DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4433

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

WEB BROWSER FORENSICS: GOOGLE CHROME

Dr. Digvijaysinh Rathod
Institute of Forensic Science
Gujarat Forensic Sciences University
Gandhinagar, Gujarat (India)

Abstract: Internet users use the web browser to perform various activities on the internet such as browsing internet, email, internet banking, social media applications, download files- videos etc. As web browser is the only way to access the internet and cybercrime criminal uses or target the web browser to commit the crime related to internet. It is very important for the digital forensic examiner to collect and analysis artifacts related to web browser usage of the suspect. There are various browsers available in the market such as Google Chrome, Internet Explorer, Firefox Mozilla, Safari and Opera etc, among which Google Chrome is very popular among the internet user community. Our literature survey shows that most of the researches used prefetch file and live memory analysis as source of information to extract artifacts. In this research paper, we analyzed default artifacts location, history, cookies, login data, topsides, shortcuts, user profile, prefetch file and RAM dump to collect artifacts related to internet activities on windows installed Google Chrome. The outcome of this research will serve to be a significant resource for law enforcement, computer forensic investigators, and the digital forensics research community.

Keywords: Browser forensics, Google Chrome, Digital forensics, RAM analysis

INTRODUCTION

The internet browser is the only way to access the internet and internet users use it to access internet for purpose such as accessing email, intent banking, accessing social networking sites etc. Malicious (suspect) users is try to steal sensitive and confidential information of the internet user to gain personal financial benefit. This confidential information can be users banking credentials; users email addresses, user address book, social security number, user address book or even hack into someone's system for personal or professional rival. It is very important for the digital forensic examiner to know various ways to perform forensics of web browser [1] and these forensically collected artifacts form the suspect's browser can be useful in examination of case related to cybercrime. The aim and objective of the research paper is to identify source of information along with sound forensic techniques to collect evidences which shows internet usage. To maintain the privacy and security of the end user, various browser vendors introduced private browsing or Incognito Mode [2]. By using this mode information such as webpage history, form data and passwords, cookies, temporary internet files, anti-phishing cache, address bar, search auto complete, automatic crash restore (ACR), and document object model (DOM) discard when the browser is closed [3]. The study [4] shows that desktop browser market share of Google Chrome, Microsoft Internet Explorer, Firefox, Microsoft Edge, Safari, Opera, and other is 59.7%, 16. %, 12.32%, 5.65%, 3.66%, 1.21% and 0.81% respectively. So Google Chrome is the leading internet browser and focus of this paper is to use various digital forensic techniques and information source to collect artifacts related to internet usage.

The rest of the paper is organized as follows - the related research paper review is discussed in section II, about Google Chrome, source of artifacts and digital forensic techniques is discussed in section III. The research paper is concluded with comments in section IV.

LITERATURE SURVEY

Donny J Ohan , Narasimha and Shashidhar [3] has conducted research on artifact extraction of Google Chrome, Mozilla Firefox, Apple safari and Internet Explore in private and portable browsing mode. Their major focus is to see that artifacts related to private browsing, browsing history, usernames / email accounts, images, and videos is discovered or not. Andrew Marrington, Ibrahim Baggili and Talal Al Ismail [5] has discussed the forensics of Google Chrome in normal and private mode and extracted evidences related to internet activity from hard disk. Research paper wrote by JunghoonOha, SeungbongLeeb and SangjinLee [1] has considered browser's log file as source of information to extracted potential artifacts. Huwida Said, Noora Al Mutawa and Ibtesam Al Awadhi [2] extracted evidences using RAM analysis.

Our literature survey shows that most of the researcher used browser log, local files or RAM analysis as source of information to extract artifacts related of internet usage. In our research paper, we used broader range of information source such as default artifacts location, history, cookies, login data, topsides, shortcuts, user profile, prefetch file and RAM analysis which gives an opportunity to extract more, related and various types of artifacts related to cybercrime.

In the next section, we discussed overview of Google Chrome, different sources of information along with digital forensic techniques to extract evidences related to internet usage.

GOOGLE CHROME FORENSICS TECHNIQUES

Google chrome store data in SQLite format and we can examine using SQLite database viewer [6]. The data base file that contains the Google chrome browsing history is

stored at default folder History. These tables are downloads, presentation, urls, keyword_search_terms, segment_usage, visits, meta, segment which is very important for forensic

Table – 1 point of view. The default artifacts location of Google Chrome shown in

Operating System	Path
Microsoft Windows Vista/7/8	History, Downloads and Cookies : C:\user\{username}\AppData\Local\Google\Chrome\User Data\Default\
	Cache **:** C:\user\{username}\AppData\Local\Google\Chrome\User Data\Default\
Apple Macintosh OS X	History, Downloads and Cookies : /Users/{users}/Library/Application Support/Google/Chrome/Default/
	Cache **:** /Users/{user}/Library/Caches/Google/Chrome/Default/Cache/
GNU / Linux	History, Downloads and Cookies : /home/{user}/.config/google-chrome/Default/
	Cache **:** /home/{user}/.cache/google-chrome/Default/Cache/

Analysis of History

History file contains all browsing information of the users like visited links (URLs), downloads, search terms, and download chains etc. This history file can be viewed using SQLite database viewer. We can see the database structure (Figure -1) of the history file. There are 9 tables in this file and 13 indices, views and triggers. There is also option of the browse data, edit pragmas, and execute SQL. Execute SQL can help examiner to parse evidence using SQL statements.

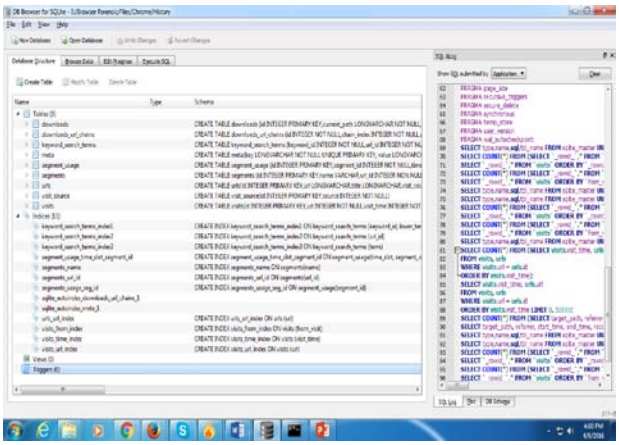


Figure -1 Database schema and plot (graph) view

We discussed the analysis of important tables of history in the next section

Downloads

This table shows (Figure -2) what type of stuffs downloads by the user. It also gives information like id, current path, target path, start time (web kit time format), received bytes, total bytes, state, danger type, Interrupt reason, end time, opened, refer, last modified, mime type, and original mime type of the downloaded file. SQLite browser gives time in web kit time stamp, so it is necessary to covert this time into readable time format.

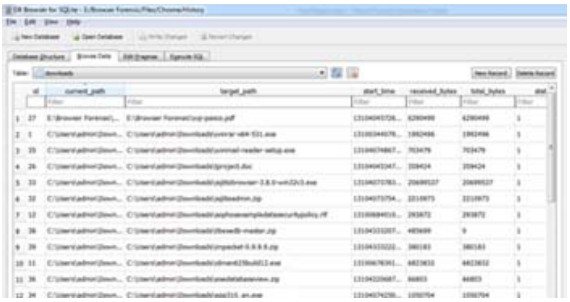


Figure -2 Database schema and plot (graph) view of Downloads

downloads_url_chains

This table (Figure – 3) gives list of URLs from which files were downloaded (audio, video, document etc.) by the user. As shown in the figure the user download WinRAR 64 bit tool from www.filehippo.com and autopsy-4.0.0-64bit from the sorcrforge.net.

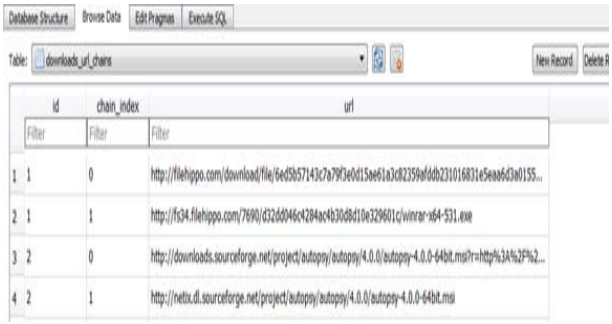
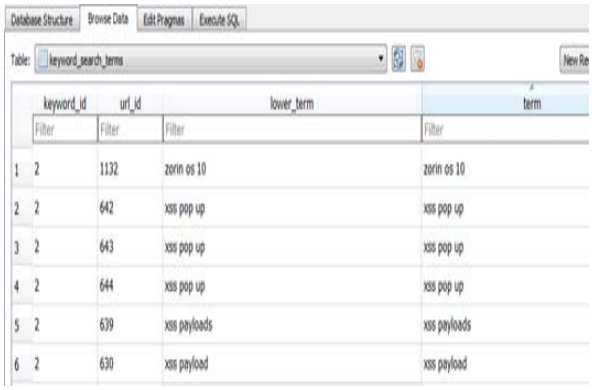


Figure 3 downloads_url_chains

keyword_search_terms

Keyword search terms play important role to understand user's psychology. This table store the user entered keyword along with keyword_id, url_id, lower_term, and term. Figure 4 shows the user entered keywords such as zorinos 10, xss pop up, xss payload, xenu tool etc.

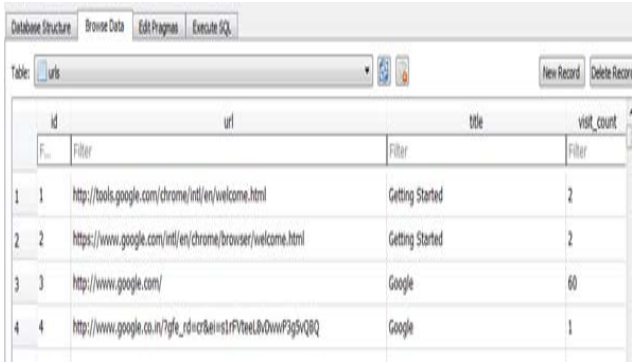


	keyword_id	url_id	lower_term	term
1	2	1132	zorin os 10	zorin os 10
2	2	642	xss pop up	xss pop up
3	2	643	xss pop up	xss pop up
4	2	644	xss pop up	xss pop up
5	2	639	xss payloads	xss payloads
6	2	630	xss payload	xss payload

Figure 4 keyword_search_terms

URLs

This is the most important table which shows the URLs list visited by the user along with id, url, title, visit count, type count, last visit time, hidden, and favicon id. Figure 5 shows the visited ulrs by the user.

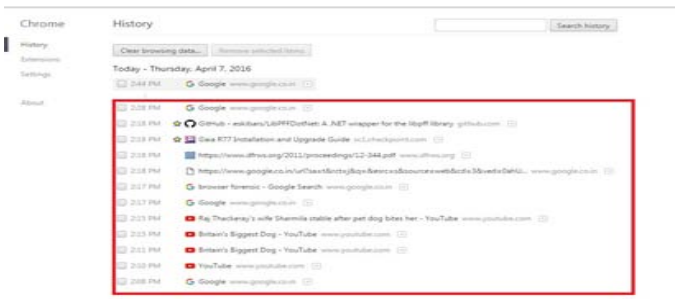


	id	url	title	visit_count
1	1	http://tools.google.com/chrome/intl/en/welcome.html	Getting Started	2
2	2	https://www.google.com/intl/en/chrome/browser/welcome.html	Getting Started	2
3	3	http://www.google.com/	Google	60
4	4	http://www.google.co.in/?gfe_rd=cr&ei=s1rFVteeLbXowP3g5vQBQ	Google	1

Figure 5 keyword_search_terms

Recovered Deleted History

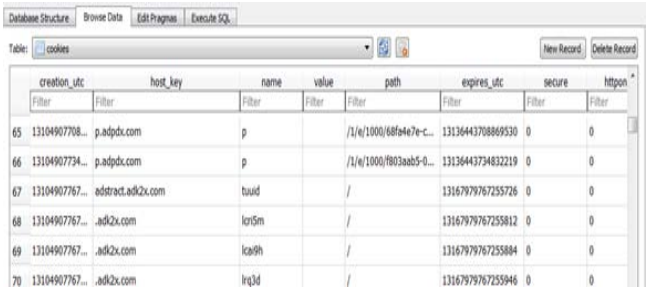
Cybercrime criminals normally delete the history of browser. We intentionally deleted the history of Goolge Chrome and tried to recovery those deleted history manually. We used System Previous versiion For manually recovey for which we negated to C:\Users\admin\AppData\Local and found Google folder; and selected properties, clicked on previous version tab (Figure 6) and click on restore option. In this tab there are so many options for previous version of browser with date and time. For case we mentioned, recovered history shown in figure 6



.Figure 6 Previous version

Analysis of Cookie

Cookie are files which are created when user visit any website. Cookies store site preference and profile number. Two types of cookie will be generated when user visit any website and another being generated for the advertisement purpose. Cookie help websites to track of user preferred setting, so that when user re-visits any website, cookie reload previous setting of the user for that same site. As shown in the Figure 7, we can get the information such as creation_utc, host_key, name, value, path, expires_utc etc. Here host_key gives details of visited link

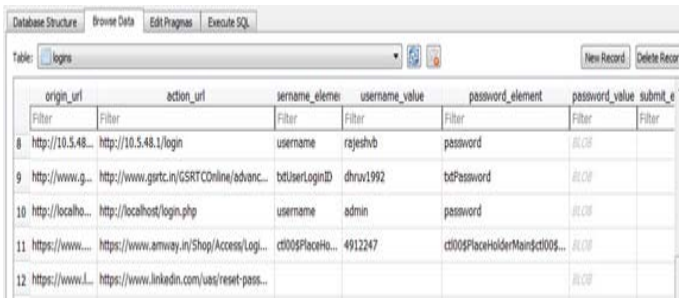


	creation_utc	host_key	name	value	path	expires_utc	secure	httpon
65	13104907708...	p.adpdx.com	p		/1/e/1000/68fa4e7e-c...	13136443708869530	0	0
66	13104907734...	p.adpdx.com	p		/1/e/1000/f803aab5-0...	13136443734832219	0	0
67	13104907767...	adstract.adk2x.com	tuuid		/	13167979767255726	0	0
68	13104907767...	.adk2x.com	lcrSm		/	13167979767255812	0	0
69	13104907767...	.adk2x.com	lca9h		/	13167979767255884	0	0
70	13104907767...	.adk2x.com	lrq3d		/	13167979767255946	0	0

Figure 7 Cookies

Login Data

This database file gives information of user login detail along with detail related to : Origin_url and action_url holds the visited websites list, username_elememt, username_value holds entered user name of the user, and password element (Figure 8) etc. Here login data file have three tables namely logins, meta and stats. Meta table contains three values like version, last_compatible_version and mmap status. In our case, there is no detail is available in Stats table.



	origin_url	action_url	username_value	password_element	password_value
8	http://10.5.48...	http://10.5.48.1/login	rajeshvb	password	BLOB
9	http://www.g...	http://www.gsrtc.in/GSRTCOnline/advanc...	txtUserLoginID	dhruv1992	txtPassword
10	http://localho...	http://localhost/login.php	username	admin	password
11	https://www....	https://www.amway.in/Shop/Access/Logi...	ctl00$PlaceHo...	4912247	ctl00$PlaceHolderMain$ctl00$...
12	https://www.l...	https://www.linkedin.com/uas/reset-pass...			

Figure 8 Login Data

Topsites

Topsites database contains top visited sites in Google chrome by the user. This information stored in thumbnails table.

Shortcuts

This database file contains two tables one is Meta and another is Omnibox history. Omni box is the advance features of Google Chrome with auto complete capabilities. This contains information such as id, text, urls, contents, and description, content_class, description, description_class, last access time, number of hits, fill_into_edit, type, and keyword.

User Profile

When user login in to chrome then one separate profile of that user created at C:\Users\admin\AppData\Local\Google\Chrome\User Data (Figure 8)

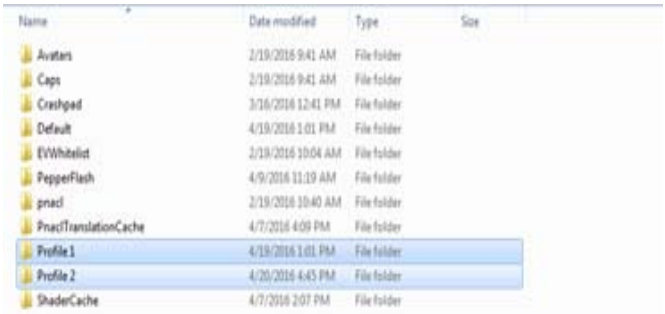


Figure 8 User Profile

Analysis of Prefetch File

Prefetch file play important role in forensic because it holds information like how many time executable file run, last executable time, volume information, directory storage, loaded resources etc. Prefetch file helps application to reduce startup time of the application. Last execution date & time of the Google chrome browser, run count, volume entry of Google Chrome file along with creation date & time and serial number shown in figure 9

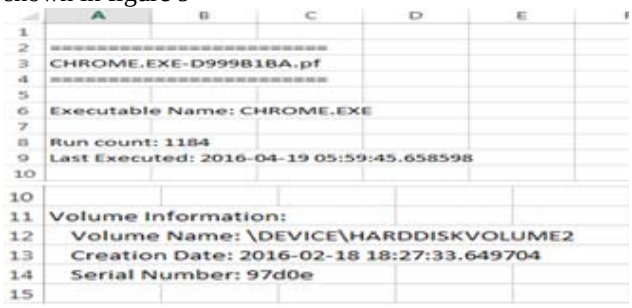


Figure 9 Last execution time and volume information

Live Memory Forensics

Private browsing artifacts will be collected using RAM dump of the system. We visited Gmail, Facebook, Twitter and Firefox in private mode and try to extract evidences related to same using RAM dump analysis. We took RAM dump of system using Belkasoft and analyzed RAM dump using HXD and apply filter to find visited web sites. As shown in figure 10, we can see the web site link visited by user in Incognito mode.

CONCLUSION

As web browser is the only way to access the internet and cybercrime criminal uses or target the web browser to commit the internet related crime. By considering this fact, web browser forensics is the most important for digital forensic examiners. As Google Chrome is the leading web browser and in this research paper, we discussed various source of information such as default artifacts location, history, cookies, login data, topsides, shortcuts, user profile, prefetch file and RAM dump to collect artifacts related to internet activities on windows installed Google Chrome. Our research clearly shows after applying various digital forensic techniques mention in this research paper to extract an evidences, digital forensic examiner can obtain information regarding last accessed date and time of Google Chrome, search items, visited URLs, and how to recover deleted data. The outcome of this research will serve to be a significant resource for law enforcement, computer forensic investigators, and the digital forensics research community.

REFERENCES

[1.] JunghoonOha, SeungbongLeeb and SangjinLee Advanced evidence collection and analysis of web browser activity, Elsevier - Digital Investigation, Volume 8, Supplement, August 2011, Pages S62-S70.

[2.] Huwida Said, Noora Al Mutawa and Ibtesam Al Awadhi, Forensic analysis of private browsing artifacts, 2011 International Conference on Innovations in Information Technology25-27 April 2011.

[3.] Donny J Ohan, Narasimha 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, December 2013, 2013:6

[4.] Desktop Browser Market Share, https://www.netmarketshare.com/browser-market-share.aspx?qprid=0&qpcustomd=0, July, 2017.

[5.] Andrew Marrington, Ibrahim Baggili and Talal Al Ismail, Portable web browser forensics: A forensic examination of the privacy benefits of portable web browsers, 2012 International Conference on Computer Systems and Industrial Informatics, 18-20 Dec. 2012.

[6.] Huwida Said, Noora Al Mutawa and Ibtesam Al Awadhi, Forensic analysis of private browsing artifacts, 2011 International Conference on Innovations in Information Technology, 25-27 April 2011

[7.] Murilo, T. P. (2009). Forensic analysis of the Firefox 3 internet history and recovery of deleted SQLite records. Digital Investigation, 5, 93-103.