Using Forensic Techniques for Internet Activity Reconstruction

ZSOLT NAGY
Institute of Mathematics and Computer Science
College of Nyiregyhaza
Nyiregyhaza, Sostoi u. 31/B
HUNGARY
info@nagyzsolt.hu

Abstract: – In this article we are searching for digital footprints of our everyday internet activity that have been left by web browsers and instant messengers. We are going to show the way in which a forensic expert can use these artefacts, and we focus on the risk of cyber crime against a single user who is not sufficiently careful to protect his or her information. We undertook this research using a real criminal investigation example, we present the kind of tools and techniques that should be used, where they should be used and by combining an expert with an individual user we find out the kind of information that has been collected and stored about a user by a client computer.

Keywords: – internet security, forensic analysis, cyber crime, web history, messenger log

1 Introduction

This article is based on a real criminal investigation. On 25th August 2011, investigators seized the computer of John Spencer who was suspected of hacking his ex-girlfriend's, Jennifer Smith's, mailbox messenger program and social media site. He had changed Jennifer's user profile, talked to others in her name and lived her social life. Investigators ordered the author to undertake a forensic investigation of the seized computer. For privacy reasons, in our article we have changed the real names and have hidden some of the characters in the usernames and passwords. At the beginning of the forensic work we were given Jennifer's email addresses and passwords, as well as the login accounts of the social media sites and messenger applications. We used these during the inspection.

Based on this case, we carefully examined the evidence to ascertain the kind of web pages visited, by whom and when the usernames and passwords were used on the seized computer.

At this point, we have to mention that it is not the job of a forensic expert to prove the guilt of the suspect, the expert only gives answers and provides proof, which can later be strong evidence in reaching a verdict. However, for scientific purposes, in the following sections we will say that "John has done something" instead of "the owner of the computer" or "someone has done something".

As the operating system (OS) of the seized computer was Windows 7, all the examples and methods are for this OS.

2 The Objectives of the Inspection

During the inspection we had to find answers for the following important questions:

a) Is there any proof that indicates that someone has logged onto Jennifer's social media sites, mailbox, used Skype or Windows Live Messenger with Jennifer's accounts from this computer?
b) What kind of conclusions could be drawn from the evidence?

To answer the abovementioned questions and make it easier to understand the techniques and tools used during the forensic inspection, we have to clarify some essential concepts.

2.1 Internet Activity Data Stored by Web Browsers

Nowadays we can choose from several web browsers (Internet Explorer, Mozilla Firefox, Google Chrome, Safari, Opera), all of which differ slightly in their services, outlook or even speed. From a forensic aspect, they all have at least one similar property.

Their common technological characteristic is that before displaying a webpage, they download the content of it (text, image, multimedia elements)

from the web server, and then open it and show it on the local computer.

In order to display the same website more quickly on future occasions, web browsers keep the downloaded web site data, so that it remains available on the computer even if the user closes the browser or shuts down the machine [1]. This is a useful feature. These downloaded web files are called caches, cached, history or temporary internet files. Depending on the OS and browser applications they are stored in different locations.

2.1.1 Cache Files

From Windows Vista, Microsoft Internet Explorer stores the temporary internet files in the following folder [2]:

```
C:\Users\<windowsUsername>\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\
```

Fig. 1: Internet Explorer cache folder

while the URLs [3] of the visited web pages (commonly known as browsing history) are stored in the folder shown in Figure 2.

```
C:\Users\<windowsUsername>\Local\Microsoft\Windows\History\History.IE5\
```

Fig. 2: Internet Explorer browsing history folder

There is also an `index.dat` file which can be very useful in case the user has deleted the browsing history. By parsing the `index.dat` file, a list of the visited web pages could even be recovered [4].

From version 3 and above, Mozilla Firefox stores its browsing history in SQLite [5] format database tables. These tables are stored in the following folder:

```
C:\Users\<windowsUsername>\AppData\Roaming\Mozilla\Firefox\Profiles\<profile folder>
```

Fig. 3: Mozilla Firefox browsing history folder

Firefox automatically creates the profile folder at the start. This folder is the storage place for the browsing history (`places.sqlite`), the list of downloaded files (`download.sqlite`) and the passwords stored by Firefox (`key3.db` and `signons.sqlite`) [6]. As these are not plain text but SQLite files, these can be viewed by a free SQLite Database Browser [7].

Under the profile folder there can also be found a `Cache` folder, where the cache files of the Firefox browser are stored.

On the computer under investigation an Opera browser was also installed, storing the relevant data shown in the folder in Figure 4. There are two important files in this directory, `global_history.dat` and `typed_history.xml`: `global_history.dat` is a plain text file which stores details for each URL visited; `typed_history.xml` is an XML file that has an entry for each URL entered manually [8].

```
C:\Users\<windowsUsername>\AppData\Roaming\Opera\Opera\
```

Fig. 4: Opera browsing history folder

However, during the forensic examination, the installed Google Chrome and Safari browsers were not found; to complete the list we show where these browsers store their browsing history. Google Chrome similar to Firefox stores information in SQLite databases in the following folder:

```
C:\Users\<windowsUsername>\AppData\Local\Google\Chrome\User Data\Default
```

Fig. 5: Google Chrome browsing history folder

We can find here the browsing history, the list of downloaded files and the given usernames and passwords via web pages. These files do not have `.sqlite` extensions, but examining the header part of these files, the „`SQLite Format 3`” string pattern makes them easily identified.

Apple's Safari browser is a part of the Mac OS X system, but can also be found in the Windows environment. The browsing history is stored in the folder in Apple property list file format (Fig.6), abbreviated to plist, (`History.plist`).

```
C:\Users\<windowsUsername>\AppData\Roaming\Apple Computer\Safari
```

Fig. 6: Safari browsing history folder

In the same place we can find other important files for the investigation procedure, such as `FormValues.plist`, `LasSession.plist` and `Bookmarks.plist`.

To search for cache files, search for the SQLite format `Cache.db` file (from Safari version 3) in the following folder [9]:

```
C:\Users\<windowsUsername>\AppData\Local\Apple Computer\Safari
```

Fig. 7: Safari cache folder

ISBN: 978-1-61804-109-8

2.1.2 Stored Passwords

Other capabilities of the browsers include the facility to store website usernames and passwords given by users during login procedures. These sites are mostly mail systems, social media sites, forums or company web portals.

It was mentioned previously that Firefox stores passwords in the `signons.sqlite` file; Internet Explorer stores account information in the Registry, Credentials File, or Protected Storage places; Google Chrome uses the `web data` folder under `Default` folder; while Opera uses the `wand.dat` file [10].

However, this browser facility can be very useful in the event that web page account details are forgotten; it can also be very dangerous as it takes only one or two minutes for a criminal to extract all the stored passwords. In the following sections we describe how to do this.

2.2 Stored Data of Instant Messenger Applications

There are several instant messenger (IM) applications; we highlight only the two most popular, Windows Live Messenger and Skype.

2.2.1 Stored Skype Data

After a simple registration, Skype provides the opportunity to initiate text, voice (VoIP) or video calls with other persons. Knowing the Skype account details, anyone can log into any Skype application on any computer [11]. Skype stores information related to users in separate folders, the name of the folder is equal to the Skype nickname of the user (Fig. 8).

```
C:\Users\<windowsUsername>\AppData\Roaming\
Skype\<skypeNickname>
```

Fig. 8: Skype user profile folder

If the computer contains more folders with different Skpye nicknames than those of the computer owner, this can provide useful information in the investigation, as it indicates that someone else has also logged into Skype from this computer. Additionally, there is another feature of Skype; it stores all the conversation history, in the folder indicated in Figure 8. There are `.dbb` or `.db` SQLite tables, depending on the Skype version [12].

2.2.2 Windows Live Messenger Stored Information

The other popular IM is Microsoft Windows Live Messenger (WLM), also known as MSN Messenger in earlier versions [13], which stores the user information in the following folder.

```
C:\Users\<windowsUsername>\AppData\Local\Mi
crosoft\Messenger\<msnEmailAddress>
```

Fig. 9: Windows Live Messenger user folder

Similar to Skype, WLM creates a new folder for every new user who logs into the messenger on the given computer. It is important to mention that, in certain cases, WLM also creates a folder for the chat partner, especially if he or she uses special backgrounds or emoticons. The expert should keep this in mind during forensic analysis.

In the `Messenger` folder, there is another file, called `ContactsLog.txt`. This file contains the complete communication events log [14], however it does not contain the communication content (conversation) itself. When a WLM user logged in and logged out of Windows Live Messenger can be ascertained by parsing this file.

Reconstruction of the internet activity from the previously mentioned information should take a very long time and could be very cumbersome. Fortunately, there are several free and commercial tools that can help in retrieving data and restoring web activity processes.

3 Artefact Discovery

As mentioned in the previous section, there are two main branches of our forensic investigation. First we extract the stored data from the web browsers (visited web pages, stored passwords) then we search for Skype and WLM artefacts related to the suspicion.

3.1 Visited Web Pages

There are several good applications for the reconstruction of web browser activities. To restore Internet Explorer (IE) web activities we can use Pasco [15], IECacheView [16] and Web Historian [17] or the commercial Internet Evidence Finder (IEF) [18]. The last two products are also capable of restoring activity from other kinds of web browsers. To reconstruct Firefox and Opera data, we have used MozillaCacheView [19] and OperaCacheView [20] applications.

For stored passwords there are also good and free tools, such as IEPassView [21], MozillaPassView [22], OperaPassView [23], and the WebBrowserPassView [24] tool which brackets many browser password extraction software applications into one program.

In the following sections we present the results of using and combining the previously mentioned forensic tools, clearly showing the conclusions derived from the evidence found.

3.1.1 First Evidence

By examining the cache files of Internet Explorer, forensic analysis found an interesting URL.

```
http://www.freemail.hu/mail/main.fm?checkuser=1&status=ok&auth=ok&tid=jYl7Y6AFUGlz4D92LOFQ&email=s*****ta@freemail.hu_1190488290
```

Fig. 10: Extracted data by IECacheView

To explain Figure 10, the given user (`email=s*****ta@freemail.hu`) successfully (`auth=ok`) logged onto the Freemail mailing system, then the system displayed to him or to her the main mailbox page (`main.fm`).

This URL proves that someone with the `s*****ta@freemail.hu` email address successfully logged into the Freemail.hu mailing system. For successful login, the username and the mail password must be known. Is it possible that this person who logged in was Jennifer?

No. IECacheView can extract the creation date of this record. The date is 26/07/2011 0:20:04; at this time Jennifer was at home with her family.

3.1.2 Second Evidence

So, it would appear that John knows Jennifer's Freemail password. We therefore need to ascertain whether or not this username and password pair is stored on the computer. Using the IE, Mozilla and Opera password viewer tools, we found more than we expected. However, we did not find the stored instance of the Freemail account, but something interesting. Examining the stored passwords of Firefox showed that someone had tried to login to the `https://www.msgplus.net` website with the `s*****ta@freemail.hu / b***1` account. Msgplus.net is the website of the Messenger Plus! application which is a popular extension for MSN Messenger [25]. We know that Jennifer's msgplus.net account is the same as her WLM account. So, if John knows Jennifer's WLM username and password, it is necessary to analyse whether or not the Windows Live Messenger activity was undertaken using Jennifer's accounts.

3.1.3 Third Evidence

Browsing the stored passwords of Opera browser, we found two relevant records related to the `https://www.facebook.com` website. It shows that someone tried to log into the `www.facebook.com` website with `s*****ta@freemail.hu / g***a`, then with the `s*****ta@freemail.hu / a***1` username/password pairs.

Based on the existing information, the first is Jennifer's original Facebook account; the second differs only in the password field. It may be indirect proof that John has changed Jennifer's
Facebook password, but one fact is clear: knowing Jennifer's details, John has logged into her Facebook account.

3.1.4 Fourth Evidence

If John knows Jennifer's Facebook account, discovery of the internet activities of the other Hungarian popular social media site, iWiW, is recommended. In the browser's password files we did not find any stored records related to this website, but we should again walk through the browser history. At this point, Mozilla Firefox History gave the results of our examination. The filtered log analysis contains the web activity of the www.iwiw.hu website for the period 06/08/2011 11:34:05 – 22/08/2011 21:29:20.

One of the records created on 21/08/2011 at 21:36:59 gives clear evidence for the fact, that someone has logged in and modified Jennifer Smith's iWiW profile page. How can we identify it?

MozillaCacheView can extract not only the visited URLs but the Last Visit Date of the URL and also the Referrer of the page. The Referrer field shows the previous web page that redirected the user to this current page [26].

From the point of view of the investigation, the following record is very interesting as it has been found as a referrer page:

```
http://iwiw.hu/pages/user/profilepersonal.jsp?method=SaveCore
```

Fig. 11: URL that saves a user's iWiW profile

This page is only accessible for logged in users, it saves the users' changed personal profile data. It is not evidence in itself, as it could be related to John's iWiW profile page. But, in continuing the investigation, it came to light that this is the referrer of the following page:

```
http://iwiw.hu/i/Jennifer-Smith-11260492/adatlap?userID=11260492#personal
```

Fig. 12: Jennifer's iWiW user profile page

The Last Visit Date of both pages is exactly the same 21/08/2011.21:36:59. Is it possible that John has modified his profile page and in the same second he opened his ex-girlfriend's personal iWiW

ISBN: 978-1-61804-109-8

page (Fig. 12)? Such a chance is very small. During the forensic investigation it was identified that, after saving the modification of personal data, the page (Fig. 11) immediately and automatically opens the logged in user's personal iWiW page (Fig. 12). Because of the nature of the mentioned technology, this could only happen if the Figure 11 page was opened by the logged in Jennifer Smith. Was Jennifer in John's house at this time? No, she was on holiday.

3.2 Skype Forensic Artefacts

If the previous evidence is not enough to prove that John has used Jennifer's accounts, here are additional artefacts provided by Skype.

As mentioned in the Section 2.2.1, it is useful to examine the Skype user profile folder. On opening the Skype folder we found two important records:

```
C:\Users\John\AppData\Roaming\Skype\sz*****001
```

Fig. 13: Jennifers's Skype profile folder

```
C:\Users\John\AppData\Roaming\Skype\d***001
```

Fig. 14: John's Skype profile folder

The name of the first folder is equal to Jennifer's Skype name, so someone has logged into Skype from this computer with Jennifer's account. Examining the creation date of this folder gives us the date the user `sz*****001` first logged in with this account. Further bad news for the suspect is that the creation date of the folder is 29/06/2011 21:21:55. At this time John and Jennifer were not together, Jennifer was not in John's house that evening.

We suspected from the name of the second folder, that `d***001` could be John's Skype name; in a later stage of the forensic analysis this suspicion was verified as we examined the stored Skype conversation. Skype logs all conversations for a given period, and can be retrieved by anyone using SkypeLogView [12], a free forensic tool.

3.3 Windows Live Messenger

As John has details of Jennifer's Windows Live Messenger account, we had to ascertain whether or not there was any evidence proving that John had used WLM with his ex-girlfriend's username and password. After examining the specific `Messenger` folder we found two usernames (Fig. 15, Fig. 16):

```
C:\Users\John\AppData\Local\Microsoft\Messenger\n***001@citromail.hu
```

Fig. 15: John's WLM profile folder

```
C:\Users\John\AppData\Local\Microsoft\Messenger\s*****ta@freemail.hu
```

Fig. 16: Jennifer's WLM profile folder

However, although we had discovered Jennifer's account, we could not be sure that the existence of the `s*****ta@freemail.hu` folder meant that someone had logged into WLM with Jennifer's account. The folder could have been created by WLM to store data about Jennifer as John's chat partner. For this reason we undertook further examination; in this case the ContactsLog.txt file gave us useful information.

In the following figure, the WLM login process can be observed, these lines were extracted from the ContactsLog.txt of the seized computer (Fig.17).

```
[21:11:05.51] 09a0             Contacts:
UserState
CUserState::RegisterApplication@003F99E8:
(User='s*****ta@freemail.hu',
Application='msnmsgr.exe', Types='7') ==
'003FAAA8', auth='7', sync='0'
[21:11:05.51] 09a0             Contacts:
UserState
CUserState::RegisterApplication@003F99E8:
(User='s*****ta@freemail.hu',
Target='Initial',
Application='msnmsgr.exe') AuthNeeded ==
<0x       0>
[21:11:05.51] 09a0             Contacts:
UserState
CUserState::IncrementClientsThatSupportNoti
fications@003F99E8:
(User='s*****ta@freemail.hu') -- enabling
policy
```

Fig. 17: WLM connection process

```
 [21:18:21.73] 05ec             Contacts:
UserState
CUserState::UnregisterApplication@003F99E8:
(User='s*****ta@freemail.hu',
Application='msnmsgr.exe') == '003FAAA8'
[21:18:21.73] 05ec             Contacts:
UserState
CUserState::DecrementClientsThatSupportNoti
fications@003F99E8:
(User='s*****ta@freemail.hu') -- disabling
policy
```

Fig. 18: WLM disconnection process

From log records created on 20/06/2011, these figures show that the `s*****ta@freemail.hu` user logged into the WLM at 21:11:05, and then logged out at 21:18:21. This user used the Messenger for more than 7 minutes on the specific day. Besides two important commands `RegisterApplication` and `UnregisterApplication`, several other processes were activated during the logging in and out period. In the interval that we analysed, there

ISBN: 978-1-61804-109-8

were more than 70 login processes with Jennifer's Messenger account. If a user gives the wrong password during the messenger login process, the `RegisterApplication` process starts, but after a few seconds authentication fails and WLM calls the `UnregisterApplication` process.

4 Conclusions

As a result of this investigation the suspect confessed to all the charges. As we have shown in this article, several forensic tools exist to discover and reconstruct the internet history of a given computer or a given user; such discovery and reconstruction can even be done manually. How these tools should be combined and which tools should be used depends on the forensic expert and the case in question. In our case, it took a year of research to find the proper software and methods for web history usage mining. Although such software provides a great deal of help to a forensic expert, it also provides opportunities for cyber criminals to collect personal information about our everyday web usage. It is worthwhile to regularly cleanse cached internet files, web history, logged IM conversations and locally stored passwords. Both criminals and forensic experts have additional tools to seek and recover confidential user information, but, if it is possible, we should make their work harder.

References:

[1] Geoff Huston, Web Caching, *The Internet Protocol Journal*, Vol. 2, No. 3, 1999, pp. 2–20.

[2] Ovie L. Carroll, Stephen K. Brannon, Thomas Song: Vista and BitLocker and Forensics! Oh My!, *United States Attorney's Bulletin*, Vol. 56, No. 1, 2008, pp. 9–28.

[3] W3.org, Hypertext Transfer Protocol. http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html

[4] Jones Keith J., Forensic Analysis of Internet Explorer Activity Files. *Foundstone*, http://www.mcafee.com/us/resources/white-papers/foundstone/wp-pasco.pdf , 2003.

[5] SQLite.org, http://www.sqlite.org, May 2012

[6] MozillaZine.org, Mozilla Profile Folder, http://kb.mozillazine.org/Profile_folder_-_Firefox, May 2012

[7] SQLite Database Browser, http://sqlitebrowser.sourceforge.net/, 2012

[8] Opera.com, Files used by Opera, http://www.opera.com/docs/operafiles/ , 2012

[9] Digital Detective, Apple Safari Browser, http://blog.digital-detective.co.uk/2011/02/apple-safari-browser.html, May 2012

[10] NirSoft.net, Password Storage Locations For Popular Windows Applications, http://www.nirsoft.net/articles/saved_password_location.html, May 2012

[11] Skype, What is Skype? from https://support.skype.com/en-us/ , 2012

[12] Nirsoft.net, SkypeLogView, http://www.nirsoft.net/utils/skype_log_view.html, 2012

[13] Wouter S. van Dongen, Forensic artefacts left by Windows Live Messenger 8.0, Digital Investigation, Vol. 4, No. 2, 2007, pp. 73–87

[14] Tayyeb Moin, Basics of Digital Forensics for Popular chat clients, http://levelinfosec.blogspot.com/2011/01/basics-of-digital-forensics-for-popular.html, 2012

[15] Keith J. Jones, Pasco v1.0 – An Internet Explorer Activity Forensic Analysis Tool, http://www.mcafee.com/us/downloads/free-tools/pasco.aspx, May 2012

[16] IECacheView, http://www.nirsoft.net/utils/ie_cache_viewer.html, May 2012

[17] Web Historian – http://www.mandiant.com/resources/download/web-historian, May 2012

[18] Internet Evidence Finder – http://www.jadsoftware.com/internet-evidence-finder/, May 2012

[19] MozillaCacheView – http://www.nirsoft.net/utils/mozilla_cache_viewer.html, May 2012

[20] OperaCacheView – http://www.nirsoft.net/utils/opera_cache_view.html, May 2012

[21] IEPassView – http://www.nirsoft.net/utils/internet_explorer_password.html, May 2012

[22] PasswordFox – http://www.nirsoft.net/utils/web_browser_password.html

[23] OperaPassView – http://www.nirsoft.net/utils/opera_password_recovery.html

[24] WebBrowserPassword – http://www.nirsoft.net/utils/web_browser_password.html

[25] Messenger Plus! The Messenger Extension – http://www.msgplus.net

[26] IETF.org, Uniform Resource Identifier (URI): Generic Syntax http://tools.ietf.org/html/rfc3986