EURASIP Journal on Information Security
a SpringerOpen Journal

RESEARCH Open Access

# Do private and portable web browsers leave incriminating evidence?: a forensic analysis of residual artifacts from private and portable web browsing sessions

Donny J Ohana* and Narasimha Shashidhar

**Abstract**

The Internet is an essential tool for everyday tasks. Aside from common use, the option to browse the Internet privately is a desirable attribute. However, this can create a problem when private Internet sessions become hidden from computer forensic investigators in need of evidence. Our primary focus in this research is to discover residual artifacts from private and portable web 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 never been enough authoritative answers to follow. As a result, we propose a new methodology for analyzing private and portable web browsing artifacts. 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 web browsers; Internet forensics; Portable browsing; Web browser artifacts; 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, people desire the option to browse the Internet while keeping their user information private. 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 concealing additional information such as cookie discoverability from websites.

According to one study [1] there are two private browsing objectives. The first objective is to allow users to browse the Internet without leaving any trace. The second is to allow users to browse the Internet while limiting identity discoverability to websites. While both of these goals are important, our research will focus on discovering information from local storage devices since the majority of computer investigations involve search and seizure of local machines. One alternative to using private browsing modes is to surf the Internet using a portable web browser, such as one stored on a Universal Serial Bus (USB) flash drive. Therefore, web browsing sessions are more likely to be stored on the portable storage device itself instead of the computer or host machine.

Private and portable web browsing artifacts, such as usernames, electronic communication, browsing history, images, and videos, may contain significant evidence to an examiner. Prior research in this area is very limited. Referring back to one of the main studies on private browsing modes [1], this research lacks an in-depth analysis of deleted and volatile information pertaining to private browsing sessions. In another study focused on portable web browsers [2], 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.

* Correspondence: djo007@shsu.edu
Department of Computer Science, Sam Houston State University, Huntsville, TX 77340, USA

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 [3].

Private and portable web browsing artifacts can be 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 web browsers. Furthermore, we plan to analyze volatile data that may be available in an incident response.

This paper is organized as follows: Section 2 provides a list of background terms. Section 3 describes prior and related work in private browsing modes and portable web browsers. Section 4 discusses the four major browsers and their privacy capabilities. Section 5 discusses several different portable web browsers. Section 6 details the implementation and experiments. Sections 7 and 8 conclude the paper with some open questions, future work, and discussion.

## 2. Background definitions

In this section, we provide a list of background terms and definitions (Table 1) to assist readers with some of the terminology used in this research.

## 3. Related work

### 3.1. Private browsing

In the study [1] on private browsing modes in modern browsers, researchers presented a list of inconsistencies between 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 takes measures to only protect against local machines, but through our research, we will exploit some of the vulnerability to that method.

The researchers found that all the web browsers (tested) failed in one way or another when analyzing policies. This is mainly because of complications introduced by browser plug-ins and extensions. It was also shown that extensions can weaken private browsing modes and therefore activities can still be recorded. One example is that Google Chrome disables all extensions during private browsing mode and Firefox does not. With regard 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 establishes a good foundation for private browsing analysis but lacks significant findings. The areas primarily studied were policy inconsistencies,

**Table 1 Terms and definitions**

| Terminology | Definition |
|---|---|
| Residual artifacts | Remaining data such as files, images, documents, and web content |
| Affirmative link | Judicially devised standard to aid Courts in determining sufficiency of evidence between subject and offense |
| ISO image | A computer file that is an exact copy of an existing file, CD, DVD, etc. |
| Virtual machine | Simulation of a real machine |
| Prefetch files (Windows) | Each time an application is run on a Windows machine, a Prefetch file referencing the loaded application is created to speed boot time |
| $I30/$MFT | New Technology File System (NTFS) Index Attribute/Master File Table |
| Browser cache | Temporary Internet files (storage) for increasing speed |
| RAM | Working memory that is volatile |
| Pagefile (paging) | Virtual memory designated on disk |
| Memdump | Action of dumping volatile memory into a file to view contents |
| Drive free space | Referencing the unallocated space on disk |
| Slack space/file slack | Unused space in a disk cluster (area between end of file and end of disk cluster) |
| System volume information | Volume shadow copy (snapshots) for system restore/backup |
| FTK orphan directory | Contains files that no longer have a parent, and the parent folder is overwritten (using $MFT as a reference) |
| Data carving | There are many different types of data carving techniques (block-based, statistical, semantic, etc.) but essentially, most data carvers extract content by looking for file headers/footers and then 'carving' data blocks in between |

browser extension weaknesses, private browsing usage, website user discoverability, and Firefox vulnerabilities. Various files and folders which were privately modified and accessed are pointed out by the researchers, but they do retrieve specific data that is deleted after a private session is terminated. Also, volatile memory artifacts were ignored because they wanted to show discoverability after the memory was cleared. When a small experiment was conducted 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. One research article [4] 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 according to the data.

### 3.2. Portable web browsing

One study on portable web browsers [2] 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 any further information. In regard to portable software discoverability, the researchers stated that it was difficult to determine portable web browser usage on a host machine. The majority of these statements were made without the basis of any true experimental findings. 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 user and session.

### 3.3. Flash drive

In comparison to current portable software, Sandisk and Microsoft worked together many years ago on a project called U3 Technology [5]. 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 with various programs installed. There are two partitions to the U3 flash drive structure: one is a mass storage device and the other is 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 [6], 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 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 [7], U3 identifiers were discovered as well by analyzing the Windows Registry and Prefetch directory. 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 data within these areas. 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. We will probably face the same barriers in our research. Overall, the U3 portable disk provided a sense of privacy and personalization to users. Over time, there had been numerous complaints about U3 devices such as potential incompatibility and malware-like behavior. SanDisk began phasing out support for U3 Technology in late 2009 [3] and the U3 disk has been discontinued.

## 4. Major browsers and private browsing

In this section, we discuss four major web browsers and their private browsing implementations.

### 4.1. Microsoft Internet Explorer

Microsoft Internet Explorer (IE) is one of the most commonly used web browsers on Windows machines. A list of areas where most IE web browsing artifacts are located is as follows:

- Cookies (Index.dat)
- History (Index.dat)
- Registry (typed URLs, search queries, auto-complete, protected storage)
- NTUSER.dat
- Temporary Internet Files and Index.dat Entries
- Downloads.

IE also 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 web pages will work correctly. Once the browsing session is ended, all of that data is discarded. Table 2 shows a list of areas affected by InPrivate Browsing and is available to the public on Microsoft's webpage. In regard to web browser extensions, IE disables all toolbars and extensions during InPrivate Browsing sessions to ensure better privacy. IE also does not clear toolbars and extensions after a private session is ended.

### 4.2. Google chrome

Google Chrome is another very popular web browser that can be found on both Windows and Mac operating systems. A list of common areas where Chrome web browsing artifacts can be located is as follows:

- JSON (JavaScript Object Notation) structure - text based open standard design for human readable data
- Downloads
- Bookmarks
- Web data
- Keyword search terms
- Keywords
- URL database
- History index (YYY-MM)
- Current and last sessions
- Top sites database
- Media cache.

Chrome also offers something called Incognito mode for users to browse the Internet in a private setting. According to Google [9], Incognito mode does not record any browsing or download histories, and all created cookies will be removed when exiting a session completely. Additionally, Google states that if users are working in Chrome OS, surfing the Internet under guest browsing essentially does the same thing. Once the guest session is closed, all browsing information is completely erased.

**Table 2 Microsoft IE InPrivate browsing features**

| Data | How InPrivate browsing affects data |
|---|---|
| Cookies | Contained in working memory but cleared after session |
| Temporary internet files | Stored on disk but deleted after session |
| Webpage history | Not stored |
| Form data and passwords | Not stored |
| Anti-phishing cache | Temporary information is encrypted and stored |
| Address bar and auto-complete | Not stored |
| Automatic cache restore | Restore is successful only if tab crashes and not entire session |
| Document object model storage | Discarded after session |

### 4.3. Mozilla Firefox

Mozilla Firefox is another popular web browser that can be found on multiple platforms. Web browsers such as Chrome and Firefox can also be found on mobile devices such as Androids, iPads, etc. A list of common areas where Firefox web browsing artifacts can be located is as follows:

- Sqlite database structure
- Prefs.js (user preferences)
- Signons.txt (encrypted data for website authentication)
- Formhistory.sqlite
- Cookies.sqlite
- Firefox cache
- Places.sqlite (bookmarks and history)
- Downloads.sqlite.

Just like all other major web browsers, Firefox offers a discreet browsing mode called Private Browsing. According to Mozilla [10], Private Browsing mode allows users to surf the Internet without saving any information about visited sites or pages. Table 3 shows a list of areas affected by Private Browsing and is available to the public on Mozilla's webpage. Mozilla makes it clear 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

**Table 3 Mozilla private browsing features**

| Data | How private browsing affects data |
|---|---|
| Visited pages | Will not be added in History menu, Library history, or other bar list |
| Form and search bar entries | Nothing entered will be saved for Form Auto-complete |
| Passwords | No new passwords will be saved |
| Download list entries | No downloaded files will be listed under Downloads |
| Cookies | Does not save |
| Cached web content | Not saved |
| Flash cookies | Latest version of Flash must be used to prevent saving |
| Offline web content and user data | Not saved |

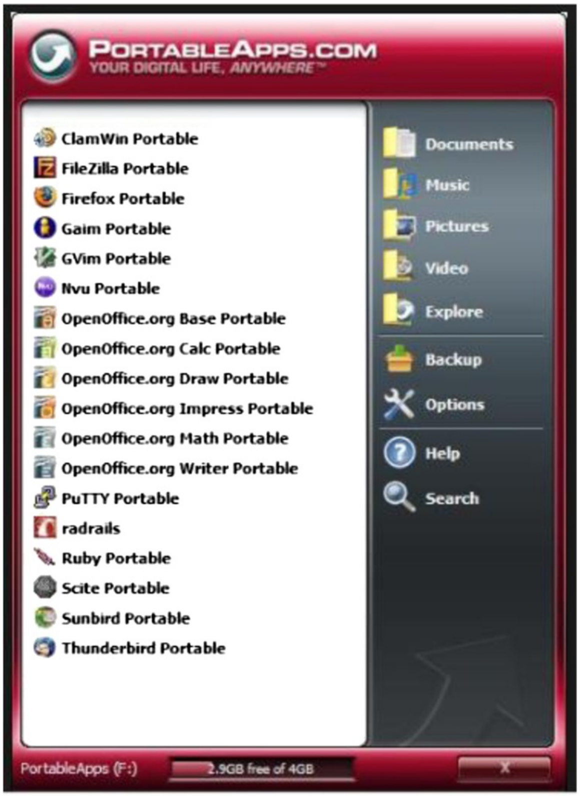


**Figure 1** PortableApps launchpad.

**Figure 2** Hard drive setup with labels.

research, these types of features will be optimized for full privacy.

### 4.4. Apple safari

The Apple Safari web browser is primarily used on Mac/iOS operating systems but is also available for Windows. A list of common areas where Safari web browsing artifacts can be located is as follows:

- .plist (Propert List) structure
- Cookies.plist
- Bookmarks.plist
- History.plist
- WebpageIcons.db
- Keychains.plist
- Downloads.plist

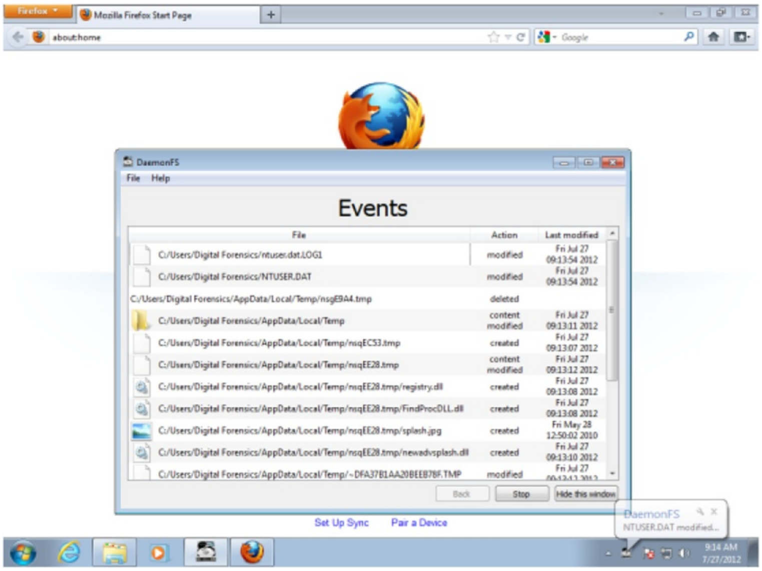
Apple's latest version of the Safari web browser for Windows is Safari 5.1.7 [11]. When Safari launched 6.0, they did not update the Windows versions. Most people have assumed that Apple is moving away from Windows compatibility. According to Apple, Private Browsing mode ensures that web pages are not 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.

## 5. Portable software

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

### 5.1. Portable application and web 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 based on an open source platform and will work with almost any portable storage device. Figure 1 shows how the launchpad is structured. 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 because it was not in fact portable. The most updated version located was not a standalone executable program and it had to be installed onto the machine. According



Events

| File | Action | Last modified |
|---|---|---|
| C:/Users/Digital Forensics/ntuser.dat.LOG1 | modified | Fri Jul 27 09:13:54 2012 |
| C:/Users/Digital Forensics/NTUSER.DAT | modified | Fri Jul 27 09:13:54 2012 |
| C:/Users/Digital Forensics/AppData/Local/Temp/nsgE9A4.tmp | deleted | |
| C:/Users/Digital Forensics/AppData/Local/Temp | content modified | Fri Jul 27 09:13:11 2012 |
| C:/Users/Digital Forensics/AppData/Local/Temp/nsqEC53.tmp | created | Fri Jul 27 09:13:07 2012 |
| C:/Users/Digital Forensics/AppData/Local/Temp/nsqEE28.tmp | content modified | Fri Jul 27 09:13:12 2012 |
| C:/Users/Digital Forensics/AppData/Local/Temp/nsqEE28.tmp/registry.dll | created | Fri Jul 27 09:13:08 2012 |
| C:/Users/Digital Forensics/AppData/Local/Temp/nsqEE28.tmp/FindProcDLL.dll | created | Fri Jul 27 09:13:08 2012 |
| C:/Users/Digital Forensics/AppData/Local/Temp/nsqEE28.tmp/splash.jpg | created | Fri May 28 12:50:02 2010 |
| C:/Users/Digital Forensics/AppData/Local/Temp/nsqEE28.tmp/newadvsplash.dll | created | Fri Jul 27 09:13:10 2012 |
| C:/Users/Digital Forensics/AppData/Local/Temp/~DFA37B1AA20BEEB78F.TMP | modified | Fri Jul 27 |

DaemonFS
NTUSER.DAT modified...

**Figure 3** **DaemonFS monitoring example.**

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 customized browsers without leaving traces on machines. That is why artifacts, such as web browsing history, passwords, and auto-fill 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.

## 6. Implementations and experiments

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

### 6.1. Tools and setup

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

***Hardware***

- 1- Desktop (PC - forensic workstation - 4-GB RAM)
- 1- Laptop (PC - forensic workstation - 6-GB RAM)
- 8–160 GB SATA Hard Drives (one dedicated drive for lab)
- 1- USB Flash Drive (8 GB)
- 1- USB External Drive (1 TB 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 data on disk with zeros
- Nirsoft Internet Tools - history, cache, and cookie viewers

**Table 4 Browser analysis during normal browsing sessions**

| 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 |

**Table 5 Browser analysis during private browsing sessions**

| Private browser | Noticeable change |
|---|---|
| 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 |

- Live View - Java based tool to convert .dd to .vmdk
- 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 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 hard drive and removing residual data using Disk Wipe [16]. Each disk was connected to a secondary forensic workstation (laptop) through a SATA to USB Adapter. The Disk Wipe tool provides several different wiping options and writes over data 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 three passes; this method proved to be more efficient. After every disk was successfully wiped, each one was installed with Windows 7 Professional - 64 bits. The 64-bit version was used so that more random-access memory (RAM) could later be tested.

Next, each disk was installed with only one specific Internet browser pre-loaded from an external hard drive, except for the portable applications. The web browsers installed were Microsoft Internet Explorer, Mozilla Firefox, Apple Safari, and Google Chrome. Each browser was configured to launch automatically into private browsing mode except for Safari, which had to be done manually. It is important to note, since prior research [1] showed browser plug-ins and extensions to cause weakness to private browsing sessions, none were installed. It is also important to note that everything was pre-configured before connecting to the Internet. Figure 2 shows the hard drives being configured and labeled.

### 6.2. Preliminary analysis

While the disks were being properly developed, a baseline was established using a laptop with VMware and a file integrity monitoring program called DaemonFS [17]. This assisted with having a general idea for which areas were modified and accessed during normal, private, and portable web 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. Figure 3 shows how the log is generated during activity. These steps included article searches, image searches, video searches, email account logins, bank account logins, and online purchase attempts. See Tables 4, 5, and 6 for results.

### 6.3. Private ate browsing experiments

Author[1] has a background in law enforcement and has experience analyzing digital media for a vast array of crimes. The Internet activities used for these experiments were adapted from an abundance of information to include past experience and knowledge. It is important to note that these principles can still be applied to all aspects of Internet forensics regardless of whether or not the scope relates to a crime. These types of browsing sessions can very well be conducted without any criminal intent. The overall purpose of digital forensics is to help establish and

**Table 6 Browser analysis using portable web browsers**

| 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 |

articulate an affirmative link between A (artifact) and B (person, place, or thing). By collecting and analyzing enough data, evidentiary content can be produced.

To begin the main experiments, each disk was separately utilized as a single primary drive. Every step was manually recorded with timestamps for future reference points. For the first four disks, only private browsing sessions were tested using the installed web browsers. For the purpose of these experiments, a ‘browsing session’ will refer to all activity conducted on one specific web browser. Once a private browsing session was launched, the same series of steps were performed for each browser. Table 7 shows the details of these standardized sessions.

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 the RAM dump was stored on the target machine's Desktop due to reasons that will later be explained. This would probably not be preferred in a real setting unless it was absolutely necessary. In any event, it is always important to document the footprints left behind on a live environment. 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 [18], 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.

### 6.4. 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 web 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 other web browsers installed. Each portable web browser was individually launched while performing the same series of standardized steps as the first four disks (Table 7). 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.

### 6.5. Forensic acquisition and analysis

The last hard disk was developed with Windows 7 and FTK 3.2 to make it a dedicated 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 using a hardware-based write blocker (Tableau), to protect any data 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 by several different hashes. Each image took anywhere from 3 to 5 h to complete. Next, individual images were forensically examined, analyzed, and classified by FTK 3.2. One disk image took up to 72 h to process and the disks with the installed browsers took the longest.

**Table 7 Internet sessions used for experiments**

| Website | Standardized steps |
|---|---|
| Google | Search for various images, sites, and forums targeted for criminal activity; click on top five links; save/download different files and images |
| Yahoo! | Search for various sites and forums targeted for criminal activity; click on top five links; save/download available files |
| YouTube | Search for how-to videos on different types hacking (social media, bank accounts, and WiFi connections); click on links to open |
| Gmail | Send email with attachments |
| Hotmail | Send email with attachments |
| Yahoo! Mail | Send email with attachments |
| SHSU Mail | Send email with attachments |
| Online Banking | Log into several accounts (stores cookies and certificates) |
| Ammunition-to-Go | Attempt to purchase large amounts (2,000+) of ammunition (various high powered rounds) by searching and adding to cart |
| Online Firearms Store | Search for high capacity magazines and various weapons |
| Craigslist | Search for different types of items for sale that might be flagged as stolen |

**Table 8 Private web browsing artifacts**

| | Artifacts | Discovered | Target locations |
|---|---|---|---|
| Microsoft internet explorer 8.0 (InPrivate browsing) | Private browsing indicator | Y | 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 | Y | Memdump; Free space; File slack (Temporary Internet Folder, Roaming\…\Custom Destinations); SysVol Info; $LogFile; $J; AppData\…\IE\Recovery\Active |
| | Usernames/email accounts | Y | Memdump; Freespace; Temporary Internet Folder; User\AppData…\IE\Recovery \Active |
| | Images | Y | Memdump (partial photos); Free space (full content); File slack (full content) |
| | Videos | N | N/A |
| Google chrome 23.0.1271.95 (Incognito) | Incognito indicators | Y | 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.declaritiveWeb Request- timestamp matches session start); ~\SysVol Information (new incognito window with timestamps); AppData\Roaming\Microsoft\Windows\Recent\Custom Destinations (new incognito window with timestamps); Chrome\UserData\Safebrowsingcookies.db (modified timestamp) |
| | Browsing history | Y | Memdump; SysVol Info (matching timestamps); Pagefile.sys (downloaded file) |
| | Usernames/email accounts | N | N/A |
| | Images | Y | Carved from Memdump (Mostly partial images) |
| | Videos | N | N/A |
| Mozilla Firefox 17.0.1 (Private browsing) | Private browsing indicators | Y | Memdump (browsing mode); SysVolume Information (Enter Private Browsing and Window's User listed below- file timestamp accurate) |
| | Browsing history | Y | 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 | N/A |
| | Images | Y | Carved from Memdump (Mostly partial images) |
| | Videos | N | N/A |
| Apple Safari 5.1.7 (Private browsing) | Private browsing indicators | Y | Memdump; ~\SysVol Information (com.apple.Safari.PrivateBrowsing timestamp) |
| | Browsing history | Y | 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 | N/A |
| | Images | Y | Carved from Memdump (Mostly partial images) |
| | Videos | N | N/A |

Aside from the default processing options in FTK, 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. We found that it was also beneficial to use a program called Live View [20] to have a better understanding of the artifacts found. Live View is an open source program that can convert a raw image to a virtual disk. The disk must be booted into safe mode for the virtual machine to work correctly without having to activate Windows. By using two screens simultaneously, one with a live virtual environment and the other with the forensic image in FTK, it allowed us to fully grasp and understand the connections. See Tables 8 and 9 for complete results.

### 6.6. Results analysis

Private browsing modes and portable web browsers do in fact leave incriminating evidence, but it depends on the browser. Some web browsers left enough information to establish an affirmative link and some did not. Out of the four major web browsers, Internet Explorer provided the most residual artifacts but not where common artifacts are typically sought. This was fairly consistent

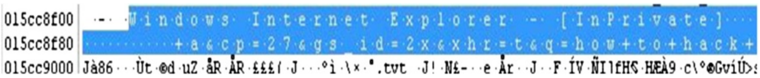
**Table 9 Portable web browsing artifacts**

| | Artifacts | Discovered | Target Locations |
|---|---|---|---|
| Google chrome portable - 24.0.1312.52 | Browser indicators | Y | 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 | Y | NTFS Allocated and Unallocated Space; Memdump; Orphan Directory; Pagefile; Users\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations (Carved .lnk) |
| | Usernames/email accounts | Y | [Orphan] directory and NTFS Unallocated Free/Slack Space |
| | Images | Y | Carved (NTFS Unallocated Space and Orphan Directory) |
| | Videos | N | N/A |
| Opera portable - 12.12 | Browser indicators | Y | 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 | Y | Memdump; AppData\Roaming\Mic\Win\Rec\CustomDestinations (Carved .lnk files with Last Access Times) |
| | Usernames/email accounts | N | N/A |
| | Images | Y | Carved from Memdump (Mostly partial images and difficult to view full content) |
| | Videos | N | N/A |
| Mozilla fireFox portable - 18.0.1 | Browser indicators | Y | Memdump; SysVol Information file timestamp (Firefox Portable appinfo) |
| | Browsing history | Y | Memdump; SysVol Information (Email only) |
| | Usernames/email accounts | Y | Memdump; SysVol Information (Email Account History) |
| | Images | Y | Carved from Memdump (Mostly partial images and difficult to view full content) |
| | Videos | N | N/A |

with all the browsers. For example, the Index.dat (history) and Registry > TypedURLs were empty, but we were still able to recover virtually all cached images, URL history, and usernames with their associated accounts. Everything was recoverable except for playable videos. Even though most of the data was recovered from RAM, free space, and slack space areas, there were sufficient findings within allocated space as well. Figure 4 shows an '[InPrivate]' indicator within RAM prior to an online search for hacking. In regard to indicators, there were a few areas where 'InPrivate' and 'Start InPrivate Browsing' were noted prior to a URL history log. Figure 5 shows one of these indicators within allocated space. It was also noted that the Microsoft 'PrivacIE' directory was found empty.

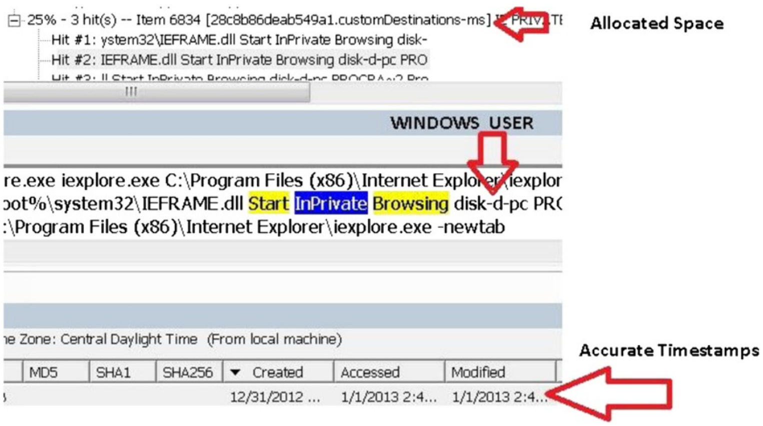
The three remaining browsers were a little more difficult to recover residual artifacts from. It appeared that the overall best way to recover residual data was to obtain the evidence from RAM or working memory, but that is not always possible for investigators. For Google Chrome Incognito artifacts, 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 historical 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 timestamps may be able to explain why something like as URL history is not there. For example, if a live search using regular expressions was used to locate one of these hidden artifacts in an unfamiliar location, an investigator can now understand why they were not found in other 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



```
015cc8f00  ·-· ·W·i·n·d·o·w·s· ·I·n·t·e·r·n·e·t· ·E·x·p·l·o·r·e·r· ·-· ·[·I·n·P·r·i·v·a·t·e·]····
015cc8f80  ··········+·a·&·c·p·=·2·7·&·g·s· ·i·d·=·2·x·&·x·h·r·=·t·&·q·=·h·o·w·+·t·o·+·h·a·c·k·+
015cc9000  Jà86 ···Ùt ·®d ·uZ ·åR ·ÅR ·£££( ·J ···°ì ·\× ·".tvt ·J! ·N£-···e ·År ··J ··F ·ÍV ·ÑI1fHS ·HÆÀ9 ·c\°®GvíÚ>:
```

**Figure 4** [InPrivate] search for 'how + to + hack + …' within RAM (Hex view).



```
⊟ 25% - 3 hit(s) -- Item 6834 [28c8b86deab549a1.customDestinations-ms] IE PRIVATE
    Hit #1: ystem32\IEFRAME.dll Start InPrivate Browsing disk-
    Hit #2: IEFRAME.dll Start InPrivate Browsing disk-d-pc PRO
    Hit #3: ll Start InPrivate Browsing disk-d-pc PROGRA~2 Pro

WINDOWS USER

re.exe iexplore.exe C:\Program Files (x86)\Internet Explorer\iexplor
oot%\system32\IEFRAME.dll Start InPrivate Browsing disk-d-pc PRC
:\Program Files (x86)\Internet Explorer\iexplore.exe -newtab

ne Zone: Central Daylight Time  (From local machine)
   MD5   SHA1   SHA256   ▼ Created      Accessed        Modified
                           12/31/2012 ...  1/1/2013 2:4...  1/1/2013 2:4...
```

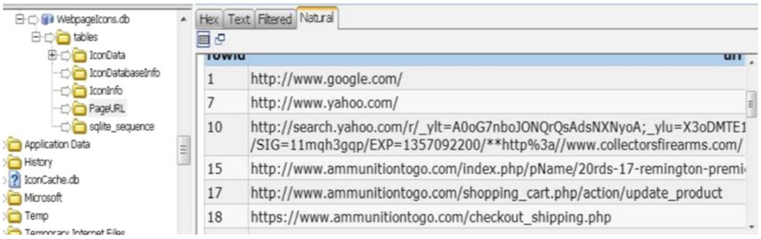
**Figure 5** InPrivate indicator in FTK.

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. Figure 6 shows some of the database artifacts using FTK. It is important to realize that this can be used to explain to courts as to why URL history would be located here and nowhere else under Safari data. It is not always about what is present, but what is absent is also of value.

With regard 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 web browsers tested, Google Chrome Portable left the most residual artifacts on the host machine. The recovery seemed as if Chrome was installed on the machine itself. Almost all artifacts to include images, browsing history, browsing method, and usernames with associated accounts, were located on the disk. Also note, these recovered artifacts were obtained without the flash drive. The importance for an investigator to distinguish that these artifacts came from Google Chrome Portable is for two reasons: (a) to be able to explain why Chrome artifacts were not located under common areas and (b) to alert the investigator that further evidence may be found on a flash drive that the investigator did not originally consider. Figure 7 provides a comparison of all the browsers tested and the strength of evidence which can be found.

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 usernames or accounts could be recovered. Firefox Portable resulted in similar findings; however, some 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 carved images from RAM, most of them were distorted but 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 the disk but none specific to user activity. Perhaps on a machine with a much higher capacity of RAM, this would be more useful.



| rowid | url |
|---|---|
| 1 | http://www.google.com/ |
| 7 | http://www.yahoo.com/ |
| 10 | http://search.yahoo.com/r/_ylt=A0oG7nboJONQrQsAdsNXNyoA;_ylu=X3oDMTE1<br>/SIG=11mqh3gqp/EXP=1357092200/**http%3a//www.collectorsfirearms.com/ |
| 15 | http://www.ammunitiontogo.com/index.php/pName/20rds-17-remington-premi |
| 17 | http://www.ammunitiontogo.com/shopping_cart.php/action/update_product |
| 18 | https://www.ammunitiontogo.com/checkout_shipping.php |

**Figure 6** Safari WebpageIcons database.

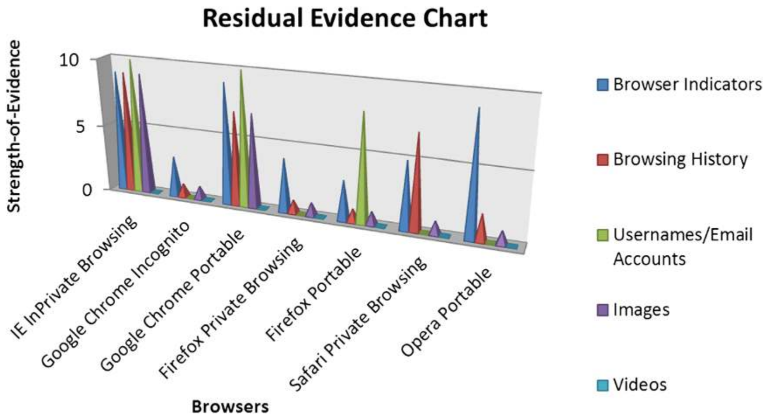


**Figure 7** Web browsers - strength of residual evidence.

### 6.7. Additional forensic results

Aside from discovering hidden web browsing artifacts, there is another finding worth mentioning due to its significant linking of 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 also a log of every folder located on the Passport. This information was transferred directly to the Windows machine while remaining on the hard drive and RAM. For this reason, a flash drive was later used to dump the memory on the Desktop to preserve data integrity without further contamination. 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 was within Trace*.fx files. Most probably the reason for the Trace*.fx files was due to the activity of a USB device configured for ReadyBoost (virtual memory).

This finding raises a number of questions and concerns. An investigator can easily document certain footprints such as plugging in devices and checking running processes. It is the unknown footprints which can cause a problem. This could violate certain policy and procedures that were once 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 also be used to know what type of contraband may be on the 'missing evidence.' This information would be extremely helpful when trying to establish an affirmative link between user and target machine.

## 7. 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 may be developed to provide investigators with whether or not these browsing artifacts exist (0/1 = False/Positive), and parse these artifacts accordingly.

## 8. Conclusion

The majority of recovered artifacts were discovered in RAM, slack/free space, and FTK [Orphan] directories. That being said, information was still obtained within allocated space. Another commonality between the browsers was information contained within the System Volume Information directory. The bottom line is that our research clearly establishes authoritative answers to which were never there before. In addition, some of our authoritative results contradict prior research statements. For example, one study [2] 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 forensic investigators must treat digital environments like a real crime scene. It is not only important to document what is found but to also note what is not there and ask why. Our research now provides an alternative way to perceive these types of findings and explain the results. We conclude that just because something is not there does not mean it never happened.

### Competing interests

The authors declare that they have no competing interests.

Received: 29 July 2013 Accepted: 4 November 2013
Published: 21 November 2013

### References

1. G Aggarwal, E Bursztein, C Jackson, D Boneh, An analysis of private browsing modes in modern browsers, in *Proc. Of 19th Usenix Security Symposium* (, Washington, DC, 2010), pp. 11–13
2. JH Choi, KG Lee, J Park, C Lee, S Lee, *Analysis framework to detect artifacts of portable web browser* (Center for Information Security Technologies, Seoul, 2012)
3. SanDisk, *U3 Launchpad End of Life Notice*, 2010. Available: http://kb.sandisk.com/app/answers/detail/a_id/5358/~/u3-launchpad-end-of-life-notice. Accessed 28 July 2012
4. C Soghoian, *Why private browsing modes do not deliver real privacy* (Center for Applied Cyber security Research, Bloomington, 2011)
5. Wikipedia, *U3*, 2013. Available: http://en.wikipedia.org/wiki/U3. Accessed 22 July 2012
6. R Tank, PAH Williams, *The impact of U3 devices on forensic analysis* (Australian Digital Forensics Conference, Perth, 2008)
7. T Bosschert, Battling anti-forensics: beating the U3 stick. J Digit Forensic Pract **1**(4), 265–273 (2007)
8. Microsoft, *InPrivate Browsing*, 2012. Available: http://windows.microsoft.com/en-US/internet-explorer/products/ie-9/features/in-private. Accessed 03 September 2012
9. Google, *Incognito mode*, 2012. Available: https://www.google.com/intl/en/chrome/browser/features.html#privacy. Accessed 03 September 2012
10. Mozilla, *Private Browsing*, 2012. Available: http://support.mozilla.org/en-US/kb/private-browsing-browse-web-without-saving-info. Accessed 03 September 2012
11. Apple, *Safari 5.1: Browse Privately*, 2012. Available: http://support.apple.com/kb/PH5000. Accessed 03 September 2012
12. PortableApps, , 2013. Available: http://portableapps.com/ Accessed 27 July 2012
13. PortableApps, *Mozilla Firefox, Portable Edition*, 2013. Available: http:// portableapps.com/apps/internet/firefox_portable. Accessed 27 July 2012
14. PortableApps, *Google Chrome Portable*, 2013. Available: http://portableapps.com/apps/internet/google_chrome_portable. Accessed 27 July 2012
15. PortableApps, *Opera, Portable Edition*, 2013. Available: http://portableapps.com/apps/internet/opera_portable. Accessed 27 July 2012
16. Disk Wipe, *Disk Wipe*, 2009. Available: http://www.diskwipe.org/. Accessed 12 December 2012
17. DaemonFS, *Sourceforge: DaemonFS*, 2010. Available: http://sourceforge.net/projects/daemonfs/. Accessed 27 July 2012
18. Nir Sofer, *NirSoft Freeware Utilities*, 2013. Available: http://nirsoft.net. Accessed 12 December 2012
19. AccessData, *FTK*, 2013. Available: http://www.accessdata.com/products/digital-forensics/ftk. Accessed 18 December 2012
20. Carnegie Mellon, *Live View*, 2006. Available: http://liveview.sourceforge.net. Accessed 18 December 2012

doi:10.1186/1687-417X-2013-6
**Cite this article as:** Ohana and Shashidhar: **Do private and portable web browsers leave incriminating evidence?: a forensic analysis of residual artifacts from private and portable web browsing sessions.** *EURASIP Journal on Information Security* 2013 **2013**:6.