

Article

Online Social Snapshots of a Generic Facebook Session Based on Digital Insight Data for a Secure Future IT Environment

Hai-Cheng Chu ¹ and Jong Hyuk Park ^{2,*}

¹ Department of International Business, National Taichung University of Education, 140 Min-Shen Road, Taichung 40306, Taiwan; E-Mail: hcchu@mail.ntcu.edu.tw

² Department of Computer Science and Engineering, Seoul National University of Science and Technology, 172 Gongneung-dong 2, Nowon-gu 139-743, Korea

* Author to whom correspondence should be addressed; E-Mail: jhpark1@seoultech.ac.kr; Tel.: +82-2-970-6702; Fax: +82-2-977-9441.

Academic Editor: Neil Y. Yen

Received: 15 February 2015 / Accepted: 21 April 2015 / Published: 4 May 2015

Abstract: Physical memory acquisition has been an import facet for digital forensics (DF) specialists due to its volatile characteristics. Nowadays, thousands of millions of global participants utilize online social networking (OSN) mechanisms to expand their social lives, ranging from business-oriented purposes to leisure motivations. Facebook (FB) is one of the most dominant social networking sites (SNS) available today. Unfortunately, it has been a major avenue for cybercriminals to commit illegal activities. Therefore, the digital traces of previous sessions of an FB user play an essential role as the first step for DF experts to pursue the disclosure of the identity of the suspect who was exploiting FB. In this research work, we provide a systematic methodology to reveal a previous session of an FB identity, as well as his/her partial social circle via collecting, analyzing, preserving and presenting the associated digital traces to obtain the online social snapshots of a specific FB user who was utilizing a computing device with Internet Explorer (IE) 10 without turning off the power of the gadget. This novel approach can be a paradigm for how DF specialists ponder the crime scene to conduct the first response in order to avoid the permanent loss of the precious digital evidence in previous FB sessions. The hash values of the image files of the random access memory (RAM) of the computing device have proven to be identical before and after forensics operations, which could be probative evidence in a court of law.

Keywords: online social networking (OSN); Facebook; social networking site (SNS); cyberspace security forensics; volatile memory

1. Introduction

Evidently, mobile smart gadgets or traditional desktop computing devices are phenomenally exploited to access social media and cloud-based application programs, like Facebook (FB), Twitter, Snapchat, and others [1,2]. There are always some intangible digital traces accidentally left behind the scenes, where indecent behaviors might have been deliberately or unintentionally conducted. Therefore, digital forensics (DF) arises accordingly, encompassing business transaction fields to personal entertainment on websites. In this research, we apply DF along with systematic and scientific methodologies to data extraction from social networking sites (SNSs), which has become an imminently important research field. Substantively, the associated forensic data collection is tightly connected to social network operators. Unarguably, it is hard to retrieve the related digital evidence from them, especially in private sectors, which require search warrants or subpoenas. However, there are still some systematic methodologies that can be conducted concerning the neglected metamorphic digital traces when generic sessions of SNSs are launched [1,3,4]

State-of-the-art communication technologies have grown exponentially, both in positive and negative directions, acting as a double-edged sword. Cyber criminals are always exploiting them as the avenue to commit illegal activities in different fields. Obviously, collecting live digital artifacts is a stringent and imminent burden for DF specialists. Notwithstanding that there are some forensically-sound software suites available on the market, the acquisition of the physical memory, the random access memory (RAM), of the computing device requires extra effort. Within the RAM, incriminating evidence is often contained that could be acquired and analyzed by the examiner. In other words, the RAM is another repository of digital traces. Regrettably, RAM is volatile memory, the data of which will vanish when the power of the computing device is no longer sustained. Consequently, isolating volatile memory where digital evidence resides is crucial and decisive when information security leakage is investigated on the spot. Without loss of generality, the importance of conducting live memory acquisition in a forensically-sound manner, along with the associated digital trails being collected, analyzed, deposited and presented, cannot be overemphasized.

DF experts can portray an individual FB participant via their daily lives through his/her posted messages or uploaded photos. Nevertheless, the mobile and location-based services embedded in smartphones encourage more people to utilize SNSs. Hence, the interactions and relationships among cyber friends become more intensive and complicated. In addition, location check-ins are also another form of catching others' attention and earning admiration. In other words, DF experts are searching for some digital traces of the executions that were left behind on the disk.

Furthermore, in this research work, the social snapshots of any FB user can be constructed after the collection of the associated products of the social tendency of exhibitionism. An FB user may create a personal profile by adding others as friends, so as to exchange messages with the automatic feed notification whenever his/her profile information has been updated. However, this platform provides a strong incentive for criminals to carry out their activities, such as drug dealing or child pornography.

Indisputably, Internet Explorer (IE) has been the major browser for facilitating the execution of a generic FB session. Undoubtedly, digital traces could be inadvertently left, and they could be disclosed, as long as sophisticated DF experts have been professional trained.

In this research, we provide the design of an experiment to illustrate volatile digital traces, which are capable of being used to sketch the profile of an FB user using IE on Windows. The partial reconstruction of a previous FB session could be fulfilled, as well as an investigation of the friend circle of the previous FB user. Since the FB user could change the profile picture or delete some pertinent friends after the seizure of the computer device, the proposed methodology is able to reflect the pertinent digital evidence, even if the cybercriminal updates the content of his/her FB profile. This paper gives some insights into the advantages of having a user activity tracking system and avoids the difficulties of getting the related data from SNS providers. Moreover, the aim of the paper is to target the contribution of knowledge sharing to DF investigators in the related research fields. The essence of the paper is to piece together the remaining digital traces for future investigation or to sketch the profile of an FB user if information security leakage occurs.

The rest of the paper is composed as follows. In Section 2, we present a comprehensive literature review, which endeavors to reveal the DF research area in terms of the methodologies and approaches with respect to the IE browser and FB application program. In Section 3, we conduct the design of the experiments in two phases to create a contrast in order to pinpoint the spirit of the research. In Section 4, we summarize and discuss the results of the design of the experiment based on the digital traces that have been embedded in the volatile memory of the computing device via the proposed methodologies in this research work. Finally, in Section 5, we provide the conclusion of the proposed research work.

2. Literature Reviews

For the Microsoft Windows operating system, the primary source of information of the system and its components is the registry, which is essentially a database for the configuration of data that is stored in a hierarchical structure. It is volatile in nature. Through the dumping of the physical memory, numerous digital traces could be disclosed, and hidden traces could be identified based on the collection and analysis of those precious pieces of information [5–8].

Examining the Internet activities of a certain user at the crime scene has become an important research field, since an increasing number of both criminal and civil cases is moving towards heavily relying on digital evidence through SNSs. Hence, the capability to isolate a criminal's browsing history is often critical for some criminal cases. When the browser is the major platform, web browser artifacts can assist DF specialists in finding offenses ranging from minor corporate policy violations, which are committed by employees of a company, to more serious crimes, like child pornography or hacking-related misconduct [3,6]. By retrieving the browser history, cookies, cached downloaded files or even the physical memory, it is possible to determine the suspect's online activities, which is critical when a digital investigation is mandatory, especially under time pressure [9–12].

The mushrooming of SNSs has dramatically changed the way heterogeneous computing devices, such as desktop computers or mobile communication gadgets, which are applied to communication. SNSs, as a part of social media, generally represent services based on websites that enable an individual to create a public profile within a closed system. In addition, social computing involves such activities as collecting, extracting, accessing, processing, computing and visualizing of all kinds of social information [12,13].

There are methods that can be used to extract the digital artifacts from the local web browser cache.

FB activities have exponentially grown along with the social networking website itself. Unfortunately, many criminal-related cases or offence incidents occur from time to time. Digital investigation embedded in the FB platform or the FB App for mobile users needs more attention from law enforcement agencies in the public sector. Various activities, such as instant chat, wall comments and group events, could generate a number of digital footprints in different locations [14,15]. Furthermore, the web browser cache is another repository for digital traces, with sufficient digital traces, and DF experts are capable of reasoning about motivations or of rebuilding the cybercrime scene.

The IE disk cache is a repository of temporary files that are written to the hard drive when a user surfs webpages on the Internet. In addition, IE uses a persistent cache to download the related content of a page, including graphic, sound and video files. Generally speaking, the cache needs 4 MB or one percent of the logical drive size, depending on which is greater. In order to identify the correct location of the cache for each user under Windows, the registry hive for the particular user must be examined for some cases [12,16].

Recently, the academic arena and law enforcement agencies have shown a great demand for digital traces to be collected, analyzed, preserved and presented in a systematic way to alleviate the flourishing exploitation of online social networking (OSN) websites as a platform to commit illegal activities. Some researches use a hybrid system that is based on a custom add-on module for social networks in combination with a web crawling component [4,17]. Social computing errands involve such activities as collecting, extracting, accessing, processing, computing and visualizing all kinds of social information [10,18].

With IE Version 10, Microsoft has changed method of storing web-related information. Instead of the old index.dat file, IE Version 10 uses a special database called WebCacheV01.dat (Microsoft, Bellevue, WA, USA) to maintain its web cache, history and cookies. The database contains a wealth of information that can be of great interest to a DF investigator. Consequently, web surfers use the web browser to visit webpages, bookmarks and every viewed document. The web history could be left on the user's system, and some of this will be loaded into the RAM of the computing device.

3. Design of the Experiment

In order to illustrate the essence of the research, the computing device being used is a desktop personal computer with 4 G of RAM running Windows 8 with IE 10 Version 10.0.9200.17183.

Phase 1: The user logs in to a generic FB session by means of IE Version 10. The DF team obtains volatile digital traces while the power of the computing device is sustained.

Step 1: The DF team utilizes RamCapture64.exe [19] to acquire the image of the RAM of the computing device on the spot, under the scenario that the previous FB session was shut off. In other words, IE was not activated at that moment, either.

The acquired image file of the volatile memory was saved as 20140614_OnSpot.mem with a file size of 4,980,736 KB. The size of the RAM of the computing devices being examined is 4864 MB, as Figure 1 demonstrates. For the integrity of the digital evidence, the DF team gathered the hash values. The message digest 5 (MD5) of this image file was DFB786BC38A9C7B723D647042DC8CBDB, and the secure hash algorithm 1 (SHA1) of the image file was BC646CE1E5F676430DE138115F642B1CC6B3B5D9, respectively [20].

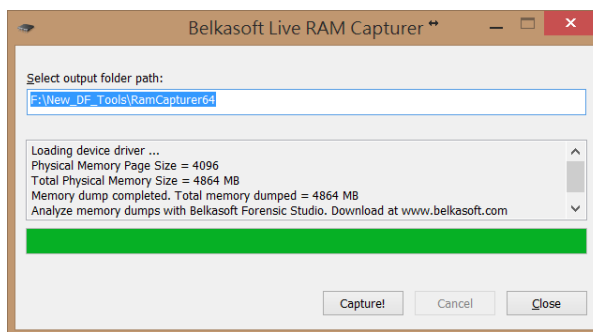


Figure 1. The screenshot of the acquisition procedure of the random access memory (RAM) of the computing device.

Step 2: The DF team utilized ProDiscover Basic Version 4.8a [21] to parse the image file of the RAM via a sequence of keywords accordingly. Initially, the DF team applied the search keyword, *profile_pic_header*, with respect to the image file of the RAM of the computing device, and the search results return 10 hits. Applying this keyword, we are able to spot the previous FB user during that session. As Figure 2 demonstrates, the FB user ID of the previous user was disclosed. Hence, we can conclude that the FB user ID in the previous session was 100001936659000, as Figure 2 indicates.

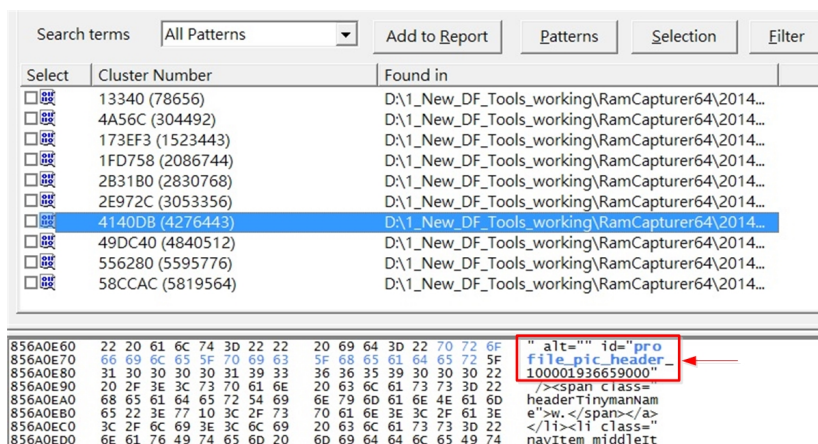


Figure 2. The current Facebook (FB) user identification (ID), 100001936659000, was disclosed via the search keyword, *profile_pic_header*.

Step 3: The DF team utilized another search keyword, *html lang=*, with regard to the image file of the RAM of the computing device. The search outcome returns 12 hits. As Figure 3 demonstrates, the revealed information identified that the current user set English as the default language preference. Consequently, this discovery provides a strong profile of the user concerning language proficiency. The preference of the language of the previous FB user might be related to other critical digital traces, which could play an essential role during the digital trail analysis.

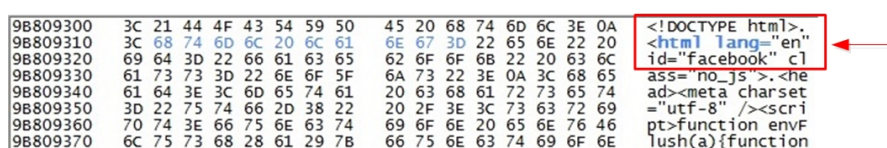


Figure 3. The previous FB user set English as the default language.

Step 4: The DF team utilized another search keyword, *alternateName*, and the search results contained quite a few FB user names. The following information was disclosed as illustrated in Figure 4.

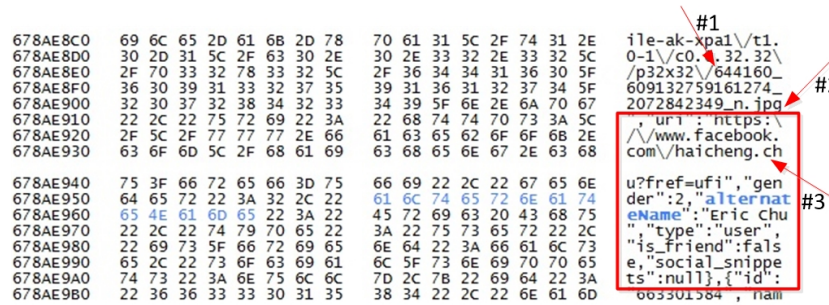


Figure 4. The related digital traces concerning the search keyword, *alternateName*.

The above rectangular area represents the following fragment of data:

For the enclosed area to which Arrow 1 and Arrow 2 point in Figure 4, the DF team can conclude that a profile picture was uploaded. As Arrow 3 points out, the DF team obtained the following:

“*https://www.facebook.com/haicheng.chu?fref=ufi*”, “gender”:2, “alternateName”: “Eric Chu”, “type”: “user”, “is_friend”:false

For the HTML format, a character is represented twice from “\” to “/” in JSON (JavaScript Object Notation) format. After securing the occurrences, “Eric Chu” substantively dominated most of the search outcomes among the various data, as Figure 4 suggests. Therefore, we can objectively predict that the previous FB user applied Eric Chu as “other names” in the previous FB session in terms of the FB settings. Additionally, we can figure out that the gender of the previous FB user was male due to the above digital trails, “gender”:2. Furthermore, the username of the previous FB user is *www.facebook.com/haicheng.chu* with respect to the FB settings. Based on the disclosed digital traces, the DF team can apply *www.facebook.com/haicheng.chu* to this distinct FB page. However, there is no guarantee that the previous FB user might have already shut off FB. Consequently, the DF team momentarily downloaded the profile picture and saved it as the suggested filename, exactly as the enclosed area to which Arrow 1 and Arrow 2 are pointing in Figure 4, which was *644160_609132759161274_2072842349_n.jpg*. For the integrity of the digital evidence, the DF team obtained the MD5 of the profile picture accordingly, which was *894BE2FB72D7EE5894CFA51575DCBE51*, and the SHA1 of the file was *24CB46C05096A9F8418F3D45E7DD359A23351395*, respectively.

In addition, the DF team sequentially obtained the following occurrences along with the outcomes of the search results, as Figure 5 indicates.

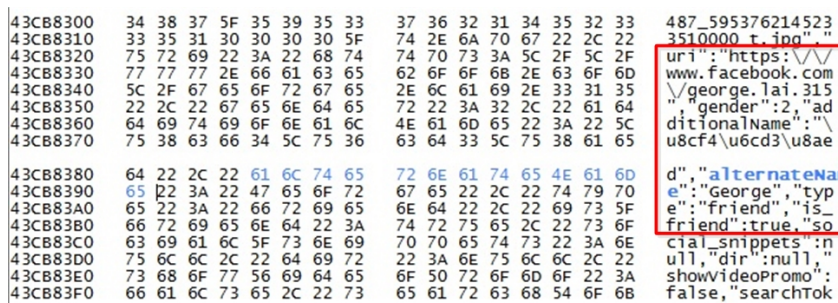


Figure 5. The related digital traces concerning the search keyword, *alternateName*.

The DF team also disclosed other information similar to the following:

“https://www.facebook.com/George.lai.315”, “gender”:2, “additionalName”: “\u8cf4\u6cd3\u8aed”, “alternateName”: “George”, “type”: “friend”, “is_friend”:true

Hence, the DF team came up with a male friend, George, with respect to www.facebook.com/vhaicheng.chu. In addition, the Unicode of “\u8cf4\u6cd3\u8aed” was interpreted as “賴泓論” with regard to Traditional Chinese.

Furthermore, the DF team sequentially obtained the following occurrences along with the outcomes of the search results, as Figure 6 indicates.

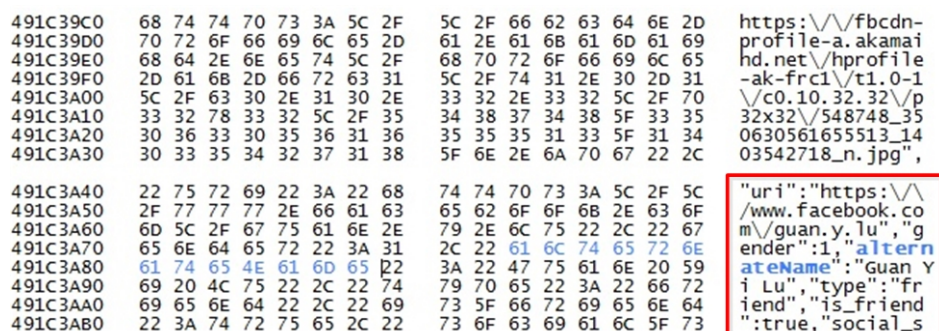


Figure 6. The related digital traces concerning the search keyword, alternateName.

Similarly, the following information was obtained:

“https://www.facebook.com/guan.y.lu,” “gender”:1, “alternateName”: “Guan Yi Lu”, “type”: “friend”, “is_friend”:true

The DF team can infer that there was a female friend, Guan Yi Lu, with respect to www.facebook.com/vhaicheng.chu. The friend does not have additionalName in the FB settings.

Furthermore, the DF team sequentially obtains the following occurrences along with the outcomes of the search results, as Figure 7 indicates.

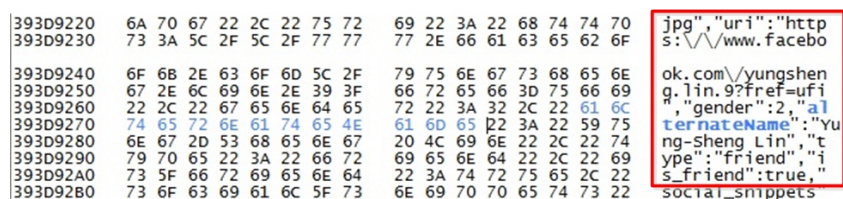


Figure 7. The related digital traces concerning the search keyword, alternateName.

Similarly, the following information is obtained:

“https://www.facebook.com/yungsheng.Lin.9?fref=ufi”, “gender”:2, “alternateName”: “Yung-sheng Lin”, “type”: “friend”, “is_friend”:true

The DF team can infer that there was a male friend, Yung-sheng Lin, with respect to www.facebook.com/vhaicheng.chu. The friend does not have additionalName in the FB settings.

Furthermore, the DF team sequentially obtains the following occurrences along with the outcomes of the search results, as Figure 8 indicates.

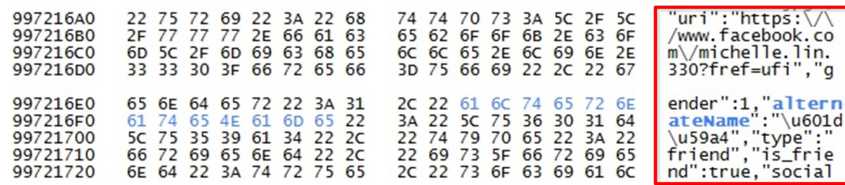


Figure 8. The related digital traces concerning the search keyword, *alternateName*.

Similarly, the following information is obtained:

"https://www.facebook.com/michelle.lin.330?fref=ufi", "gender": 1, "alternateName": "\u601d\u59a4", "type": "friend", "is_friend": true

The DF team can infer that there was a female friend with respect to *www.facebook.com/vhaicheng.chu*. The friend does not have *additionalName* in the FB settings. Furthermore, the Unicode of "\u601d\u59a4" was interpreted as “思好” with regard to Traditional Chinese.

Step 5: The DF team utilized another search keyword, *mobileFriends*, and the search results returned several FB user IDs with 24 occurrences, as Figure 9 indicates.

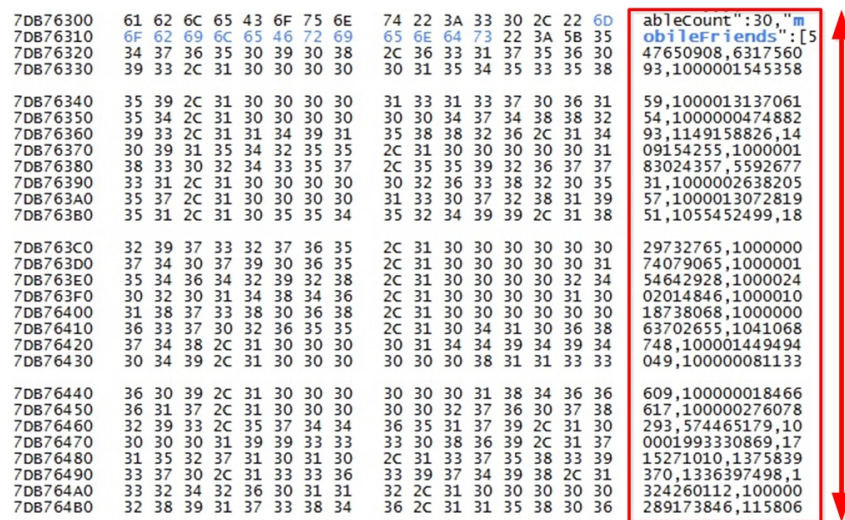


Figure 9. The related digital traces concerning the search keyword, *mobileFriends*.

From the Figure, we can identify the following FB users that have the FB instant messaging functionality installed within their mobile computing devices, such as smartphones, based on the partial outcomes after securing the aforementioned digital traces. Based on the above digital trails, we obtain the following FB user IDs:

- 547650908, 631756093, 100000154535859, 100001313706154, 100000047488293, 1149158826, 1409154255, 100000183024357, 559267731, 100000263820557, 100001307281951, 1055452499, 1829732765, 100000074079065, 100000154642928, 100002402014846, 100001018738068, 100000063702655, 1041068748, 100001449494049, 100000081133609, 100000018466617, 100000276078293, 574465179, 100001993330869, 1715271010, 1375839370, 1336397498, 1324260112, 100000289173846, etc.

At this moment, the DF team can sketch out the circle of friends of the previous session of the FB user, *www.facebook.com/haicheng.chu*. Basically, from the above digital traces, we can conclude that the circle of friends is greater than 30. Without losing the essence of the research, we interpret the username of the FB accordingly.

We define a symbolic representation to simplify the following statements:

§ $FB(ID_i)$ is the function that will return the user name of the FB profile and the argument is the FB user ID, ID_i . The value of i ranges from one to the upper limit of the number of friends in their circle, with $I = 0$ representing the current FB user ID. In other words, $ID_0 = 100001936659000$.

Without losing the essence of the research, we partially interpret the following:

- § $FB(547650908) = \text{Jessie Chen}$
- § $FB(631756093) = \text{Ann S'c Wu}$
- § $FB(100000154535859) = \text{郭瑞祥}$
- § $FB(100001313706154) = \text{羅季盈 (Bear)}$
- § $FB(100000047488293) = \text{Yuwen Lin}$
- § $FB(1149158826) = \text{Hui-Yin Hsu}$
- § $FB(1409154255) = \text{Vicky Chuang}$
- § $FB(100000183024357) = \text{蕭蓓霖}$

The above digital traces contributed to obtaining the online social snapshots of the previous FB participant.

Step 6: Based on the previous search results, we can conclude that those FB user IDs represent the partial friend circle of the previous session of the FB user, *www.facebook.com/haicheng.chu*. Therefore, the DF team utilized the search keyword, *haicheng.chu*, and the search results returned 71 occurrences, as Figure 10 indicates. The most representative information was disclosed, as Figure 10 indicates.

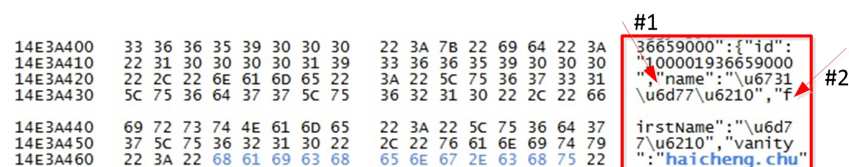


Figure 10. The related digital traces concerning the search keyword, *haicheng.chu*.

As Arrow 1 points out in the Figure, the DF team interpreted the Unicode “\u6731\u6d77\u6219” to be “朱海成” with regard to Traditional Chinese, which is the displayed user name on FB. In addition, as Arrow 2 points out in the figure, the first name of the previous user is “u6d77\u6219” in Unicode format, which was interpreted to be “海成” with respect to Traditional Chinese.

Step 7: The DF team utilized another search keyword, *InitialChatFriendsList*, and the search results returned several FB user IDs with 23 occurrences, as Figure 11 indicates.

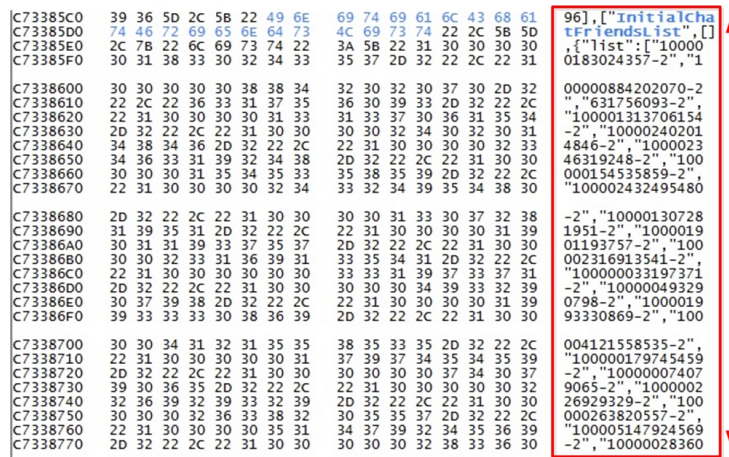


Figure 11. The related digital traces concerning the search keyword, *InitialChatFriendsList*.

From the Figure, we can identify that the following FB users have a high tendency to interact with the previous session of the FB user, www.facebook.com/vhaicheng.chu. After securing the above digital traces, henceforth, we obtain the following partial FB user IDs based on the digital trails retrieved:

- 100000183024357-2, 100000884202070-2, 631756093-2, 100001313706154-2, 100002402014846-2,
- 100002346319248-2, 100000154535859-2, 100002432495480-2, 100001307281951-2,
- 100001901193757-2, 100002316913541-2, 100000033197371-2, 100000493290798-2,
- 100001993330869-2, 100004121558535-2, 100000179745459-2, 100000074079065-2,
- 100000226929329-2, 100000263820557-2, 100005147924569-2.

At this moment, The DF team can infer that the above friends have frequent interactions with respect to the previous session of the FB user, www.facebook.com/vhaicheng.chu. Additionally, we can retrieve the individual FB user name via the FB user ID. For instance, for the digital trace, 100002402014846-2, we can apply <https://www.facebook.com/100002402014846> to successfully disclose the username of the FB user, Johnny Liu, accordingly. “-2” is the coding mechanism of FB, and we can skip that momentarily to conduct the following operations. Hence, we literately interpret the FB user ID as belonging to the corresponding user name accordingly:

- § FB(100000183024357-2) = 蕭蓓霖
- § FB(100000884202070-2) = 鄧鈞之
- § FB(631756093-2) = Ann S'c Wu
- § FB(100001313706154-2) = 羅季盈
- § FB(100002402014846-2) = Johnny Liu
- § FB(100002346319248-2) = 黃安鈺
- § FB(100000154535859-2) = 郭瑞祥
- § FB(100002432495480-2) = Duc Anh Lam

The interpretation of the above FB user IDs partially overlaps the previous one, which proved that the digital traces are capable of identifying the circle of friends of the previous FB user from different aspects.

Phase 2: Rebooting the computing device and obtaining the RAM acquisition momentarily without launching any application programs, including IE.

Step 1: The DF team acquired the image file of the RAM of the computing device and saved it as 20140614_reboot.mem with a file size of 4,980,736 KB.

Step 2: The DF team repeated the same forensic procedure as Step 2 in Phase 1. The search results are negative.

Step 3: The DF team repeated the same forensic procedure as Step 3 in Phase 1. The search result is positive, with one occurrence, as Figure 12 indicates. However, near the offset of the image of the RAM, 5196E1B0_h, that piece of the digital trails does not provide probative digital evidence in terms of the previous FB session.

```

5196E180 5D 00 2E 00 68 00 74 00 6D 00 00 00 00 00 00 00 J...h.t.m.....
5196E190 80 00 00 00 38 01 00 00 00 00 18 00 00 00 01 00 ...8.....
5196E1A0 1A 01 00 00 18 00 00 00 3C 21 64 6F 63 74 79 70 .....<!doctype
5196E1B0 65 20 68 74 6D 6C 3E 0A 3C 68 74 6D 6C 20 6C 6 e html>.<html la
5196E1C0 6E 67 3D 65 6E 3E 0A 20 20 20 20 3C 68 65 61 6 ng=en>. <head
5196E1D0 3E 0A 20 20 20 20 20 20 20 20 3C 6D 65 74 61 20 >. <meta
5196E1E0 63 68 61 72 73 65 74 3D 75 74 66 2D 38 3E 0A 20 charset=utf-8>.
5196E1F0 20 20 20 20 20 20 20 20 3C 74 69 74 6C 65 3E 50 72 <title>Pr

```

Figure 12. The related digital traces concerning the search keyword, *html lang=*.

Step 4: The DF team repeated the same forensic procedure as Step 4 in Phase 1. The search result was negative.

Step 5: The DF team repeated the same forensic procedure as Step 5 in Phase 1. The search result was negative.

Step 6: The DF team repeated the same forensic procedure as Step 6 in Phase 1. The search result was negative.

Step 7: The DF team repeated the same forensic procedure as Step 7 in Phase 1. The search result was negative.

Based on the information demonstrated in Phase 2, we can identify that the digital traces in Phase 1 were volatile in nature, and they could vanish forever once the power of the computing device is no longer sustained. Furthermore, the MD5 of the image file of the RAM, 2014-614_OnSpot.mem, was DFB786BC38A9C7B723D647042DC8CBDB, and the corresponding SHA1 value was BC646CE1E5F676430DE138115F642B1CC6B3B5D9, as shown Figure 13, respectively. These values are identical after the above digital trace manipulations. Consequently, the image file of the RAM of the computing device was not contaminated and can be the probative evidence in a court of law.

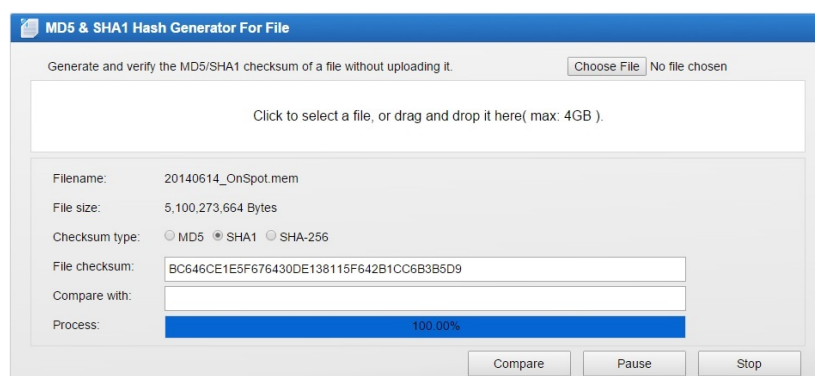


Figure 13. The message digest 5 (MD5) and secure hash algorithm 1 (SHA1) hash values of the digital evidence.

4. Discussion among Phases

Based on Step 6 of Phase 1, we can sketch a portion of the FB profile of the user haicheng.chu as Figure 14 depicts, even if the suspect has changed the photo immediately after the criminal behaviors were committed.



Figure 14. Sketching a portion of the FB profile for the user, haicheng.chu.

In addition, we could compile the digital traces in Step 5 and 7 of Phase 1 to reconstruct the possible outcomes of the user’s circle of friends after piecing together the digital traces, as Figure 15 indicates. This provides precious digital evidence on which the associated DF investigator can focus in a timely manner. Even if the previous user altered the content of his/her Facebook, like deleting or changing the snapshot image, the above collected, analyzed and preserved digital trials could be probative evidence in a court of law.

At this moment, it is not hard to figure out the snapshot of the profile of the previous FB user, which was hard to imagine at the beginning of the investigation. However, after piecing together the related digital traces, the DF team was able to sketch the profile of the FB user in the former session. All of the seizures of digital evidence suggest that once the power of the computing device is no longer sustained, the precious digital traces will vanish forever, as Phase 2 demonstrated.



Figure 15. The possible outcomes of the user’s circle of friends.

5. Conclusions

SNSs have been a phenomenally wide spreading platform for thousands of millions of global social networking participants, and FB is one of the most predominant SNSs in the related arena. Although there are some forensically sound DF suites available on the market, there are still some limitations in their usages. Additionally, there are some urgent concerns with the noncompliance of information security in private sectors that need to be responded to in a timely manner, for which it is not suitable for law enforcement agencies to get involved under the time constraints. Consequently, identifying the digital trails from a generic session of FB in terms of obtaining the online social snapshots of the circle of friends has become one of the entry points for the associated DF experts to ponder first. The paper contributes to the aforementioned research arena by collecting and piecing together the intangible digital traces by trying to reconstruct the partial profile status of the previous FB session for a certain user. Carrying out the investigation of digital traces in a systematic manner from Facebook activities is becoming essential as FB gradually becomes the avenue for committing cybercrimes. While the proposed methods apply to the vast majority of SNSs, their feasibility is demonstrated using the Facebook case study as a generic approach. The research work provides systematic methodologies to illustrate the essence of the acquisition of the volatile memory of contemporary computing devices from the DF point of view.

Acknowledgments

The authors would like to acknowledge the funding support of the Ministry of Science and Technology (MOST), Taiwan. This research was also supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (NIPA-2014-H0301-14-4007) supervised by NIPA (National IT Industry Promotion Agency).

Author Contributions

Hai-Cheng Chu wrote the draft of the paper; and Jong Hyuk Park contributed to the initial design of the experiment and the revision for this research publication.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Huber, M.; Mulazzani, M.; Leithner, M.; Schrittwieser, S.; Wondracek, G.; Weippl, E. Social snapshots: Digital forensics for online social networks. In Proceedings of 27th Annual Computer Security Applications Conference (ACSAC), Orlando, FL, USA, 5–9 December 2011; pp. 113–122.
2. Yang, Y.; Lutes, J.; Li, F.; Luo, B.; Liu, P. Stalking online: On user privacy in social networks. In Proceedings of the Second ACM Conference on Data and Application Security and Privacy, San Antonio, TX, USA, 7–9 February 2012; pp. 37–48.

3. Asuncion, A.U.; Goodrich, M.T. Turning privacy leaks into floods: Surreptitious discovery of social network friendships and other sensitive binary attribute vectors. In Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society (WPES'10), Chicago, IL, USA, 4–10 October 2010; pp. 21–30.
4. Stutzman, F.; Capra, R.; Thompson, J. Factors mediating disclosure in social network sites. *Comput. Hum. Behav.* **2011**, *27*, 590–598.
5. Boshmaf, Y.; Muslukhov, I.; Beznosov, K.; Ripeanu, M. The socialbot network: When bots socialize for fame and money. In Proceedings of the 27th Annual Computer Security Applications Conference (ACSAC'11), Orlando, FL, USA, 5–9 December 2011; pp. 93–102.
6. Garfinkel, S.L. Digital forensics research: the next 10 years. *Digit. Investig.* **2010**, *7*, S64–S73.
7. Stein, T.; Chen, E.; Mangla, K. Facebook immune system. In Proceedings of the 4th Workshop on Social Network Systems (SNS'11), Salzburg, Austria, 10–13 April 2011; pp. 8:1–8:8.
8. Malhotra, A.; Totti, L.; Meira, W., Jr.; Kumaraguru, P.; Almeida, V. Studying user footprints in different online social networks. In Proceedings of the 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), Istanbul, Turkey, 26–29 August 2012; pp. 1065–1070.
9. Yin, M.; Zhang, J.; Sun, H.; Gu, W. Multi-cue-based camshift guided particle filter tracking. *Expert Syst. Appl.* **2011**, *38*, 6313–6318.
10. Yang, Z.; Wilson, C.; Wang, X.; Gao, T.; Zhao, B.Y.; Dai, Y. Uncovering social network sybils in the wild. *ACM Trans. Knowl. Discov. Data* **2011**, *8*, doi: doi.org/10.1145/2556609.
11. Krombholz, K.; Merkl, D.; Weippl, E. Fake identities in social media: A case study on the sustainability of the facebook business model. *J. Serv. Sci. Res.* **2012**, *4*, 175–212.
12. Grobauer, B.; Walloschek, T.; Stocker, E. Understanding cloud computing vulnerabilities. *IEEE Secur. Priv.* **2011**, *9*, 50–57.
13. Hay, B.; Nance, K.; Bishop, M. Storm clouds rising: Security challenges for IaaS cloud computing. In Proceedings of the 44th Hawaii International Conference on System Sciences–HICSS 2011, Kauai, HI, USA, 4–7 January 2011; pp. 1–7.
14. Fusco, S.J.; Michael, K.; Michael, M.G. Using a social informatics framework to study the effects of location-based social networking on relationships between people: A review of literature. In Proceedings of the 2010 IEEE Internet Symposium on Technology and Society, Wollongong, Australia, 7–9 June 2010; pp. 157–171.
15. Gao, H.; Hu, J.; Wilson, C.; Li, Z.; Chen, Y.; Zhao, B.Y. Detecting and characterizing social spam campaigns. In Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS'10), Chicago, IL, USA, 4–8 October 2010; pp. 681–683.
16. James, J.; Gladyshev, P.; Abdullah, M.T.; Zhu, Y. Analysis of Evidence Using Formal Event Reconstruction. In Proceedings of the 1st International Conference on Digital Forensics & Cyber Crime, Albany, NY, USA, 30 September–2 October 2009; pp. 85–98.
17. Jin, L.; Takabi, H.; Joshi, J.B. Towards active detection of identity clone attacks on online social networks. In Proceedings of the First ACM Conference on Data and Application Security and Privacy, San Antonio, TX, USA, 21–23 February 2011; pp. 27–38.

18. Reilly, D.; Wren, C.; Berry, T. Cloud computing: forensic challenges for law enforcement. In Proceedings of the International Conference for Internet Technology and Secured Transactions–ICITST, London, UK, 8–11 November 2010; pp. 1–7.
19. Belkasoft. Available online: <http://www.belkasoft.com/> (accessed on 15 January 2015).
20. OnlineMD5. Available online: <http://onlinemd5.com/> (accessed on 13 January 2015).
21. ARC Group. Available online: <http://www.arcgroupny.com/> (accessed on 10 January 2015).

© 2015 by the authors; licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>).