

Forensic Investigation of User's Web Activity on Google Chrome using various Forensic Tools

Narmeen Shafqat,

NUST, Pakistan

Summary

Cyber Crimes are increasing day by day, ranging from confidentiality violation to identity theft and much more. The web activity of the suspect, whether carried out on computer or smart device, is hence of particular interest to the forensics investigator. Browser forensics i.e forensics of suspect's browser history, saved passwords, cache, recent tabs opened etc. , therefore supply ample amount of information to the forensic experts in case of any illegal involvement of the culprit in any activity done on web browsers. Owing to the growing popularity and widespread use of the Google Chrome web browser, this paper will forensically analyse the said browser in windows 8 environment, using various forensics tools and techniques, with the aim to reconstruct the web browsing activities of the suspect. The working of Google Chrome in regular mode, private "Google Incognito Mode" and portable modes of operation is discussed at length in this paper.

Keywords

Browser forensics, Private web browsing, Chrome Incognito, Chrome forensics, Portable browser forensics, Chrome artifacts.

1. Introduction

Internet has become the need of hour today. According to the Internet Live Stats (2015), 40% of the world's population uses internet daily for a couple of tasks involving browsing internet for information or entertainment, social networking, email, e-commerce, gaming, blogging, banking etc. With such large number of internet users throughout the world, the number of cyber criminals has also come to a rise. Where the good guys benefit a lot from the internet, the bad guys also use it to carry out cyber-attacks, communicate with their peers, search for attack methods, preparing themselves for the crime etc.

It is interesting to note that, from the websites visited, to the items downloaded, every web activity of the user gets stored on his device. Even a single word searched by the user leaves its trace somewhere in his computer and thus can be obtained by the forensic analyst if he/she carries out forensic analysis of the suspect's browser. Thus, browser forensics supply ample amount of information to the forensic experts in case of illegal involvement of the culprit in any activity done on web browsers.

Forensic Experts should therefore have full grasp on not only the forensic analysis of well-known and well

acknowledged browsers like Internet Explorer, Google Chrome, Mozilla Firefox, Safari, Opera etc. but should also have hands on experience of less popular web browsers like Erwise, Arena, Cello, Netscape, iCab, Cyberdog etc. Not only this, the forensic experts should also know how to find artifacts of interest from older versions of well-known web browsers; Internet Explorer, Chrome and Mozilla Firefox atleast, because he might experience a case where the suspected person is using older versions of these browsers.

According to StatCounter Global market share for the web browsers (2015), Google Chrome, Mozilla Firefox and Microsoft's Internet Explorer make up 90% of the browser usage. Owing to the growing popularity of the Google Chrome web browser, having 48.71% of the web browser share alone, this paper will move around this web browser. The forensic analysis of Google Chrome, as carried out on HP Pavilion laptop running Windows 8 OS, in normal/regular, private (incognito) and portable modes of operation is discussed at length in this paper, to help the forensic investigators in investigations relating to web browsers.

Various open-source forensic tools have been used throughout the research to provide maximum amount of human readable information to the forensic investigator/practitioner, as retrieved from the Google Chrome's default files and folders. The results have been tested with different forensic softwares/ tools to ensure the validity and accuracy of the obtained forensic results.

2. Literature Review

Current research in the field of browser forensics targets the stored files of widely used web browsers notably Google Chrome, Internet Explorer, Mozilla Firefox, Safari and Opera to extract data of interest. Emphasis nowadays is also laid on the structural analysis of internet log files from a forensic point of view to gather traces of the internet habits of the suspect under investigation.

Where the web browser vendors endeavor to provide safe and secure browsing features to its customers, the forensic researchers are trying hard to dig out methods to combat these anti-forensics attempts on the web browsers and reveal more and more internet activity of the user that gets

stored on the disk even in the private or portable web browsing mode of operation.

A number of freeware tools exist on the internet for carrying out the forensic analysis of the web browser's history, cache, cookies, login data files etc. Most of the tools however, target only a single web browser and cannot create a real picture of the case if the culprit uses more than one web browser on his device.

Since the scope of the research is confined to the forensic analysis of Google Chrome only, we assume that the suspect uses only Chrome on his computer, and thus the available open source Chrome analysis tools are sufficient to analyze the case forensically.

2.1 Basics of Google Chrome

Google Chrome, is the fastest and most used web browser in the world today. For Windows 8, Chrome stores its files and database in the following default locations in C drive. C:\Users\[USERNAME]\AppData\Local\Google\Chrome\UserData\Default.

The folder contains files of our interest i.e. Bookmarks, Cookies, Current Tabs, History, Last tabs, Login Data, Preferences, Top Sites and Web Data. These web browsing artifacts are stored in SQLite, SNSS (Session Saver) and JSON (Java Script Object Notation) formats. The structure of the DB file is quite different from that of other renowned browsers e.g. Mozilla Firefox. (Russ Taylor, 2014).

Google Chrome stores the timestamps in Webkit format i.e. number of microseconds passed since 00:00:00 UTC of Jan 1, 1601. (Junghoon, Seungbong & Sangjin, 2011). However, some of the Chrome files have also been observed to follow a flavor of the Windows File time, which is basically 100 nano-second intervals since January 1, 1601 UTC, divided by factor 10. For examination, any Chrome time decoder e.g. DCode etc. can be used by the forensic investigator to convert the timings given in history files to the desired format.

2.2 Google Chrome's Web Browsing Mode

Chrome web browser works in the following modes:

2.2.1 Regular Mode

It is the default mode that is most commonly used. It stores entire user's activity on disk.

2.2.2 Private Mode

This mode is designed to give user privacy while surfing the Internet. It does not keep a track of all of the user's activity.

2.2.3 Portable Mode

The mode allows user to install a portable web browser on a USB or cloud media, and run it on any PC. It provides the user portability to keep his browser files, websites' passwords etc. with him all the time.

3. Chrome Browser Forensics: Preparation and Procedure

Forensic research in this paper is carried out on HP Pavilion laptop running Windows 8. Chrome 40 was installed on the PC for experimenting with regular and private mode of operation. It was made sure that Chrome is in use for more than one week, so that abundant amount of information is present to carry out its forensic analysis. However, for portable mode forensics, Goggle Chrome Portable Application was installed in USB and the experiment was repeated.

In general, the investigation methodology depends largely on the OS installed on suspected PC, the web browser under investigation, the type of evidence etc. One way to analyze the browser forensically is to take the image of the hard drive, select some user's search words from the history file, and use FTK Live Search option to search those keywords in the imaged drive. The data can then be authenticated using CRC (cyclic redundancy check), SHA-1 (Secure Hash Algorithm) or MD-5 (Message Digest Algorithm).

The second approach for browser forensics is to open each file present in the Default Chrome folder and analyze it separately for internet evidences using various forensic tools and techniques. Then, validate all the results with alternative open source tools too, if proprietary softwares have not been used in the investigation. This subsection however attempts to find artifacts using the second method. However, methodology 1 has also been used in the paper.

Well for any methodology, it is important for the forensic team to know where he can find the data of his interest, for reconstructing the culprit's web browsing activity, as shown in Table 1.

Table 1. Where to find Chrome Contents

| Content? | Found in (File/ Folders) |
|------------------|--|
| Websites visited | History, Cache, Cookies, Recovery Folders, Suggested Sites |
| Visit count | History |
| Visit time | History, Cookie, Cache, Recovery Folders |
| Search Words | Auto Complete, Cache |
| Downloads | Downloads, Cache |
| Sites saved | Bookmarks |

The forensic investigator must be equipped with a good collection of various open-source and proprietary browser forensics tools before starting the investigation. Table 2 below enlists the softwares that will be used for forensic analysis of Google Chrome in this paper.

Table 2. Web Browser Forensic Tools

| Forensics Tool | Contents analyzed |
|--------------------------------|---------------------------------------|
| Phrozen Browser Forensics Tool | Scans browser's history and keywords |
| History Viewer | History, Top sites, Cookies, Keyword, |

| | |
|---------------------------|--|
| | Downloads, |
| MyLastSearch | Search queries |
| ChromeCookie View | Cookies |
| Chrome Password Decryptor | Decrypts password |
| ChromeCache View | Cache |
| Internet Evidence Finder | Internet artifacts from unallocated space, default folders, pagefile.sys, hiberfil.sys |
| Cookie Cutter | Google Analytics cookies, Search terms |
| Chrome Analysis | History, Bookmarks , Cookies, Search words, Downloads |
| Chrome Session Parser | Current and last sessions and tabs |
| Web Historian | History |

The forensic investigator while investigating any case involving web browser or any other illegal internet activity, should proceed with the following steps. (Newman, 2007).

- 1) Precisely define the scope of the investigation,
- 2) Maintain a detailed log of investigation activities,
- 3) Secure the computer/ laptop under investigation, Document the peripherals attached, hardware and software configurations of the system,
- 4) Connect a software or hardware write blocker to the PC, to prevent accidental damaging of any kind of potential evidence. Take snapshot or print any result that shows internet-abuse,
- 5) Preserve any data opened on PC, and the time stamps,
- 6) Run “Phrozen Browser Forensics Tool” to identify the web browser that the suspect uses most. This tool scans the history of widely known web browsers and provides statistics according to the browser usage,
- 7) If the browser is opened, check whether you can view Incognito sign or recent tabs in the Chrome Menu. Presence of sign and absence of recent tabs both indicate that the private mode has been enabled. In that case first collect the evidence from Chrome’s own settings bar before the session expires. Also collect Chrome’s default files and folder for further analysis. However, incase the browser is running in regular/ normal mode, simply collect all the default files and folders and analyze them using forensic tools.
- 8) If browser is closed, simply collect files from the default folder. The absence of URL name for even some of the results, indicate the usage of private web browsing mode by the suspect. Else it is evident that the user uses Chrome in normal/ regular mode,
- 9) Check registry entries for the USB devices connected to the computer so far and determine whether portable mode was enabled or not. If Chrome has been used in portable mode, trace the residual artifacts in the computer,
- 10) Also search File slack space, Swap Files, Pagefile.sys, Hyberfil.sys, \$Logfile, Volume shadow copies, Unpartitioned space, Uninitialized file area, Unallocated clusters, \$mft, etc. for trace of Internet activity.

- 11) Validate all results with alternative open source tools, if proprietary softwares have not been used in the investigation,
- 12) Present your findings.

4. Chrome’s Forensics in Regular Mode

This section will discuss the analysis of the artifacts stored on disk in the Regular Browsing mode from the forensic point of view. Chrome version 40 was installed on the laptop running Windows 8. This section covers the forensic analysis of Google Chrome by opening the files present in the Default Chrome folder i.e. History, Cookies, Bookmarks, Top Sites, WebData, Shortcuts etc., separately in various forensic tools and analyzing them for required internet evidences.

4.1History:

The History file found in the ../Chrome/Default/History folder is basically a database file that contains record of user’s all web history. It contains tables for downloads, visits, urls, segment_usage, keyword_search_terms, meta, presentation, and segments, that provide useful information to the forensic experts about the victim’s web activity. The forensic investigator can simply use History Viewer tool to open the History file present in the Chrome Default folder. The software makes search easy for the investigator as seen in the Figure 1 below.

| History Viewer | | | |
|--------------------------------|--------------------------------------|-----------|----------------------|
| URL History | Title | Visit ... | Last Visited Time |
| http://www.digital-detectiv... | Digital Detective I Training | 1 | 1/17/2015 7:30:34 PM |
| https://www.google.com.p... | mcs.nust.edu.pk - Google Search | 1 | 1/17/2015 7:31:32 PM |
| https://www.google.com.p... | | 1 | 1/17/2015 7:31:40 PM |
| http://www.nust.edu.pk/A... | Military College of Signals (MCS) - | 1 | 1/17/2015 7:31:42 PM |
| http://www.nust.edu.pk/A... | Military College of Signals (MCS) - | 1 | 1/17/2015 7:31:42 PM |
| https://www.google.com.p... | | 1 | 1/17/2015 7:31:49 PM |
| https://lms.nust.edu.pk/lm... | NUST LMS: Military College of Sig... | 3 | 1/17/2015 7:48:07 PM |
| https://lms.nust.edu.pk/po... | NUST LMS Portal: Login to the site | 1 | 1/17/2015 7:32:31 PM |
| https://www.google.com.p... | Google | 2 | 1/17/2015 8:16:47 PM |
| https://www.google.com.p... | | 1 | 1/17/2015 7:37:06 PM |
| http://www.howtogeek.co... | How to Recover Accidentally Dele... | 1 | 1/17/2015 7:37:10 PM |
| https://www.google.com.p... | | 1 | 1/17/2015 7:37:10 PM |
| http://productforums.googl... | Google Groups | 1 | 1/17/2015 7:37:13 PM |
| https://productforums.goo... | Google Groups | 1 | 1/17/2015 7:37:13 PM |
| https://productforums.goo... | Google Groups | 1 | 1/17/2015 7:37:13 PM |
| https://www.google.com.p... | | 1 | 1/17/2015 8:14:53 PM |
| https://www.google.com.p... | | 1 | 1/17/2015 8:14:58 PM |
| https://play.google.com/st... | TextSecure Private Messenger - A... | 1 | 1/17/2015 8:15:10 PM |

Fig. 1 History file opened in History Viewer

To speed up the investigation, instead of looking for evidences in whole history file, forensic investigator can use Browser Forensic tool, to make up a list of keywords that he needs to search for in the history and start scan. Figure 2 below shows part of keyword list generated for a sample search.

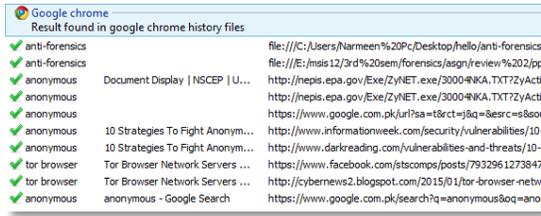


Fig. 2 Search Results for specific keywords searched

Since open source tool has been used for the research, the forensic investigator can also view user's web history details and download information in Chrome Analysis tool to verify his results. The problem for the forensic investigator while investigating history files is that Google keeps each web history artifact for a period of three months only, after which it automatically gets deleted. The artifacts however do not get wiped off from the drive and are kept in archived history database. The forensic investigator can get the URL and download information from there, while the visit time gets expire. Hence it is difficult for the investigator to prepare timelines for evidences of cases more than three months old. (Craig Wilson, 2014)

4.2 Search Keywords

It is important for the forensic examiner to understand that the words searched by the user, on the web browser, simply get stored in the URL. Thus, if for instance, he comes across a URL say, <http://www.google.com/search?hl=en&source=hp&q=chrome&aq=f&oq=&aqi=g10> then it means that the suspect used Google.com host to search for the variable q i.e. Chrome in this case. (Junghoon, Seungbong & Sangjin, 2011).

The recent search words of the suspect can be viewed by opening the Default Chrome folder in tool like MyLastSearch, History Viewer etc.

4.3 Cookies

Cookies are basically the SQL files, that websites create to store the users' browsing information such as his/her site preferences, location or personal profile information etc. Cookies also help analyze web traffic and are often necessary for website's functionality. The cookies are of two types; first party (set by site domain) and third party cookies (comes from sources that display items or adds on that particular page.)

Google Chrome stores its cookies in `../Chrome/ UserData/ Default` folder. The users are given 5 options for cookies; allow, block, delete, make exception list, or keep cookies until the browser is open. Users, who do not wish to be tracked, must disable cookies. To view the cookies from Google Chrome, go to Chrome Menu > Settings > Show advance settings > Privacy section > All cookies

and site data. This will open up the cookie console. Any cookie value when clicked opens up the dialog box showing name, content, domain, path, time of creation and expiration. For forensic investigator, detail as small as a cookie even helps progress the investigation because cookies prove that the user accessed that website at some time.

Since there is no fixed structure for cookies, forensic investigator may face problem analyzing them. The best solution for that is to use any cookie viewing tool like Cookie Spy or Chrome Cookie Viewer. Figure 3 below shows a snapshot of the Chrome Cookie Viewer when run on the target PC. It provides the name of the cookie, host name, path, HTTP use, creation date, last access date, expiry date and whether security feature is enabled or not.

The screenshot shows the Chrome Cookie Viewer application window. It displays a table of cookies with the following columns: Host Name, Path, Name, Value, Sec., H., Last Accessed, Created On, and Expires. The table contains several entries for various websites like yandex.ru, yimg.com, zenoviaexchange.co..., accounts.google.com, and answers.yahoo.com.

| Host Name | Path | Name | Value | Sec. | H. | Last Accessed | Created On | Expires |
|------------------------|------|-------------|-------|------|-----|--------------------|--------------------|--------------------|
| yandex.ru | / | yandeurid | | No | No | 1/17/2015 12:32... | 1/17/2015 12:32... | 1/14/2025 12:32... |
| yimg.com | / | ypcrlb | | No | No | 1/18/2015 10:26... | 1/18/2015 10:26... | 1/15/2015 10:26... |
| zenoviaexchange.co... | / | _jdeuvid | | No | Yes | 1/17/2015 12:35... | 1/17/2015 12:33... | 1/16/2017 12:33... |
| accounts.google.com | / | ACCOU... | | Yes | Yes | 1/18/2015 10:27... | 1/17/2015 12:47... | 1/16/2017 12:47... |
| accounts.google.com | / | LSID | | Yes | Yes | 1/18/2015 10:27... | 1/17/2015 11:12... | 1/16/2017 11:12... |
| accounts.google.com | /o | LSOSID | | Yes | Yes | 1/18/2015 10:27... | 1/17/2015 11:12... | 1/16/2017 11:12... |
| accounts.google.com | / | GAP5 | | Yes | Yes | 1/18/2015 10:27... | 1/17/2015 11:43... | 1/16/2017 11:43... |
| answers.yahoo.com | / | ywandp | | No | No | 1/18/2015 10:28... | 1/18/2015 10:28... | 1/15/2025 10:28... |
| answers.yahoo.com | / | fpc | | No | No | 1/18/2015 10:28... | 1/18/2015 10:28... | 1/18/2016 10:28... |
| beacon-1.newrelic.c... | / | JSESSION... | | No | No | 1/18/2015 10:28... | 1/18/2015 10:28... | |

Fig. 3 Cookies opened in Chrome Cookie View

Many websites nowadays, however use Google Analytics (GA) cookies. GA cookies are more structured than the standard HTTP cookies, and hence provides more authentic information regarding the user of that website, insight on how he found/ accessed that particular site, how many pages did he view and whether the user had established active session with the site before closing Google Chrome or not. (Nelson, 2012)

4.4 Login Data

This file in the `../Chrome/Default` folder stores the login credentials of user for various websites. The file stores the URL of website, username, password, actual name, date of creation in plain text as record.

It is to be noted that Google Chrome leaves it upon the OS to secure the saved passwords. In most cases, the passwords will be stored in plain text. Figure 4 below shows the Login Data file present in `../Chrome/ UserData/ Default` folder opened in a freely available SQLite DB browser.

However in some cases, the user's password is encrypted with triple DES algorithm, with the seeding input as the user's own login password. The user is prompted to type his master password to view the Chrome passwords. Figure 5 as seen below, shows part of Chrome Password Decryptor, that the forensic analyst may use to decrypt the encrypted Chrome password. (Securityxplored, n.d.)

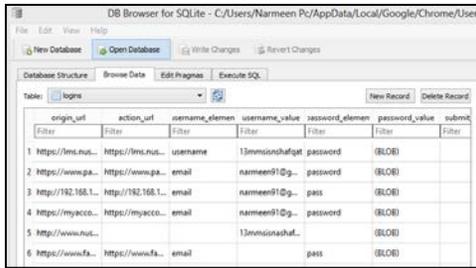


Fig. 4 Login Credentials opened in SQLite Viewer



Fig. 5 Chrome Password Decryptor

4.5 Shortcuts

The shortcuts are the guess words that might help the user while typing his search keyword in the URL bar. They will appear as suggestion to him, like fac for facebook.com, gm for gmail.com etc. The Shortcuts file can be viewed in SQLite DB Browser to reveal the shortcuts.

4.6 Top Sites

Top sites, or the sites most visited by the user can be viewed by opening the ../UserData/Default/Top Sites file in DB Browser for SQLite. It provides URL along with data_count etc. for the most viewed sites. However, "History Viewer" software can also show these details, as seen in Figure 6.

| URL | Rank | title |
|---|------|---------------------------|
| http://gmail.com/ | 0 | Gmail |
| https://www.facebook.com/ | 1 | (1) Facebook |
| http://security.didici.cc/ | 2 | News : security.didici.cc |
| http://elance.com/ | 3 | Hire freelancers and find |
| http://www.google.com/chrome/intl/en/wel... | 4 | Welcome to Google Cho |
| https://chrome.google.com/webstore?hl=en | 5 | Chrome Web Store |

Fig. 6 Top Sites file opened in History Viewer

4.7 Web Data

The Web Data Chrome file stores the login credentials and auto fill data of the Chrome users.

- a. The login credentials are only stored for the websites that the user has permitted to store the credentials for.
- b. The auto fill data is the data with which the user has already filled any web form with. Chrome stores this data for user's ease so that it may auto suggest the stored input when the user is about to fill the form. (Sarah, 2010)

Figure 7 shows snapshot of the WebData file from ../Chrome/UserData/Default folder opened in SQLite DB Browser.

| | name | value | value_lower |
|---|-------|---------------------|---------------------|
| 1 | email | elishbakh@gmail.com | elishbakh@gmail.com |
| 2 | Email | narmeen91 | narmeen91 |

Fig. 7 WebData file opened in SQLite DB Viewer

4.8 Preferences

The Preferences file present in the ../Chrome/UserData/Default folder indicates the user's preferred settings for the Google Chrome web browser. The forensic investigator can simple open it in Chrome by double clicking on the file in the folder. Figure 8 shows part of the data of the Preferences file.

```

{
  "browser": {
    "clear_lso_data_enabled": true,
    "last_clear_browsing_data_time": "13066064110775054",
    "last_known_google_url": "https://www.google.com.pk/",
    "last_prompted_google_url": "https://www.google.com.pk/",
    "pepper_flash_settings_enabled": true,
    "window_placement": {

```

Fig 8: Snapshot of Preferences file

4.9 Bookmarks

Bookmarks are URI's (Universal Resource Identifiers) that are basically the shortcuts to the favorite or saved pages. If the website has been bookmarked, the user doesn't need to remember the URL for opening it. Thus these bookmarks provide the forensic investigator idea of what kind of data or website does the user deems important. Bookmarked sites can be opened from the Chrome Menu > Bookmarks.

Bookmarks tab only shows the URL of the websites that the user has bookmarked. This information is insufficient for a forensic analyzer to determine which bookmarks are recent. He may therefore open the bookmarks file located in Chrome/ UserData/ Default folder in notepad or chrome to see other bookmark's parameters such as time of bookmarking, URL, type etc., as seen in Figure 9.

```

{
  "checksum": "1981a695d49f48540974b124aa9eda82",
  "roots": {
    "bookmark_bar": {
      "children": [ {
        "date_added": "13065978661439098",
        "id": "138",
        "name": "Browser Forensics ",
        "type": "url",
        "url": "http://www.browser-forensics.net/"
      }, {
        "date_added": "13061632869000000",
        "id": "50",
        "name": "Security news aggregated",
        "type": "url",
        "url": "http://security.didici.cc/news"
      }
    ]
  }
}

```

Fig. 9 Chrome Bookmarks opened in Chrome

To interpret the date_added field as seen in figure 13, the forensic investigator may use Dcode Time decoder, or any other freely available decoder. Figure 10, shows the first date_added value converted to Pakistan standard time i.e. GMT+05.

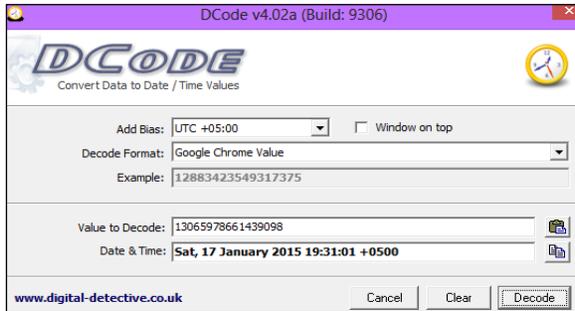


Fig. 10 Chrome Time Decoding

4.10 Bookmarks.bak

Bookmarks.bak file contains the recent backup of the Chrome bookmarks, since the user last launched it. It overwrites this backup every time the user launches the Google Chrome web browser.

Incase the suspect has deleted the bookmarks before running away from the crime scene, the forensic investigator can restore them by deleting the bookmarks file present in ../Chrome/UserData/Default folder and renaming the Bookmarks.bak file to Bookmarks. All previously deleted bookmarks will be restored to the bookmarks bar and can be viewed upon opening the web browser.

4.11 Cache

Cache transparently stores website's data so that future requests for that data can be served faster. The Chrome's Cache folder consists of an index file, four data files and another hex file. Figure 11 below shows the view of cache folder, as seen from the Chrome Cache Viewer tool.

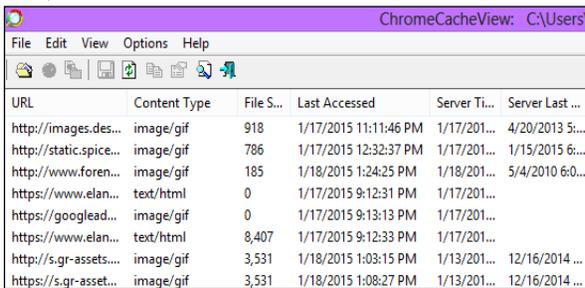


Fig. 11 Cache file opened in Chrome Cache View

Clicking on them, open up a dialog box, revealing more information regarding the cached object, for instance URL, content type, file size, last accessed date and time, server time, expire time, server response, eTag, Cache Control etc.

4.12 Other Internet Artifacts

Part of the memory of computer's PC also stores artifacts/ message traces of web mailing and social networking sites like Facebook, Gmail, Yahoo etc. Therefore, the investigator must also look upon the pagefile.sys, hyperfil.sys, unallocated space, etc. for their artifacts too.

The Internet Evidence Finder software can be used by the forensic investigator to find traces of social networking apps, webmail services, mapping queries, instant messaging applications, cloud based services etc. from different memory locations including the pagefile.sys, hiberfil.sys, \$mft, unallocated clusters etc. A search summary and scan, was conducted as part of research using the Internet Evidence Finder tool to find the left over internet artifacts. The results of the search summary can be seen in the figure 12 below.

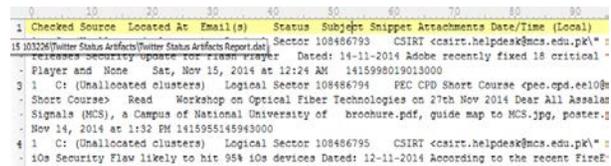


Fig. 12 IEF Scan Results

4.13 Deleted Chrome Data

If however the culprit/user deletes the browsing history from the Chrome Menu > Clear History, all the history files present in the memory gets deleted. However, the downloads, cookies, and cache files are initialized to zeroes. (Junghoon, Seungbong & Sangjin, 2011). The default folder when opened in Access Data FTK Imager showed deleted files with a red cross, as seen in the Figure 13 below.

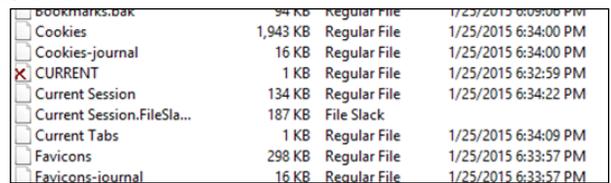


Fig. 13 Deleted File shown in FTK Imager

In short, we observe that Google Chrome really stores a wealth of internet artifacts on the user's drive. Among all the files, the history file alone provides sufficient information to the forensic investigator to reconstruct the timeline of user's activity or at the least get the idea of his intention. The cached web pages not only provides user content of the sites visited by the suspect but also proves that the user has visited those particular sites. This observation is important in cases of child pornography, electronic fraud, non-repudiation cases etc. Moreover, the forensic investigator must also analyze the cookie's file to get the session ID of the user, top sites file to look for

suspect’s most visited sites, login data file to note suspect’s credentials for various websites, etc. In terms of privacy, the regular mode of operation is not at all secure, since it stores almost all the surfing activity of the user on the hard drive. However, with the availability of various browser forensics tools in the market, the forensic investigation of web browsers has been made quite easy for the forensic investigators.

5. Google Incognito (Private Web Browser) Forensics

Like Chrome, other well-known web browsers also allow user to surf internet in Private mode. The private browsing feature of web browsers gives the user freedom of browsing the internet, without keeping any record of his browsing history, cookies, temporary Internet files, usernames/passwords, form data etc. The feature also helps prevent him from third party websites that usually track user’s browsers activity. Thus, these types of browsing features tend to make the job of forensic expert or forensic investigator hard. (Donny & Narasimha, 2013) For the user to start the private browsing in Chrome, press Chrome Menu > New Incognito window. Alternatively incognito window can be opened from Ctrl+Shift+N shortcut. The user can enjoy private browsing unless he himself turns it off.

5.1 Google Incognito providing false sense of security

From a logical view point, it does make sense that for the browser to function normally, even in the private mode, it needs to write some amount of useful data or commands/instruction to a portion of disk. Where is it written, and whether it gets deleted or not, is a million dollar question because Google do not provide any public specification document on Google Chrome’s Incognito Mode Implementation. (Jessica, n.d).

Google Chrome does not store any web activity of the user who has enabled private browsing mode in his browser, but it certainly doesn’t stop the operating system, websites and the router from keeping account of what the user do. Thus in reality, these web browsers give a false sense of security to the users, and do not completely guarantee the secrecy and privacy of the user’s browsing activities.

5.2 Detecting private mode:

Since the evidence extraction for private mode of operation is slightly different from the regular mode the forensic examiner needs to know whether the suspect uses private mode or not. A simple indication for private mode on an opened browser is the presence of Incognito sign and the absence of Recent tabs bar. But if the browser if closed, the forensic examiner can run Chrome Cross-mode

Interference inspector application on the suspect’s PC to see when the private mode was enabled and where was the data stored.

The subsection that follows gives brief forensic analysis of the Google Chrome’s Incognito mode. Before this experiment, Google Chrome was fully uninstalled and then reinstalled so as not to confuse between the artifacts obtained from regular and private modes of Chrome. The chrome was opened in private incognito mode and some browsing, downloading and surfing was done to check whether private browsing mode keeps artifacts or not. The results of the research are:

5.2.1 Web Activity

Private browsing mode though enabled keeps track of user internet activity. The History file, present in the default Chrome Folder, when opened in SQLite browser after closing the browser, as proved by the snapshot in Figure 14 below, shows that Chrome does store visit time but not the actual URL of the page visited. However using BelkaSoft RAM capturer, the analysis of the captured RAM indicates the presence of browsed websites in the RAM. (Noorulla, 2014)

| id | url | visit_time | from_visit | transition | segment_id | visit_dt |
|----|-----|-----------------|------------|------------|------------|----------|
| 1 | 1 | 130660731943... | 0 | 805306368 | 0 | 0 |
| 2 | 2 | 130659111083... | 0 | 805306368 | 0 | 0 |
| 3 | 3 | 130659071785... | 0 | 805306368 | 0 | 0 |

Fig. 14 SQLite DB (History file after browser was closed)

5.2.2 Cache

Like regular browsing mode, private browsing mode stores cache files in the Temporary Internet Files folder of Google Chrome. Snapshot shown in Figure 15 below shows the cache files viewed in Chrome Cache Viewer, after the browser was closed.

| URL | Content Type | File S... | Last Accessed | Server Ti... | Server Last... |
|------------------------|-----------------------|-----------|-----------------------|--------------|-----------------|
| https://oauth.go... | text/javascript | 22,632 | 1/18/2015 10:22:36 PM | 1/18/201... | |
| https://ssl.gstatic... | text/javascript | 3,408 | 1/18/2015 10:22:36 PM | 1/14/201... | 1/8/2015 5:2... |
| https://apis.goog... | application/javasc... | 4,933 | 1/18/2015 10:22:36 PM | 1/18/201... | |
| https://www.goo... | image/png | 2,372 | 1/18/2015 10:22:35 PM | 1/18/201... | 11/20/2013... |
| https://www.goo... | text/javascript | 1,934 | 1/18/2015 10:22:35 PM | 1/18/201... | 4/2/2014 5:3... |
| https://www.goo... | image/png | 9,737 | 1/18/2015 10:22:35 PM | 1/18/201... | 12/1/2012 1:... |

Fig. 15 Cache file opened in Chrome Cache Viewer

5.2.3 Cookies

In private browsing mode, the cookies are associated with a session time, and hence expire once the browser closes. They can thus only be copied, if the browser is left open.

5.2.4 Bookmarks

They can be easily seen, by just clicking the Bookmarks file present in Default folder, even after session expires. Thus, bookmarks need to be manually deleted by user.

5.2.5 Third Party Websites

Private browsing may temporarily hide the data from someone, trying to search for browsing activity in browser history, but the third party websites are still able to trace the IP, track user's activity and send malwares via links/pop-ups.

5.2.6 Downloads

The download list is cleared after the browser closes, but the downloads can still be seen in the downloads window and needs to be manually deleted.

5.2.7 Other Observations

WebData and Shortcut files when viewed in SQLite Viewer gave no data. Neither Chrome gives suggestions when typing URL/ form data nor it saves any user credentials.

Though data is deleted at the expiry of the session in private web browsing but this data certainly does not get wiped off the drive. The forensic examiner should therefore know all places and folders where the internet activity of the user and browser preferences gets stored. He may use any forensic tool e.g. FTK Toolkit etc. to view the deleted data. (DFIRninja, 2014)

6. Google Chrome's Portable Web Browser Forensics

Operating in Portable mode means that the user installs the portable version of web browser i.e. "Google Chrome Portable" on a portable medium (e.g. a removable hard disk) or cloud service and uses it on any PC. Since the browser has been installed on the portable medium, the artifacts get stored in the same installation folder too.

The portable feature allows the user to keep his data including downloads, bookmarks, saved videos, music, browser extensions etc. with him, all the time, in his portable drive. This not only loads the webpages faster but also provides greater privacy to the user by storing the browser related data in portable drive.

Bad guys can use it in corporate computers where no browser is installed/ allowed. Portable browser however, is a great challenge for forensic investigators, because if the removable media is unplugged by the suspect/criminal, the artifacts are out of the reach of the forensic examiner. (Divyesh & Nagoor, 2014). Essentially all the browsing history, cookies, cache files, downloads, auto fill data was required to be stored in the removable disk from which the browser was running, but it was interesting to note that Chrome's portable mode of operation also leaves artifacts

like browsing history, images, downloads, credentials, etc. on the host system in the NTFS Allocated and Unallocated space, Pagefile.sys, Memdump, System32/Winevt/logs etc. (Donny & Narasimha, 2013). Hence the objective of this research was to find any artifacts of user's activity in Google Chrome Portable that might have got stored in his PC.

Another problem that forensic investigator faces while handling cases of portable web browsing is that there is no way to determine whether any web browser was used in portable mode or not. In such criminal cases, where the forensic analysis of web browser in portable media is required, the forensic analyzer must first check the list of portable/ removable media attached to the computer, by analyzing the Windows Pre-fetch files or the Windows' registry via regedit command. He should then check locations where Portable Chrome might save artifacts, and then conclude his observations.

Experiment involves downloading the Google Chrome Portable browser in Kingston 16 GB USB and installing it. Google Chrome application present in USB was then run on HP Pavilion laptop. For traces to be available in Chrome folder and other memory locations, surfing was done for quite some time and then changes in the default Chrome Folder were noted. As part of research, other important drive locations were also searched for internet evidences.

The image of both hard drive and USB were taken via FTK Imager and then the search keywords were analyzed via FTK Search function. It was revealed that part of the browsing data was stored in GoogleChromePortable/data/profile/Default folder and free space in USB. However browsing history, cookies, cached websites, saved passwords etc., also got stored in the ../LocalSettings/Temp/GoogleChromePortable folder in the C drive, and remained there even after the USB, containing Portable Chrome application, was detached. Although the artifacts retrieved from the drive in this experiment were less than the artifacts found in normal Chrome browsing session, they are sufficient for the forensic investigator to reconstruct the browser session. Thus, Google Chrome Portable version also provides a false sense of security to the users.

6.1 Forensics of Chrome Portable Incognito mode

The private web browsing mode also exists within the portable Chrome browser. This Portable Incognito mode is even safer than the normal Incognito or portable mode of operation. Same experiment was conducted, but with Incognito mode enabled in Google Chrome Portable web browser. The results obtained from the FTK Live Search indicate that web browsing data get stored in the free disk space of USB. The incognito mode, despite its claim to rarely leave any trace on computer's disk, leaves abundant internet artifacts in the virtual swap file. (Marrington, I,

2012). The wealth of artifacts, however, varies according to the amount of PC's RAM, number of active processes, and size of swap file. Since this virtual swap file is quite frequently overwritten, the investigator can only extract data for the most recent portable browsing sessions only.

7. Summary of Preliminary Changes

The working of Google Chrome in all three modes of operation is quite different. Table 3 below, summarizes the forensic analysis of Google Chrome in normal, private and portable mode of operation.

Table 3. Summary of Chrome Mode of Operation

| Mode | Forensic Analysis |
|-------------------------|--|
| Normal Mode | <ul style="list-style-type: none"> Browsing history, cached websites, cookies, downloads, saved passwords etc. are stored in ..\Chrome\User Data Directory in C drive |
| Private Mode | <ul style="list-style-type: none"> Cookies, Bookmarks, History etc. gets stored in the Default Chrome folder <ul style="list-style-type: none"> Browsed websites can be seen in RAM New timestamp replaces chrome_shutdown_ms.txt on session expiry User credentials and videos not stored |
| Portable mode | <p>Forensic artifacts were found in</p> <ul style="list-style-type: none"> Drive: Data is stored in ..\LocalSettings/Temp/GoogleChromePortable folder in C drive <ul style="list-style-type: none"> USB: Data gets stored in GoogleChromePortable\data/profile/Default folder and also in free space in USB |
| Portable Incognito mode | <p>Forensic artifacts were found in</p> <ul style="list-style-type: none"> USB: Data gets stored in free space in USB Drive: Data gets stored in pagefile.sys |

8. Future Trends

Web Browser forensics has become an important field of research for the forensic researchers. Today, most of the Web browser Forensic tools target any specific web browsers, and those few that are able to analyze multiple web browsers, lacks the accurate artifacts extraction. In order to address this issue, a methodology should be designed to analyze multiple browsers simultaneously with one tool, and integrate their data according to the timestamps for integrated artifact analysis. Based on this designed methodology, a forensic tool should be developed for the forensic experts, to speed up their process of investigation. Moreover, since the web browsers are updated frequently, forensic analysts must be able to forensically analyze the newer versions too.

Like regular browsing mode stores a lot of data pertaining to the user's web activity on the drive, the private and portable web browsing modes that though claim to provide privacy to users are not really secure. Before accepting claims of privacy of portable and private modes of other web browsers i.e. Mozilla Firefox, Internet Explorer, Opera etc., the forensic examiners need to

forensically analyze them too and find a way to trace the internet artifacts efficiently. Browser forensics should similarly be conducted on other Operating systems too.

Artifacts of web mail, instant messaging and social media applications like Facebook, Gmail, Yahoo, Twitter, MySpace etc., as discussed in the paper, gets stored mostly in the hyberfil.sys and pagefill.sys. Thus these system files must also be forensically analyzed in depth for more details.

However, since the trend of computer is gradually shifting towards the smartphone, the forensic investigator must also thoroughly carry out browser forensic of smart phones.

9. Conclusion

No user can browse safely on the internet. Whether the user has enabled the privacy mode or is working on a portable browser application, the browser tends to store a large amount of data regarding the user's surfing activity, his username passwords, downloads, temporary files, cache, form data and other browser specific data on the user's hard disk, and that is from where the forensic examiner can collect the artifacts from, to reconstruct the timeline of user's web activity.

Browser Forensic Tools are the best source for the forensic experts to find the artifacts from web browser, in case of any suspected illegal Internet activity. The forensic experts can therefore utilize the efficiency of these forensic tools to find internet artifacts from various different locations in the computer's memory. Though the stored web data can be traced down to the exact folder, the deletion of any evidence by the culprit can seriously affect the progress of the case.

References

- [1] Junghoon, Seungbong Leeb, Sangjin Leea. (2011) Advanced evidence collection and analysis of web browser activity. 11th Annual Digital Forensics Research Conference: volume 8.
- [2] Christopher Soghoian. (2010). Why Private Browsing Modes Don't Deliver Real Privacy. Google Scholar Citation.
- [3] D. Ohana; N. Shashidhar. (2013). Do Private and Portable Web Browsers Leave Incriminating Evidence? IEEE Symposium on Security and Privacy Workshops 2013. (pp. 135-142)
- [4] Divyesh G, Nagoor A R. (2014). Forensic Evidence Collection by Reconstruction of Artifacts in Portable Web Browser. International Journal of Computer Applications. vol. 91, issue 4. (pp. 32-35)
- [5] Marrington, I Baggili, Talal Ali. (2012). Portable Web Browser Forensics: A forensic examination of the privacy benefits of portable web browsers. 2012 International Conference on Computer Systems and Industrial Informatics (ICCSII), (pp. 1-6).

- [6] Satvat, Forshaw, Hao, Paper: On the Privacy of Private Browsing - A Forensic Approach. Journal of Information Security and Applications. Volume 19, Issue 1. (pp. 88-100)
- [7] Sandeep Kumar Khanikekar. (2010). Web Forensics. Graduate Thesis, A&M University, Texas.
- [8] Emad Sayed Noorulla (2014). Web Browser Private Mode Forensics Analysis, Graduate Thesis, Rochester Institute of Technology
- [9] DFIRninja (2014). In-Private Browsing: Not so private anymore. Retrieved from <http://malwerewolf.com/2014/06/inprivate-browsing-private-anymore/>
- [10] Kristinn (2010). Google Chrome Forensics. SANS Digital Forensics and Incident Response Blog. Retrieved from <http://digital-forensics.sans.org/blog/2010/01/21/google-chrome-forensics/>
- [11] Exposing the password secrets of Google Chrome. Retrieved from <http://securityxploded.com/googlechromesecrets.php>
- [12] Jessica Riccio. Can You Browse Internet in Secrecy? Retrieved from http://burgessforensics.com/Browse_Web_Secret.php
- [13] Gaurang Patel (2014). Anti-forensics techniques for browsing artifacts. Retrieved from <http://www.slideshare.net/gaurang17/anti-forensicstechniquesforbrowsing-artifacts>
- [14] Sarah Holmes (2010). How Google Chrome stores Web History. Retrieved from <http://www.lowmanio.co.uk/blog/entries/how-google-chrome-stores-web-history/>
- [15] StatCounter Global Stats - Top 5 Desktop, Tablet and Console Browsers (2015). Retrieved from <http://gs.statcounter.com/>
- [16] Robert C. Newman (2007). Computer Forensics: Evidence Collection and Management. In Computer Abuse Investigation (pp. 66)