Forensic Evidence Collection by Reconstruction of Artifacts in Portable Web Browser

Divyesh G Dharan D
PG Scholar
Information Security and Computer Forensics
SRM University, India

Nagoor Meeran A R
Assistant Professor
Information Security and Computer Forensics
SRM University, India

ABSTRACT
A web browser installed on a removable disk makes it a portable one. The main motive behind the development of a portable web browser is to personalize the browsing session of the user by limiting the history residues. The enhanced privacy benefits the user at large by reducing the interaction of browsing activity with the computer disk, but poses a challenge for forensic examiners to collect evidence in case of cyber crimes and internet fraud. This paper examines the need of developing a methodology which would help the investigators to tackle the situation and collect evidence to prove the crime. Also, this paper puts forward a tool which would help the investigators in evidence collection.

General Terms
Browser Security, Digital Forensics, History Recreation, Incident response

Keywords
Browser Forensics, Privacy Claims, Portable web browser, Private browsing artifacts, Reconstruction

1. INTRODUCTION
Internet has emerged as an essential tool for everyday activities. Web browsers are used to connect to the Internet. They are generally used for searching information in the World Wide Web. It provides a means for communication through emails or instant messaging, social networks. Internet has revolutionized banking with e-commerce which in turn resulted in growing financial frauds by extracting the critical data left by the users after their browsing sessions.

Web browsers are designed to record and retain a lot of information such as cache files, URLs, search keywords, cookies related to the user's activities. These files are stored on the local computer and can be retrieved by anyone who uses the same computer. Hence there was a need to personalize the browsing activity of user, to protect the critical data from theft, by enhancing the privacy of browsers. As a result, all major vendors started providing a new feature called Private Browsing Mode [1] which restricts the browser from storing the web browsing history. However, the private browsing mode can be virtually impaired by using third party packages to retrieve the history [2]. An alternative to private browsing mode is the usage of portable web browser.

A web browser installed on a removable drive serves the purpose as the browser is no longer an integral part of the computer. When a user plugs in the USB drive to a computer with internet connectivity, one can browse the internet. Privacy is enhanced by storing the browsing sessions on the portable device instead of a computer. Therefore portable web browsers are a challenge for the forensic examiners to investigate a suspect's Internet activities in cases where questionable web sites were visited or criminal acts were conducted through them.

Past research on portable web browsers is limited and doesn't provide an in-depth analysis of the findings made. This paper takes up the issue and we plan to overcome the shortcomings by analyzing the after effects of the portable web browsing session in both Live and Offline modes. This research used an experimental methodology to forensically examine the privacy benefits of portable web browser through forensic analysis of the artifacts left by it on the local hard disk. A reconstruction module has been added to automate the process of identifying the browsing activity of the user.

2. RELATED WORK
2.1 Web Browser Forensics
Web browser forensics [3] has acquired much importance in digital forensics due to the growing number of internet fraud. Forensic analysis of the browser in a user's machine is the primary activity in such investigations as the information generated from web browsers can be of great use in reconstructing the browsing behavior of the user. Improper use of the internet can be detected from the information obtained. Since browsers are adaptable with the frequent version changes it is highly essential for the digital forensics community to ensure that they are familiar with the new updates in order to perform a forensic analysis. It has been identified that the web browser history, cache, cookies, preferences and the registry are the areas to be searched for evidence. Therefore, investigators have to obtain information from numerous locations in order to be confident that they have identified all the digital evidence pertaining to a user's web browser usage. The need for extended privacy in web browsing led to the creation of private browsing mode.

The motivation for a user to browse privately is to conceal evidence of unusual browsing activity. A study on the private browsing artifacts of the installed browsers has shown that the private browsing modes of the Google Chrome, Mozilla Firefox and Microsoft Internet Explorer browsers have left artifacts. Microsoft Internet Explorer left forensic artifacts of the private browsing session, in the form of deleted files on the hard disk. Mozilla Firefox left artifacts on the hard disk in the pagefile.sys file.

A recent experiment conducted has shown the weakness of private browsing modes. Running a memory leaking program, can pull artifacts from private browsing sessions in to the memory. DNS resolutions are cached by the operating system, and an analysis of the cache and Time to live values, it can be concluded if the user visited a particular site. Further traces can be obtained by checking the swapped pages.

2.2 Portable Web Browser

A study on portable web browser [4] shows that the browsing artifacts are stored in the installation folder which is primarily in the removable storage disk. However once it is unplugged, the medium is unavailable for the forensic examiner. The researchers concluded that it was difficult to trace further information. These conclusions were drawn theoretically and it lacks practical proof as it is extremely important to map a link between the user and browsing session. Forensic evidence can be obtained by searching the Windows registry and Prefetch Files.

2.3 Flash Drives

A joint venture between Microsoft and SanDisk [5] on a project titled U3 Technology was to enable the users to customize their usage expectations. It is achieved by grouping personalized files and web browsers in a removable disk. The idea came from the plug and play mode. The drive has a launch pad [6] which will activate the browser once it is plugged in to a computer. Such devices recorded user actions by creating a folder on host computers which is automatically removed when the device is unplugged. But the Windows Prefetch files analysis clearly shows the activity performed by the user from these devices breaking the strength of these drives.

3. METHODOLOGY

A methodology that would help investigators to effectively examine activities associated with portable web browser starts with the preliminary examination in lines with incident response. The pre-incident preparation includes designing a check list pertaining to the browser. The steps included are as following:

Fig 1: Detailed Methodology

The hardware and software requirements for forensic investigation are as following.

Hardware

- Desktop PC- forensic workstation
- 80GB SATA Hard Drive
- True Imager
- True back
- USB Flash Drive

Software

- Microsoft Windows XP SP3
- Internet Explorer, Firefox, Chrome
- Disk Wipe- to replace all data on disk with zeros
- Nirsoft Tools- history, cache, cookie viewers
- FTK Imager- used to create forensic images
- FTK Imager Lite- portable version
- WinHex, HxD Analysis of forensic images
- IR toolkit

The process of evidence collection depends on the status of the computer.

1. Live analysis
2. Offline analysis

3.1 Live Analysis

Live analysis can be performed only when the system is not switched off after the incident. In this case, the important step is to collect the volatile data. The response toolkit should be populated with executables which helps the investigators to identify the current number of users logged in, network status, list of process running, data and time, list of ports open etc [7]. The remote system status and the open ports help the investigators to easily identify the website visited by the user. It is highly essential to record the commands executed on the system. Once the volatile information is gathered, checking the registry for the USB event helps in identifying the presence of a removable flash drive. Performing a string search to check for common cookies also helps in gathering the information. Acquisition can only be done after imaging the RAM and analyzing the hex codes in the image. Forensic tools like Encase, True Back, and FTK Imager are a few tools for capturing the perfect image.

3.2 Offline Analysis

A portable web browser is installed in a USB flash drive and it is plugged in to a computer system. A short browsing session is carried out from the browser installed in the USB drive. The flash drive is removed and the system is switched off. Now investigating the system to collect evidence to prove the browsing activity [8] is a challenge for the examiners as the portable browser limits the dependence on the host system.

3.3 Data Collection

The hard drive from the victim system is removed and an evidence tag is added to it. The evidence tag is mandatory to track the hands using the evidence medium. The registry is checked for the entry of new devices and eventvwr is also analyzed for anomalies [10]. The information obtained from these checks is saved for analysis.

3.4 Forensic Duplication

Now an image of the hard disk is created by using the forensic imaging tool. The extension of the image should be properly noted to avoid any confusions regarding duplication. The image file with a P01 extension is fed in to the target medium

for analysis. Bit by bit analysis of the image can be done using WinHex and HxD viewers. Each sector is carefully identified for possible traces.

3.5 Trace Collection

The traces obtained during the analysis are saved along with the list of commands executed on the forensic workstation. [10] The best way to record the commands is to use a doskey utility. Running a batch file containing a pre designed list of files is also helpful in some way to identify the traces.

3.6 Trace Analysis

Trace analysis begins with counting the number of letters obtained from the image and identifying the absolute sector where traces of browsing history are left as shown:

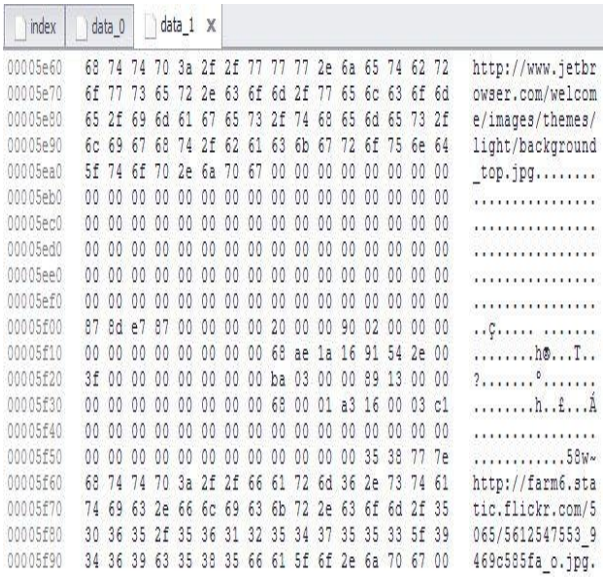

Fig 2: Traces found on the hard disk

The letters are identified individually and they are fed in to a lister which would generate the possible combinations of the letters obtained from the image. This is done by running a .exe file which employs a recursion function to list down the permutations. The output of the lister is saved to a text file.

3.7 Identifying the URL

A database is populated with all possible keywords that would appear in any browsing session. Each table in the database points to a particular scenario and the possible keywords that would appear during the browsing activity are exclusively populated into the table. In case of an email fraud, the table consists of almost all the keywords that appear in an email header. The text file that consists of all the possible permutations is loaded in to a table. A one to one mapping of the trace is carried out using specific keywords. The mapping begins with the first keyword and continues till the end. Every successful hit is stored in to another table. A logical analysis of the matched string helps the investigator to identify the URL.

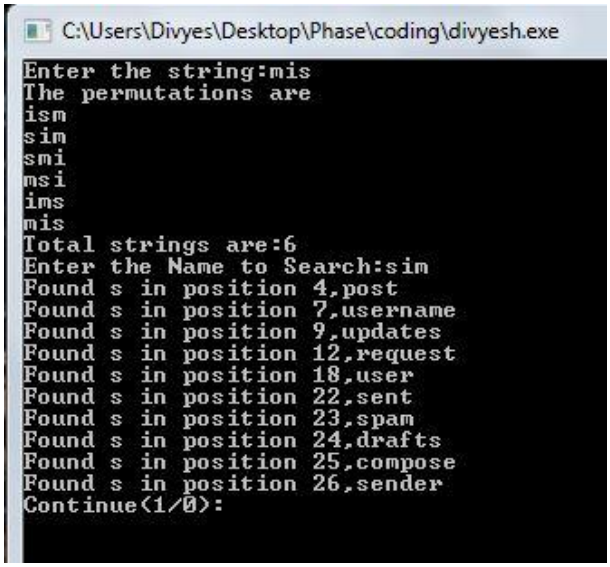

Fig: Reconstruction

4. RESULTS

The browsing session included facebook account usage and an email account. A mail has been forwarded to a recipient regarding catering service. On analyzing the image the following hits were obtained:

Table 1: Keyword Hits

Keyword	Live	Offline
Tables	End	Last
Figures	Good	Similar

Reconstruction was carried out by mapping various combinations obtained from the probable strings. The three stain arrays are analyzed independently and it has been clearly understood that the portable web browser leaves forensic artifacts. Similar data can be obtained from the windows prefetch files where website authentication signatures were found [11] [12]. In case of banking frauds, analyzing the saved passwords and auto fills can also help in analyzing the browsing activity of the suspicious users. The number of keyword hits is more in installed browser than portable browser. The experimental results prove that portable web browser leaves traces both in live and offline modes.

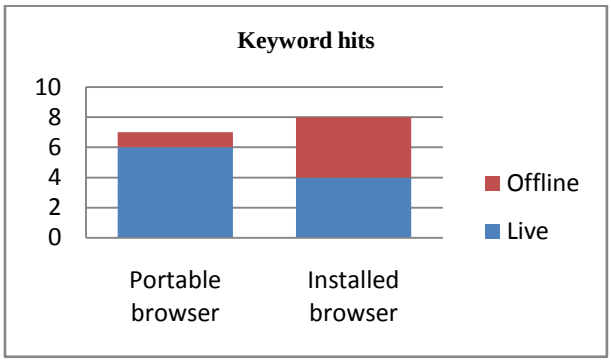

Fig 3: Comparison between portable and installed browser traces

5. FUTURE WORKS

Future enhancements include analyzing the incognito modes of the portable web browsers which deletes the device registry from the events. An analysis and comparison between the leading portable web browsers in terms of security is of high importance. More efficient methodology for live analysis would be the priority for future enhancements.

6. CONCLUSION

A close examination of the computer system in live mode shows more forensic traces when compared to offline analysis. System volume information and windows prefetch files are a huge source of information where traces are found. This paper has addressed the issues in live analysis by introducing a fully equipped IR toolkit and a methodology to obtain as much traces as possible from the scene of crime. The tool that has been developed as part of the methodology ensures that the investigators have a easy hand in examining the computer. The user friendly GUI helps investigators with least knowledge to perform effective investigation. However, identifying the sectors where traces are stored is still a manual process since human intelligence is considered miles ahead of artificial computation.

7. ACKNOWLEDGMENT

We thank every person who helped us in finishing this work perfectly.

8. REFERENCE

[1] G. Aggarwal, E. Bursztein, C. Jackson, and D. Boneh, "An analysis of private browsing modes in modern browsers," *In Proc. Of 19th Usenix Security Symposium,* 2010.

[2] C. Soghoian, "Why private browsing modes do not deliver real privacy," *Center for Applied Cybersecurity Research,* 2011.

[3] T. Bosschert, "Battling anti-forensics: beating the U3 stick," *Journal of Digital Forensic Practice,* June 2007

[4] J.H. Choi, K.G. Lee, J. Park, C. Lee, and S. Lee, "Analysis framework to detect artifacts of portable web browser," *Center for Information Security Technologies,* 2012.

[5] R. Tank, and P.A.H. Williams, The impact of U3 devices on forensic analysis," *Australian Digital Forensics Conference,* Dec. 2008.

[6] SanDisk. (2010). *U3 Launchpad End Of Life Notice.* http://kb.sandisk.com /app/answers/detail/a_id/5358/~/u3-launchpad-end-of-life-notice

[7] Google. (2012). *Incognito mode.*[Online]. Available:https://www.google.com/intl/en/chrome/browser/features.html#privacy

[8] Microsoft. (2012). *InPrivate Browsing.* [Online]. Available: http://windows.microsoft.com/en-US/internet-explorer/products/ie-9/features/in-private

[9] K.J. Jones, and R. Belan (2010), "Web Browser Forensics," *SecurityFocus* [Web Document]. http://www.securityfocus.com/infocus/1827.

[10] Junghoon O., Seungbong L., Sangjin L. (2011, Aug.), "Advanced evidence collection and analysis of web browser activity," *Digital Investigation.* 8, pp. S62-S70.

[11] M.T. Pereira (2009, Mar.), "Forensic analysis of the Firefox 3 Internet history and recovery of deleted SQLite records", *Digital Investigation*"

[12] K.J. Jones (2003), "Forensic Analysis of Internet Explorer Activity Files", [Web Document]. http://nys.fd.org/cja/forensics/ieactivity.pdf.