Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 7, Issue. 7, July 2018, pg.112 – 122

Investigating Google Chrome 66.0.3359 Artefact: Internet Forensics Approach

Ntonja Morris[1]
Digital Forensics
Cranfield University, United Kingdom
m.ntonja@cranfield.ac.uk

Ashawa Moses[2]
Cyber Defense and Security
Cranfield University, United Kingdom
m.ashawa@cranfield.ac.uk

Abstract*: *Evidence identification, extraction and analysis are crucial in the field of digital forensics and security at large. Evidence credibility, integrity and admissibility can help in deciding whether a criminal will be refuted or charged in a law court. One of the founts through which evidence is mined is Google chrome. Apart from Explorer, Edge, Firefox, Safari, Opera, UC Browser among many other browsers, Google chrome is one of the leading web browser versions which is compatible with many OS platforms including Android devices. Suspects can exploit web browsers in many ways, for instance by using them to collect information about their targets, to hide their crime as well as to search about new crime methods. Significantly, searching for artefacts left by browsing activities is significant in unearthing these activities. This research aims to establish forensic artefacts left by Google chrome web browser when using History Eraser version 4.8.7.5 extension installed on Google Chrome version 66.0.3359.181 running on Windows 10 operating system.

Keywords: Forensics artefacts, Google chrome browser, $130 file, History database, extensions

I. INTRODUCTION

With the increased number of web users across the world, web browsers have become some of the most widely used computer applications. Indeed, web browsers provide a platform for internet browsing, e-mail access, social networks access, internet download, file sharing as well as numerous other online activities. Some of the browsers commonly used are internet explorer, edge, Firefox, chrome, safari, opera, uc browser among many other browsers compatible with a variety of operating systems used in computers and mobile devices. A global market survey conducted by statistic in 2018 on leading web browser versions [1, 2] as of February 2018 indicated that Google chrome version 66 was the most popular browser accounting to 27.62% of users while Google chrome version 63 was a second most popular browser with 13.76% popularity. The originality of the research is from the fact that no one has investigated on this latest browser version.

According to [3] suspects can exploit web browsers in many ways, for instance by using them to collect information about their targets, to hide their crime as well as to search about new crime methods. Significantly, searching for artefacts left by browsing activities is significant in unearthing these activities. The release of new

chrome versions and continuous development of addons by various developers is likely to present a challenge to internet forensic investigators looking to find evidence left by use of chrome browser. While researches have been conducted on artefacts left by use of google chrome browser and little documented on using chrome on forensic implications of using on incognito mode, there is no single research that has addressed the use of artefact wiping addons on chrome.

This paper brings some contributions in the internet forensics research. First, the paper involves experimentation using chrome browser version 66.0.3359.181 running on windows ten computers. Secondly, the paper investigates artefacts produced by use of history clear 4.8.7.5 addon installed on Google chrome browser version 66.0.3359.181 running on windows 10. This is an important contribution to the research as there is limited documentation on research regarding this browser extension. Thirdly, there is no research which has been done on history clear addon as an artefact wiping tool and therefore this brings a completely new area of research on chrome web browser forensics. Finally, this paper will shed light on some implications of using history addon on chrome browser.

II. RELATED WORK

Certainly, many digital crime investigations involved analysis of web browsers for evidence related to user activities such as websites visited, search words, files downloaded and the access times using Internet forensics techniques. According to [4, 5, 6] internet forensics involves extraction, examination and identification of evidence associated with digital device online activities. Indicatively, most of the online activities are carried through the web browsers. As such, the internet or online related evidence may include artefacts such as history files, cached contents, cookies, as well as traces of data that are found in computer RAM as a result of browser use.

Also, [7, 8, 9, 10, 11, 12] in their research on Vista/7/8/10identified that Google chrome files are located in the following path; C:\Users\[Username]\AppData\Local\Google\Chrome. The research highlighted some essential extensions in Chrome browser such as History, Cache, Cookies and Bookmarks, for artefacts storage. It concluded that such extensions can be found on C:\Users\[Username]\AppData\Local\Google\Chrome\ User Data\Default, C:\Users\[Username]\AppData\Local\Google\Chrome\UserData\Default\Cache, C:\Users\[Username]\AppDataLocal\Google\Chrome\User Data\Default\Cookies and C:\Users\[Username]\AppData\Local\Google\Chrome\User Data\Default\Bookmarks.bak respectively.

The research of [13] on chrome focused on the analysis of forensic artefacts left by chrome installed on a Chromebook using Windows XP operating system virtual machine (VM). His investigation approach involved generating user artefacts on chrome browser running on a Chromebook and then using the active Gmail account registered on Chromebook to log on chrome browser installed on Windows XP VM. The research established the synced artefacts on chrome browser between the two operating systems. While the major strength of his research was on chrome forensic artefacts on Chromebook, one limitation noted was installing the ChromeAnalysis tool on Windows XP VM in order to parse the generated artefacts other than acquiring the dead image of the VM and then analysing it. It is generally suggested that disk imaging provides more forensically sound results hence it would be better to acquire a dead image of the VM and rather than analysing it using the software.

[14] Examined Web browser Private Mode forensics analysis provided some insight on chrome forensic artefacts that are generated when a user enables the incognito browsing setting in Windows 7 and 8 operating systems separately. The study involved launching chrome on incognito mode and accessing sites and then closing the browser and capturing the RAM for analysis of the possible artefacts. While this research focused on live analysis. This study is similar to the one carried out by [15, 16, 17, 18, 19, 20, 21, 22] which investigated how artefacts are mined in private browsers. The researchers however did not address artefacts left on lifeless imaging. The researcher did also not address the use of extensions to clear browsing data on chrome and their implications to chrome forensic artefacts investigation.

Similar to the above research, [23, 24, 25,] noted that the internet aids many criminal and illegal activities. Without any doubt, in the modern day digital forensics investigation, searching the artefacts left by use of browsers has become a significant part of the investigation process the law enforcement agencies. Examiners are likely to encounter a variety of browsers of which they are required to investigate. However, this is not without challenges of evidence destruction by criminals [26]. Evidence destruction can be accomplished by use of anti-

forensics techniques and methods [27, 28, 29, 30]. According to [31, 32], to avoid evidence detection during investigation, criminals deploy some tools and techniques to evade detection. One of the anti-forensic techniques used is artefact wiping which can be done using erasing tools.

III.METHODOLOGY

3.1 Introduction

Section 3.1 has discussed the need for research on web browsers artefacts and emphasised the importance of research on Google chrome which is currently the most popular web browser as reported by market share surveys. This section outlines the methodology used in the research including the research question, overall method, choice of experimental samples, tools used and finally the experiments conducted.

3.1.1 Research Question

Based on the following criteria;

I. The use of History Clear addon to clear chrome browsing history.
II. Settings on History Clear addon that can wipe all the browser artefacts.
III. The possibility of failing to detect the usage of addon by internet forensic investigators.

A research question has been formulated.

"Is it possible to identify usage of History Eraser version 4.8.7.5 extension installed on Google Chrome version 66.0.3359.181 running on Windows 10 operating system when used to wipe the browser data?"

3.1.2 Research Objectives

To answer the research question the following objectives were set;

i. To identify history artefacts that exist when windows 10 is installed with Google Chrome 66.0.3359.
ii. To identify history artefacts present when History Eraser V.4.8.7.5 addon is installed on Google Chrome 66.0.3359.
iii. To determine uninstalled $130 files artefacts when Google Chrome version 66.0.3359 is used.
iv. To identify history database and extensions artefacts present on Google Chrome Browser version 66.0.3359 files when History Eraser V.4.8.7.5 addon is installed and set to clear history data on each of the EASY, MEDIUM, HARD and DEVELOPER modes.
v. To identify history database and extensions artefacts present on Google Chrome Browser version 66.0.3359 files when History Eraser V.4.8.7.5 addon is installed and set to clear history on DEVELOPER mode and then UNINSTALLED from the browser.

3.1.3 Tools

Tools and software used in this research for experimental setup and data extraction are listed in the table below with their respective versions and methods.

Table 1: Tools and Software were used for Experimentation.

#	TOOL	VERSION	METHOD
1	VMware® Workstation	14 Pro	Used as virtualization tool for virtual machine construction
2	Windows 10 Home	1803	Used as the operating system in the virtual machines
3	Google Chrome	66.0.3359	The sampled browser which was being investigated
4	History Eraser	4.8.7.5	The chrome extension which was being investigated
5	AccessData FTK Imager	3.1.1.8	A tool used in the acquisition of the virtual machine as well as visualization of chrome directory files

6	Arsenal mounter version	4.2.6	Used to mount acquired virtual machine images and extract the chrome files for investigation
7	Winhex version	4.0.1	Used in artefacts analysis
8	DB Browser for SQLite	3.10.1	Used in artefacts analysis

IV. EXPERIMENTATION

To achieve the aim stated in the research objectives, a total of eight (8) different but related experiments were performed. Experimentation was conducted using virtual machines running on Windows 10 Home operating system. The virtual machines were created and installed with the Google Chrome version 66.0.3359.181 which was then installed with History Eraser version 4.8.7.5 extension. History Eraser version 4.8.7.5 extension was then used to clear Chrome browser on Easy, Medium, Hard and Developer modes and then uninstalled. Significant artefacts resulting from each experiment were analysed using Winhex Hex Editor and DB Browser for SQLite tool. It was established that changes in few chrome files which included History database, extension cookies and $130 file which is produced when the extension is uninstalled would essentially help in identification of usage of History Eraser version 4.8.7.5 extension or any other extension installed on Google chrome browser.

For experimentation purposes, there was a need to make some particular choices. First, Windows 10 operating system was chosen as a workstation for virtualization and experimental artefacts analysis as it supports Google chrome latest version. The choice to use Google Chrome 66.0.3359 was made as it was the most popular web browser worldwide. Finally, the choice to use History Eraser extension was made due to its excellent rating and review in Google chrome website (https://chrome.google.com/webstore/detail/history-eraser/gjieilkfnnjoihjjonajndjldjoagffm/reviews?hl=en). As of the time of this research, the extension had over 692624 users as per the website statistics.

V. RESULTS

5.1 Important artefacts in the experimentation

Prior to chrome databases analysis it was essential to understand how chrome timestamps work. Google chrome browser timestamp is formatted as numeral of microseconds since January 1601. As such the following command can be used in time and date conversion (time / 1000000 + (strftime('%s', '1601-01-01')), 'unixepoch') [33].

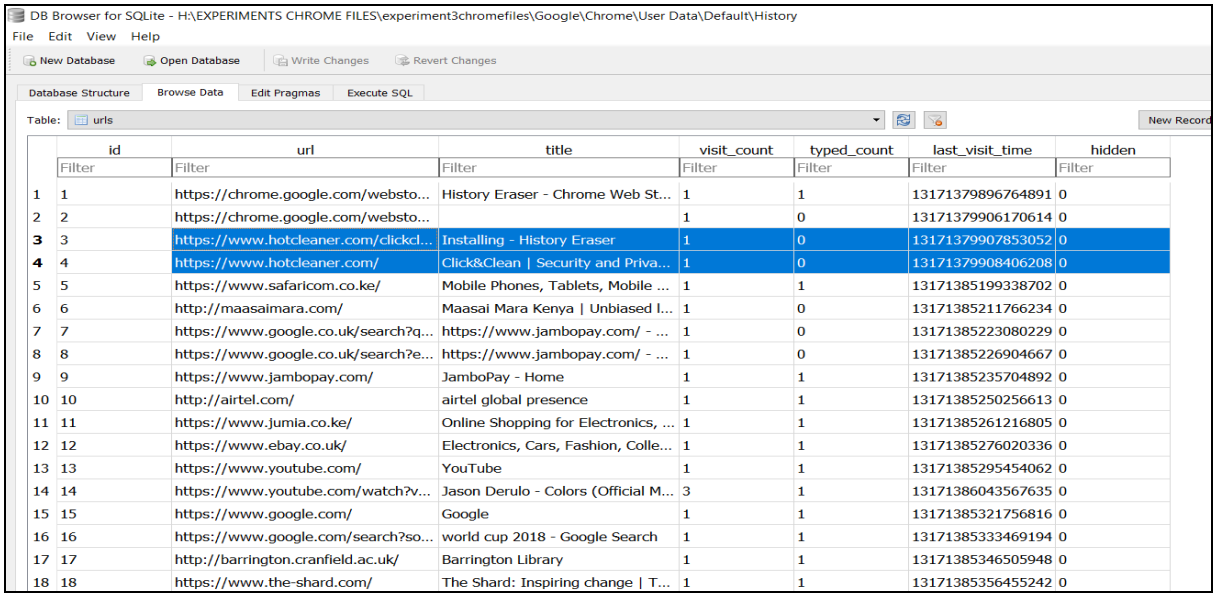
5.2 History Database

Analysis on history database on experiment 2 established a link https://www.hotcleaner.com/clickclean/install-eraser.html which was used in installing the history eraser extension ID: gjieilkfnnjoihjjonajndjldjoagffm on 2018-05-21 12:38:27. This was established after execution of SQL query;

```
SELECT
  url, title, visit_count, datetime(last_visit_time / 1000000
+ (strftime('%s', '1601-01-01')), 'unixepoch')
FROM urls
ORDER BY last_visit_time  DESC
```

Figure 1: History Database during SQL query

Sqlite_sequence table on the history database kept statistic of all the accessed URLS by the browser. While the subsequent history databases involved clearing browsing history, analysis of deleted history artefacts in the final experiment could establish if the extension had been installed at some point. The recovered history is shown below. It showed the Url visited and the information of the meta-data sought for. The activity ID for each Url, the visit_count, typed_count, last_visit_time were respectively recovered as.


DB Browser for SQLite - H:\EXPERIMENTS CHROME FILES\experiment3chromefiles\Google\Chrome\User Data\Default\History

File Edit View Help

New Database | Open Database | Write Changes | Revert Changes

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: urls

	id	url	title	visit_count	typed_count	last_visit_time	hidden
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	https://chrome.google.com/websto...	History Eraser - Chrome Web St...	1	1	13171379896764891	0
2	2	https://chrome.google.com/websto...		1	0	13171379906170614	0
3	3	https://www.hotcleaner.com/clickcl...	Installing - History Eraser	1	0	13171379907853052	0
4	4	https://www.hotcleaner.com/	Click&Clean | Security and Priva...	1	0	13171379908406208	0
5	5	https://www.safaricom.co.ke/	Mobile Phones, Tablets, Mobile ...	1	1	13171385199338702	0
6	6	http://maasaimara.com/	Maasai Mara Kenya | Unbiased I...	1	0	13171385211766234	0
7	7	https://www.google.co.uk/search?q...	https://www.jambopay.com/ - ...	1	0	13171385223080229	0
8	8	https://www.google.co.uk/search?e...	https://www.jambopay.com/ - ...	1	0	13171385226904667	0
9	9	https://www.jambopay.com/	JamboPay - Home	1	1	13171385235704892	0
10	10	http://airtel.com/	airtel global presence	1	1	13171385250256613	0
11	11	https://www.jumia.co.ke/	Online Shopping for Electronics, ...	1	1	13171385261216805	0
12	12	https://www.ebay.co.uk/	Electronics, Cars, Fashion, Colle...	1	1	13171385276020336	0
13	13	https://www.youtube.com/	YouTube	1	1	13171385295454062	0
14	14	https://www.youtube.com/watch?v...	Jason Derulo - Colors (Official M...	3	1	13171386043567635	0
15	15	https://www.google.com/	Google	1	1	13171385321756816	0
16	16	https://www.google.com/search?so...	world cup 2018 - Google Search	1	1	13171385333469194	0
17	17	http://barrington.cranfield.ac.uk/	Barrington Library	1	1	13171385346505948	0
18	18	https://www.the-shard.com/	The Shard: Inspiring change | T...	1	1	13171385356455242	0

Figure 2: History artefacts

5.3 Extension Cookies

Analysis of extension cookies in all the experiment indicated that extension Cookies has two tables named cookies and metadata of importance to the analysis and forensics was found to be cookies which stores the extension ID which is found under the host_key column and the creation and last access times which are found under creation_utc and last_access_utc columns respectively. These times were decoded using the following commands. Cookies like the last_access and trftime were recovered.

```
SELECT
  host_key, datetime(creation_utc / 1000000 + (strftime ('%s',
'1601-01-01')), 'unixepoch'), datetime(last_access_utc /
1000000 + (strftime('%s', '1601-01-01')), 'unixepoch')
FROM cookies
ORDER BY last_access_utc DESC
```

Figure 3: Extension Cookies

Analysis of extension cookies showed that extension keeps track of the last accessed time which appeared to be similar to the creation time. This implied that extension cookies are created when the extensions are last used.

Also, some important artefacts such as portable incognition of both the USB and the HDD sessions and the installed sessions were also recovered as shown below.

Image	Location
Portable Session HDD	\Documents and Settings\Administrator\Local Settings\Temp\GoogleChromePortable
Portable Session USB	\GoogleChromePortable\Data\profile\Default and drive free space
Portable Incognito Session HDD	pagefile.sys
Portable Incognito Session USB	Drive free space only
Installed Session HDD	\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome\User Data

Figure 4: artefacta recovery from pottable Google Chrome

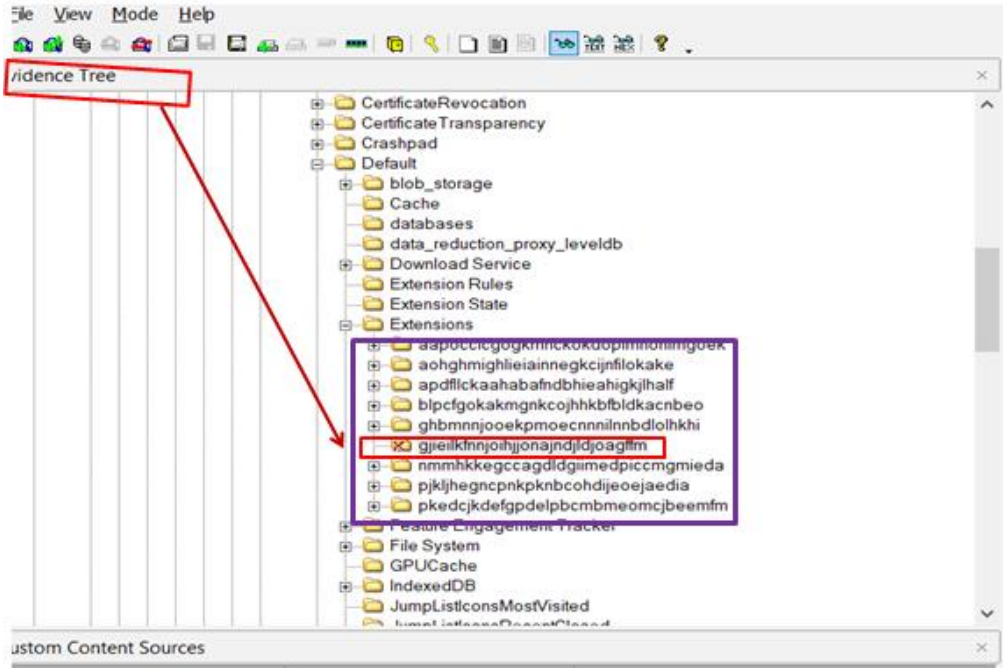


Figure 5: recoverage of the deleted file among the extensions

As shown from the listed of file extensions in the above figure, the deleted extension file from the data reduction level database was recovered from the bob_storage after it was deleted.

5.4 $130 file

$130 file was created when the extension was uninstalled from the browser. A keyword search of the extension **ID gjieilkfnnjoihjjonajndjldjoagffm** using Winhex HexEditor produced a hit implying that the extension had earlier been installed after it was uninstalled as shown below. The offset of the $130 file was found between sector 00001428 and 00001479 respectively.

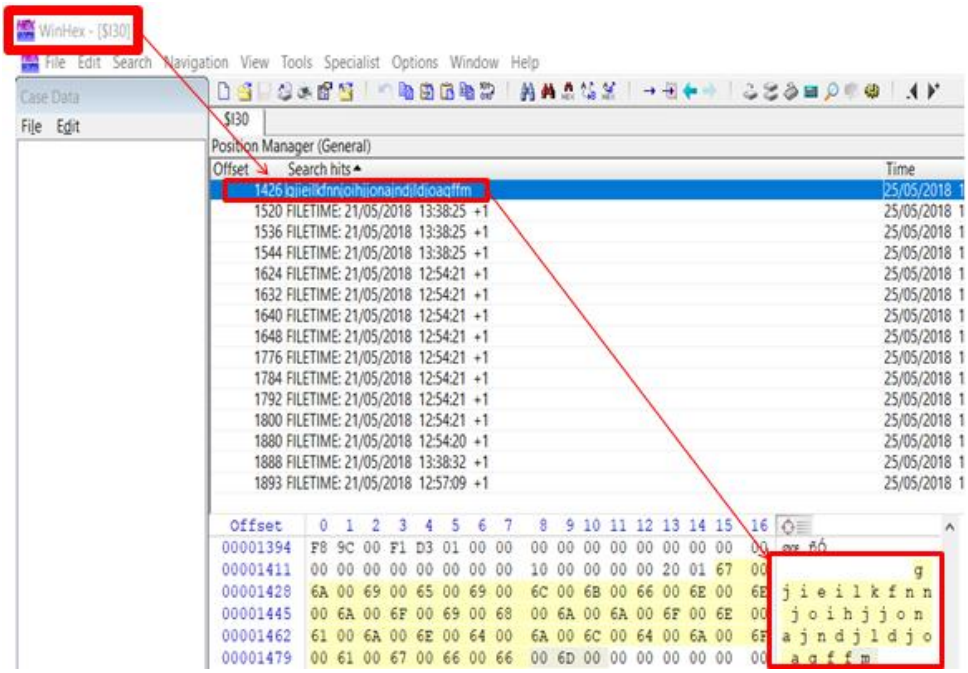


Figure 6: $130 files recovery

VI. SUMMARY OF FINDINGS

Research observation on key selected artefacts History database, extension cookies and $130 file are presented in the summary table below.

Table 2: Summary of Findings

EXPERIMENT	History SQLite Database	History Eraser Addon files	Extension Cookies	$130 file
1	Present but contained no browsing data. All the 12 history tables were empty.	Absent Extension directory contained 8 default extensions. History Eraser 4.8.7.5 extension ID gjieilkfnnjoihjjonajndjldjoagffm Did not exist.	Absent	Absent
2	Present The history database contained 12 tables. 10 TABLES all which were empty except URLS table which had 4 entries of URLs. These websites were the once accessed during installation of the History Eraser extension while another one was a resulting pop up. Sqlite_sequence table indicated 4 URLs entries.	Present: History Eraser 4.8.7.5 extension ID gjieilkfnnjoihjjonajndjldjoagffm Which was stored in the extensions Sub directory with file name gjieilkfnnjoihjjonajndjldjoagffm was introduced. A sub directory of this extension was introduced in the Chrome extensions directory making extensions sub-directories 9 in total.	Present	Absent
3	Present The history database contained 12 tables. The url table contained URL information of 57 links of sites and pages visited and the keyword searches. Sqlite_sequence table indicated 57 URLs entries	Present History Eraser 4.8.7.5 extension ID gjieilkfnnjoihjjonajndjldjoagffm Which was stored in the extensions Sub directory with file name gjieilkfnnjoihjjonajndjldjoagffm Continued to exist with all its settings files present. There was no evidence of the wiped data. The history Eraser extension directory gjieilkfnnjoihjjonajndjldjoagffm only contained settings to make the extension run.	Present Examination indicated Extension ID: gjieilkfnnjoihjjonajndjldjoagffm Creation utc: 2018-05-21 14:23:12 Last access: 2018-05-21 14:28:21	Absent
4	Present The history database contained 12 tables which were all found empty except one Sqlite_sequence table which appeared to keep statistic of cleared websites . The History Clear Extension had cleared all the history artefacts except Sqlite_sequence which indicated 57 URLs entries.	Present History Eraser 4.8.7.5 extension ID gjieilkfnnjoihjjonajndjldjoagffm Which was stored in the extensions Sub directory with file name gjieilkfnnjoihjjonajndjldjoagffm Continued to exist with all its settings files present. There was no evidence of the wiped data. The history Eraser extension directory gjieilkfnnjoihjjonajndjldjoagffm only contained settings to make the extension run.	Present Examination indicated Extension ID: gjieilkfnnjoihjjonajndjldjoagffm Creation utc: 2018-05-21 23:19:41 Last access: 2018-05-21 23:19:41	Absent
5	Present The history database contained 12 tables which were all found empty except one Sqlite_sequence table which appeared to keep statistic of cleared websites. The History Clear Extension had cleared all the history artefacts except Sqlite_sequence which indicated 57 URLs entries.	Present History Eraser 4.8.7.5 extension ID gjieilkfnnjoihjjonajndjldjoagffm Which was stored in the extensions Sub directory with file name gjieilkfnnjoihjjonajndjldjoagffm Continued to exist with all its settings files present. There was no evidence of the wiped data. The history Eraser extension directory gjieilkfnnjoihjjonajndjldjoagffm only contained settings to make the extension run.	Present Examination indicated Extension ID: gjieilkfnnjoihjjonajndjldjoagffm Creation utc: 2018-05-21 23:27:59 Last access: 2018-05-21 23:27:59	Present

6	Present The history database contained 12 tables which were all found empty except one Sqlite_sequence table which appeared to keep statistic of cleared websites. The History Clear Extension had cleared all the history artefacts except Sqlite_sequence which indicated 57 URLs entries.	Present History Eraser 4.8.7.5 extension ID gjieilkfnnjoihjjonajndjldjoagffm Which was stored in the extensions Sub directory with file name gjieilkfnnjoihjjonajndjldjoagffm Continued to exist with all its settings files present. There was no evidence of the wiped data. The history Eraser extension directory gjieilkfnnjoihjjonajndjldjoagffm only contained settings to make the extension run.	Present Examination indicated Extension ID: gjieilkfnnjoihjjonajndjldjoagffm Creation utc: 2018-05-21 23:43:11 Last access: 2018-05-21 23:43:11	Absent
7	Present The history database contained 12 tables which were all found empty except one Sqlite_sequence table which appeared to keep statistic of cleared websites. The History Clear Extension had cleared all the history artefacts except Sqlite_sequence which indicated 57 URLs entries.	Present History Eraser 4.8.7.5 extension ID gjieilkfnnjoihjjonajndjldjoagffm Which was stored in the extensions Sub directory with file name gjieilkfnnjoihjjonajndjldjoagffm Continued to exist with all its settings files present. There was no evidence of the wiped data. The history Eraser extension directory gjieilkfnnjoihjjonajndjldjoagffm only contained settings to make the extension run.	Present Examination indicated Extension ID: gjieilkfnnjoihjjonajndjldjoagffm Creation utc: 2018-05-22 09:49:58 Last access: 2018-05-22 09:56:01	Absent
8	Present The history database contained 12 tables which were all found empty except one Sqlite_sequence table which appeared to keep statistic of cleared websites. The History Clear Extension had cleared all the history artefacts except Sqlite_sequence which indicated 60 URLs entries. The extra 3 URLS were as a result of pop ups which resulted after the application was uninstalled.	Present History Eraser 4.8.7.5 extension ID gjieilkfnnjoihjjonajndjldjoagffm Which was stored in the extensions Sub directory with file name gjieilkfnnjoihjjonajndjldjoagffm Continued to exist but this time all its settings files had been deleted. The directory gjieilkfnnjoihjjonajndjldjoagffm remained though all its files had been deleted	Present The database was found to be empty	Present The deletion of the History Eraser 4.8.7.5 extension from chrome resulted to introducti on of $130 file in the extensions directory. A keyword search of the extension ID using winhex HexEditor reported 0ne hit gjieilkfnnj oihjjonajn djldjoagff m which was the history Eraser Addon

VII. RESEARCH EVALUATION

The virtual machines and all the experiments worked very well. Experiments indicated a number of important artefacts locations that can be investigated when carrying out digital forensic investigations involving usage of extensions to wipe the google chrome browser data. These artefacts locations were as follows;

C:\Users\InternetForensics\AppData\Local\Google\Chrome\User Data\Default\Extensions

C:\Users\InternetForensics\AppData\Local\Google\Chrome\User Data\Default\Extensions\$130

C:\Users\InternetForensics\AppData\Local\Google\Chrome\User Data\Default\History

C:\Users\InternetForensics\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies.

It was noted that when History Clear extension was uninstalled from the browser two artefacts that would indicate its usage was left. These were the directory with its ID as a name where the extension settings were stored and the $130 file which was created after it was uninstalled. As Google chrome names extension directories with their unique IDs then the remaining directory after they are uninstalled can play a significant role in reconstruction of the extension used and of which had been uninstalled from the browser. However, this could not be generalised to happen to all other extensions as the experiment was conducted using only one sampled extension. It would be important to test how chrome uninstalls various extensions and what can kind of artefacts are left after they are uninstalled. For future research on Google chrome extensions, this could be considered.

While the experimentation involved observing changes in few chrome files which included History database, extension cookies and $130, in future experiments, it would be essential to look at how extension activities would affect browser cookies, top sites, last sessions, last tabs, favicons, current tabs and all other chrome databases. The future work on this experiment will involve examination of the history database and the $130 file for possibilities of recovering the deleted data and artefacts.

VIII. CONCLUSIONS AND FUTURE WORK

The research was a great success and indicated that it was indeed possible to identify usage of History Eraser version 4.8.7.5 extension installed on Google Chrome version 66.0.3359.181 running on Windows 10 operating system when used to wipe the browser data. This research has shown that History database, extension cookies and $130 can play an important role in investigation of Google chrome extensions that are used to wipe browser history as an anti-forensic method. Further, this research has shown that $130 file which is deposited when the addon is uninstalled from the browser can be valuable artefacts in the investigation of extension usage in the Google chrome browser since it can provide user IDs of the uninstalled extension. The future work of this project will include identification of the deleted data in the History and extension cookies databases as well as studying the structure of the $130 file to determine possibility of recovery of metadata involving the uninstalled extension.

REFERENCES

1. Statista (2018) *Most popular internet browser versions 2018 | Statistic*. [Online]. Available. https://www.statista.com/statistics/268299/most-popular-internet-browsers/.
2. Netmarketshare.com (2018) Browser market share. [Online]. Available. https://www.netmarketshare.com/browser-market-share.aspx?.
3. B. Christian, T. Heath, and T. Berners-Lee, "Linked data: The story so far," in *Semantic services, interoperability and web applications: emerging concepts*, pp. 205-227. IGI Global, 2011.
4. Belkasoft (2018) *Internet Forensics*. [Online]. Available. https://belkasoft.com/internet-forensics.
5. W. Christopher, E. El-Sheikh, and N.Le-Khac. "Privacy preserving internet browsers: forensic analysis of browzar," in *Computer and Network Security Essentials*, pp. 369-388. Springer, Cham, 2018.

6. B. Jacques and N. Le-Khac. "Forensic framework to identify local vs synced artefacts," *Digital Investigation* 24 (2018): S68-S75.
7. Simon (2015) *Google Chrome Browser Forensics – Analyze Chrome Data*. [Online]. Available. http://www.acquireforensics.com/blog/google-chrome-browser-forensics.html.
8. R. D. Mahendrasinh. "Web Browser Forensics: Google Chrome," *International Journal of Advanced Research in Computer Science* vol.8, no. 7, pp. 383-397, 2017.
9. B. V. Prasanth, P. Kanakam, and S. M. Hussain. "Cyber Forensic Science to Diagnose Digital Crimes-A study," *International Journal of Scientific Research in Network Security and communication (IJSRNSC)* 50, no. 2, pp. 107-113, 2017.
10. A. Izzat, R. Burdwell, A. Aleroud, A. Wahbeh, M. A. Al-Qudah, and A. Al-Omari, "Disk and Computer Forensics: Lesson Plans," In *Practical Information Security*, pp. 201-244. Springer, Cham, 2018.
11. A. Irfan, V. Roussev, and A. A. Gombe, "Robust fingerprinting for relocatable code," In *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*, pp. 219-229. ACM, 2015.
12. B. V. Prasanthi, P. Kanakam, and S. M. Hussain, "Cyber Forensic Science to Diagnose Digital Crimes-A study." *International Journal of Scientific Research in Network Security and communication (IJSRNSC)* 50, no. 2, pp. 107-113, 2017.
13. G. Corbin (2014) The Google Chrome Operating System Forensic Artifacts. [Online]. Available. https://search.proquest.com/openview/9e6a7eeb46d70e0a6fce3c85871636cf/1?pq-origsite=gscholar&cbl=18750&diss=y.
14. N. E. Sayed (2014) '*Web Browser Private Mode Forensics Analysis*' [Online]. Available. http://scholarworks.rit.edu/theses.
15. R. Tri, I. Riadi, and Y. Prayudi. "Live Forensics for Anti-Forensics Analysis on Private Portable Web Browser," *International Journal of Computer Applications*, vol 164, no. 8, pp. 31-37, 2017.
16. R. S. Rodrigo, F. P. Amatte, K. J. B. Park, and R. Winter, "Overconfidence: Personal behaviors regarding privacy that allows the leakage of information in private browsing mode," *International Journal of Cyber-Security and Digital Forensics* 4, no. 3, pp. 404-417, 2015.
17. G. Ahmad, and S. A. Seno, "Analysis of privacy of private browsing mode through memory forensics." *International Journal of Computer Applications* 132, no. 16, 2015.
18. N. Rahul, "Computer Forensics for Private Web Browsing of UC Browser," *IOSR Journal of Computer Engineering (IOSR-JCE)* vol 19, no. 4, pp. 56-60, 2017.
19. F. Cassandra, A. Mansour, and H. M. Al-Khateeb, "Web browser artefacts in private and portable modes: a forensic investigation." *International Journal of Electronic Security and Digital Forensics* 8, no. 2, pp. 99-117, 2016.
20. E. D. Adautin, and N. Meeran, "Forensic Reconstruction and Analysis of Residual Artifacts from Portable Web Browse," *International Journal of Computer Applications* 128, no. 18, 2015.
21. S. Narmeen, "Forensic Investigation of User's Web Activity on Google Chrome using various Forensic Tools." *IJCSNS*, vol 16, no. 9, pp. 123, 2016.
22. A. M. Shumail, A. Aziz, and W. Iqbal, "Forensic Analysis of Edge Browser In-Private Mode," *International Journal of Computer Science and Information Security* vol 14, no. 9, pp. 256, 2016.
23. W. David (2015), "The Internet as a conduit for criminal activity. [Online]. Available. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=740626.
24. L. Anita, "The online trade in counterfeit pharmaceuticals: new criminal opportunities, trends and challenges," *European Journal of Criminology* vol 12, no. 2, pp. 226-241, 2015.
25. C. Mohamed, A. Darwish, M. A. Khan, and S. Tyagi, "419 scam: an evaluation of cybercrime and criminal code in Nigeria," In *Cybercrime, Digital Forensics and Jurisdiction*, pp. 129-144. Springer, Cham, 2015.
26. K.. Conlan, I. Baggili and, F. Breitinger, 'Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy', Digital Investigation, 18 Elsevier, pp. S66–S75, 2016.
27. P. K. Jea, J. Park, E. Kim, C. G. Cheon, and J. I. James, "Anti-Forensic Trace Detection in Digital Forensic Triage Investigations," *Journal of Digital Forensics, Security and Law* vol 12, no. 1, pp. 8, 2017.
28. S. A. Kumar, C. S. Rawat, and A. Bhatia, "Alleviation of quantization artifact using anti-forensic in image processing," In *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, pp. 2697-2701. IEEE, 2017.
29. S. Po-Chyi, P. Suei, M. Chang, and J. Lain, "Forensic and anti-forensic techniques for video shot editing in H. 264/AVC," *Journal of Visual Communication and Image Representation* vol 29, pp. 103-113, 2015.
30. V. Giuseppe, S. Tubaro, and M. Tagliasacchi, "Anti- Forensics of Multimedia Data and Countermeasures," *Handbook of Digital Forensics of Multimedia Data and Devices, pp.* 612-651. 2015.

31. M. Oza (2013) Anti forensic. [Online]. Available. https://www.slideshare.net/MilapOza/anti-forensic?next_slideshow=1.
32. P. Ameer, M. Lazarescu, and S. T. Soh, "Cloud forensics: Technical challenges, solutions and comparative analysis," *Digital Investigation* 13, pp. 38-57, 2015.
33. stackoverflow.com (2014) sqlite - What is the format of Chrome's timestamps? - Stack Overflow. [Online]. Available. https://stackoverflow.com/questions/20458406/what-is-the-format-of-chromes-timestamps.

