Social media risks from forensic point of view

Zsolt Nagy

***Abstract*—** In the age of Facebook children are better computer or mobile phone users than their parents; we do not know any teenagers who do not have a social media profile, an email or an instant messenger account. It became the part of their everyday life; however they do not care and even do not know much about the other side of the social life. The Internet gives freedom for everyone, but in this big freedom we forget to teach our children and ourselves how to handle and protect sensitive information properly. In this article we focus on the risk of cyber crime against a single user who is not sufficiently careful to protect his or her information, we are going to show the way in which a forensic expert or even a cyber criminal can use internet activity reconstruction tools. We undertook this research using a real criminal investigation example, find out the kind of information that has been collected and stored about a user by a client computer and give some useful advices how to protect ourselves against cyber criminals.

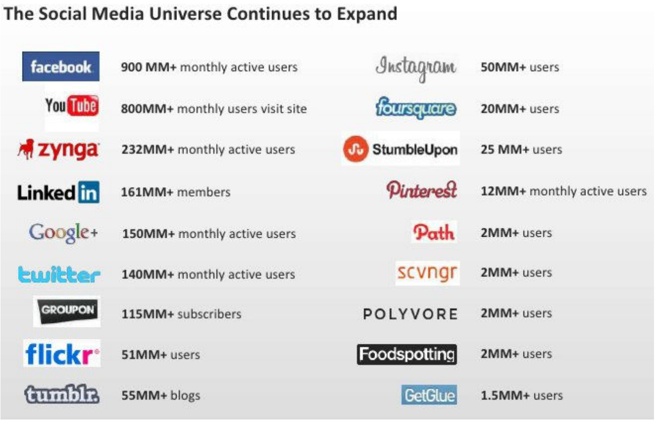
***Keywords*—** Cyber crime, Forensic tools, Internet activity, Social media, Web 2.0

I. Introduction

SINCE we have entered into the age of Web 2.0 we know that the Web is no longer simply an online resource of information, not a collection of websites to be consulted, searched and acted upon. It is rather a collection of web services; it has become a network of social communities and information databases that are constantly growing and improving as they continue to harness the collective intelligence of users. It could therefore be argued that whereas Web 1.0 served essentially as a broadcast medium as an information source Web 2.0 [1] takes the form of a platform whereby the creator of content, has become the active part of the system. The recent development of Web 2.0 has provided for an enormous increase in human interactions across all corners of the earth. The main objective of the development is to harness the resources of the users via web applications like community sites, blogs, RSS, wikis and other kind of social web applications.

One manifestation of this is the growth of computer mediated social networks. Social networking is also one of many consumer technologies, including blogs, wikis, media sharing and virtual community, to cross over into the corporate world. In fact, digital social networks are interactive networks that use internet as a media for making a relation between human [2].

Social media has grown rapidly. Referring to Nielsen's Social Media Report [3], today nearly 4 in 5 active Internet users visit social networks and blogs, Americans spend more time on Facebook than they do on any other U.S. website. The situation is the same in other countries. 62 percent of adults worldwide now use social media, and more than 22 percent of time online spent on social media sites, like Facebook, Twitter or Youtube [4].



The Social Media Universe Continues to Expand

facebook	900 MM+ monthly active users	Instagram	50MM+ users
YouTube	800MM+ monthly users visit site	foursquare	20MM+ users
zynga	232MM+ monthly active users	StumbleUpon	25 MM+ users
LinkedIn	161MM+ members	Pinterest	12MM+ monthly active users
Google+	150MM+ monthly active users	Path	2MM+ users
twitter	140MM+ monthly active users	scvngr	2MM+ users
GROUPON	115MM+ subscribers	POLYVORE	2MM+ users
flickr	51MM+ users	Foodspotting	2MM+ users
tumblr	55MM+ blogs	GetGlue	1.5MM+ users

Fig. 1 Social media users in 2012 [5]

However social media sites are good places for criminals as well. Predators and scam artists often rely on the inexperience and innocence of youth to collect information they can use to exploit others for their own benefit. Everyone could be a victim of his enemy whether the enemy is her neighbor, classmate or ex-boyfriend.

The Council of Europe's Cybercrime Treaty defines a new word for it, *cybercrime* as a range of crime that is committed using computer, network and hardware [6]. The Internet, however, is too valuable resource to try to keep our children and ourselves away from it. As we have learned everything in our life, we have to learn how to live in the digital world how to safely navigate on the information highway.

When engaging with digital information from a legal or ethical standpoint, one of the most effective strategies is case studies. Therefore in this article we present a social media related real criminal investigation.

On 25th August 2011, investigators seized the computer of John Spencer who was suspected of using his ex-girlfriend's, Jennifer Smith's, mailbox messenger program and social media site without Jennifer's permission. He had changed Jennifer's user profile, talked to others in her name and lived

Zsolt Nagy is member of The Chamber of Hungarian Forensic Experts, Debrecen, Hungary (phone: +36 70 315-9450; e-mail: info@ nagyzsolt.hu).

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.

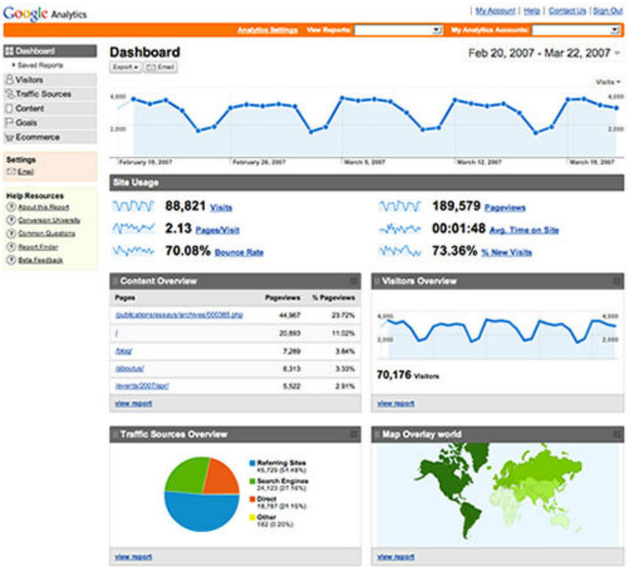
Based on this case, we carefully examined the evidence to ascertain the kind of web pages visited, by whom and when the usernames and passwords were used on the seized computer.

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.

II. Initial Problem

Computers store large amount of user data both on client and server side. Only one click, one second on a web page and the owner of the web portal has gathered at least 10 different facts about a visitor, especially if the website is powered by a web traffic analyzer system like Google Analytics.



Pages	Pageviews	% Pageviews
/publications/essays/archives/000385.php	44,967	23.72%
/	20,893	11.02%
/blog/	7,289	3.84%
/aboutus/	6,313	3.33%
/events/2007/apr/	5,522	2.91%

Fig. 2 Google Analytics sample website data [7]

Google Analytics (GA) is a free, cross-platform web traffic analyser application, which can be easily integrated into any website. GA is very popular amongst marketers as the various types of generated reports about collected user data give valuable information for marketing experts [7].

To tell the truth web service providers do not need any web traffic analyser software to gather user data; even a novice programmer can write a six-line source code which easily acquires user's browser and operating system type, the name of his internet service provider, the screen resolution of his monitor or the type of his mobile device.

We should not have illusions; everyday data collection belongs to our normal Internet life, although web servers are well secured and for web service providers there are strict national and international regulations for storing and managing data.

On client side it is our responsibility to take care of our private data and to protect our computer physically. The biggest problem is that most of the users are not aware of the risks of losing their sensitive information they even do not know what kind of data are stored on their computer.

Jennifer has got a bitter lesson about the importance of securing her usernames and passwords. During the forensic inspection we have examined the ex-boyfriend's seized computer on several ways with several tools and we can declare, if someone knows our social network accounts and we do not recognize it in time, he can easily and quickly ruin our carrier and our life as well.

In the following pages we will use a real criminal investigation as an example to describe and show where can an expert, a criminal or an individual search for sensitive data and we line up the proper tools and methods for restoring it.

III. 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. [8]

A. *Internet Activity Data Stored by Web Browsers*

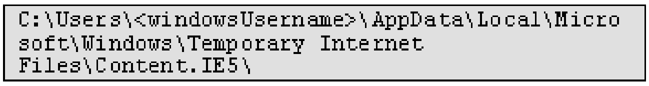
Nowadays we can choose from several web browsers (Internet Explorer, Mozilla Firefox, Google Chrome, Safari, Opera), all of which differ slightly in their services, outlook or even speed. From a forensic aspect, they all have at least one similar property.

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 [9]. 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.

1) *Cache Files*

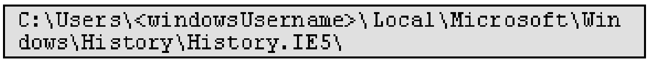
From Windows Vista, Microsoft Internet Explorer stores the temporary internet files in the following folder [10]:



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

Fig. 3 Internet Explorer cache folder

while the URLs [11] of the visited web pages (commonly known as browsing history) are stored in the folder shown in Figure 4.

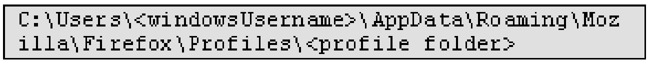


```
C:\Users\<windowsUsername>\Local\Microsoft\Win
dows\History\History.IE5\
```

Fig. 4 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 [12].

From version 3 and above, Mozilla Firefox stores its browsing history in SQLite [13] format database tables. These tables are stored in the following folder:



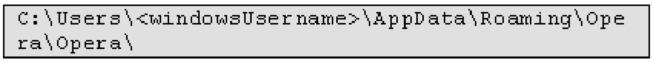
```
C:\Users\<windowsUsername>\AppData\Roaming\Moz
illa\Firefox\Profiles\<profile folder>
```

Fig. 5 Mozilla Firefox browsing history folder

Firefox automatically creates the profile folder at the first 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*) [14]. As these are not plain text but SQLite files, these can be viewed by a free SQLite Database Browser [15].

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

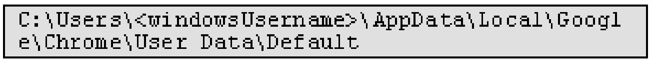
On the computer under investigation an Opera browser was also installed, storing the relevant data shown in the folder in Figure 5. There are two important files in this directory, *global_history.dat* and *typed_history.xml*: *global_history.dat* is a plain text file which stores details for each URL visited; *typed_history.xml* is an XML file that has an entry for each URL entered manually [16].



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

Fig. 6 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:

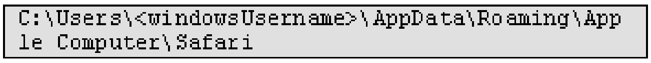


```
C:\Users\<windowsUsername>\AppData\Local\Googl
e\Chrome\User Data\Default
```

Fig. 7 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.8), abbreviated to plist, (*History.plist*).

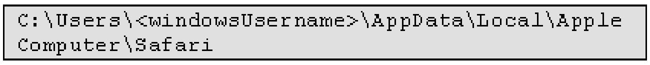


```
C:\Users\<windowsUsername>\AppData\Roaming\App
le Computer\Safari
```

Fig. 8 Safari browsing history folder

In the same place we can find other important files for the investigation procedure, such as *FormValues.plist*, *LastSession.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 [17]:



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

Fig. 9 Safari cache folder

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 [18].

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.

B. Stored Data of Instant Messenger Applications

Our Internet activity is not limited to web pages, proficient web users – as well as Jennifer – also use instant messenger software for communication. There are several instant messenger (IM) applications; we highlight only the two most popular, Windows Live Messenger (WLM) and Skype.

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 [19]. Skype stores information related to users in separate folders, the name of the folder is equal to the Skype nickname of the user (Fig. 10).

```
C:\Users\<windowsUsername>\AppData\Roaming\Sky
pe\<skypeNickname>
```

Fig. 10 Skype user profile folder

If the computer contains more folders with different Skype 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 10. There are .dbb or .db SQLite tables, depending on the Skype version [20].

2) Windows Live Messenger Stored Information

The other popular IM is Microsoft Windows Live Messenger, also known as MSN Messenger in earlier versions [21], which stores the user information in the following folder.

```
C:\Users\<windowsUsername>\AppData\Local\Micro
soft\Messenger\<msnEmailAddress>
```

Fig. 11 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 [22], 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.

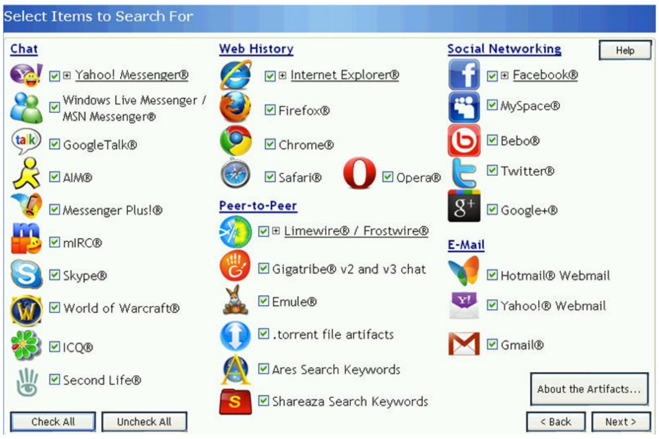
Reconstruction of the internet activity from the previously mentioned information should take a very long time and could be very cumbersome. Fortunately, there are several free and commercial tools that can help in retrieving data and restoring web activity processes.

IV. 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.

A. 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* [23], *IECacheView* [24] and *Web Historian* [25] or the commercial *Internet Evidence Finder* (IEF) [26]. 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* [27] and *OperaCacheView* [28] applications.



Select Items to Search For

Chat
☑ ⊞ Yahoo! Messenger®
☑ Windows Live Messenger / MSN Messenger®
☑ GoogleTalk®
☑ AIM®
☑ Messenger Plus!®
☑ mIRC®
☑ Skype®
☑ World of Warcraft®
☑ ICQ®
☑ Second Life®

Web History
☑ ⊞ Internet Explorer®
☑ Firefox®
☑ Chrome®
☑ Safari®
☑ Opera®

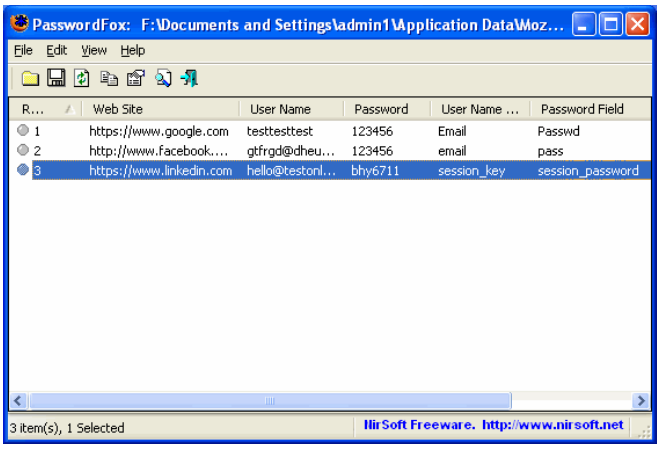
Peer-to-Peer
☑ ⊞ Limewire® / Frostwire®
☑ Gigatribe® v2 and v3 chat
☑ Emule®
☑ .torrent file artifacts
☑ Ares Search Keywords
☑ Shareaza Search Keywords

Social Networking
☑ ⊞ Facebook®
☑ MySpace®
☑ Bebo®
☑ Twitter®
☑ Google+®

E-Mail
☑ Hotmail® Webmail
☑ Yahoo!® Webmail
☑ Gmail®

Fig. 12 Internet Evidence Finder

For stored passwords there are also good and free tools, such as *IEPassView* [29], *PasswordFox* [30], *OperaPassView* [31], and the *WebBrowserPassView* [32] tool which brackets many browser password extraction software applications into one program.



PasswordFox: F:\Documents and Settings\admin1\Application Data\Moz...

R...	Web Site	User Name	Password	User Name ...	Password Field
1	https://www.google.com	testtesttest	123456	Email	Passwd
2	http://www.facebook....	gtfrgd@dheu...	123456	email	pass
3	https://www.linkedin.com	hello@testonl...	bhy6711	session_key	session_password

3 item(s), 1 Selected

NirSoft Freeware. http://www.nirsoft.net

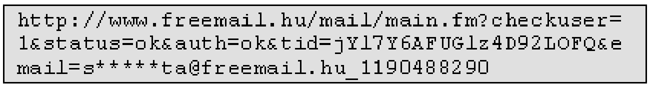
Fig. 13 PasswordFox – Free tool for Mozzilla password recovery

The greatest advantage of these free applications that they do not require any installation procedure; these can be run from a single pendrive. If we think about it a bit it can be a very dangerous weapon at the same time. It is enough to leave alone our computer only for five minutes and a cyber criminal steals all of our login information with these forensic tools.

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.

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&e
mail=s*****ta@freemail.hu_1190488290
```

Fig. 14 Extracted data by IECacheView

To explain Figure 14, 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.

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 [33]. 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) 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.

4) Fourth Evidence

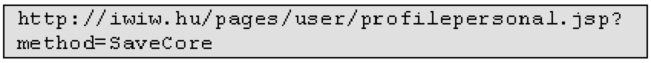
If John knows Jennifer's Facebook account, discovery of the internet activities of the other Hungarian popular social media site, iWiW, is recommended. In the browser's password files we did not find any stored records related to this website, but we should again walk through the browser history.

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 [34].

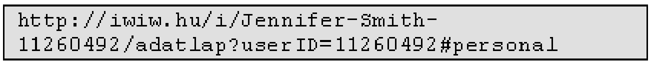
From the point of view of the investigation, the following record is very interesting as it has been found as a referrer page:



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

Fig. 15 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. 16 Jennifer's iWiW user profile page

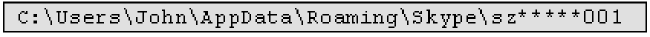
The *Last Visit Date* of both pages is exactly the same *21/08/2011.21:36:59*. Is it possible that John has modified his profile page and in the same second he opened his ex-girlfriend's personal iWiW page (Fig. 15)? Such a chance is very small. During the forensic investigation it was identified that, after saving the modification of personal data, the page (Fig. 15) immediately and automatically opens the logged in user's personal iWiW page (Fig. 16). Because of the nature of the mentioned technology, this could only happen if the Figure 15 page was opened by the logged in Jennifer Smith. Was

Jennifer in John’s house at this time? No, she was on holiday.

B. *Skype Forensic Artefacts*

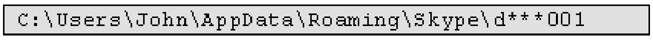
If the previous evidence is not enough to prove that John has used Jennifer’s accounts, here are additional artefacts provided by Skype.

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. 17 Jennifers’s Skype profile folder



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

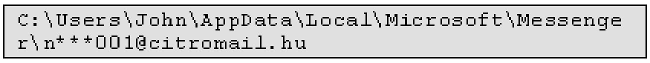
Fig. 18 John’s Skype profile folder

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* [20], a free forensic tool.

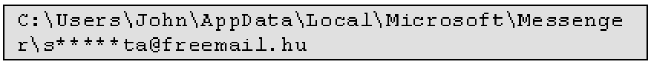
C. *Windows Live Messenger*

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. 19, Fig. 20):



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

Fig. 19 John’s WLM profile folder

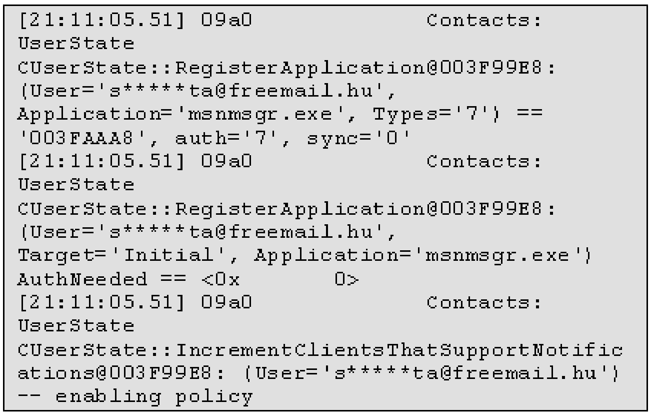


```
C:\Users\John\AppData\Local\Microsoft\Messenge
r\s*****ta@freemail.hu
```

Fig. 20 Jennifer’s WLM profile folder

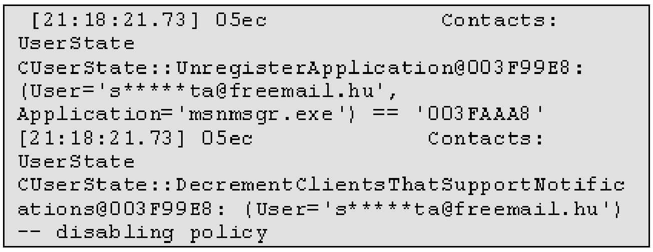
However, although we had discovered Jennifer’s account, we could not be sure that the existence of the *s*****ta@freemail.hu* folder meant that someone had logged into WLM with Jennifer’s account. The folder could have been created by WLM to store data about Jennifer as John’s chat partner. For this 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. 21).



```
[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::IncrementClientsThatSupportNotific
ations@003F99E8: (User='s*****ta@freemail.hu')
-- enabling policy
```

Fig. 21 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::DecrementClientsThatSupportNotific
ations@003F99E8: (User='s*****ta@freemail.hu')
-- disabling policy
```

Fig. 22 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 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.

V. Privacy advices

As we have seen from the previous sections there are several places where our computer stores our internet activity footprints and there are several tools that can easily retrieve them as well.

Hereby we suggest 3 simple advices in order to prevail and live safe in the world of social networks.

A. *Password protection*

The first and most important step is about our passwords. We know that it is not worth to store our passwords written on a sticker next to our display, however we saw, we are not safe in case our computer stores our login information itself. Therefore the most important advice - beyond we are not allow strangers to access our PC physically; do not ask neither allow your web browser to store your login information.

On the other hand if we are careful enough and choose different passwords for each web locations we authenticate ourselves, it is impossible to memorize all of them. Fortunately every operating system offers effective software based solutions to store our secure information; we have to memorize only one master passphrase which unlocks all our sensitive data.

We can store our passwords in the best safe of the world it is useless, if it is easy to guess our password. A whole generation has grown up since the Internet became the active part of our everyday life, nonetheless we can still meet that kind of passphrases that are equal with its owner's pet's name relative's name or with his or her birthday.

Although major systems constrain users to choose adequate passwords during registration process; it is worth to listen to them.

B. *Careful sharing*

Our second advice is to accept the fact that everything we share on a social media site, upload to a web page or send via Skype or MSN gets out of our control. It will not be our private data anymore; after sharing it can appear anytime and anywhere. We can trust in that imagined fact that the picture we sent to our friend will not get out from his hand or only our friends can see our photos on Facebook, do not fool ourselves; from a time we have shared something it is potentially reachable by everyone.

It is possible that our friend will not abuse with our private pictures, but if he does not protect his data properly anyone can get all his confidential data including our ones as well.

Therefore we should pay special attention for sharing only that kind of information during our social life which do not cause nuisance for us later.

It is important to know that a Facebook profile could affect a hiring potential as well. Almost half of executives say they are likely to make a hiring decision based on a prospective employee's online identity or Facebook profile and over 30 percent also believes a company has the right to fire an employee based on inappropriate comments the employee made on his/her Facebook page [35]. It is worth to have another think before we comment or share something on social media sites about our previous, present or future job.

C. *The Clean Sheet*

Our third and last advice is to remember that our every movement on the Web leaves several footprints on our computer. Do not forget to delete your browsing history, your temporary Internet files and instant messenger conversations regularly. Cleaning browsing history requires only two button clicks and five seconds.

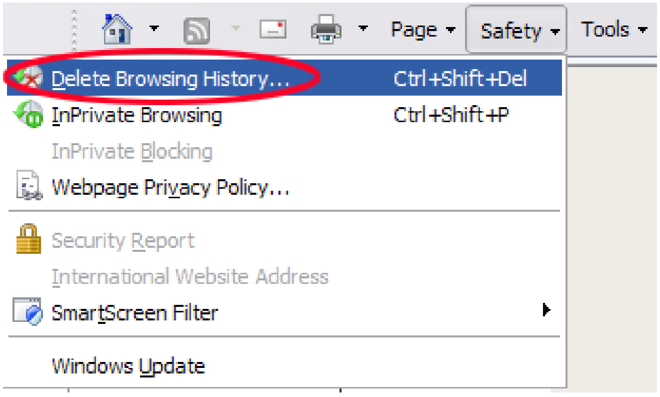
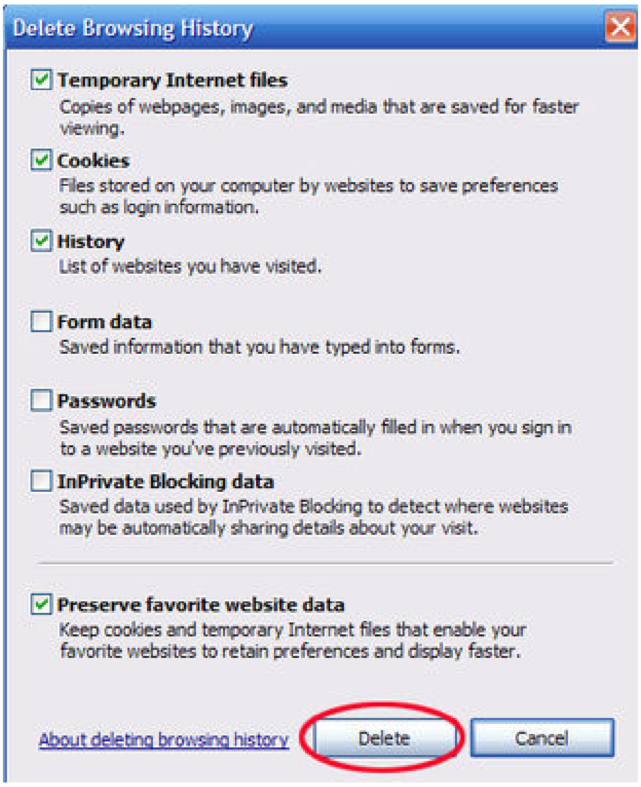

Page
Safety
Tools
Delete Browsing History... Ctrl+Shift+Del
InPrivate Browsing Ctrl+Shift+P
InPrivate Blocking
Webpage Privacy Policy...
Security Report
International Website Address
SmartScreen Filter
Windows Update

Fig. 23 Deleting Internet Explorer 8 browsing history - Step 1 [36]



Delete Browsing History

☑ **Temporary Internet files**
Copies of webpages, images, and media that are saved for faster viewing.

☑ **Cookies**
Files stored on your computer by websites to save preferences such as login information.

☑ **History**
List of websites you have visited.

□ **Form data**
Saved information that you have typed into forms.

□ **Passwords**
Saved passwords that are automatically filled in when you sign in to a website you've previously visited.

□ **InPrivate Blocking data**
Saved data used by InPrivate Blocking to detect where websites may be automatically sharing details about your visit.

☑ **Preserve favorite website data**
Keep cookies and temporary Internet files that enable your favorite websites to retain preferences and display faster.

About deleting browsing history

Fig. 24 Deleting Internet Explorer 8 browsing history - Step 2 [36]

On this form we can clear our stored browser passwords as well. It is worth to devote the time; it could be the best investment of your life. You never know the time when your computer fall into wrong hands (or even seized by an investigator) it is better to start with clean sheet.

VI. Teaching digital citizenship

Web 2.0 and social networks became quickly the part of our everyday life, we began to use it before we have got all the information about it. Therefore it is important to prepare ourselves and our children for the rules and dangers of digital life; the keyword is *digital citizenship*.

Digital citizenship may be defined as the ability to use technology safely, responsibly, critically, productively, and civically. For learners to deal with digital information, they must first become aware of it. [37]

It is the responsibility of educators and parents to equip children with both their digital rights as well as their digital responsibilities. Because technology keeps expanding and changing continuously, laws are behind practice, and even social norms of behavior are dynamic. When engaging with digital information from a legal or ethical standpoint, one of the most effective strategies is case studies: educators can share legal cases dealing with technology issues that arise in access to confidential information, broadcasting inappropriate information, social networking, file transfer, pirating or plagiarizing information, and other intellectual property issues [37].

Cyber security exercises are a very effective way of learning the practical aspects of information security, however designing a cyber security exercise is not an easy task and requires the work of several people. [38].

Educators need to teach explicit guidelines for evaluating the quality of digital information and its relevance. To check for learner understanding, and to engage them in active examination, debate, and self-reflection, educators can use a variety of technological tools: e-learning platform, threaded discussion, online chat, blogs, wikis, and online conferencing.

Many educators use technology on a personal basis, such as communication, but have not had formal training in technology-integrated instructional design. Therefore, many do not feel comfortable in using such educational technology in the classroom or online. Not only should educators learn technology, including web 2.0 tools, but they should also seek opportunities to commingle with technology users.

On the other hand, educators have life experiences and a developed moral sense that they can leverage when incorporating digital citizenship [37].

The situation is the same if we are talking about parents. They also use technology on a personal basis, but can not handle the situation when their child would like to join to the information highway. New York State Office of the Attorney General recognized this problem and made a fifteen pages booklet [39] for parents about how to stay safe while taking advantage of all the Internet has to offer.

VII. conclusionss

Social media networks have many benefits. Social network activities may lead to new friendships, better quality of communication and writing skills. It is very encouraging to see how children and young people develop a shared culture on the Internet, they bravely use all the new technologies. Unfortunately cyber criminals also know that, our children and every less experienced web user can be easily vulnerable to hacking, digital bullying, fraud attempts and even grooming or physical attacks. It is very important to teach and train ourselves and our children about Internet security and safe and reasonable behaviour on the Web.

In our real case 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] Fan Yang, Zhi-Mei Wang, A Mobile Locationbased Information Recommendation System Based on GPS and WEB2.0 Services, *WSEAS TRANSACTIONS on COMPUTERS*, Issue 4, Volume 8, April 2009, pp. 725-734

[2] Cheng-Jung Lee, Chang-Chun Tsai,Shung-Ming Tang, Liang-Kai Wang, "Innovation: Web 2.0, Online-Communities and Mobile Social Networking,“ *WSEAS TRANSACTIONS on COMPUTERS*, Issue 11, Volume 8, November 2009, pp. 1825-1834

[3] Nielsen (2012, August). *State of the Media : The Social Media Report Q3 2011*. Available: http://blog.nielsen.com/nielsenwire/social/

[4] Cara Pring (2012, May). *99 New Social Media Stats for 2012*, The Social Skinny. Available: http://thesocialskinny.com/99-new-social-media-stats-for-2012/

[5] Esteban Contreras (2012, August). *The State of Social Media and Social Media Marketing in 2012*. Available: http://www.slideshare.net/socialnerdia/the-state-of-social-media-and-social-media-marketing-in-2012-10743590

[6] Khairul Akram Zainol Ariffin, Ahmad Kamil Mahmood, Jafreezal Jaafar, "Investigating the PROCESS block for memory analysis, " *Proceedings of the 11th WSEAS international conference on Applied Computer Science*, 2011, pp. 21-29

[7] Google Analytics, August 2012, http://www.google.com/analytics

[8] Zsolt Nagy, "Using Forensic Techniques for Internet Activity Reconstruction,“ *Proceedings of the 16th WSEAS International Conference on Computers*, 2012. pp. 248–253

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

[10] 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.

[11] W3.org (2012, May). Hypertext Transfer Protocol. Available : http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html

[12] Jones Keith J. (2012, May). Forensic Analysis of Internet Explorer Activity Files. Available : http://www.mcafee.com/us/resources/white-papers/foundstone/wp-pasco.pdf

[13] SQLite.org (2012, May) - http://www.sqlite.org

[14] MozillaZine.org (2012, May). Mozilla Profile Folder. Available : http://kb.mozillazine.org/Profile_folder_-_Firefox

[15] SQLite Database Browser (2012, May) - http://sqlitebrowser.sourceforge.net/

[16] Opera.com (2012, May). Files used by Opera, Available : http://www.opera.com/docs/operafiles/

[17] Digital Detective (2011, May). Apple Safari Browser [Online] Available : http://blog.digital-detective.co.uk/2011/02/apple-safari-browser.html

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

[19] Skype (2012, May). What is Skype?. Available : https://support.skype.com/en-us/

[20] Nirsoft.net (2012, May). SkypeLogView, http://www.nirsoft.net/utils/skype_log_view.html

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

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

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

[24] IECacheView (2012, May). Available: http://www.nirsoft.net/utils/ie_cache_viewer.html

[25] Web Historian (2012, May). Available: http://www.mandiant.com/resources/download/web-historian

[26] Internet Evidence Finder (2012, May) . Available: http://www.jadsoftware.com/internet-evidence-finder/

[27] MozillaCacheView (2012, May). Available: http://www.nirsoft.net/utils/mozilla_cache_viewer.html

[28] OperaCacheView (2012, May). Available: http://www.nirsoft.net/utils/opera_cache_view.html

[29] IEPassView (2012, May). Available: http://www.nirsoft.net/utils/internet_explorer_password.html

[30] PasswordFox (2012, May). Available: http://www.nirsoft.net/utils/passwordfox.html

[31] OperaPassView (2012, May). Available: http://www.nirsoft.net/utils/opera_password_recovery.html

[32] WebBrowserPassword (2012, May). Available: http://www.nirsoft.net/utils/web_browser_password.html

[33] Messenger Plus! The Messenger Extension (2012, May). Available: http://www.msgplus.net

[34] IETF.org (2012, May). Uniform Resource Identifier (URI): Generic Syntax. Available: http://tools.ietf.org/html/rfc3986

[35] LiveCareer.com (2012, May). *Your Facebook Profile Could Affect Your Hiring Potential*. Available: http://www.livecareer.com/press-releases/your-facebook-profile-could-affect-your-hiring-potential

[36] About.com (2012, August). *How to Delete Browsing History In Internet Explorer 8*. Available: http://browsers.about.com/od/internetexplorertutorials/ss/ie8privatedata.htm

[37] Lesley S. J. Farmer, "Teaching Digital Citizenship, " *Proceedings of the 9th WSEAS International Conference on Education and Educational Technology*, 2010, pp. 387-392

[38] Victor-Valeriu Patriciu,Adrian Constantin Furtuna, "Guide for designing cyber security exercises," *Proceedings of the 8th WSEAS International Conference on E-Activities and information security and privacy*, 2009, pp. 172-177

[39] New York State Office of the Attorney General (2012, August). Your Child's Digital Life: Safety Tips for Parents. Available: http://www.ag.ny.gov/sites/default/files/pdfs/publications/Internet%20Safety%20FINAL%20Handout%206-19.pdf