Scholars Journal of Engineering and Technology (SJET)
Sch. J. Eng. Tech., 2017; 5(10):561-570
©Scholars Academic and Scientific Publisher
(An International Publisher for Academic and Scientific Resources)
www.saspublishers.com

ISSN 2321-435X (Online)
ISSN 2347-9523 (Print)

Computer Forensics of Dcard Application on Windows 10

Ching-Yu Lin[1], Ming-Sang Chang[2*]
[1,2]Department of Information Management, Central Police University, Taoyuan, Taiwan

***Corresponding author**
Ming-Sang Chang

Article History
Received: 17.10.2017
Accepted: 25.10.2017
Published: 30.10.2017

DOI:
10.36347/sjet.2017.v05i10.006

Abstract: Nowadays, with the great popularity of social networking sites, many people have gradually changed their way of living habits. There are varied social networking sites coming out, such as Facebook, Twitter, Instagram, YouTube, Dcard and so on. 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. Thanks to the cyber worlds are flourishing, there are several kinds of crimes emerge in endlessly in recent years. This paper focuses on the computer forensics of Dcard application by running on two different browsers, including Google Chrome and Microsoft Edge. They are running respectively under windows 10 operating systems. In this paper, we strive to search the digital evidence that user has been done on the computer. We make good use of authoritative computer forensic tools to obtain significant evidences and analyze the correlation between these evidences in detail. Besides, this paper finds that which behavior of suspect will leave what kind of evidence in the computer. These findings could be an important reference for law enforcement agency to investigate the computer crime.

Keywords: social networking sites, computer forensics, crime investigation, Dcard

INTRODUCTIOIN

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 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 [2]. Furthermore, social networking sites can connect people and maintain relationships from all parts of their lives [3]. 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 a frequent daily activities.

Due to the advance of technology, the type of crime is getting much more complexity than before. At present, the traditional crime is on the decrease. In other words, the 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, the 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, the cybercrime is definitely different to the traditional crime. The following shows the characteristics of cybercrime [4]:

- Making use of the computer characteristics to commit the crime.
- High dark figure of crime.
- The time and dimension features between crime behaviors and crime results.
- Take computer as a crime scene.
- Take 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 [5]. This will cause wide range harm to the 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 [6]. Over the past few years, various kinds of cyber criminals 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 [7]. Therefore, we can realize that the social networking websites have seriously become a hotbed of cybercrimes based on these significant literatures.

According to the survey of eBizMBA, popular social networking sites are prevalent nowadays, such as Facebook, Twitter, Instagram, and YouTube and so on [8]. Many of them have over than one million members, a quite large number for the time. As for various social networking sites, there are still a lot of outstanding social networking sites in Taiwan, such as Dcard, Plurk, Pixnet, Xuite and so forth. It is worth noting a thing, the young people between at the age of twelve and twenty-four, the visiting ratio of YouTube, Instagram, PPT and Dcard is far higher than the other age people. This situation shows that the Dcard is gradually famous for the Taiwan college students. Online Word-of-Mouth i-Buzz [9] indicates that the public praise of Dcard websites has been increased to three times as compared with last year. According to the statistics from 2015 to 2016, the number of the titles has been grown from 451,789 to 491,089. The growth rate has already increased 8.7 percentages. On the other hand, the number of the responses has been grown from 11,624,479 to 13,111,043. The growth rate has increased 12.8 percentages as well [10]. The registration members have over than one million people. The average of posts and articles are created per every ten seconds. However, there are two factors that make the Dcard website successful, the privacy and the anonymity. Consequently, we can observe that Dcard will be the mainstream of the social networking sites without dispute in the near feature.

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

RELATED WORK

Dcard Social Networking Site

Dcard is a well-known social networking site service for college students in Taiwan. Dcard website was launched by Chin Yu, Chien on December 16, 2011 [11]. According to the survey of Alexa, Dcard was ranked 26th relative to other websites in Taiwan and 1,050th relative to other websites in the world [12]. The participants of Dcard is only for college students, therefore, the survey reveals important information for us that the market share rate is still very high. On the other hand, Dcard permitted more college students to register it last year. Up to now, there are 169 universities participating in the Dcard in Taiwan. In consequence, we guess the Dcard website will come out on top in the next few years. Recently, Dcard provides an advanced service, allowing foreign students of other countries to participate in the activities of Dcard social networking sites. There are some basic functions of Dcard. Dcard allows users to write a post in order to share their daily activities or express their feelings with other users. Other users can also make any comments with anonymity on its news feed. However, one of its advantages is anonymity. When you post an article on the news feed, nobody knows who you are. Thanks to this advantage of Dcard, it would easily cause a person with bad intentions to commit a computer crime. Therefore, as for the computer crime investigation, it is difficult for investigators to investigate a computer crime because of its anonymity characteristic. Besides, Dcard allows users to chat with friends in the chat room. However, they cannot chat with strangers. They can just only chat with friends they added. In the midnight, college students can draw a card to make a chance for meeting a new friend. If both of them like each other and send the friend request to each other, then they can be good friends on their personal account. Otherwise, they will no longer meet with each other on the Dcard. This is one goal of Dcard, let all the college students in Taiwan have a chance to acquaint with each other.

However, there are many kinds of literatures focus on the forensic analysis of social networking sites nowadays. Abdullah Azfar, et al. proposed the utility model for the evidence extraction of five social networking applications, including Twitter, POF Dating, Snapchat, Fling and Pinterest [13]. Thakur focused on the forensic analysis of WhatsApp application on storage devices and volatile memory [14]. Mutawa et al. focused on the forensic analysis of three popular social networking sites, including Facebook, Twitter and Myspace [15]. Nevertheless, the technical literature about Dcard forensics is relatively scarce. From the point of this view, this paper focuses on the evidence extraction and crime analysis of Dcard application. This paper studies the behavior of the user who login into the Dcard from different browsers. We strive to extract the evidence of creating posts, 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 the correlation amid these evidences and discusses the how these evidences can help law enforcement agencies to investigate a crime.

Tools

There are a lot of forensic tools on the markets today. The mainstream of digital forensic products such as Autopsy, Forensic Toolkit and EnCase forensic have support computer 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 in order to extract and analyze the data generated by Dcard website. With the advanced development of forensic tools, the forensic tools and techniques should keep investigators ahead of the criminals [16].

K.K. Arthur et al. conducted an investigation into some of forensic tools, including PC Inspector File Recovery, En Case, Forensic Toolkit and FTK Imager. However, the main function of FTK Imager is to view and to image storage devices [17]. In light of these advantages, we adopt Access Data FTK Imager V4.1.1 to create an image file for the hard disk. Forensic Toolkit is computer forensics software made by Access Data. It scans a hard disk searching for various types of information. The toolkit comprises a standalone disk image 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 the physical memory for the sake of achieving memory forensics. Therefore, this paper adopts MANDIANT tool to create an image file for the memory. MANDIANT is an open source tool which can be downloaded on the Internet. There are 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 in the computer.
- HookDetection.bat: This batch file is used to list which hooks file is executing in 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 corporation 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.

METHODOLOGY

Research Goal

The study described in this paper has been performed by a serious of processes, each one referring to a specific scenario. In the experiment, we login into the Dcard websites via two different browsers. All of these operations are executed under Windows 10 operating system. After we login into the Dcard websites, we do a series of same behaviors, for example, login to the account, adding friends, chatting with friends, writing posts, making comments, clicking “Like” button, clicking “collect” button and so forth. Afterwards, 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.

Experiment Elaboration

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

Scenario 1: Google Chrome

In the scenario 1, all the operations were conducted via Google Chrome browser. We entered the personal account and password to login into the Dcard website. After login into the Dcard website, we wrote a post and uploaded the pictures. Moreover, we did a lot of user common behaviors, for example, adding friends, chatting with friends, making comments, clicking "Like" button, clicking "Collect" button, browsing other users' articles and so forth. On the other hand, we also let others users make any comments on our posting, click "Like" button for our posting, click "Collect" button for our posting and follow our posting. After we did these behaviors, we did not do anything anymore. We created the image files for the hard disk and memory respectively. Thereafter, we adopted Forensic Toolkit Imager to extract and analyze the digital evidence.

Scenario 2: Microsoft Edge

In the scenario 2, all the operations were conducted via Microsoft Edge browser. We entered the personal account and password to login into the Dcard website. After login into the Dcard website, we wrote a post and uploaded the pictures. Moreover, we did a lot of user common behaviors, for example, adding friends, chatting with friends, making comments, clicking "Like" button, clicking "Collect" button, browsing other users' articles and so forth. On the other hand, we also let others users make any comments on our posting, click "Like" button for our posting, click "Collect" button for our posting and follow our posting. After we did these behaviors, we did not do anything anymore. We created the image files for the hard disk and memory respectively. Thereafter, we adopted Forensic Toolkit Imager to extract and analyze the digital evidence.

RESULTS AND FINDINGS

We login into the Dcard website by entering the email account and password on the computer. Afterwards, we execute a series of processes, for example, writing a post, chatting with friends, making comments, adding friends and so on. After executing these normal behaviors, we create an image files for the hard disk and memory. We separate the analysis into two parts, hard disk and memory. We make use of one practical function of FTK Imager to quickly search the keyword. The followings are the analysis and the description of forensic results according to the previous scenarios we mentioned.

Findings: Scenario 1: Google Chrome

Account and password

In the hard disk, there are various kinds of evidence we can extract. First, when we searched the key string "www.dcard.tw", we found some important information. By analyzing its contexts, we can infer that the user has used Google Chrome to browse the Dcard website. On the other hand, we also found out the user account information by searching the key string "www.dcard.tw/login". As shown in the Fig. 1(a), we can see there is a key string "www.dcard.tw/loginemail". This key string reveals us an important information the login e-mail account and password. Unfortunately, we can't find out the password information because the text of password was garbled. We cannot comprehend its meaning by our intuition. Therefore, we infer that the password may be encrypted. In the memory, we can only find out the login account information. The password was also garbled. We cannot comprehend its meaning by our intuition.

Posting evidence

Every posting has its classification and its post ID. The post ID is a unique string of number. The classification can be divided into several groups, such as boyslove, fitness, relationship, girl, makeup, dressup, entertainer, sport, funny, vehicle, talk, marvel, horoscopes, food, pet, handicrafts, trending, mood, movie, music, game, boy, photography, job, travel, book, language, abroad, literature, exam, course, sex, and so on. When a user writes a post on the Dcard, the system will automatically assign a unique ID and classify its category to the posting, for example, www.dcard.tw/f/photography/p/227017698. The photography is a classification and 227017698 is a post ID. Therefore, we can easily realize that the majority of posting network address is often built in the form of "www.dcard.tw/f/*classification*/p/*post ID*". In the hard disk, by searching the keyword "postCreated", we can find out the creating evidence and creating date of posting, as shown in the Fig. 1(b). There is a post ID combined with keyword "postCreated". Therefore, we can match the post ID we found in the FTK Imager and the network address. If both of them are the same, we can definitely infer that they must have posted that article on the Dcard website in the past. Moreover, we also found the posting title and its contents by searching the key string. In the memory, we can also find out the creating evidence and creating date of posting by searching the keyword "postCreated". Moreover, we can also find out the posting title and its contents by searching the key string.

Making comment evidence

On the other hand, Dcard allows any people to make any comments on any articles with anonymity. In the hard disk, by searching the key string, we can find out the comment evidence that any other users made on my own posting. However, we can just find out the leaving messaging only. We cannot find out the user's

ID who left messages on the posting. We guess that the ID may be hidden by the website because of its anonymity characteristic. Therefore, we actually don't know who makes comments on the posting. On the contrary, by searching the key string, we can find out the comment evidence that we made on the other user's posting as well. As same as previous situation, we cannot extract the user's ID. In the memory, the situation is the same as in the hard disk, we can also find out the comment evidence by searching the string. Nevertheless, we cannot find out the user's ID who left messages on the posting.

Browsing evidence

When a user browsed the other users' posting, the local device would record browsing history in the hard disk. All of the browsing behaviors would leave browsing evidence in the hard disk. Therefore, when we search the keyword "postViewed", there is an obvious post ID we can see in the contexts. By examining the post ID, we can easily realize that the user must have browsed that posting in the past. If the post ID is same to my own post ID, this situation represents that I have browsed my own posting in the past. On the contrary, if the post ID is different to my own post ID, this situation represents that I have browsed the other users' posting in the past. In the memory, we can also find out the browsing evidence by searching the keyword "postViewed". We can realize a user's preference by examining this kind of evidence.

Chatting records

In the hard disk, we can as well extract the chatting record evidence. Every user has their personal ID which was assigned when their personal account was created. Moreover, this ID is unique to every user. When the user chatted with friends, the network address of chatting page would show the friend's ID, for example, www.dcard.tw/messages/2027586. The "messages" represents the user must have chatted with friend in the past. The 2027586 is an ID of friends. As a result, we can realize that the user must have chatted with friend 2027586 in the past. Therefore, we can easily understand that the majority of chatting record network address is often built in the form of "www.dcard.tw/messages/*personal ID*". By searching the key string "www.dcard.tw/messages/", we can easily find out the chatting record evidence, as shown in the Fig. 1(c). Furthermore, we can also find out the chatting contents evidence by searching the key string. In the memory, we can also find out the chatting record evidence by searching the key string "www.dcard.tw/messages/". Also, we can find out the chatting contents evidence by searching the key string.

Clicking "Like" button evidence

There is a function on the Dcard website called "Like". If people like an article, they may click "Like" button on that article. In the hard disk, we can find out the clicking "Like" evidence by searching the keyword "postLiked". In the memory, we can also find out the clicking "Like" evidence by searching the keyword "postLiked". As a result, by analyzing the clicking "Like" evidence, the investigator can easily realize the preference of a perpetrator.

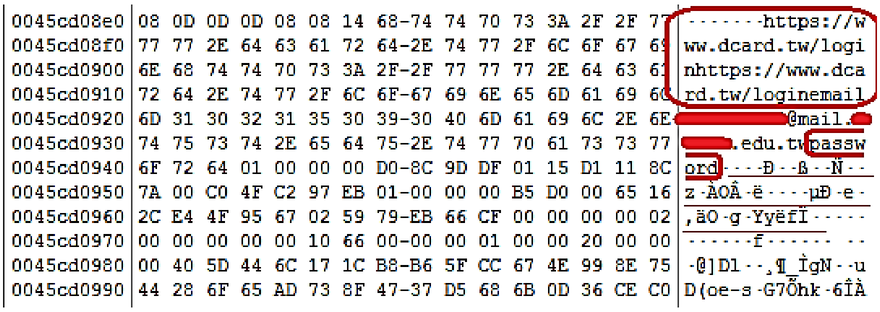
Clicking "Collect" button evidence

In addition, there is also a function on the Dcard website called "Collect". If people like an article, they can click "Collect" button to collect this article in their personal page. After that, they can view the posting they like in their personal page at any time. In the hard disk, we found the clicking "Collect" evidence by searching the keyword "postCollected". In the memory, we can also find out the clicking "Collect" evidence by searching the keyword "postCollected". Therefore, by analyzing the clicking "Collect" evidence, the investigator can also realize the preference of a perpetrator.

Friend list and friend request

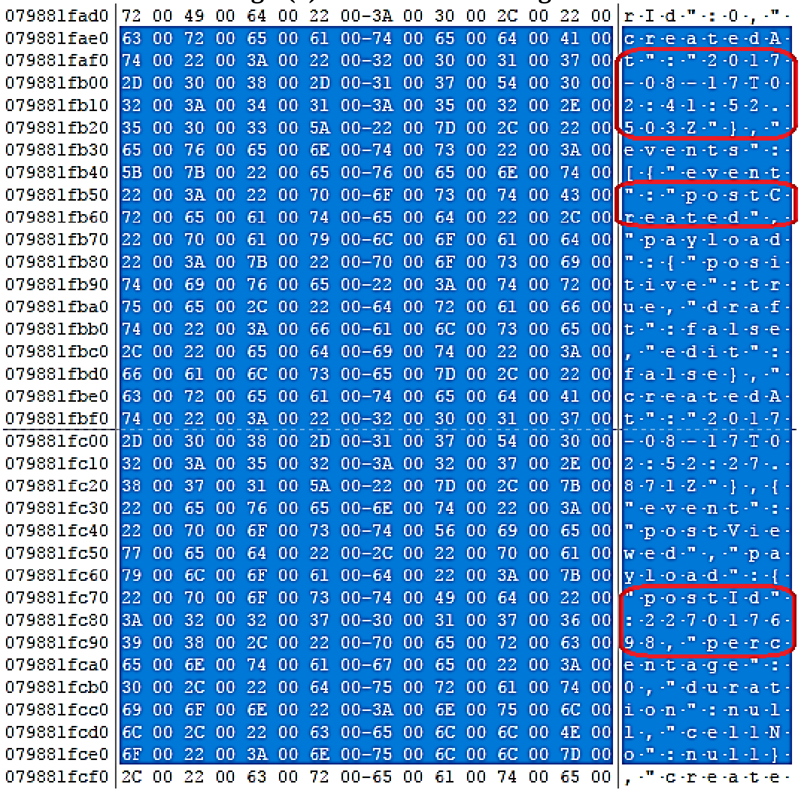
However, when we searched the keyword in the hard disk and in the memory, for example, "friend request", "request", "www.dcard.tw/my/friends", "www.dcard.tw/my/following" and so on, this paper cannot find out the friend request, friend list and the following list evidence in the Google Chrome browser.

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



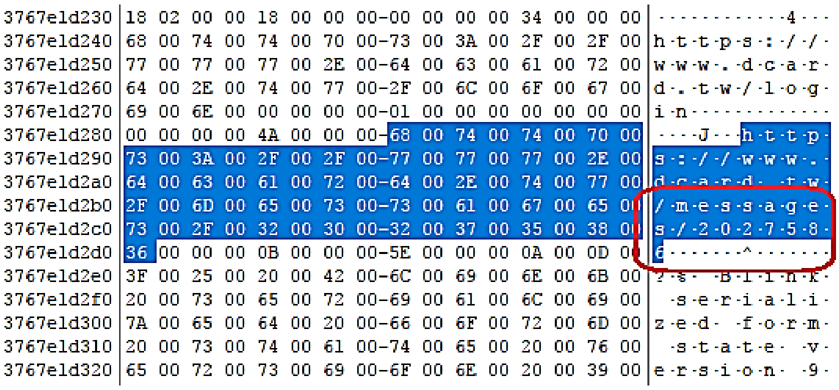
```
0045cd08e0 08 0D 0D 0D 08 08 14 68-74 74 70 73 3A 2F 2F 77 ·······https://w
0045cd08f0 77 77 2E 64 63 61 72 64-2E 74 77 2F 6C 6F 67 69 ww.dcard.tw/logi
0045cd0900 6E 68 74 74 70 73 3A 2F-2F 77 77 77 2E 64 63 61 nhttps://www.dca
0045cd0910 72 64 2E 74 77 2F 6C 6F-67 69 6E 65 6D 61 69 6C rd.tw/loginemail
0045cd0920 6D 31 30 32 31 35 30 39-30 40 6D 61 69 6C 2E 6E [redacted]@mail.[redacted]
0045cd0930 74 75 73 74 2E 65 64 75-2E 74 77 70 61 73 73 77 [redacted].edu.twpassw
0045cd0940 6F 72 64 01 00 00 00 D0-8C 9D DF 01 15 D1 11 8C ord····Đ··ß··Ñ··
0045cd0950 7A 00 C0 4F C2 97 EB 01-00 00 00 B5 D0 00 65 16 z·ÀOÂ·ë····µĐ·e·
0045cd0960 2C E4 4F 95 67 02 59 79-EB 66 CF 00 00 00 00 02 ,äO·g·YyëfÏ·····
0045cd0970 00 00 00 00 00 10 66 00-00 00 01 00 00 20 00 00 ······f······ ··
0045cd0980 00 40 5D 44 6C 17 1C B8-B6 5F CC 67 4E 99 8E 75 ·@]Dl··¸¶_ÌgN··u
0045cd0990 44 28 6F 65 AD 73 8F 47-37 D5 68 6B 0D 36 CE C0 D(oe-s·G7Õhk·6ÎÀ
```

Fig-1(a): The evidence of login



```
079881fad0 72 00 49 00 64 00 22 00-3A 00 30 00 2C 00 22 00 r·I·d·"·:·0·,·"·
079881fae0 63 00 72 00 65 00 61 00-74 00 65 00 64 00 41 00 c·r·e·a·t·e·d·A·
079881faf0 74 00 22 00 3A 00 22 00-32 00 30 00 31 00 37 00 t·"·:·"·2·0·1·7·
079881fb00 2D 00 30 00 38 00 2D 00-31 00 37 00 54 00 30 00 -·0·8·-·1·7·T·0·
079881fb10 32 00 3A 00 34 00 31 00-3A 00 35 00 32 00 2E 00 2·:·4·1·:·5·2·.·
079881fb20 35 00 30 00 33 00 5A 00-22 00 7D 00 2C 00 22 00 5·0·3·Z·"·}·,·"·
079881fb30 65 00 76 00 65 00 6E 00-74 00 73 00 22 00 3A 00 e·v·e·n·t·s·"·:·
079881fb40 5B 00 7B 00 22 00 65 00-76 00 65 00 6E 00 74 00 [·{·"·e·v·e·n·t·
079881fb50 22 00 3A 00 22 00 70 00-6F 00 73 00 74 00 43 00 "·:·"·p·o·s·t·C·
079881fb60 72 00 65 00 61 00 74 00-65 00 64 00 22 00 2C 00 r·e·a·t·e·d·"·,·
079881fb70 22 00 70 00 61 00 79 00-6C 00 6F 00 61 00 64 00 "·p·a·y·l·o·a·d·
079881fb80 22 00 3A 00 7B 00 22 00-70 00 6F 00 73 00 69 00 "·:·{·"·p·o·s·i·
079881fb90 74 00 69 00 76 00 65 00-22 00 3A 00 74 00 72 00 t·i·v·e·"·:·t·r·
079881fba0 75 00 65 00 2C 00 22 00-64 00 72 00 61 00 66 00 u·e·,·"·d·r·a·f·
079881fbb0 74 00 22 00 3A 00 66 00-61 00 6C 00 73 00 65 00 t·"·:·f·a·l·s·e·
079881fbc0 2C 00 22 00 65 00 64 00-69 00 74 00 22 00 3A 00 ,·"·e·d·i·t·"·:·
079881fbd0 66 00 61 00 6C 00 73 00-65 00 7D 00 2C 00 22 00 f·a·l·s·e·}·,·"·
079881fbe0 63 00 72 00 65 00 61 00-74 00 65 00 64 00 41 00 c·r·e·a·t·e·d·A·
079881fbf0 74 00 22 00 3A 00 22 00-32 00 30 00 31 00 37 00 t·"·:·"·2·0·1·7·
079881fc00 2D 00 30 00 38 00 2D 00-31 00 37 00 54 00 30 00 -·0·8·-·1·7·T·0·
079881fc10 32 00 3A 00 35 00 32 00-3A 00 32 00 37 00 2E 00 2·:·5·2·:·2·7·.·
079881fc20 38 00 37 00 31 00 5A 00-22 00 7D 00 2C 00 7B 00 8·7·1·Z·"·}·,·{·
079881fc30 22 00 65 00 76 00 65 00-6E 00 74 00 22 00 3A 00 "·e·v·e·n·t·"·:·
079881fc40 22 00 70 00 6F 00 73 00-74 00 56 00 69 00 65 00 "·p·o·s·t·V·i·e·
079881fc50 77 00 65 00 64 00 22 00-2C 00 22 00 70 00 61 00 w·e·d·"·,·"·p·a·
079881fc60 79 00 6C 00 6F 00 61 00-64 00 22 00 3A 00 7B 00 y·l·o·a·d·"·:·{·
079881fc70 22 00 70 00 6F 00 73 00-74 00 49 00 64 00 22 00 "·p·o·s·t·I·d·"·
079881fc80 3A 00 32 00 32 00 37 00-30 00 31 00 37 00 36 00 :·2·2·7·0·1·7·6·
079881fc90 39 00 38 00 2C 00 22 00-70 00 65 00 72 00 63 00 9·8·,·"·p·e·r·c·
079881fca0 65 00 6E 00 74 00 61 00-67 00 65 00 22 00 3A 00 e·n·t·a·g·e·"·:·
079881fcb0 30 00 2C 00 22 00 64 00-75 00 72 00 61 00 74 00 0·,·"·d·u·r·a·t·
079881fcc0 69 00 6F 00 6E 00 22 00-3A 00 6E 00 75 00 6C 00 i·o·n·"·:·n·u·l·
079881fcd0 6C 00 2C 00 22 00 63 00-65 00 6C 00 6C 00 4E 00 l·,·"·c·e·l·l·N·
079881fce0 6F 00 22 00 3A 00 6E 00-75 00 6C 00 6C 00 7D 00 o·"·:·n·u·l·l·}·
079881fcf0 2C 00 22 00 63 00 72 00-65 00 61 00 74 00 65 00 ,·"·c·r·e·a·t·e·
```

Fig-1(b): The evidence of writing a post



```
3767e1d230 18 02 00 00 18 00 00 00-00 00 00 00 34 00 00 00 ············4···
3767e1d240 68 00 74 00 74 00 70 00-73 00 3A 00 2F 00 2F 00 h·t·t·p·s·:·/·/·
3767e1d250 77 00 77 00 77 00 2E 00-64 00 63 00 61 00 72 00 w·w·w·.·d·c·a·r·
3767e1d260 64 00 2E 00 74 00 77 00-2F 00 6C 00 6F 00 67 00 d·.·t·w·/·l·o·g·
3767e1d270 69 00 6E 00 00 00 00 00-01 00 00 00 00 00 00 00 i·n·············
3767e1d280 00 00 00 00 4A 00 00 00-68 00 74 00 74 00 70 00 ····J···h·t·t·p·
3767e1d290 73 00 3A 00 2F 00 2F 00-77 00 77 00 77 00 2E 00 s·:·/·/·w·w·w·.·
3767e1d2a0 64 00 63 00 61 00 72 00-64 00 2E 00 74 00 77 00 d·c·a·r·d·.·t·w·
3767e1d2b0 2F 00 6D 00 65 00 73 00-73 00 61 00 67 00 65 00 /·m·e·s·s·a·g·e·
3767e1d2c0 73 00 2F 00 32 00 30 00-32 00 37 00 35 00 38 00 s·/·2·0·2·7·5·8·
3767e1d2d0 36 00 00 00 0B 00 00 00-5E 00 00 00 0A 00 0D 00 6·······^·······
3767e1d2e0 3F 00 25 00 20 00 42 00-6C 00 69 00 6E 00 6B 00 ?·%· ·B·l·i·n·k·
3767e1d2f0 20 00 73 00 65 00 72 00-69 00 61 00 6C 00 69 00  ·s·e·r·i·a·l·i·
3767e1d300 7A 00 65 00 64 00 20 00-66 00 6F 00 72 00 6D 00 z·e·d· ·f·o·r·m·
3767e1d310 20 00 73 00 74 00 61 00-74 00 65 00 20 00 76 00  ·s·t·a·t·e· ·v·
3767e1d320 65 00 72 00 73 00 69 00-6F 00 6E 00 20 00 39 00 e·r·s·i·o·n· ·9·
```

Fig-1(c): The evidence of chatting record.

Findings: Scenario 2: Microsoft Edge

In the 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 to the previous scenario. In the scenario 2, we did the experiment on the Microsoft Edge browser.

Account and password

As the same to the previous scenario, in the hard disk, when we searched the key string “www.dcard.tw” and analyzed its context, we can observe that the user has used Microsoft Edge to browse the Dcard website. On the other hand, we also found out the user account information by searching the key string “www.dcard.tw/login”, as shown in the Fig. 2(a). Unfortunately, when we strove to find out the password by searching the keyword “password”, “pwd” and so on, we can’t find out the password information in the hard disk. In the memory, the situation is the same, we can only find out the login account information. The password was still not found.

Posting evidence

As the same to the previous scenario, we can realize that the majority of posting network address is often built in the form of “www.dcard.tw/f/*classification*/p/*post ID*”. In the hard disk, by searching the keyword “postCreated”, we can find out the creating evidence and creating date of posting, as shown in the Fig. 2(b). There is a post ID combined with keyword “postCreated”. Therefore, we can match the post ID we found in the FTK Imager and the network address. If both of them are the same, we can definitely infer that they must have posted that article on the Dcard website in the past. Moreover, we also found out the posting title and its contents by searching the key string. In the memory, we can also find out the creating evidence and creating date of posting by searching the keyword “postCreated”. Moreover, we can also find out the posting title and its contents by searching the key string.

Making comment evidence

In the Microsoft Edge, we can also find out the comment evidence that any other users made on my own posting by searching the key string. However, as the same to the previous scenarios, we can just find out the leaving messaging only. We cannot find out the user’s ID who left messages on the posting. We guess that the ID may be hidden by the website because of its anonymity characteristic. Therefore, we actually don’t know who makes comments on the posting. On the contrary, by searching the key string, we can find out the comment evidence that we made on the other user’s posting as well. As same as the previous situation, we cannot extract the user’s ID. In the memory, the situation is the same as in the hard disk, we can also find out the comment evidence by searching the string. Nevertheless, we cannot find out the user’s ID who left messages on the posting.

Browsing evidence

As the same to the previous scenario, when a user browsed the other users’ posting, the local device would record browsing history in the hard disk. All of the browsing behaviors would leave browsing evidence in the hard disk. Therefore, when we search the keyword “postViewed”, there is an obvious post ID we can see in the contexts. By examining the post ID, we can easily realize that the user must have browsed that posting in the past. If the post ID is same to my own post ID, this situation represents that I have browsed my own posting in the past. On the contrary, if the post ID is different to my own post ID, this situation represents that I have browsed the other users’ posting in the past. In the memory, we can also find out the browsing evidence by searching the keyword “postViewed”. We can realize a user’s preference by examining this kind of evidence.

Chatting records

In the Microsoft Edge, we can as well extract the chatting record evidence in the hard disk. The majority of chatting record network address is often built in the form of “www.dcard.tw/messages/*personal ID*”. By searching the key string “www.dcard.tw/messages/”, we can easily find out the chatting record evidence, as shown in the Fig. 2(c). Furthermore, we can also find out the chatting contents evidence by searching the key string. In the memory, we can also find out the chatting record evidence by searching the key string “www.dcard.tw/messages/”. Also, we can find out the chatting contents evidence by searching the key string.

Clicking “Like” button evidence

With respect to the clicking “Like” function in the Microsoft Edge, we also found out the click “Like” evidence by searching the keyword “postLiked” in the hard disk. In the memory, we can also find out the clicking “Like” evidence by searching the keyword “postLiked”. As a result, by analyzing the clicking “Like” evidence, the investigator can easily realize the preference of a perpetrator.

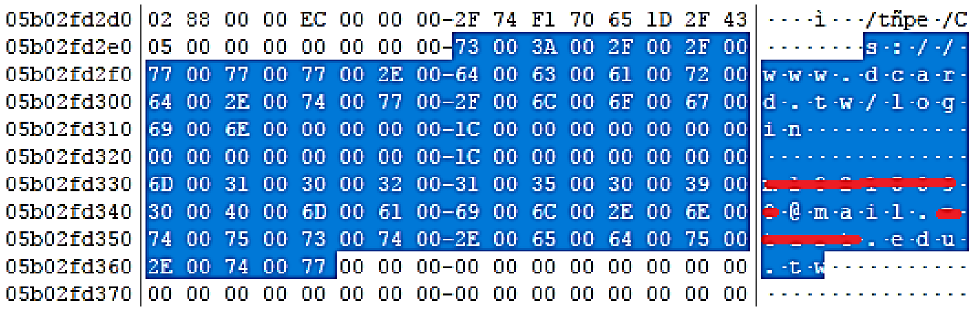
Clicking “Collect” button evidence

Moreover, as the users click “Collect” function in the Microsoft Edge, we also found out the click “Collect” evidence by searching the keyword “postCollected” in the hard disk. In the memory, we can also find out the clicking “Collect” evidence by searching the keyword “postCollected”. Therefore, by analyzing the clicking “Collect” evidence, the investigator can also realize the preference of a perpetrator.

Friend list and friend request

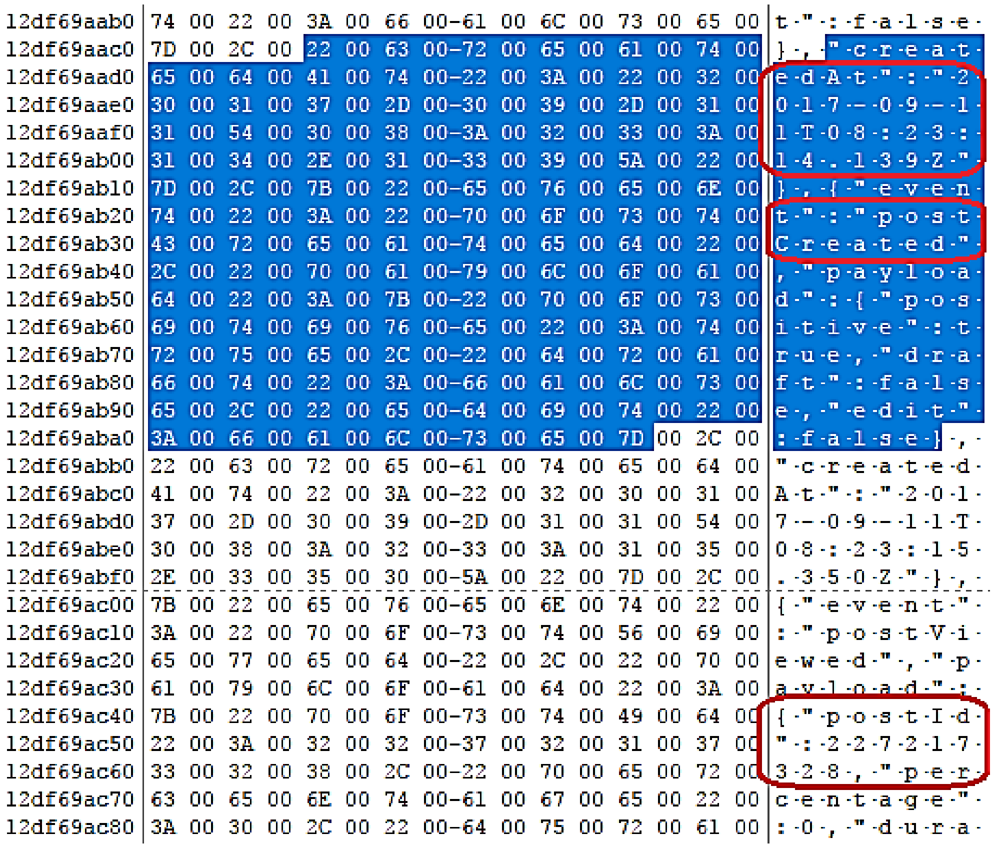
However, when we searched the keyword in the hard disk and in the memory, for example, “friend request”, “request”, “www.dcard.tw/my/friends”, “www.dcard.tw/my/following” and so on, we cannot find out the friend request, friend list and the following list evidence in the Microsoft Edge browser.

To sum up, as the same to the previous scenario, the evidence we found in the memory is quite the same in the hard disk. In the memory, we also found out the login information, the evidence of writing a post, browsing other postings, making comments, chatting with friends, clicking “Like” records, clicking “collect” records and so on. Therefore, there is no difference between hard disk and memory that the evidences we found on the Microsoft Edge browser.



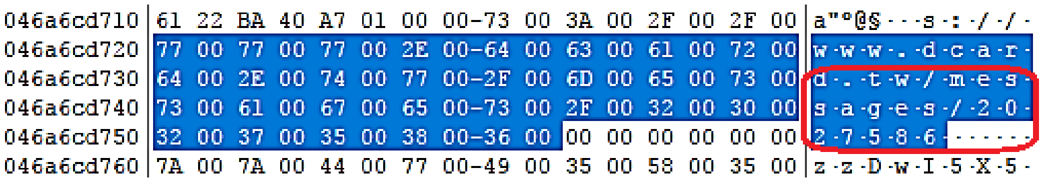
```
05b02fd2d0 02 88 00 00 EC 00 00 00-2F 74 F1 70 65 1D 2F 43  ····i···/tñpe·/C
05b02fd2e0 05 00 00 00 00 00 00 00-73 00 3A 00 2F 00 2F 00  ········s·:·/·/·
05b02fd2f0 77 00 77 00 77 00 2E 00-64 00 63 00 61 00 72 00  w·w·w·.·d·c·a·r·
05b02fd300 64 00 2E 00 74 00 77 00-2F 00 6C 00 6F 00 67 00  d·.·t·w·/·l·o·g·
05b02fd310 69 00 6E 00 00 00 00 00-1C 00 00 00 00 00 00 00  i·n·············
05b02fd320 00 00 00 00 00 00 00 00-1C 00 00 00 00 00 00 00  ················
05b02fd330 6D 00 31 00 30 00 32 00-31 00 35 00 30 00 39 00  [redacted]·
05b02fd340 30 00 40 00 6D 00 61 00-69 00 6C 00 2E 00 6E 00  [redacted]·@·m·a·i·l·.·[redacted]·
05b02fd350 74 00 75 00 73 00 74 00-2E 00 65 00 64 00 75 00  [redacted].·e·d·u·
05b02fd360 2E 00 74 00 77 00 00 00-00 00 00 00 00 00 00 00  .·t·w···········
05b02fd370 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
```

Fig-2(a): The evidence of login



```
12df69aab0 74 00 22 00 3A 00 66 00-61 00 6C 00 73 00 65 00  t·"·:·f·a·l·s·e·
12df69aac0 7D 00 2C 00 22 00 63 00-72 00 65 00 61 00 74 00  }·,·"·c·r·e·a·t·
12df69aad0 65 00 64 00 41 00 74 00-22 00 3A 00 22 00 32 00  e·d·A·t·"·:·"·2·
12df69aae0 30 00 31 00 37 00 2D 00-30 00 39 00 2D 00 31 00  0·1·7·-·0·9·-·1·
12df69aaf0 31 00 54 00 30 00 38 00-3A 00 32 00 33 00 3A 00  1·T·0·8·:·2·3·:·
12df69ab00 31 00 34 00 2E 00 31 00-33 00 39 00 5A 00 22 00  1·4·.·1·3·9·Z·"·
12df69ab10 7D 00 2C 00 7B 00 22 00-65 00 76 00 65 00 6E 00  }·,·{·"·e·v·e·n·
12df69ab20 74 00 22 00 3A 00 22 00-70 00 6F 00 73 00 74 00  t·"·:·"·p·o·s·t·
12df69ab30 43 00 72 00 65 00 61 00-74 00 65 00 64 00 22 00  C·r·e·a·t·e·d·"·
12df69ab40 2C 00 22 00 70 00 61 00-79 00 6C 00 6F 00 61 00  ,·"·p·a·y·l·o·a·
12df69ab50 64 00 22 00 3A 00 7B 00-22 00 70 00 6F 00 73 00  d·"·:·{·"·p·o·s·
12df69ab60 69 00 74 00 69 00 76 00-65 00 22 00 3A 00 74 00  i·t·i·v·e·"·:·t·
12df69ab70 72 00 75 00 65 00 2C 00-22 00 64 00 72 00 61 00  r·u·e·,·"·d·r·a·
12df69ab80 66 00 74 00 22 00 3A 00-66 00 61 00 6C 00 73 00  f·t·"·:·f·a·l·s·
12df69ab90 65 00 2C 00 22 00 65 00-64 00 69 00 74 00 22 00  e·,·"·e·d·i·t·"·
12df69aba0 3A 00 66 00 61 00 6C 00-73 00 65 00 7D 00 2C 00  :·f·a·l·s·e·}·,·
12df69abb0 22 00 63 00 72 00 65 00-61 00 74 00 65 00 64 00  "·c·r·e·a·t·e·d·
12df69abc0 41 00 74 00 22 00 3A 00-22 00 32 00 30 00 31 00  A·t·"·:·"·2·0·1·
12df69abd0 37 00 2D 00 30 00 39 00-2D 00 31 00 31 00 54 00  7·-·0·9·-·1·1·T·
12df69abe0 30 00 38 00 3A 00 32 00-33 00 3A 00 31 00 35 00  0·8·:·2·3·:·1·5·
12df69abf0 2E 00 33 00 35 00 30 00-5A 00 22 00 7D 00 2C 00  .·3·5·0·Z·"·}·,·
12df69ac00 7B 00 22 00 65 00 76 00-65 00 6E 00 74 00 22 00  {·"·e·v·e·n·t·"·
12df69ac10 3A 00 22 00 70 00 6F 00-73 00 74 00 56 00 69 00  :·"·p·o·s·t·V·i·
12df69ac20 65 00 77 00 65 00 64 00-22 00 2C 00 22 00 70 00  e·w·e·d·"·,·"·p·
12df69ac30 61 00 79 00 6C 00 6F 00-61 00 64 00 22 00 3A 00  a·y·l·o·a·d·"·:·
12df69ac40 7B 00 22 00 70 00 6F 00-73 00 74 00 49 00 64 00  {·"·p·o·s·t·I·d·
12df69ac50 22 00 3A 00 32 00 32 00-37 00 32 00 31 00 37 00  "·:·2·2·7·2·1·7·
12df69ac60 33 00 32 00 38 00 2C 00-22 00 70 00 65 00 72 00  3·2·8·,·"·p·e·r·
12df69ac70 63 00 65 00 6E 00 74 00-61 00 67 00 65 00 22 00  c·e·n·t·a·g·e·"·
12df69ac80 3A 00 30 00 2C 00 22 00-64 00 75 00 72 00 61 00  :·0·,·"·d·u·r·a·
```

Fig-2(b): The evidence of writing a post



```
046a6cd710 61 22 BA 40 A7 01 00 00-73 00 3A 00 2F 00 2F 00  a"º@§···s·:·/·/·
046a6cd720 77 00 77 00 77 00 2E 00-64 00 63 00 61 00 72 00  w·w·w·.·d·c·a·r·
046a6cd730 64 00 2E 00 74 00 77 00-2F 00 6D 00 65 00 73 00  d·.·t·w·/·m·e·s·
046a6cd740 73 00 61 00 67 00 65 00-73 00 2F 00 32 00 30 00  s·a·g·e·s·/·2·0·
046a6cd750 32 00 37 00 35 00 38 00-36 00 00 00 00 00 00 00  2·7·5·8·6·······
046a6cd760 7A 00 7A 00 44 00 77 00-49 00 35 00 58 00 35 00  z·z·D·w·I·5·X·5·
```

Fig-2(c): The evidence of chatting record

Experiment Comparison

After we conducted these two scenarios, we drew a table to clearly comparing the difference between them.

As shown in the 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 or in the Microsoft Edge were the same. Moreover, all the searching keywords 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.

Table-1: The comparison of findings between two browsers.

	Google Chrome		Microsoft Edge	
	Hard Disk	Memory	Hard Disk	Memory
Account	Found	Found	Found	Found
Password	None	None	None	None
Posting evidence	Found	Found	Found	Found
Posting timestamp	Found	Found	Found	Found
Posting contents	Found	Found	Found	Found
Other users make comments on my posting	Found	Found	Found	Found
Making comments on other users' posting	Found	Found	Found	Found
The evidence of other user browses my posting	None	None	None	None
The evidence of browsing other users' posting	Found	Found	Found	Found
Other users click "Like" button on my posting	None	None	None	None
Clicking "Like" button on other users' posting	Found	Found	Found	Found
Other users click "Collect" button on my posting	None	None	None	None
Clicking "Collect" button on other users' posting	Found	Found	Found	Found
Chatting records	Found	Found	Found	Found
Chatting contents	Found	Found	Found	Found
Friend list	None	None	None	None
Friend request	None	None	None	None

CONCLUSIONS

Thousands of new social networking sites have sprung up over the past few years, such as Facebook, Twitter, Instagram, Dcard, Plurk and so on. Nowadays, thanks to the rapid development of new technologies, various kinds of cybercrime emerge endlessly. In order to assist investigators to investigate a cybercrime, this paper proposes a forensic way to investigate a perpetrator that commits a crime via Dcard social networking site on the computer. We did a series of normal behaviors that users may operate it. All of these behaviors were conducted respectively on two different browsers, including Google Chrome and Microsoft Edge. Moreover, these two different browsers were conducted respectively on two different clean computers.

After completing these procedures, we adopt a forensic tool called FTK Imager to create image file for the hard disk. On the other hand, we adopt MANDIANT tool to create image file for the memory. Thereafter, in order not to influence the integrity of digital evidence, we use FTK Imager to analyze the image files on the other clean computer. In our experiment, we can find many kinds of evidences, for example, writing a post, making comments, browsing evidence, chatting records, clicking "Like" button on the postings and so forth. Finally, we compare the findings between these two different browsers, as shown in the Table 1. All of findings can be used for the crime investigation. The investigators can analyze the preference or daily behaviors of a perpetrator based on this important information. Furthermore, if the computer crime happened, all of the evidences extracted and analyzed by the investigator can be a crucial admission on the court.

As a future work, we want to do another experiment on more different browsers and take mobile forensic for the Dcard application on the mobile phone. In this paper, our main goal is to extract the digital evidences for the Dcard from two different browsers on the real computer system. In this paper, we are not aim at the mobile forensic. Therefore, in order to make completion for different login methods on Dcard, we are going to do the experiment on the more browsers and mobile phone next.

REFERENCES

1. Abhyankar, Anjali. Social networking sites. SAMVAD. 2011;2: 18-21.
2. Dwyer C, Hiltz S, Passerini K. Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. AMCIS

2007 proceedings. 2007 Dec 31:339.
3. Ellison NB. Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication. 2007 Oct 1;13(1):210-30.
4. Criminal Investigation Bureau, https://www.cib.gov.tw/Crime/Detail/981, Access date: Jul. 20; 2017
5. Jaishankar K, editor. Cyber criminology: exploring internet crimes and criminal behavior. CRC Press; 2011 Feb 22.
6. Buçaj E. The Need for Regulation of Cyber Terrorism Phenomena in Line With Principles of International Criminal Law. Acta U. Danubius Jur.. 2017:140.
7. Marcum CD, Higgins GE, editors. Social Networking as a Criminal Enterprise. CRC Press; 2014 Apr 28.
8. Graber DA, Dunaway J. Mass media and American politics. Cq Press; 2017 Aug 8.
9. I-Buzz Research, http://www.i-buzz.com.tw/, Access date: Jul. 17, 2017
10. Brain, Forum ancestor PTT reflects the social values, the rising star Dcard becomes new base for youngers, http://www.brain.com.tw/news/articlecontent?ID=44582&sort=, Access date: Jul. 18, 2017
11. Wiki Dcard，2016.08, https://zh.wikipedia.org/wiki/Dcard, Access date: Jul. 22, 2017
12. Alexa, http://www.alexa.com/siteinfo/dcard.tw, Access date: Jul. 22, 2017
13. Azfar A, Choo KK, Liu L. An android social app forensics adversary model. InSystem Sciences (HICSS), 2016 49th Hawaii International Conference on 2016 Jan 5 (pp. 5597-5606). IEEE.
14. Thakur NS. Forensic analysis of WhatsApp on Android smartphones. (2013).
15. Al Mutawa N, Baggili I, Marrington A. Forensic analysis of social networking applications on mobile devices. Digital Investigation. 2012 Aug 31;9:S24-33.
16. Stephenson P. The right tools for the job. Digital Investigation. The International Journal of Digital Forensics and Incidence Response, Vol 1, No 1, 2004. pp 24-27.
17. Arthur KK, Venter HS. An Investigation into Computer Forensic Tools. InISSA 2004 Jun (pp. 1-11).