Forensic Analysis and Evidence Collection for Web Browser Activity

Apurva Nalawade
Dept. of Computer Engineering
Ramrao Adik Inst. of Technology
Nerul, Navi Mumbai, India
*Email:
nalawadeapurva20@gmail.com

Smita Bharne
Dept. of Computer Engineering
Ramrao Adik Inst. of Technology
Nerul, Navi Mumbai, India
Email: smita.bharne@rait.ac.in

Vanita Mane
Dept. of Computer Engineering
Ramrao Adik Inst. of Technology
Nerul, Navi Mumbai, India
Email: vanita.mane@rait.ac.in

Abstract— **Digital Forensics is a branch of forensic science. Today the internet users continue to grow day by day, therefore crimes related to the internet also increases. The process of digital forensic is using digital devices to extract the information and identify whether the device has been hacked before or being viewed. The prime objective of Digital Forensic is to gather the "evidence" of crime scene. Digital forensic is a continuation of computer forensic, it includes digital electronic technology likes mobile phone, printers. Web browser forensics is a major part within computer forensics, because an greater number of criminal and civil cases may be based on evidence collected from user internet activities. Both criminals as well as investigators use internet. Web browser is used by criminals to collect or inquire information for a new crime technique, to conceal his/her crime. Every moment criminal leaves the traces on computer while using web browser. This proof is found in the browser history, temporary files, index.dat, cookies, download files, unallocated space and the cache etc. In this paper, we studied major tools used for web browser analysis. Also, we compare them and find out its benefits and limitations.**

Keywords— Digital forensic, Web browser forensic, private browsing

I. INTRODUCTION

Digital forensic is a branch of forensic science concerned with the use of digital information (produced, stored and transmitted by computers) as source of evidence in investigations and legal proceedings. An alternative definition for digital forensics science is "The practice of scientifically obtained and established techniques toward the uploading, accumulation, validation, recognition, examination, understanding, documentation and presentation of digital proof derived from digital sources for the purpose of help or furthering the rebuilding of events found to be criminal, or helping to predict unauthorized actions shown to be disturbing to planned operations"[1].

Digital Forensic Life Cycle steps [2]:
1. Preparing for the Evidence and Identifying the Evidence
2. Gathering and Registering Digital Evidence
3. Storing and delivering Digital Proof
4. Inspecting/ studying Digital Evidence
5. Analysis, Interpretation and Attribution
6. Reporting
7. Testifying

II. LITERATURE REVIEW

Web browser may be used by the suspect to retrieve information or to conceal his/her criminal activities and to explore new crime techniques. Searching for evidence left by web browsing activity is typically a crucial component of digital forensic investigations. When suspect uses web browser all his activities leaves mark on the computer. This proof can provide useful information to the investigator while examining the suspect's information. It is feasible to study this proof for web sites visited, time and frequency of access, and search engine keywords used by the suspect after recovering data such as cache, history, cookies, and download list from a suspect's computer.

Author Junghoon Oh, Seungbong Lee and Sangjin Lee [3] suggest a new evidence collection and analysis methodology and tool (WEFA) to aid this process.

There are many research studies and tools present for Web Browser Forensic and most of them share typical features.
1. These studies and methods are aimed to a peculiar web browser or a peculiar log file from a fixed web browser.
2. Present study and approach remain at the level of plain parsing.
For above mentioned purpose, a new evidence collection and analysis tool is needed. [3]

A. Advanced evidence analysis

- *Integrated analysis*- For integrated analysis, the critical information, more than all other information, is time information. Every web browser's log file contains time information, and therefore it is possible to construct a timeline array using this time information
- *Timeline analysis*- By performing a timeline analysis, the investigator can trace the criminal activities of the suspect in their entirety.
- *Analysis of search history*- A single word or a sentence, Search words might give keywords for suspect's crime.
- *Analysis of URL encoding*- Decoding encoded characters is relevant for investigators in non-English speaking nations.
- *Analysis of user activity*- The investigator must access each appropriate web site to guess user activity.
- *Recovery of deleted information*-Web browsers can recover the deleted information from temporary internet files, session log files, cookies, cache files.

978-1-5090-2080-5/16/$31.00 ©2016 IEEE

B. *Private browsing*

Private browsing is a privacy feature in all major browsers to disable browsing history, and the web cache. This allows person to browse the web without storing local data that could be retrieved at a later date.

G. Aggarwal, E. Bursztein, C. Jackson, and D. Boneh [5] gives the main goals of private browsing modes. [6] Private browsing modes have two primary goals [5]: privacy against the web and privacy against local machines, but all major web browsers are failed in providing private browsing mode. This is mainly because browser plug-ins and extensions develop difficulties to private browsing sessions. User activities can be recorded because many browser extensions disempowered private browsing modes. For example, Google Chrome weaken all extensions during private browsing and Firefox does not.

C. Major browsers and privacy capabilities

- *Microsoft Internet Explorer*

Microsoft IE offers users a private browsing feature called InPrivate browsing[6]. According to Microsoft, InPrivate browsing facilitates users to surf the internet without leaving a hint on their computer. In InPrivate browsing, information such as cookies and temporary files are momentarily stored so that webpage performs properly. All this data is removed once the browsing session is finished. In regards to browser extensions, IE disables all toolbars and extensions during InPrivate browsing sessions to make certain more good privacy. IE also does not clear anything regarding toolbars and extensions after a private session is closed.

- *Google Chrome*

There is a provision of Incognito mode to browse the internet in a private session [6]. According to Google, Incognito mode does not log any browsing or download histories and any generated cookies will be removed after leaving an ongoing session completely.

- *Mozilla Firefox*

Mozilla Firefox offers a secret browsing mode called Private Browsing [6]. According to Mozilla, private browsing allows users to surf the internet without saving any information about visited sites or pages. Mozilla does make it clear as some of the other web browsers do that private browsing modes do not make users incognito from web sites, ISP's, and networks. Besides from other privacy features, there is an option to activate the Do-Not-Track feature in Firefox, which ask that websites do not track user browsing behaviour. This request is accepted intentionally.

- *Apple Safari*

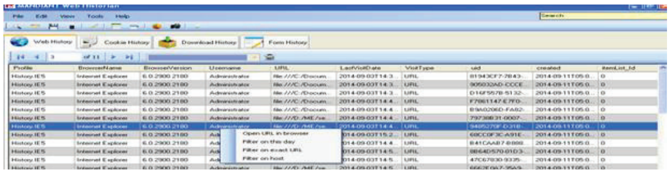
According to Apple, when using private browsing mode in Safari, webpages are not added to the history list, cookie changes are removed, searches are not stored to the search fields, and websites cannot change data stored on the computer.[6]

III.WEB BROWSER FORENSIC TOOL

A. *WebHistorian 1.3*

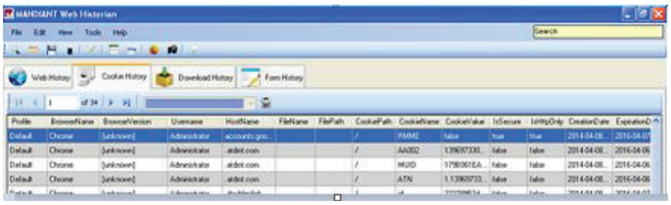
Web Historian 1.3 [3,10] is a tool that allows an investigator to collect, display and analyze web history data. It bolsters windows o.s and most of the browsers.

Fig 1, 2, 3 shows web history,cookie history, website analyzer respectively.



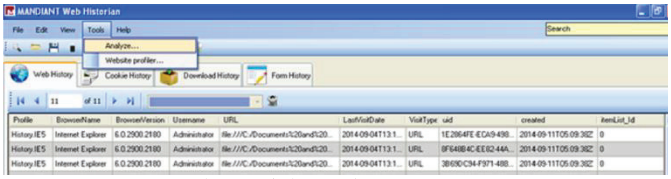
Profile	BrowserName	BrowserVersion	Username	URL	LastVisitDate	VisitType	uid	created	itemList_Id
History.IE5	Internet Explorer	6.0.2900.2180	Administrator	file:///C:/Docum...	2014-09-03T14:3...	URL	81943CF7-7843-...	2014-09-11T05:0...	0
History.IE5	Internet Explorer	6.0.2900.2180	Administrator	file:///C:/Docum...	2014-09-03T14:3...	URL	905032AD-CCCE...	2014-09-11T05:0...	0
History.IE5	Internet Explorer	6.0.2900.2180	Administrator	file:///C:/Docum...	2014-09-03T14:3...	URL	D16F5578-5132-...	2014-09-11T05:0...	0
History.IE5	Internet Explorer	6.0.2900.2180	Administrator	file:///C:/Docum...	2014-09-03T14:4...	URL	F7061147-E7F0-...	2014-09-11T05:0...	0
History.IE5	Internet Explorer	6.0.2900.2180	Administrator	file:///C:/Docum...	2014-09-03T14:4...	URL	B9A0206D-FA02-...	2014-09-11T05:0...	0
History.IE5	Internet Explorer	6.0.2900.2180	Administrator	file:///D:/ME/se...	2014-09-03T14:4...	URL	79738831-0007-...	2014-09-11T05:0...	0
History.IE5	Internet Explorer	6.0.2900.2180	Administrator	file:///D:/ME/se...	2014-09-03T14:4...	URL	9485270F-D318-...	2014-09-11T05:0...	0
History.IE5	Internet Explorer	6.0.2900.2180	Ad		014-09-03T15:2...	URL	60CC0F3C-A91E-...	2014-09-11T05:0...	0
History.IE5	Internet Explorer	6.0.2900.2180	Ad		014-09-03T14:4...	URL	B41CAAB7-B998...	2014-09-11T05:0...	0
History.IE5	Internet Explorer	6.0.2900.2180	Ad		014-09-03T14:5...	URL	8B64D570-01D3-...	2014-09-11T05:0...	0
History.IE5	Internet Explorer	6.0.2900.2180	Ad		014-09-03T14:5...	URL	47C67030-9335-...	2014-09-11T05:0...	0
History.IE5	Internet Explorer	6.0.2900.2180	Administrator	file:///D:/ME/se...	2014-09-03T14:5...	URL	6662E0A7-35A9...	2014-09-11T05:0...	0

Fig.1 Web History



Profile	BrowserName	BrowserVersion	Username	HostName	FileName	FilePath	CookiePath	CookieName	CookieValue	IsSecure	IsHttpOnly	CreationDate	ExpirationD
Default	Chrome	[unknown]	Administrator	accounts.goo...			/	RMME	false	true	true	2014-04-08...	2016-04-07
Default	Chrome	[unknown]	Administrator	.atdmt.com			/	AA002	1396973330...	false	false	2014-04-08...	2016-04-06
Default	Chrome	[unknown]	Administrator	.atdmt.com			/	MUID	1798067EA...	false	false	2014-04-08...	2016-04-06
Default	Chrome	[unknown]	Administrator	.atdmt.com			/	ATN	1.13969733...	false	false	2014-04-08...	2016-04-06

Fig.2 Cookie History



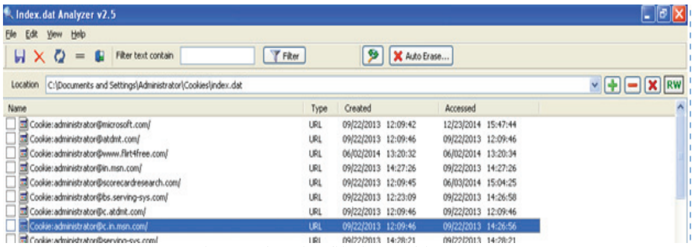
Profile	BrowserName	BrowserVersion	Username	URL	LastVisitDate	VisitType	uid	created	itemList_Id
History.IE5	Internet Explorer	6.0.2900.2180	Administrator	file:///C:/Documents%20and%20...	2014-09-04T13:1...	URL	1E2864FE-ECA9-498...	2014-09-11T05:09:38Z	0
History.IE5	Internet Explorer	6.0.2900.2180	Administrator	file:///C:/Documents%20and%20...	2014-09-04T13:1...	URL	8F648B4C-EE82-44A...	2014-09-11T05:09:38Z	0
History.IE5	Internet Explorer	6.0.2900.2180	Administrator	file:///C:/Documents%20and%20...	2014-09-04T13:1...	URL	3B69DC94-F971-488...	2014-09-11T05:09:38Z	0

Fig 3.Website Analyzer

B. *Index.dat Analyzer 2.5*

Internet Explorer saves numerous files named "index.dat" within each user's home directory on the computer system. It gives all tracks of online activity, what sites visited, list of URLs, recently accessed files and documents. Index.dat Analyzer works on windows o.s and retrieve index.dat file from IE [3, 11]. Index.dat Analyzer automatically scan the computer for all Index.dat items, and investigator can select which ones he wants to explore. Index.dat Analyzer works on windows O.S and retrieve index.dat file from IE.

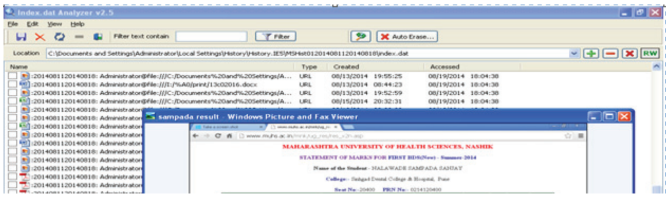
Fig 4, 5, 6 shows index.dat file in cookie, history and temporary internet files respectively.



Location: C:\Documents and Settings\Administrator\Cookies\index.dat

Name	Type	Created	Accessed
Cookie:administrator@microsoft.com/	URL	09/22/2013 12:09:42	12/23/2014 15:47:44
Cookie:administrator@atdmt.com/	URL	09/22/2013 12:09:46	09/22/2013 12:09:46
Cookie:administrator@www.flirt4free.com/	URL	06/02/2014 13:20:32	06/02/2014 13:20:34
Cookie:administrator@in.msn.com/	URL	09/22/2013 14:27:26	09/22/2013 14:27:26
Cookie:administrator@scorecardresearch.com/	URL	09/22/2013 12:09:45	06/03/2014 15:04:25
Cookie:administrator@bs.serving-sys.com/	URL	09/22/2013 12:23:09	09/22/2013 14:26:58
Cookie:administrator@c.atdmt.com/	URL	09/22/2013 12:09:46	09/22/2013 12:09:46
Cookie:administrator@c.in.msn.com/	URL	09/22/2013 12:09:46	09/22/2013 14:26:56
Cookie:administrator@serving-sys.com/	URL	09/22/2013 14:28:21	09/22/2013 14:28:21

Fig 4.Index.dat file in cookie



Location: C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\MSHist012014081120140818\index.dat

Name	Type	Created	Accessed
:2014081120140818: Administrator@file:///C:/Documents%20and%20Settings/A...	URL	08/13/2014 19:55:25	08/19/2014 18:04:38
:2014081120140818: Administrator@file:///I:/%A0/print/13c02016.docx	URL	08/13/2014 08:44:23	08/19/2014 18:04:38
:2014081120140818: Administrator@file:///C:/Documents%20and%20Settings/A...	URL	08/13/2014 19:52:59	08/19/2014 18:04:38
:2014081120140818: Administrator@file:///C:/Documents%20and%20Settings/A...	URL	08/15/2014 20:32:31	08/19/2014 18:04:38
:2014081120140818: Administrator			
:2014081120140818: Administrator			
:2014081120140818: Administrator			
:2014081120140818: Administrator			
:2014081120140818: Administrator			
:2014081120140818: Administrator			
:2014081120140818: Administrator			
:2014081120140818: Administrator			
:2014081120140818: Administrator			
:2014081120140818: Administrator			

MAHARASHTRA UNIVERSITY OF HEALTH SCIENCES, NASHIK

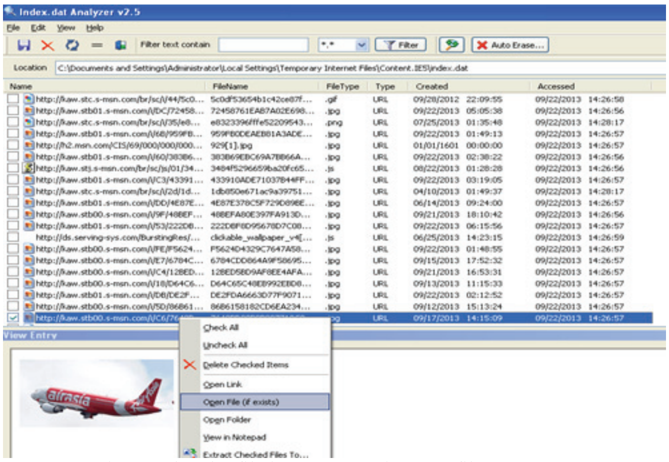
STATEMENT OF MARKS FOR FIRST BDS(New) - Summer-2014

Name of the Student - HALAWADE SAMPADA SANJAY

College:- Sinhgad Dental College & Hospital, Pune

Seat No:- 20400 PRN No:- 0214120400

Fig5. Index.dat file in history

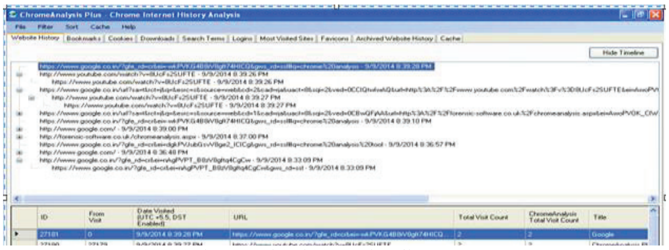


Name	FileName	FileType	Type	Created	Accessed
http://kaw.stc.s-msn.com/br/sc/i/44/5c0...	5c0df53654b1c42ce87f...	.gif	URL	09/28/2012 22:09:55	09/22/2013 14:26:58
http://kaw.stb01.s-msn.com/i/DC/72458...	72458761EAB7A02E698...	.jpg	URL	09/22/2013 05:05:38	09/22/2013 14:26:56
http://kaw.stc.s-msn.com/br/sc/i/35/e8...	e8323396fffe52209543...	.png	URL	07/25/2013 01:35:48	09/22/2013 14:28:17
http://kaw.stb01.s-msn.com/i/6B/959FB...	959FB0DEAEB81A3ADE...	.jpg	URL	09/22/2013 01:49:13	09/22/2013 14:26:57
http://h2.msn.com/CIS/69/000/000/000...	929[1].jpg	.jpg	URL	01/01/1601 00:00:00	09/22/2013 14:26:57
http://kaw.stb01.s-msn.com/i/60/383B6...	383B69EBC69A7B866A...	.jpg	URL	09/22/2013 02:38:22	09/22/2013 14:26:56
http://kaw.stj.s-msn.com/br/sc/js/01/34...	3484f5296659ba20fc65...	.js	URL	08/22/2013 01:28:28	09/22/2013 14:26:56
http://kaw.stb01.s-msn.com/i/C3/43391...	433910ADE71037844FF...	.jpg	URL	09/22/2013 03:19:05	09/22/2013 14:26:57
http://kaw.stc.s-msn.com/br/sc/i/2d/1d...	1db850e671ac9a39751...	.jpg	URL	04/10/2013 01:49:37	09/22/2013 14:28:17
http://kaw.stb01.s-msn.com/i/DD/4E87E...	4E87E378C5F729D898E...	.jpg	URL	06/14/2013 09:24:00	09/22/2013 14:26:57
http://kaw.stb00.s-msn.com/i/9F/488EF...	488EFA80E397FA913D...	.jpg	URL	09/21/2013 18:10:42	09/22/2013 14:26:56
http://kaw.stb01.s-msn.com/i/53/222D8...	222D8F8D95678D7C08...	.jpg	URL	09/22/2013 06:15:56	09/22/2013 14:26:57
http://ds.serving-sys.com/BurstingRes/...	clickable_wallpaper_v4[...	.js	URL	06/25/2013 14:23:15	09/22/2013 14:26:59
http://kaw.stb00.s-msn.com/i/FE/F5624...	F5624D4329C7647A58...	.jpg	URL	09/22/2013 01:48:55	09/22/2013 14:26:57
http://kaw.stb00.s-msn.com/i/E7/6784C...	6784CDD864A9F58695...	.jpg	URL	09/15/2013 17:52:32	09/22/2013 14:26:57
http://kaw.stb00.s-msn.com/i/C4/128ED...	128ED58D9AF8EE4AFA...	.jpg	URL	09/21/2013 16:53:31	09/22/2013 14:26:57
http://kaw.stb00.s-msn.com/i/18/D64C6...	D64C65C48EB992EBD8...	.jpg	URL	09/13/2013 11:15:33	09/22/2013 14:26:57
http://kaw.stb01.s-msn.com/i/DB/DE2F...	DE2FDA6663D77F9071...	.jpg	URL	09/22/2013 02:12:52	09/22/2013 14:26:57
http://kaw.stb00.s-msn.com/i/5D/86861...	8686158182CD6EA234...	.jpg	URL	09/12/2013 15:13:24	09/22/2013 14:26:57
http://kaw.stb00.s-msn.com/i/C6/76...	[illegible]	.jpg	URL	09/17/2013 14:15:09	09/22/2013 14:26:57

Fig. 6 Index.dat file in temporary internet file

C. ChromeAnalysis Plus

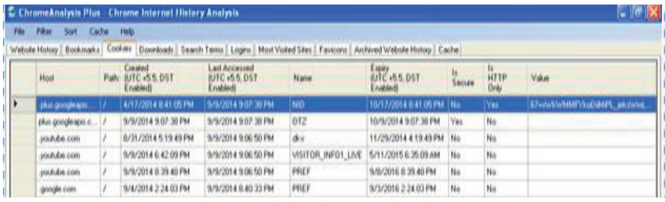
ChromeAnalysis Plus [3, 12] is a software tool for getting, viewing and studying internet history from the Google Chrome web browser. It extract history regarding bookmarks, cookies, downloads, favicons, logins, most visited sites, search terms and website visits. Fig 7 to 12 shows web history, cookie history, download history and search term timelines, login information, cache analysis respectively.


ChromeAnalysis Plus - Chrome Internet History Analysis
File Filter Sort Cache Help
Website History Bookmarks Cookies Downloads Search Terms Logins Most Visited Sites Favicons Archived Website History Cache
Hide Timeline

https://www.google.co.in/?gfe_rd=cr&ei=wkPVKG4B8V8gh74HICQ&gws_rd=ssl#q=chrome%20analysis - 9/9/2014 8:39:28 PM
http://www.youtube.com/watch?v=8UcFs2SUFTE - 9/9/2014 8:39:26 PM
https://www.youtube.com/watch?v=8UcFs2SUFTE - 9/9/2014 8:39:26 PM
https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&sqi=2&ved=0CCIQtwIwAQ&url=http%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3D8UcFs2SUFTE&ei=AwoPV
http://www.youtube.com/watch?v=8UcFs2SUFTE - 9/9/2014 8:39:27 PM
https://www.youtube.com/watch?v=8UcFs2SUFTE - 9/9/2014 8:39:27 PM
https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&sqi=2&ved=0CBwQFjAA&url=http%3A%2F%2Fforensic-software.co.uk%2Fchromeanalysis.aspx&ei=AwoPVOK_CIv
https://www.google.co.in/?gfe_rd=cr&ei=wkPVKG4B8V8gh74HICQ&gws_rd=ssl#q=chrome%20analysis - 9/9/2014 8:39:10 PM
http://www.google.com/ - 9/9/2014 8:39:00 PM
http://forensic-software.co.uk/chromeanalysis.aspx - 9/9/2014 8:37:00 PM
https://www.google.co.in/?gfe_rd=cr&ei=dgkPVJubGsvV8ge2_ICICg&gws_rd=ssl#q=chrome%20analysis%20tool - 9/9/2014 8:36:57 PM
http://www.google.com/ - 9/9/2014 8:36:48 PM
http://www.google.co.in/?gfe_rd=cr&ei=nAgPVPT_B8zV8ghq4CgCw - 9/9/2014 8:33:09 PM
https://www.google.co.in/?gfe_rd=cr&ei=nAgPVPT_B8zV8ghq4CgCw&gws_rd=ssl - 9/9/2014 8:33:09 PM

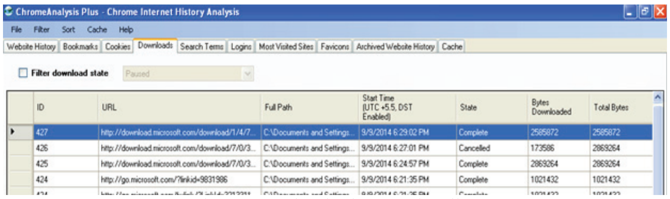
ID	From Visit	Date Visited (UTC +5.5, DST Enabled)	URL	Total Visit Count	ChromeAnalysis Total Visit Count	Title
27181	0	9/9/2014 8:39:28 PM	https://www.google.co.in/?gfe_rd=cr&ei=wkPVKG4B8V8gh74HICQ...	2	2	Google
27180	27179	9/9/2014 8:39:27 PM	https://www.youtube.com/watch?v=8UcFs2SUFTE	2	2	ChromeAnalysis Pl

Fig 7.Web History Timeline


ChromeAnalysis Plus - Chrome Internet History Analysis
File Filter Sort Cache Help
Website History Bookmarks Cookies Downloads Search Terms Logins Most Visited Sites Favicons Archived Website History Cache

Host	Path	Created (UTC +5.5, DST Enabled)	Last Accessed (UTC +5.5, DST Enabled)	Name	Expiry (UTC +5.5, DST Enabled)	Is Secure	Is HTTP Only	Value
plus.googleapis...	/	4/17/2014 8:41:05 PM	9/9/2014 9:07:38 PM	NID	10/17/2014 8:41:05 PM	No	Yes	67=vIvWvMMFVIuDiMPL_jak....
plus.googleapis.c...	/	9/9/2014 9:07:38 PM	9/9/2014 9:07:38 PM	OTZ	10/9/2014 9:07:38 PM	Yes	No	
.youtube.com	/	8/31/2014 5:19:49 PM	9/9/2014 9:06:50 PM	dkv	11/29/2014 4:19:49 PM	No	No	
.youtube.com	/	9/9/2014 6:42:09 PM	9/9/2014 9:06:50 PM	VISITOR_INFO1_LIVE	5/11/2015 6:35:09 AM	No	No	
.youtube.com	/	9/9/2014 8:39:40 PM	9/9/2014 9:06:50 PM	PREF	9/8/2016 8:39:40 PM	No	No	
.google.com	/	9/4/2014 2:24:03 PM	9/9/2014 8:40:33 PM	PREF	9/3/2016 2:24:03 PM	No	No	

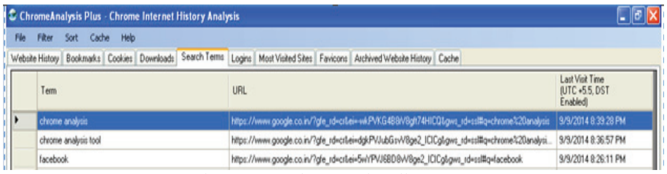
Fig 8.Cookie History Timeline


ChromeAnalysis Plus - Chrome Internet History Analysis
File Filter Sort Cache Help
Website History Bookmarks Cookies Downloads Search Terms Logins Most Visited Sites Favicons Archived Website History Cache

☐ Filter download state Paused

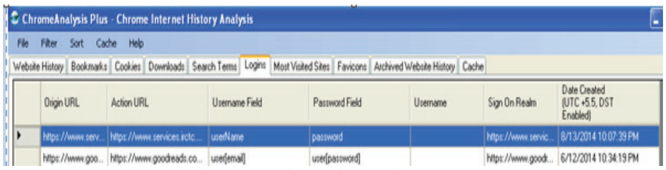
ID	URL	Full Path	Start Time (UTC +5.5, DST Enabled)	State	Bytes Downloaded	Total Bytes
427	http://download.microsoft.com/download/1/4/7...	C:\Documents and Settings...	9/9/2014 6:29:02 PM	Complete	2585872	2585872
426	http://download.microsoft.com/download/7/0/3...	C:\Documents and Settings...	9/9/2014 6:27:01 PM	Cancelled	173586	2869264
425	http://download.microsoft.com/download/7/0/3...	C:\Documents and Settings...	9/9/2014 6:24:57 PM	Complete	2869264	2869264
424	http://go.microsoft.com/?linkid=9831986	C:\Documents and Settings...	9/9/2014 6:21:35 PM	Complete	1021432	1021432

Fig 9.Download History Timeline


ChromeAnalysis Plus - Chrome Internet History Analysis
File Filter Sort Cache Help
Website History Bookmarks Cookies Downloads Search Terms Logins Most Visited Sites Favicons Archived Website History Cache

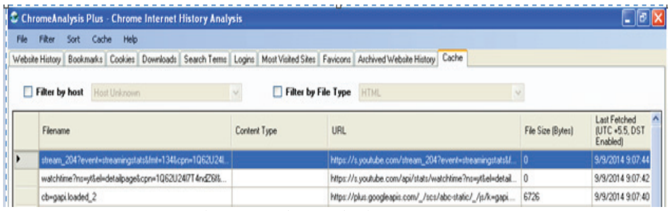
Term	URL	Last Visit Time (UTC +5.5, DST Enabled)
chrome analysis	https://www.google.co.in/?gfe_rd=cr&ei=wkPVKG4B8V8gh74HICQ&gws_rd=ssl#q=chrome%20analysis	9/9/2014 8:39:28 PM
chrome analysis tool	https://www.google.co.in/?gfe_rd=cr&ei=dgkPVJubGsvV8ge2_ICICg&gws_rd=ssl#q=chrome%20analysi...	9/9/2014 8:36:57 PM
facebook	https://www.google.co.in/?gfe_rd=cr&ei=5wYPVJ6BD8vV8ge2_ICICg&gws_rd=ssl#q=facebook	9/9/2014 8:26:11 PM

Fig 10.Search term timelines


ChromeAnalysis Plus - Chrome Internet History Analysis
File Filter Sort Cache Help
Website History Bookmarks Cookies Downloads Search Terms Logins Most Visited Sites Favicons Archived Website History Cache

Origin URL	Action URL	Username Field	Password Field	Username	Sign On Realm	Date Created (UTC +5.5, DST Enabled)
https://www.serv...	https://www.services.irctc...	userName	password		https://www.servic...	8/13/2014 10:07:39 PM
https://www.goo...	https://www.goodreads.co...	user[email]	user[password]		https://www.goodr...	6/12/2014 10:34:19 PM

Fig 11.Logins Information


ChromeAnalysis Plus - Chrome Internet History Analysis
File Filter Sort Cache Help
Website History Bookmarks Cookies Downloads Search Terms Logins Most Visited Sites Favicons Archived Website History Cache

☐ Filter by host Host Unknown ☐ Filter by File Type HTML

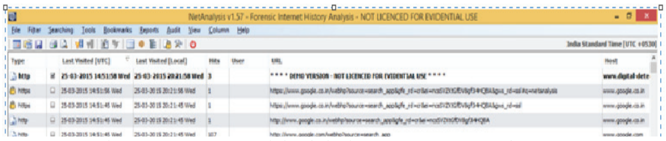
Filename	Content Type	URL	File Size (Bytes)	Last Fetched (UTC +5.5, DST Enabled)
stream_204?event=streamingstats&fmt=134&cpn=1Q62U24l...		https://s.youtube.com/stream_204?event=streamingstats&f...	0	9/9/2014 9:07:44
watchtime?ns=yt&el=detailpage&cpn=1Q62U24l7T4nd26l&...		https://s.youtube.com/api/stats/watchtime?ns=yt&el=detail...	0	9/9/2014 9:07:42
cb=gapi.loaded_2		https://plus.googleapis.com/_/scs/abc-static/_/js/k=gapi...	6726	9/9/2014 9:07:40

Fig 12.Cache analysis

D. NetAnalysis v1.52

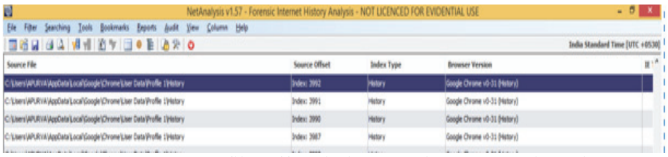
NetAnalysis v1.52 [3, 13] is web browser forensic tool, it supports all major five browsers. It is mainly used to analyze history information.

Fig 13, 14, 15 shows different tabs and sql query builder.


NetAnalysis v1.57 - Forensic Internet History Analysis - NOT LICENCED FOR EVIDENTIAL USE
File Filter Searching Tools Bookmarks Reports Audit View Column Help
India Standard Time [UTC +0530]

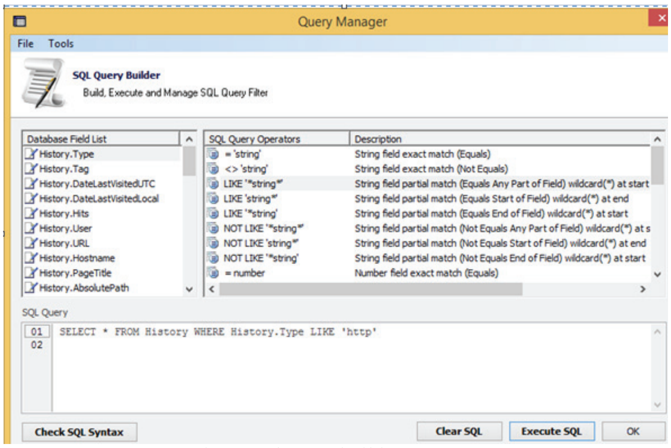
Type		Last Visited [UTC]	Last Visited [Local]	Hits	User	URL	Host
http	☑	25-03-2015 14:51:58 Wed	25-03-2015 20:21:58 Wed	3		* * * * DEMO VERSION - NOT LICENCED FOR EVIDENTIAL USE * * * *	www.digital-dete
https	☐	25-03-2015 14:51:56 Wed	25-03-2015 20:21:56 Wed	1		https://www.google.co.in/webhp?source=search_app&gfe_rd=cr&ei=[illegible]&gws_rd=ssl#q=netanalysis	www.google.co.in
https	☐	25-03-2015 14:51:45 Wed	25-03-2015 20:21:45 Wed	1		https://www.google.co.in/webhp?source=search_app&gfe_rd=cr&ei=[illegible]&gws_rd=ssl	www.google.co.in
http	☐	25-03-2015 14:51:45 Wed	25-03-2015 20:21:45 Wed	1		http://www.google.co.in/webhp?source=search_app&gfe_rd=cr&ei=[illegible]	www.google.co.in
http	☐	25-03-2015 14:51:45 Wed	25-03-2015 20:21:45 Wed	107		http://www.google.com/webhp?source=search_app	www.google.com

Fig 13. Type, Last visited timings, URL, Host tabs


NetAnalysis v1.57 - Forensic Internet History Analysis - NOT LICENCED FOR EVIDENTIAL USE
File Filter Searching Tools Bookmarks Reports Audit View Column Help
India Standard Time [UTC +0530]

Source File	Source Offset	Index Type	Browser Version
C:\Users\APURVA\AppData\Local\Google\Chrome\User Data\Profile 1\History	Index: 3992	History	Google Chrome v0-31 (History)
C:\Users\APURVA\AppData\Local\Google\Chrome\User Data\Profile 1\History	Index: 3991	History	Google Chrome v0-31 (History)
C:\Users\APURVA\AppData\Local\Google\Chrome\User Data\Profile 1\History	Index: 3990	History	Google Chrome v0-31 (History)
C:\Users\APURVA\AppData\Local\Google\Chrome\User Data\Profile 1\History	Index: 3987	History	Google Chrome v0-31 (History)

Fig 14. Source file, offset, index type, browser version tab



Database Field List
History.Type
History.Tag
History.DateLastVisitedUTC
History.DateLastVisitedLocal
History.Hits
History.User
History.URL
History.Hostname
History.PageTitle
History.AbsolutePath

SQL Query Operators	Description
= 'string'	String field exact match (Equals)
<> 'string'	String field exact match (Not Equals)
LIKE '*string*'	String field partial match (Equals Any Part of Field) wildcard(*) at start
LIKE 'string*'	String field partial match (Equals Start of Field) wildcard(*) at end
LIKE '*string'	String field partial match (Equals End of Field) wildcard(*) at start
NOT LIKE '*string*'	String field partial match (Not Equals Any Part of Field) wildcard(*) at s
NOT LIKE 'string*'	String field partial match (Not Equals Start of Field) wildcard(*) at end
NOT LIKE '*string'	String field partial match (Not Equals End of Field) wildcard(*) at start
= number	Number field exact match (Equals)

SQL Query

```
SELECT * FROM History WHERE History.Type LIKE 'http'
```

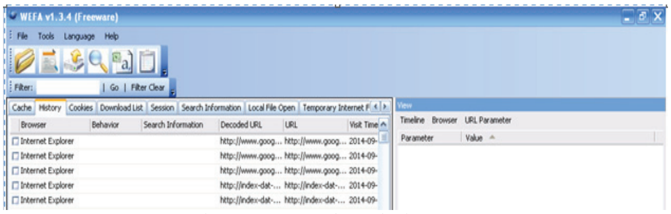
Fig 15.Sql query builder

E. The WEFA (Web Browser Forensic Analyzer)

WEFA tool [3, 14] gives improvements to the weak points of other tools and provides effective analysis of web browsers. This tool provides an integrated analysis function for all five web browsers in various time zones, in addition it provides online user activity, search words, and URL parameters, which are significant information for digital forensics. Also this tool gives a decoding function, when the search word information is encoded in unknown characters or if the search words are in different languages.

An investigator can find out the motive of the illegal actions as well as the intention of the untrustworthy person with these functions. Available tool environments include Windows o.s and the targeted web browsers for analysis are Internet Explorer, Firefox, Chrome, Safari, and opera.

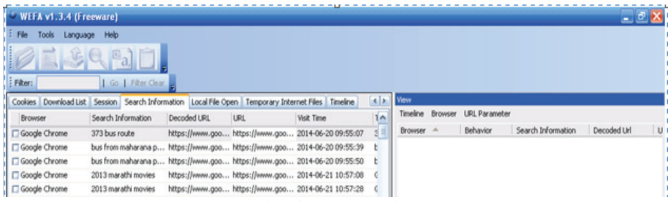
Fig 16 to 21 shows different analysis of web browser by WEFA.


WEFA v1.3.4 (Freeware)
File Tools Language Help
Filter: | Go | Filter Clear
Cache History Cookies Download List Session Search Information Local File Open Temporary Internet F
View
Timeline Browser URL Parameter

Browser	Behavior	Search Information	Decoded URL	URL	Visit Time
□ Internet Explorer			http://www.goog...	http://www.goog...	2014-09-
□ Internet Explorer			http://www.goog...	http://www.goog...	2014-09-
□ Internet Explorer			http://www.goog...	http://www.goog...	2014-09-
□ Internet Explorer			http://index-dat-...	http://index-dat-...	2014-09-
□ Internet Explorer			http://index-dat-...	http://index-dat-...	2014-09-

Parameter	Value

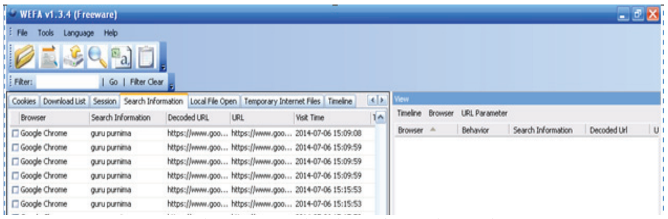
Fig16. Integrated Analysis


WEFA v1.3.4 (Freeware)
File Tools Language Help
Filter: | Go | Filter Clear
Cookies Download List Session Search Information Local File Open Temporary Internet Files Timeline
View
Timeline Browser URL Parameter

Browser	Search Information	Decoded URL	URL	Visit Time
□ Google Chrome	373 bus route	https://www.goo...	https://www.goo...	2014-06-20 09:55:07
□ Google Chrome	bus from maharana p...	https://www.goo...	https://www.goo...	2014-06-20 09:55:39
□ Google Chrome	bus from maharana p...	https://www.goo...	https://www.goo...	2014-06-20 09:55:50
□ Google Chrome	2013 marathi movies	https://www.goo...	https://www.goo...	2014-06-21 10:57:08
□ Google Chrome	2013 marathi movies	https://www.goo...	https://www.goo...	2014-06-21 10:57:28

Browser	Behavior	Search Information	Decoded Url	U

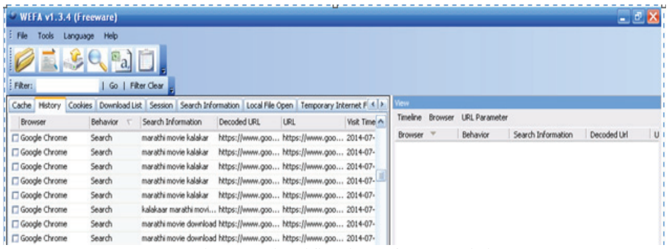
Fig 17.Timeline Analysis


WEFA v1.3.4 (Freeware)
File Tools Language Help
Filter: | Go | Filter Clear
Cookies Download List Session Search Information Local File Open Temporary Internet Files Timeline
View
Timeline Browser URL Parameter

Browser	Search Information	Decoded URL	URL	Visit Time
□ Google Chrome	guru purnima	https://www.goo...	https://www.goo...	2014-07-06 15:09:08
□ Google Chrome	guru purnima	https://www.goo...	https://www.goo...	2014-07-06 15:09:59
□ Google Chrome	guru purnima	https://www.goo...	https://www.goo...	2014-07-06 15:09:59
□ Google Chrome	guru purnima	https://www.goo...	https://www.goo...	2014-07-06 15:09:59
□ Google Chrome	guru purnima	https://www.goo...	https://www.goo...	2014-07-06 15:15:53
□ Google Chrome	guru purnima	https://www.goo...	https://www.goo...	2014-07-06 15:15:53

Browser	Behavior	Search Information	Decoded Url	U

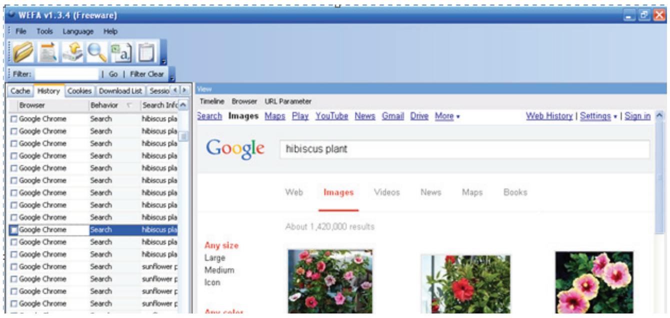
Fig 18.Investigation of search word


WEFA v1.3.4 (Freeware)
File Tools Language Help
Filter: | Go | Filter Clear
Cache History Cookies Download List Session Search Information Local File Open Temporary Internet F
View
Timeline Browser URL Parameter

Browser	Behavior	Search Information	Decoded URL	URL	Visit Time
□ Google Chrome	Search	marathi movie kalakar	https://www.goo...	https://www.goo...	2014-07-
□ Google Chrome	Search	marathi movie kalakar	https://www.goo...	https://www.goo...	2014-07-
□ Google Chrome	Search	marathi movie kalakar	https://www.goo...	https://www.goo...	2014-07-
□ Google Chrome	Search	marathi movie kalakar	https://www.goo...	https://www.goo...	2014-07-
□ Google Chrome	Search	marathi movie kalakar	https://www.goo...	https://www.goo...	2014-07-
□ Google Chrome	Search	kalakaar marathi movi...	https://www.goo...	https://www.goo...	2014-07-
□ Google Chrome	Search	marathi movie download	https://www.goo...	https://www.goo...	2014-07-
□ Google Chrome	Search	marathi movie download	https://www.goo...	https://www.goo...	2014-07-

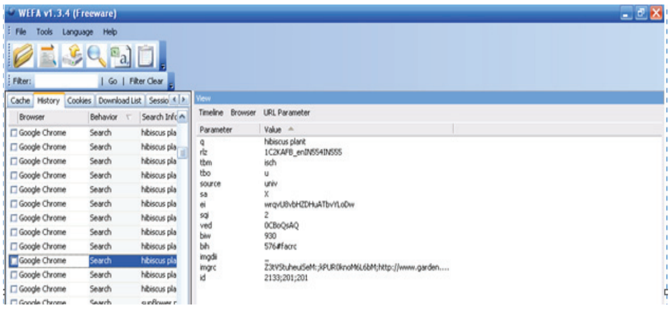
Browser	Behavior	Search Information	Decoded Url	U

Fig 19. Classification of user activity


WEFA v1.3.4 (Freeware)
File Tools Language Help
Filter: | Go | Filter Clear
Cache History Cookies Download List Sessio
View
Timeline Browser URL Parameter
Search Images Maps Play YouTube News Gmail Drive More ▾
Web History | Settings ▾ | Sign in
Google
hibiscus plant
Web Images Videos News Maps Books
About 1,420,000 results
Any size
Large
Medium
Icon

Browser	Behavior	Search Info
□ Google Chrome	Search	hibiscus pla
□ Google Chrome	Search	hibiscus pla
□ Google Chrome	Search	hibiscus pla
□ Google Chrome	Search	hibiscus pla
□ Google Chrome	Search	hibiscus pla
□ Google Chrome	Search	hibiscus pla
□ Google Chrome	Search	hibiscus pla
□ Google Chrome	Search	hibiscus pla
□ Google Chrome	Search	hibiscus pla
□ Google Chrome	Search	hibiscus pla
□ Google Chrome	Search	hibiscus pla
□ Google Chrome	Search	hibiscus pla
□ Google Chrome	Search	sunflower p
□ Google Chrome	Search	sunflower p
□ Google Chrome	Search	sunflower p
□ Google Chrome	Search	sunflower p

Fig 20.Cache/history examination


WEFA v1.3.4 (Freeware)
File Tools Language Help
Filter: | Go | Filter Clear
Cache History Cookies Download List Sessio
View
Timeline Browser URL Parameter

Browser	Behavior	Search Info
□ Google Chrome	Search	hibiscus pla
□ Google Chrome	Search	hibiscus pla
□ Google Chrome	Search	hibiscus pla
□ Google Chrome	Search	hibiscus pla
□ Google Chrome	Search	hibiscus pla
□ Google Chrome	Search	hibiscus pla
□ Google Chrome	Search	hibiscus pla
□ Google Chrome	Search	hibiscus pla
□ Google Chrome	Search	hibiscus pla
□ Google Chrome	Search	hibiscus pla
□ Google Chrome	Search	hibiscus pla
□ Google Chrome	Search	hibiscus pla

Parameter	Value
q	hibiscus plant
rlz	1C2KAFB_enIN554IN555
tbm	isch
tbo	u
source	univ
sa	X
ei	wrqvU8vbHZDHuATbvYLoDw
sqi	2
ved	0CBoQsAQ
biw	930
bih	576#facrc
imgdii	_
imgrc	Z3tVStuheuISeM:;kPUR0knoM6L6bM;http://www.garden....
id	2133;201;201

Fig 21.Aanalysis of URL parameter

IV. COMPARATIVE ANALYSIS

TABLE I. Describe comparative analysis of different technology used to investigate data

Tools/Technology	Targeted web browser/O.S	Information to be analyzed	Information Retrieved
Web Historian 1.3 [10]	IE, Firefox, Safari, chrome / Windows	Web history,cookie history, download history	• Shows name of the browser, browser version, windows account name that created this record, web page visited. • Download history tab gives information about type of download operation, name of the file that was downloaded, • URL from which the file was downloaded, local directory where the file was downloaded to, entire HTTP header that caused the download, date the file was last accessed and modified.
Index.dat Analyzer 2.5 [11]	IE / Windows	Index.dat	Index.dat Analyzer enables to view the content of index.dat files which has hint to cookies, browser history and cached pages.
ChromeAnalysis plus [12]	Chrome	It get's history related to bookmarks, cookies, downloads, favicons, logins, most visited sites, search terms and website visits.	• Shows host name, cookie created and last accessed date and time information, cookie name and expiry date and timing from cookie history timeline. • Download history gives information about downloaded file URL, path, and downloading state. • Search term timeline gives the information about what search words are used by suspect. • Login information gives username field and password field information. • Most visited sites tab indicates websites suspect visited frequently.

			• Favicons shows the icon associated with a website for which suspect is searching for. • Archieved Website History extracts archieved search terms and web history. • Cache analysis gives the cache file information. It shows the properties of cache file, file name, URL of cached files and last fetched date and time.
NetAnalysis 1.52 [13]	IE, Firefox, Chrome, Safari, Opera / Windows	History	Shows type of protocol, last visited timings, URL, Host name, page title, source file , browser version. Find type of protocol, last visited time, URL and host .From this investigator can retrieve the information of criminals internet activity. Integrated and timeline analysis can be done.
WEFA [14]	IE,Firefox, Chrome, Safari, Opera/windows	Cache, History, Cookies, Download List	Easy to perform integrated and Timeline analysis. Provides Search word analysis, URL decoding function. Classification of user activity through specific keywords from HTTP URLs.

We analyzed here history, cookies, cache, bookmarks, download list, search words and index.dat file.

Web Historian 1.3[10] Shows name of the browser, browser version, windows account name that created this record, web page visited. Download history tab gives information about type of download operation, name of the file that was downloaded, URL from which the file was downloaded, local directory where the file was downloaded to, entire HTTP header that caused the download, date the file was last accessed and modified.

Index.dat analyzer [11] is used to view the data of index.dat files which has references to cookies, browser history and cached pages.

ChromeAnalysis [12] plus Shows host name, cookie created and last accessed date and time information cookie name and expiry date and timing from cookie history timeline. Download history gives information about downloaded file URL, path, and downloading state. Search term timeline gives the information about what search words are used by suspect. Login information gives username field and password field information. Most visited sites tab shows which websites suspect visited frequently. Favicons shows the icon associated with a website for which suspect is searching for. Archieved Website History extracts archieved search terms and web history. Cache analysis gives the cache file information. It shows the properties of cache file, file name, URL of cached files and last fetched date and time.

NetAnalysis [13] Shows type of protocol, last visited timings, URL, Host name, page title, source file, browser version. find type of protocol, last visited time, URL and host. From this investigator can retrieve the information of criminal's internet activity. Also gives collective and timeline analysis. WEFA [14] is Easy to perform integrated and Timeline analysis. Provides search word analysis, URL decoding function. Classification of user activity through specific keywords from HTTP URLs.

VI. CONCLUSION

Forensic evidence could be collected from a web browser such as cache, history, cookies, download list. Private browsing is a privacy feature in all major browsers to disable browsing history, and the web cache. This allows criminal to browse the web without storing local data.

InPrivate browsing records were found in the database file,WebCacheV01.dat, in related log files, and in other areas on the disk. It can be recovered by using some carving tool such as ESECarve.

Some other techniques that can use to recover browsing data – WEFA tool provides improvements to the weak points of other tools and has the strength of providing efficient analysis of Web browsers compared to past tools. If the unauthorised person has deleted log information then these log files can be recovered with this tool. After analyzing information from the tool, it is possible to use the different search functions such as keyword search, regular expression search, and search by time period. Depending on the information the investigator selects, he can create the reports. All tools mentioned in this paper are running in windows environment, future scope will be web browser forensic in various operating systems.

REFERENCES

[1] Ranveet Kaur,Amandeep Kaur, " Digital Forensics" International Journal of Computer Applications pp 0975 –8887 Volume 50 – No.5, July 2012.

[2] Nina Godbole, Sunit Belapure, Cyber Security, Wiley India, New Delhi.(reference)

[3] Junghoon Oh,Seungbong Lee,Sangjin Lee,"Advanced evidence collection and analysis of web browser activity", DIGITAL INVESTIGATION S62-S70 ,2011.

[4] Junghoon Oh , Namheun Son, Sangjin Lee, and Kyungho Lee. "A Study for Classification of Web Browser Log and Timeline Visualization",WISA-2012.

[5] F.Aggarwal, E. Bursztein, C. Jackson, and D. Boneh, "An analysis of private browsing modes in modern browsers," In Proc. Of 19th Usenix Security Symposium, 2010.

[6] Donny Jacob Ohana,Narasimha Shashidhar,"Do Private and PortableWeb Browsers Leave Incriminating Evidence?",IEEE Security and Privacy Workshops,2013.

[7] Howard Chivers "Private browsing: A window of forensic opportunity",Digital Investigation 20–29,2014.

[8] Howard Chivers, Christopher Hargreaves. "Forensic data recovery from the Windows Search Database" , Digital Investigation 114–26,2011.

[9] Muhammad Yasin, Ahmad R. Cheema, Firdous Kausar, "Analysis of Internet Download Manager for collection of digital forensic artefacts", DIGITAL INVESTIGATION 90-94,2010.

[10] Web Historian Tool. Available at- http://download.cnet.com/Web-Historian/3000-2653 4-10373157.html

[11] Index.dat Analyzer v2.5 tool. Available at-http://www. Systenance .com/indexdat.php

[12] ChromeAnalysis Plus tool. Available at- http://www.forensic-software.co.uk/ Chrome Analysis.aspx

[13] NetAnalysis v1.52 tool. Available at-
http://www.fileol.com/security/netanalysis-1.52.html

[14] Berners-Lee T, Masinter L. RFC 1738:Uniform Resource Locator(URL), Available at http:// tools.ietf.org/html/rfc1738.

[15] Jones Keith j, Rohyt Blani. Web browser forensic. Security focus, Available athttp:// www.securityfocus.com/infocus/1827; 2005a

[16] Jones Keith j, Rohyt Blani. Web browser forensic. Security focus, Available athttp:// www.securityfocus.com/infocus/1832; 2005b.