Web Browser Artefacts in Private and Portable Modes: A Forensic Investigation

Cassandra Flowers, Ali Mansour and Haider M. Al-Khateeb

Abstract - Web browsers are essential tools for accessing the Internet. Extra complexities are added to forensic investigations when recovering browsing artefacts as portable and private browsing are now common and available in popular web browsers. Browsers claim that whilst operating in private mode, no data is stored on the system. This paper investigates whether the claims of web browsers discretion are true by analysing the remnants of browsing left by the latest versions of Internet Explorer, Chrome, Firefox, and Opera when used in a private browsing session, as a portable browser, and when the former is running in private mode. Some of our key findings show how forensic analysis of the file system recovers evidence from IE while running in private mode whereas other browsers seem to maintain better user privacy. We analyse volatile memory and demonstrate how physical memory by means of dump files, hibernate and page files are the key areas where evidence from all browsers will still be recoverable despite their mode or location they run from.

Keywords - Web browser forensics; Portable applications; Private Browsing; Incognito mode; Physical Memory; Windows; IE; Chrome; Firefox; Opera; OSForensics

I. INTRODUCTION

Web browser applications are an essential tool for accessing websites via the Internet. The web browser enables users to search for information, read emails, communicate via instant messaging or social networks, use Internet banking and shop via e-commerce websites (Dharan and Meeran, 2014). Forensic artefacts left by a browser after a session include, but are not limited to cache, history, cookies, and file download lists. When conducting a digital investigation on a system, an investigator can gather evidence from such artefacts. This evidence can divulge the websites that a user visited, the time and frequency of access, and also search engine keywords that were used (Oh et al., 2011).

The Apple Safari web browser introduced a feature known as ‘Private browsing’ in 2005 which prevented the web browser from leaving traces of browsing history, temporary files, form data, usernames, passwords and cookies on a system (Satvat et al., 2014). To date, all other popular web browsers now include this feature. In Mozilla Firefox the feature is known as ‘Private Browsing’ (Mozilla Foundation, 2014). In Chrome it is known as ‘Incognito mode’ (Google, 2014). In IE it is known as ‘InPrivate

Browsing' (Microsoft, 2014). When launching these browsers in private mode they all claim to maintain user privacy by not keeping any traces of web surfing sessions such as visited websites, search history, download history, web form history, cookies, or any temporary Internet files.

Portable application versions of popular desktop software are now becoming increasingly popular allowing users' access to their favourite applications on systems that they do not have administrative rights to. These portable applications are becoming even more common due to their fast execution times and ability to run without being installed (Marrington et al., 2012). Portable applications also add an additional layer of security due to their data being stored on and accessed from the external device that they are run from. Web browsers are an example of a popular portable application. Not only does a portable web browser allow users to carry around their favourite browser and website bookmarks with them on a tiny USB stick, but it also adds the ability to surf the Internet anonymously from any device with enabled USB ports. There is therefore a requirement to analyse the impact of these new browser features on digital investigations to secure evidence. In contrast to the objective of maintaining user privacy, the perspective of digital forensics and incident response is that digital evidence is needed to identify a threat, malicious perpetrator or ascertain whether a user has actually been falsely framed to take the responsibility of breaking cyber laws and legislations. Jahankhani (2007) reviews cyber legislations and their impact on the society.

Data from W3Counter.com (2014) show the popularity of different browsers over time. Statistics show a steep decline in the number of Internet users operating Microsoft Internet Explorer (IE) from 67.6% in May 2007 to 21.2% in July 2014. Google Chrome, however, has rapidly grown in popularity from its introduction in September 2008. It now dominates the web browser market share at 38.5%. As Chrome, IE, Firefox and Opera are shown to be the most popular Windows-based browsers at present, this paper will concentrate on analysing forensic methods used for recovering evidence which may have been viewed using these browsers in both private and portable modes. The latest versions of these browsers will be used so as to provide an update to previous studies and discover whether web browsers' claims of not storing data about private browsing sessions are now true.

When web browsers are used, they store artefacts relevant to the user activity such as images in temporary locations on the hard disk while the physical memory also caches processed data to speed the functionality of the software. New file versions automatically replace existing local ones while users can configure the software to delete these temporary files once active sessions are terminated. Likewise, Cookies are special type of temporary files placed and utilised by external websites to store information about the user or his computer for future use e.g. to recall login details or user preferences (Oh et al., 2011). To store and organise browsing data, self-contained, serverless and zero configuration rational database management systems such as SQLite are utilised (Pereira, 2009). Unlike client-server models, this approach requires no standalone process, instead the library is integrated as part of the browser. Similar concept is applied in the `.dat` files used by IE, as it works as a repository of redundant information (e.g. URLs, search queries etc). IE used the `index.dat` database file until v10, then used the Extensible Strage Engine (ESE) `WebCacheV01.dat` afterwords (Chivers, 2014). These files can not be deleted easily because they are always open when Windows is running which makes them of significant value for digital investigations. File format could vary between browsers, so while data is saved as binary in `index.dat`, ASCII was used in the old `history.dat` within Firefox. Generally speaking, a URL is cached when visited, if there is no local copy of the page, new files are download and cached on the hard drive. Each file is then assigned a unique name (e.g. alphabetical value) inside the `.dat` file to the actual filename stored on the hard disk. However, the internal structure of such databases is not necessarily known (when not published by the developers as in IE) but certain facts are recovered through forensic investigations.

The remaining parts of this paper are organised as follows: Section II review existing literature. Section III details the test-bed and methodology used during the experiments and the browsing modes that will be investigated. Section IV identifies the locations that browsers in normal, private, portable and portable private modes store files when in use. Section V analyses the locations noted in section III to discover the artefacts that can be recovered after browser sessions in the various modes. Section VI discusses the findings with the conclusions stated in Section VII.

II. RELATED STUDIES

Pereira (2009) examined how SQLite databases are used in Firefox and found that records can be recovered after they have been deleted by the user because SQLite utilises unallocated disk space to support transactions. Said et al. (2011) analysed artefacts from different browsers running in private mode and demonstrated how Google Chrome is relatively more secure although evidence is still recoverable from memory. Eleutério and Eleutério (2011) took a different approach and conducted an experiment to argue that the implementation of web applications has a considerable effect on the investigator's ability to recover artefacts.

Several studies have examined the true extent of privacy that 'Private browsing' and portable browsers actually provide. Chivers (2013) examined the use of IE10's InPrivate browsing feature to discover what evidence could be recovered. He found that IE10 maintains a database of history records and cache in the `WebCacheV01.dat` file. InPrivate browsing records were stored in the same tables as normal browsing records and then removed when the browser was closed. He also found evidence in log files that were not removed until IE10 was re-opened. InPrivate browsing records were identified in `pagefile.sys` and the system volume information directory. He claimed that over 80% of evidence on browsing history was recoverable from non-database areas.

Satvat et al. (2014) examined the remains left by Firefox 19.0, Safari 5.1.7, Chrome 25.0.1364.97 and IE 10.0.9200.16521. They observed that when Firefox was cleanly closed, evidence from private browsing sessions could not be found in its database, however, if the browser was not cleanly terminated, evidence could be recovered until the browser was re-opened. The authors highlighted that evidence was leaked due to extensions being used in private mode and developed their own extensions to prove that vulnerabilities exist. The authors compared bookmarks added in private mode versus those added in normal mode and noted that it was possible to identify the usage of private mode through these records. Other useful information was contained in DNS cache artefacts left in RAM and cookie timings.

Marrington et al. (2012) conducted research to determine whether Chrome portable left similar forensic artefacts to the installed version. They compared the footprints left by both the installed version, portable version and portable version in incognito mode on a Windows XP SP3 system. During these three scenarios the authors watched YouTube videos, searched for images via Google image search and browsed for items on eBay. After examining forensic images of all scenarios, the authors identified traces of browsing history in all images. In the case of the portable sessions, however, the results were mostly found in unallocated space or the page file. They identified many results in the user's `local settings/temp` directory during the normal Chrome portable browsing session indicating that the browser was storing files on the hard disk rather than the USB stick. Evidence from the Incognito portable browsing session was only found in `pagefile.sys`. From these results, they concluded that there was no significant difference between using the installed or portable version of Chrome in normal browsing mode as both versions left evidence that could be easily recovered from the hard disk via conventional digital forensic methods.

Ohana and Shashidhar (2013) investigated the artefacts left by private and portable browsers. They studied IE, Chrome, Firefox and Safari by searching on Google and Yahoo, viewing YouTube videos, sending email with attachments via Gmail, Hotmail, Yahoo! Mail and SHSU mail, logging in to online banking, attempting to purchase ammunitions and searching for suspected stolen items on Craigslist. From these experiments they discovered that portable and private browsing do leave artefacts on systems, however, the number of artefacts left depends on the browser used. IE left the most artefacts, although not in the typical locations. With other browsers, RAM appeared to be the best place to obtain evidence. Chrome Portable proved to leave the most artefacts on the host machine.

There have also been few attempts to extract and analyse specific artefacts related to web browsers. For instance, Matsumoto and Sakurai (2014) have scoped their work on the acquisition of WebStorage data from memory dumps. WebStorage is a method used to store data in a web browser locally, it comes as part of HTML5 as a new coming alternative to cookies.

III. METHODOLOGY AND TEST-BED SETUP

A. Instruments

To investigate the artefacts that portable and private browsers left on a system, VMWare virtual machines running Windows 7 SP1 with 1GB of RAM were built. To perform browsing sessions, the latest supported major official releases of web browsers were installed: IE11.0.9600.17207, Firefox 36.0, Chrome 41.0.2272 and Opera 28. Opera Portable version 12.17 was, however, the latest portable version of the web browser available at the time of the experiment.

To determine the storage locations of the artefacts and those changed during browsing, OSForensics (PassMark, 2014) was installed. OSForensics allows for file snapshots to be captured and then compared to analyse and show which files were created, modified and deleted. FTK Imager (AccessData, 2014) was used on the host system to mount the virtual disks and take forensic images of file systems and physical memory (volatile memory). Additionally, tools such as Hex Workshop from BreakPoint Software (2014), Bulk_Extractor (Garfinkel, 2013) and Volatility from Volatility Foundation (2014) were essential to analyse and recover data from memory dumps.

B. Experiments

The VM was cloned so as to use a clean system each time and then the following tests run for the experiments. During each trial, we attempted to imitate the behaviour of end users, the web browser was used to navigate to http://www.youtube.com and watch a video, navigate to http://news.bbc.co.uk and open two news articles, navigate to http://images.google.com and search for "meerkat" then click to view two images. These actions were performed on Internet Explorer InPrivate, Firefox Private, Opera Private, Chrome Incognito, Firefox Portable, Opera Portable, Chrome Portable, Firefox Portable Private, Opera Portable Private, and Chrome Portable Incognito. Forensic images for the file system and memory were taken, and a copy of the pagefile.sys was exported, prior and after each browsing session. Further reflections on each experiment are shared with analysis provided in sections IV and V.

IV. LOCATING BROWSER ARTEFACTS

A. Locating artefacts after normal browsing

To determine a baseline for tests and discover areas to investigate for files during private and portable browsing, the tests were first run in normal browsing mode. Locations of browser artefacts were noted with any files covered in our analysis. Tables 1 to 4 show the locations of these relevant artefacts.

Table 1. Default locations of IE artefacts in Windows 7

Artefact	**Location within** `C:\Users\{user}\AppData\Local\Microsoft`
History	`…\Windows\History\`

Cache	`…\Windows\WebCache\`
	`…\Windows\Temp…Files\Content.IE5\`
	`…\Windows\Temp…Files\Low\Content.IE5\`

Recovery	`…\Internet Explorer\Recovery`
Downloads	`…\Windows\Temp… Files\Content.IE5\`
	Location within `C:\Users\{user}\AppData\`
Digital Cert.	`…LocalLow\Microsoft\CryptnetUrlCache\Content\` `…LocalLow\Microsoft\CryptnetUrlCache\MetaData\`

Cookies	`…\Roaming\Microsoft\Windows\Cookies\`
	`…\LocalLow\Microsoft\Internet Explorer\DOMStore\`

Bookmarks	`C:\Users\{user}\Favorites`

Table 2. Default locations of Firefox artefacts in Windows 7

Artefact	
	Location within `C:\Users\{user}\AppData\Local\Mozilla\Firefox\Profiles`

Cache	`…\<randomtext>.default\Cache`
	`…\<randomtext>.default\jumpListCache`

	Location within `C:\Users\{user}\AppData\Roaming\Mozilla\Firefox\Profiles`

Cookies	…\ngn1mdm2.default\cookies.sqlite
History & Bookmarks	…\<randomtext>.default\places.sqlite
Digital Cert.	…\<randomtext>.default\cert8.db
Session Store	…\<randomtext>.default
Downloads	…\<randomtext>.default\downloads.sqlite

Table 3. Default locations of Chrome artefacts in Windows 7

Type of File	**Location within** C:\Users\{user}\AppData\Local\Google\Chrome\User Data\Default
History	…\History …\History-journal
Cookies	…\Cookies …\Cookies-journal
Cache	…\Cache\; …\Favicons; …\Favicons-journal
Login Passwords	…\Web Data; …\Web Data-journal
Bookmarks	…\Bookmarks

Table 4. Default locations of Opera artefacts in Windows 7

Artefact	**Location within** C:\Users\{user}\AppData
Main data directory	…\Roaming\Opera\Opera\
Cache	…\Local\Opera\Opera\cache\

B. Locating artefacts during and after private browsing

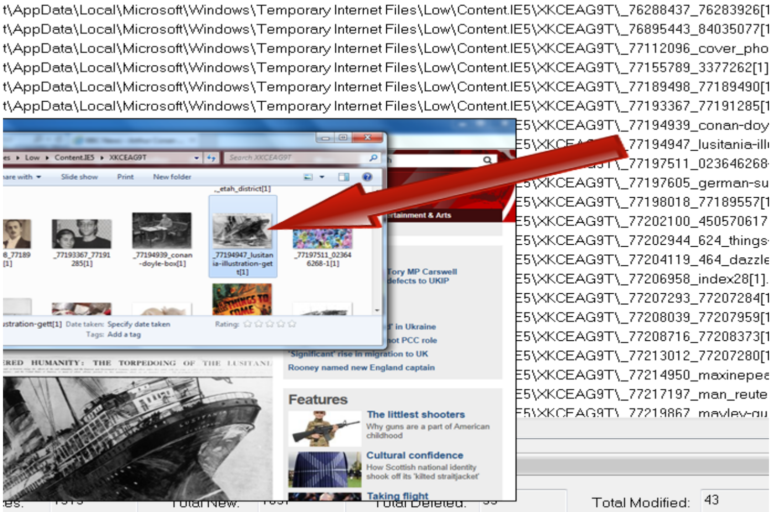
Each browser was tested during private browsing. The locations noted in section A were monitored to capture potential artefact locations.

IE 11

During private browsing, IE created .dat files in the Recovery directory like during normal browsing mode in order to give users the ability to recover sessions after crashes. It also heavily utilised the Low\Content.IE5\ directory to cache files during InPrivate browsing.

Existing .log files in the WebCache folder were removed and new logs created in the same directory for the current session. In private mode, the browser still utilised the CryptnetUrlCache\Content\ directory to store certificates. When the browser was then closed, IE performed a clean-up task. It removed the files in the Recovery directory and deleted files it had cached at Low\Content.IE5\. Some of the WebCache log files were deleted, but not all, which left V0100010.log through to V0100017.log available for further analysis along with WebCacheV01.dat and V01.log. These files are not removed until IE is re-opened.

Figure 1 shows the files stored on the hard drive during IE InPrivate mode. These files can be matched to the websites being visited.



```
t\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\XKCEAG9T\_76288437_76283926[1
t\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\XKCEAG9T\_76895443_84035077[1
t\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\XKCEAG9T\_77112096_cover_pho
t\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\XKCEAG9T\_77155789_3377262[1]
t\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\XKCEAG9T\_77189498_77189490[1
t\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\XKCEAG9T\_77193367_77191285[1
E5\XKCEAG9T\_77194939_conan-doy
E5\XKC      _77194947_lusitania-ill
         T\_77197511_023646268
E5\XKCEAG9T\_77197605_german-su
E5\XKCEAG9T\_77198018_77189557[1
E5\XKCEAG9T\_77202100_450570617
E5\XKCEAG9T\_77202944_624_things
E5\XKCEAG9T\_77204119_464_dazzle
E5\XKCEAG9T\_77206958_index28[1].
E5\XKCEAG9T\_77207293_77207284[1
E5\XKCEAG9T\_77208039_77207959[1
E5\XKCEAG9T\_77208716_77208373[1
E5\XKCEAG9T\_77213012_77207280[1
E5\XKCEAG9T\_77214950_maxinepea
E5\XKCEAG9T\_77217197_man_reute
E5\XKCEAG9T\_77219867_mayley-gu
```

Total Modified: 43

Low ▸ Content.IE5 ▸ XKCEAG9T
Search XKCEAG9T
Share with
Slide show
Print
New folder
_etah_district[1]
_77193367_77191285[1]
_77194939_conan-doyle-box[1]
_77194947_lusitania-illustration-gett[1]
_77197511_023646268-1[1]
Date taken: Specify date taken
Tags: Add a tag
Rating:
Entertainment & Arts
Tory MP Carswell defects to UKIP
'Significant' rise in migration to UK
Rooney named new England captain
Features
The littlest shooters
Why guns are a part of American childhood
Cultural confidence
How Scottish national identity shook off its 'kilted straitjacket'
Taking flight
Total New:
Total Deleted:

Figure 1. Comparing snapshots taken when IE was open and closed shows that files cached were deleted when IE restarted. However, investigation also shows that files are stored on the hard drive during IE InPrivate mode. These files can be matched to the websites being visited.

Firefox

During private browsing, there was very little hard drive activity from Firefox. Files were not cached, however, Firefox did store `.sqlite-wal` (Write Ahead Logging files for the SQLite databases) on the hard drive. Once Firefox was closed, a clean-up operation was observed. The `.sqlite-wal` and `.sqlite-shm` files were deleted from the drive and `.sqlite` files were modified. `_CACHE_001_`, `_CACHE_002_`, `_CACHE_003_`, and `_CACHE_MAP_` were then modified. These files contain information to manage the Firefox cache and hold metadata (Ritchie, 2014).

Chrome

While using Chrome Incognito browsing there was a considerable amount of hard drive activity, however, very little of this was for cached files. The majority of this activity was in the extensions directory related to default Chrome extensions;
…`\AppData\Local\Google\Chrome\User_Data\Default\Extensions`

There were many other files created and modified under the `User Data` folder including Chrome database files.

Opera

There was very little hard drive activity whilst Opera was used in private mode. In the directory located in
…`\Roaming\Opera Software\Opera Stable\`
The database file `Visited Links` was modified as was `Preferences` and `History`. `data_0` and `data_1` were also modified, located in
…`\Local\Opera Software\Opera Stable\Cache\`

C. Locating artefacts during and after browsing in portable browsers

Firefox

Firefox portable did not store files on the hard drive whilst in use. Instead, all `sqlite` databases and other files were stored on the USB stick at `\FirefoxPortable\Data\profile\`. By default, the cache in Firefox portable is set to 0MB therefore no cache files are created. If it were enabled, Firefox Portable would store the files at `\FirefoxPortable\Data\profile\` and not on the hard drive.

Chrome

Google Chrome portable stored cache files on the hard drive rather than the USB stick. At `C:\Users\{user}\AppData\Local\Temp\` a folder named `GoogleChromePortable` was created with the cache folder inside populated with the files whilst Chrome portable was in use.

These files were still in place when Chrome Portable was closed, but removed when the USB stick was ejected. Other common Chrome browser files (e.g. Database files) were not found on the hard drive, but on the USB stick instead.

Opera

Opera portable didn’t use the hard disk to store files. The USB stick that it was running from showed considerable file activity. Cache folders and databases were held on the USB stick at `\OperaPortable\Data\Profile`.

D. Locating artefacts during and after private browsing in portable browsers

Firefox

The portable version of Firefox stored very few artefacts on the hard disk during private browsing. Instead, it used the USB stick to store `sqlite` databases and other files. There are considerably fewer files created when in portable private browsing in comparison with portable normal browsing.

Chrome

In portable Incognito mode, Chrome did not store files on the hard disk, unlike when used in normal mode. There were also very few files stored on the USB stick.

Opera

In portable private mode, Opera did not utilise the hard disk to store files. Instead the USB stick was heavily utilised to store files related to the browsing session. Once the web browser is closed, however, a clean-up job appears to run which deleted and modified files that were written while the browser was in use.

V. RECOVERING EVIDENCE OF BROWSING HISTORY FROM ARTEFACTS

The artefacts gathered in Section IV were analysed and examined for activity of the known browser history in each session. There were several notable artefacts discovered in the forensic images of user profiles that we discuss and analyse further.

A. Notable Artefacts

IE Web cache directory

Until version 10, IE used the `index.dat` database file as a repository for history, cookies and temporary files (Satvat et al., 2014). From version 10 an ESE (Extensible Storage Engine) database, `WebCacheV01.dat`, is used to maintain history, cache and cookies (Chivers, 2013). This directory also contains the files V01.log (Transaction log file), `V01.chk` (checkpoint file), and `V01xxxx.log`.

Whilst the operating system is in use it is not possible to copy `WebCacheV01.dat`. In the …`\AppData\Local\Microsoft\Windows\` folder the `WebCacheLock.dat` file resides, indicating that the database is locked. After a forensic image is taken, the contents of `WebCache` can be analysed further.

The `esentutl.exe` tool, built into Windows, provides utilities for ESE databases, such as `WebCacheV01.dat`. According to Chivers (2013), when copied from a system, this file will most often be marked as dirty, i.e. requiring that the logs be flushed to the database. The `esentutl.exe` provides a command to check the state of a `WebCacheV01.dat` file:

```
> esentutl /mh WebCacheV01.dat
```

Running this on the file extracted after the IE11 private browsing session shows a dirty shutdown state. To flush the log files extracted with the database, `esentutl.exe` provides a recovery command to flush the log files in the current directory to the database:

```
> esentutl /r V01 /d
```

When the database state is checked again, it shows as being clean. This places the file in a state ready for analysis.

$I30 Files

On NTFS file systems, folder and directory information is stored separately from file `inode` data. The `$I30` files store this information (Philipp, et al., 2010). Even if the original files have been moved or deleted, the `$I30` file may still contain entries which reveal file names and access times. INDXParse.py (Ballenthin, 2014) is a Python script created to extract data from `$I30` files to a `csv` file.

B. Internet Explorer 11 in InPrivate browsing mode

Artefacts for analysis after IE11 was tested in InPrivate browsing mode were: A memory dump, `pagefile.sys`, a forensic image of the user profile, the `webcache` folder and `$I30` files in the `webcache` and `Content.IE5/Low` folders.

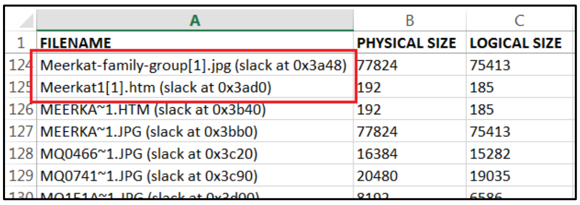
IE11 Webcache

After `WebCacheV01.dat` was placed in a clean state using `esentutl.ese` it was opened in a Hex editor and searched for evidence of the private web browsing session. Evidence of the top level domains visited during InPrivate browsing could be located in the database, however, search terms were not. Evidence of bbc.co.uk, google.com and youtube.com were all found.

$I30 files

On examining the `\Content.IE5\` folder from the image taken of the user profile, a `$I30` file of more than zero bytes was found in two of the cache folders: `JHNO3QUG` and `XKCEAG9T`.

Evidence in these files showed timestamps of web browsing and some filenames of the files created during the browsing session. The extract of the `$I30` file from the `JHNO3QUG` cache folder revealed the files that were returned during the Google image search. The word meerkat was detected twice in filenames as shown in Figure 2.



	A	B	C
1	FILENAME	PHYSICAL SIZE	LOGICAL SIZE
124	Meerkat-family-group[1].jpg (slack at 0x3a48)	77824	75413
125	Meerkat1[1].htm (slack at 0x3ad0)	192	185
126	MEERKA~1.HTM (slack at 0x3b40)	192	185
127	MEERKA~1.JPG (slack at 0x3bb0)	77824	75413
128	MQ0466~1.JPG (slack at 0x3c20)	16384	15282
129	MQ0741~1.JPG (slack at 0x3c90)	20480	19035
130	MQ1F1A~1.JPG (slack at 0x3d00)	8192	6586

Figure 2. $I30 files in the IE cache folders reveal filenames to help identify search history after the cache was cleared.

Page file and Memory Dump

Both `pagefile.sys` and a live memory dump were taken from the system after IE was closed. `Pagefile.sys` showed no evidence, however, this would have partially been due to the system having a large amount of RAM available and not swapping to the page file.

The less common searches of meerkat and bbc.co.uk were found many times throughout memory showing that it is possible to find private search history in live memory. With URL matches for bbc.co.uk there was also HTML for the pages that had been viewed making it possible to further analyse the actual pages that had been accessed.

User profile Deleted files

The ‘Deleted Files’ function of OSForensics was used to automatically detect and display the deleted files which were automatically discovered in the forensic image of the user profile. Several images of Meerkats were discovered.

C. Mozilla Firefox in private browsing mode

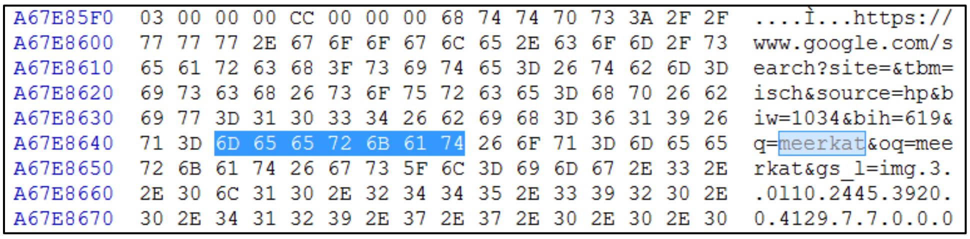
Artefacts for analysis after Firefox was tested in private mode were `\CACHE\_CACHE_001_`, `_CACHE_002_`, `_CACHE_003_`, `_CACHE_MAP_`, `pagefile.sys` and the live memory dump.

Firefox stored very little on disk whilst in private mode. The only remnants were the `_cache_map_` files. These were parsed using Firefox Cache Forensics parser (Ritchie, 2014). The only website that this showed data for was `http://clients1.google.com/ocsp`.

`Pagefile.sys` and the memory dump were scanned for the search terms. *meerkat* was detected in four places, however, *bbc.co.uk* was not. *Youtube* and *google.com* were detected many times.

D. Google Chrome in incognito browsing mode

Artefacts for analysis after using Chrome Incognito mode revealed no artefacts on the system hard drive. Therefore only the live memory dump and `pagefile.sys` were available for analysis. Live memory provided many matches when searched as shown in Figure 3.



```
A67E85F0  03 00 00 00 CC 00 00 00 68 74 74 70 73 3A 2F 2F  ....Ì...https://
A67E8600  77 77 77 2E 67 6F 6F 67 6C 65 2E 63 6F 6D 2F 73  www.google.com/s
A67E8610  65 61 72 63 68 3F 73 69 74 65 3D 26 74 62 6D 3D  earch?site=&tbm=
A67E8620  69 73 63 68 26 73 6F 75 72 63 65 3D 68 70 26 62  isch&source=hp&b
A67E8630  69 77 3D 31 30 33 34 26 62 69 68 3D 36 31 39 26  iw=1034&bih=619&
A67E8640  71 3D 6D 65 65 72 6B 61 74 26 6F 71 3D 6D 65 65  q=meerkat&oq=mee
A67E8650  72 6B 61 74 26 67 73 5F 6C 3D 69 6D 67 2E 33 2E  rkat&gs_l=img.3.
A67E8660  2E 30 6C 31 30 2E 32 34 34 35 2E 33 39 32 30 2E  .0l10.2445.3920.
A67E8670  30 2E 34 31 32 39 2E 37 2E 37 2E 30 2E 30 2E 30  0.4129.7.7.0.0.0
```

Figure 3. After Chrome was used in Incognito mode, many artefacts could be detected in the memory dump

E. Opera in private browsing mode

Although there was some hard disk activity when Opera was used in private browsing mode, the files examined contained no evidence of the browsing session. Live memory contained evidence of the browsing.

Artefacts extracted from these different browsers running in private mode are compared in Table 5.

Table 5. Useful artefacts located from different browsers running in private mode

Browser	Search Term	Cache	Other Artefacts	Pagefile	Live Memory	Profile/ Deleted files	Artefacts Showing Results
IE11	meerkat	0	2	0	23	11	*Memory dump, WebCacheV01.dat + logs, $I30 in cache folders, Deleted files in cache folders*
	youtube	30	0	10	100+	0	
	bbc.co.uk	3	0	0	92	0	
	google.com/search	0	0	0	0	0	
	google.com	11	0	66+	100+	0	
Firefox	meerkat	0	0	0	4	0	*Memory dump*
	youtube	0	0	10	67	0	
	bbc.co.uk	0	0	0	0	0	
	google.com/search	0	0	0	6	0	
	google.com	0	0	100+	100+	0	
Chrome	meerkat	0	0	0	3	0	*Memory dump*
	youtube	0	0	10	100+	0	
	bbc.co.uk	0	0	0	87	0	
	google.com/search	0	0	0	22	0	
	google.com	0	0	100+	100+	0	
Opera	meerkat	0	0	0	3	0	*Memory dump*
	youtube	0	0	2	17	0	
	bbc.co.uk	0	0	0	57	0	
	google.com/search	0	0	0	1	0	
	google.com	0	0	100+	100+	0	

F. Mozilla Firefox portable in normal browsing mode

Although there is very little evidence available on the hard drive after browsing in normal mode on portable Firefox, many files were created on the USB stick that it was run from: `cert8.db`, `places.sqlite`, `jumpListCache content-prefs.sqlite`, `healthreport.sqlite`, `permissions.sqlite`, `webappsstore.sqlite`, `cookies.sqlite`, folder and `thumbnails` folder.
These were available for analysis along with `pagefile.sys` and the live memory dump.

The `cookies.sqlite` file reveals some useful information about sites that were visited in a portable browsing session. *Youtube.com*, *google.com* and *bbc.co.uk* all had cookies stored for them. *Nationalgeographic.com* and *scorecardresearch.com* were not visited, however, were recorded in the `moz_cookies` table, presumably because one of the other sites linked to them. `permissions.sqlite` showed an entry for the ssl settings for *ssl.bbc.co.uk*. Analysis of `places.sqlite` showed several entries of sites visited across the different tables with the `moz_places` table holding the most data including the URL and title of the page that had been visited. Image artefacts were found in the `jumpListCache` as well as the `thumbnails` folder which could be matched to browsing history.

G. Chrome portable in normal browsing mode

Chrome utilised the `/Local/Temp/GoogleChromePortable` folder for storing cache, however, files were removed once the USB stick was removed. The USB stick held many artefacts related to the portable browsing session under the `GoogleChromePortable/Data/Profile` folder. The history database file held the URLs of sites that were visited in the `segments` and `urls` tables. Like with the `moz_places` table in Firefox's `places.sqlite` database, the full URL and titles could be located. Artefacts were also found in the `omni_box_shortcuts` table of the shortcuts database and the cookies table of the cookies database.

H. Opera portable in normal browsing mode

After normal browsing using Opera portable, no relevant files were discovered on the hard disk, however, several files placed on the USB stick during normal browsing using Opera Portable contained evidence of browsing history. The vps (Visited Pages Search) files contained in the `OperaPortable\Data\profile\vps\0000` directory. The `OperaPortable\Data\Sessions` directory contained autosave and temporary data of preferences for the sessions. These files include sections labelled 'history url' and 'history title' which store URLs visited in the sessions. Data was also located in the `opssl6.dat` certificate store, `typed_history.xml` file, `cookies4.dat` file and `global_history.dat` file. A considerable amount of evidence of websites visited during the browsing session was obtained from these files.

Table 6 compares artefacts founds from the different portable browsers running in normal mode.

Table 6. Useful artefacts located from different portable browsers running in normal mode. The asterisk (*) indicates that artefacts were found on the USB stick, not hard drive.

Browser	**Search Term**	**Cache**	**Other Artefacts**	**Pagefile**	**Live Memory**	**Profile/ Deleted files**	**Artefacts Showing Results**
Firefox	meerkat	0	0	0	46	11*	*Memory dump, cookies.sqlite*, permissions.sqlite*, places.sqlite*, Thumbnails folder*, jumpListCache folder**
	youtube	0	0	5	23	8*	
	bbc.co.uk	0	0	0	250	19*	
	google.com/search	0	0	0	9	11*	
	google.com	0	0	100+	80	28*	
Chrome	meerkat	0	0	0	55	7*	*Memory dump, history*, shortcuts*, cookies**
	youtube	0	0	4	100+	9*	
	bbc.co.uk	0	0	0	161	13*	
	google.com/search	0	0	0	0	7*	
	google.com	0	0	100+	100+	15*	
Opera	meerkat	0	0	0	200+	39*	*Memory dump, md.dat*, autosave.win*, opr91C3/tmp*, opr773D.tmp*, global_history.dat*, cookies4.dat*, opssl6.dat*, typed_history.xml**
	youtube	0	0	3	100+	36*	
	bbc.co.uk	0	0	0	200+	17*	
	google.com/search	0	0	0	54	7	
	google.com	0	0	100+	200+	23*	

I. Firefox portable in private browsing mode

After the Firefox portable private browsing, no artefacts remained on the USB stick or the hard disk. The only evidence found was in the `moz_cookies` table of the cookies database, however, it is likely that as this entry is for *google.com* the entry was created by default. The live memory dump, however, did reveal evidence of search history.

J. Chrome portable in incognito browsing mode

Chrome portable incognito browsing did not leave artefacts on the USB stick or hard disk. The only match for the browsing history was the URL: *http://www.google.com/favicon.ico* in the favicons table of the favicons database. This is possibly because this is a default homepage rather than a link to browsing history. Again, the live memory dump provided matches for all browser history.

K. Opera portable in private browsing mode

Only one artefact was recovered from the USB stick that Opera portable was run from in private mode, `opssl6.dat`. This certificate store listed `ssl.bbc.co.uk`. Additional evidence of the browsing session was only found in the live memory dump.

Table 7 compares artefacts founds from the different portable browsers running in private mode.

Table 7. Useful artefacts located from different portable browsers running in private mode. The asterisk (*) indicates that artefacts were found on the USB stick, not hard drive.

Browser	Search Term	Cache	Other Artefacts	Pagefile	Live Memory	Profile/ Deleted files	Artefacts Showing Results
Firefox	meerkat	0	0	0	0	0	*Memory dump, cookies.sqlite**
	youtube	0	0	5	41	0	
	bbc.co.uk	0	0	0	118	0	
	google.com/search	0	0	0	0	0	
	google.com	0	0	100+	100+	1*	
Chrome	meerkat	0	0	0	54	0	*Memory dump, favicons**
	youtube	0	0	5	100+	0	
	bbc.co.uk	0	0	0	39	0	
	google.com/search	0	0	0	32	0	
	google.com	0	0	100+	100+	2*	
Opera	meerkat	0	0	0	2	0	*Memory dump, opssl6.dat**
	youtube	0	0	2	100+	0	
	bbc.co.uk	0	0	0	14	1	
	google.com/search	0	0	0	1	0	
	google.com	0	0	100+	100+	0	

VI. DISCUSSION

The results show that evidence was still recoverable during portable and private browsing sessions, although the amount of evidence varied depending on the browser used. Even during InPrivate browsing, IE left a considerable number of artefacts on the hard drive in the same locations used during normal browsing. Using forensic techniques it was possible to recover cache files that the browser had deleted. The `WebCacheV01.dat` file was recoverable from the hard drive, as long as IE had not been re-opened. Therefore, it is possible for artefacts from the previous web browsing session to be recovered from this file during a forensic investigation, however, older evidence may not be obtainable. Evidence of cached file names was recoverable from `$I30` files in cache folders during forensic recovery as well.

Chrome portable stored cache files on the hard disk during normal browsing rather than on the USB stick that it was run from. Although in these experiments it was not possible to recover these files after they had been deleted, they may be recoverable in other circumstances. Unlike Chrome portable, Firefox portable and Opera portabledid not store any files on the hard disk so artefacts could not be recovered. In private browsing modes, both Firefox, Chrome, and Opera Portable did not store any artefacts on the hard drive.

Windows terminology labels the different parts of memory as available, free or cached. It is the cached space that is most relevant to us because this is where data for the most recently accessed files reside. To boost performance, application cached data will remain even after they are closed which explains the wealth of evidence recovered from the live memory dumps in each of our experiments. Further, Evidence was not recoverable from `pagefile.sys` in any of the scenarios. It can be argued that the reason is the relatively large RAM size installed in the host machine if compared to the short web browsing session; when the physical memory is exhausted, Windows compensates by virtually extending RAM space into the hard drive to create what is known as virtual memory, or a paging file, and moves inactive (but still needed) data to `pagefile.sys`. However, another reason as to why the value of the pagefile was very limited is that Windows, for security reasons, splits files moved from RAM to the page file into small chunks of data that can only be readable if mapped back in the right order to reconstruct the former state. (Al-Khateeb, 2014)

Nevertheless, memory dumps showed some false (or irrelevant) evidence too. *Youtube.com* and *google.com* were found to appear over 100 times in most memory dumps. They were often found listed with other popular search engines or websites indicating that these results were populated from elsewhere such as default browser search URLs.

VII. CONCLUSIONS

From the results, the live memory dump held the most evidence of artefacts created during private and portable browsing sessions. Unfortunately capturing a live memory dump is not always possible when evidence is being recovered from a scene. It is also possible that doing so could alter original data and affect the forensic value of artefacts. The tests performed in these scenarios included far shorter browsing sessions than would be recovered from a system under daily use. Therefore, some of the evidence found in live memory is possibly recoverable from `pagefile.sys` or `hiberfile.sys` even if systems have been shut down. When a virtual environment is used, users can take snapshots of the running state of the system or suspend the active session and save everything including physical memory to a file, usually to one of the following formats:

.vmem or .vmss, these files are increasingly becoming a very rich resource to extract artefacts during digital investigations.

If suspects have been using IE InPrivate browsing mode in the hope of hiding browser activities, the results from tests have shown that the artefacts IE leaves on hard drives can lead to the sites and search terms which have been used. $I30 was a particularly useful file which had not been mentioned in previous studies on portable and private browser forensics and should be considered as an artefact which may contain evidence for browsers that were identified to store files on the hard drive during usage (Chrome Portable and IE InPrivate browsing). Firefox Portable, Chrome Portable Incognito, Opera Portable Private, and Firefox Portable Private browsing modes stored no artefacts on the system hard disk. With Firefox Portable, Chrome Portable and Opera portable normal browsing, many artefacts could be recovered from the USB stick. This demonstrates how important it is for forensic investigators to recover all devices from a scene, particularly as the USB stick may contain the sqlite databases containing detailed evidence of browsing history.

These tests have also shown that by default some web browsers leave URLs in their databases and in live memory when run before any browsing activity has occurred. In these tests, results for *google.com* and *youtube.com* were particularly prominent. Forensic investigators will therefore need to be extra vigilant when analysing browser artefacts to ensure that evidence was not placed by the browser.

The results outlined in this work show that evidence of web browsing sessions is recoverable from all systems regardless of whether portable or private browsing modes are in use in the most recent versions of Chrome, Firefox, Opera and IE. In all scenarios, artefacts were recoverable. Web browser claims that browsing history will not be recoverable in private modes may prevent an average computer user from finding evidence, but using forensic techniques plenty of evidence was recoverable which may prove to be crucial to a forensic investigation. It is also crucial for Internet users to learn that browsers security does not make them anonymous when their network is monitored by an Internet Service provider or a Network Administrator at the workplace. Similarly, spyware and key loggers can also violate their privacy if any of these malicious software is installed on their client machines.

REFERENCES

Access Data (2014) FTK Imager (Version 3.2.0) [Computer Program]. Available from http://www.accessdata.com/support/product-downloads (Accessed 1st Mar 2015)

Al-Khateeb, H. M. (2014) ‘Recovering User Passwords From Memory’, Digital Forensics Magazine, 2014(20): 8-12.

Ballenthin, W. (2014) INDXParse.py (Version 1.1.8) [Computer Program]. Available from https://github.com/williballenthin/INDXParse (Accessed: 1st Mar 2015).

BreakPoint Software (2014), Hex Workshop (Version 6.7.3) [Computer Program]. Available from http://www.hexworkshop.com/ (Accessed: 1st Mar 2015)

Chivers, H. (2014) ‘Private browsing: A window of forensic opportunity’, Digital Investigation, 11(1), pp. 20-29 [Online].

Dharan, G. D. and Meeran, A. R. (2014) ‘Forensic Evidence Collection by Reconstruction of Artefacts in Portable Web Browser’, International Journal of

Computer Applications, 91(4) [Online]. Available at: http://research.ijcaonline.org/volume91/number4/pxc3894862.pdf (Accessed: 1st Mar 2015).

Eleutério, P. M., & Eleutério, J. D. A. S. (2011) 'Webmail evidence recovery: a comparison among the most used Web browsers and webmail services'. ICoFCS 2011, 182-189.

Garfinkel, S. L. (2013). Digital media triage with bulk data analysis and bulk_extractor. Computers & Security, 32, 56-72.

Google (2014) 'Browse in private (incognito mode)'. Available at: https://support.google.com/chrome/answer/95464?hl=en-GB (Accessed: 1st Mar 2015).

Jaha nkhani, H. (2007) 'Evaluation of cyber legislations: trading in the global cyber village'. International Journal of Electronic Security and Digital Forensics,1(1), 1-11.Marrington, A., Baggili, I., Ismail, T. and Kaf, A. (2012) 'Portable web browser forensics: A forensic examination of the privacy benefits of portable web browsers', 2012 International Conference On Computer Systems & Industrial Informatics, p. 1 EBSCOhost [Online].

Matsumoto, S., and Sakurai, K. (2014) 'Acquisition of Evidence of Web Storage in HTML5 Web Browsers from Memory Image' In Information Security (ASIA JCIS), 2014 Ninth Asia Joint Conference on (pp. 148-155). IEEE.

Microsoft Windows (2014) 'InPrivate Browsing'. Available at: http://windows.microsoft.com/en-GB/internet-explorer/products/ie-9/features/in-private (Accessed: 1st Mar 2015).

Mozilla Foundation (2014) 'Private Browsing - Browse the web without saving information about the sites you visit'. Available at: https://support.mozilla.org/en-US/kb/private-browsing-browse-web-without-saving-info (Accessed: 1st Mar 2015).

Said, H., Al Mutawa, N., Al Awadhi, I., & Guimaraes, M. (2011) 'Forensic analysis of private browsing artifacts'. In Innovations in information technology (IIT), 2011 International conference on (pp. 197-202). IEEE.

Oh, J., Lee, S. and Lee, S. (2011) 'Advanced evidence collection and analysis of web browser activity', Digital Investigation, 8, pp. S62-S70 EBSCOhost [Online].

Ohana, D. and Shashidhar, N. (2013) 'Do private and portable web browsers leave incriminating evidence?: A forensic analysis of residual artefacts from private and portable web browsing sessions', EURASIP Journal On Information Security, 1(1) EBSCOhost [Online].

Passmark (2014), OSForensics (Version 3.0) [Computer Program]. Available from http://www.osforensics.com/osforensics.html (Accessed: 1st Mar 2015)

Philipp, A., Cowen, D., and Davis, C. (2010) 'Hacking Exposed: Computer Forensics'. New York; London: McGraw-Hill.

Pereira, M. T. (2009) 'Forensic analysis of the Firefox 3 Internet history and recovery of deleted SQLite records'. Digital Investigation, 5(3), 93-103.

Ritchie, J. (2014), 'Firefox Cache Find (Version 0.3)' [Computer Program]. Available at: https://code.google.com/p/firefox-cache-forensics/downloads/detail?name=ff_cache_find_0.3.pl (Accessed: 1st Mar 2015).

Satvat, K., Forshaw, M., Hao, F. and Toreini, E. (2014), 'On the Privacy of Private Browsing - A Forensic Approach', Journal of Information Security and Applications, 19, pp. 88-100. Available at: http://homepages.cs.ncl.ac.uk/m.j.forshaw1/privatebrowsing/artefacts/DPM13.pdf (Accessed: 1st Mar 2015).

Volatility Foundation (2014), Volatility (Version 2.4) [Computer Program]. Available from http://www.volatilityfoundation.org/#!24/c12wa (Accessed: 1st Mar 2015)

W3Counter (2014) ‘July 2014 Web Browser Market Share’. Available at: http://www.w3counter.com/globalstats.php?year=2014&month=7 (Accessed: 1st Mar 2015).