Facebook®: Do You Leave a Trace?
A Forensic Analysis of Facebook® Artifacts

Katherine Helenek, BS, Josh Brunty, MS, Christopher Vance, BS, Terry Fenger, PhD
Marshall University, Huntington, WV 25701
Forensic Science Program

> Abstract

- Much of the population now uses digital devices
- Threats shifting from corporeal world into the realm of cyberspace
- Internet crime increasing each year[3] (see Figure 1)
- Law enforcement agencies claim at least half of their cases now contain a digital component[3]
- Reflecting the increase in Internet use, popularity of social networking sites has risen as well
- At least 750 million active users on Facebook®, more than half of whom log on daily[8]
- A forensic analysis was performed to recover the location of Facebook® chat and message artifacts
- Potential evidence can be accessed quickly by forensic investigators

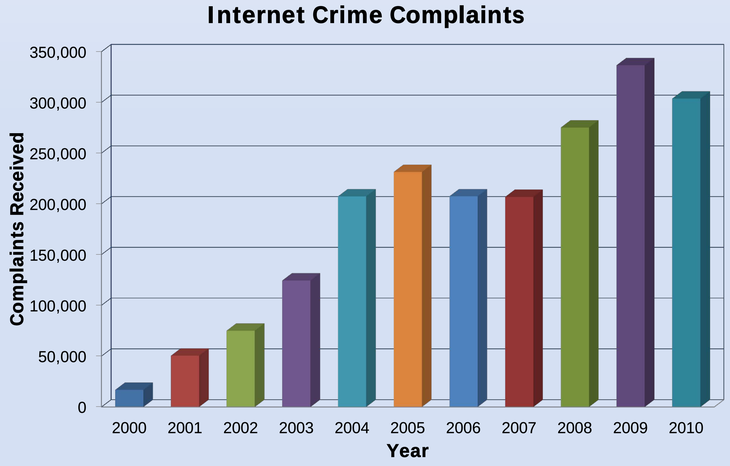

Figure 1: Internet Crime Complaint Center (IC3) complaints per year of crimes consisting of an Internet component

> Materials

- Dell Precision 690 computer containing hot swap bay and externally attached NexStar Hard Drive Dock from Vantec®
- Seagate® 500 Gigabyte hard drive and Seagate® 250 Gigabyte hard drive
- Category 5 Ethernet (CAT 5e) cable connected to a 16-port gigabit switch
- AccessData's Forensic Toolkit® version 3.2.0.32216
- VMware® Workstation version 7.2.1 build 301548
- Forensic Toolkit® Imager version 3.0.1.1467
- DCode version 4.02a build 9306

This project was supported by Award No. 2010-IJ-CX-K025 awarded by the National Institute of Justice (NIJ), Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this publication and/or exhibition are those of the author(s) and do not necessarily reflect the views of the Department of Justice.

> Methods

Facebook® Profile Creation

- Three Gmail™ accounts set up from Google©
- Three new user profiles created on Facebook® in order to have pure data

Virtual Machine (VM) Creation

- VM created with Microsoft® Windows 7™ Ultimate
- Original cloned 3 times to create IE®8 VM
- Process repeated for Windows® Internet Explorer® 9, Mozilla Firefox® 4, Mozilla Firefox® 5, Google© Chrome 11, Google© Chrome 12, and Apple© Safari 5

Single Facebook® Chat Study

- One profile logged into Facebook® on each VM
- Chat initiated between 2 profiles
- One VM imaged using FTK® Imager
- Imaged loaded into Forensic Toolkit® for examination
- Repeated for each browser

Facebook® Message Study

- One profile logged into Facebook® on each VM
- One profile sent message, next profile read new inbox message, last profile read already read message
- Each VM imaged using FTK® Imager
- Imaged loaded into Forensic Toolkit® for examination
- Repeated for each browser

Simultaneous Facebook® Chat Study

- One profile logged into Facebook® on each VM
- Chat initiated between 3 profiles
- One VM imaged using FTK® Imager
- Imaged loaded into Forensic Toolkit® for examination
- Repeated for each browser

> Results

Single Facebook® Chat Study

- Chats recovered for each tested browser (see Table 1 for locations)
- Same chat format recovered in each tested browser (see Figure 2)
- Each chat artifact gives the header and footer, transaction, contact ID, sequence ID, entered text, time and date stamp, sender, and receiver


```
for (;;);{
"t":"msg",
"c":"p_100002455245156",
"s":8,
"ms":[{"msg":{
"text":"hey whats up",
"time":1307640759009,
"clientTime":1307640750694,
"msgID":"2844576584"},
"from":100002375414629,
"to":"100002455245156",
"from_name":"Ethan Misde",
"from_first_name":"Ethan",
"from_gender":2,
"fl":1,
"to_name":"Lucy Misde",
"to_first_name":"Lucy",
"to_gender":1,
"type":"msg"}]}
```


Figure 2: Chat artifact recovered using FTK®

Browser	File Name	File Path	File Category
Internet Explorer® 8	p_*FacebookID* = *#*[1].txt	*/ImageName*/Partition 2/NONAME [NTFS]/[root]/Users/*UserName*/AppData/Local/Microsoft/Windows/Temporary Internet Files/Low/Content.IE5/*XXXXXXXX*/p_*FacebookID*= *#*[1].txt	JSON file
Internet Explorer® 9	p_*FacebookID* = *#*[1].txt	*/ImageName*/Partition 2/NONAME [NTFS]/[root]/Users/*UserName*/AppData/Local/Microsoft/Windows/Temporary Internet Files/Low/Content.IE5/*XXXXXXXX*/p_*FacebookID*= *#*[1].txt	JSON file
Mozilla Firefox® 4	_CACHE_001_	*/ImageName*/Partition 2/NONAME [NTFS]/[root]/Users/*UserName*/AppData/Local/Mozilla/Firefox/Profiles/f0vypw4f.default/Cache/_CACHE_001_	Unknown
Mozilla Firefox® 5	_CACHE_001_	*/ImageName*/Partition 2/NONAME [NTFS]/[root]/Users/*UserName*/AppData/Local/Mozilla/Firefox/Profiles/f0vypw4f.default/Cache/_CACHE_001_	Unknown
Google© Chrome 11	data_1	*/ImageName*/Partition 2/NONAME [NTFS]/[root]/Users/*UserName*/AppData/Local/Google/Chrome/User Data/Default/Cache/data_1	Unknown
Google© Chrome 12	data_1	*/ImageName*/Partition 2/NONAME [NTFS]/[root]/Users/*UserName*/AppData/Local/Google/Chrome/User Data/Default/Cache/data_1	Unknown
Apple© Safari 5	Cache.db	*/ImageName*/Partition 2/NONAME [NTFS]/[root]/Users/*UserName*/AppData/Local/Apple Computer/Safari/Cache.db	SQLITE Database

Table 1: Location of chat artifacts in tested browsers

Simultaneous Facebook® Chat Study

- Same results as Single Facebook® chat study
- Sequence ID reflected exact order of entered text throughout both conversations

Facebook® Message Study

- Unable to recover, partially recovered, or fully recovered (see Table 2)
- Message artifacts recovered in various areas: Internet History, Cache, Temporary Internet Files, Slack Space, Unallocated Space

Browser	Sent Message	New Inbox Message	Already Read Message
Internet Explorer® 8	Full message recovery	Partial message recovery	Unable to recover
Internet Explorer® 9	Unable to recover	Unable to recover	Unable to recover
Mozilla Firefox® 5	Full message recovery	Unable to recover	Unable to recover
Google© Chrome 12	Partial message recovery	Full message recovery	Full message recovery
Apple© Safari 5	Unable to recover	Unable to recover	Full message recovery

Table 2: Chat artifacts recovered in tested browsers

> Discussion

- Artifacts from social networking sites can be an important source of information and evidence
- Full Facebook® chat and message artifacts can be recovered
- Repeat with other popular social networks
- Normally schedule analyses when browsers updated

> References

1. CacheBack 3 Now Recovers and Rebuilds Facebook Chat [Internet]. 2010. SiQuest Corporation; [cited 2011 June 30]. Available from: http://www.cacheback.ca/news/news_release-20101110-1.asp
2. Dwyer C, Hiltz S, Passerini K. Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace. Proceedings of the Thirteenth Americas Conference on Information Systems; 2007 Aug 9-12; Keystone, CO.
3. Gogolin, G. The Digital Crime Tsunami. Digital Investigation 2010;7:3-8.
4. Kenneally EE. The Internet Is the Computer: The Role of Forensics in Bridging the Digital and Physical Divide. Digital Investigation 2005;2:41-44.
5. Livingstone S, Brake DR. On the Rapid Rise of Social Networking Sites: New Findings and Policy Implications. Children & Society 2010;24:75-83.
6. NEW! IEF Version 4 Released! [Internet]. 2011. JADsoftware; [cited 2011 June 30]. Available from: http://www.jadsoftware.com/go/?page_id=141
7. Nosko A, Wood E, Molema S. All About Me: Disclosure in Online Social Networking Profiles: The Case of FACEBOOK. Computers in Human Behavior 2010;26:406-418.
8. Statistics [Internet]. 2011. Facebook; [cited 2011 June 20]. Available from: http://www.facebook.com/press/info.php?statistics