Do Private and Portable Web Browsers Leave Incriminating Evidence?

A Forensic Analysis of Residual Artifacts from Private and Portable Web Browsing Sessions

Donny Jacob Ohana
Sam Houston State University
Huntsville, TX, USA
djo007@shsu.edu

Narasimha Shashidhar
Sam Houston State University
Huntsville, TX, USA
karpoor@shsu.edu

***Abstract*— The Internet is an essential tool for everyday tasks. Aside from common usage, users desire the option to browse the Internet in a private manner. This can create a problem when private Internet sessions become hidden from computer investigators in need of evidence. Our primary focus in this research is to discover residual artifacts from private and portable browsing sessions. In addition, the artifacts must contain more than just file fragments and enough to establish an affirmative link between user and session. Certain aspects of this topic have triggered many questions, but there have not been enough authoritative answers to follow. As a result, we propose a new methodology for analyzing private and portable web browsing artifacts. Furthermore, our research will serve to be a significant resource for law enforcement, computer forensic investigators, and the digital forensics research community.**

Keywords- Private Browsing; Portable Browsers; Untraceable Browsing; Secret Browsing; USB Browser; Browser Artifacts; Internet Forensics; RAM Analysis.

1. INTRODUCTION

In the last 20 years, the Internet has become drastically essential for everyday tasks associated with stationary and mobile computer devices. Aside from common Internet usage, users desire privacy and the option to browse the Internet in a private manner. As a result, new web browsing features were slowly developed for all major web browsers, asserting the option of "private browsing". This method works by either removing information at the end of a private session, or by not writing the data at all. Other private browser features may include hiding additional information, such as concealing cookie discoverability from websites.

According to one study on private browsing modes [1], there are two essential private browsing objectives. The first is to allow users to browse the Internet without leaving any traces on machines. The second is to allow users to browse the Internet while limiting identity discoverability to website servers. While both of these goals are important, our research will focus on discovering information from local machines, since the majority of computer investigations tend to stem from search and seizure of local storage devices. One alternative to using private browsing modes is to surf the Internet using a portable web browser, such as one stored on a USB flash drive. Browsing sessions are therefore more likely to be stored on a portable storage device instead of a computer.

Artifacts from private and portable browsing sessions such as usernames, electronic communication, browsing history, images, and videos, may contain significant evidence to a computer investigator. Prior research in this area is very limited. Referring back to one of the main studies on private browsing forensics [1], this research lacks an in-depth analysis of deleted and volatile information pertaining to private browsing sessions. In regards to another study focused on portable web browsers [3], many statements were made without the basis of true experimental findings. Furthermore, there are virtually no published studies on residual artifacts from current portable web browsers existing on host machines. In the past, similar studies have been conducted on the SanDisk U3 flash drive and its portable applications. Since U3-USB devices had a pre-installed read-only partition, it was challenging for forensic investigators to discover electronic evidence. In the latter year of 2009, SanDisk began phasing out support for U3 Technology and it has been discontinued because of many irresolvable issues [6].

Forensic examinations of private and portable web browsing artifacts are extremely valuable. Prior research either lacks significant findings or does not provide sufficient answers. We plan to overcome these shortcomings by analyzing both allocated and unallocated space on entire disks, while measuring our results against multiple browsers. Furthermore, we plan to analyze any volatile data that would be available in a common incident response setting.

This paper is organized as follows: Section 2 describes prior and related work in private browsing modes and portable web browsing. Section 3 discusses the four major browsers and their privacy capabilities. Section 4 discusses several different portable browsers. Section 5 details the implementation and experiments. Section 6 and 7 conclude the paper with some open questions, future work and discussion.

2. RELATED WORK

2.1 PRIVATE BROWSING

In a study on private browsing modes in modern browsers [1], the researchers presented a list of inconsistencies between

DOI 10.1109/SPW.2013.18

private browsing goals and browser implementations. They also defined private browsing modes to have two primary goals: privacy against the web and privacy against local machines. Meaning, the user's identity should not be identified over the Internet (web), and the user's activity should not be recorded on the machine (local). One example is that Mozilla Firefox and Google Chrome both take steps to remain private against websites during private mode. Apple Safari on the other hand only protects against local machines.

The researchers [1] also found that all tested web browsers failed in one way or another, in regards to private browsing policies. This is mainly because browser plug-ins and extensions introduce complications to private browsing sessions. They also showed that many browser extensions weaken private browsing modes and therefore user activities can still be recorded. One example is that Google Chrome disables all extensions during private browsing and Firefox does not. With regards to inconsistencies within a single browser, the researchers found that cookies set in public mode in Firefox 3.6 are not available to the web when browsing privately, however SSL certificates and passwords are.

Ultimately, this study [1] establishes a good foundation for private browsing analysis but lacks significant findings. Primarily, they studied browser policy inconsistencies, browser extension weaknesses, private browsing usage, website user discoverability, and Firefox vulnerabilities. They specifically ignore volatile memory artifacts because they wanted to show discoverability after the memory was cleared. However, a small experiment was conducted and after running a memory leaking program, certain artifacts from private browsing sessions were discovered in the memory. The reason for this was explained that Operating Systems often cache DNS resolutions, and therefore by analyzing the cache and TTL values, an investigator can learn if and when the user visited a particular site. In addition, the Operating System can swap memory pages leaving further traces of user activity.

In contrast to this research, we plan to examine all four major web browsers utilizing a different acquisition method. Our goal is to extract as much data as possible, including deleted and volatile data, to obtain sufficient information within the artifacts retrieved. This research [1] points out various files and folders that are privately modified and accessed, but they do retrieve any specific data that is deleted after a private session is terminated. One research article [2] argues that browser vendors deliver exactly what they claim but consumers have limited knowledge as to what private browsing modes can actually do. Comparing this article to the first study [1] proves otherwise. There are clearly private policy inconsistencies within the four major browsers.

2.2 Portable Web Browsing

One study on portable web browsers [3] explained that portable web browsing artifacts are primarily stored where the installation folder is located (removable disk). Residual artifacts, such as USB identifiers and portable programs, can be discovered by analyzing the Windows Registry and Windows Prefetch files. Furthermore, they state that if the removable disk is not accessible to the investigator, it is *impossible* to trace further information. In regards to portable software discoverability, the researchers stated that it was difficult to determine portable web browser usage on host machines. The majority of these statements were made without the basis of any true experimental results. Therefore, every one of these statements will be fully tested in our research to determine authoritative answers. We plan to recover significant residual artifacts located on host machines, testing several different portable web browsers. Even though USB identifiers are important to obtain, it is even more important to establish an affirmative link between the user and session activity.

2.3 U3 Flash Drive

In comparison to current portable software, Sandisk and Microsoft worked together many years ago on a project called U3 Technology [10]. Essentially, the idea was to allow consumers to carry a portable disk containing personalized files and web browsers. U3 flash drives were pre-installed with a U3 Launchpad, similar to an OS start menu and installed programs. There are two partitions to the U3 flash drive structure: one being a mass storage device and the other a virtual CD-ROM. The virtual partition was actually an .ISO image, which was why information was read but not written to the disk. According to one study [4], U3 devices created a folder on host machines and recorded user activity. Once the disk was ejected, a cleanup program was executed and automatically removed all the user activity from that system. By analyzing the Windows Prefetch files, researchers were able to identify which programs were run from the U3 device.

In another study on battling U3 anti-forensics [5], U3 identifiers were discovered also by analyzing the Windows Registry and Prefetch files. It seemed as if though the majority of traces were located within slack space and free space of the hard drive. For this reason, our research experiments will be conducted using separate physical hard drives to incorporate the possibility of discovering slack space/file slack data. Even though sufficient evidence was obtained to support which U3 programs were launched, it was still extremely difficult for researchers to identify other significant artifacts. These difficulties are very similar to the obstacles we will face in our research. Overall, the U3 portable disk provided a sense of privacy and personalization to users. Over time, there had been been numerous complaints about U3 devices, such as potential incompatibility with embedded equipment and malware-like behavior. SanDisk began phasing out support for U3 Technology in late 2009 [6] and essentially the U3 disk has been discontinued.

3. Major Browsers and Private Browsing

In this section, we discuss four major web browsers that are tested in this research and their private browsing implementations.

3.1 Microsoft Internet Explorer

Microsoft IE offers users a private browsing feature called InPrivate Browsing. According to Microsoft [8], InPrivate

Browsing enables users to surf the Internet without leaving a trace on their computer. However, while using InPrivate Browsing, some information such as cookies and temporary files are temporarily stored so that webpages will work correctly. Once the browsing session is ended, all of that data is discarded. In regards to browser extensions, IE disables all toolbars and extensions during InPrivate Browsing sessions to ensure better privacy. IE also does not clear anything regarding toolbars and extensions after a private session is ended.

3.2 Google Chrome

Google Chrome offers something called Incognito mode for users to browse the Internet in a private session. According to Google [7], Incognito mode does not record any browsing or download histories and any created cookies will be removed upon exiting a session completely. Additionally, Google states that if users are working in Chrome OS, surfing the Internet using guest browsing essentially does the same thing. Once the guest session is closed, all browsing information is completely erased.

3.3 Mozilla Firefox

Mozilla Firefox offers a discreet browsing mode called Private Browsing. According to Mozilla [9], Private Browsing allows users to surf the Internet without saving any information about visited sites or pages. Mozilla does make it clear as some of the other web browsers do that private browsing modes do not make users anonymous from web sites, ISP's, and networks. In other words, Private Browsing is merely affected in the Application Layer recognized in the OS. Aside from other privacy features, there is an option to enable the Do-Not-Track feature in Firefox, which requests that websites do not track user browsing behavior. This request is honored voluntarily and Apple Safari offers the same. In the experimental phase of our research, these types of features will be optimized for full privacy.

3.4 Apple Safari

The Apple Safari web browser is primarily used on Apple OS machines but is also available for Windows. Apple's latest version of the Safari web browser for Windows is Safari 5.1.7 [11]. When Safari launched 6.0, they did not update the Windows versions. Most people have assumed that Apple is going to move away from Windows compatibility. According to Apple, when using Private Browsing mode in Safari, webpages are not added to the history list, cookie changes are discarded, searches are not added to the search fields, and websites cannot modify information stored on the computer.

4. Portable Software

In this section, we discuss several major web browsers that are made available in portable formats and were used for this research.

4.1 Portable Application and Browsers

To allow for certain portable browsers to work, a free program called PortableApps [12] was used for this research. PortableApps is similar to the previously mentioned U3 Launchpad, in that it allows you to take portable applications with you as you go. It is a fully open source platform and will work with almost any portable storage device. In our study, the application was installed on a USB flash drive. Three portable web browsers were selected through PortableApps: Mozilla Firefox Portable 18.0.1 [13], Google Chrome Portable 24.0.1312.52 [14], and Opera Portable 12.12 [15]. The reason Apple Safari Portable was not selected was because it was not in fact portable. The most updated version that was located was not a standalone executable program and it had to be installed onto the machine. According to Mozilla, the Portable Edition leaves no personal information behind on the machine it runs on [13]. All the portable browsers were essentially designed for users to carry their customized browsers without leaving traces on host machines. That is why artifacts such as web browsing history, passwords, and autofill forms, are stored where the portable browser installation folder is located. Privacy modes can also be enabled to help block flash cookies and other artifacts from storing within the installation folder.

5. Implementations and Experiments

In this section, we provide a brief overview of several private and portable browsing sessions that will be analyzed using computer forensics.

5.1 Tools and Setup

The following tools were used for the assessments, acquisitions, examinations, and analysis:

Hardware:

- 1- Desktop (PC- forensic workstation- 4GB RAM)
- 8- 160GB SATA Hard Drives (one dedicated drive)
- 1- USB Flash Drive (8GB)
- 1- USB External Drive (1TB WD Passport)
- 1- SATA to USB Adapter
- 1- Tableau USB Write Blocker (IDE/SATA)
- Antistatic Bags and Antistatic Wrist Strap

Software:

- Microsoft Windows 7 Professional (64)
- Internet Explorer, Firefox, Safari, Chrome
- VMware- virtualization software
- DaemonFS- file integrity monitoring program
- Disk Wipe- to replace all data on disk with zeros
- Nirsoft Internet Tools- history, cache, and cookie viewers
- PortableApps- portable application Launchpad
- Firefox Portable, Chrome Portable, Opera Portable
- FTK Imager- used to create forensic images
- FTK Imager Lite- portable version
- AccessData FTK version 3.2 (Licensed)- used to analyze forensic images and organize information

The key to our research was for us to conduct a standardized test across multiple controlled environments. Therefore, all the experiments were handled in a forensically

sound manner and as if we were handling real evidence. Photographs were taken, forensic images were created, procedures were properly documented, and evidence was safely preserved.

We began by taking every SATA hard drive and removing residual data using Disk Wipe [17]. Each disk was connected to the forensic workstation through a SATA to USB Adapter. The Disk Wipe tool provides several different wiping options and writes over with zeros. The first disk was tested by examining it forensically after wiping it with only one pass. Since there was some residual data that was found, a DoD Algorithm was selected next to wipe the disk using 3 passes; this method proved to be more efficient. After every disk was successfully wiped, each one was installed with Windows 7 Professional- 64bit. The 64bit version was used so that more RAM could later be tested.

Next, each disk was installed with only one specific Internet browser, pre-loaded from an external hard drive (WD Passport), except for the portable browsers. The web browsers installed were Microsoft Internet Explorer, Mozilla Firefox, Apple Safari, and Google Chrome. Each browser was configured to launch automatically into private mode except for Safari, which had to be done manually. It is important to note that since prior research [1] showed that browser plug-ins and extensions cause weakness to private browsing sessions, none were installed. It is also important that everything was pre-configured before connecting any of the drives to the Internet.

5.2 Preliminary Analysis

While the disks were being properly developed, a baseline was established using VMware and a file integrity monitoring program called DaemonFS [18]. This assisted with having a general idea for which areas were modified and accessed during normal, private, and portable browsing sessions. Once DaemonFS was launched, it was set to monitor all activity within the local hard drive (root). After the logical parameter was set, each web browser was individually launched and tested using a series of standardized steps. These steps included article searches, image searches, video searches, email account logins, bank account logins, and online purchase attempts. See Figures 1, 2, and 3 for results.

Browser	Primary Changes
Internet Explorer 8.0	Temp File Directory files (Content.IE, History.IE5, Cookies, Recovery, Custom Destinations, Index.dat) are created, modified, and deleted.
Google Chrome 23.0.1271.95	Directory Chrome\User Data (Safe Browsing Whitelist, Default\ Cache, Current Session, Default\History, Default\Session Storage) files are created, modified, and deleted.
Firefox 17.0.1	Directory Firefox\Profiles (Cache, jumpListCache, etc) and Win CustomDestinations, files are created, modified, and deleted
Safari 5.1.7	Directory AppleComputer\Safari (Cache, History, Webpage Previews, Cookies, WebpageIcons.db) files are created, modified, and deleted

Fig. 1 Browser Analysis during Normal Browsing Sessions

Private Browser	Noticeable Changes
IE InPrivate Browsing	Everything gets deleted when exiting the browser and the entire session is terminated
Google Chrome Incognito Mode	Safe Browsing databases, Cookies, and History are modified, no changes during session but the chrome_shutdown_ms.txt is replaced with a new timestamp when session ends
Firefox Private Browsing	Safe Browsing database gets modified, nothing appears to be written while surfing, but when session ends, some Firefox\Profile files are modified
Safari Private Browsing	Only NTuser.dat appears to be modified

Fig. 2 Browser Analysis during Private Browsing Sessions

Portable Browser	Host Machine Activity
Opera Portable	Temp files appear to be created on disk and then are deleted when session ends
Firefox Portable	Mozilla\Roaming directory was modified, and a few temp files under Local AppData were created/deleted
Google Chrome Portable	Folder called GoogleChromePortable had files created, modified, and deleted, including Sys32\Winevt\Logs, and Portable Chrome Cache
Safari Portable	Setup files are portable but must be installed on system (not standalone.exe) therefore will not be used for testing

Fig. 3 Browser Analysis using Portable Web Browsers

5.3 Private Browsing Experiments

To begin the main experiments, each disk was separately utilized as a single primary drive. Every step was manually recorded with specific timestamps for future reference points. For the first four disks, only private browsing sessions were tested on the installed web browsers. For the purpose of these experiments, a "browsing session" will refer to all activity conducted on one specific browser. Once a private browsing session was launched, the same series of steps were performed for each browser, such as: searching for articles on hacking, searching for different images and videos, logging into different email accounts and sending attachments; logging into bank accounts, attempting to purchase large quantities of ammunition, searching to purchase stolen property, and viewing different criminal-related websites. These activities were performed using different search engines such as Yahoo! and Google. Furthermore, these activities were selected and tailored from real scenarios that would have created an alarming response.

After each browsing session was complete, the web browser process tree was terminated (verified) and the RAM was dumped into a file using FTK Imager Lite (installed on USB). Not only was the memory dumped, but Registry files were obtained, the pagefile.sys was extracted, and an .ad1 image file of the RAM was created as well. The location of these files was stored on the target machine's Desktop due to reasons that will later be explained. Initially, the data was extracted to an external hard drive. The machine was then unplugged from the back and the disk was carefully removed. As noted, a few extra things were done to preserve sound results. The working memory was dumped before and after

every disk session, to ensure that residual data was not left over in the RAM from the session before. In addition, several Internet tools from Nirsoft [16], such as cache viewer, history viewer, and cookie viewer, were executed after each browsing session was terminated and yielded negative results. Meaning, nothing could be discovered using these tools after private browsing sessions were used.

5.4 Portable Browsing Experiment

The next three disks were used in conjunction with portable web browsers running from a USB flash drive. The flash drive was installed with a program called PortableApps. Essentially, PortableApps allows you to run different programs from a flash drive, similar to an OS Start menu. After setting up the Launchpad, three portable browsers were installed on the flash drive: Mozilla Firefox Portable, Google Chrome Portable, and Opera Portable. Again, each hard disk was separately used as a primary hard drive but this time without any regular web browsers installed. Each portable browser was individually launched while performing the same series of standardized steps as the first four disks. Whenever a disk was complete, it was carefully placed into an antistatic bag and into a cool dry place for storage. In addition, an antistatic wrist band was used while handling all internal electronic components.

5.5 Forensic Acquisition and FTK Analysis

The last hard disk was developed with Windows 7 and FTK 3.2 to make it a complete computer forensic workstation. AccessData's Forensic Toolkit (FTK) [19] is a court accepted program used for examining computers and mobile devices at the forensic level. Each disk was individually connected to the Desktop through a Tableau USB hardware-based write blocker. This was used to protect any data on the hard drive from being altered by the computer. Digital evidence preservation is the most important factor next to chain of custody, when it comes to forensic integrity. Using FTK Imager, a bit stream image of each evidence disk was created as a compressed .E01 image file, and was verified through several different hashes. Each image took anywhere from 3-5 hours to complete. Next, each image was forensically examined, analyzed, and classified by FTK 3.2. Each disk image took anywhere from 6-72 hours to process. The disks with the installed browsers took the longest. Aside from default FTK analysis options, additional refinements were selected to carve different types of data and parse complex information. Once FTK finished processing the evidence files, numerous hours were spent sifting through the data. See figures 7 and 8 for complete results.

5.6 Result Analysis

As we can see from the results, private browsing modes and portable browsers do in fact leave incriminating evidence, but it depends on the browser. Some browsers left enough information to establish an affirmative link and some did not. Out of the four major browsers that were installed and tested, Internet Explorer provided the most residual artifacts but not where artifacts are typically located. This was fairly consistent with all the browsers. For example, the Index.dat (history) and Registry>TypedURLs were empty. We recovered virtually all cached images, URL history, and usernames with their associated accounts. Everything was recoverable except for playable videos. Most of the data was recovered from free space and slack space areas. Similar data was also recovered from the memory dumps. In regards to indicators, there were a few areas where "InPrivate" and "Start InPrivate Browsing" were noted prior to URL and file history.

The three remaining browsers were a little more difficult to recover residual artifacts from. It appeared that the overall best way to recover residual data was to obtain the evidence from RAM or working memory, but that is not always possible for investigators. For Google Chrome Incognito artifacts, there were many browsing indicators and changes in timestamps to show Chrome usage. However, it was difficult to establish an affirmative link between the user and session because none of the usernames and other history information was accessible; the same resulted for Mozilla Firefox. In both of these cases, any documents that were temporarily opened from the Internet were recoverable. This information is important because browsing indicators, along with certain timestamps, may be used to explain why something is not there such as URL history. For example, if a live search using regular expression patterns was used to locate one of these hidden artifacts, an investigator can now understand why there were no hits under common areas.

Apple Safari seemed to fall in the middle by keeping most things private while still leaving traces on the machine. The easiest way to view the browsing history for Safari private browsing sessions was to locate the "WebpageIcons" database under Safari artifacts. This database provided a good log of every visited URL along with other pertinent information. It is important to note that this can be used to explain to courts as to why URL history would be located there and nowhere else under Safari data.

With regards to residual portable browsing artifacts, it appeared that everything was just as easily obtained from the memory dumps as it was with the installed browsers. However, not everything was located on the target hard drives. Out of the three portable browsers tested, Google Chrome Portable left the most residual artifacts on the host machine. The recovery almost seemed as if Chrome was fully installed on the machine itself. Everything including images, browsing history, browsing method, and usernames with associated accounts, were located on the disk. This is important because the recovered artifacts were obtained without the flash drive. It is important for an investigator to distinguish that these artifacts came from Chrome Portable for two reasons: one is so that it can be explained as to why Google Chrome artifacts are not located under common areas, and second is to alert the investigator that further evidence may be linked to a flash drive that the investigator did not originally consider.

Opera Portable on the other hand, did not leave as much information as Chrome. There were many portable browsing indicators but most history artifacts were limited; none of the

Microsoft Internet Explorer 8.0- InPrivate Browsing		
Artifacts	***Discovered***	***Target Locations***
Private Browsing Indicator	✓	Memdump; Free/Slack Space ("Start InPrivate Browsing"- prior to URL history); $I30 (…\Content.IE5- "inprivate[1]"- prior to list of *.jpeg's); Pagefile;
Browsing History	✓	Memdump; Free space; File slack (Temporary Internet Folder, Roaming\...\Custom Destinations); SysVol Info; $LogFile; $J; AppData\...\IE\Recovery\Active;
Usernames/ Email Accounts	✓	Memdump; Freespace; Temporary Internet Folder; User\ AppData…\IE\Recovery\Active
Images	✓	Memdump (partial photos); Free space (full content); File slack (full content);
Videos	✗	N/A
Google Chrome 23.0.1271.95- Incognito		
Artifacts	***Discovered***	***Target Locations***
Incognito Indicators	✓	Memdump; Chrome\...\Installer\chrome.7z & chrome.dll (timestamp matches); $I30 (safebrowsing timestamp) AppData\Local\Google\Chrome\User Data\chrome_shutdown_ms.txt (always updates with timestamp); AppData\Local\Google\Chrome\User Data\Default\Extension State*.log (declarative_rules.incognito.declaritiveWebRequest- timestamp matches session start); ~\SysVol Information (new incognito window with timestamps); AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations (new incognito window with timestamps); Chrome\UserData\Safebrowsingcookies.db (modified timestamp)
Browsing History	✓	Memdump; SysVol Info (matching timestamps); Pagefile.sys (downloaded file);
Usernames/ Email Accounts	✗	N/A
Images	✓	Carved from Memdump (Mostly partial images)
Videos	✗	N/A
Mozilla Firefox 17.0.1- Private Browsing		
Artifacts	***Discovered***	***Target Locations***
Private Browsing Indicators	✓	Memdump (browsing mode); SysVolume Information (Enter Private Browsing and Window's User listed below- file timestamp accurate)
Browsing History	✓	Memdump; Free space- AppData\...\Temp; Win\Prefetch (.rtf temp file download discovered); AppData\...\Firefox\Profiles (blacklist.xml- matching timestamps); Firefox\Profiles\ (file timestamps update)
Usernames/ Email Accounts	✗	N/A
Images	✓	Carved from Memdump (Mostly partial images)
Videos	✗	N/A
Apple Safari 5.1.7- Private Browsing		
Artifacts	***Discovered***	***Target Locations***
Private Browsing Indicators	✓	Memdump; ~\SysVol Information (com.apple.Safari.PrivateBrowsing timestamp)
Browsing History	✓	Memdump; Free/Slack Space (URL History); AppData\Local\AppleComp\Safari\WebpageIcons.db>>tables; AppData\Local\AppleComp\Safari\ (databases timestamp updates) AppData\...\AppleComp\Safari & Preferences\(several *.plist timestamp updates) Pagefile (URL's and modified timestamps update)
Usernames/ Email Accounts	✗	N/A
Images	✓	Carved from Memdump (Mostly partial images)
Videos	✗	N/A

Fig. 4 Private Browsing Results

Google Chrome Portable		
Artifacts	***Discovered***	***Locations***
Browser Indicators	✓	NTFS Allocated and Unallocated Space; Prefetch; Pagefile; Memdump; $Logfile; Users\AppData\Roaming\Microsoft\ Windows\Recent\CustomDestinations; ~\System Volume Information; AppData\Local\Temp; AppData\LocLow\Mic\CryptnetUrlCache; Win\AppCompat\Prog\RecentFileCache; Win\Mic.NET\Framework\log (fileslack); Win\Sys32\LogFiles\WUDF\ (fileslack)
Browsing History	✓	NTFS Allocated and Unallocated Space; Memdump; Orphan Directory; Pagefile; Users\AppData\Roaming\Microsoft\ Windows\Recent\CustomDestinations (Carved .lnk)
Usernames/ Email Accounts	✓	[Orphan] directory and NTFS Unallocated Free/Slack Space
Images	✓	Carved (NTFS Unallocated Space and Orphan Directory)
Videos	✗	N/A
Opera Portable		
Artifacts	***Discovered***	***Locations***
Browser Indicators	✓	NTFS Allocated and Unallocated Space; Pagefile; Memdump; $LogFile; ~\System Volume Information; NTUSER.DAT; AppData\Local\Mic\Win\UsrClass.dat; Users\AppData\Roaming\Microsoft\ Windows\Recent\CustomDestinations (Carved .lnk); Win\Prefetch; Win\Sys32\LogFiles\SQM\SQMLogger
Browsing History	✓	Memdump; AppData\Roaming\Mic\Win\Rec\CustomDestinations (Carved .lnk files with Last Access Times)
Usernames/ Email Accounts	✗	N/A
Images	✓	Carved from Memdump (Mostly partial images and difficult to view full content)
Videos	✓	N/A
Mozilla FireFox Portable		
Artifacts	***Discovered***	***Locations***
Browser Indicators	✓	Memdump; SysVol Information file timestamp (Firefox Portable appinfo)
Browsing History	✓	Memdump; SysVol Information (Email only)
Usernames/ Email Accounts	✓	Memdump; SysVol Information (Email Account History)
Images	✓	Carved from Memdump (Mostly partial images and difficult to view full content)
Videos	✗	N/A

Fig. 5 Portable Browsing Results

usernames or accounts could be recovered. Firefox Portable resulted in similar findings however, and specific user activity was found to be recoverable. All of the usernames associated with their respected email accounts were recovered along with FireFox browsing indicators.

In reference to the carved images from RAM, most of them were distorted. However, a few of the images could be seen as a whole. One solution was to try and match a distorted image from RAM with a whole image on the hard drive using FTK's fuzzy hash option. This would be a great way to link carved contraband to working memory artifacts and therefore strengthening evidence against the user. The program attempts to match files by determining a fundamental level of similarity between hashes. This

method did not always work as hoped. Some of the thumbnails stored in RAM were successfully matched with ones on disk but none specific to user activity. Perhaps on a machine with a much higher capacity of RAM, this would be more useful.

5.7 Additional Forensic Results

Aside from discovering hidden browsing artifacts, there is another finding worth mentioning due to the significance of linking users and machines. Every time the external hard drive (WD Passport) was connected to one of the machines via USB, not only did it leave unique identifiers, but a log of every folder located on the Passport was transferred automatically to the Windows machine and remained on the hard drive and RAM. For this reason, a flash drive was later used to dump the memory and preserve evidence integrity. The Passport files were discovered within several different locations on the hard drive. One was within a log file called the Circular Kernal Context Logger (BootCKCL.etl), and the other area was located within Trace*.fx files.

This finding raises a number of questions and concerns. For example, this process could violate certain policy and procedures that were considered forensically sound. On the other hand, it could provide an investigator with enough information to understand that the file paths may be pointing to an external device. So not only will information from the Registry provide unique identifiers, but this could be used to know what type of contraband may be on the "missing evidence". In addition, this information would be extremely helpful when trying to establish an affirmative link between the user and session, or user and target machine.

6. Future Work

Future work may include further RAM experiments, and more efficient methods to extract information over an extended period of time instead of one controlled browsing session. In addition, forensic tools or carving options should be developed to provide investigators on whether or not these browsing artifacts exist (0/1) and categorize them accordingly.

7. Conclusion

The majority of recovered artifacts were discovered in RAM, slack/free space, and FTK [Orphan] directories. That being said, there was still enough information to provide useful information about the user(s). Another commonality between the browsers is information contained within the System Volume Information. Our research clearly establishes authoritative answers to which were never there before. In addition, some of our authoritative results contradicts prior research statements. For example, one study [3] made the statement that it would be *impossible* to trace residual information, other than USB identifiers, if a portable storage device was not accessible to the investigator. Our research clearly shows that further data can still be recovered on host machines without the portable storage device being present. Overall, our research is a valuable resource pertaining to private and portable web browsing artifacts. Not every web browser will leave incriminating evidence but some will, depending on the situation. These residual artifacts may or may not be important to a case but on the other hand, it may be the only way to explain certain results. Computer investigators must treat computers like real crime scenes in the sense that it is not only important to document what is found, but to also document what is not present and the reasons as to why. Our research now provides another way to look at these types of findings and explain the results. We conclude that just because something is not present does not mean it never happened.

References

[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] 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.

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

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

[6] SanDisk. (2010). *U3 Launchpad End Of Life Notice.* [Online]. Available: 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] Mozilla. (2012). *Private Browsing.* [Online]. Available: http://support.mozilla.org/en-US/kb/private-browsing-browse-web-without-saving-info

[10] Wikipedia. (2013, Feb. 9). *U3.* [Online]. Available: http://en.wikipedia.org/wiki/U3

[11] Apple. (2012, July 12). *Safari 5.1: Browse Privately*. [Online]. Available: http://support.apple. com/kb/PH5000

[12] PortableApps. (2013, Feb. 1). [Online]. Available: http://portableapps.com/

[13] PortableApps.(2013 Feb. 5). *Mozilla Firefox, Portable Edition.* [Online]. Available: http:// portableapps.com/apps/internet/firefox_portable

[14] PortableApps.(2013, Jan. 30). *Google Chrome Portable.* [Online]. Available: http://portableapps. com/apps/internet/google_chrome_portable

[15] PortableApps.(2013, Feb. 7). *Opera, Portable Edition.* [Online]. Available: http://portableapps .com/apps/internet/opera_portable

[16] Nir Sofer. (2013). *NirSoft Freeware Utilities*. [Online]. Available: http://nirsoft.net

[17] Disk Wipe. (2009). *Disk Wipe*. [Online]. Available: http://www.diskwipe.org/

[18] DaemonFS. (2010, Aug. 6). *Sourceforge: DaemonFS.* [Online]. Available: http://sourceforge .net/projects/daemonfs/

[19] AccessData. (2013). *FTK*. [Online]. Available: http://www.accessdata.com/products/digital-forensics/ftk