Web Browsing Forensics

By [redacted]

Abstract

A web browser is more than just a tool that is used to access the internet/WWW. Web browsers can be used to be able to access crucial information about the user. Web browsers can be used as a computer forensics tool. In this paper I will inform you in detail of how a web browser can be used as a computer forensics tool. I will also tell you how to be able to analysis a web browsers memory and what traces of browsing activity remains in the memory. Then I will show you the results of the analysis on four different web browsers.

1 Introduction

A web browser is more than just a tool that is used to access the internet/WWW. Web browsers can be used to be able to access crucial information about the user. By using the information that is accessed by the web browser you can be able to know what the user has been searching. Web browsers can be used as a computer forensics tool.

I will also be able to show some tests that were done on four different web browsers and be able to shine some light on what information is being left on the web browser and as will to see how well the level of security is provided by each one of the web browser.

2 Web browser used as a computer forensics tool

This section gives you an insight on how a web browser can be used to shine a light on what the user is doing on the internet. This gives us special attention to the evidential value of a web history and cache files of a browser.

A web browser is an important thing to consider, since it is the gateway to the internet. When you want to investigate a web browser for information, it is very crucial that you understand how a web browser works, how it gathers the data and how it stores it on the computer. The first thing that you want to do is to analysis the data that was captured by the web browser.

When a user uses a web browser he usually enters a URL of the website that he wishes to use or searches for it on one of the web browsers using keywords. Then the web browser searches for the website, locates it and then connects to it by breaking the URL into an IP address, this will help make the URL more unique and it insures that the web browser won't connect to a different website. Also the web browser will also do a number of other things, like create log files, store data in cache files, and etc., on the user's device.

3 Results

The results are taken from the article *"Forensic Analysis of private Browsing Mode in popular Browsers"* by Aditya Mahendrakar, Irving, and Patel. [2] In their article they did a test of four web browsers. In their test they were able to determine how much data was able to be recovered from the web browser after it was closed.

3.1 Firefox

They were able to find less than one megabyte of their signature HTML text in the full memory dump and also able to recover their signature SSL certificate, form password, data, and cookies. They were not able to recover any new URLs or images from this web browser. [2]

3.2 Explorer

Explorer showed the same results as Firefox but there was less than one megabyte of new HTML data recovered. Also they were able to recover every URL that they entered during the recovery of their test. [2]

3.3 Chrome

Google chrome was the same as the explorer web browser. [2]

3.4 Safari

Safari also showed the same results as the others but gave them some new information like the form password and the generated cookies. [2]

	Firefox	IE	Chrome	Safari
URL	✓ (1 in cert)	✓ (many)	✓ (many)	✓ (all)
HTML	✓ (< 1 MB)	✓ (< 1 MB)	✓ (< 1 MB)	✓
Images				✓
Form Data	✓	✓	✓	✓
Password	✓	✓	✓	✓
Certificates	✓	✓	✓	✓
Cookies	✓	✓	✓	✓

Table. 3: Artifacts left in entire memory including kernel. [2]

6 Conclusion

To conclude, in this paper I have talked about what a web browser is and how it can be used as a forensics tool, also I was able to find information on four web browsers, also the results of the test that was done on them by Aditya Mahendrakar, Irving, and Patel. I hope that this paper has shined light on this topic.

References

[1] Jain, Ravi. *"Web Browser as a Forensic Computing Tool."*< http://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?sid=6631f86a-42d0-458e-baf8-7b801f048534%40sessionmgr4004&vid=1&hid=4111 > Web. 29 Sept. 2015.

[2] Mahendrakar, Aditya, James Irving, and Shivam Patel. *"Forensic Analysis of Private Browsing Mode in Popular Browsers."* < http://mocktest.net/paper.pdf >Web. 29 Sept. 2015.