Symmetry **2015**, *7*, 546-560; doi:10.3390/sym7020546

OPEN ACCESS

symmetry

ISSN 2073-8994

www.mdpi.com/journal/symmetry

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.

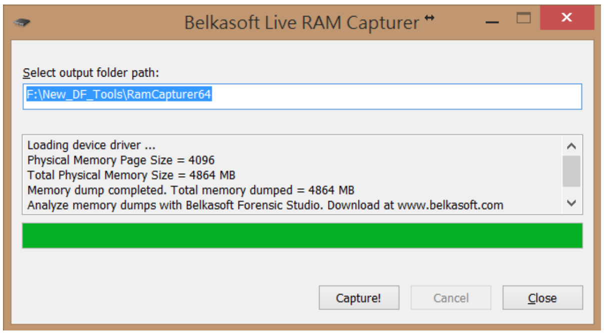
3. Design of the Experiment

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].

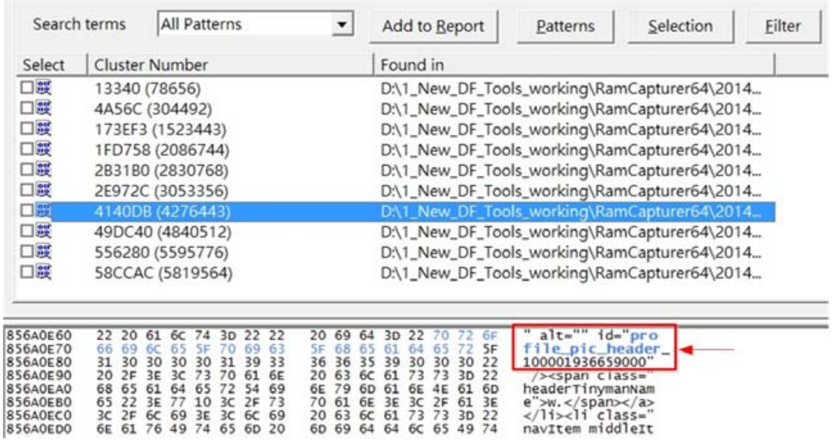


Select output folder path:
F:\New_DF_Tools\RamCapturer64

```
Loading device driver ...
Physical Memory Page Size = 4096
Total Physical Memory Size = 4864 MB
Memory dump completed. Total memory dumped = 4864 MB
Analyze memory dumps with Belkasoft Forensic Studio. Download at www.belkasoft.com
```

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.

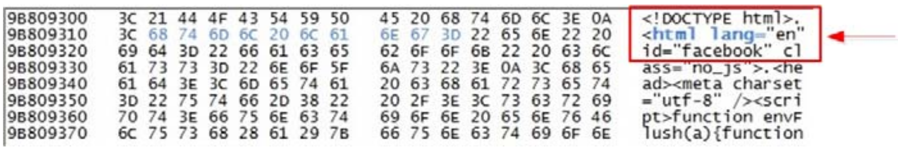


Select	Cluster Number	Found in
□	13340 (78656)	D:\1_New_DF_Tools_working\RamCapturer64\2014...
□	4A56C (304492)	D:\1_New_DF_Tools_working\RamCapturer64\2014...
□	173EF3 (1523443)	D:\1_New_DF_Tools_working\RamCapturer64\2014...
□	1FD758 (2086744)	D:\1_New_DF_Tools_working\RamCapturer64\2014...
□	2B31B0 (2830768)	D:\1_New_DF_Tools_working\RamCapturer64\2014...
□	2E972C (3053356)	D:\1_New_DF_Tools_working\RamCapturer64\2014...
□	4140DB (4276443)	D:\1_New_DF_Tools_working\RamCapturer64\2014...
□	49DC40 (4840512)	D:\1_New_DF_Tools_working\RamCapturer64\2014...
□	556280 (5595776)	D:\1_New_DF_Tools_working\RamCapturer64\2014...
□	58CCAC (5819564)	D:\1_New_DF_Tools_working\RamCapturer64\2014...

```
856A0E60   22 20 61 6C 74 3D 22 22   20 69 64 3D 22 70 72 6F   " alt="" id="pro
856A0E70   66 69 6C 65 5F 70 69 63   5F 68 65 61 64 65 72 5F   file_pic_header_
856A0E80   31 30 30 30 30 31 39 33   36 36 35 39 30 30 30 22   100001936659000"
856A0E90   20 2F 3E 3C 73 70 61 6E   20 63 6C 61 73 73 3D 22    /><span class="
856A0EA0   68 65 61 64 65 72 54 69   6E 79 6D 61 6E 4E 61 6D   headerTinymanNam
856A0EB0   65 22 3E 77 10 3C 2F 73   70 61 6E 3E 3C 2F 61 3E   e">w.</span></a>
856A0EC0   3C 2F 6C 69 3E 3C 6C 69   20 63 6C 61 73 73 3D 22   </li><li class="
856A0ED0   6E 61 76 49 74 65 6D 20   6D 69 64 64 6C 65 49 74   navItem middleIt
```

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

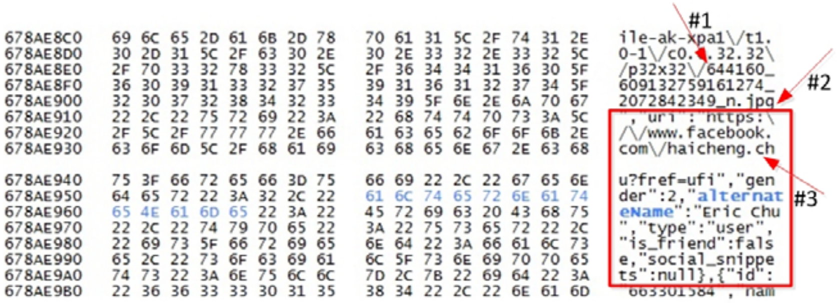
Step 3: The DF team utilized another search keyword, *html lang=*, with regard to the image file of the RAM of the computing device. The search outcome returns 12 hits. As Figure 3 demonstrates, the revealed information identified that the current user set English as the default language preference. 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.



```
9B809300   3C 21 44 4F 43 54 59 50   45 20 68 74 6D 6C 3E 0A   <!DOCTYPE html>.
9B809310   3C 68 74 6D 6C 20 6C 61   6E 67 3D 22 65 6E 22 20   <html lang="en"
9B809320   69 64 3D 22 66 61 63 65   62 6F 6F 6B 22 20 63 6C   id="facebook" cl
9B809330   61 73 73 3D 22 6E 6F 5F   6A 73 22 3E 0A 3C 68 65   ass="no_js">.<he
9B809340   61 64 3E 3C 6D 65 74 61   20 63 68 61 72 73 65 74   ad><meta charset
9B809350   3D 22 75 74 66 2D 38 22   20 2F 3E 3C 73 63 72 69   ="utf-8" /><scri
9B809360   70 74 3E 66 75 6E 63 74   69 6F 6E 20 65 6E 76 46   pt>function envF
9B809370   6C 75 73 68 28 61 29 7B   66 75 6E 63 74 69 6F 6E   lush(a){function
```

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.



```
678AE8C0   69 6C 65 2D 61 6B 2D 78   70 61 31 5C 2F 74 31 2E   ile-ak-xpa1\/t1.
678AE8D0   30 2D 31 5C 2F 63 30 2E   30 2E 33 32 2E 33 32 5C   0-1\/c0.0.32.32\
678AE8E0   2F 70 33 32 78 33 32 5C   2F 36 34 34 31 36 30 5F   /p32x32\/644160_
678AE8F0   36 30 39 31 33 32 37 35   39 31 36 31 32 37 34 5F   609132759161274_
678AE900   32 30 37 32 38 34 32 33   34 39 5F 6E 2E 6A 70 67   2072842349_n.jpg
678AE910   22 2C 22 75 72 69 22 3A   22 68 74 74 70 73 3A 5C   ","uri":"https:\
678AE920   2F 5C 2F 77 77 77 2E 66   61 63 65 62 6F 6F 6B 2E   /\/www.facebook.
678AE930   63 6F 6D 5C 2F 68 61 69   63 68 65 6E 67 2E 63 68   com\/haicheng.ch

678AE940   75 3F 66 72 65 66 3D 75   66 69 22 2C 22 67 65 6E   u?fref=ufi","gen
678AE950   64 65 72 22 3A 32 2C 22   61 6C 74 65 72 6E 61 74   der":2,"alternat
678AE960   65 4E 61 6D 65 22 3A 22   45 72 69 63 20 43 68 75   eName":"Eric Chu
678AE970   22 2C 22 74 79 70 65 22   3A 22 75 73 65 72 22 2C   ","type":"user",
678AE980   22 69 73 5F 66 72 69 65   6E 64 22 3A 66 61 6C 73   "is_friend":fals
678AE990   65 2C 22 73 6F 63 69 61   6C 5F 73 6E 69 70 70 65   e,"social_snippe
678AE9A0   74 73 22 3A 6E 75 6C 6C   7D 2C 7B 22 69 64 22 3A   ts":null},{"id":
678AE9B0   22 36 36 33 33 30 31 35   38 34 22 2C 22 6E 61 6D   "663301584","nam
```

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

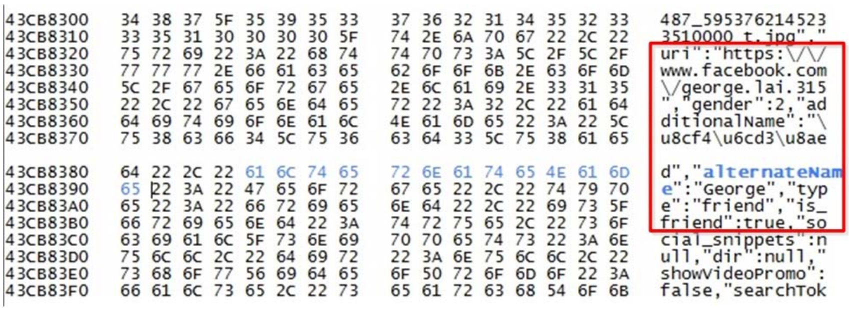
The above rectangular area represents the following fragment of data:

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.



```
43CB8300   34 38 37 5F 35 39 35 33   37 36 32 31 34 35 32 33   487_595376214523
43CB8310   33 35 31 30 30 30 30 5F   74 2E 6A 70 67 22 2C 22   3510000_t.jpg","
43CB8320   75 72 69 22 3A 22 68 74   74 70 73 3A 5C 2F 5C 2F   uri":"https:\/\/
43CB8330   77 77 77 2E 66 61 63 65   62 6F 6F 6B 2E 63 6F 6D   www.facebook.com
43CB8340   5C 2F 67 65 6F 72 67 65   2E 6C 61 69 2E 33 31 35   \/george.lai.315
43CB8350   22 2C 22 67 65 6E 64 65   72 22 3A 32 2C 22 61 64   ","gender":2,"ad
43CB8360   64 69 74 69 6F 6E 61 6C   4E 61 6D 65 22 3A 22 5C   ditionalName":"\
43CB8370   75 38 63 66 34 5C 75 36   63 64 33 5C 75 38 61 65   u8cf4\u6cd3\u8ae

43CB8380   64 22 2C 22 61 6C 74 65   72 6E 61 74 65 4E 61 6D   d","alternateNam
43CB8390   65 22 3A 22 47 65 6F 72   67 65 22 2C 22 74 79 70   e":"George","typ
43CB83A0   65 22 3A 22 66 72 69 65   6E 64 22 2C 22 69 73 5F   e":"friend","is_
43CB83B0   66 72 69 65 6E 64 22 3A   74 72 75 65 2C 22 73 6F   friend":true,"so
43CB83C0   63 69 61 6C 5F 73 6E 69   70 70 65 74 73 22 3A 6E   cial_snippets":n
43CB83D0   75 6C 6C 2C 22 64 69 72   22 3A 6E 75 6C 6C 2C 22   ull,"dir":null,"
43CB83E0   73 68 6F 77 56 69 64 65   6F 50 72 6F 6D 6F 22 3A   showVideoPromo":
43CB83F0   66 61 6C 73 65 2C 22 73   65 61 72 63 68 54 6F 6B   false,"searchTok
```

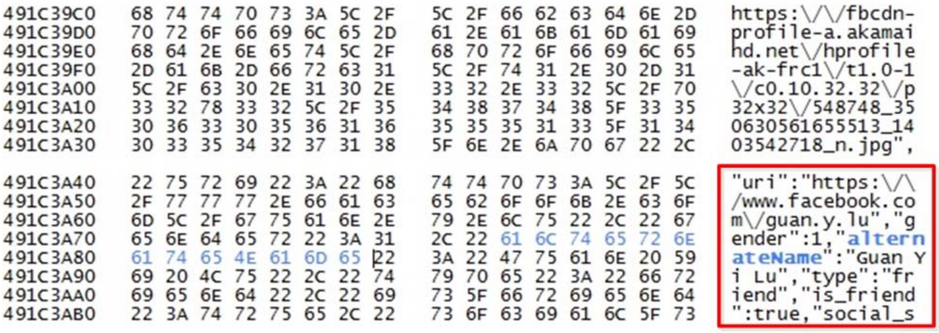
Figure 5. The related digital traces concerning the search keyword, *alternateName.*

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\/haicheng.chu. In addition, the Unicode of "\u8cf4\u6cd3\u8aed"* was interpreted as "賴泓諭" 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.



```
491C39C0   68 74 74 70 73 3A 5C 2F   5C 2F 66 62 63 64 6E 2D   https:\/\/fbcdn-
491C39D0   70 72 6F 66 69 6C 65 2D   61 2E 61 6B 61 6D 61 69   profile-a.akamai
491C39E0   68 64 2E 6E 65 74 5C 2F   68 70 72 6F 66 69 6C 65   hd.net\/hprofile
491C39F0   2D 61 6B 2D 66 72 63 31   5C 2F 74 31 2E 30 2D 31   -ak-frc1\/t1.0-1
491C3A00   5C 2F 63 30 2E 31 30 2E   33 32 2E 33 32 5C 2F 70   \/c0.10.32.32\/p
491C3A10   33 32 78 33 32 5C 2F 35   34 38 37 34 38 5F 33 35   32x32\/548748_35
491C3A20   30 36 33 30 35 36 31 36   35 35 35 31 33 5F 31 34   0630561655513_14
491C3A30   30 33 35 34 32 37 31 38   5F 6E 2E 6A 70 67 22 2C   03542718_n.jpg",

491C3A40   22 75 72 69 22 3A 22 68   74 74 70 73 3A 5C 2F 5C   "uri":"https:\/\
491C3A50   2F 77 77 77 2E 66 61 63   65 62 6F 6F 6B 2E 63 6F   /www.facebook.co
491C3A60   6D 5C 2F 67 75 61 6E 2E   79 2E 6C 75 22 2C 22 67   m\/guan.y.lu","g
491C3A70   65 6E 64 65 72 22 3A 31   2C 22 61 6C 74 65 72 6E   ender":1,"altern
491C3A80   61 74 65 4E 61 6D 65 22   3A 22 47 75 61 6E 20 59   ateName":"Guan Y
491C3A90   69 20 4C 75 22 2C 22 74   79 70 65 22 3A 22 66 72   i Lu","type":"fr
491C3AA0   69 65 6E 64 22 2C 22 69   73 5F 66 72 69 65 6E 64   iend","is_friend
491C3AB0   22 3A 74 72 75 65 2C 22   73 6F 63 69 61 6C 5F 73   ":true,"social_s
```

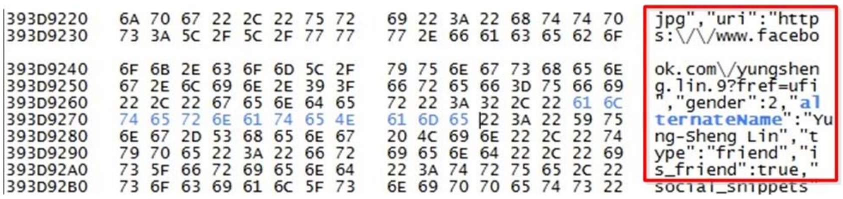
Figure 6. The related digital traces concerning the search keyword, *alternateName*.

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\/haicheng.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.



```
393D9220   6A 70 67 22 2C 22 75 72   69 22 3A 22 68 74 74 70   jpg","uri":"http
393D9230   73 3A 5C 2F 5C 2F 77 77   77 2E 66 61 63 65 62 6F   s:\/\/www.facebo

393D9240   6F 6B 2E 63 6F 6D 5C 2F   79 75 6E 67 73 68 65 6E   ok.com\/yungshen
393D9250   67 2E 6C 69 6E 2E 39 3F   66 72 65 66 3D 75 66 69   g.lin.9?fref=ufi
393D9260   22 2C 22 67 65 6E 64 65   72 22 3A 32 2C 22 61 6C   ","gender":2,"al
393D9270   74 65 72 6E 61 74 65 4E   61 6D 65 22 3A 22 59 75   ternateName":"Yu
393D9280   6E 67 2D 53 68 65 6E 67   20 4C 69 6E 22 2C 22 74   ng-Sheng Lin","t
393D9290   79 70 65 22 3A 22 66 72   69 65 6E 64 22 2C 22 69   ype":"friend","i
393D92A0   73 5F 66 72 69 65 6E 64   22 3A 74 72 75 65 2C 22   s_friend":true,"
393D92B0   73 6F 63 69 61 6C 5F 73   6E 69 70 70 65 74 73 22   social_snippets"
```

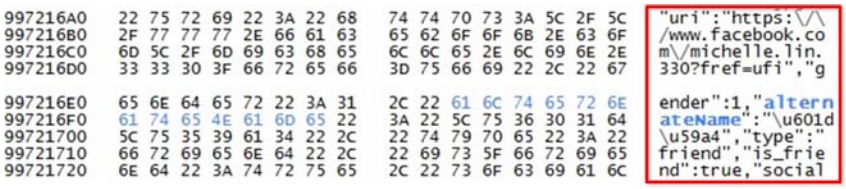
Figure 7. The related digital traces concerning the search keyword, *alternateName*.

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\/haicheng.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.



```
997216A0   22 75 72 69 22 3A 22 68   74 74 70 73 3A 5C 2F 5C   "uri":"https:\/\
997216B0   2F 77 77 77 2E 66 61 63   65 62 6F 6F 6B 2E 63 6F   /www.facebook.co
997216C0   6D 5C 2F 6D 69 63 68 65   6C 6C 65 2E 6C 69 6E 2E   m\/michelle.lin.
997216D0   33 33 30 3F 66 72 65 66   3D 75 66 69 22 2C 22 67   330?fref=ufi","g

997216E0   65 6E 64 65 72 22 3A 31   2C 22 61 6C 74 65 72 6E   ender":1,"altern
997216F0   61 74 65 4E 61 6D 65 22   3A 22 5C 75 36 30 31 64   ateName":"\u601d
99721700   5C 75 35 39 61 34 22 2C   22 74 79 70 65 22 3A 22   \u59a4","type":"
99721710   66 72 69 65 6E 64 22 2C   22 69 73 5F 66 72 69 65   friend","is_frie
99721720   6E 64 22 3A 74 72 75 65   2C 22 73 6F 63 69 61 6C   nd":true,"social
```

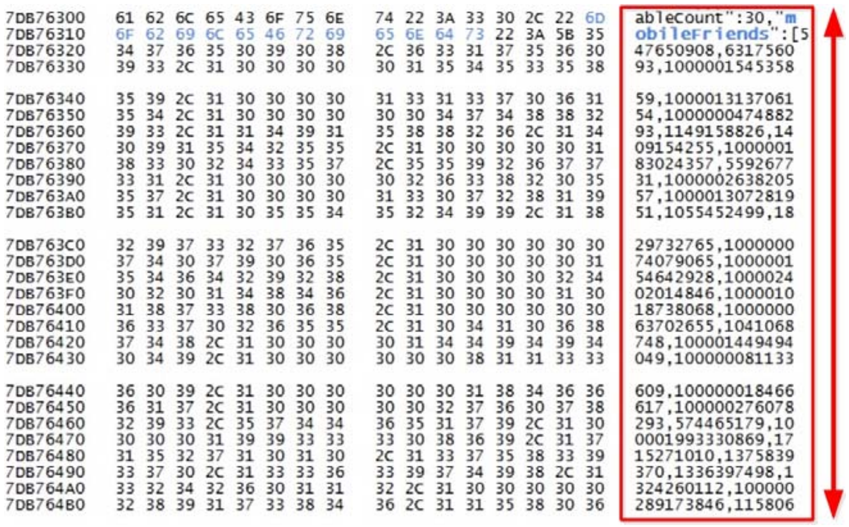
Figure 8. The related digital traces concerning the search keyword, *alternateName*.

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\/haicheng.chu*. The friend does not have *additionalName* in the FB settings. Furthermore, the Unicode of "\u601d\u59a4" was interpreted as "思妤" 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.



```
7DB76300   61 62 6C 65 43 6F 75 6E   74 22 3A 33 30 2C 22 6D   ableCount":30,"m
7DB76310   6F 62 69 6C 65 46 72 69   65 6E 64 73 22 3A 5B 35   obileFriends":[5
7DB76320   34 37 36 35 30 39 30 38   2C 36 33 31 37 35 36 30   47650908,6317560
7DB76330   39 33 2C 31 30 30 30 30   30 31 35 34 35 33 35 38   93,1000001545358

7DB76340   35 39 2C 31 30 30 30 30   31 33 31 33 37 30 36 31   59,1000013137061
7DB76350   35 34 2C 31 30 30 30 30   30 30 34 37 34 38 38 32   54,1000000474882
7DB76360   39 33 2C 31 31 34 39 31   35 38 38 32 36 2C 31 34   93,1149158826,14
7DB76370   30 39 31 35 34 32 35 35   2C 31 30 30 30 30 30 31   09154255,1000001
7DB76380   38 33 30 32 34 33 35 37   2C 35 35 39 32 36 37 37   83024357,5592677
7DB76390   33 31 2C 31 30 30 30 30   30 32 36 33 38 32 30 35   31,1000002638205
7DB763A0   35 37 2C 31 30 30 30 30   31 33 30 37 32 38 31 39   57,1000013072819
7DB763B0   35 31 2C 31 30 35 35 34   35 32 34 39 39 2C 31 38   51,1055452499,18

7DB763C0   32 39 37 33 32 37 36 35   2C 31 30 30 30 30 30 30   29732765,1000000
7DB763D0   37 34 30 37 39 30 36 35   2C 31 30 30 30 30 30 31   74079065,1000001
7DB763E0   35 34 36 34 32 39 32 38   2C 31 30 30 30 30 32 34   54642928,1000024
7DB763F0   30 32 30 31 34 38 34 36   2C 31 30 30 30 30 31 30   02014846,1000010
7DB76400   31 38 37 33 38 30 36 38   2C 31 30 30 30 30 30 30   18738068,1000000
7DB76410   36 33 37 30 32 36 35 35   2C 31 30 34 31 30 36 38   63702655,1041068
7DB76420   37 34 38 2C 31 30 30 30   30 31 34 34 39 34 39 34   748,100001449494
7DB76430   30 34 39 2C 31 30 30 30   30 30 30 38 31 31 33 33   049,100000081133

7DB76440   36 30 39 2C 31 30 30 30   30 30 30 31 38 34 36 36   609,100000018466
7DB76450   36 31 37 2C 31 30 30 30   30 30 32 37 36 30 37 38   617,100000276078
7DB76460   32 39 33 2C 35 37 34 34   36 35 31 37 39 2C 31 30   293,574465179,10
7DB76470   30 30 30 31 39 39 33 33   33 30 38 36 39 2C 31 37   0001993330869,17
7DB76480   31 35 32 37 31 30 31 30   2C 31 33 37 35 38 33 39   15271010,1375839
7DB76490   33 37 30 2C 31 33 33 36   33 39 37 34 39 38 2C 31   370,1336397498,1
7DB764A0   33 32 34 32 36 30 31 31   32 2C 31 30 30 30 30 30   324260112,100000
7DB764B0   32 38 39 31 37 33 38 34   36 2C 31 31 35 38 30 36   289173846,115806
```

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:

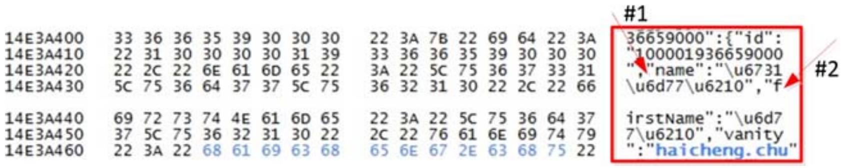
∮FB(ID_i) is the function that will return the user name of the FB profile and the argument is the FB user ID, ID_i. The value of *i* ranges from one to the upper limit of the number of friends in their circle, with I = 0 representing the current FB user ID. In other words, ID_0 = 100001936659000.

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

∮FB(547650908) = Jessie Chen
∮FB(631756093) = Ann S'c Wu
∮FB(100000154535859) = 郭瑞祥
∮FB(100001313706154) = 羅季盈 (Bear)
∮FB(100000047488293) = Yuwen Lin
∮FB(1149158826) = Hui-Yin Hsu
∮FB(1409154255) = Vicky Chuang
∮FB(100000183024357) = 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.



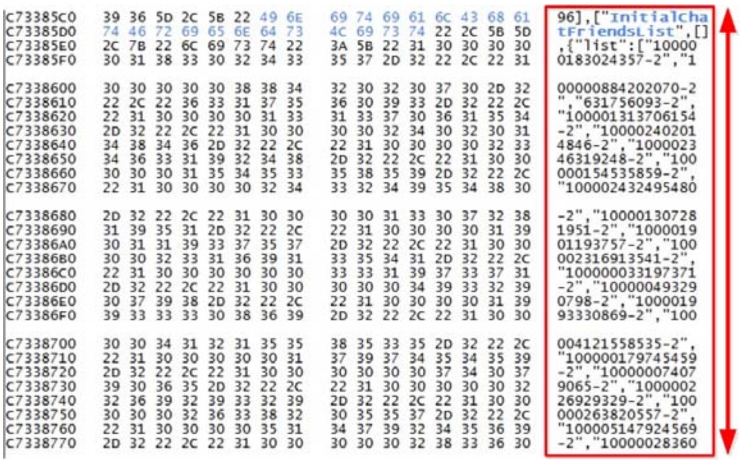
```
14E3A400   33 36 36 35 39 30 30 30   22 3A 7B 22 69 64 22 3A   36659000":{"id":
14E3A410   22 31 30 30 30 30 31 39   33 36 36 35 39 30 30 30   "100001936659000
14E3A420   22 2C 22 6E 61 6D 65 22   3A 22 5C 75 36 37 33 31   ","name":"\u6731
14E3A430   5C 75 36 64 37 37 5C 75   36 32 31 30 22 2C 22 66   \u6d77\u6210","f

14E3A440   69 72 73 74 4E 61 6D 65   22 3A 22 5C 75 36 64 37   irstName":"\u6d7
14E3A450   37 5C 75 36 32 31 30 22   2C 22 76 61 6E 69 74 79   7\u6210","vanity
14E3A460   22 3A 22 68 61 69 63 68   65 6E 67 2E 63 68 75 22   ":"haicheng.chu"
```

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.



```
C73385C0   39 36 5D 2C 5B 22 49 6E   69 74 69 61 6C 43 68 61   96],["InitialCha
C73385D0   74 46 72 69 65 6E 64 73   4C 69 73 74 22 2C 5B 5D   tFriendsList",[]
C73385E0   2C 7B 22 6C 69 73 74 22   3A 5B 22 31 30 30 30 30   ,{"list":["10000
C73385F0   30 31 38 33 30 32 34 33   35 37 2D 32 22 2C 22 31   0183024357-2","1

C7338600   30 30 30 30 30 38 38 34   32 30 32 30 37 30 2D 32   00000884202070-2
C7338610   22 2C 22 36 33 31 37 35   36 30 39 33 2D 32 22 2C   ","631756093-2",
C7338620   22 31 30 30 30 30 31 33   31 33 37 30 36 31 35 34   "100001313706154
C7338630   2D 32 22 2C 22 31 30 30   30 30 32 34 30 32 30 31   -2","10000240201
C7338640   34 38 34 36 2D 32 22 2C   22 31 30 30 30 30 32 33   4846-2","1000023
C7338650   34 36 33 31 39 32 34 38   2D 32 22 2C 22 31 30 30   46319248-2","100
C7338660   30 30 30 31 35 34 35 33   35 38 35 39 2D 32 22 2C   000154535859-2",
C7338670   22 31 30 30 30 30 32 34   33 32 34 39 35 34 38 30   "100002432495480

C7338680   2D 32 22 2C 22 31 30 30   30 30 31 33 30 37 32 38   -2","10000130728
C7338690   31 39 35 31 2D 32 22 2C   22 31 30 30 30 30 31 39   1951-2","1000019
C73386A0   30 31 31 39 33 37 35 37   2D 32 22 2C 22 31 30 30   01193757-2","100
C73386B0   30 30 32 33 31 36 39 31   33 35 34 31 2D 32 22 2C   002316913541-2",
C73386C0   22 31 30 30 30 30 30 30   33 33 31 39 37 33 37 31   "100000033197371
C73386D0   2D 32 22 2C 22 31 30 30   30 30 30 34 39 33 32 39   -2","10000049329
C73386E0   30 37 39 38 2D 32 22 2C   22 31 30 30 30 30 31 39   0798-2","1000019
C73386F0   39 33 33 33 30 38 36 39   2D 32 22 2C 22 31 30 30   93330869-2","100

C7338700   30 30 34 31 32 31 35 35   38 35 33 35 2D 32 22 2C   004121558535-2",
C7338710   22 31 30 30 30 30 30 31   37 39 37 34 35 34 35 39   "100000179745459
C7338720   2D 32 22 2C 22 31 30 30   30 30 30 30 37 34 30 37   -2","10000007407
C7338730   39 30 36 35 2D 32 22 2C   22 31 30 30 30 30 30 32   9065-2","1000002
C7338740   32 36 39 32 39 33 32 39   2D 32 22 2C 22 31 30 30   26929329-2","100
C7338750   30 30 30 32 36 33 38 32   30 35 35 37 2D 32 22 2C   000263820557-2",
C7338760   22 31 30 30 30 30 35 31   34 37 39 32 34 35 36 39   "100005147924569
C7338770   2D 32 22 2C 22 31 30 30   30 30 30 32 38 33 36 30   -2","10000028360
```

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\/haicheng.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\/haicheng.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

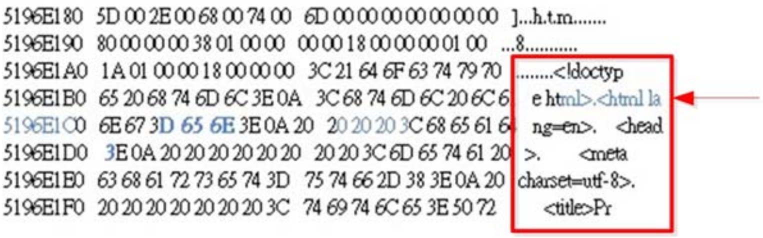
The interpretation of the above FB user IDs partially overlaps the previous one, which proved that the digital traces are capable of identifying the circle of friends of the previous FB user from different aspects.

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, 5196E1B0h, 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  ]...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  ........<!doctyp
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 3C  74 69 74 6C 65 3E 50 72         <title>Pr
```

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

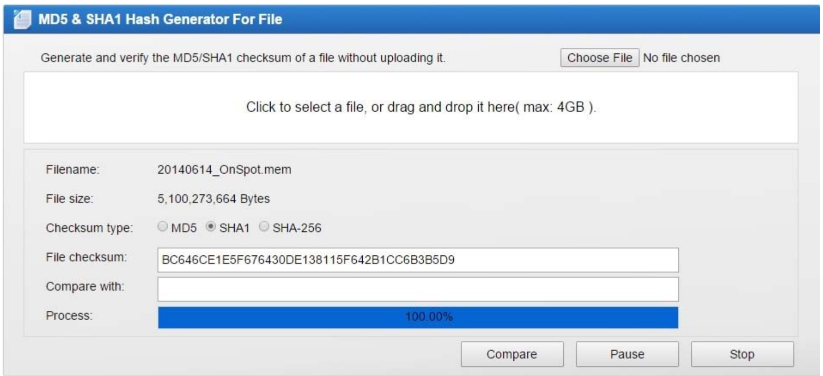
Step 4: The DF team repeated the same forensic procedure as Step 4 in Phase 1. The search result was negative.

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.



MD5 & SHA1 Hash Generator For File

Generate and verify the MD5/SHA1 checksum of a file without uploading it.

Choose File No file chosen

Click to select a file, or drag and drop it here(max: 4GB).

Filename: 20140614_OnSpot.mem

File size: 5,100,273,664 Bytes

Checksum type: ○ MD5 ● SHA1 ○ SHA-256

File checksum: BC646CE1E5F676430DE138115F642B1CC6B3B5D9

Compare with:

Process: 100.00%

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.

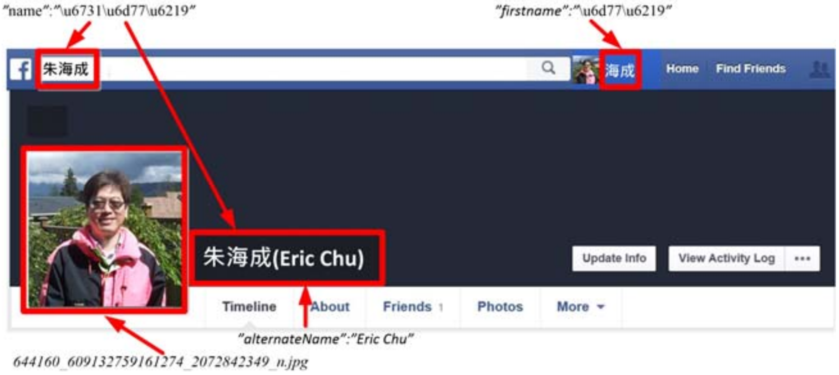
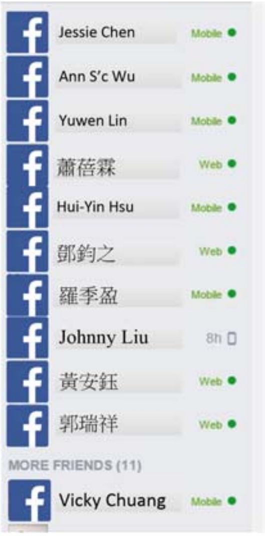

"name":"\u6731\u6d77\u6219"
"firstname":"\u6d77\u6219"
朱海成
海成
Home
Find Friends
朱海成(Eric Chu)
Update Info
View Activity Log
•••
Timeline
About
Friends 1
Photos
More
"alternateName":"Eric Chu"
644160_609132759161274_2072842349_n.jpg

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.



Jessie Chen Mobile ●
Ann S'c Wu Mobile ●
Yuwen Lin Mobile ●
蕭蓓霖 Web ●
Hui-Yin Hsu Mobile ●
鄧鈞之 Web ●
羅季盈 Mobile ●
Johnny Liu 8h ▯
黃安鈺 Web ●
郭瑞祥 Web ●
MORE FRIENDS (11)
Vicky Chuang Mobile ●

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).