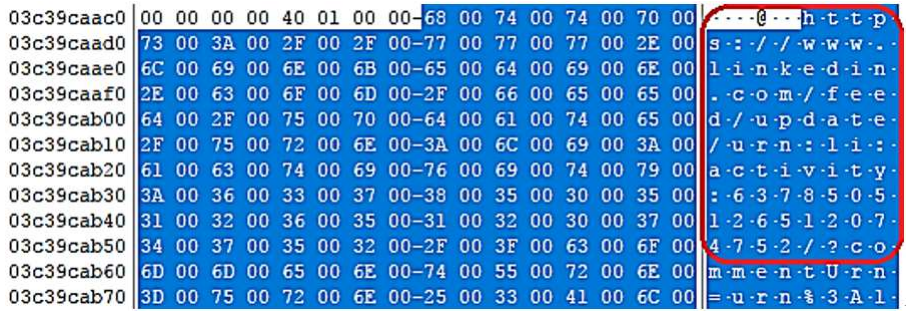

Figure 2: The evidence of post creation was found

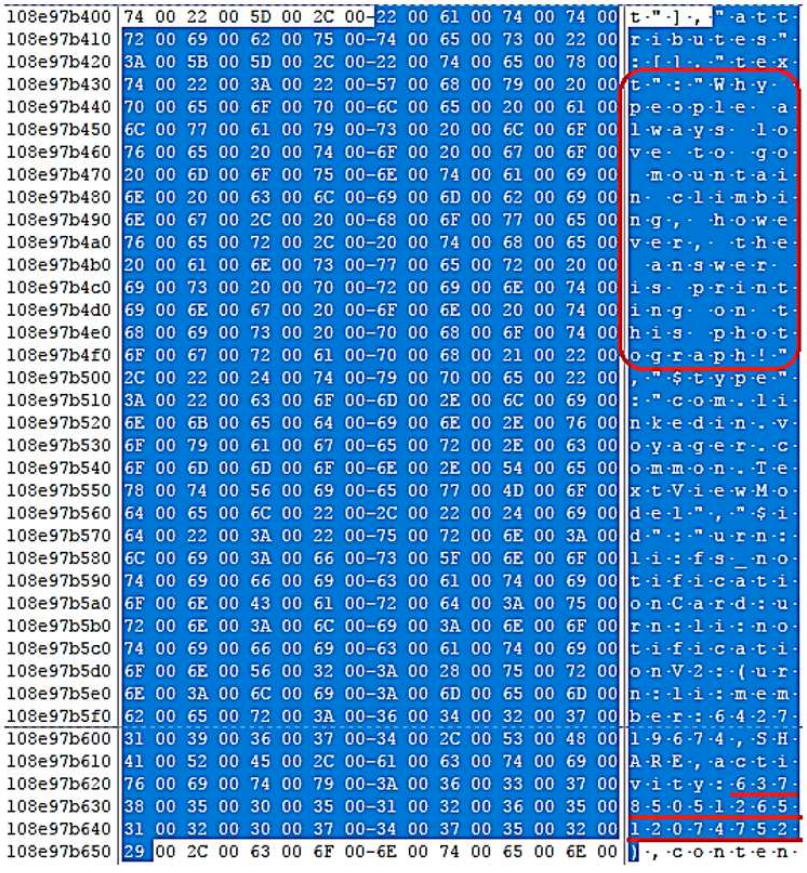

Figure 3: Post content was found by searching key string

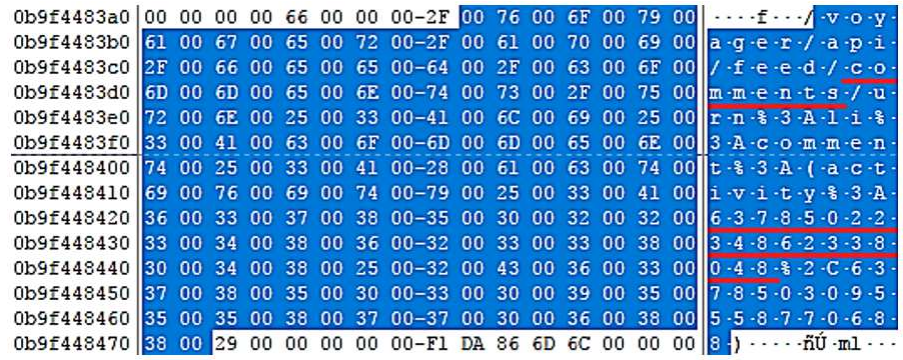

Figure 4: The evidence of comment creation was found by searching keyword "comment"

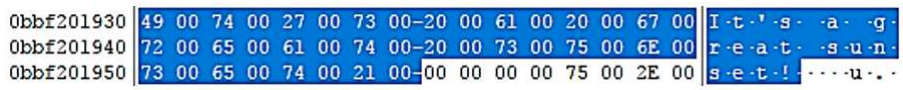

Figure 5: Post content was found by searching key string

Figure 6: The evidence of chat record

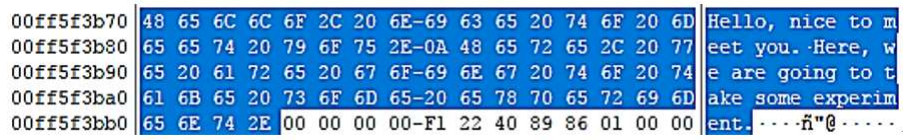

Figure 7: The evidence of chat content

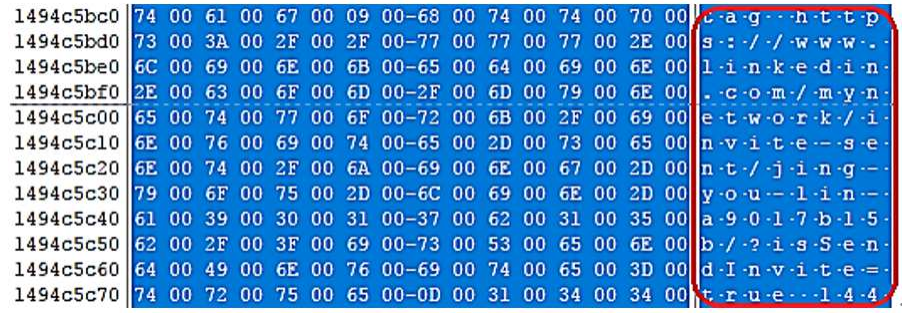

Figure 8: The evidence of friend request

To sum up, the evidence we found in the memory is quite the same in the hard disk. In the part of memory, we also found login information, the evidence of post creation, making comments, chatting records, clicking "Like" records and so on. Therefore, there is no difference between in the hard disk and in the memory that evidences we found on the Mozilla Firefox browser.

4.3 Findings: Scenario 3: Microsoft Edge

In scenario 3, we also aim to the hard disk and memory forensics. We did the same thing as the previous scenarios did. However, the forensic target in this scenario is different from the previous two scenarios. In scenario 3, we did the experiment on the Microsoft Edge browser.

4.3.1 Account and Password

In Microsoft Edge, we can find user account and password information by looking for the string in reverse searching. By typing account string and password string, we can see there is a key string "www.linkedin.com" in the context. Therefore, we can easily realize that the user must have been used this computer to perform LinkedIn activities.

In the part of memory, the situation is the same as in the hard disk. We can find login account and password information by searching account string and password string directly.

4.3.2 Posting Evidence

As the same to the previous scenarios, every posting has it's unique post ID. Post ID is a string of numbers. When a user writes a post on the feed, the system will automatically assign a unique ID to the posting. The posting network address is often built in the form of "https://www.linkedin.com/feed/update/urn:li:activity: Post ID". In the hard disk, by searching the key string "https://www.linkedin.com/feed/update/urn:li:activity:", we can find the evidence of post creation. Therefore, we can match the post ID we found in the image file and the network address. If both of them are the same, we can definitely infer that they must have posted that article on the LinkedIn website in the past. Furthermore, we can find the content of posting by inverse searching.

In the part of memory, we can also find out the evidence of post creation and its contents by searching the key strings.

4.3.3 Making Comment Evidence

As the same to the previous scenarios, LinkedIn allows any people to make any comments on any articles. In the hard disk, by searching the keyword "comment", we can find out comment evidence that we made on the other user's posting.

In the part of memory, the situation is the same as in the hard disk, we can also find comment evidence and its content by searching the keyword "comment".

4.3.4 Chatting Records

As the same to the previous scenarios, the majority of chatting record network address is often built in the form of "https://www.linkedin.com/messaging/thread/Chat-ID". Therefore, by searching the key string "https://www.linkedin.com/messaging/thread/", we can easily find out the chatting record evidence as well. Furthermore, we can also find chatting content by looking for the key string in reverse searching.

In the part of memory, we can also find out chatting record evidence by searching the key string "https://www.linkedin.com/messaging/thread/", and find chatting content by looking for the key string in reverse searching.

4.3.5 Clicking "Like" Button Evidence

As the same to the previous scenarios, we can find out clicking "Like" evidence by searching the keyword "likes" no matter in the hard disk or in the memory.

4.3.6 Friend List and Friend Request

As the same to the previous scenarios, we can find out friend request evidence in the hard disk. The majority of friend-request format is often built in the form of "https://www.linkedin.com/mynetwork/invite-sent/Personal-ID/?isSendInvite=true". By searching the key string "https://www.linkedin.com/mynetwork/invite-sent/", we could easily understand whether the user had sent a friend request to other LinkedIn members or not. However, when we searched the key string "https://www.linkedin.com/mynetwork/invite-connect/connections/" in the hard disk, we cannot find out the friend list as well.

In the part of memory, we can also find out friend request evidence by searching the key string "https://www.linkedin.com/mynetwork/invite-sent/". However, we cannot find out friend list by searching the key string "https://www.linkedin.com/mynetwork/invite-connect/connections/" as well. To sum up, the evidence we found in the memory is quite the same in the hard disk. In the part of memory, we also found login information, the evidence of post creation, making comments, chatting records, clicking "Like" records and so on. Therefore, there is no difference between in the hard disk and in the memory that evidences we found on the Microsoft Edge browser.

4.4 Experiment Comparison

After we conducted these three scenarios, we drew a table to clearly comparing the difference between them. As shown in Table 1, we can realize that there is no difference between them. No matter the evidence stored in the hard disk or in the memory, the evidence we can find in the Google Chrome, in the Mozilla Firefox or in the Microsoft Edge were the same. Moreover, all the searching keywords

Table 1: The comparison of findings between browsers

Category / Activity	Google Chrome		Mozilla Firefox		Microsoft Edge	
	Hard Disk	Memory	Hard Disk	Memory	Hard Disk	Memory
Account	O	O	O	O	O	O
Password	—	—	O	O	O	O
Post evidence	O	O	O	O	O	O
Make comment evidence	O	O	O	O	O	O
Click "Like" button evidence	O	O	O	O	O	O
Chat records	O	O	O	O	O	O
Chat contents	O	O	O	O	O	O
Friend list	—	—	—	—	—	—
Friend request	O	O	O	O	O	O

O: Found —: None

or key strings are the same in the hard disk as compared in the memory. Therefore, the majority of evidence can be found in the hard disk and in the memory.

5 Conclusions

Nowadays, thanks to the rapid development of new technologies, thousands of new social networking sites have sprung up over the past few years, such as Facebook, Twitter, Instagram, and so on. However, there are still some problems we should concern, that is, various kinds of cybercrime emerge endlessly in recent years. In order to assist investigators to investigate cybercrimes, this paper proposes a forensic way to investigate a perpetrator who commits a crime via the LinkedIn social networking site on the computer. We did a series of user activities that users may operate it. All of these behaviors were conducted respectively on three different browsers, including Google Chrome, Mozilla Firefox, and Microsoft Edge. Moreover, these three different browsers were conducted respectively on three different clean computers.

After completing these procedures, we adopt a forensic tool called FTK Imager to create an image file for the hard disk. On the other hand, we adopt the MANDIANT tool to create an image file for the memory. Thereafter, in order not to influence the integrity of digital evidence, we make use of FTK Imager to analyze image files on the other clean computer. In our experiment, we can find many kinds of evidences, for example, post creation, comment creation, browsing evidence, chatting records, clicking the "Like" button on the other postings and so forth. Finally, we compare our findings between these three different browsers, as shown in Table 1.

All of the findings could be used for cybercrime investigation. The investigators can analyze preference or daily activities of a perpetrator based on important information. Furthermore, if computer crime happened, all of the evidences extracted and analyzed by the investigator could be a crucial admission on the court.

References

[1] A. Abhyankar, "Social networking sites," *SAMVAD*, vol. 2, pp. 28–21, 2011.

[2] Alexa, *Linkedin [Online]*, Apr. 2018. (`https://www.alexa.com/siteinfo/linkedin.com`)

[3] H. Arshad, A. Jantan, and E. Omolara, "Evidence collection and forensics on social networks: Research challenges and directions," *Digital Investigation*, vol. 28, pp. 126–138, 2019.

[4] K. K. Arthur and H. S. Venter, "An investigation into computer forensic tools," in *Proceedings of the ISSA Enabling Tomorrow Conference*, pp. 1–11, 2004.

[5] A. Azfar, K. K. R. Choo, and L. Lin, "An android social app forensics adversary model," in *The 49th Hawaii International Conference on System Sciences (HICSS'16)*, pp. 5597–5606, 2016.

[6] D. Boyd and N. Ellison, "Social network sites: Definition, history, and scholarship," *IEEE Engineering Management Review*, vol. 38, no. 3, pp. 16–31, 2010.

[7] Criminal Investigation Bureau, *2017 Cybercrime overview [Online]*, 2017. (`https://www.cib.gov.tw/Crime/Detail/981`)

[8] F. N. Dezfouli, B. Eterovic-Soric A. Dehghantanha, and K. K. R. Choo, "Investigating social networking applications on smartphones detecting Facebook, Twitter, Linkedin and Google+ Artefacts on Android and Ios platforms," *Australian Journal of Forensic Sciences*, vol. 48, pp. 469–488, 2016.

[9] C. Dwyer, S. Hiltz, and K. Passerini, "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace," in *Americas Conference on Information Systems (AMCIS'07)*, 2007. (`https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1849&context=amcis2007`)

[10] eBizMBA, *Top 15 Most Popular Social Networking Sites [Online]*, 2019. (`http://www.ebizmba.com/articles/social-networking-websites`)

[11] K. Jaishankar, "Cyber criminology as an academic discipline: History, contribution and impact," *Inter-*

national Journal of Cyber Criminology, vol. 12, no. 1, pp. 1–8, 2018.

[12] LinkedIn, *About US Statistics [online]*, 2018. (https://news.linkedin.com/about-us\#statistics)

[13] C. D. Marcum and G. E. Higgins, *Social Networking as a Criminal Enterprise*, pp. 49–144, 2014.

[14] N. A. Mutawa, I. Baggili, and A. Marrington, "Forensic analysis of social networking applications on mobile devices," *Digital Investigation*, vol. 9, pp. 24–33, 2012.

[15] Ministry of the Interior Republic of China National Police Agency, *The Cybercrime Rate in January to June, 2017 [online]*, 2017. (https://wsww.npa.gov.tw/NPAGip/wSite/ct?xItem=86451\&ctNode=12594\&mp=1)

[16] S. T. Neha, *Forensic analysis of WhatsApp on Android smartphones (master's thesis)*, 2013. (https://scholarworks.uno.edu/cgi/viewcontent.cgi?article=2736&context=td)

[17] Account Restricted, *Linkedin Help Center [Online]*, 2018. (https://www.linkedin.com/help/linkedin?lang=en)

[18] P. Stephenson, "The right tools for the job," *Digital Investigation*, vol. 1, no. 1, pp. 24–27, 2004.

[19] Wikipedia, *Linkedin [Online]*, 2019. (https://en.wikipedia.org/wiki/LinkedIn)

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.