The Digital Traces Uncovering of Generic *Gmail* / *Facebook* Instant Messaging Sessions via the IE Browser as Probative Evidences

Hai-Cheng Chu[1] Ching-Hsien Hsu[2] Ming-Hao Yin[3] Gai-Ge Wang[4*]

[1] Department of International Business, National Taichung University of Education
Taichung 40306, Taiwan
hcchu@mail.ntcu.edu.tw

[2] Department of Computer Science and Information Engineering, Chung Hua University
Hsinchu 30012, Taiwan
chh@chu.edu.tw

[3] School of Computer Science and Information Technology, Northeast Normal University
Changchun, Jilin 130024, China
ymh@nenu.edu.cn

[4*]School of Computer Science and Technology, Jiangsu Normal University
Xuzhou, Jiangsu 221116, China
gaigewang@gmail.com

Received 13 March 2014; Revised 1 January 2015; Accepted 22 April 2015

Abstract. Nowadays, the on-line Instant Messaging (IM) is extensively utilized from leisure purposes to business-oriented missions, which undoubtedly plays an essential role in contemporary digital era. There are several popular IM tools available in the digital communities. Hence, the spirit of the research is focusing on the discovery of digital traces in typical *Gmail / Facebook Chat* sessions due to the pervasive utilization of IM under ubiquitous mobile computing infrastructures. Additionally and literally, as Information Communication Technology (ICT) has gradually and unknowingly become a crucial part of our daily lives, digital trails have become probative evidences in the modern jurisdictional systems with respect to some cybercrimes. Furthermore, on account of the admissibility of digital evidences except their concealments, frangibility, and intangibility, some of them are volatile in their natures and they are unwarily ignored on the crime scenes with imperceptible characteristics in some cases. Consequently, Digital Forensics (DF) is substantively become the stringent, unparalleled, and indispensable challenges for the associate DF specialists or law enforcement officers concerning the pervasive IM Application Programs (APs). This research paper contributes the paradigms regarding the status of Internet Explorer (IE) (execution or shut-off) focusing on the digital evidence collections during representative *Gmail* / *Facebook Chat* sessions. The essence of the paper will pinpoint the consequences of the aforementioned status of IE in respect of collecting, analyzing, and preserving those negligible digital traces to be presented as probative evidences in a court of law.

Keywords: Internet Explorer (IE); *Gmail Chat*; *Facebook Chat*; Instant Messaging (IM); volatile digital traces acquisition; Digital Forensics (DF)

1 Introduction

Unquestionably, Instant Messaging (IM) has been predominantly utilized in our daily lives from leisure motivations to business-oriented purposes in contemporary digital era. Based on its real-time message delivering mechanism, IM has substantively become an irreplaceable Information Communication Technology (ICT) toolkit of real-time communications for hundreds of millions global participants. Evidently, countless global users apply a unique virtual identity instead of presenting real identity when IM is exploited in some cases, especially in connection with the mushrooming cybercrimes. There are several popular IM APs being utilized by various service providers. For example, *Yahoo! MSN Messenger*, *AOL IM (AIM)*, *Google Chat*, *I Seek You (ICQ)*, *Skype*, *Facebook Chat* [2,4,9]. Nowadays, under such circumstances, some of the cybercrime syndicate will take advantage of this state-of-the-art ubiquitous communication technology to commit conspiracies for their lucrative and sinister purposes. Rigorously, the cyberterrorism has also emerged as a new threat in comparison to traditional terrorism or racial extremists approximate a decade ago [7]. Unarguably, cyberterrorism is a new threat of virtual warfare, which encompasses the illegitimate usage of digital forces or violence against individuals or properties in order to intimidate a government or the communities in furtherance of political or social objectives with the

accumulation of all intangible fears. IM toolkits have been literally exploited by some cybercrime syndicate to conduct and synchronize the operations of attack. [1,5,11]

Proverbially, by the virtue of the pervasiveness of ubiquitous wireless computing infrastructures in contemporary digital era, there is a trend that the highly educated and politically motivated hacktivists launch cyber terrorist attacks concerning national critical infrastructures including airports, power grids, oil and gas distribution channels, telecommunication, public hygiene systems, and nuclear power plants. The previous potential incidents are becoming an imminent threat that will cause life-threatening issues through the utilization of IM to launch the operations. Astonishingly, cyberterrorists can conduct large scale and devastating attacks with a mouse click and the targets could be thousands of miles away. Recently, cybercrimes and computer-related crimes are gradually exploiting the IM as a new channel to commit unscrupulous conspiracy. The virtual identity would be initially difficult to decoded, which increase the challenge, complexity, and overhead for law enforcement agencies to trace and stimulate the motivation in a timely manner. Notwithstanding, the IM plays an essential role and new media for cybercrime syndicates like *Gmail Chat* or *Facebook Chat*. The Digital Forensics (DF) techniques can deal with this unprecedented abuse of ICT and prevent the similar information security incidents from relentless occurring.

Obviously, the screen name of *Gmail Chat* / *Facebook Chat* could be a fake or impersonated identity. Accordingly, the digital breadcrumb trails concerning the usage of previous IM become a critical and substantial element in terms of cybercrime investigations. Some of the IM toolkits, they need to install programs on the computing device, which is a prerequisite to perform the functionalities. Under such circumstances, there will be more hidden digital trails in the operating system of the computing devices. Generally speaking, the IM participants will register a unique identifier as the screen name. Therefore, in this paper, we will focus on a typical *Gmail* / *Facebook Chat* IM session with the status of IE being shut down or still executing after the running of the above APs. The corresponding acquisition procedures of the Random Access Memory (RAM) of the computing device will be performed accordingly in order to distinguish the differences between the execution statuses of the Internet Explorer (IE), which is a common web browser in most Windows operating system.

The rest of the paper is organized as follows. In section 2, we conduct comprehensive literature reviews, which have been done in the related DF research arena. In section 3, we present the design of the experiment with respect to the DF of typical *Gmail* / *Facebook Chat* sessions in a stage-by-stage manner. In section 4, we summarize, review, and conclude the corresponding DF results based on the digital evidences, which have been collected, analyzed, integrated, and presented in forensics sound procedures with conclusion presented.

2 Literature Review

Generally speaking, IM is a form of computer-mediated communication with unique characteristics that reflects a realistic presentation of an author's online stylistic characteristics. Nowadays, IM participants could use pure texts, audio clips, video clips, or the icons to send to the counterparts. Substantively, the pervasive application of IM application suites is becoming rapidly blooming from business perspectives to individual entertainment motivations [3,6,8]. Generally speaking, IM is capable of replacing e-mail in certain situations from effective communication point of view. Unfortunately, the prevalence of IM in respect of its convenience increases the risks to proprietary, sensitive, and personal information being vandalized, intercepted, or misused. In addition, phishing, social engineering, cyber bullying, cyber stalking, and IM threatening are occurring momentarily [2,6,10,13]. There is an imminent necessity for the DF specialist in both public and private sectors seeking the solutions for these stringent challenges in the cyber communities. Proverbially and unfortunately, the IM is another real-time communication channel for gangs, racial extremists, or cyber intruders. In many cases, on account of applying the anonymous identity in its nature, the IM has been extensively utilized as a communication tool for cyber intruders, cyber terrorists, and local gangs in global countries. In some occasions, the traceability is slim because of the availability and accountability of the DF methodologies being applied [7,10,14]. Phenomenally, the cybercrime syndicate impersonates other IM participants or forges multiple screen names for the purpose of harassing or deceiving unsuspecting victims in plausible manners. Evidently, the cyber DF investigation for IM heavily relies on message exchanged, or conversations as probative evidence in a court of law [4,8,12,15]. Eventually, the spirit of DF in the IM communication application arena is to prevent similar cyber criminal cases from relentless occurring in the near coming future. Undoubtedly, the social media is a group of Internet-based APs that connect individuals by means of web and mobile computing devices for the purpose of allowing the creation and exchange of User Generated Content (UGC) [15]. The social media is represented in various forms such as weblogs, social blogs, microblogging, *WeChat*, podcast, etc. *Gmail* / *Facebook Chat* are two of the most popular social media currently.

Unquestionably, the pervasive utilization of IM has changed the way of global ICT end users. Hundreds of thousands of mobile computing users send IM right in the palm by fingers. This phenomenon has been substantively penetrated into the arena from leisure purposes to business-oriented errands. For many desktop computing devices, the IE is one of the most popular browser. Disclosing the digital artifices of IE browser is an urgent task

for law enforcement agencies in the public sector or the DF specialists in the private sector on the crime scenes in order to collect, preserve, analyze, extract, and present the hidden or volatile digital traces as probative evidences in a court of law to judge the suspect to be innocent or guilty with compelling ones. Undoubtedly, in this digital era, there will be digital traces unknowingly deposited within the browser, RAM, cache, or the storage devices of the computing devices. IE contains a wealthy deposit for DF specialists and many of them have been unintentional ignored. Quite a few digital evidences could be disclosed for some cases as critical digital evidences. For DF, some off-the-shelf forensics sound software suites have the complete functions for the extraction, analysis, and presentation of forensic evidence relating to Internet browsers and user activities on the computing devices. Some of them have data recovery solutions designed to recover deleted browser artifacts, which can be imported into and analyzed in the software suites [7,10]. For web browsing forensics, the software suites are capable of supporting all the major desktop or mobile browsers in terms of analyzing the history, cache, cookies and other artifacts. One of the more recent shifts in evidence handling has been the shift away from simply pulling the plug as the first step in evidence collection to the adoption of methodologies to acquire evidence live from suspect's computing devices [6,8,14]. If those digital traces are resided in volatile memory, which mean those temporary data will be vanished forever once the supporting power becomes no longer sustainable. In this way, those precious and decisive digital traces will be lost forever, which is irreversible by their nature. Demonstrably, the wide usage of utilization of *Gmail / Facebook Chat* as communication tools is exponentially increasing based on the fact that the convenience of the aforementioned ones to manage and integrate various data from varied, heterogeneous, and multiple computing devices.

3 Design of the Experiment

For the purpose of disclosing the digital traces or artifacts with respect to the status of the IE when the cybercrimes occur respecting the DF in generic *Gmail* / *Facebook Chat* sessions on a Personal Computer (PC) running Windows XP, which is the local side of the experiment. Furthermore, the paper proposes the following generic design of experiment to pinpoint the essence of the research. The design of the experiment will focus on *Gmail Chat* first (Phase 1) and then *Facebook Chat* (Phase 2) will be another research target accordingly.

3.1 Phase 1 *Gmail Chat* section on the client and remote sides:

Stage 1: The initialization of the *Gmail Chat* session

Initially, *Gmail Chat* is being launched on the local side with the associate IM participant on the remote side. The current local side Gmail user, *testman df* whose e-mail address is *dftestman@gmail.com*, received the online chat message, *cellular number*, from the corresponding one, *bravedean*, with e-mail address *bravedean@gmail.com* on the remote side. The design, construction, and the deployment of the experiment are illustrated as Figure 1 depicts.

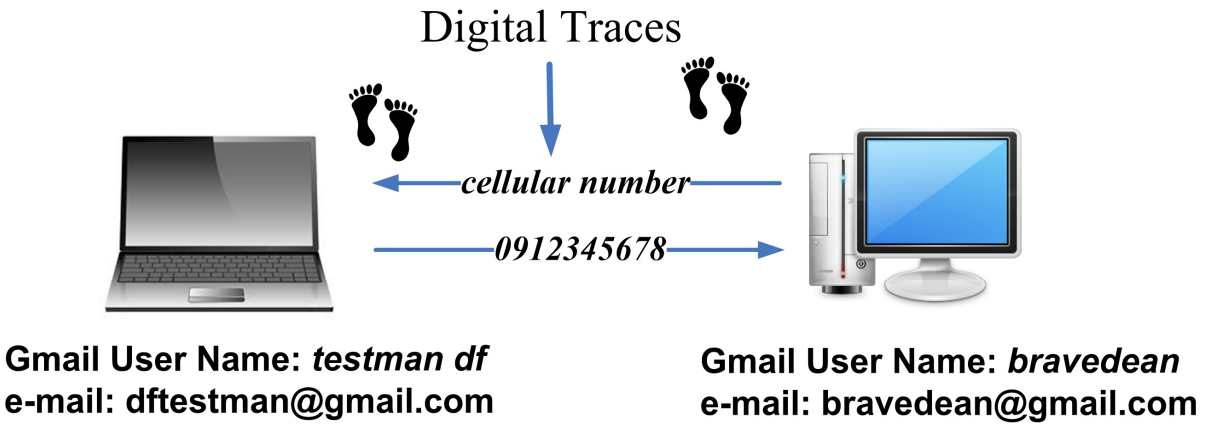

Fig. 1. The design, construction, and the layout of the experiment in terms of *Gmail Chat* function

From the figure, we can clearly identify that the former user (*testman df*) replied the online Chat message, *0912345678*, back to the latter one, with the *Gmail* user name *bravedean*. Fig. 2 shows a part of the communication dialog.

Fig. 2. The screenshot of a typical *Gmail Chat* session with mutual dialog

Stage 2: Live data acquisition of the PC running the *Gmail Chat*

After the online instant communication of the *Gmail Chat* dialog, the *Gmail* user, *testman df*, logged off from *Gmail* with IE still running. The DF staff applied *Helix* FTK® (Forensics Tool Kit) ver. 2.0 software suite to obtain the image file of the RAM of the current PC. The capacity of the volatile memory of the computing device is 1,033 MB. The name of the image file of the RAM was *image.dd* and it was deposited in an anti-static forensic evidence bag for future investigation.

Stage 3: Conducting the analysis procedures of the image file, *image.dd*, of the RAM of the PC

The DF team applied the *AccessData* FTK® ver. 1.62 to interpret and analyze the image file of the RAM of the PC. The goal at this stage is to disclose hidden probative digital evidences that could be critical, decisive, and essential.

Stage 4: Carrying on target string search to disclose the hidden digital breadcrumb trail

The DF staff utilized the specific keywords as the target search string in this distinct forensics stages based on the sophisticated experience accumulated in the DF field with respect to the *Gmail Chat* session. Hence, after obtaining the image file of the RAM of the PC, the DF team utilized *AccessData* FTK® ver. 1.62 to proceed the live data search focusing on the keyword *"active"* and the result turns 31 hits in 19 files as Figure 3 indicated. As the Figure suggests, at the offset $E7E768_h$ (15198056_{10}) of the image file of the RAM, hidden digital traces were revealed, which were the received IM, *cellular number*, with the Unix time stamp, *1303889653798*, respectively. Besides, among those discoveries, we are capable of figuring out the e-mail account to be *bravedean@gmail.com*, who sent the IM, *cellular number*, on *Wednesday, April 27th, 2011, at 07:34:13 GMT* after being decoded from the acquisition of the RAM. The interpretation of the digital evidence is presented in the figure as the arrow points.

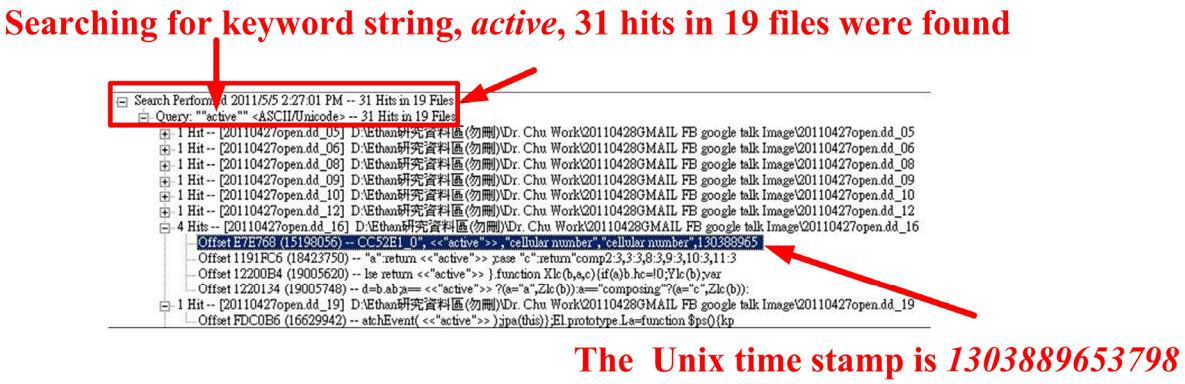

Fig. 3. The search result turns 31 hits in 19 files with the search keyword "active" as well as the time stamp, *1303889653798*

Stage 5: Advanced digital evidences investigation

The DF staff conducted the 2nd experiment by deleting all the browsing records and caches of IE with the rebooting of the PC. The purpose of this procedure is to ensure that there will be no digital residuals deposited to make the contrast to the previous stages. Hence, the DF staff repeated all procedures from previous stages except log-out off and shutting down IE browser before the collection of digital evidences for the purpose of providing the contrast of the proposed experiment. The DF staff applied the same search keyword, *active*, searching for the possible results. Notwithstanding the search results turn 19 hits in 6 files, unfortunately, the results turned negative concerning the *Gmail* user account, IM text, or the time stamp this time as Figure 4 indicates.

Fig. 4. The e-mail account of the sender was *bravedean@gmail.com* and it was disclosed with the sent the IM, *cellular number*. The IM was sent on *Wednesday, April 27th, 2011, at 07:34:13 GMT* based on the previous interpretation of the time stamp, *1303889653798*

In addition, from the digital evidences being obtained and analyzed, the DF team can identify that the corresponding IM participant was *bravedean@gmail.com* with the sent IM, *cellular number* as Figure 5 indicated.

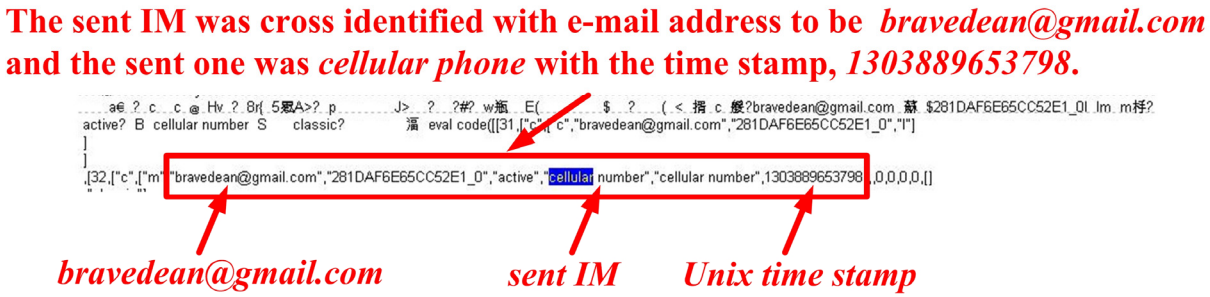

Fig. 5. The DF team can also identified that the IM was sent by *bravedean@gmail.com* with the IM, *cellular number*

3.2 Phase 2 *Facebook Chat* section on the client and remote sides:

Stage 6: IM on *Facebook Chat*

In this phase, the DF team conducted the IM experiments on a generic *Facebook Chat* session. The *Facebook* user, *deangarnett@yahoo.com.tw (Testman Df)*, received the IM message, *cellular number?*, from the corresponding participant, *lambert_ethan@yahoo.com.tw (Ethan Wang)*. In addition, for the *Facebook* user name, *Testman Df*, replied the IM, *0912345678*, back to the corresponding *Facebook* user name, *Ethan Wang*, as Figure 6 demonstrates. Furthermore, the actual IM dialog was illustrated as Figure 7.

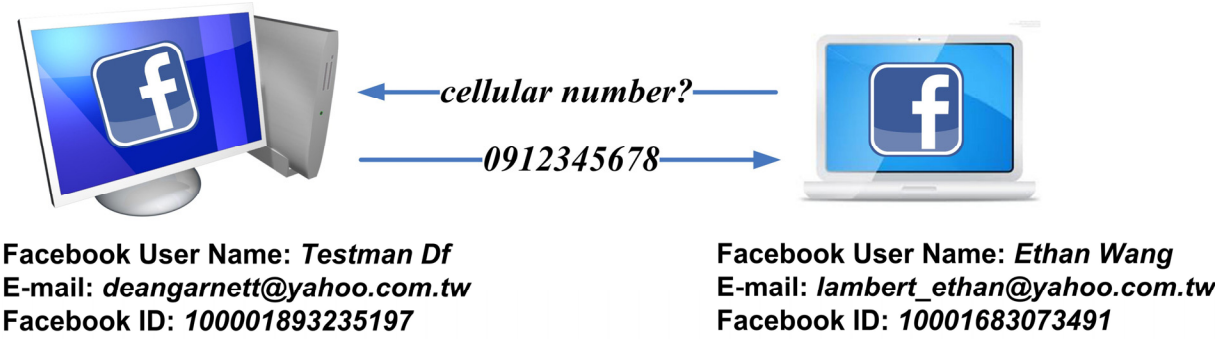

Fig. 6. The complete *Facebook Chat* session between *Testman Df* and *Ethan Wang*

Fig. 7. The complete *Facebook Chat* session between the *Facebook* user names *Testman Df* (replier) and *Ethan Wang* (sender), respectively

Stage 7: Acquiring the image of the RAM with the running status of execution of the IE

After the IM conversion is completed, the *Facebook* user, *Testman Df*, whose e-mail address is listed as *deangarnett@yahoo.com.tw* logout off from the *Facebook* with the existing status of the IE. Firstly, The DF team repeated the pervious stages in order to obtain the image file of the RAM of the PC. At this moment, the DF team applied the target search string, *msgID*, in regard to the image file being acquired. Secondly, the search results turn 52 hits in 27 files as Figure 8 demonstrated.

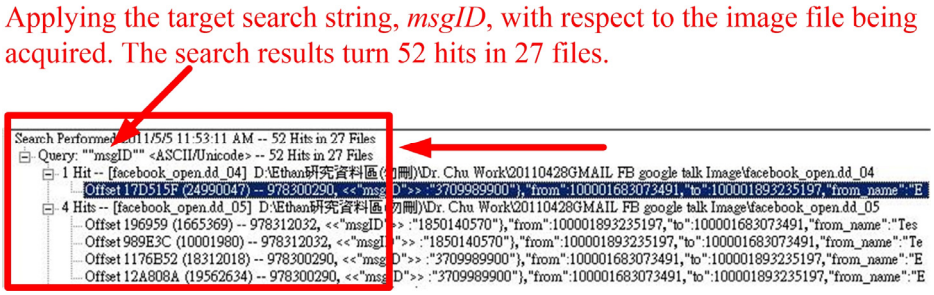

Fig. 8. Applying the target search string, *msgID*, in regard to the image file of the RAM, the search results turn 52 hits in 27 files

Stage 8: Conducting Analysis with respect to the digital evidences being obtained

Based on the digital evidences being obtained, the DF team came up with the following synthesized data: The *Facebook* ID of user *Ethan Wang* is *10001683073491*; the *Facebook* ID of user *Testman Df* is *100001893235197*, correspondingly. Furthermore, the *Facebook* user *Testman Df*, initially received the IM, *cellular number?*, from *Facebook* user *Ethan Wang* with the Unix time stamp *1303978300862* (which is interpreted as Thu, 28 Apr 2011 08:11:40 GMT) as Figure 9 demonstrated. Furthermore, The *Facebook* user *Ethan*

Wang received the replied IM, *0912345678*, from the *Facebook* user *Testman Df* with the Unix time stamp *1303978316619*, which is interpreted as Thu, 28 Apr 2011 08:11:56 GMT, as Figure 10 indicated.

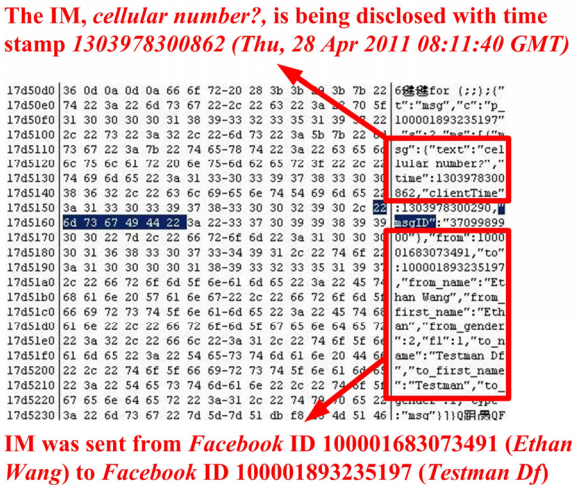

Fig. 9. Disclosing the IM, which was sent from *Facebook* ID *100001683073491* (*Ethan Wang*) to *Facebook* ID *100001893235197* (*Testman Df*) with the time stamp *1303978300862*

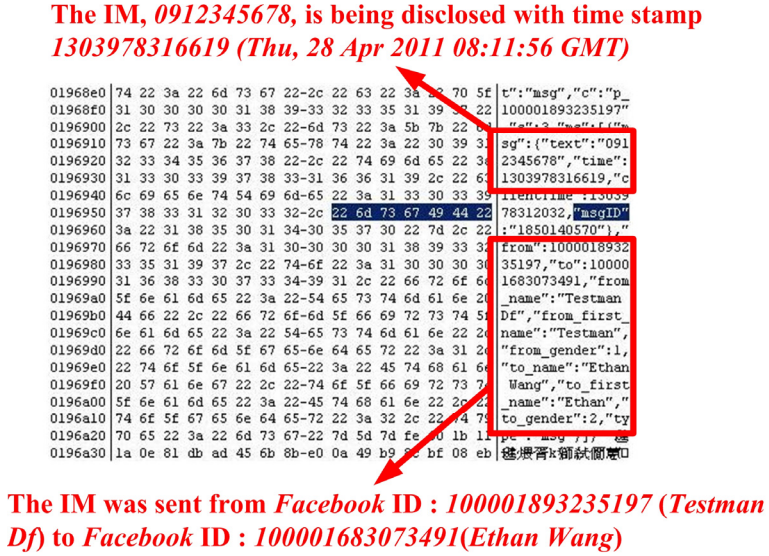

Fig. 10. Disclosing the IM, which was sent from *Facebook* ID *100001893235197* (*Testman Df*) to *Facebook* ID *10001683073491* (*Ethan Wang*) with the Unix time stamp, *1303978316619*

Stage 9: Acquiring the image of the RAM with the clearance of all the caches and temporary files within IE as well as the shutting down of the IE before acquisition of RAM

Before conducting the same previous DF procedures, the DF team intentionally purged the cache data, history records, and the temporary files within the IE to make the contrast to the previous one. Moreover, the *Facebook* user was forced to logout out from the application and then shut down the IE browser. Momentarily, the DF team repeatedly acquired the image of the RAM of the PC applying the same target search string, *msgID*. Eventually, the received / replied IM texts, *Facebook* usernames, *Facebook* IDs, and the associated time stamps were also being successfully disclosed.

3.3 Experiment summary for *Gmail / Facebook Chat*

Firstly, for phase 1, the *Gmail Chat* section, with the IE not being shutting down, the DF team was capable of disclosing the IM text from the sender side with the time stamp via the specific target search string, *active*. Unfortunately, the DF team was not able to find the IM text that the receiver replied to the sender. On the other hand, with the IE being shutting down, the DF team was not able to find the IM with respect to the *Gmail Chat*. Additionally, the DF team was not capable of spotting the IM text being received and the time stamp, either.

Consequently, this research paper strongly recommend the DF team to conduct the RAM acquisition of the PC on the crime scene without shutting down the IE to avoid the evaporation of the intangible digital traces, which is a permanent and irreversible phenomenon.

Secondly, for phase 2, the *Facebook Chat* section, it does not matter whether the IE was being shut down or not, the previous acquisition procedures were able to identify the IM text, the time stamp, *Facebook* ID, and *Facebook* user name. Consequently, this paper provides substantive paradigms or guidelines for the DF specialists or law enforcement agencies to consider when the related cybercrimes occurs especially when *Facebook Chat* are involved in the information incident.

In addition, for both phases, this paper also pinpoints the essences of digital traces collection, analysis, and presentation between these two contemporary IM APs with respect to the execution statuses of IE.

4 Conclusion

Unquestionably, the pervasiveness of the ubiquitous IM communication channel provides the unparalleled convenience for global communities in terms of ICT. Unfortunately, it provides plethora of opportunities for heinous cyber crime syndicate to commit illegal conspiracies due to its convenience. Imperceptible digital traces would be inadvertently left behind somewhere in the computing system when IM is involved, especially the web browser. Demonstrably, those UGC digital traces could be probative evidences in a court of law nowadays. Consequently, this research paper suggests that the status of the IE (execution or shut-off) could result in the admissibility of the evidences in some cybercrimes when *Gmail* / *Facebook Chat* sessions are involved from the aforementioned design of experiment. The paper presents the availability for researchers and practitioners in terms of digital trails investigation during generic *Gmail* / *Facebook Chat* sessions. In conclusion, this paper substantively plays a decisive and critical role for the DF experts to ponder when the similar situations are facing concerning some information security issues under time constraint manner.

Acknowledgement

The author would like to acknowledge the funding support of National Taichung University of Education of Taiwan concerning the research grant of year 2013 (NTCU-F102104).

References

[1] A. Distefano, G. Me, "An Overall Assessment of Mobile Internal Acquisition Tool," *Digital Investigation*, Vol. 5, Supplement, pp. S121-S127, 2008.

[2] A. Orebaugh, J. Allnutt, "Data Mining Instant Messaging Communication to Perform Author Identification for Cybercrime Investigation," in *Proceedings of ICDF2C 2009*, Vol. 31 of LNICST, pp. 99-110, 2010.

[3] C. Jisung, J. Sangjun, P. Jungheum, L. Sangjin, "A Digital Forensic Analysis for Mac OS X Main Artifacts," in *Proceedings of Conference of the Korea Information Processing Society (KIPS)*, Vol. 18, No. 2, pp. 846-849, 2011.

[4] H. Luo, M. Shyu, "Quality of Service Provision in Mobile Multimedia - A Survey," *Human-centric Computing and Information Sciences*, Vol. 1, Article 5, 2011.

[5] J. Lee, H. Chung, C. Lee, S. Lee, "Methodology for Digital Forensic Investigation of iCloud, Information Technology Convergence, Secure and Trust Computing, and Data Management," in *Proceedings of ITCS 2012 & STA 2012*, Vol. 180 of LNEE, pp. 197-206, 2012.

[6] M. Taylora, J. Haggertyb, D. Grestyc, R. Hegarty, "Digital Evidence in Cloud Computing Systems," *Computer Law & Security Review*, Vol. 26, No. 3, pp. 304-308, 2010.

[7] M. W. Andrew, "Defining a Process Model for Forensic Analysis of Digital Evidence Devices and Storage Media," in *Proceedings of the 2nd International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE)*, IEEE Press, pp. 16-30, 2007.

[8] N. Ruff, "Windows memory forensics," *Journal of Computer Virology*, Vol. 4, pp. 83-100, 2008.

[9] P. Grabosky, "Requirements of prosecution services to deal with cyber crime," *Crime Law and Social Change*, Vol. 47, No. 4, pp. 201-223, 2007.

[10] S. Anson, S. Bunting, *Windows Network Forensics and Investigation*, Elsevier Science Publishers, Amsterdam, the Netherlands, 2007.

[11] S. Krasser, G. Conti, J. Grizzard, J. Gribschaw, H. Owen, "Real-time and Forensic Network Data Analysis Using Animated and Coordinated Visualization," in *Proceedings of 6th Annual IEEE Information Assurance Workshop (IAW)*, pp. 42-49, 2005.

[12] V. Viswanathan, I. Krishnamurthi, "Finding Relevant Semantic Association Paths through User-Specific Intermediate Entities," *Human-centric Computing and Information Sciences*, Vol. 2, Article 9, 2012.

[13] X. Wang, Y. Sang, Y. Liu, and Y. Luo, "Considerations on Security and Trust Measurement for Virtualized Environment," *Journal of Convergence*, Vol. 2, No. 2, pp. 19-24, 2011.

[14] Y. Gao, G. G. III. Richard, V. Roussev, "Bluepipe: A Scalable Architecture for On-the-spot Digital Forensics," *International journal of Digital Evidence*, Vol. 3, pp. 1-18, 2004.

[15] Y. P. Lai, P. L. Hsia, “Using the Vulnerability Information of Computer Systems to Improve the Network Security,” *Computer Communications*, Vol. 30, pp. 2032-2047, 2007.