Mozilla Firefox Browsing Artifacts in 3 Different Anti-forensics Modes

Deepak Gupta[1] and Babu M. Mehtre[2(✉)]

[1] School of Computer and Information Science,
University of Hyderabad, Hyderabad, India
Deepkguptal989@gmail.com
[2] Institute for Development and Research in Banking Technology
(Established by Reserve Bank of India), Hyderabad, India
BMMehtre@idrbt.ac.in

Abstract. There are several techniques which can assist a user to avoid leaving traces (Digital Evidence) of Internet activity so that one can frustrate forensic investigation. In this paper we examined three different usage scenarios of Internet browsing using Mozilla Firefox. These different usage scenarios were a sandbox environment, browsing with portable tools, and browsing with virtual box. We tried to find the artifacts created and left by web browsing activities in each of these usage scenarios. In our experiments, we performed identical web browsing activity for each of the three scenarios and investigated whether the traces were left behind.

Keywords: Forensics investigation · Digital evidences · Artifacts · Anti-forensics techniques · Portable environment · Virtual box · Sandboxie

1 Introduction

Various software products are now available on the Internet, both free and commercial. Many products can be used either to carry out malicious activity or assist in doing so. Software artifacts are by-products produced during installation and/or use of these software products which can be used as evidence during the crucial investigation. Software artifact forensics is the collection of these byproducts to investigate and/or prove a theory of a crime. Unfortunately in the past couple of years, many tools and techniques have been made available which can help a user to get rid of these traces and to frustrate a digital investigation. These tools provide an ostensibly trace-free environment for criminals to carry out their malicious intent without leaving any trails on their computer.

This paper aims to investigate the artifacts created by the web browsing activities of Mozilla Firefox in three different anti-forensics modes: using a portable web browser version, browsing inside a sandbox environment, and browsing inside a virtual machine. For investigation purposes we started with a traditional digital forensics approach in which we search common places in which artifacts are generally found. Next we used the forensics tool EnCase for deep investigation. Physical memory (RAM) was also captured and analyzed for evidence.

P. Gladyshev et al. (Eds.): ICDF2C 2013, LNICST 132, pp. 247–251, 2014.
DOI: 10.1007/978-3-319-14289-0_17

2 Related Work

In this paper we have mainly focused on 3 different techniques to use various browsers without leaving activity traces on the host's hard disk. We could have chosen any browser for experimental purposes, but our main focus was on these techniques, so we chose only one browser, Mozilla Firefox, due to its worldwide popularity. Here we will first discuss all these three techniques in brief and how can they serve as anti-forensics mechanisms.

A **sandbox** is an isolated environment initially used by software developers to test new programming code. Various software products like *Sandboxie* [1] can now be used to create isolated environments for general users. It allows various computer programs to run in an isolated environment and prevent them from making any permanent change to other programs and data in computer. Once Sandboxie is closed along with the program running within it, it will automatically dump all the changes made by that program in such a manner that they will not be reflected anywhere else in the computer. By using a sandbox environment one can avoid leaving various activity traces like browsing history, cookies, cache, temporary files and many more. For this experiment's purposes, we used the tool Sandboxie version 3.76.

Portable software is an executable program that runs independently without any need for installation on the host computer's hard disk drive. These kinds of applications can be stored on removable storage media such as USB flash drives or portable hard disks. After storing a portable application on a portable device it can be used on any number of compatible machines. These applications do not leave program files or data on the host system. Generally they also do not write to the Windows registry or configuration files of the user's profile on the host system. There are lots of portable tools available on the Internet for various functions. For our experiment we used *Firefox Portable* [2] for web browsing.

A **virtual machine (VM)** is essentially a simulation of a computer within a physical computer. A VM is a computer application which creates a virtual environment which allows a user to run any number of operating systems on a single computer at the same time. A VM can be carried on removable media and can be accessed on nearly any computer. These VMs can be encrypted and disposing of them is a very easy task compared to disposing of a physical computer. When a person wants to carry out any malicious activity, it is possible to simply setup a VM and perform all activities using this VM only [3]. Thus by using virtual machines and disposing of them successfully, one can avoid creating almost all of the artifacts that could be used to prove a crime had taken place.

In recent years, some papers have been published which use advanced forensics analysis to discover evidence left behind despite the use of various anti-forensic techniques. Said et al. [4] uses RAM forensics to find traces of activities done in private browsing mode while [5] uses advanced forensics to find out the password of an encrypted volume by analyzing the hibernation file. To the best of our knowledge nobody has addressed the issue of all three of the techniques we employ in this paper so far. This is the first attempt to address such kinds of anti-forensic mechanisms by investigating the artifacts left by using these modes.

3 Investigation Methodology

This section describes the tests that we conducted on the three different anti-forensics usage scenarios. We used three workstations with the same hardware and software configuration. To perform the experiments we used an IBM compatible PC with an Intel Core i5 CPU, 4 GB RAM and 160 GB hard disk running Windows 7 Professional and the NTFS file system. We used various software products including- Sandboxie V3.76, Mozilla Firefox 20.0, FTK Imager Lite 3.1.1.8 for capturing physical memory (RAM), Hex Workshop 6.7 for analyzing RAM, Encase 7.06 for advance analysis and Oracle VirtualBox V4.1.18 to create a virtual machine.

On workstation one, we installed Sandboxie, on the second workstation, we used a portable version of Mozilla Firefox hosted on a USB drive and on the third workstation, we created a Windows 7 virtual machine using Oracle VirtualBox. We then performed the same Internet activity on all three machines using Firefox.

For experimental web browsing activity, we made a small list of URLs (to be entered in browser's address bar) and keywords (to be used as search queries in different search engines) to be entered in the web browsers on all three workstations. Table 1 shows the lists of URLs and keywords that we used for experiments.

Table 1. Unique URLs and keywords used in our experiments.

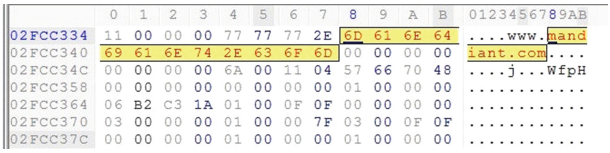
URLs	Keywords
Mandiant.com	Secret123—google.com
Osforensics.com	Artifactsinv—yahoo.com
Isro.org	Kammaro – bing.com

After performing these experiments, we terminated the respective mode and then for each session, physical memory (RAM) was captured using FTK Imager and finally images of the complete hard disks were captured using Encase for further analysis.

4 Evidence Analysis and Results

For all three techniques, we started our analysis by examining the artifacts in common places [6] for web browsing history. In all cases no traces were found in these common places. Next we searched for evidence using Hex Workshop on physical memory (RAM) that we captured during experiments. We did a string search of all the URLs and keywords used in experiments and we were able to find various instances of each URL and Keyword of all browser activities for all three cases. For example, in the case of *Sandboxie,* we found 7 entries for the URL "mandiant.com" and 16 entries for the keyword "Secret123". In the case of "Portable mode", we were able to find 19 entries for the URL "osforensics.com" and 12 entries for the keyword "Artifactsinv". In comparison to the other two modes, for the "virtual machine mode", the numbers of hits were very large in the RAM capture. For example, we were able to find 94 hits for the URL "isro.org" and 260 entries for the keyword "kammaro" and 592 entries for "secret123". For all three cases we were also able to retrieve blocks of HTML code from the web sites we visited.

Finally Encase was used for forensics analysis of the captured image of the hard disk. In the case of "Sandboxie", we were able to find various hits at different locations on the hard disk. Some URL entries were also retrieved from *pagefil.sys*. Also entries of URLs and keywords used during tests were also found in many files such as some *dat* files, *lex* files and some other files. It appeared to us that during sandbox mode web pages and cache files are stored on the hard disk and then deleted once the sandbox environment is terminated. Thus the files still reside on the hard disk and could be recovered until they are overwritten. For "Portable mode", again several traces, scattered all over the hard disk were found. We were able to get the search hits for the entered URLs and keywords from various kinds of files such as.*dat, MFT*, *pagefil.sys*, *hiberfil.sys*. Finally for "VM mode", we found various evidence scattered all over the hard disk, but most hits for URLs and keywords were in unallocated clusters. Figures 1 and 2 demonstrate some of our findings.



	0	1	2	3	4	5	6	7	8	9	A	B	0123456789AB
02FCC334	11	00	00	00	77	77	77	2E	6D	61	6E	64	....www.mand
02FCC340	69	61	6E	74	2E	63	6F	6D	00	00	00	00	iant.com....
02FCC34C	00	00	00	00	6A	00	11	04	57	66	70	48	....j...WfpH
02FCC358	00	00	00	00	00	00	00	00	01	00	00	00	....
02FCC364	06	B2	C3	1A	01	00	0F	0F	00	00	00	00	....
02FCC370	03	00	00	00	01	00	00	7F	03	00	0F	0F	....
02FCC37C	00	00	00	00	01	00	00	00	01	00	00	00	....

Fig. 1. "Mandian.com" found in RAM in "Sandboxie" case

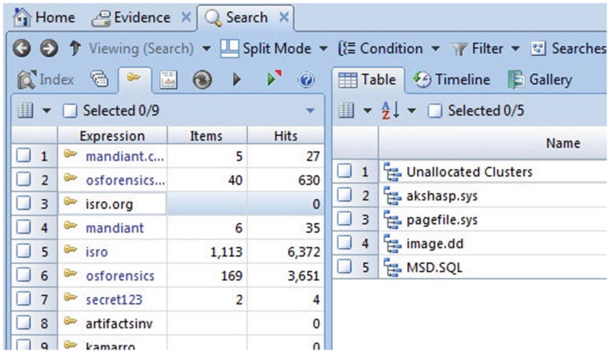


Fig. 2. Evidences in the Encase in "Portable mode" case

For common storage location analysis, no traces for any activity were found for any of the three modes. All of our findings are summarized in Table 2 such that we can also compare the results. RAM forensics and Encase forensics provided a good number of traces. Browsing within a virtual machine leaves the most number of traces in RAM, as shown in the results, while the sandbox environment leaves a lesser quantity of traces in RAM. With the help of Encase, we were able to find a good number of traces for all three usage scenarios in different locations on the hard disk.

Table 2. Summary of Results

Mode	Analysis of physical memory	Advanced analysis using the Encase
Sandboxie	- 7 entries for "mandiant.com" - 6 entries for "isro.org" - 1 entries for "osforensics.com" - 16 entries for "secret123" - 12 entries for "kammaro" - 18 entries for "artifactsinv"	- Results were scattered all over the hard disk in different files, including .dat, .lex, pagefile. sys and many more. -We were able to reconstruct pages partially
Portable	- 58entries for "mandiant.com" - 8 entries for "isro.org" - 19 entries for "osforensics.com" - 151 entries for "secret123" - 18 entries for "kamarro" - 12 entries for "artifactsinv"	-Results were scattered all over the hard disk in different files, including .MFT, hibefil.sys, pagefi-le.sys and many more -We reconctructed few page partially
Virtual Machine	- 401 entries for "mandiant.com" - 94 entries for "isro.org" - 70 entries for "osforensics.com" - 592 entries for "secret123" - 260 entries for "kammaro" - 136 entries for "artifactsinv"	-Results were scattered all over the hard disk in different files, mostly in unallocated clusters

5 Conclusion

The results presented in the paper suggest the level of isolation and privacy provided by the tested techniques are sufficient for an average user. No traces should be found in common storage locations for any web browser activity if a user decides to work in any of these three modes. However, complete isolation does not occur, and significant amounts of data are dumped into the main memory (RAM) as well as in various files and unallocated clusters on the hard disk. This could help forensic examiners investigating a case where suspected malicious browsing activities were performed using these modes.

References

1. Sandboxie. http://www.sandboxie.com
2. Firefox portable. http://portableapps.com/apps/internet/firefox_portable
3. Bares, R.A.: Hiding in a virtual world: using unconventionally installed operating system. In: International Conference on Intelligence and Security Informatics, pp. 276–284 (2009)
4. Said, H., Al Mutawa, N, Al Awadhi, I.: Forensic analysis of private browsing artifacts. In: International Conference on Innovations in Information Technology (IIT), pp. 197–202 (2011)
5. Mrdovic, S., Huseinovic, A.: Forensic analysis of encrypted volumes using hibernation file. In: 19th Telecommunications Forum (TELFOR), pp. 1277–1280 (2011)
6. Oha, J.J., Leeb, S., Leea, S.: Advanced evidence collection and analysis of web browser activity. Digital Invest. **8**, 62–70 (2011)