Forensic Reconstruction and Analysis of Residual Artifacts from Portable Web Browser

Esther D. Adautin
Department of Information Technology
SRM University
Chennai, India

Nagoor Meeran A.R.
Department of Information Technology
SRM University
Chennai, India

ABSTRACT
In order to protect sensitive information, users have started to effect changes in their often overlooked surfing habit. Portable web browser is considered as one of the techniques which provide the much desired user privacy. Yet it poses a great challenge to forensic investigators who tries to reconstruct the past browsing history, in case of any computer incidence. This research paper examines the residual traces left over by Portable Google Chrome browser. It also proposes a methodology that will help investigators to effectively analyze activities associated with portable web browser with respect to incidence response. Furthermore, it examines the IconCache database file, for its evidential potential. The reconstruction of residual artifacts left on the victim computer by this browser which can serve as evidence that is admissible in court of law is also discussed.

General Terms
Digital Investigation, Portable Browser Forensics, User Privacy

Keywords
IconCache Database, Residual Artifact, Forensic Reconstruction

1. INTRODUCTION
In recent times, the Internet has become pervasive for daily tasks associated with desktop and mobile computer devices. In most cases, an accessibility constraint to personal computing devices necessitates the unprecedented use of foreign computing domains, resuming work with the use of removable drives. One of the most common activities is accessing the internet and such circumstances may demand privacy and other security conditions to protect vital user information and browsing history. Consequently, new browsing features were continually integrated into existing browsers such as; "private browsing", "multiple user feature" and "blocking of 3rd party cookies"[1]. For instance, Google Chrome has incognito mode which enables users to surf the internet with a little or none their sensitive data being cached in the host machine [2]. Though these developments were to avert the security and privacy challenges in browsing, users were still not satisfied with browsing data being cached in the foreign host, hence the development of portable web browsers [3].

The portable browsers are browsers that are stored and hosted on a portable or removable storage device such as the USB flash drive [4] . This implies that the browser is not an integral part of the computer and can be launched from the portable drive on any supported host and platform [5]. When using a portable web browsers the assumption is that user privacy is enhanced because the browsing data is cached in the portable storage device rather than the host persistent storage [1]. In addition to the portable web browsing are features which are incorporated to enhance more privacy to users. This poses a great challenge to forensic investigators who dive into retrieving and analyzing evidence (known as artifacts) on such machines in case of any computer incidence.

This paper aims at analyzing the artifacts created and retained in the victim PC for evidential potentials after a thumb drive containing an executable (Google Chrome portable) had been connected to a Windows 7 Operating system. In addition, it explores the possible locations in the victim PC for portable web browsing artifacts, thus extends the recovery of artifacts beyond memory dump and registry analysis. It also provides an efficient forensic solution by reconstructing portable web browsing history to establish an affirmative link between a user and his portable web browsing activities.

2. RELATED WORK
2.1 Private Browsing Mode
In context of private browsing, researchers suggest that data obfuscation methods have entered the mainstream consciousness and have created a new problem for forensic professionals [1]. The goal of introducing this specialized mode into current mainstream internet browsers was to prevent the traces of the web browsing activities from being left over on the host machine.

In addition, other researchers suggest that the major web browsers were not created equally in regard to the type and quantity of data that they leave behind on the host machine [5]. These researchers examined the various internet browsers in order to determine what traces of browsing activity were retained in the physical memory after using the private browsing modes of each browser. They discovered that the tested browser had failed to offer the much desired user privacy due to the traces left after each browsing session.

2.2 Portable Web Browsers Forensic
Initial researchers of the forensic reconstruction of portable web browser artifacts focused mainly on the identification and extraction of residual artifacts from the portable device. These researchers in their studies on the use of portable browsers inferred that when a removable flash drive is inaccessible to the forensic investigator then it becomes impossible to trace further information [3]. In the context of 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.

Other researchers revealed that portable web browsing artifacts were easily obtained from the memory dumps as it

were with the installed version of these browsers. In fact they suggested that not all the artifacts were located on the target hard drives but Google Chrome Portable left the most residual artifacts on the host machine out of the browsers tested. The recovery almost seemed as if Chrome was fully installed on the machine itself. Every search made such as image search, document search, video search together with accessed email accounts were all recovered. This analysis is of great important because the recovered artifacts were obtained without the flash drive contradicting the statement made by earliest researchers.

2.3 USB Connectable Device

The U3 technology was a concept developed by Microsoft and SanDisk to evade trails on the host PC such that after usage, the U3 smart drive does not record or leave any evidential potential. The U3 flash drive was pre-installed using the U3 Launch pad. It was believed that since folders were created which recorded the details of user's activities, once the device is ejected, the 'Cleanup.exe' is executed to erase every activity linking the usage of the device to the host machine. A study on the Forensic analysis of USB drive proved that artifacts of users' activities were discovered from Prefetch files and in a subfolder called "temp"[6].

Further studies also showed that when a USB storage device such as a thumb drive, is connected to a Windows system, several identifiers are created on the system [7]. To eliminate the need to manually configure drivers, devices have evolved to support so-called Plug and Play capabilities. Thus, when a user connects a USB storage device to a Windows system, Windows interrogates the device, determines what driver to use and most importantly records information about the device and driver pairing within a series of keys stored in the ENUM/USBSTOR and the DeviceClasses "keys" of the System Registry hive [8]. These identifiers, or artifacts, persist even after the system has been shut down.

3. WINDOWS ICONCACHE

From Windows 95 and other higher versions, almost everything visible to the eyes has an icon is associated with it. Every time the shell displays a folder full of files it needs to obtain icons for each of those items from somewhere [9]. Considering the expense of such an operation, it is obviously not something that it would want to repeat unnecessarily. By saving icons that it has already retrieved in a cache in memory, the shell is relieved of the need to constantly retrieve icons from disk. This makes a vast difference to the system performance, especially when accessing network drives and other slow media. The place where the shell stores its cached icons is called the System Imagelist, or Shell Icon Cache. IconCache database is a hidden system file stored in different locations, depending on the particular version of the Windows operating system. For Windows 7, we have:

C:\Users\Username\AppaData\Local\IconCache.db

IconCache.db file is associated with a specific user account of the host PC. It does not exist on a clean installation of the operating system but default system icons are automatically created at system startup [10]. The caches of icons exist only in the memory and are later written to disk after a Windows shutdown or restart. IconCache database is not static; it grows as information is added to it through processes and activities which take place in the host machine. This database can serve as a useful source to a forensic analyst who seeks to explore new areas where artifacts can be found on the investigated PC [10].

4. RESEARCH METHODOLOGY

This paper proposes a methodology that enables Forensic investigators to delve deep into Portable web Browser Forensic for new areas where artifacts may be discovered on the host PC, thus establishes an affirmative link between a user and his/her web browsing activity.

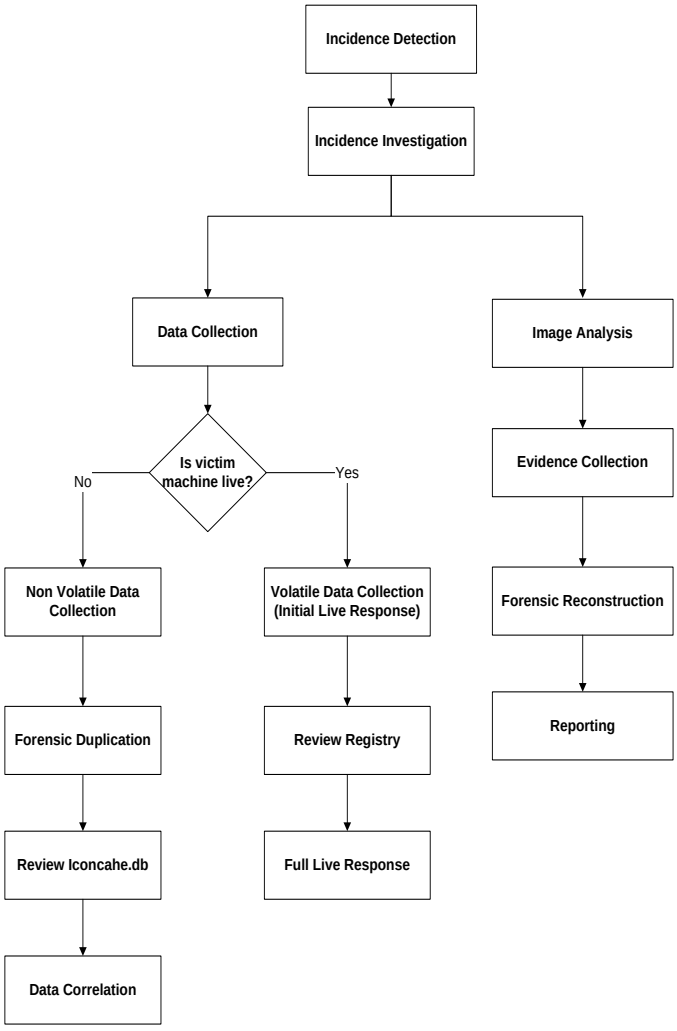

Fig 1: Methodology

Based on the proposed methodology above, the major investigative steps in response to any computer incidence involves: detection of incidence, evidence preservation, data acquisition, data analysis and finally reporting.

4.1 Tools and Setup

The tools used during the forensic data acquisitions, assessments, examination and analysis include:

Hardware:

- Forensic workstation
- Desktop Computer - Victim PC
- External Hard Disk - Evidence media
- SanDisk USB Flash Drive - 16GB
- USB External Hard Drive -1TB
- SATA to USB Adapter
- Tableau USB Write Blocker -IDE/SATA

Software:

- Microsoft Windows 7 Ultimate-Operating system
- Google Chrome Portable - Portable Web Browser
- TrueBack Imager - Imaging evidence device
- F-Dac 2.0 – Imaging Carving
- CyberCheck 6.0 - Forensic Image Analyzer
- IconCache Database Viewer.
- WinHex

4.2 Experiment

A formal test environment was established, and all the experiments were carried out in forensically sound manner such that it acceptable in court of law. The basic operating system used was Windows 7 Ultimate (32 bits). The experiment began with a clean installation the test operating system in which a singular user account was set up. A brand new blank SanDisk Flash drive was used for the installation of Google Chrome Portable.

For the sole purpose of this research, experiment was carried out on a freshly installed operating system to ascertain what happens in the victim PC as result of the following activities:

- Ascertain IconCache.db content on the installation of a clean operating system.
- Ascertain its contents before and after Google Chrome Portable) has been run from the USB Flash drive.
- Ascertain locations of residual artifacts from portable web browsing session.

4.2.1) Portable Web Browsing session

On a newly installed Windows operating system, the experiment was carried out based on a single username and computer name to ensure consistency. The web browsing session was performed from a USB flash drive containing an executable, Google Chrome portable which is connected to the system. During the portable web browsing sessions, various activities were performed such as: images search, document search, email login, video search on hacking and attempted online purchase. Google which is one of the most popular search engines was used in carrying out all the above mentioned activities. The web browsing session depicts that of an ordinary user who is naive about any form of anti-forensic activity.

4.2.2) Data Acquisition

i). Volatile Data acquisition

During the volatile data collection, the portable web browsing artifacts were being obtained from the victim PC while it was still powered on after the incidence has taken place. The investigator while carrying out this step must ensure that he documents every step rapidly in a forensically sound manner, because these artifacts gets lost as soon as the victim machine is turned off. Full live response provides in-depth volatile data which can be acquired from Memory Dump and thereafter performing Live RAM analysis using forensic tools such as Encase, CyberCheck to mention a few. A review of the Windows Registry for activities connected to the use of USB connectivity can be found in the location given below:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR

This helped in tracing and establishing the fact that indeed a USB flash drive had been connected to the victim machine. This step provided useful information such as the Flash Drive GUID.

ii). Non Volatile Acquisition

Non volatile data can only be obtained when the victim machine is powered off after the incidence has taken place. The entire web browsing artifacts can be acquired by analyzing the PC's Hard Disk image. After browsing with Portable Google Chrome browser, the victim PC was shutdown and disconnected from its power source. The victim's machine hard disk was carefully removed and connected to e-SATA to USB adapter, and then connected to the forensic workstation. Using TrueBack, the forensic duplicate (fresh image) of the evidence media was made with a file extension.P01 which will be analyzed later at the forensic workstation. The image was saved in a sterile external Hard Disk to avoid data contamination.

4.3 Artifacts Analysis

The forensic image created was fed into Cybercheck for analysis of the residual artifacts left on the victim PC. Cybercheck with its efficient suite of tools provides an easy to use interface for the analysis of forensic image created the imaging software: TrueBack. The integrity of the evidence file is verified by Cybercheck using the MD5 algorithm.

Among the qualities which makes Cybercheck an outstanding forensic analysis tools for the reconstruction of portable web browsing activities is its ability to provide:

- block by block verification of the entire evidence file,
- picture view of image file,
- search with GREP expression,
- extraction of data from Disk partitions, files and slacks,
- extraction of data from lost clusters and unused unallocated clusters.

By conducting a thorough investigation of the evidence file, traces of the user's web portable browsing activities were discovered. This process took several hours of sifting through the evidence files. The investigative steps to navigate to the portable web browser indicators and ultimately traces of portable web browsing history as obtained from Cybercheck and Winhex probe analysis are shown in the figures below:

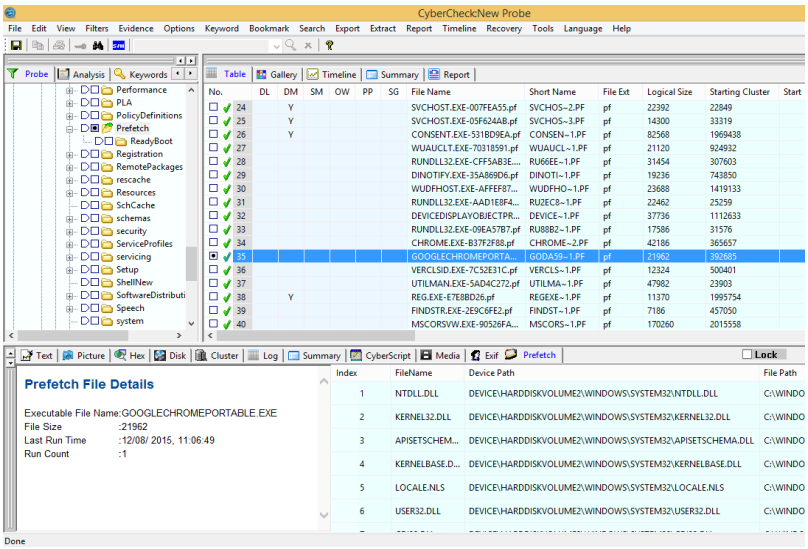

Fig. 2: Prefetch as Portable Browser Indicator

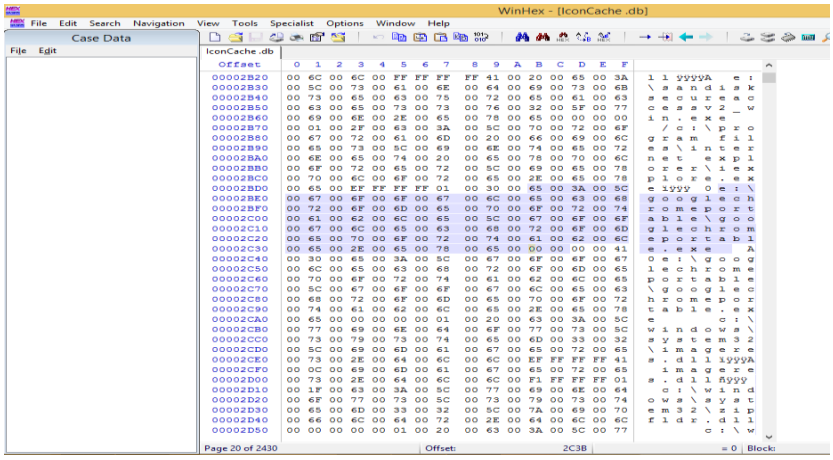

Fig 3: Windows Iconcache.db as Portable Browser Indicator

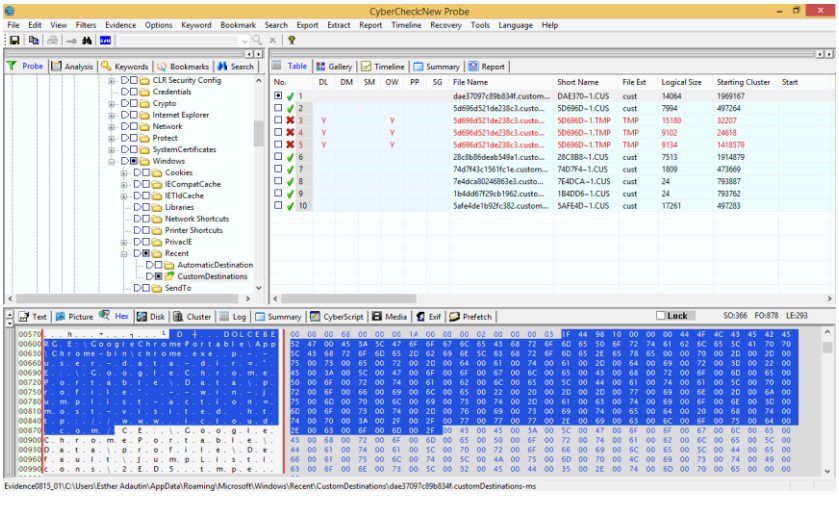

Fig 4: Windows CustomDestinations as Portable Web browsing History Indicator

4.4 Result

During the course of the experiment, it was observed that Widows IconCache database file was not created on a clean installation of the operating system, but created only after a system reboot or after the system must have been shut down. The size of the IconCache.db files continued to grow as processes and activities took place in the system. Analysis of the Windows IconCache database file indicated the use of portable browser on the host machine.

Table 1. Changes in Windows 7 IconCache.db file

Experimental activity	Original size on Disk	Modified Size on Disk	Number of icons
On a clean installation of OS	n/a	n/a	n/a
First instance of Iconcache.db on system reboot	920KB	n/a	197
Before and after running an executable from a USB Flash drive	0.98MB	298MB	245

A summary of the location of artifacts left behind during portable web browsing session is given in the table 2 below:

Table 2. Google Chrome Portable

Residual Artifacts	Location
Web Browsing Label	• Drive name:\Windows\Prefetch • Drive name:\Pagefile.sys • ~Users\Username\AppData\Local\IconCache.db • ~Users\Username\AppData\Roaming\Windows\ Microsoft\Recent\CustomDestinations
Web Browsing History	• ~Pagefile.sys • ~Hiber.sys • ~Users\Username\AppData\Roaming\Windows\ Microsoft\Recent\CustomDestinations
Image Search	• Carved NTFS Allocated and Unallocated Space
YouTube Video Indicator	• ~PageFile.sys
Email related activities	• ~PageFile.sys
Document Search	• ~Users\Username\AppData\Roaming\Windows\ Microsoft\Recent\CustomDestinations

In the context of installed Google Chrome, it is comparatively easy to reconstruct residual artifacts from a user's web browsing without undergoing a very thorough forensic analysis. Artifacts are easily recovered from browser forensic. The reconstruction of residual artifacts from a portable web browser requires a thorough forensic analysis to obtain data related to a user's portable web browsing activities. Most information about visited URLs during portable web browsing sessions were obtained from the Windows binary file CustomDestinations and through keyword searches. Searched images were all recovery from the forensic reconstruction process using Data Carving Technique. It is worthy of note that the residual artifacts from the portable web browsing activitis were obtained in the absence of the USB flash drive containing Google Chrome Portable. This implies limited user privacy as affirmative link can be established between the user and his portable browsing session.

Most traces left from portable web browsing session were obtained from keyword searches. These traces were located in Pagefile. Artifacts related to hacking, email account login, document search and image searches were generated by parsing the keyword as string into the Forensic tool: CyberCheck and the number of times each string was found was presented as the number of Hits. Analyzing artifacts from the portable web browser yielded a substantial amount of information regarding its usage. Hence no user privacy is guaranteed.

Table 3. Keywords Search Result

Visited Websites	Keyword search	Keyword Hits from Disk image
www.flipkart.com	Blazer	Available
www.icloud.com	icloud	Available
www.youtube.com	Hacking	Available
Photobucket.com	Kim Kardashian	Available

5. FUTURE WORK

Further research for artifacts left from Portable web browsing should be done by performing in-depth analysis on Windows IconCache database file and Pagefile. An improvement should be implemented in the design and development of carving tools such that it can tell the original creation date and time of carved images. High versions of Widows operating system including the newly released Windows 10 are also recommended for future analysis.

6. CONLCUSION

Windows Iconcache database files constitute one of the indicators of portable web browsing activities. Windows binary files CustomDestinations, Pagefile and Prefetch files yielded a vast amount of information for the forensic reconstruction the portable browsing history. If the intention of using a portable web browser is to evade detection, then it is worthwhile to note that forensic reconstruction of residual artifacts can trace portable web browsing session back to the user.

7. ACKNOWLEDGMENT

My sincere gratitude goes to God Almighty who in his infinite mercies saw me through this work. I also appreciate my project supervisor for his guidance and my beloved family and friends for their support towards successful completion of this work.

8. 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] Google. (2015). Incognito mode. [Online]: https://tools.google.com/dlpage/res/chrome/en/more/privacy.html.

[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] A. Marringhton, I. Baggili, T. AI Ismail, A. AI Kaf, "Portable Web Browser Forensics: A forensic examination of the privacy benefits of portable web browsers," IEEE Journal 2013.

[5] D. J. Ohana, N. Shashidhar, "Do Private and Portable Web Browsers Leave Incriminating Evidence: A Forensic Analysis of Residual Artifacts from Private and Portable Web Browsing Sessions," IEEE Security and Privacy Workshops, 2013.

[6] D. G. Dharan, N. Meeran, "Forensic Evidence Collection by Reconstruction of Artifacts in Portable Web Browser," ijcaonline.org, 2014.

[7] H. Carvey, C. Altheide, "Tracking USB storage: analysis of windows artifacts generated by USB storage devices," Digital Investigation, 2005.

[8] V. Mee, A.Jones, "Windows Operating System Registry: a central repository of evidence, In Proceedings from e-crime and computer evidence conference, 2005.

[9] J. Collie, "The Windows Iconcahe.db: A resource for forensic artifacts from USB connectable devices", Digital investigation (2013).

[10] Undocumented Widows95, "The shell icon cache," [Online]: http://koti.mbnet.fi/vaultec/files/miscellaneous/undocw95/iconcache.html