Forensic Analysis of Private Browsing Artifacts

Huwida Said, Noora Al Mutawa, Ibtesam Al Awadhi and Mario Guimaraes
College of Information Technology
Zayed University, Dubai
United Arab Emirates
{Huwida.said, M80000952, M80000938, Mario.guimaraes}@zu.ac.ae

Abstract - **The paper investigates the effectiveness of the privacy mode feature in three widely used Web browsers, and outlines how to investigate when these browsers have been used to perform a criminal or illegal act. It performs an identical test on a privacy mode session for each of the three Web browsers and investigates whether traces are left behind. The analysis is done in three phases. First, common places where history and cache records are usually stored are examined. Then, other locations on the local machine are examined using special forensic tools. Also, the physical memory (RAM) is captured and examined for traces.**

Index Terms *- Private browsing, artifacts left by private browsing, incognito, in-private and Firefox private browsing.*

1. INTRODUCTION

Web browsers are used to perform different activities over the Internet. People use them to search for information, shop online, communicate through emails or instant messaging, and join online blogs or social networks, and many other functions. Web browsers are designed in a fashion that enables them to record and retain a lot of information related to their users' activities. This included caching files, visited URLs, search terms, cookies, and others. These files are stored on the local computer and can be easily accessed and retrieved by any person who uses the same computer. This also makes it relatively easy for forensic examiners to investigate a suspect's Internet activities in cases where questionable web sites were visited or criminal acts were conducted through the Internet.

In recent years however, many of the well known web browser companies have shown more concern regarding users' privacy while surfing the Internet. Therefore, a new feature was introduced into web browsers that enables Internet users a greater control over their privacy. This feature is known as private browsing, and aims at allowing users to surf the Internet without leaving data trails on their computers.

This paper aims to investigate the effectiveness of the privacy mode feature in three widely used Web browsers: IE InPrivate, Google Chrome Incognito, and Mozilla Firefox Private Browsing. It also outlines how to investigate when these browsers have been used to perform criminal or illegal acts. It performs identical tests on privacy mode sessions on each of the three Web browsers and investigates whether traces are left behind. The analysis is done in three phases. First, common places where history and cache records are usually stored are examined. Then, other locations on the local machine are examined using special forensic tools. Finally, the physical memory RAM is captured and examined. The tests and analysis focuses on traces regarding visited URLs, cached Web pages, and keywords used in search engines or forums. Other artifacts left by Web browsing are outside the scope of this paper. Also, the paper assumes that the reader is knows the basic steps in a forensic examination of a computer's hard disk and will not cover this process.

2. LITERATURE REVIEW

ADbC Private browsing mode feature was first introduced in 2005 by Apple Safari 2.0. It was followed after three years by Google chrome 1.0 (Incognito). Later, in 2009 Microsoft Internet Explorer 8 and Mozilla Firefox 3.5 introduced their versions of private browsing modes known respectively as InPrivate and Private Browsing (Dan, 2010). Many papers have been written investigating the privacy mode features provided in modern Web browsers including Internet Explorer, Google Chrome, and Firefox, and comparing them to one another. According to one of the papers (Belani, Jones, 2005), the vendors of all these Web browsers claim that none of the visited Web sites, form field data, addresses typed into the address bar, visited links, and search queries, are stored on the local computer of the user (Brookman, 2010). If these claims are true, users will have a greater privacy while surfing the Internet, and will not have to worry about curious people trying to find out their browsing habits or personal data. On the other hand, cybercriminals can take advantage of this feature and use it to reduce or even eliminate traces to their criminal behavior. They will be able to conduct search queries and participate in illegal acts without leaving any traces on the local computer. In fact, a survey study found that private browsing was more popular at adult Web sites than at gift shopping or news Web sites. This suggests that Web browser vendors may be mischaracterizing the main use of this tool when describing it as a tool for buying surprise gifts (Aggarwal, Boneh, Bursztein, & Jackson, 2010). This brings up an important question; how will this feature affect the digital forensics field? This will certainly

978-1-4577-0314-0/11/$26.00 ©2011 IEEE

impact the reconstruction of a suspect's questionable behavior conducted through the Internet (Olzak, 2008).

Even though papers have been written on privacy mode feature of modern Web browsers, we did not find any that investigated the artifacts left on the local computer by the use of this feature. Therefore, we decided to conduct some tests that would provide a better understanding of this feature, the artifacts left by the use of it, and how it could affect investigations in the digital forensics field. The following section describes the methodology that we followed.

3. METHODOLOGY

This section describes the test and analysis we conducted on the privacy mode feature of three popular web browsers. These web browsers are Internet Explorer (InPrivate), Firefox (Private Browsing), and Google Chrome (Incognito). In order to perform the test, several hardware and software tools have been used. The following is a list of all the hardware and software that are used throughout the paper:

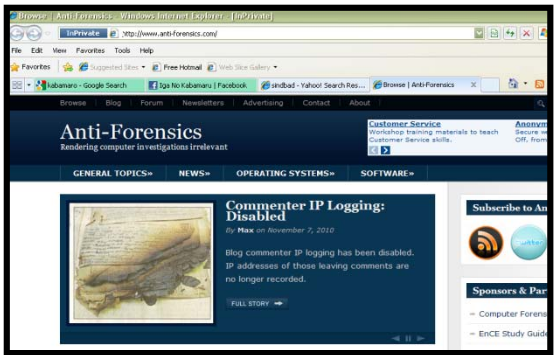
- *Three Dell Precision PWS 490 workstations with 3.25 GB RAM, Windows XP Professional Service Pack 2 and a 300 GB hard-disk formatted with NTFS.*
- *Internet Explorer version 8.0.6001.18702.*
- *Mozilla Firefox version 3.6.11.*
- *Google Chrome version 7.0.517.41.*
- *FTK Imager Lite 2.9.0 for capturing physical memory RAM.*
- *Winhex 15.6 for analyzing physical memory RAM.*
- *Cache and History viewers.*
- *EnCase version 6.8.1.8 for forensic examination.*

We used three workstations with the same hardware and software specifications. They were Dell Precision PWS 490 workstations with 3.25 GB RAM, Windows XP Professional Service Pack 2 and a 300 GB hard-disk formatted with NTFS. We installed Internet Explorer version 8.0.6001.18702 on the first workstation, Mozilla Firefox version 3.6.11 on the second, and Google Chrome version 7.0.517.41 on the third. We then made three small lists that included URLs to be entered in the Web browsers address bars, and keywords that will be used in search queries using different search engines and forum search options. The URLs and keywords were unique to the workstations to ensure the accuracy of the test. Table 1 is one of the lists we made of the unique URLs and keywords we used to conduct the test.

URLs	Keywords used in search queries
anti-forensics.com lesmills.com munfitnessblog.com	kabamaro – google.com sindbad – yahoo.com timestomp – anti-forensics forum

TABLE 1: UNIQUE URLS, KEYWORDS USED IN THE TEST

The test was carried out on each of the three web browsers. First, the private browsing mode was activated. Then, the same list of URLs was entered in the address bars of each web browser. Also, embedded links within web pages were clicked and opened in new tabs or new windows, and different keywords were queried using different search engines or forum search options. This was to imitate the behaviors of users in real life. Finally, the private browsing mode was turned off by exiting the web browser. The tests and analysis were carried out three times on three different private browsing mode sessions for each Web browser using the three different lists we made. After ending each session, an analysis was conducted by capturing physical memory and analyzing it, examining common locations of Web browsing history and cache of each Web browser, and examining other location where artifacts may reside by using forensic analysis tools. Conducting three tests were to double check our findings and make sure that the results were accurate. Figures 1-4 illustrates some of the tests performed. The results of the tests are discussed in the next section.


Browse | Anti-Forensics - Windows Internet Explorer - [InPrivate]
InPrivate
http://www.anti-forensics.com/
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Free Hotmail
Web Slice Gallery
kabamaro - Google Search
Iga No Kabamaru | Facebook
sindbad - Yahoo! Search Res...
Browse | Anti-Forensics
Browse Blog Forum Newsletters Advertising Contact About
Anti-Forensics
Rendering computer investigations irrelevant
GENERAL TOPICS» NEWS» OPERATING SYSTEMS» SOFTWARE»
FULL STORY
Subscribe to An
Sponsors & Par
Computer Forens
EnCE Study Guide

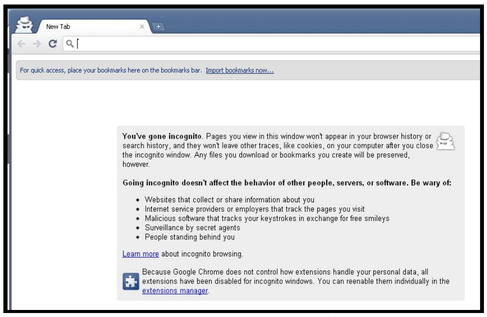
Customer Service
Workshop training materials to teach Customer Service skills.

Commenter IP Logging: Disabled

By Max on November 7, 2010

Blog commenter IP logging has been disabled. IP addresses of those leaving comments are no longer recorded.

FIGURE 1- URLS AND KEYWORDS IN PRIVATE MODE ON IE



For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...

You've gone incognito. Pages you view in this window won't appear in your browser history or search history, and they won't leave other traces, like cookies, on your computer after you close the incognito window. Any files you download or bookmarks you create will be preserved, however.

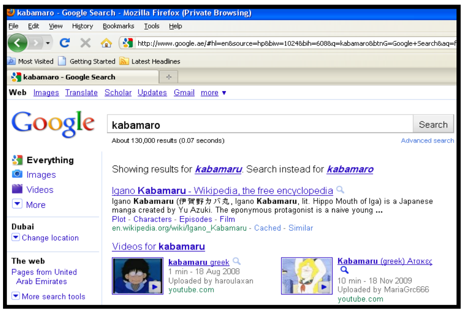
Going incognito doesn't affect the behavior of other people, servers, or software. Be wary of:

- Websites that collect or share information about you
- Internet service providers or employers that track the pages you visit
- Malicious software that tracks your keystrokes in exchange for free smileys
- Surveillance by secret agents
- People standing behind you

Learn more about incognito browsing.

Because Google Chrome does not control how extensions handle your personal data, all extensions have been disabled for incognito windows. You can reenable them individually in the extensions manager.

FIGURE 2– ACTIVATE PRIVATE MODE in GOOGLE CHROME.


kabamaro - Google Search - Mozilla Firefox (Private Browsing)
File Edit View History Bookmarks Tools Help
Most Visited
Getting Started
Latest Headlines
kabamaro - Google Search
Web Images Translate Scholar Updates Gmail more
Google
Search
Advanced search
Everything
Images
Videos
More
Dubai
Change location
The web
Pages from United Arab Emirates
More search tools

http://www.google.ae/#hl=en&source=hp&biw=1024&bih=608&q=kabamaro&btnG=Google+Search&aq=f

kabamaro

About 130,000 results (0.07 seconds)

Showing results for *kabamaru*. Search instead for *kabamaro*

Igano **Kabamaru** - Wikipedia, the free encyclopedia

Igano **Kabamaru** (伊賀野カバ丸, Igano **Kabamaru**, lit. Hippo Mouth of Iga) is a Japanese manga created by Yu Azuki. The eponymous protagonist is a naive young **...**

Plot - Characters - Episodes - Film

en.wikipedia.org/wiki/Igano_Kabamaru - Cached - Similar

Videos for **kabamaru**

kabamaru greek
1 min - 18 Aug 2008
Uploaded by haroulaxan
youtube.com

Kabamaru (greek) Ατακες
10 min - 18 Nov 2009
Uploaded by MariaGrc666
youtube.com

FIGURE 3- TESTING URLS AND KEYWORDS INPRIVATE MODE ON *MOZILLA FIREFOX.*

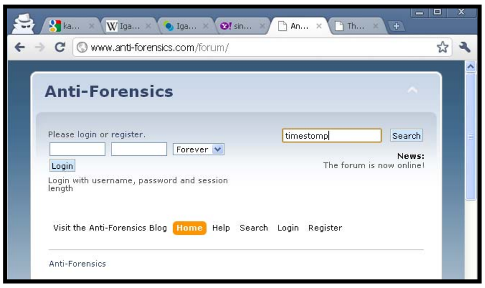


FIGURE 4- TESTING URLS AND KEYWORDS IN PRIVATE MODE ON GOOGLE CHROME

4. ANALYSIS AND RESULTS

This section describes our finding from the tests and analysis we conducted on each Web browser. After conducting each test, and before conducting any analysis, we used FTK Imager Lite to capture an image of the physical memory of each workstation and set it aside. Then, we started analyzing common history and cache locations of each Web browser to find out whether traces of the tests we made could be found. After that, we went back to the files of captured physical memories and used *Winhex* to analyze each of them. Finally, we used *EnCase* to acquire an image of each hard disk and perform a forensic analysis by looking into other locations where traces could be found. Figures 5-7 our findings in each of the Web browsers we tested.

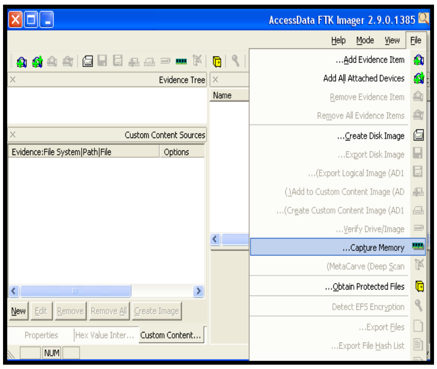
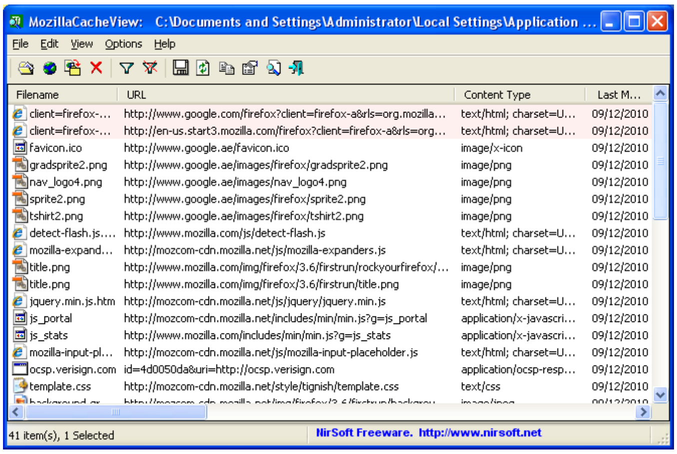


FIGURE 5- USING FRK IMAGER LITE TO CAPTURE THE PHYSICAL MEMORY OF THE THREE MACHINES.

4.1 Mozilla Firefox

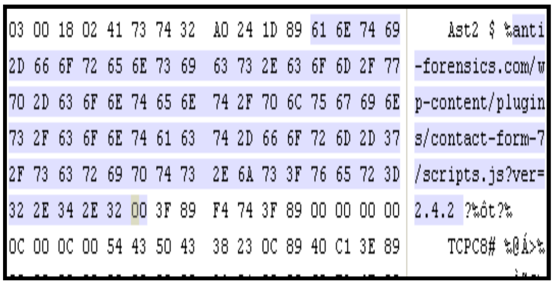
The first step was to analyze the common places where Mozilla Firefox stores Web browsing history and cache. We used *MozillaCacheView* and *MozillaHistoryView* to analyze cache and history records. Reviewing those records showed files and URLs that were related to Web browsing activities performed using Mozilla Firefox in normal mode. However, there were no traces of Web browsing activities performed during Web privacy mode. We did not find any URLs or keywords we used during the test, nor did we find any other files related to the visited Web sites. We then moved to the second step and started analyzing the captured image of the physical memory. Running a string search showed hits on all URLs and keywords we used during the test. For example, there were 143 entries for the visited URL "***anti-forensics.com***", 33 entries for the queried keyword ***"sindbad"***, and 4 entries for the keyword ***"kabamaro".*** We were also able to find ***blocks of HTML code*** that constructs Web sites we visited.


MozillaCacheView: C:\Documents and Settings\Administrator\Local Settings\Application ...
File
Edit
View
Options
Help
NirSoft Freeware. http://www.nirsoft.net

Filename	URL	Content Type	Last M...
client=firefox-...	http://www.google.com/firefox?client=firefox-a&rls=org.mozilla...	text/html; charset=U...	09/12/2010
client=firefox-...	http://en-us.start3.mozilla.com/firefox?client=firefox-a&rls=org...	text/html; charset=U...	09/12/2010
favicon.ico	http://www.google.ae/favicon.ico	image/x-icon	09/12/2010
gradsprite2.png	http://www.google.ae/images/firefox/gradsprite2.png	image/png	09/12/2010
nav_logo4.png	http://www.google.ae/images/nav_logo4.png	image/png	09/12/2010
sprite2.png	http://www.google.ae/images/firefox/sprite2.png	image/png	09/12/2010
tshirt2.png	http://www.google.ae/images/firefox/tshirt2.png	image/png	09/12/2010
detect-flash.js....	http://www.mozilla.com/js/detect-flash.js	text/html; charset=U...	09/12/2010
mozilla-expand...	http://mozcom-cdn.mozilla.net/js/mozilla-expanders.js	text/html; charset=U...	09/12/2010
title.png	http://www.mozilla.com/img/firefox/3.6/firstrun/rockyourfirefox/...	image/png	09/12/2010
title.png	http://www.mozilla.com/img/firefox/3.6/firstrun/title.png	image/png	09/12/2010
jquery.min.js.htm	http://mozcom-cdn.mozilla.net/js/jquery/jquery.min.js	text/html; charset=U...	09/12/2010
js_portal	http://mozcom-cdn.mozilla.net/includes/min/min.js?g=js_portal	application/x-javascri...	09/12/2010
js_stats	http://www.mozilla.com/includes/min/min.js?g=js_stats	application/x-javascri...	09/12/2010
mozilla-input-pl...	http://mozcom-cdn.mozilla.net/js/mozilla-input-placeholder.js	text/html; charset=U...	09/12/2010
ocsp.verisign.com	id=4d0050da&uri=http://ocsp.verisign.com	application/ocsp-resp...	09/12/2010
template.css	http://mozcom-cdn.mozilla.net/style/tignish/template.css	text/css	09/12/2010

41 item(s), 1 Selected

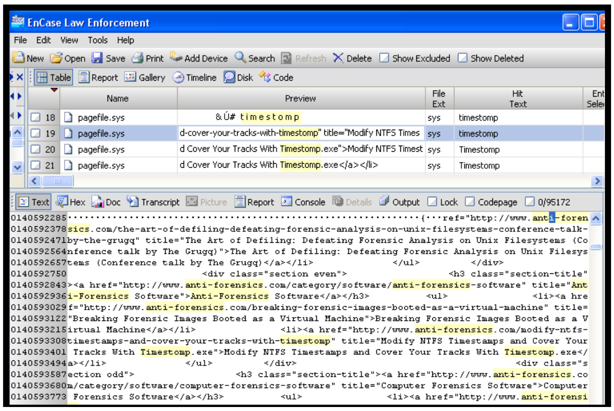
FIGURE 6- COMMON CACHE AND HISTORY PLACES OF FIREFOX DO NOT HAVE TRACES OF PRIVATE MODE WEB ACTIVITIES.



```
03 00 18 02 41 73 74 32  A0 24 1D 89 61 6E 74 69    Ast2 $ ‰anti
2D 66 6F 72 65 6E 73 69  63 73 2E 63 6F 6D 2F 77   -forensics.com/w
70 2D 63 6F 6E 74 65 6E  74 2F 70 6C 75 67 69 6E   p-content/plugin
73 2F 63 6F 6E 74 61 63  74 2D 66 6F 72 6D 2D 37   s/contact-form-7
2F 73 63 72 69 70 74 73  2E 6A 73 3F 76 65 72 3D   /scripts.js?ver=
32 2E 34 2E 32 00 3F 89  F4 74 3F 89 00 00 00 00   2.4.2 ?‰ôt?‰
0C 00 0C 00 54 43 50 43  38 23 0C 89 40 C1 3E 89       TCPC8# ‰@Á>‰
```

FIGURE 7- "ANTI-FORENSICS" LINKS FOUND IN PHYSICAL MEMORY OF THE MACHINE THAT USED MOZILLA FIREFOX

The final step was to perform the forensic analysis. After acquiring an image of the hard disk and verifying it, we started analyzing some files and folders that we thought might include some trails. First, we examined the common folders where Mozilla Firefox stores Web browsing history and cache suspecting that we might find some deleted cache files or history records related to our test. No trails were found. Examining unallocated space and slack space did not reveal any trails as well. However, examining pagefile.sys showed some positive hits (Figure 8). We found 89 entries for "***anti-forensics.com"*** with block of HTML code that we were able to recover and use to reconstruct the visited Web pages. There were also 6 entries for the keyword ***"timestomp",*** 2 entries for the keyword ***"kabamaro",*** and 6 entries for the keyword ***"sindbad"***. Running a string search of all URLs and keywords used during the test on the entire hard disk did not reveal any traces other the ones found in pagefile.sys.


EnCase Law Enforcement
File Edit View Tools Help
New Open Save Print Add Device Search Refresh Delete □ Show Excluded □ Show Deleted
Table Report Gallery Timeline Disk Code
Text Hex Doc Transcript Picture Report Console Details Output □ Lock □ Codepage □ 0/95172

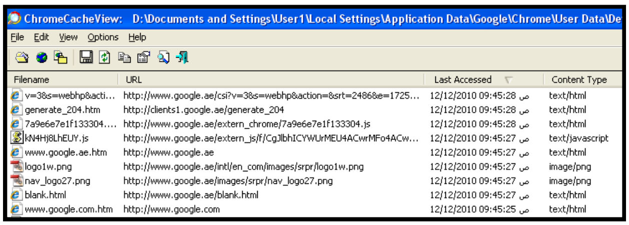
	Name	Preview	File Ext	Hit Text	Ent Sele
□ 18	pagefile.sys	&Ú# timestomp	sys	timestomp	
□ 19	pagefile.sys	d-cover-your-tracks-with-timestomp" title="Modify NTFS Times	sys	timestomp	
□ 20	pagefile.sys	d Cover Your Tracks With Timestomp.exe">Modify NTFS Timest	sys	Timestomp	
□ 21	pagefile.sys	d Cover Your Tracks With Timestomp.exe</a></li>	sys	Timestomp	

```
0140592285··························································{···ref="http://www.anti-foren
0140592378sics.com/the-art-of-defiling-defeating-forensic-analysis-on-unix-filesystems-conference-talk-
0140592471by-the-grugq" title="The Art of Defiling: Defeating Forensic Analysis on Unix Filesystems (Co
0140592564nference talk by The Grugq)">The Art of Defiling: Defeating Forensic Analysis on Unix Filesys
0140592657tems (Conference talk by The Grugq)</a></li>              </ul>          </div>
0140592750                        <div class="section even">                  <h3 class="section-title"
0140592843><a href="http://www.anti-forensics.com/category/software/anti-forensics-software" title="Ant
0140592936i-Forensics Software">Anti-Forensics Software</a></h3>          <ul>              <li><a hre
0140593029f="http://www.anti-forensics.com/breaking-forensic-images-booted-as-a-virtual-machine" title=
0140593122"Breaking Forensic Images Booted as a Virtual Machine">Breaking Forensic Images Booted as a V
0140593215irtual Machine</a></li>               <li><a href="http://www.anti-forensics.com/modify-ntfs-
0140593308timestamps-and-cover-your-tracks-with-timestomp" title="Modify NTFS Timestamps and Cover Your
0140593401 Tracks With Timestomp.exe">Modify NTFS Timestamps and Cover Your Tracks With Timestomp.exe</
0140593494a></li>              </ul>          </div>                                        <div class="s
0140593587ection odd">                  <h3 class="section-title"><a href="http://www.anti-forensics.co
0140593680m/category/software/computer-forensics-software" title="Computer Forensics Software">Computer
0140593773 Forensics Software</a></h3>          <ul>                <li><a href="http://www.anti-forensi
```

FIGURE 8- TRACES FOUND ON THE ACQUIRED IMAGE OF THE MACHINE THAT USED MOZILLA FIREFOX.

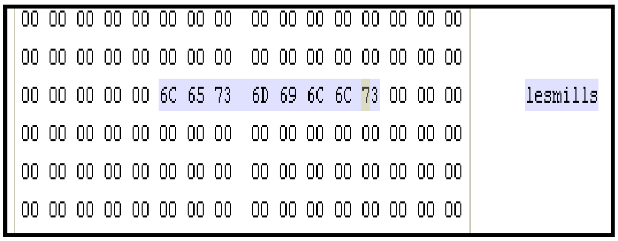
4.2 Google Chrome

Similar to Mozilla Firefox, analyzing the common locations of ***cache and history of Google Chrome*** revealed no traces of visited URLs and Web sites during privacy mode, nor did it show any other files related to the Web browsing activities we conducted during the test. Analyzing the physical memory however showed many trails (Figure 9-10). For example, we found 42 entries for the visited URL ***"lesmills.com"***, 100 entries for the searched keyword ***"sindbad"***, and 75 entries for the visited URL ***"anti-forensics.com"***. Blocks of HTML code were also found, retrieved, and used to reconstruct Web pages related to our test.


ChromeCacheView: D:\Documents and Settings\User1\Local Settings\Application Data\Google\Chrome\User Data\De
File Edit View Options Help

Filename	URL	Last Accessed	Content Type
v=3&s=webhp&acti...	http://www.google.ae/csi?v=3&s=webhp&action=&srt=2486&e=1725...	12/12/2010 09:45:28 ص	text/html
generate_204.htm	http://clients1.google.ae/generate_204	12/12/2010 09:45:28 ص	text/html
7a9e6e7e1f133304....	http://www.google.ae/extern_chrome/7a9e6e7e1f133304.js	12/12/2010 09:45:28 ص	text/html
kN4Hj8LhEUY.js	http://www.google.ae/extern_js/f/CgJlbhICYWUrMEU4ACwrMFo4ACw...	12/12/2010 09:45:27 ص	text/javascript
www.google.ae.htm	http://www.google.ae	12/12/2010 09:45:27 ص	text/html
logo1w.png	http://www.google.ae/intl/en_com/images/srpr/logo1w.png	12/12/2010 09:45:27 ص	image/png
nav_logo27.png	http://www.google.ae/images/srpr/nav_logo27.png	12/12/2010 09:45:27 ص	image/png
blank.html	http://www.google.ae/blank.html	12/12/2010 09:45:27 ص	text/html
www.google.com.htm	http://www.google.com	12/12/2010 09:45:25 ص	text/html

FIGURE 9- COMMON CACHE AND HISTORY PLACES OF GOOGLE CHROME DO NOT HAVE TRACES OF PRIVATE MODE WEB ACTIVITIES.



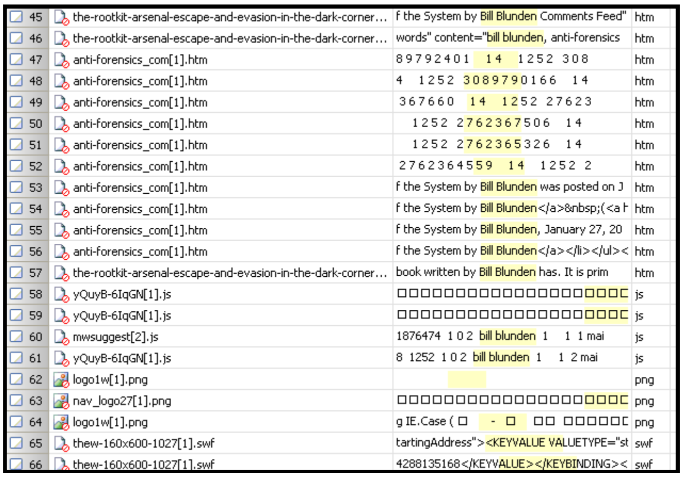
```
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 6C 65 73  6D 69 6C 6C 73 00 00 00     lesmills
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

FIGURE 10- THE STRING "LESMILLS" FOUND IN PHYSICAL MEMORY OF MACHINES THAT USED GOOGLE CHROME.

During the forensic analysis, we did not find any deleted cache or history files. Analyzing unallocated space and slack space did not reveal any traces as well. Also, ***examining page.sys*** file showed no traces at all. Finally, a string search on the entire hard disk resulted in zero hits for all URLs and keywords we used during our test.

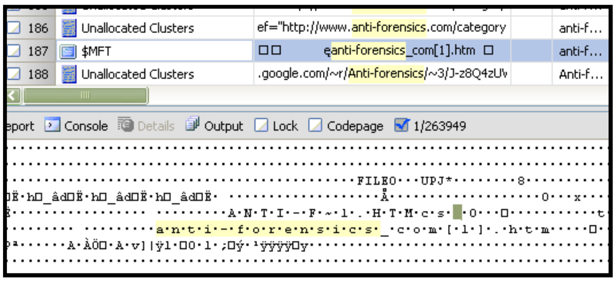
4.3 Internet Explorer

Similar to the first two Web browsers, analyzing the common locations of cache and history of Internet Explorer revealed no traces of visited URLs and Web sites during privacy mode, nor did it show any other files related to the Web browsing activities we conducted during the test. However, analyzing the physical memory revealed many trails (Figure 11-12). For example, we found 37 entries for the keyword ***"kabamaro"***, 138 entries for the searched keyword "***sindbad"***, 9 entries for the keyword ***"timestomp"***, and 1302 entries for the visited URL ***"anti-forensics.com"***. Blocks of HTML code were also found, retrieved, and used to reconstruct Web pages related to our test.



□ 45	the-rootkit-arsenal-escape-and-evasion-in-the-dark-corner...	f the System by Bill Blunden Comments Feed"	htm
□ 46	the-rootkit-arsenal-escape-and-evasion-in-the-dark-corner...	words" content="bill blunden, anti-forensics	htm
□ 47	anti-forensics_com[1].htm	89792401 14 1252 308	htm
□ 48	anti-forensics_com[1].htm	4 1252 3089790166 14	htm
□ 49	anti-forensics_com[1].htm	367660 14 1252 27623	htm
□ 50	anti-forensics_com[1].htm	1252 2762367506 14	htm
□ 51	anti-forensics_com[1].htm	1252 2762365326 14	htm
□ 52	anti-forensics_com[1].htm	2762364559 14 1252 2	htm
□ 53	anti-forensics_com[1].htm	f the System by Bill Blunden was posted on J	htm
□ 54	anti-forensics_com[1].htm	f the System by Bill Blunden</a> (<a h	htm
□ 55	anti-forensics_com[1].htm	f the System by Bill Blunden, January 27, 20	htm
□ 56	anti-forensics_com[1].htm	f the System by Bill Blunden</a></li></ul><	htm
□ 57	the-rootkit-arsenal-escape-and-evasion-in-the-dark-corner...	book written by Bill Blunden has. It is prim	htm
□ 58	yQuyB-6IqGN[1].js	□□□□□□□□□□□□□□□□□□□□	js
□ 59	yQuyB-6IqGN[1].js	□□□□□□□□□□□□□□□□□□□□	js
□ 60	mwsuggest[2].js	1876474 1 0 2 bill blunden 1 1 1 mai	js
□ 61	yQuyB-6IqGN[1].js	8 1252 1 0 2 bill blunden 1 1 2 mai	js
□ 62	logo1w[1].png		png
□ 63	nav_logo27[1].png	□□□□□□□□□□□□□□□□□□□□	png
□ 64	logo1w[1].png	g IE.Case (□ - □ □□ □□□□□□	png
□ 65	thew-160x600-1027[1].swf	tartingAddress"><KEYVALUE VALUETYPE="st	swf
□ 66	thew-160x600-1027[1].swf	4288135168</KEYVALUE></KEYBINDING><	swf

FIGURE 11- TRACES FOUND ON THE ACQUIRED IMAGE OF THE MACHINE THAT USED INTERNET EXPLORER.

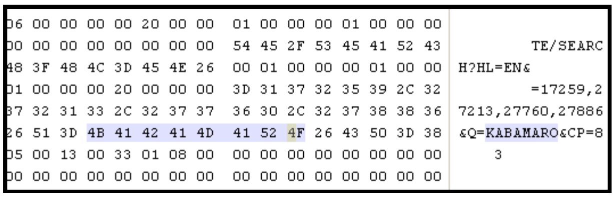


□ 186	Unallocated Clusters	ef="http://www.anti-forensics.com/category	anti-f...
□ 187	$MFT	□□ eanti-forensics_com[1].htm □	anti-f...
□ 188	Unallocated Clusters	.google.com/~r/Anti-forensics/~3/J-z8Q4zUv	Anti-f...

```
·······································································
·······································································
····································FILE0···UPJ*·········8··········
Ë·h□_âd□Ë·h□_âd□Ë·h□_âd□Ë· ···················Å·····················0···x···
Ė················ ·········A·N·T·I·—·F·~·l·.·H·T·M·c·s·▮·0···□··········t
········· ·········a·n·t·i·-·f·o·r·e·n·s·i·c·s·_·c·o·m·[·l·]·.·h·t·m·····□·
ª·······A·ÀÖ□·A·v]|ÿl·□0·l·;□ý·¹ÿÿÿÿ□y·······································
·······································································
```

FIGURE 12-TRACES FOUND ON THE ACQUIRED IMAGE OF THE MACHINE THAT USED INTERNET EXPLORER.

During the forensic analysis, we came upon a big surprise. Evidence was scattered all over the hard disk. Intact, deleted files related to the Web browsing activities performed during the test were found in common Internet Explorer Cache and History folders. It seems that during privacy mode, Internet Explorer caches Web pages and stores the files on the hard disk. It deletes them when the private browsing session is terminated. Therefore, the files reside on the hard disk and could be recovered until they are overwritten by other files (Figure 13). Also, entries of URLs and keywords used during the test were found in many files such as *MFT*, some *dat* files, *dll* files, and others. Unallocated space was also rich with evidence and traces related to the conducted test. In other words, the entire Web browsing activity conducted during our test could be easily reconstructed using the evidence we found.



```
06 00 00 00 00 20 00 00  01 00 00 00 01 00 00 00
00 00 00 00 00 00 00 00  54 45 2F 53 45 41 52 43          TE/SEARC
48 3F 48 4C 3D 45 4E 26  00 01 00 00 00 01 00 00  H?HL=EN&
01 00 00 00 20 00 00 00  3D 31 37 32 35 39 2C 32          =17259,2
37 32 31 33 2C 32 37 37  36 30 2C 32 37 38 38 36  7213,27760,27886
26 51 3D 4B 41 42 41 4D  41 52 4F 26 43 50 3D 38  &Q=KABAMARO&CP=8
05 00 13 00 33 01 08 00  00 00 00 00 00 00 00 00      3
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

FIGURE 13- THE STRING "KABAMARO" FOUND IN PHYSICAL MEMORY OF THE MACHINES THAT USED INTERNET EXPLORER.

5. ANALYSIS OF RESULTS

The results mentioned in the previous section show that the level of privacy provided by the three browsers is sufficient for the average user. No trails or traces could be found in common places where the Web browsers usually store their cache and history files. Therefore, unless the user has more knowledge in computer technology, he/she will not be able to find Web browsing activities performed during a private session of Web browsing. However, a complete privacy does not occur. All Web browsers dump a sufficient amount of data related to the Web browsing privacy session into the physical memory RAM. So, if the private browsing session was terminated, but the computer was still running, there is a big chance that data related to the private browsing session can be recovered from RAM. Also, in cases where RAM is fully used and there is need for more virtual memory, part of the hard disk behaves as though it was RAM and stores this data. The file that stores the RAM data is called pagefile.sys. So, if the subject computer was turned off after the private browsing session, and data in physical memory was lost, there is still a chance to find data in pagefile.sys. This could help forensic examiners while investigating a case where questionable Web activities were performed during Web browsing private sessions.

Comparing the results (Table 2) of each Web browser suggests that Google Chrome is the most secure of all, in terms of not storing any browsing history, cache files, and keywords used in search queries on the local computer. Mozilla Firefox could be as secure, however, further tests and analysis should be conducted on different computers to confirm or deny this. Meanwhile, Internet Explorer seems to store all Web browsing history, cache files, and keywords used in search queries on the local computer and then deletes them when the private Web browsing session is terminated. As a result, all files reside on the local computer until they are overwritten by other files. This makes it easy for forensic examiners to extract Web browsing files and reconstruct questionable Web activities even though private Web browsing sessions were used to conceal these activities.

Web Browser	Analysis of Cache and Web history in the privacy mode	Analysis of Physical Memory	Forensics Analysis of the Hard drive's Image
Firefox	-No traces of URL and Keywords were found in the web browsing history and caches.	-Many traces were found in the physical memory **-42** entries for visited URL *"Lesmills.com"* **-33** entries for searched keyword *"sindbad"* **-143** entries for visited *"antiforensics.com"* *-Blocks* of *HTML* code were found	- No traces of URL and Keywords when examining the common folder and files. - Traces of URL and keywords are ONLY found when examining the ***pagefile.sys*** file as **-9** entries for keyword ***" timestomp"*** **-2** entries for keyword ***" kabamaro"*** **-6** entries for searched keyword ***"sindbad"*** **-89** entries for visited **"antiforensics.com"** ***-Blocks*** of ***HTML*** code were found
Google Chrome	-No traces of URL and Keywords were found in the web browsing history and caches.	-Many traces were found in the physical memory **-42** entries for visited URL ***" Lesmills.com"*** **-100** entries for searched keyword ***"sindbad"*** **-75** entries for visited **"antiforensics.com"** ***-Blocks*** of ***HTML*** code were found	-Forensics analysis shows no traces of deleted caches or history files as well as unallocated spaces. -Examining the "***examiningpage.sys"*** file shows no traces -This browser was the hardest to retrieve any entries.
Internet Explorer	-No traces of URL and Keywords were found in the web browsing history and caches.	Many traces were found in the physical memory **-9** entries for keyword ***" timestomp"*** **-37** entries for keyword ***" kabamaro"*** **-138** entries for searched keyword ***"sindbad"*** **-1302** entries for visited **"antiforensics.com"** ***-Blocks*** of ***HTML*** code were found	-Evidence was scattered all over the hard drive -During the privacy mode IE caches the web pages in the hard disk. And deleted them when the session is terminated - Entries found in files like ***.MFT, .dat, .dll***

TABLE 2- SUMMARY OF RESULTS

6. CONCLUSION

Traces left by Web browsing activities can be a source of potential digital evidence in an investigation. However, the privacy mode built in new Web browsers can prevent digital analysts from finding these information when examining a subject computer. This paper examined the artifacts left by conducting Web browsing privacy mode sessions in three widely used Web browsers, and analyzed the effectiveness of this tool in each Web browser. It focused on traces regarding Web browsing history, cached files, and keywords used in different search queries. Experiments in this area should increase to cover more aspects of Web browsing such as cookies, flash cookies, certificates, form passwords, and others. For all three web browsers, we concluded that although there was no visible evidence displayed during private browsing, forensic evidence can still be retrieved by using appropriate tools and methodology. It was also concluded that from the user's view point, Google Chrome and Firefox Mozilla are currently better private browsing solutions.

REFERENCES

Aggarwal, G., Boneh, D., Bursztein, E., & Jackson, C. (2010). An analysis of private browsing modes in modern browsers. Stanford University. Retrieved from http://www.usenix.org/events/sec10/tech/ (2010, December 4).

Belani, R., Jones, K., (2005, March, 29). Web browser forensics. Retrieved from http://www.symantec.com/connect/articles/web-browser-forensics-part-1 (2010, December 3).

Brookman, J. (2010, December). Browser privacy features: a work in progress. Center for Democracy & Technology. Retrieved from http://cdt.org/files/pdfs/20101209_browser_rpt.pdf (2010, December 10).

Dan (2010, July, 22). Anonymous search, porn mode browsing, and increasing privacy concerns. Digitoll Blog. Retrieved from http://digitollblog.com/anonymous-search-porn-mode-browsing-and-increasing-privacy-concerns (2010, December 4).

Google. Tab and windows: Incognito mode (private browsing). Retrieved from http://www.google.com/support/chrome/bin/answer.py?hl=en&answer=95464 (2010, December 3).

Olzak, T. (2008, November, 12). How do new private browsing capabilities affect forensics?. Tech Republic. Retrieved from http://blogs.techrepublic.com.com/security/?p=654 (2010, December 4).