B14 Facebook®: Do You Leave a Trace? A Forensic Analysis of Facebook® Artifacts

Katherine Helenek, BS, Joshua L. Brunty, MS, Chris Vance, BS, and Terry Fenger, PhD, Marshall University Forensic Science Center, 1401 Forensic Science Drive, Huntington, WV 25701*

After attending this presentation, attendees will learn where Facebook® chat artifacts are stored in different browsers and what the specific format means. Furthermore, attendees will understand how Facebook® message artifacts are saved and which browsers keep full messages.

This presentation will impact the forensic science community by demonstrating how forensic scientists, specifically the digital forensics community, can obtain potential evidence quickly and effectively from Facebook® artifacts.

As the use of technological devices has increased and become widespread, the internet has become mainstream for global communications used by persons, informal groups, public organizations, corporations, and governments.[1] In turn, social networks have increased in popularity as a means of contact and communication. The generic structure involves creating a profile, making connections with existing friends, and meeting new people through the site.[2] In addition, social networks allow the user to upload photos, describe their interests, explain their work and education history, post a relationship status, reveal personal stories and activities, give their current location, and even plan events.[2,3]

Facebook® was originally designed in 2004 as a social networking site specifically for Harvard University students, but has been developed throughout the years for any user over the age of thirteen.[3] Presently, Facebook® is available for general use with more than 750 million active users, half of whom log on at least once every day.[4] It is up to the users to set their own privacy settings in order to control others' access to their personal profiles; and their choices in the resulting levels of privacy are based upon their trust of the website and their trust of other users.[3]

As society has become more technologically developed, crime has transitioned from the corporate world into the digitized world of cyberspace. Law enforcement agencies claim that at least 50% of cases have a digital component, and that the number is currently rising. In 2009, the internet Crime Complaint Center (IC3) reported 336,665 complaints of internet offenses. Since 2000, the number of complaints has been increasing each year by 24.5%. The internet is a method of communication that consists of noncommittal interactions; this facet creates an easy means to take advantage of users.[5] A variety of online assaults and crimes occur every day; bullying, harassment, theft of personal information, sexual grooming, encouragement to harm others and the self, racist attacks, financial crimes, and fraud are just some of the various internet crimes that exist.[5,6]

Disclosure of certain personal information online, combined with other tools available for use on the internet, such as reverse directories, can aid fraudsters to obtain home phone numbers, full addresses, ages, and genders. These few pieces of information provide a means to acquire identity based information such as credit cards and driver's licenses, and in some cases make it possible to forge even more critical legal documents like passports.[3] It is important to recognize that these digital artifacts are contained within sources such as web pages, computer logs, internet newsgroups, and online chat rooms.[1]

A vast amount of the global population uses the internet and Facebook® each day for their activities. Unfortunately, some people are using these common places of communication for malicious and nefarious purposes. It is necessary for forensic investigators to have the ability to quickly and easily extract information from these sources so that evidence may be acquired as efficiently as possible. It should be feasible to recover Facebook® chat artifacts and discern a common pattern in order to quickly search for any previous chats. Furthermore, Facebook® messages may be able to be recovered, or parts of messages, in order to attain some information or at least create an apparent link between users.

In order to start off with pure profiles, three new user profiles were created on Facebook®. This was performed by first setting up three Gmail™ accounts from Google©; it was then possible to use these email addresses to create Facebook® profiles. Three virtual machines (VMs) were created (one per profile) for each browser that was to be tested. The "Windows 7 Original" VM was cloned and Internet Explorer® 8 was used to download each additional browser to be examined. This process was followed to set up three virtual machines each for Windows® Internet Explorer® 9, Mozilla Firefox® 4, Mozilla Firefox® 5, Google© Chrome 11, Google© Chrome 12, and Apple© Safari 5, totaling twenty-one virtual machines to use for the analysis. A *Single Chat Study*, a *Simultaneous Chat Study*, and a *Sent Message, New Inbox Message, and Already Read Message Study* were performed. A forensic duplicate image was taken from each VM using FTK® Imager and loaded into Forensic Toolkit® for examination.

References:

1. Kenneally EE. The Internet Is the Computer: The Role of Forensics in Bridging the Digital and Physical Divide. Digital Investigation 2005;2:41-44.
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. 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.

 ** Presenting Author*

4. Statistics [Internet]. 2011. Facebook; [cited 2011 June 20]. Available from: *http://www.facebook.com/press/info.php?statistics*
5. Gogolin, G. The Digital Crime Tsunami. Digital Investigation 2010;7:3-8.
6. Livingstone S, Brake DR. On the Rapid Rise of Social Networking Sites: New Findings and Policy Implications. Children & Society 2010;24:75-83.

Facebook®, Internet, Digital

 ** Presenting Author*