

Virtual Forensics: Social Network Security Solutions

Marilyn Silva, Rajeswari Ian, Anu Nagpal, Anthony Glover, 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. The area of Social Networking currently has many security issues. 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. Making tools available to users which can provide the ability to retrieve other online user information via chat, website, along other tools which can be installed on the user's computer will be ideal in helping to tackle such issues. These will be the tools addressed in the paper.

1. Introduction

This paper aims to describe the forensic security software tools our team has developed to protect Social Network Site users from some of the currently existing security threats. First, we identified the security issues in the Social Network Sites. Although there are many security threats in Social Network Sites, we focused on creating tools to assist in the tracking down of criminals.

The tools we developed concern retrieval of Social Network Site user's non-personal-identifiable information, such as IP address, operating system, MAC address, etc. Retrieval of this information is to occur 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 going forward.

The Social Network Site security issues are: [1] 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.

1.1. Case Studies

The following is an actual NYPD criminal case that helped motivate this work. A person, let's say John, was contacted on a Social Network and decided to meet this other person. Unfortunately, the other person's intent was to rob John. In trying to escape, John ran into the street and was killed by an oncoming vehicle. This then became a homicide case.

There was another case in which a mother was convicted of charges in computer fraud for her involvement in creating a phony account on MySpace to trick a teenager, who later committed suicide [12].

There are many cases such as these, and the cases continue to grow with the expanded use of social network sites. The tools found in this paper can be used to track and help minimize or prevent crimes related to social networks.

2. Methodology

The methods used in designing the data retrieval tools and storage mechanisms include Java with some use of Java applets, Java web application, PHP code, Access database with use of SQL for storage of information retrieved from database located on the server, and NetStat via MSDOS scripting.

3. User Data Retrieval

3.1. Overview

It is possible to retrieve information about the users who visits your profile on Social Network Site such as MySpace, Face Book, etc. Some of the Social Network Site have built-in application that shows the user names of the people who visit your profile. Some Social Network Site's store log transcripts, which capture chat session information such as IP address, Mac Address, Date, etc.

Connect Systems uses a method called "click tracking" to log the visit of the users to their website [2]. It collects the IP address, Web browser type, domain name, access times, referring URLs and page views for each session.

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) [6], 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.

The users of Second Life have the ability to add scripts and objects to retrieve other visiting user's information.

MySpace users are given the ability to track other (MySpace) users that visit their profiles, by using a free third-party service called *whovisited* [16].

The function of user data retrieval can be accomplished within a website with user incorporation of either Java Script or PHP code [13]. 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. For instance, MySpace does not allow Java Script code to be used in their site [4].

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 scripts or commands.

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 [17][18].

3.2. Data Retrieved via PHP: Social Network Site

Visiting person's non-personal-identifiable information can be retrieved from a Social Network site. This can be achieved by using PHP script, and incorporating packaged link within the Social Network site. The application behind this link has been set up to automatically retrieve and store visitor's user information into a database, as soon as the visitor enters (could be a user or non-user of the Social Network). The following is the link to our user

data retrieval website, which is coded in PHP scripting language to capture user information:

<http://www.virtualforensics.net/track.php>

The captured user information is added to then included to the list of visitors already in the database. All tracked visitor information is then retrieved from the database log and displayed to following link for viewing:

<http://www.virtualforensics.net/>

In order to have this work, type enter the following line into (contains the PHP information retrieval code) into the "Headline" section of the MySpace or Facebook site which is to be monitored.

```

```

Figure 3 displays lists the user information retrieved via PHP, and Figure 4 shows the PHP source code.

```
GATEWAY_INTERFACE = CGI/1.1
SERVER_ADDR = 192.168.1.2
SERVER_NAME = 76.124.82.116
SERVER_SOFTWARE = Apache/2.2.10 (Win32) PHP/5.2.6
SERVER_PROTOCOL = HTTP/1.1
REQUEST_METHOD = GET
REQUEST_TIME = 1227063352
DOCUMENT_ROOT = C:/Program Files/Apache Software
Foundation/Apache2.2/htdocs
HTTP_ACCEPT = image/gif, image/x-xbitmap, image/jpeg,
image/pjpeg, application/x-ms-application, application/vnd.ms-
xpsdocument, application/xhtml+xml, application/x-ms-xbap,
application/x-shockwave-flash, application/x-silverlight,
application/x-silverlight-2-b2, application/vnd.ms-excel,
application/vnd.ms-powerpoint, application/msword, */*
HTTP_ACCEPT_ENCODING = gzip, deflate
HTTP_ACCEPT_LANGUAGE = en-us
HTTP_CONNECTION = Keep-Alive
HTTP_HOST = 76.124.82.116:8081
HTTP_USER_AGENT = Mozilla/4.0 (compatible; MSIE 7.0;
Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; .NET CLR
3.0.04506)
REMOTE_ADDR = 76.124.82.116
REMOTE_PORT = 49297
SCRIPT_FILENAME = C:/Program Files/Apache Software
Foundation/Apache2.2/htdocs/php/files/all.php
SERVER_ADMIN = rajj_ian@yahoo.com
SERVER_PORT = 8081
SCRIPT_NAME = /php/files/all.php
REQUEST_URI = /php/files/all.php
```

Figure 3: User's information retrieved via PHP

```

GATEWAY_INTERFACE = <?php echo
$_SERVER['GATEWAY_INTERFACE']; ?> <br>
SERVER_ADDR = <?php echo
$_SERVER['SERVER_ADDR']; ?> <br>
SERVER_NAME = <?php echo
$_SERVER['SERVER_NAME']; ?> <br>
SERVER_SOFTWARE = <?php echo
$_SERVER['SERVER_SOFTWARE']; ?> <br>
SERVER_PROTOCOL = <?php echo
$_SERVER['SERVER_PROTOCOL']; ?> <br>
REQUEST_METHOD = <?php echo
$_SERVER['REQUEST_METHOD']; ?> <br>
REQUEST_TIME = <?php echo
$_SERVER['REQUEST_TIME']; ?> <br>
DOCUMENT_ROOT = <?php echo
$_SERVER['DOCUMENT_ROOT']; ?> <br>
HTTP_ACCEPT = <?php echo
$_SERVER['HTTP_ACCEPT']; ?> <br>
HTTP_ACCEPT_ENCODING = <?php echo
$_SERVER['HTTP_ACCEPT_ENCODING']; ?>
HTTP_ACCEPT_LANGUAGE = <?php echo
$_SERVER['HTTP_ACCEPT_LANGUAGE']; ?>
HTTP_CONNECTION = <?php echo
$_SERVER['HTTP_CONNECTION']; ?> <br>
HTTP_HOST = <?php echo
$_SERVER['HTTP_HOST']; ?> <br>
HTTP_USER_AGENT = <?php echo
$_SERVER['HTTP_USER_AGENT']; ?>
REMOTE_ADDR = <?php echo
$_SERVER['REMOTE_ADDR']; ?> <br>
REMOTE_PORT = <?php echo
$_SERVER['REMOTE_PORT']; ?> <br>
SCRIPT_FILENAME = <?php echo
$_SERVER['SCRIPT_FILENAME']; ?> <br>
SERVER_ADMIN = <?php echo
$_SERVER['SERVER_ADMIN']; ?> <br>
SERVER_PORT = <?php echo
$_SERVER['SERVER_PORT']; ?> <br>
SCRIPT_NAME = <?php echo
$_SERVER['SCRIPT_NAME']; ?> <br>
REQUEST_URI = <?php echo

```

Figure 4: PHP code used for information retrieval

3.3. Device Type Retrieval: Social Network Site

Device type can be retrieved with use of PHP scripting code. The PHP code within following link detects if the site visitor is accessing through a PC, mobile, or other:

<http://www.virtualforensics.net/mobiledetect/detect.php>

Taking it a step further, if the site visitor is using a mobile device the PHP code within following link will detect the mobile's model (ie: Blackberry, I-Phone, etc.):

<http://www.virtualforensics.net/mobiledetect/detectmobile.php>

3.4. User Data Retrieval: IM Chat Session

Retrieval of other person's IP address during an IM chat session (Virtual Meeting) can be accomplished with a program such as NetStat (Network Statistics). NetStat is a tool that displays incoming and outgoing network connections, routing tables, and various other network interface statistics [7].

The following example will demonstrate the use of **NetStat** command for retrieving the IP address and Mac

address of the person you are chatting with using Yahoo Messenger. From the MS-DOS prompt type the following command:

NetStat -n 3

Sample result output:

```

TCP 111.00.000.00:3333 22.2.22.22:7777 Established
TCP 000.00.000.00:4444 66.6.66.666:7777 Established

```

The IP address on the left hand side (111.00.000.00) represents your IP address. The IP address on the right hand side (22.2.22.22) represents the IP address of foreign machine. The 4 digit value following each IP address represents the port to which it is connected to.

You can connect to the foreign IP address by typing the following command. From the MS-DOS prompt type the following command:

C:\>nbtstat -A 66.6.66.666

As stated, the 66.6.66.666 represents the foreign machine's IP address. This entered command will output the values of the Node, IP address, NetBIOS Remote Machine Table, and the MAC address.

Sample output result:

```

Local Area Connection:
Node IPaddress: [000.00.000.00] Scope Id: []
NetBIOS Remote Machine Name Table
Name Type Status
-----
JHU45 <11> UNIQUE Registered
KJL <22> GROUP Registered
BVC <33> UNIQUE Registered
BVCDSAP6 <7Y> GROUP Registered
MAC Address = 88-N2-I4-V5-LB-7X

```

3.5. User Data Retrieval: Email

You can retrieve the IP address of a person who has sent you an email. For example, using a hotmail email account do the following:

```

Go to inbox
Right click on email sender (do not open the email)
Select source code
Result: The sender's IP address will appear.

```

3.6. User Data Retrieval: Website

3.6.1. Data retrieved using JAVA

The following is a list of non-personal-identifiable information which can be retrieved for the website coded using Java. In this list, "request" refers to 'HttpServletRequest' object.

Context Path of the web application.

Method used: request.getContextPath() [3]

LocalAddress returns the local iNet address object to which the specified datagram socket or socket is bound to.
Method used: `request.getLocalAddr()` [14]

LocalName returns the Local Name of the System
Method used: `request.getLocalName()` [14]

LocalPort returns the port number on the local host, to which the specified datagram socket, server socket, or socket object is bound.
Method used: `request.getLocalPort ()` [14]

Locale retrieves user locale from the HTTP Accept-Language Header.
Method used: `request.getLocale()` [3]

Protocol returns the type of protocol.
Method used: `request.getProtocol()` [3]

RemoteAddress returns the client's IP Address.
Method used: `request.getRemoteAddr()` [3]

RemoteHost indicates the fully qualified domain name (e.g., `white_house.gov`) of the client that made the request. The IP address is returned if the domain name cannot be determined.
Method used: `request.getRemoteHost()` [3]

RequestedSessionID
Defaults to null, when the first request submitted to the client has not yet requested a session. When you call `getSession(true)`, a session id is generated and returned to the client.
Method used: `request.getRequestedSessionId()`[5]

RequestURI value returned is a URL denoting path from the protocol name up to query string.
Method used: `request.getRequestURI()`[5]

RequestURL returns the browser's URL.
Method used: `request.getRequestURL()`[5]

ServerName returns name of the server.
Method used: `request.getServerName()` [3]

ServerPort returns port number of the server.
Method used: `request.getServerPort()` [3]

ServletPath returns servlet path.
Method used: `request.getServletPath()` [3]

Referer contains the URL of the page from which the user came
Method used: `request.getHeader("referer")` [14]

ContentType is an entity-header field that indicates the media type of the entity-body sent to the recipient. In the case of the HEAD method, it is the media type that would have been sent had the request been a GET.
Method used: `request.getHeader("content-type")` [15]

Accept_language is a request-header field which is similar to Accept, but restricts the set of natural languages that are preferred as a response to the request. Each language-range may be given an associated quality value which represents an estimate of the user's preference for the languages specified by that range.
Method used: `request.getHeader("accept-language")` [15]

Accept_Encoding is a request-header field which is similar to Accept, but restricts the content-coding that are acceptable in the response.
Method used: `request.getHeader("accept-encoding")` [15]

Connection is a general-header field which allows the sender to specify options that are desired for that particular connection and must not be communicated by proxies over further connections.
Method used: `request.getHeader("connection")` [14]

UserAgent specifies the software program used by the original client. This is used for statistical purposes and the tracing of protocol violations. It should be included. The first white space delimited word must be the software product name, with an optional slash and version designator[5].

Host is a request-header field that specifies the Internet host and port number of the resource being requested, as obtained from the original URI given by the user or referring resource (generally an HTTP URL, as described in section). The Host field value must represent the naming authority of the origin server or gateway given by the original URL. This allows the origin server or gateway to differentiate between internally-ambiguous URLs, such as the root "/" URL of a server for multiple host names on a single IP address [15].

Cache_Control is a general-header field which is used to specify directives that must be obeyed by all caching mechanisms along the request/response chain. The directives specify behavior intended to prevent caches from adversely interfering with the request or response.
Method used: `request.getHeader("cache-control")`[5].

Cookie retrieves cookie value from the client request by name, specified in the cookie-Name argument. The user may specify a default return value in the cookie Default argument for the case where the specified cookie is not found.
Method used: `request.getHeader("cookie")` [3].

Accept is a header that specifies the MIME types that the browser or other clients can handle. A servlet that can return a resource in more than one format, therefore it can examine the Accept header to decide which format to use.
Method used: request.getHeader("accept") [15].

Scheme

Method used: request.getScheme() [14]

Our application automatically stores the retrieved user data to a database. Figure 1 lists the user data retrieved. The following is a link to our test data-user-retrieval site: <http://76.124.82.116:8080/ClientUI/>

Login: user
Password: user

Context Path :	/ClientUI
Local Address :	192.168.1.2
Local Name :	jay
Local Port :	8080
Locale :	en_US
Protocol :	HTTP/1.1
Remote Address :	207.59.110.42
Remote Host :	207.59.110.42
Remote Port :	29096
Remote User :	null
Requested SessionID :	6C31FB1772B9D7881BA39CA9DB00587A
Request URI :	/ClientUI/servlet/Application
Request URL :	http://76.124.82.116:8080/ClientUI/servlet/Application
Scheme :	http
Server Name :	76.124.82.116
Server Port :	8080
Servlet Path :	/servlet/Application
User Principal :	null
Referer :	http://76.124.82.116:8080/ClientUI/
Content Type :	application/x-www-form-urlencoded
Accept Language :	en-us
Accept Encoding :	gzip, deflate
User Agent :	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .N
Host :	76.124.82.116:8080
Connection :	sun.jdbc.odbc.JdbcOdbcConnection@651e95
Cache Control :	no-cache
Cookie :	JSESSIONID=6C31FB1772B9D7881BA39CA9DB005
Accept Value :	image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, appli application/vnd.ms-powerpoint, application/msword, */*

Figure 1: User's information retrieved via Java

3.6.2. MAC address retrieval using Java applets

In computer networking, a Media Access Control address (MAC address) or Ethernet Hardware Address (EHA),

hardware address, adapter address or physical address is a quasi-unique identifier assigned to most Network Adapters or network interface cards (NIC) by the manufacturer for identification. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number.

Figure 2, displays the user's MAC address retrieved.

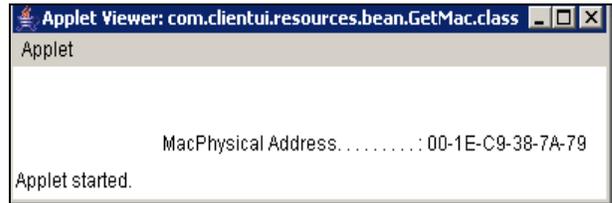


Figure 2: MAC address retrieved via Java applets

The source code with Java applet used to access above user information is as follows:

```
import java.applet.Applet;
import java.awt.Color;
import java.awt.Event;
import java.awt.Graphics;
import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStream;
import java.net.InetAddress;
import java.text.ParseException;
import java.util.StringTokenizer;
public class GetMac extends Applet {
String PhysicalAdd;
public void init() {
setLayout(null);
setBackground(Color.red);
setForeground(Color.yellow);
try {
String macAdd = windowsRunIpConfigCommand();
int len = macAdd.length();
int AddressDet = macAdd.indexOf("Ethernet adapter Local Area Connection:");
String add = macAdd.substring(AddressDet,len);
int loc = add.indexOf(':');
int tLen = add.length();
String MacAddress =
add.substring(loc+1,tLen);
int PhysicalAddLoc = add.indexOf("Physical Address. . . :");
PhysicalAdd=add.substring(PhysicalAddLoc,(PhysicalAddLoc
+ 55));}
catch(Exception e){ }
public void paint(Graphics g)
{g.drawString("Mac" + PhysicalAdd , 100, 100) }
private final static String
windowsRunIpConfigCommand() throws IOException
{Process p = Runtime.getRuntime().exec("ipconfig /all");
InputStream stdoutStream =
new BufferedReader(p.getInputStream());
StringBuffer buffer= new
StringBuffer();
for (;) {int c = stdoutStream.read();
if (c == -1) break; buffer.append((char)c);}
```

```
String outputText = buffer.toString(); stdoutStream.close();
    return outputText;}
private final String windowsParseMacAddress(String
ipConfigResponse) throws ParseException
{
    String localhost = null;
try{localhost = InetAddress.getLocalHost().getHostAddress();}
catch(java.net.UnknownHostException ex)
{ ex.printStackTrace();
    throw new ParseException(ex.getMessage(), 0);}
StringTokenizer tokenizer =
new StringTokenizer(ipConfigResponse, "\n");
String lastMacAddress = null;
while(tokenizer.hasMoreTokens())
{ String line = tokenizer.nextToken().trim();
// Following checks if line contains IP address
if(line.endsWith(localhost) && lastMacAddress != null)
{return lastMacAddress;}    return lastMacAddress;} }
```

4. Computer Data Logs

4.1. Software's to Monitor the Computer

Spytech NetVizor is an award winning, powerful computer spy software that allows you to monitor EVERYTHING users do on your computer - in total stealth. Spy Agent provides essential computer monitoring features, as well as website and application content filtering, chat client blocking, lockdown scheduling, and remote delivery of logs via email or FTP. Spy Agent's advanced, yet easy to use feature-set is unmatched, and provides the ultimate all-in-one computer monitoring software package. Logs Keystrokes Typed Logs Website Visits and Searches Logs Applications Opened and Closed Logs Internet Connections Made Logs Files Opened and Printed Logs Chat Conversations Logs Windows Opened Logs Email Sent and Received Logs Internet Traffic Data Sends Activity Logs via Email or FTP Records Screenshots Built-In Web and App Content Filtering Easy Log Management and Viewing Powerful Graphical Interface Extensive Report Generators Activity Triggered Smart Logging Disables Spyware Detectors [8].

NetworkGazer is a valuable tool that allows you to monitor and maintain your network by giving you a real-time glimpse of your network current configuration. Lookup network shares on a computer and find out who has access to that network share. Not only find out who has access you can determine what level of access. Easily access to remote machine event logs or retrieve Internet history (cookies, Internet temporary files, webpage history). Scan the network to retrieve computer ids, IP to MAC address relationship cross-referenced to the login user. Retrieve disk drives, processor(s), network adapter(s) and operating system data on network-connected computers [8].

Universal IM History Decoder decodes message history files of most popular Instant Messengers. It supports: MSN Messenger Yahoo! Messenger ICQ Messenger Miranda Messenger [separate items by commas]. Using this program, you can decode and view not only yours, but also other's conversations, while offline, without password. For ICQ and Miranda it also recovers stored passwords. All decoded messages could be saved to txt file. Also includes auto-detection of all installed user profiles and date filter selection [8].

IM-History is the first service on the globe for saving your chat history online. People use it all over the world for managing history of almost any instant messenger. The service offers you powerful online storage, comfortable and easy surfing over your messages and contacts. Now your history is accessible to you from any location, merged automatically from all your messengers, and in a safer and more reliable storage than your HDD IM-History Client Suite is easy to install and simple to manage. Your messages are stored on secure dedicated servers and nobody except you can access them [8].

4.2. Digital Forensic Tools

Guidance Software EnCase Forensics is one of the industry's most popular tools to conduct computer forensic investigations. With an intuitive GUI, superior analytics, enhanced email/Internet support and a powerful scripting engine, EnCase provides investigators with a single tool, capable of conducting large-scale and complex investigations from beginning to end. Law enforcement officers, government/corporate investigators and consultants around the world benefit from the many features EnCase Forensic provides [8].

AccessData Ultimate Toolkit (UTK)

The Ultimate Toolkit contains everything needed to investigate, secure and analyze computer or digital data. The UTK includes the Forensic Toolkit, Registry Viewer, Password Recovery Toolkit, Distributed Network Attack (1-Server / 50 Client Licenses), FTK Asia, NTAccess, WipeDrive 20-Pak, FTK Imager and includes technical phone support with free software subscription service for twelve months [8].

Maresware provides an essential set of tools for investigating computer records and securing private information. It is highly flexible to meet the needs of all types of investigators including: law enforcement, intelligence agency, private investigator, corporate security officers, and human resources personnel. Used within a forensic paradigm, the software enables discovery of evidence for use in criminal or civil legal proceedings. Internal investigators can develop documentation to support disciplinary actions, yet do so

non-invasively, to preserve evidence that could end up in court [8].

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 [8].

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) [8].

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 [8].

4.3. Data Recovery/Investigation Tools

Rifiuti is a Recycle Bin Forensic Analysis Tool. Rifiuti, the Italian word meaning "trash", was developed to examine the contents of the INFO2 file in the Recycle Bin. Rifiuti will parse the information in an INFO2 file

and output the results in a field delimited manner so that it may be imported into your favorite spreadsheet program. Rifiuti is built to work on multiple platforms and will execute on Windows, Mac OS X, Linux, and *BSD platforms [8].

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 [8].

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 [8]:

- 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 quickly and easily determines whether malware is present on a system under investigation. The Forensic Pro Edition is designed for forensic investigators, examiners, law enforcement personnel, private investigators, and forensic lab use. The Forensic Pro version includes all the malware datasets, travelling license, dataset creator, dataset converter, a single-user license of Mount Image Pro™ allowing forensic image investigations and other tools including a USB thumb drive for covert investigations and a 1-year subscription to the Digital Evidence Time Stamping service [8].

DiskCat catalogues all files on disks. It is short for "disk cataloguer". It creates a listing (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 purposes and for file maintenance. Output is a fixed length record and database compatible (for further analysis/sorting) [8].

Active Partition Recovery is a very 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 [10]

4.4. PDA Investigation Tools

Pilot-Link is used to retrieve information from ROM and RAM of Palm PDA hand-held. **Pilot-xfer** can additionally be used to allow acquisition [8].

Paraben PDA Seizure is the only forensic tool designed to capture data and report on data from a PDA. As an examiner you know better than anyone that the difference between making a case and losing a case is hard evidence. And with more bad guys going high tech, obtaining that evidence is becoming more difficult than ever. Paraben's PDA Seizure is a comprehensive tool that allows PDA data to be acquired, viewed, and reported on, all within a Windows environment. Now with USB support [9].

4.5. 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 [9].

5. Conclusion

Security has become a major concern on Social Networks. It is very important that we find the right solutions (through stricter regulations, user education, and so on) to tackle the different security problems on the Social Network Site's today. 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, but can also be used to help protect users from the start of their Social Network Site interactions, to prevent 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.

6. 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 or Opera or Safari which are safer to use. In summary, Social Network Site security has space for more research and further development.

7. 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

8. References

- [1] Helen, Drislane and Heffner, Kelly, <http://www.eecs.harvard.edu/cs199r/fp/HelenKelly.pdf>, accessed December 2008
- [2] <http://connectsystems.co.uk/>, accessed December 2008
- [3] <http://docs.djangoproject.com/en/dev/ref/request-response/?from=olddocs>, accessed December 2008
- [4] <http://eventful.com/faq>, accessed December 2008
- [5] <http://www.forensics.nl/tools>, accessed December 2008
- [6] <http://publishing2.com/2007/10/31/facebook-vulnerabilities/>, accessed December 2008
- [7] <http://thehackers.freeservers.com>, accessed December 2008
- [8] <http://www.forensic-computing.ltd.uk/tools.htm>, accessed December 2008
- [9] <http://java.sun.com/products/servlet/2.1/api/javax.servlet.http.HttpServletRequest.html>, accessed December 2008
- [10] <http://www.forinsect.de/forensics/forensics-tools.html>, accessed December 2008
- [11] http://www.freeloadscenter.com/Utilities/Backup_and_Copy_Utilities/Yahoo_Messenger_Chat_Recovery.html, accessed December 2008
- [12] <http://www.nytimes.com/2008/11/27/us/27myspace.html?ref=todayspaper>, accessed December 2008
- [13] <http://www.opentracker.net/forum/tracking-a-myspace-homepage-t536.html>, accessed December 2008
- [14] <http://www.w3.org/Protocols/HTTP/HTRQ-Headers.html>, accessed December 2008
- [15] <http://www.w3.org/Protocols/rfc2616/rfc2616-sec5.html>, accessed December 2008
- [16] <http://www.whovisited.com>, accessed December 2008
- [17] <http://www.geobytes.com/IpLocator.htm>, accessed December 2008
- [18] <http://www.whatismyipaddress.com>, accessed December 2008