Forensics Evaluation of Privacy of Portable Web Browsers

Ahmad Ghafarian
Department of Computer Science
and Information Systems
University of North Georgia
Dahlonega, GA 30005, USA

Seyed Amin Hosseini Seno
Department of Computer Engineering
Faculty of Engineering
Ferdowsi University of Mashhad
Mashhad, Iran

ABSTRACT
Browsers claim private mode browsing saves no data on the host machine. Most popular web browsers also offer portable versions of their browsers which can be launched from a removable device. When the removable device is removed, it is claimed that traces of browsing activities will be deleted and consequently private portable browsers offer better privacy. This makes the task of computer forensics investigators who try to reconstruct the past browsing history, in case of any computer incidence, more challenging. However, whether or not all data is deleted beyond forensic recovery is a moot point. This research examines privacy of popular private portable browsers, including Firefox, Chrome, Safari, and Opera through both static and volatile memory forensics. In static memory, we examine the content of registry, recent, cache, cookies and temp files. In volatile memory forensics, we analyze the content of live memory. Results of this experiment show that traces of web browsing activities can be found, even after removing the portable browser device.

General Terms
Computer forensics, portable browser, private browsing mode

Keywords
Computer forensics tools, RAM forensics, volatile memory, artifacts, registry and private.

1. INTRODUCTION
When we surf the web, browsers save information about our surfing activities in various locations. In an attempt to maintain the privacy of users, most popular web browsers offer a private mode browsing which is claimed to not save any traces of browsing activities. Most popular web browsers, including Mozilla Firefox, Google Chrome, Opera and Apple Safari also offer portable browsers which can be launched from a removable device. When the removable device is removed, it is believed that traces of browsing activities will be deleted and consequently private portable browsers offer even better privacy. However, whether or not all data is deleted beyond forensic recovery is a moot point.

Generally, web browsers save traces of browsing activities on the portable browser device, server and various places on the host machine [1]. The local machine saves browsing data in both static media such as hard drive as well as random access memory (RAM), also known as volatile memory [2]. The data contained within the two types of sources varies significantly. Static media are primarily used for long term storage and contain data such as executables, images, documents and browser history. On the other hand, physical memory is a temporary working space for data that are being used by the system. The major difference between the data sources in relation to a computer forensic investigation is that the latter is a less tangible source of evidence [3].

A study of tools and techniques for memory forensics can be found in [4]. The author has evaluated several command line and graphical user interface tools and provide the steps needed for memory forensics. Retrieving portable browsing forensics artifacts left behind from main memory have recently attracted some attention [5, 6]. The authors used limited memory forensics to retrieve forensics artifacts left after a private portable browsing session. They argue that memory forensics is very promising in establishing a link between the suspect and the retrieved data.

When we are dealing with portable browsing artifacts, memory forensics would be challenging. This is because once the portable browser device is ejected from the suspect machine; the portable browser-related data content in the main memory will gradually disappear. Different browsers handle this differently. Some browsers like Firefox replace the data with zeroes. Others delete them.

This research examines privacy of the popular private portable web browsers through both static memory and volatile memory forensics. For RAM forensics, we capture live memory after a browsing session and then analyze the captured memory looking for forensics artifacts in memory. For static memory forensics, we examine host computer log files such as registry, cache, cookies, temporary files and recent files. The experiment is carried out in both cases, by removing the portable browser device from the machine and leaving it attached to the machine. The results show that with a combination of static and volatile memory forensics we can retrieve forensically valuable information due to a private portable browsing.

The remainder of this paper is organized as follows: Section 2 gives background, section 3 research methodology, results appear in section 4, section 5 covers conclusion, and future research is shown in section 6, acknowledgement and references given in section 7 and 8 respectively.

2. BACKGROUND
In this section, we first review the browser's claim of privacy of portable web browser. Subsequently, we review the existing research on the privacy of private portable web browsers.

2.1 Browser's Claim of Privacy
Below is the privacy claim of the portable browsers that we have used in our experiment.

Portable Mozilla Firefox [7] statement of privacy: "Private Browsing allows you to browse the Internet without saving any information about which sites and pages you've visited".

Google Chrome Portable [8] statement of privacy: "Passwords Not Saved Between PCs By Default, Certificates Not Portable, Some Settings Locked Per PC: Note that other portable browsers such as Mozilla Firefox, Portable Edition do not have any of the issues mentioned above."

The privacy features of Opera Portable [9]: "No traces left after exiting - files are overwritten, not just deleted. Doesn't make your USB drive tired - all program files and data are stored in a temporary place on the host computer. Create multiple profiles for use in different situations."

The privacy feature of portable Safar [10]: "Safari's security features also make surfing more secure, protecting your privacy. Safari stops keeping track of your web history, and storing your searches, cookies, and the data in any online forms you fill out. Greater control can be found in Safari's preferences."

2.2 Related Research

Report on the privacy of Google Chrome portable browser using static media forensics appears in [11]. The authors indicate that portable Google Chrome does leave traces of browsing activities on the hard drive, but the details are not clear in their paper. Another study of the privacy of Google Chrome portable appears in [12]. The researchers examined the content of the *IconCache.db* database, Windows registry and RAM and found evidence of portable browsing activities. However, the authors provided no details of the memory forensics process. It is worth to notice that in their experiment, the portable flash drive was still attached to the suspect machine, but is not clear whether the web browsers were still open or closed after a browsing session.

In another study [13], the authors experimented with portable Internet Explorer, Firefox, Opera, and Google Chrome. The researchers performed memory dump and analyzed the dumped file with hexadecimal editor. Similar to the previous research, the portable browser device was still connected to the machine during their experiment. There is no statement to indicate the establishment of a link between retrieved forensics artifacts and the suspect.

Retrieving forensics artifacts from Windows registry keys and *prefetch* files due portable browsing activities can also be found in [14]. The researchers performed both live and offline forensics and reported evidence of portable web browsing activities in both cases. However, their experiment description is very fuzzy and they did not disclose the portable browser they experimented with.

The authors in [6], along with other forensics investigation methods, performed memory forensics with three portable web browsers, namely Mozilla Firefox portable, Google Chrome portable and Opera portable. They conclude that the best way to recover residual data is to obtain the evidence from RAM. However, it is not clear whether during the memory capture the portable flash drive was connected to the suspect machine or not. They also did not disclose details of memory forensics, including the tools and methodologies used.

Other researchers, including [15, 16, 17] used memory forensics to retrieve forensics artifacts when standard private browsers were used. However, since their experiment was performed in a controlled research setting environment, their result cannot be replicated. A theoretical discussion of RAM forensics tools, techniques and guidelines can be found in [3, 18, 19]. The authors discuss the way physical memory works in Windows and Linux operating systems as well as the types of forensically valuable data that can be extracted from physical memory.

3. RESEARCH METHODOLOGIES

In this section we list the hardware and software tools and the detailed process of performing the experiment.

3.1 Technology and Setup

In preparation for the forensics experiment, the following hardware and software tools were used.

Hardware:

- One laptop (4GB RAM) for forensics workstation activities
- Four laptops (4GB RAM) for suspect activities
- Four USB Flash Drive (8GB) each containing a portable web browsers
- Four USB External device (8GB) to save captured RAM files
- SATA to USB adaptor
- USB write blocker

Software:

- Microsoft Windows 7, Pro 32 bits, SP1
- DaemonFS 1.1, file integrity monitoring software
- Paragon DiskWipe v 12
- NirSoft Internet Tools- history, cache, and cookie viewers
- Firefox Portable 33.0, Google Chrome portable 42.0.2311.90, Opera portable 12.7, and Safari portable 5.1.7
- FTK Imager Lite- portable version
- SQLite Maestro software
- WinHex
- Mandiant Redline Memory forensics tool
- DumpIt memory capture software
- VMware workstation 10

3.2 Experiment Details

We installed VMware Workstation (VM) on all four laptops and then installed Windows 7 on VM. Subsequently, we installed DaemonFS [20] a tool that monitors in real time files on the hard disk. We also installed several tools [21] on the machines for viewing history, cache and cookies. Next, we used Paragon Disk Wiper [22] to wipe all external devices and installed PortableApps [23] on them. This utility allows you to run different programs from a flash drive. Subsequently, we installed one portable web browser on each external device and connected them to the suspect laptops. Write-blocker was used to preserve the integrity. We should note that no regular browser was installed. At this point we were ready to do the web browsing activities. Each portable browser was individually launched in private mode followed by the same series of web activities for all four browsers, i.e. email account login, a bank account login, sending/receiving email, searching for images and videos, uploading and downloading files and streaming some video.

3.3 Static Media Forensics

Traces of web browsing activities will be kept in the in various logging files including registry keys, cache, cookies, temp, and recent, files

Recent executables, logging information and visited locations can be found in the registry keys. The registry is structured as a group of hives as shown below.

- HKEY_USERS: contains all the loaded user profiles
- HKEYCURRENT_USER: profile of the currently logged-on user
- HKEYCLASSES_ROOT: configuration information on the application used to open files
- HKEYCURRENT_CONFIG: hardware profile of the system at startup
- HKEYLOCAL_MACHINE: configuration information including hardware and software settings
- HKEY_CURRENT_USER\Software\Microsoft\Mozila_Firefox\TypedURLs; URL of the visited websites

1) Examination of the above registry keys showed that even after closing the browser and removing portable browser device from the suspect machine, valuable information that can link the suspect with the incident is retrievable (see Table 1).

Table 1- Retrievable artifact from registry keys

Portable Browser	Registry report of host machine activity
Chrome	Flash drive vendor Id, product Id, version, serial number, drive letter, URLs visited was retrievable. Some registry keys was created but deleted after the browser was closed
Firefox	Flash drive vendor Id, product Id, version, serial number, drive letter, URLs visited was retrievable. The time/date the browser launched was also visible
Safari	Flash drive vendor Id, product Id, version, serial number, drive letter, and URLs visited were retrievable.
Opera	Flash drive vendor Id, product Id, version, serial number, drive letter, URLs visited was retrievable. The time/date the browser launched was also visible

Table 1 entries show information such as flash drive vendor Id, product Id, serial number, URL history, and date/time the browsers were launched. These are important evidential information that establishes a link between the suspect and browsing activities. However, we were not able to see the details of browsing activities. This suggests that examining the registry data only is not sufficient.

2) Evaluation of the contents of temp files, recent items, and cache files, show that most of the browsing activities information created, modified and then deleted from the host machine (see Table 2).

Table 2- Retrieved portable browsing artifacts

Portable Browser	Suspect machine Activity
Chrome	*temp, recent, and cache* created and then deleted. some account login info and *downloaded* files created but not deleted
Firefox	*temp, recent,* and *cache* created and then deleted
Safari	*temp, recent cache* created and then deleted for email login we noticed that some *Appdata/Ntuser.dat* modified on the host machine but not deleted
Opera	*temp, recent, and cache* created and then deleted

Table 2 entries show portable Firefox and Opera offer slightly more privacy than portable Chrome and Safari. This is because with portable Chrome we were able to see some account login information such as date and time and information about downloaded files. Similarly portable Safari leaves traces of email communication activities such as email id, date and time email was sent. We repeated the process to verify the validity of the results and obtained the same results the second time. Note that the portable browser removal had an impact on the amount and type of data that retrieved after a private portable browsing session.

3) *Webappstore.sqlite-shm* is a file in the profile folder of the SQLite database and contains web storage data. This data is set by web browser in the same way as cookies. Web browsers use two mechanisms to set the data, i.e. *.sessionStorage* and *localStorage*. The data set through *sessionStorage* mechanism disappear after the browser is closed, but the *LocalStorage* data set persist even after the browser is closed. The *sessionStorage* mechanism also handles three other files within the SQLite profile folder called *cookies.sqlite-wal* and *cookies.sqlite-shm*. and *places.sqlite*. These files stored annotations, bookmarks, favorite icons, input history, keywords, and browsing history. For Mozilla Firefox, for example, the path for these files is listed below.

- C:/Users/MA/Desktop/Mozilla.Firefox.33.0.Portable/Data/Profile/webappsstore.sqlite-wal
- C:/Users/MA/Desktop/Mozilla.Firefox.33.0.Portable/Data/Profile/cookies.sqlite-shm
- C:/Users/MA/Desktop/Mozilla.Firefox.33.0.Portable/Data/Profile/cookies.sqlite-wal
- C:/Users/MA/Desktop/Mozilla.Firefox.33.0.Portable/Data/Profile/places.sqlite-wal

We used NirSoft Maestro freeware tools and examined the SQLite database files listed above. Table 3 entries show the activities on the host machine reported by SQLite profile files.

Table 3- SQLite files report of portable browsing session

Portable Browser	Suspect machine Activity
Chrome	*cookies.sqlite-wal* *cookies.sqlite-shm* *places.sqlite-shm webappsstore.sqlite-shm* were created and then deleted
Firefox	*cookies.sqlite-wal*

	cookies.sqlite-shm *places.sqlite-shm webappsstore.sqlite-shm* were created and then deleted
Safari	*cookies.sqlite-wal* *cookies.sqlite-shm* *places.sqlite-shm webappsstore.sqlite-shm* were created and then deleted
Opera	*cookies.sqlite-wal* *cookies.sqlite-shm* *places.sqlite-shm webappsstore.sqlite-shm* were created and then deleted

Table 3 entries shows SQLite files contain some browsing activities, but the data are not saved to the local machine, but are saved in the portable browser device, e.g. for Firefox the path for this data is: Mozilla.Firefox.33.0.Portable/

3.4 Live Memory Forensics

Memory forensics involve two steps, RAM capture and analysis of the captured RAM. For RAM capture, there are some free tools such as FTK imager, Belksoft RAM capture, DumpIt, etc. For memory analysis, there are both proprietary and free tools. Table 4 shows a comparison of the most popular memory analysis tools.

Table 4-Comparisson of Memory Analysis Tools

	Redline Memoryze	HBgary Responder	Volatility Framework	Encase Encrypt
Support Win OS	All	All	All	All
Supported Image format	Raw	Raw	Raw crash dump hibernation	Ram crash dump
Supported CPU	Intel x86 AMD 64	Intel x86 AMD 64	Intel x86	Intel x86 AMD 64
Extracts closed processes & apps	No	No	Yes	yes

We selected Mandiant Redline [24] for the following reasons:

- Supports both RAM capture and analysis for free
- Graphical User Interface
- Allows users to choose only browsing related processes and disabling all the other processes and files
- Allow to import memory analysis results to a file such as MS Word for offline processing
- Relatively easy to use.

In Redline, RAM capture tool is called Collector and RAM analysis tool is called Memoryze. Users can make these based on their needs. We created the Collector and Memoryze software and saved them on an external device and the forensics workstation respectively.

We used two scenarios, 1) after a portable browsing session, use Collector to capture memory 2) remove the portable browser flash drive from the suspect machine after the browsing session, close the browser, and then capture RAM. Since Redline Collector cannot collect information about terminating processes and closed files (see Table 4) we also used WinHex [25] Hexadecimal editor to evaluate the content of memory.

3.5 RAM Forensics Experiment

To make data extracting less cumbersome, we cleared all cookies, cache, history, bookmarks, etc. that may have been left on the suspect machines from our earlier experiment. We also disabled physical address extension mode on the Redline. Then we followed the below steps:

1. Attached the portable browser external device to the suspect machine and configured the browser as the default browser with extensions and plug-ins disabled. Then we performed a browsing session, attached the Collector external drive to the suspect machine, captured RAM, and saved the file onto an external device.
2. Step 1 was repeated for the other three portable browsers.
3. We repeated steps 1 and 2 above, but this time we removed the portable browser flash drive, closed the browser, immediately captured RAM and saved it to the external device.
4. Configured Memoryze to retrieve only browsing related information and processes. This action reduced the amount and time of data analysis. We imported the memory parsed data to a MS Word file for offline analysis. We should note that Redline only provide information about running processes and programs that were running before the RAM was captured.
5. Step 4 was repeated for the other three captured memory files.

Overall, we had four captured RAM files for the cases when portable browsers flash drives were still attached to the suspect machines during the RAM capture process and four captured memory files for the case when portable storage flash drives were removed after each browsing session. The total memory files that we captured were eight. Considering each memory capture took, on average thirty minutes, we spent four hours to capture RAMs. The process of memory capture and analysis were performed according to the forensics investigations rules and regulations.

4. RESULTS

Results of memory forensics analysis due to a portable browsing session while portable browser devices were still attached to the computer and the browsers were open are shown in Table 5. When we removed the portable browsers from the machines and then captured and analyzed RAM, results are shown in table 6.

Table 5-RAM forensics artifacts when portable browsers devices were attached to the machines

Data Item	Firefox	Opera	Chrome	Safari
Browser process	√	√	√	√
URL History	√	√	√	√
Cookies	√	√	√	√
downloads	√	√	√	√
Timelines	√	√	√	√
Browsing history	√	√	√	√

Email password	–	–	–	–
Email ID	√	√	√	√
SSL Certificate	√	√	√	√
Search history	√	√	√	√

Table 6-RAM forensics artifacts when portable browsers devices were removed from the machines

Data Item	Firefox	Opera	Chrome	Safari
Browser process	-	-	√	-
URL History	√	√	√	√
Cookies	–	–	–	–
downloads	√	√	√	√
Timelines	–	–	√	–
Browsing history	√	√	√	√
Email password	–	–	–	–
Email ID	√	√	√	√
SSL Certificate	√	√	√	√
Search history	√	√	√	√

Table 5 entries show with the exception of email password, everything else was retrievable. That means if the portable USB flash drive is attached to the machine during RAM capture, private portable browser provides no privacy at all. In this case, the information that was retrieved from memory is enough to conclude browsing activities and establishing link between the web browsing activities and the suspect. For example, Table 5 shows email Id for the suspect. This information is sufficient to establish a link between the suspect and browsing activities. However, when we removed the portable browser from the machine and then captured RAM, forensics artifacts retrieved from main memory slightly varies among various browsers (see Table 6). This variation is discussed below.

For Mozilla Firefox analysis of the memory dumped file showed considerable browser related entries in memory indicating web browser activity. We were able to detect email communication details, browsing and URL history, search history and downloaded files (documents, images, and videos). On the other hand; some information such as cookies, email password, timelines and process Id could not be retrieved. We also used Winhex to analyze the captured RAM, but did not find any of aforementioned data either. This indicates that when the portable browser flash drives were removed, some of the browsing information was replaced with zeroes or deleted from the memory. Nevertheless, different browser handles this issue differently.

Similar results were observed for Opera. Analysis of the RAM showed that portable browser flash drive removal had an impact on the amount of data retrievable from memory. Similar to Firefox; cookies, timelines, email passwords and Process Id were deleted before we captured memory. This is because once the portable browser flash drive was removed, the data structure tree that handle cookies for example, are not accessible. On the other hand, we were able to identify data containing various types of information, including the SSL Certificate for accessing a secure website, URL, file downloaded and more.

Google Chrome revealed forensically valuable artifacts such as Certificate, HTML text file, URL history, and files downloaded. We should note that only Google Chrome saved process Id in memory. Similar to Firefox we were not able to see cookies, email password and timeline. Based on our study, Google Chrome portable left the most residual artifacts among the four portable browsers.

For Safari, the amount of retrieved data from portable browsing session is identical to Firefox and Opera. Meaning cookies, timeline and email password were not retrievable from main memory. However, like Firefox we were able to see forensically valuable information such as history, file downloads, Certificates, etc.

In an attempt to validate the retrieved data from main memory through Redline Collector, we used another open source software tool called DumpIt [26] and captured the physical memory after a browsing session and closure of the browser. We used WinHex to analyze the captured images. Analysis of the results for both Redline and DumpIt showed the same results.

4.1 Analysis of the Results

Interpretation of the data captured from memory indicates that private portable browsing does leave browsing evidence, even after the browser flash drives were removed from the suspect machines in all four portable browsers under this experiment. The type and the amount of data varied slightly among the browsers. For example, Table 6 above shows the timeline and process Id is retrievable with portable Google Chrome. Figure 1 below shows (see read arrow) the date, time and the site that was visited. Among all the browsers in our study Google Chrome portable left the most residual artifacts on the volatile memory of the suspect machine.

Figure 1-Analysis of captured RAM after the private portable Google Chrome browsing session.

Windows registry keys showed flash drive information such as vendor Id, product Id, serial number, etc. This information is sufficient to establish a link between the suspect and the browsing activities. In addition, evaluation of the SQLite database files showed information about the browsing activities were saved but then deleted. It is worth to do further research on this topic to find the amount and type of data being deleted. Similarly, examination of temp, recent, and cache showed browser activity, but all the data were deleted after closure of the browser.

We used the *Ipconfig/displaydns* command to generate the site address and the IP addresses of the sites visited even after the browser media is removed. Figures 2 and Figure 3 show the sites visited with their IP addresses. However, closure of the browser causes the Time-to-Live of the process to be reduced

from 42 to 7 seconds. This indicates that the speed of browser closing and capturing RAM is important.

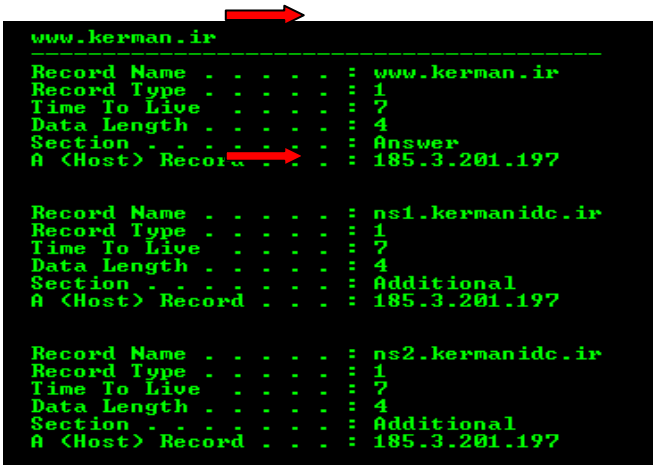

Figure 2- Time-to Live of browser's process before closing of the browser

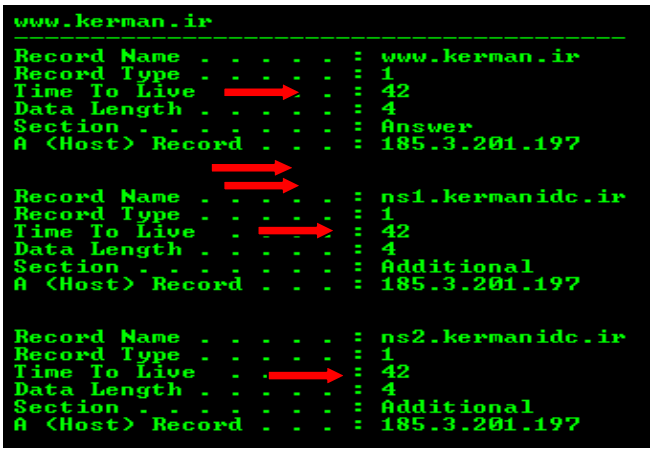

Figure 3- Time-to Live of browser's process after closing of the browser

5. CONCLUSIONS

We applied both static media forensics and volatile memory forensics to retrieve forensics artifacts after a private portable browsing session. The portable browsers we experimented with include Firefox, Opera, Chrome and Safari. We found that through a combination of static memory and RAM forensics we can retrieve forensically valuable information about suspect's activity, such as sites visited, Internet searches, secure sites login credentials, traces of email communication, even after the portable browsers flash drive were removed from the machine. This information is important forensics artifacts for an investigator. Moreover, the artifacts such as flash drive vendor Id, product Id, version, serial number, drive letter, URLs visited constitute a link between the data and the suspect browsing activities. Our experiment shows that the vendor's claim of privacy can be nullified through a combination of various computer forensics investigations. Among portable browsers under our experiment Google Chrome portable left the most residual artifacts on the host machine. For example, the date and time of browsing activities were still retrievable after a browsing session.

Examination of the log files such as cache, recent, history, temp, and browser related SQLite database files show that browser activities were recorded, but immediately deleted upon removal of the portable browser devices from the suspect machines.

Due to the dynamic nature of physical memory, the time gap between removing the portable browser device media from the machine and capturing RAM is very important. The more time is spent; there would be more chance of losing data in volatile memory. Also, when the browsers are closed, we can retrieve the last information saved to the clipboard and analyze for possible evidential information. Finally, we showed the registry keys are a good source for retrieving portable browsing artifacts when it is used along with memory forensics.

We should note that the browsing sessions in this experiment were much shorter than what a normal web browsing would have been. For the longer browsing session, the data captured from RAM, possibly could be retrieved from pagefile.sys and hyberfile.sys.

6. FUTURE WORK

This research can be extended in several ways. First, repeat the same experiment with different tool such as Volatility. Second, extract information over an extended period of time instead of one specified browsing session.

ACKNOWLEDGEMENT

This research was supported by the 2015 UNG Presidential semester award. The author would like to thank all the individuals who were involved in the establishment and the implementation process of this award.

7. REFERENCES

[1] Choi, J. H., K.G. Lee, J. Park, C. Lee, and S. Lee. Analysis framework to detect artifacts of portable web browser: ITCF, Springer, pp. 207-214, (2012).

[2] Aggarwal, G., Bursztien, E., Jackson C., & Boneh, D. An analysis of private browsing modes in modern browsers. Proceedings of the 19th Usenix Security Symposium, pp. 1-15, (2012).

[3] Simon, M. and Slay, J. Enhancement of Forensics Computing Investigations through Memory Forensics Techniques. Proceedings of the International Conference on Availability, Reliability and Security, pp. 995-1000, (2009).

[4] Davis, N. Live memory forensics for Windows Operating Systems. Eastern Michigan University, IA 328, (2015). http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.173.6197&rep=rep1&type=pdf

[5] Oh, O., Lee, S., and Lee, S. Advanced evidence collection and analysis of web browser activity. Journal of digital investigation 8, pp. 62-70, (2011).

[6] Ohana, D.J. and Shashidhar, N. Do private and portable web browsers leave incriminating Evidence? A forensic analysis of residual artifacts from private and portable web browsing sessions. EURASIP J, on Inf. S. 201(6), pp. 1-13, (2013).

[7] Mozilla Firefox (2015). https://support.mozilla.org/en-US/kb/private-browsing-use-firefox-without-history?redirectlocale=en-US&redirectslug=Private+Browsing

[8] Google Chrome (2015). http://portableapps.com/apps/internet/google_chrome_portable

[9] Opera (2015). http://www.kejut.com/operaportable

[10] Apple safari (2015).http://safari.soft32.com/

[11] Marringhton, A., I. Baggili, T. AI Ismail, A. AI Kaf. Portable Web Browser Forensics: A forensic examination of the privacy benefits of portable web browsers. ICCSII, pp. 1-6, (2012).

[12] Adautin, E.D. and Meeran, N. Forensic Reconstruction and Analysis of Residual Artifacts from Portable Web Browse. International Journal of Computer Applications. Vol 128, No18, pp. 19-24, (2015).

[13] Flowers, C., Mansour, A. and Al-Khateeb, H.M. Web browser artefacts in private and portable modes: a forensic investigation', Int. J. Electronic Security and Digital. Vol. 8, No. 2, pp.99–117, (2016).

[14] Dharan, D.G. and Meeran, N.A.R. Forensic Evidence Collection by Reconstruction of Artifacts in Portable Web Browser. International Journal of Computer Applications, Vol 91, No 4, pp. 32-35, (2014).

[15] Mahendrakar, A., Irving, J., and Patel, S. Forensic Analysis of Private Browsing Mode in Popular Browsers (2014). http://mocktest.net/paper.pdf

[16] Said, H., Mutawa, A.H., Awadhi, A.I., Guimaraes, M. Forensic analysis of private browsing artifacts. Proceedings of the International Conference on Innovations in Information Technology (IIT), (2011).

[17] Hejazi, S.M., Talhi, C. & Debbabi, M. Extraction of Forensically Sensitive Information from Windows Physical Memory. Digital Investigation, Elsevier publishing Co, 6, pp. 121-131., (2009).

[18] Satvat, K., Forshaw, M., Hao, F. and Toreini E. On the Privacy of Private Browsing – A Forensic approach. Journal of Information Security and Application, Vol 19, pp. 88-100, (2014).

[19] Amari, K.. Techniques and Tools for Recovering and Analyzing Data from Volatile Memory. SANS Institute InfoSec Reading Room, (2009).

[20] DaemonFS, (2015). http://sourceforge.net/projects/daemonfs/

[21] NirSoft. NirSoft Freeware Utilities, (2013) http://nirsoft.net.

[22] Paragon Disk Wiper, (2015). http://www.paragon-software.com/home/dw-professional/download.html

[23] PortableApps. (2013). http://portableapps.com/

[24] Mandiant Redline (2014). https://dl.mandiant.com/EE/library/Redline1.7_UserGuide.pdf

[25] WinHex (2015). http://www.x-ways.net/winhex/

[26] Suitche. DumpIt memory capture tool. (2015) http://www.moonsols.com/wp-content/uploads/downloads/2011/07/DumpIt.zip