Proceedings of Student-Faculty Research Day, CSIS, Pace University, May 8th, 2009

Forensics Tools for Social Network Security Solutions

Janet Cheng, Jennifer Hoffman, Therese LaMarche, Ahmet Tavil, Amit Yavad, and Steve Kim
Seidenberg School of CSIS, Pace University, White Plains, NY 10606, USA

Abstract

The usage of Social Network Sites has increased rapidly in recent years. Since the success of a Social Network Site depends on the number of users it attracts, there is pressure on providers of Social Network sites to design systems that encourage behavior which increases both the number of users and their connections. However, like any fast-growing technology, security has not been a high priority in the development of Social Network Sites. As a result, along with the benefits of Social Network Sites, significant security risks have resulted. Providing Social Network Site users with tools which will help protect them is ideal. Tools are developed for installation on a user's computer to provide them the ability to retrieve other online user information via chat and social network websites. These tools will also benefit law enforcement agents when crimes are committed.

1. Introduction

This paper analyzes and extends the forensic tools developed in an earlier study for protecting Social Network Site users from security threats [14]. First, we will identify the security issues found in Social Network Sites. Second, we will demonstrate how our tools can provide users with more information which we hope will help prevent them from becoming victims. Finally, if a crime has been committed, we will detail the tools available to assist in apprehending the perpetrator.

The tools we developed retrieve Social Network Site user's non-personal-identifiable information, such as IP address, operating system, browser type, etc. Retrieval of this information occurs upon the virtual contact from that other person, be it by them simply browsing our personal page, or by other person contacting via Virtual Meeting, for example chatting. This paper covers methodologies used, test results, and future goals.

The Social Network Site security issues are: [4] Corporate Espionage; Cross Site Scripting, Viruses & Worms; Social Network Site Aggregators; Spear Phishing & Social Network specific Phishing; Infiltration of Networks Leading to data leakage; I.D. Theft; Bullying; Digital Dossier Aggregation Vulnerabilities; Secondary Data Collection Vulnerabilities; Face Recognition Vulnerabilities; CBIR (Content-based Image Retrieval); Difficulty of Complete Account Deletion; Spam; and Stalking.

2. Case Studies

There are many criminal activities arising from the use of social network sites. For example, a mother was convicted of computer fraud for her involvement in creating a phony account on MySpace to trick a teenager, who later committed suicide [15]. The tools found in this paper can be used to track and help minimize or prevent crimes related to social networks.

3. Methodology

The methods used in designing the data retrieval tools and storage mechanisms include PHP websites with MySQL databases, Java applets, a Java web application with an Access database and NetStat via MSDOS scripting. We anticipate that many of the methods can be used on any computer without any technical know-how.

4. Social Networking Websites

4.1. Definition

We define social network sites as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site [2].

4.2. Privacy Issues

Facebook's Beacon service tracks activities from all users in third-party partner sites, including people who never signed up with Facebook or who have deactivated their accounts. This is an example of a vulnerability in Facebook (among others) [10], yet a user can use this vulnerability to their advantage.

Beacon captures data details on what users do on the external partner sites and sends it back to Facebook server, along with users' IP addresses, the addresses of Web pages the user visits, etc.

4.3. Security Features and Privacy

We have evaluated the security features on the Top Ten (10) Social Networking Websites of 2009 [18]. Table 1 summarizes these security features. The website support of third party scripts is considered a security hole which this study's visitor tracker utilizes.

Social Network	Supports HTML	Visitor Tracker	Customizable Privacy Settings
Bebo	No	No	Yes
Facebook	No	No	Yes
Friendster	No	Yes	Yes
Hi5	Yes	Yes	Yes
MySpace	Yes	No	Yes
Netlog	No	No	Yes
Orkut	No	Yes	Yes
PerfSpot	Yes	Yes	Yes
Yahoo!360	Yes	No	Yes
Zorpia	No	No	Yes

Table 1. Security features on top ten social networks. "Supports HTML" means the network allows HTML code implemented into the user's profile. "Visitor Tracker" means the websites enables users to view who had viewed their profiles. "Customizable Privacy Settings" means the website allow you to control who can view your profile.

4.3.1. Facebook

Facebook's security and privacy settings are more advanced than other sites, allowing it to be discussed separately. It offers robust, customizable privacy settings which allow users to show or hide different sections of their profile. The settings can be specific to a single user, list of users, networks, the entire member base and internet users querying search engines with your name.

Facebook does not allow users to embed any code on their user pages. However, it does allow third party applications to be installed on a user's page, which opens up security issues if a developer decides to create an application that does not behave as advertised. Caution should be exercised when installing any third party applications.

4.3.2. Websites that Allow Third Party Scripting

The websites listed in this section allow third party scripting (e.g. HTML, Javascript). This opens up an opportunity for third party scripts to be executed when visitors access a user's page.

MySpace does not allow Java Script code to be used in their site [5]. But, it does allow HTML code.

The users of MySpace and Hi5 have the ability to add HTML code which can link to scripts and objects designed to retrieve other visiting user's information. The users of PerfSpot are also allowed to add HTML code to their pages, but there are restrictions on the contents of this code.

While some had strict security settings, Yahoo!360 lack detailed security controls as to who can view the user's profile. Their option is either everyone can view their blog or just friends. In other social networks such as, Facebook and MySpace, specific security features are available to provide users with more control over their personal information.

4.3.3. Websites Which Provide a Visitor Tracker

Friendster, Hi5, Orkut, and PerfSpot users have the benefit of monitoring their profile visitors. This option increases awareness, protection and eases user tracking. Orkut is the only social network that forces the user's viewing history to be revealed if he/she decides to track other users who had viewed their profiles.

5. User Data Retrieval

5.1. User Data Retrieval from Social Networking Websites

It is possible to retrieve information about the users who visits your profile on Social Network Sites. Some of these sites provide built-in applications which show the user names of the people who visit your profile. Other sites store log transcripts, which capture chat session information such as username and date.

The function of user data retrieval can be accomplished within a website with user incorporation of either Java Script or PHP code [12]. Some Social Network Sites have restrictions in place to make Java Script and/or PHP code inactive, when a user tries to incorporate into their site.

Covered in this paper are the different methods for capturing the non-personal identifiable information, of users visiting/communicating with us in the virtual world. We have established that user data retrieval can be achieved with use of web based scripts.

The user data retrieval methods presented take place in the online environments of websites, IM chat sessions (virtual meetings), and emails. From the user data retrieval methods used, the most important non-personal-identifiable user information we have retrieved is the IP address. An IP address can be used for tracking back to a user's location, or the user's ISP location. After retrieving the IP address, there are many links available to for retrieving the geographical location of the user [9].

5.2. Data Retrieved by PHP

Program: Social Networking Visitor Tracker

In this study we have extended this tracker program into a website called "Social Networking Visitor Tracker" [17]. The scripts work on any social networking website which allows you to embed HTML code in your homepage. A group of social networking website users was assembled to test this program and provide recommendations for improvements.

The following social networking websites have been tested to be compatible with our program. At the beginning of this study, the list in Table 2 consisted of the Top 10 Social Networking Websites of 2009 [18] as shown in Table 1. As the study progressed, additional modules where provided to meet testing team requests.

Social Networking Website	Supports Visitor Tracker Program
AOL Instant Messenger	Yes
Bebo	No
DeviantArt.com	No
eBay	Yes
Facebook	No
Friendster	Yes
Hi5	Yes
NetLog	No
MySpace	Yes
Orkut	No
PerfSpot	No
Yahoo!360	Yes
Zorpia	No

Table 2. Summary of modules available on this study's tracking site along with their compatibility.
Testing occurred on all top ten (10) social networking sites, regardless of any existing visitor tracking functionality.

The website was built using PHP and MySQL. This new site provides the following features:

- Users must create an account on the tracking website and login to access logs.
- Logs are saved into a MySQL Database.
- The link embedded into the social networking profile page is unique to each user, generated after the user logs into the tracking website and generates their module.
- Project team members will have access to a user management section.
- IP Address
- The ability to track the IP of the visitor back to their ISP, which can reveal their geographic location.
- Browser name and version.
- Operating system and version

5.3. Data Retrieved by Facebook API

Program: Facebook Application

Currently, creating a visitor log for Facebook using the Facebook programming API is against the Facebook Developer terms and conditions. Users who attempt to create an application which tracks profile hits without visitor knowledge will be banned from the site if the application is found. At the time of this publication, this study was continuing to investigate ways to implement a visitor tracker and progress will be reported on the "How it Works" section of the Social Networking Visitor Tracker website.

5.4. Data Retrieved by Java

Program: ClientUI

The previous study developed a Java website called ClientUI [14]. After examining the code, however, we conclude that this website is unnecessary because it accomplishes the same goals as the PHP website.

5.5. User Data Retrieval: Email

The following section discusses how to retrieve the sender's IP address from an email you received at your Gmail, Hotmail and Yahoo! Mail accounts.

Gmail

1. Access your inbox
2. Select the message you would like to trace for its IP
3. Click on the upside down triangle located on the right, next Reply. You will see options such as

“Reply to all”, “Forward”, “Filter Messages like This”, and etc.
4. Select “Show Original”

Hotmail
1. Make sure you are in classic mode
2. Right click on the message
3. Select “View Message Source”

Yahoo! Mail
1. Select the message
2. Right click on the message
3. Click on “View Full Headers”

5.6. Purpose

Knowing more about the person communicating with you online can protect you. Due to the increased amount of crimes being committed over the internet, knowing the true identity and location of others can add another layer of protection.

6. MAC Addresses

A media access control address (MAC) is a unique identifier assigned to most network adapters and network interface (NIC) cards. When this identifier is assigned by the manufacturer, the MAC address is usually the encoded manufacturer’s registered ID number. A MAC address can be compared to the license plate on an automobile. Each registered vehicle has a unique license plate number. Similarly, each network adapter / NIC card has a unique MAC address.

6.1. MAC Address Retrieval

6.1.1. MAC Address Retrieval using operating system commands

The commands in Table 3 display the current configuration of the network interface on a computer.

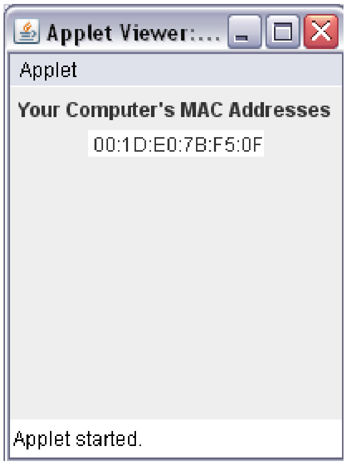
Operating System	Command
Most *nix systems (LINUX / MAC OS 10.4+ / UNIX)	Ifconfig –a
Windows (versions NT and newer)	Ipconfig \all

Table 3. Network interface commands

6.1.2. MAC Address Retrieval using Java Applets

The current study has produced an applet which returns the MAC Address of each enabled network card installed on the client computer. Note: When this applet is run on the project server, the applet takes a long time load. If the applet is run on a local computer, the load time is a few seconds.

Figure 1 displays a screenshot of the applet, which displays the user’s MAC address.



Your Computer's MAC Addresses
00:1D:E0:7B:F5:0F
Applet started.

Figure 1: MAC address retrieved via Java applets

6.1.3. MAC Address Retrieval using C# .NET 2.0

This study has developed an executable that returns the MAC address of the computer it is executed on. Currently, the application returns the first MAC address and associated IP. Future development can include returning all MAC addresses and their associated IP addresses.

6.2. MAC Address Spoofing

6.2.1. What is MAC Address Spoofing

MAC Address Spoofing is a technique used by hackers to change the MAC address of their computer. The hacker obtains a valid MAC address using a network analyzer (such as Wireshark), then changes their MAC address to this value using the steps in the next section.

6.2.2. How to Spoof a MAC Address

*NIX Systems (LINUX / MAC OS 10.4+ / UNIX)

The Ifconfig can be used in most *NIX systems to change your MAC address. The following command will bring down the driver for the given interface.

```
ifconfig {name of interface} down {MAC
Address}

example: ifconfig eth0 down 00:00:00:00:00:01
```

Figure 2: Disable network device

The next command activates the interface:

```
ifconfig {name of interface} up

example: ifconfig eth0 up
```

Figure 3: Enable network device

Windows Systems

There are several ways to change the MAC Addresses on your network devices.

MAC Addresses can be changed manually on a Windows OS by modifying the properties of the network adapter, if that adapter supports Clone MAC Addresses.

If the adapter does not support this, you will need to modify the registry entries. If you are not familiar with regedit, there is a program called SMAC which can accomplish this task. SMAC is a MAC address Spoofer which runs on Windows 2000, Server 2003, XP and Vista. It can allow you to change your MAC Addresses registry information with a user friendly application.

6.2.3. Reasons Hackers Spoof MAC Addresses

This technique allows the hacker to circumvent MAC address filtering in a router in order to gain access to a wireless network. A valid MAC address was sniffed out of the air by running a network analyzer in monitor mode. The hacker then changes their MAC address to the address found using the steps in “How to Spoof a MAC Address”. Now the hacker can access the network under a false identity, keeping their real MAC address out of the Dynamic Host Configuration Protocol (DHCP) logs.

6.3. Purpose

6.3.1. How Cyber Forensic Investigators use MAC Addresses

Office productivity applications (Microsoft Office) can embed various pieces of system information into the documents they create. A cyber forensic investigator would be interested in these documents because they can contain the user name of the person who created the document, the license number of the application used to create the document or even the MAC address of the system used to create the document.

6.3.2. How Users can benefit from MAC Addresses knowledge.

Users can also benefit from MAC Address knowledge by allowing them to keep track of who they are communicating with over the internet. This can possibly be very beneficial to parents who wish to monitor their children’s web surfing and chatting habits.

7. Tools and Applications

7.1. Computer Data Logs

The following section presents some of the software applications that are recommended in the cyber forensics field. Even though this software is commonly utilized in the field, the investigator should grasp a deep understanding of the case environment and specifications and understand the limits of the tools before performing any investigations. For example, the user should consider whether the forensic tools can perform searches on the specific computer platform such as Windows, Linux, MAC, and so on [11].

7.1.1. Software to Monitor Computer

Spytech NetVizor is powerful computer spy software that monitors all activities performed on the computer. Tasks include from keystrokes typed email activity to application content filter in. Logs and reports can be viewed real time. Some of the crucial functions involve detailed reporting and activity breakdown to your customization, protecting network data from theft, preventing certain behaviors, such as website, files, or application accessing, and permitting large scale of computer network monitoring ability including on and off site [6].

Universal IM History Decoder decodes message history from MSN Messenger, Yahoo! Messenger ICQ Messenger, and Miranda Messenger. This powerful program can let you view not limited to your history message but also other’s conversations including offline and without password. It also recovers stored passwords. All decoded messages could be saved to .txt or .tf file. It also includes auto-detection of all installed user profiles and date filter selection [6].

IM-History is a web service that allows users to access their chat history online. Users may manage their chat histories and contacts through a server, having unlimited access from PC, laptop or any web-enabled hand held devices. The service permits quick searches in information. Even though this is a web service, IM-History Client Suite must be installed into the computer and be running in the tray bar for application to save all contacts and chat logs. Supported messengers include Skype, Yahoo! Messenger, AIM, Windows Live Messenger, ICQ, Trillian, Pidgin, Miranda, and QIP 2005. Message history is stored on secure servers and nobody except you can access them. [6].

Digital Forensics

Guidance Software EnCase Forensics is one of the many common applications used in the industry. The program has a complex GUI, analytics, and powerful scripting engine. The application can investigate and analyze different operating systems, such as, Windows, Linux, AIX, OS X, Solaris, and etc. It also can manage a large volume of data including the deleted files, and there are customizable reports for presentation [6].

X-Ways Forensics is an advanced work environment for computer forensic examiners. Some of the functions performed by this tool includes: disk cloning and imaging; data recovery; file carving, support for FAT and NTFS, hard disk cleaning, mass hash calculation for files, and reviewing slack space.

Spider shows all of the URLs and cookies stored in the index.dat file, and will then allow the user to remove them [6].

D.I.M Digital Investigation Manager
A software tool for managing Incident Response and Forensic Acquisition procedures D.I.M. allows operations to be organized by case. Each case may contain an unlimited number of Hosts (Workstations, Servers, Laptops, PDAs, etc.). Items of evidence are associated with each host (Hard Disk, CD/DVD-ROM, Memory Card, Log File, Network Dump) [6].

Yahoo Messenger Chat Recovery easily decodes all your private messages like instant messages, conferences and mobile SMS. Yahoo archive viewer can recover and view not only yours but others chats conversation, while offline and saves it in plain or RTF rich text format. This software retrieves all chat history that is stored on your PC. The program allows you to read Yahoo's archive (.dat) files, enabling you to see all chat records which take place on your computer. Following are the details on the software's usability:

- Retrieve chat history files stored on your system or any other system on the network
- Recover all encoded archive file of any yahoo account
- Works with all versions of Yahoo Instant Messenger
- Software can auto detects stored yahoo chat conversation logs and decode it
- Program recovers all SMS messages that are sends from yahoo messenger to any mobile phone numbers
- Enable and disable yahoo archive setting even you are not login
- Import any external yahoo archive file and decode it when it is not in yahoo directory
- View any yahoo archive file on your computer even you don't know the password of that account [6].

7.1.2 Data Recovery/Investigation Tools

Registry Information Extractor is a test release of a software utility that is in development and under testing. It is a Windows 95/98/ME system.dat registry information extractor. It will be updated to extract a lot more information from the registry. At present it will only extract system.dat information from Windows 95/95 and ME. It can extract the following information: Registered Owner, Registered Organization, Windows Version, Windows Version Number, Windows Installed Date & the Computer Name. RIE can also be used as a File Viewer from within EnCase [6].

PC Inspector File Recovery is a data recovery program that supports the FAT 12/16/32 and NTFS file systems. Some of the features in PC Inspector File Recovery 3.x are as follow [6]:

- Finds partitions automatically, even if the boot sector or FAT has been erased or damaged (does not work with the NTFS file system)
- Recovers files with the original time and date stamp
- Supports the saving of recovered files on network drives
- Recovers files, even when a header entry is no longer available

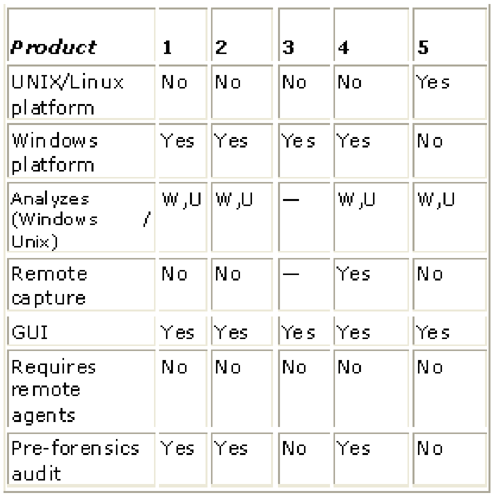
Gargoyle Forensic Pro is a program that can determine if any malware is present on a system, any application that can disrupt or damage the computer. It can perform threat management, compliance audits, detects “bad” programs, and provides potential suspects. The software is capable of organizing data into relational database. Each dataset is created for the different malware category [6][20].

DiskCat catalogues all files on disks. It is short for “disk cataloguer”. It creates a list (catalogue) of all files and/or directories on a hard or floppy disk. With its many options, the operation can be customized to your needs. It is especially useful for forensic investigations. Output is a fixed length record and database compatible (for further analysis/sorting) [6].

Active Partition Recovery is a small, easy to use DOS Program, which allows you to [8]:

- Recover deleted partitions (FAT and NTFS)
- Restore deleted FAT and NTFS Logical Drives
- Create Drive Image - for backup purposes
- Scan hard drives and detect deleted FAT and NTFS partitions and/or Logical Drives
- Preview files and folders on deleted partition or drive, to recover proper data
- Backup MBR (Master Boot Record), Partition Table, Boot Sectors Restore MBR, Partition Table and Boot Sectors from backup if damaged [1].

Table 4 summarizes the capabilities of the forensics tools such as the platforms that it can analyze, GUI, Pre-forensics audit.



Product	1	2	3	4	5
UNIX/Linux platform	No	No	No	No	Yes
Windows platform	Yes	Yes	Yes	Yes	No
Analyzes (Windows / Unix)	W,U	W,U	—	W,U	W,U
Remote capture	No	No	—	Yes	No
GUI	Yes	Yes	Yes	Yes	Yes
Requires remote agents	No	No	No	No	No
Pre-forensics audit	Yes	Yes	No	Yes	No

Table 4. Capabilities of forensics tools [11].
Product 1-Encase Forensic (Guidance Software)
Product 2-Forensic Toolkit (AccessData)
Product 3-i2Analyst's Notebook (i2 Inc.)
Product 4-ProDiscover Incident Response (Tech Partners)
Product 5-Sleuth Kit/Autopsy Browser (Open source)

7.1.2. PDA Investigation Tools

Pilot-Link is used to retrieve information from ROM and RAM of Palm PDA hand-held. The synchronization allows information retrieval from devices, back up information, and etc.

Pilot-xfer can additionally be used to allow acquisition [6][13].

Paraben PDA Seizure the program is designed to capture data information from PDA devices for Palm & Windows CE operating systems. The application embedded quick searches and bookmarking, such as Text and hex views on data HTML reporting [16].

7.2. Network Investigation Tool

Spector CNE can be used to record everything your employees do online, including instant messages, chats, emails sent and received, web sites visited, applications launched, files downloaded and keystrokes typed [16].

7.3. Purpose

The forensics tools discussed in this section can be used to help monitor who a person or a person’s child is communicating with over the internet and which websites they are visiting. They can add another layer of protection between a user and the World Wide Web.

8. Conclusion

Security has become a major concern on Social Networks. It is very important that we find the right solutions to tackle the different security problems on the Social Network Site’s today. Some of these solutions can be stricter regulations, better user education and tougher penalties for criminals. The scripts described in this paper should be utilized to their fullest advantage in the virtual communication world. The tools described here can be used to help in investigations of Social Network Site crimes and to raise user awareness. These tools can be used to help protect and educate users from the start of their Social Network Site interactions, thereby preventing crimes from even occurring. We should also utilize the free software that is available on different websites to track the activities of the visitors on the website, among others available.

9. Recommendations

If a user decides they want to go out to meet someone they have met on Social Network Site, they should take precautions, and our Social Network Site software add-on is highly recommended. It would be useful if the Social Network Sites were to make this available to their users.

We can also do things such as refrain from using Internet Explorer as our browser to protect us from hacking. There are alternative browsers that do not support ActiveX, such as Firefox, Opera or Safari which are safer to use. In summary, Social Network Site security has space for more research and further development.

10. Future Enhancements

- Assigning the applet used to identify the Mac address of the client to the website
- Retrieving the UserName of other user accessing the monitored Social Network page
- Develop a visitor tracker application which complies with the Facebook Developer Terms and Services.
- Develop additional modules for the Social Networking Visitor Tracker. (CraigsList, Second Life, other versions of AOL Instant Messenger)

11. References

[1] Anonymous. (2009). Forensics-tools. http://www.forinsect.de/forensics/forensics-tools.html, accessed December 2008

[2] Boyd, d. m., and Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication, 13(1), article 11. http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html

[3] Django Software Foundatioin.(2009). Request and response objects. http://docs.djangoproject.com/en/dev/ref/request-response/?from=olddocs, accessed December 2008

[4] Drislane, H. and Heffner, K. http://www.eecs.harvard.edu/cs199r/fp/HelenKelly.pdf, accessed December 2008

[5] Eventful Inc., (2009). http://eventful.com/faq, accessed December 2008

[6] Forensics Computing Ltd. (2004). Computer forensic software tools downloads. http://www.forensic-computing.ltd.uk/tools.htm, accessed December 2008

[7] Forensics. NL. (2009). Computer forensics tools, digital evidence software, utilities. http://www.forensics.nl/tools, accessed December 2008

[8] Free Downloads Center. (2009). Yahoo messenger chat recovery 2.0.1.5. http://www.freedownloadscenter.com/Utilities/Backup_and_Copy_Utilities/Yahoo_Messenger_Chat_Recovery.html, accessed December 2008

[9] Geobytes, Inc. (2003). IP address locator tool. http://www.geobytes.com/IpLocator.htm, accessed December 2008

[10] Karp, S. (2007, October 31). Facebook's vulnerabilities. http://publishing2.com/2007/10/31/facebooks-vulnerabilities/, accessed December 2008

[11] Marcella, A. and Menendez, D. (2008.) Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes

[12] Opentracker.net. (2009). Tracking a MySpace homepage. http://www.opentracker.net/forum/tracking-a-myspace-homepage-t536.html, accessed December 2008

[13] Pilot-link. (2009). Welcome to the pilot-link community. http://www.pilot-link.org/, accessed March 2009

[14] Silva, M. and Ian, R. and Nagpal, A, and Glover, A and Kim, S. (2008). "Virtual Forensics: Social Network Security Solutions," Proc. CSIS Research Day, Pace Univ., December 2008.

[15] Steinhauer. J. (2008). Verdict in MySpace suicide case. http://www.nytimes.com/2008/11/27/us/27myspace.html?ref=todayspaper, accessed December 2008

[16] Sun Microsystems. (2009). Interface. http://java.sun.com/products/servlet/2.1/api/javax.servlet.http.HttpServletRequest.html, accessed December 2008

[17] Team 6. (2009). Social networking visitor tracker. http://www.spajennios.com/tracker/ accessed May 2009

[18] TopTenReviews. (2009). 2009 Social networking websites product comparisons. http://social-networking-websites-review.toptenreviews.com/

[19] W3C. (1994, May 3). HTTP request fields. http://www.w3.org/Protocols/rfc2616/rfc2616-sec5.html, accessed December 2008

[20] W3C. (1994, May 3). Http requested fields. http://www.w3.org/Protocols/HTTP/HTRQ_Headers.html, accessed December 2008

[21] WetStone Technologies.(2009). Main Page. https://www.wetstonetech.com/cgi/shop.cgi?view,2, accessed March 2009

[22] Whovisited. (2006). Who visited. http://www.whovisited.com, accessed December 2008

[23] http://thehackers.freeservers.com, accessed December 2008

[24] http://connectsystems.co.uk/, accessed December 2008