iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** V **Month of publication:** May 2019

DOI: https://doi.org/10.22214/ijraset.2019.5332

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Framework for Analysis and Forecasting on Browser Forensics

[1]Krishna Punwar, [2]Dr.Ravi K Sheth, [3]Dr.Sunil B Mane
[1, 2]Department of Information and Technology Raksha Shakti University, Ahmedabad, India
[3]Department of computer science College of Engineering Pune, India

Abstract: ***Nowadays, Browser and Internet users day by day using emerging quickly and the web browser through providing various web activities like browsing internet, emails, social media applications, internet banking, cloud storage, downloads etc. A number of crimes happen on computer resources can examine user activities by analysing the evidence of web browsers. It is most important for the forensic analyst to gather and examine output associate with web browser usage of the evidence. Current days, we have different types of web browser available like Google Chrome, Safari, Opera, Internet Explorer, Firefox Mozilla, Tor Browser, Lynx etc.***

In this project, we analyzed how to collect history, cookies, location, log files, login data, user profile, user activities, download files and dump files then we retrieve data from web browser.

The main focus on recovering deleted data and depth analysis of browser activities using tools and some techniques. Also, we compare used tools result based on analysis and identify the dark side of the tools then how to overcome the situation. In tools there are many limitations of recover data and it may be reduced limitations of tools by designing a framework which shall help in removing some constraints and easily access some browser forensics tools on single platform.

Keywords: Web Browser, Forensics Tools, Web activities

I. INTRODUCTION

Web browsers are the most crucial tools on many of the crimes happened on digital resources. Examining the evidence which is the subject of criminal records is an important step examination of your browser.

Browser files enclosed crucial evidence related to Suspect's Internet activities and therfore its investigation is essential in both offline and live forensic analysis. Web browsers create a number of files in the local system when a user browses Internet. These files may hold History, Cookies, Cache, Bookmarks and other forensically relevant information. Whenever a user makes request in the web browser, the details of that access will be added in the browser files.

Browser Forensics is the main part of Internet Forensics which deals with extraction and investigation of browsers files generated by web browsers.

Web Browsers keep information related to Visited Sites, Downloads, Search History, Cookies and Cache Information in a predefined location in the Suspect's machine. Browser Forensics does a crucial role in providing forensically relevant information in a cybercrime investigation.

This is because, web browsers creates a number of files in the local system at the time of Internet Browsing. These files may hold History, Cookies, Cache, Bookmarks and other forensically relevant information. Whenever a user makes request in the web browser, the details of that access will be added in the browser files. Browser Files once created can be accessed and analyzed for retrieving forensic evidence from it. So, evidences of Cyber Crimes based on Internet usage including social media can be identified through browser forensics.

A portable browser that can be saved on a removable digital media like USB drive. The browser can then be launched from the flash drive which is not necessary for the fitting on the host system. on the basis of disgital forensics, browsing evidence could be stored on the handy browser flash drive, server and the host machine. The local user machine saves browsing information in the both immovable media such as hard disk as well as in RAM, which is also called volatile memory. When we are dealing with portable browsing artefacts, memory forensics is very challenging only because if we remove the handy browser flash media from the targeted system, the handy browser based on data contained in the main memory will slowly be deleted. The focus of this research is the examination of various sources such as main memory, temporary files, recent files, event files, Windows Registry, and Cache.dll file in the suspect machine looking for residual artefacts left behind after private hany web browsing action .

II. LITERATURE REVIEW

Andrew Marrington, Ibrahim Baggili, Talal Al Ismail and Ali Al Kaf have conducted research on a forensic examination of the privacy benefits of portable web browsers. Their main focus on Portable web browsers are installed on removable storage devices which can be taken by a user from computer to computer. In their work, one of the stated benefits of portable web browsers is increased privacy of browser, through minimization of the traces of browsing activity leave on the host's hard disk. On the basis of this state, it would have the appear portable web browsers pose a challenge to digital forensic examiners trying to reconstruct past web browsing activity in the context of a digital investigation. The research examines one popular portable web browser, Google Chrome in both normal and private browsing mode, and compares the forensic traces of its use to forensic traces of the installed version of the same browser. The results show that Google Chrome Portable leaves traces of web browsing activity on the host computer's hard disk, and demonstrate a need for forensic testing of the privacy claims made for the use of portable web browsers.
Anuradha P., Raj Kumar T. and Sobhana N.V. have conducted research on Recovering Deleted Browsing Artifacts from Web Browser Log Files in Linux Environment. Their main focus on recovering such deleted browsing artifacts from the installed browser by an in depth analysis of the image of the hard disk used by the suspects involved in the crime.

III. ANALYSIS OF BROWSER

Browsers are one of the most commonly used applications in digital devices. Users perform their internet activities with web browsers in different operating systems. Web browsers are used for many purposes like, searching information, e-mail, e-commerce, and news, e-banking and social media. For this reason, it is one of the most important parts of evidence analysis. Information like which URLs was visited by the user, which words was searched, when these actions were made, are used by digital forensics experts to determine the crime. Also, usage of various web browsers in the same duration must be analyzed. A browser creates a number of files in the local system at the time of Internet Browsing. These files may hold History, Cookies, Cache, Bookmarks and other forensically relevant information and it is very important for investigation process. These tables are downloads, history, presentation, URL, keyword search, segment usage,
Visits, Meta, segment which is very important for forensics. Below tables through we can find evidence in suspect's machine.

Browser	OS	Path
Google Chrome	Windows 10	C:\Program Files (x86)\Google\Chrome\Application
Mozilla Firefox	Windows 10	C:\Users\username\AppData\Roaming\Mozilla\Firefox\Profiles\%PROF ILE%.default\places.sqlite
Internet Explore	Windows 10	C:\Program Files\internet explorer C:\Users\a\AppData\Local\Microsoft\Windows
TOR Browser	Windows 10	C:\Data\Browser\Caches\

Table 1: File location in the browser OS

Browser Artifacts	Information
History	URL, Timestamp, visited ID, Transition Type, Transition Qualifiers
Cookies	Domain, Host, Name, Access ID, Path, Timestamp
Cache	URL, Timestamp, Hits, Folder Name, File Size, Path, Filename
Downloads	Timestamp, MIME Type, Path, Referrer, URL, Response Header
Keyword Search	URL, Searched Sentence
Bookmarks	Name, Type, URL, Timestamp
Login Data	User name, Login ID, URL, Sign, Passwords, Sign
Network	URL, Sites, Number of Hits, User Text

Table 2: Important artifacts in browser for investigation

A. Technology and Setup

In preparation for the browser forensic analysis, the following tools were used.

1) Hardware

a) Desktop PC (4GB RAM)
b) USB External Drive (16 GB) for portable browser forensics

2) Software (free versions)

a) Windows 10
b) FTK Imager
c) Autopsy
d) Wireshark
e) RAM dump
f) Nirsoft Tools
g) Google chrome
h) Mozilla Firefox
i) Internet Explorer

In this paper we are using different web browser and different modes like regular mode, portable and privacy mode. Then analyze browser's malicious activities and recovering deleted information, to using some tools and techniques.

IV. ANALYSIS OF THE RESULTS

In this paper, the information that was retrieved from memory is enough to conclude browsing activities and establishing link between the web browsing activities and the suspect. For example, browsing history, search history, cache files, cookies and file download were retrieved from memory for all of the browsers we studied and analyzed. These are important evidential information for digital forensics investigators.

For normal browser, which is already installed in computer, the forensics artifacts retrieved from cookies, cache, downloads and history. Analysis of the memory dumped file showed browser related entries in memory indicating various browser activities. And we are able to detect browsing and URL history, search history, and downloaded files, some information such as cookies, email password, timelines, and process ID. These all are information retrieved from various Nirsoft browser forensics tools.

```
==========================================
URL             : http://192.168.0.1/index.htm
Title           : WiFi Router
Visited On      : 03/05/2016 8:31:30 PM
Visit Count     : 30
Typed Count     : 1
Referrer        : http://192.168.0.1/login.cgi
Visit ID        : 2156
Profile         : ChromeDefaultData
URL Length      : 28
Transition Type : Link
Transition Qualifiers: Chain End,Client Redirect
==========================================
```

Fig 1: Details of retrieved browsing history

Filename	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hits	File Size	Subfolder Name	Full Path
0000018f_index[...	application/octet-...	http://dlupdate.quickheal.com/1100/updates/00...	22/01/2019 11:16:5...	21/01/2019 7:29:46...	22/01/2019 10:16:5...	N/A	1	0	W7B66CL2	C:\Users\Adn
0000029c_index[...	application/octet-...	http://dlupdate.quickheal.com/1700/updates/00...	24/01/2019 11:17:5...	23/01/2019 6:16:29...	24/01/2019 10:17:5...	N/A	3	0	W7B66CL2	C:\Users\Adn
000002a2_index[...	application/octet-...	http://dlupdate.quickheal.com/1700/updates/00...	22/01/2019 11:16:5...	21/01/2019 7:30:43...	22/01/2019 10:16:5...	N/A	1	0	D08YJXS2	C:\Users\Adn
0000030a_index[...	application/octet-...	http://dlupdate.quickheal.com/oc0100/updates/...	28/01/2019 11:22:2...	27/01/2019 5:24:38...	28/01/2019 11:25:5...	N/A	6	0	M5FRS89C	C:\Users\Adn
0000030c_index[...	application/octet-...	http://dlupdate.quickheal.com/oc0100/updates/...	28/01/2019 11:22:2...	27/01/2019 5:24:38...	28/01/2019 10:22:2...	N/A	2	0	M5FRS89C	C:\Users\Adn
0000030e_index[...	application/octet-...	http://dlupdate.quickheal.com/oc0100/updates/...	28/01/2019 11:22:2...	27/01/2019 5:24:39...	28/01/2019 11:27:2...	N/A	1	0	0U930P87	C:\Users\Adn
000004cd_index[...	application/octet-...	http://dlupdate.quickheal.com/oc0100/updates/...	28/01/2019 11:22:2...	27/01/2019 5:25:04...	28/01/2019 11:29:2...	N/A	6	0	0U930P87	C:\Users\Adn
00366[1].jpg	image/jpeg	https://images.springer.com/sgw/journals/medi...	28/01/2019 11:27:1...	15/03/2017 1:44:13...	29/01/2019 1:43:40...	N/A	1	61,306	QZN93R3T	C:\Users\Adn
04998b8b0c824e...	text/html; charset...	https://d6tizftlrpuof.cloudfront.net/live/i/55916f...	28/01/2019 11:29:5...	21/01/2019 4:49:27...	17/10/2021 4:52:03...	N/A	1	2,038	QZN93R3T	C:\Users\Adn
0661[1].js	application/x-java...	https://dnn506yrbagrg.cloudfront.net/pages/scri...	28/01/2019 11:27:1...	25/01/2019 7:14:37...	28/01/2019 11:28:1...	N/A	1	95,364	FB8ZNR24	C:\Users\Adn
0b297e2e[1].js	application/x-java...	https://www.bing.com/rb/3v/cj,nj/fffaae5f/0b29...	23/01/2019 2:05:35...	20/01/2019 9:35:44...	22/07/2019 2:05:34...	N/A	1	259,701	QZN93R3T	C:\Users\Adn
0eabae8d[1].js	application/x-java...	https://www.bing.com/rs/3R/aB/cj,nj/31615488/...	23/01/2019 2:05:33...	17/01/2019 4:19:57...	21/07/2019 3:42:53...	N/A	4	757	QYQU3QPJ	C:\Users\Adn
0eabae8d[1].js	application/x-java...	https://www.bing.com/rs/3R/aF/cj,nj/31615488/...	28/01/2019 11:29:0...	26/01/2019 8:22:52...	27/07/2019 11:29:0...	N/A	2	757	QZN93R3T	C:\Users\Adn
1-s2.0-S1742287...	image/jpeg	https://ars.els-cdn.com/content/image/1-s2.0-S...	22/01/2019 3:28:09...	07/09/2011 6:54:14...	N/A	N/A	1	27,180	QZN93R3T	C:\Users\Adn
1-s2.0-S1742287...	image/jpeg	https://ars.els-cdn.com/content/image/1-s2.0-S...	22/01/2019 3:28:06...	07/09/2011 6:54:14...	N/A	N/A	1	37,241	QZN93R3T	C:\Users\Adn
1-s2.0-S1742287...	image/jpeg	https://ars.els-cdn.com/content/image/1-s2.0-S...	22/01/2019 3:28:06...	07/09/2011 6:54:14...	N/A	N/A	1	32,600	QZN93R3T	C:\Users\Adn
1-s2.0-S1742287...	image/gif	https://ars.els-cdn.com/content/image/1-s2.0-S...	22/01/2019 3:28:03...	07/09/2011 6:54:14...	N/A	N/A	1	7,344	FB8ZNR24	C:\Users\Adn
1-s2.0-S1742287...	image/jpeg	https://ars.els-cdn.com/content/image/1-s2.0-S...	22/01/2019 3:28:04...	07/09/2011 6:54:14...	N/A	N/A	1	16,925	FB8ZNR24	C:\Users\Adn
1-s2.0-S1742287...	image/gif	https://ars.els-cdn.com/content/image/1-s2.0-S...	22/01/2019 3:28:03...	07/09/2011 6:54:14...	N/A	N/A	1	986	FB8ZNR24	C:\Users\Adn
1-s2.0-S1742287...	image/jpeg	https://ars.els-cdn.com/content/image/1-s2.0-S...	22/01/2019 3:28:04...	07/09/2011 6:54:14...	N/A	N/A	1	8,329	FB8ZNR24	C:\Users\Adn
1-s2.0-S1742287...	image/gif	https://ars.els-cdn.com/content/image/1-s2.0-S...	22/01/2019 3:28:04...	07/09/2011 6:54:14...	N/A	N/A	1	8,206	QZN93R3T	C:\Users\Adn
1-s2.0-S1742287...	image/jpeg	https://ars.els-cdn.com/content/image/1-s2.0-S...	22/01/2019 3:28:04...	07/09/2011 6:54:14...	N/A	N/A	1	20,085	9MNGY083	C:\Users\Adn
1-s2.0-S1742287...	image/gif	https://ars.els-cdn.com/content/image/1-s2.0-S...	22/01/2019 3:28:04...	07/09/2011 6:54:14...	N/A	N/A	1	4,728	9MNGY083	C:\Users\Adn
1-s2.0-S1742287...	image/jpeg	https://ars.els-cdn.com/content/image/1-s2.0-S...	22/01/2019 3:28:04...	07/09/2011 6:54:14...	N/A	N/A	1	31,870	QYQU3QPJ	C:\Users\Adn
1-s2.0-S1742287...	image/gif	https://ars.els-cdn.com/content/image/1-s2.0-S...	22/01/2019 3:28:03...	07/09/2011 6:54:14...	N/A	N/A	1	7,470	9MNGY083	C:\Users\Adn
1-s2.0-S1742287...	image/jpeg	https://ars.els-cdn.com/content/image/1-s2.0-S...	22/01/2019 3:28:05...	07/09/2011 6:54:14...	N/A	N/A	1	30,213	FB8ZNR24	C:\Users\Adn
1-s2.0-S1742287...	image/gif	https://ars.els-cdn.com/content/image/1-s2.0-S...	22/01/2019 3:28:03...	07/09/2011 6:54:14...	N/A	N/A	1	9,387	QYQU3QPJ	C:\Users\Adn
1-s2.0-S1742287...	image/jpeg	https://ars.els-cdn.com/content/image/1-s2.0-S...	22/01/2019 3:28:06...	07/09/2011 6:54:14...	N/A	N/A	1	84,212	QYQU3QPJ	C:\Users\Adn
1-s2.0-S1742287...	image/jpeg	https://ars.els-cdn.com/content/image/1-s2.0-S...	22/01/2019 3:28:05...	07/09/2011 6:54:14...	N/A	N/A	1	42,893	QYQU3QPJ	C:\Users\Adn
1-s2.0-S1742287...	image/jpeg	https://ars.els-cdn.com/content/image/1-s2.0-S...	22/01/2019 3:28:04...	07/09/2011 6:54:14...	N/A	N/A	1	32,100	QYQU3QPJ	C:\Users\Adn
1-s2.0-S1742287...	image/jpeg	https://ars.els-cdn.com/content/image/1-s2.0-S...	22/01/2019 3:28:06...	07/09/2011 6:54:14...	N/A	N/A	1	42,159	QZN93R3T	C:\Users\Adn

Fig 2: Retrieved information of cache data

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

For portable browser analysis, we take one USB drive and installed portable browser version. Try some activities on various browsers then removed all activities for analysis purpose. Then we followed the below steps:

1) Attached the portable browser USB drive to the machine and configured the browsers as the default browser with extensions and plug-ins disabled.
2) Then we performed a browsing session, attached the external drive to the suspect machine and captured RAM, saved the file onto the external drive and removed external drive for RAM analysis.
3) Then reduced the amount and time of data analysis.
4) Next, analysis of the memory dumped file showed browser-related entries in memory indicating web browser activity. We got some information like search history, metadata, web cookies, thumbnails, raw files, images and videos.

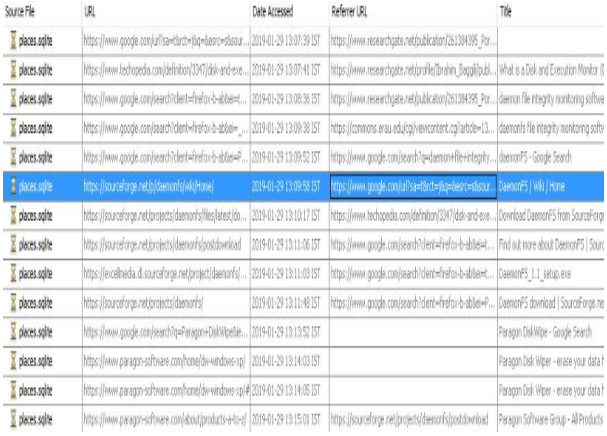


Fig 3: Recovered data from cookies

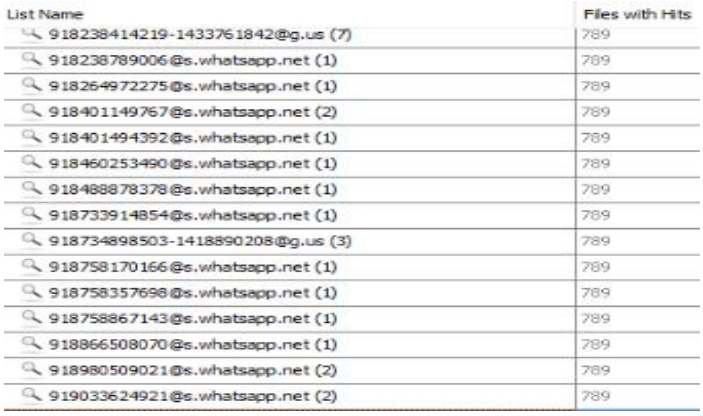


Fig 4: Getting contact number through RAM analysis

For private browsing, we are using TOR browser, show some artifacts for investigation using different methods. There are some methods like RAM dump, packet capturing, registry files and network analysis. When we are using RAM dump, it provided several different file types of carved data that linked back to the browsing protocol used.

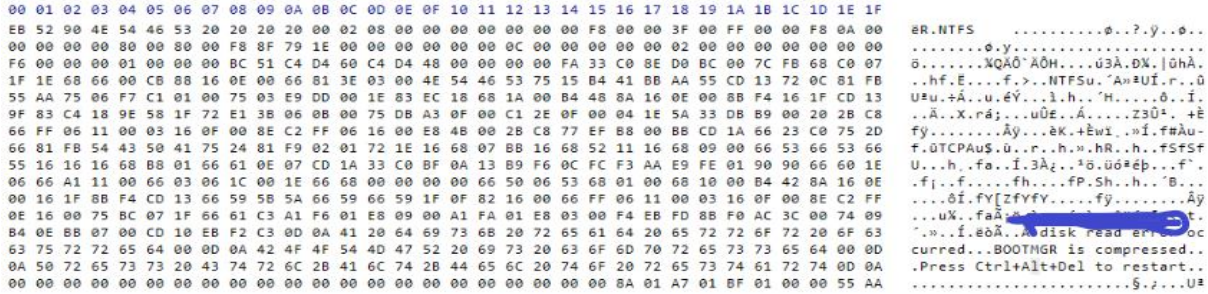


Fig 5: Data dump information of network

The Registry files indicated that Tor was downloaded and executed on the machine and RegShot, open-source software that allows for the comparison of the state of the Registry at different moments in time, provided the types of changes made to the registry during installation and uninstallation of Tor.
HKEY_CURRENT_USER\Software\TOR\TypedURL. Network forensics will be carried out by wireshark and extracted evidences provide information related to web traffic.

V. FRAMEWORK

Retrievable browser forensics artifacts after different browsing session via memory forensics for browsers are summarized in below table:

Browsing Mode	Forensics Analysis Techniques & Tools	Limitations
Normal Browsing (Google Chrome, Internet Explorer, Mozilla Firefox)	ChromeCookie View ChromeCache View My Last Search MozillaCookies View IECookies View IECache View	We are able to analyze multiple web browsers, lacks the accurate artifacts extraction. The process is time consuming because there is no single tool for analysis of browser data recovery so we are using different tools for extraction. And some tools are not supported in windows 10.
Portable Browsing (Google Chrome, Internet Explorer, Mozilla Firefox)	Registry Editor FTK Imager Autopsy	Won't be any traces of Internet activities in the local machine once the browsing is completed. These data will be available only if these portable devices are identified and seized from the scene of crime.
Private Browsing(TOR)	Wireshark Registry Editor RAM dump	In private browsing, information only temporarily. Once the user leave browsing session, the browser will erase most of the records from history, cookies, cached files etc.

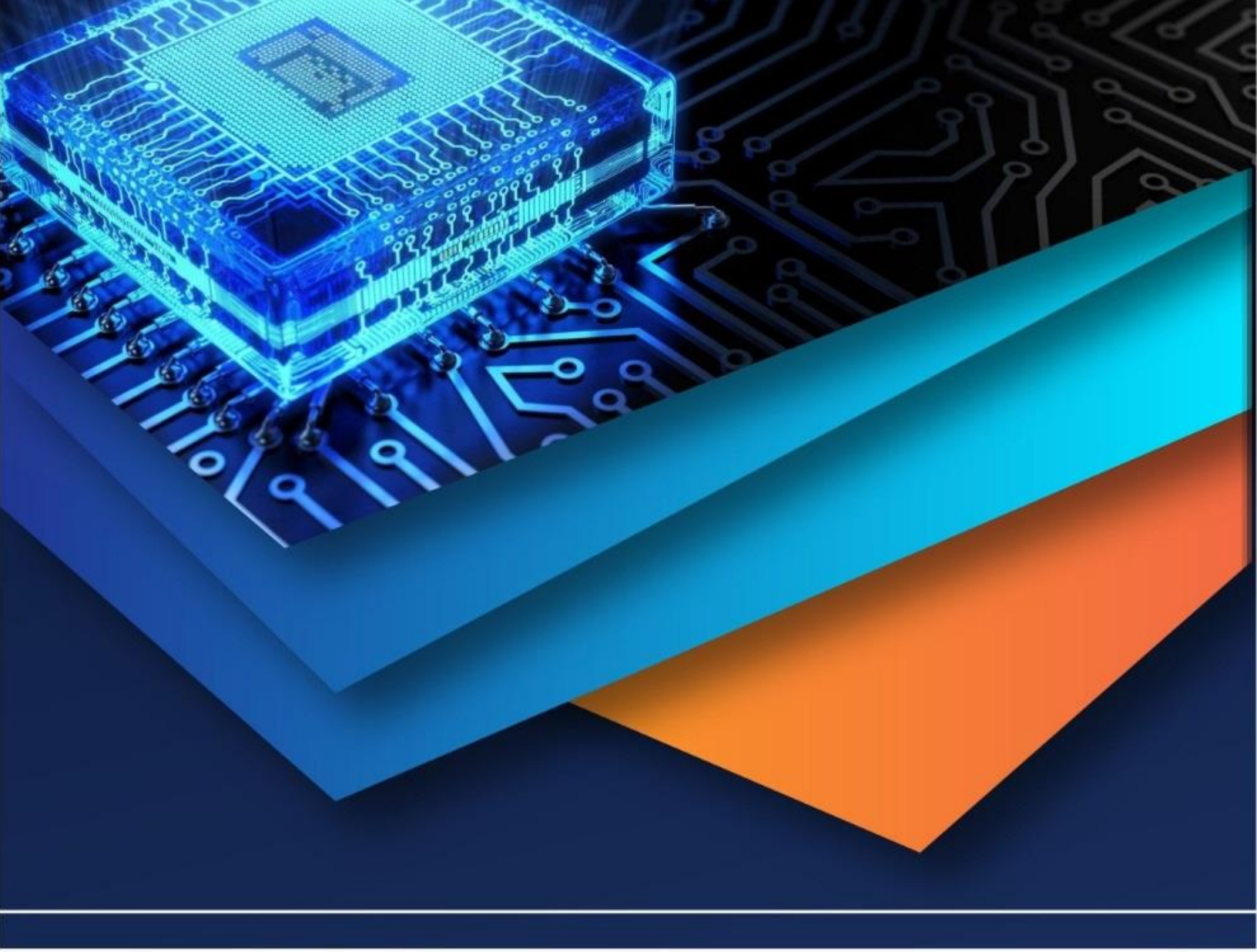
Above table information are shows analysis of browser data extraction, analysis and forecasting said browsers. Secondly we are developing one framework for browser forensic analysis process, in this framework we are combine different browser forensics tools through this process investigator easily access tools at single platform. Because of these challenges, there are currently no single tool or framework for recovering all data at once tool, or implement the time consuming of data collection from a running system. In this framework, for front end programming languages are html, css and JavaScript and back end programming language is python supported. This framework ensures that browser forensics makes easier for investigator; there should be one appropriate Framework through some limitations can be minimized. If the application or tools requires a investigator to find artifacts in each time to use different tools, so this framework through investigate and deals with different artifacts to find suspect. To carry out the work in firstly, multiple tools available in this, at that time which one you have to use for forensic process along with the useful information. A framework that allows incident responders to extract and analyze at system.

VI. CONCLUSION AND FUTURE WORK

A number of crimes happen on computer resources can examine user activities by examining the records of web browsers. It is most important for the forensic analyst to gather and examine output associate with web browser usage of the evidence. There are difference web browsers available like Google Chrome, Safari, Opera, Internet Explorer, Firefox Mozilla, Tor Browser etc. In this, discuss different browser and its results. We used analyzed log files, history, location, user activities, dump files, passwords and registry through browser analysis. Also used forensics tools and techniques which can be useful for acquisition and collect deleted information. As we cannot extract each and every data from the forensics tools obtainable in the market, this paper will explain and discuss about a framework which will be fruitful to solve the above said problem. In browser forensics, most important thing is TOR browser which works anonymously and we are not able find actual IP address of suspect's machine so this one main challenge for us and our future research goal on Dark web forensics for preventing malicious activities on internet.

REFERENCES

[1] Erhan Akbal1*, Fatma Güneş1, Ayhan Akbal2 1 Department of Digital Forensics Engineering, Fırat University Technology Faculty, 23119, Elazig, Turkey, Digital Forensic Analyses of Web Browser Records(2016)
[2] Dr. Digvijaysinh Rathod Institute of Forensic Science Gujarat Forensic Sciences University Gandhinagar, Gujarat , Web Browser Forensics: Google Chrome(2017)
[3] asaf varol, faculty of technology, Turkiye, Forensic Analysis and Evidence Collection for Web Browser Activity(2017) III
[4] https://www.nirsoft.net
[5] https://www.digitalforensics.com/blog/an-overview-of-web-browser-forensics/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY