Web Browser Forensic Tools: Autopsy, BHE and NetAnalysis

Hassan Adamu[1], Abdullahi Adamu Ahmad[2], Adamu Hassan[3], Sa'ad Barau Gambasha[4]

[1]Binyaminu Usman Polytechnic, Hadejia, Jigawa State, Nigeria
[2]Kano Electricity Distribution Company (KEDCO), Kano State, Nigeria
[3]Ajaokuta Steel Company Limited, Kogi State, Nigeria
[4]Binyaminu Usman Polytechnic, Hadejia, Jigawa State, Nigeria

***Abstract*—Information and communication technology (ICT) are becoming an integral part of everyone´s lives which affects all sectors of human activity. Nowadays, the level of computer crimes rises and it is alarming, for such, digital forensic investigation plays a vital role in tackling computer-related crimes such as cyberbullying, fraud, cyber intrusion, hacking an et cetera. The main goal of digital forensic investigation is to preserve any evidence found in its most original form and to make sure that the evidence is not tempered. Digital forensic investigators use log files to extract, analyse and present a report based on the criminal activities found on the web browsers, such log files include history, cache, download and cookies. This survey paper evaluates the features of the three selected web browsers forensic tools namely; Browser History Examiner, Autopsy and NetAnalysis, and make comparative analysis between them. The findings of the evaluation based on the features of the selected tools shows that Autopsy is the best forensic tool among them. Therefore, in this paper, Autopsy has been recommended fora digital investigator or examiner to use as their forensic tool among others.**

***Keywords* –Web Browsers, Digital Forensic Tools, Autopsy, NetAnalysis, Browser History Examiner**

I. INTRODUCTION

This survey paper focuses on web browsers forensic tools. A web browser is a computer program or application that is use to surf an internet. Nowadays, millions of people use to search an information through web browsers, such information include checking emails, online transactions, downloading educational materials, social networking, online bankingand others [1].

Digital criminals usually conduct their criminal activities via web browsers. As such, it is very important for digital forensic examiners to acquire, extract and analyse the evidences found from the suspect with respect to the usage of the web browsers [2]. There are several web browsers that are available online which includes Mozilla Firefox, Google Chrome, Internet Explorer and many more.

According to Blaine Stephens "Digital forensic is the science of identifying, preserving, recovering, analyzing and presentation of fact on digital evidences found on computers or any other media storage devices"[3]. Digital forensic usually investigates the collected data from storage media devices such as hard drive and other devices with sticking to standard policies and procedures.

Autopsy, Browser History Examiner (BHE) and NetAnalysis are the digital forensic tools chosen in this survey paper to investigate their features and makecomparison between them. Kent, K. and Grance, T. [4] developed a computer forensic Model to help investigators conduct their digital investigation. They named the Model as Four Step Forensic Process (FSFP)

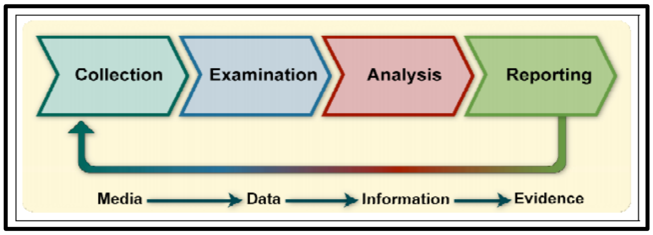


Fig. 1 Four Step Forensic Process [4]

1. Collection is the first phase in four step forensic process;In this phase, data is identified and put in a chain of custody, preserveand safeguard its integrity.
2. The second phase of the forensic investigation model is to examine the data collected at the crime scene and choose an appropriate forensic tool to be used in order to filter-out useful information from the collected data.
3. The third phase of the model is the analysis of the results. The digital evidence found and extracted from the examined data is to be analysed to addressed the questions that were motivated during collection and examination.
4. The final phase is reporting in which the analysed results were presented, with the kind of actioned performed and the recommendations. [4]

The analysis phase is very important in digital forensic investigation because an investigator gets the results based on the collected evidence. In this regard, web browser forensic tool is use to examine and analyse data acquired during collection. The investigators usually conduct their investigation from the web browser by checking, extracting and investigating the browser log file such as history, cache, cookies, and downloads. There are various analysis tools for web browsers, in that, their features, performance and compatibility with some browsers may differ [5].

This survey paper evaluates the features of the three selected browsers forensic tools namely; Browser History Examiner, Autopsy and NetAnalysis and make comparative analysis between them. WHY? It contains four sections, section I is the introduction, section II is the related works, section III discussed the selected three web forensic tools and section IV evaluate their features and comparison between the forensic tools.

II. RELATED WORKS

A web browser is an important application use to search for an information regarding businesstransactions, educational research, sport, entertainment and so much more. Web browsers such as Firefox, Chrome etc. has the ability to store log file in its memory. REPEATED? With the help of the log files, digital investigators can be able to identify, extract, collect and analyse digital evidence found in suspect computers with regard to any kind of crimes committed by the criminals. If a suspect use different web browser in committing crime, all the information on the browsers should be generated, retrieved and analysed on the same timeline.

S. Mahaju and T. Atkison on the topic “Evaluation of Firefox Browser Forensics Tools” provided a survey on forensic analysis tool for web browser and evaluates their features and performance in regard to the selected browser which is Firefox. The analysis tools that were selected in conducting the survey are NetAnalysis V2, FoxAnalysis V1.6.0, PasswordFox, Browser History Examiner and MZ History Viewer. They tested the tools based on their memory consumption, time constraints and their availability. After the evaluation, the results show that the selected tools in the survey paper had their own strength and weaknesses but, they eventually choose FoxAnalysis as one of the suitable tools that can perform the job [5].

E. Akbal, Futma G. and Ayhan in their research paper titled “Digital Forensic Analyses of Web Browser Records” explain how web browsers store information and how OS store records. They show how digital evidence collected during the cost of investigation can be analyse on web browser forensic tools. In some part of their research paper, they briefly discussed the features and performance of some forensic tools [6].

Amor. L, Thabet S. in their research paper “Forensics Investigation of Web Application Security Attacks” discussed the concept of web application forensic in which they described it as a sub-set of networks forensic, they proposed a methodology that would help an investigation of web application security to successfully be accomplished. In their research paper, they selected many web application forensic tools and describe them in detail and finally, they provided a technical comparison between the selected tools to help an investigator to choose anyone that is relevant to his investigation [7].

D. Rathod, in his research paper “Web Browser Forensic: Google Chrome” discussed many techniques that can be used to collect data or information by the digital forensic examiner, such techniques include; prefetch, history, cookies, login data, RAM dump etc. the researcher explained that if an investigator applied these techniques, they would help him to extract an evidences like visited websites, last accessed, date and time and how to recover deleted files by the suspect on Google Chrome [3], [8].

J. Oh, S. Lee ,Sangjin L. in their research paper titled “Advanced evidence collection and analysis of web browser activity” selected some web browser forensic tools which include: WEFA, Cache Back 3.17, Encase 6.13, FTK 3.2 and NetAnalysis 1.52. They discussed their features and advantages and make functional comparison between them, after the comparison, they suggested that WEFA forensic tool is the most useful forensic tool for collecting digital evidence from web browsers and it helps investigators to conduct their analysis faster compared to other tools [9],[11].

M. Kaur, N. Kaur, S. Khurana, in their research paper titled “A Literature Review on Cyber Forensic and its Analysis tools” extensively discussed the concept behind digital forensic and further explained useful information with regard to the tools operated in forensic investigation. They also examined different kind of forensic tool for security flaws in digital investigation process such as analysis of volatile memory, network packets, toolkit, disk and encrypted drives [10],[12].

Several researches were conducted on different computer forensic tools, most of the research studies focuses on one or more tools and choose some specific browsers as their case studies in order to test the performance and compare the tools on the particular selected browser. This study focuses on the three selected web browser forensic tools, their comparison based on their features were explained in the last section of this survey paper. SECTION IV AND V?

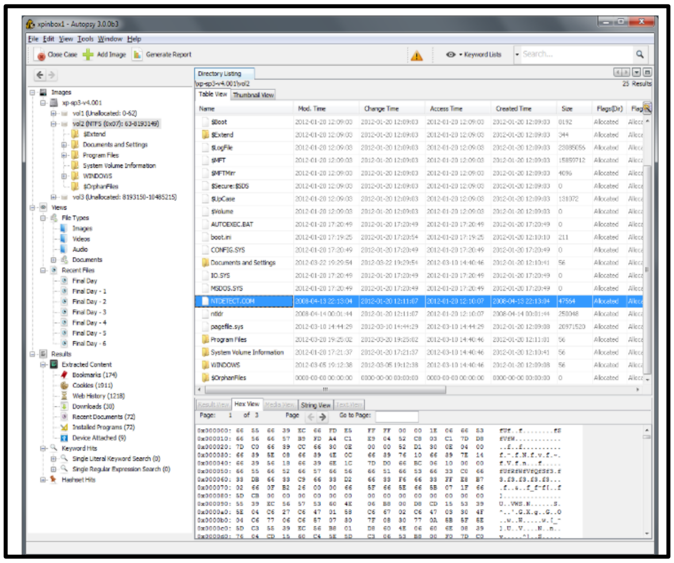
III. WEB BROWSER FORENSIC TOOLS

A. Autopsy Forensic Tool

Autopsy is an open source and digital forensic investigation tool which is use by law enforcement agencies, corporate examiners, military etc. Autopsy uses Sleuth Kit to analyze pictures. Sleuth kit empowers the examination of computerized media and the recovery of erased contents [8]. it is a powerful forensic tool capable of extracting web browser history, cookies from different type of browsers such as Google Chrome, Mozilla Firefox and Internet Explorer. It is fast, easy to use, cost effective and extensible such as time analysis, hash filtering, web artifact and keyword searching etc.

Features of Autopsy:

1. Many user cases: This allow more than one examiner on a huge case to work with a single tool at the same time.
2. Keyword Search: Enable an investigator to extract text and search index modules to find files that mention specific terms and find regular expression patterns
3. It allows an examiner to extract artifact from web browsers
4. Easy to install on windows
5. It supports internal and external hard drives and smartphones
6. It uses hash set filtering to filter out known good files and bad files using MD5sum and Hash keeper format
7. It recovers deleted file carving from unallocated space using PhotoRec
8. It uses multimedia to extract EXIF from pictures and videos
9. Timeline analysis: to show and identify an events activity in a graphical interface
10. It supports an extraction of data from Android such as SMS, contact, call logs and et cetera
11. It reviews the image galleries
12. It has a feature of extracting email messages



Name	Mod. Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flag
$Boot	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	8192	Allocated	Alloc
$Extend	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	344	Allocated	Alloc
$LogFile	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	23085056	Allocated	Alloc
$MFT	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	15859712	Allocated	Alloc
$MFTMirr	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	4096	Allocated	Alloc
$Secure:$SDS	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	0	Allocated	Alloc
$UpCase	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	131072	Allocated	Alloc
$Volume	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	0	Allocated	Alloc
AUTOEXEC.BAT	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Alloc
boot.ini	2012-01-20 17:19:25	2012-01-20 17:20:54	2012-01-20 17:19:25	2012-01-20 12:10:10	211	Allocated	Alloc
CONFIG.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Alloc
Documents and Settings	2012-03-22 19:29:54	2012-03-22 19:29:54	2012-03-10 14:40:46	2012-01-20 12:10:41	56	Allocated	Alloc
IO.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Alloc
MSDOS.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Alloc
NTDETECT.COM	2008-04-13 22:13:04	2012-01-20 12:11:07	2012-01-20 12:10:07	2008-04-13 22:13:04	47564	Allocated	Alloc
ntldr	2008-04-14 00:01:44	2012-01-20 12:11:07	2012-01-20 12:10:07	2008-04-14 00:01:44	250048	Allocated	Alloc
pagefile.sys	2012-03-10 14:44:29	2012-03-10 14:44:29	2012-03-10 14:44:29	2012-01-20 12:09:08	20971520	Allocated	Alloc
Program Files	2012-03-20 19:25:02	2012-03-20 19:25:02	2012-03-10 14:40:46	2012-01-20 12:11:01	56	Allocated	Alloc
System Volume Information	2012-01-20 17:21:37	2012-01-20 17:21:37	2012-03-10 14:40:46	2012-01-20 12:10:41	56	Allocated	Alloc
WINDOWS	2012-03-05 19:12:38	2012-03-05 19:12:38	2012-03-10 14:40:46	2012-01-20 12:09:08	56	Allocated	Alloc
$OrphanFiles	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Alloc

```
0x000000: 66  55  66  39  EC  66  FD  E5    FF  FF  00  00  1E  06  66  53    fUf..f.........fS
0x000010: 66  56  66  57  B9  FD  A4  C1    E9  04  52  C8  03  C1  7D  D8    fVfW.............
0x000020: 7D  C0  66  89  CC  66  30  0E    00  00  52  D1  30  0E  04  00    ..f..f...........
0x000030: 66  89  5E  08  66  89  4E  0C    66  89  76  10  66  89  7E  14    f.^.f.N.f.v.f.~.
0x000040: 66  39  56  18  66  39  6E  1C    7D  D0  66  BC  06  10  00  00    f.V.f.n...f.....
0x000050: 66  55  66  52  66  57  66  56    66  51  66  53  66  33  C0  66    fUfRfWfVfQfSf3.f
0x000060: 33  DB  66  33  C9  66  33  D2    66  33  F6  66  33  FF  E8  B7    3.f3.f3.f3.f3...
0x000070: 02  66  0F  B2  26  00  00  66    5F  66  5E  66  5B  07  1F  66    .f..&..f_f^f[..f
0x000080: 5D  CB  00  00  00  00  00  00    00  00  00  00  00  00  00  00    ]...............
0x000090: 55  39  EC  56  57  53  60  4E    06  B8  00  D8  CD  15  53  39    U..VWS.N......S.
0x0000a0: 5E  04  C6  27  C6  47  01  58    C6  67  02  C6  47  03  30  4F    ^..'.G.X.g..G..O
0x0000b0: 04  C6  77  06  C6  67  07  30    7F  08  30  77  0A  6B  5F  6E    ..w..N.....w.[_~
0x0000c0: 5D  C3  56  39  EC  56  B8  01    D8  60  4E  06  60  6E  08  39    ].U..V....N..n..
```

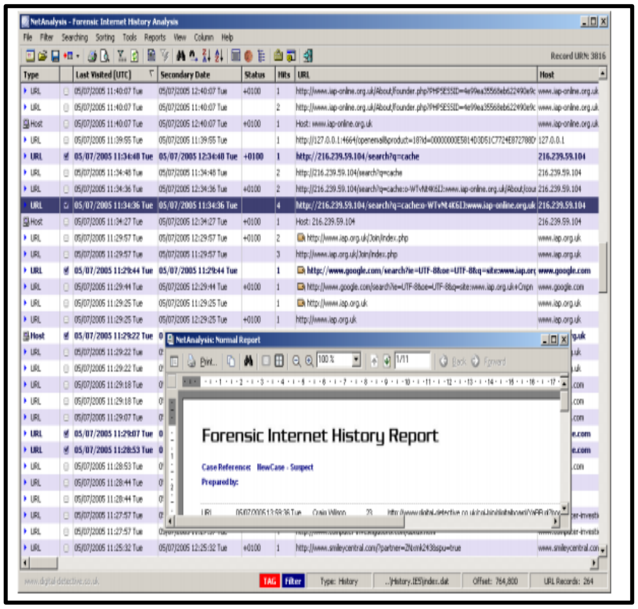
Fig. 2 Default view of an Autopsy [8]

B. Browser History Examiner (BHE)

Browser History Examiner is a digital forensic investigation tool developed by Foxton Forensics, it captures, analyses and report web history from web browsers, it supported Google Chrome, Mozilla Firefox, Edge and Internet Explorer. BHE also supports several digital forensic investigations such as employee activity reporting, human resources investigations an et cetera. It extracts and analyse different kind of data types like visited websites, cookies, cache files and downloaded items [9],[13].

Features of Web Browser Forensic Tool.

1. BHE recognizes internet activity using interactive website timeline
2. It uses an advanced filtering such as keywords and date/time range
3. It is capable of searching history on search engines.
4. It can view automatically extracted email addresses found on the web browsers.
5. It can filter malicious websites using URL category filter.
6. It can perform different kind of time conversion with time zone.
7. It can automatically collect and captures the history of a remote computers on a network
8. It has a feature to export data and report builder such as PDF, XLSX, CSV and et cetera.



Type		Last Visited (UTC)	Secondary Date	Status	Hits	URL	Host
URL	□	05/07/2005 11:40:07 Tue	05/07/2005 12:40:07 Tue	+0100	1	http://www.iap-online.org.uk/About/Founder.php?PHPSESSID=4e99ea35568eb622490e9c	www.iap-online.org.uk
URL	□	05/07/2005 11:40:07 Tue	05/07/2005 11:40:07 Tue		2	http://www.iap-online.org.uk/About/Founder.php?PHPSESSID=4e99ea35568eb622490e9c	www.iap-online.org.uk
Host	□	05/07/2005 11:40:07 Tue	05/07/2005 12:40:07 Tue	+0100	1	Host: www.iap-online.org.uk	www.iap-online.org.uk
URL	□	05/07/2005 11:39:55 Tue	05/07/2005 11:39:55 Tue		1	http://127.0.0.1:4664/openemail&product=18?id=00000000E5814D3D51C7724E8727880	127.0.0.1
URL	☑	05/07/2005 11:34:48 Tue	05/07/2005 12:34:48 Tue	+0100	1	http://216.239.59.104/search?q=cache	216.239.59.104
URL	□	05/07/2005 11:34:48 Tue	05/07/2005 11:34:48 Tue		2	http://216.239.59.104/search?q=cache	216.239.59.104
URL	□	05/07/2005 11:34:36 Tue	05/07/2005 12:34:36 Tue	+0100	2	http://216.239.59.104/search?q=cache:o-WTvNt4K6IJ:www.iap-online.org.uk/About/Fou	216.239.59.104
URL	☑	05/07/2005 11:34:36 Tue	05/07/2005 11:34:36 Tue		4	http://216.239.59.104/search?q=cache:o-WTvNt4K6IJ:www.iap-online.org.uk	216.239.59.104
Host	□	05/07/2005 11:34:27 Tue	05/07/2005 12:34:27 Tue	+0100	1	Host: 216.239.59.104	216.239.59.104
URL	□	05/07/2005 11:29:57 Tue	05/07/2005 12:29:57 Tue	+0100	2	http://www.iap.org.uk/Join/index.php	www.iap.org.uk
URL	□	05/07/2005 11:29:57 Tue	05/07/2005 11:29:57 Tue		3	http://www.iap.org.uk/Join/index.php	www.iap.org.uk
URL	☑	05/07/2005 11:29:44 Tue	05/07/2005 11:29:44 Tue		1	http://www.google.com/search?ie=UTF-8&oe=UTF-8&q=site:www.iap.org	www.google.com
URL	□	05/07/2005 11:29:44 Tue	05/07/2005 12:29:44 Tue	+0100	1	http://www.google.com/search?ie=UTF-8&oe=UTF-8&q=site:www.iap.org.uk+Crspn	www.google.com
URL	□	05/07/2005 11:29:25 Tue	05/07/2005 11:29:25 Tue		1	http://www.iap.org.uk	www.iap.org.uk
URL	□	05/07/2005 11:29:25 Tue	05/07/2005 12:29:25 Tue	+0100	1	http://www.iap.org.uk	www.iap.org.uk
Host	☑	05/07/2005 11:29:22 Tue					
URL	□	05/07/2005 11:29:22 Tue					
URL	□	05/07/2005 11:29:22 Tue					
URL	□	05/07/2005 11:29:18 Tue					
URL	□	05/07/2005 11:29:18 Tue					
URL	□	05/07/2005 11:29:07 Tue					
URL	☑	05/07/2005 11:29:07 Tue					
URL	☑	05/07/2005 11:28:53 Tue					
URL	□	05/07/2005 11:28:53 Tue					
URL	□	05/07/2005 11:28:44 Tue					
URL	□	05/07/2005 11:28:44 Tue					
URL	□	05/07/2005 11:27:57 Tue					
URL	□	05/07/2005 11:27:57 Tue					
URL	□	05/07/2005 11:25:32 Tue	05/07/2005 12:25:32 Tue	+0100	1	http://www.smileycentral.com/?partner=ZNxmk243&spu=true	www.smileycentral.com

Forensic Internet History Report

Case Reference: NewCase - Suspect

Prepared by:

Fig. 3 Default View of Web Browser History [9]

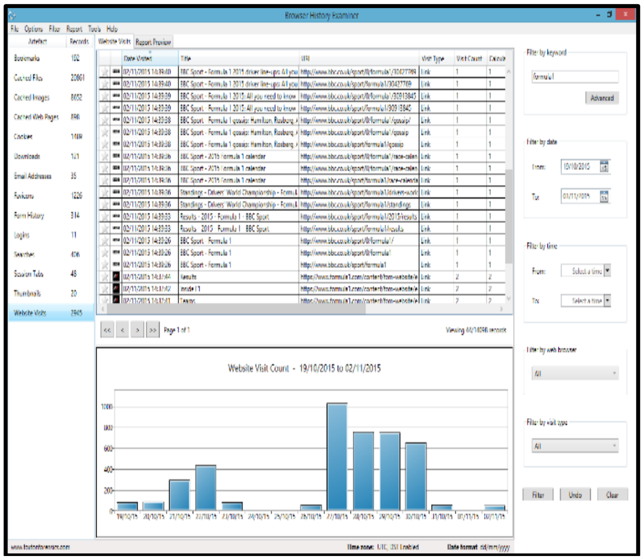
C. NetAnalysis Forensic Tool

Cases in digital forensic investigation differs significantly; some cases deal with identity theft by attempting to gain an access to someone users account details.Some cases involve hacking, cyberbullying, cyber-stalking, scamming, fraud and et cetera. Whatever cases happened, it is highly important for a digital forensic investigator to extract and examine evidence quickly and present it in an understandable format to read [10],[14]

NetAnalysis is a digital forensic investigation tool developed by Digital Detective Company, it was developed in order to help digital examiners to extract, analyse and present forensic evidence with regard to web browsers. It captures and collect all the activities of users on computer or internet browsers on mobile devices such as Mozilla Firefox, Google Chrome, Safari, Opera and internet Explorer. It also supports an investigator to examine cookies, browser history, cache and other components.

Features of NetAnalysis Forensic Tool

1. It has a wonderful feature to extract history of web browsers slack spaces especially on browsers like safari and internet explorer.
2. It can reconstruct and examine temporary cache files.
3. NetAnalysis tool have the ability to identify login credentials through search engines
4. It can recognize email addresses such as Yahoomail, Gmail, Hotmail and other email activities.
5. It has the ability to extract history from digital forensic images
6. It can analyse web browser history without restoring the suspect drive
7. It has powerful and multiple keyword searching which enable an examiner to import or export his keyword list.
8. NetAnalysis can be able to identify the user profile when visited any site.
9. It is fast in searching or filtering an information using the keyword within web pages.
10. It can search thousands of web pages or URL in a second.



Artefact	Records
Bookmarks	102
Cached Files	20861
Cached Images	8052
Cached Web Pages	898
Cookies	1409
Downloads	121
Email Addresses	35
Favicons	1226
Form History	314
Logins	11
Searches	406
Session Tabs	48
Thumbnails	20
Website Visits	2945

Date Visited	Title	URL	Visit Type	Visit Count	Calculat
02/11/2015 14:39:40	BBC Sport - Formula 1 2015 driver line-ups All you	http://www.bbc.co.uk/sport/0/formula1/30427769	Link	1	1
02/11/2015 14:39:40	BBC Sport - Formula 1 2015 driver line-ups All you	http://www.bbc.co.uk/sport/formula1/30427769	Link	1	1
02/11/2015 14:39:39	BBC Sport - Formula 1 2015: All you need to know	http://www.bbc.co.uk/sport/0/formula1/30913845	Link	1	1
02/11/2015 14:39:39	BBC Sport - Formula 1 2015: All you need to know	http://www.bbc.co.uk/sport/formula1/30913845	Link	1	1
02/11/2015 14:39:38	BBC Sport - Formula 1 gossip: Hamilton, Rosberg,	http://www.bbc.co.uk/sport/0/formula1/gossip/	Link	1	1
02/11/2015 14:39:38	BBC Sport - Formula 1 gossip: Hamilton, Rosberg,	http://www.bbc.co.uk/sport/0/formula1/gossip	Link	1	1
02/11/2015 14:39:38	BBC Sport - Formula 1 gossip: Hamilton, Rosberg,	http://www.bbc.co.uk/sport/formula1/gossip	Link	1	1
02/11/2015 14:39:36	BBC Sport - 2015 Formula 1 calendar	http://www.bbc.co.uk/sport/0/formula1/race-calen	Link	1	1
02/11/2015 14:39:36	BBC Sport - 2015 Formula 1 calendar	http://www.bbc.co.uk/sport/0/formula1/race-calen	Link	1	1
02/11/2015 14:39:36	BBC Sport - 2015 Formula 1 calendar	http://www.bbc.co.uk/sport/formula1/race-calenda	Link	1	1
02/11/2015 14:39:36	Standings - Drivers' World Championship - Formul	http://www.bbc.co.uk/sport/formula1/drivers-worl	Link	1	1
02/11/2015 14:39:36	Standings - Drivers' World Championship - Formul	http://www.bbc.co.uk/sport/formula1/standings	Link	1	1
02/11/2015 14:39:33	Results - 2015 - Formula 1 - BBC Sport	http://www.bbc.co.uk/sport/formula1/2015/results	Link	1	1
02/11/2015 14:39:33	Results - 2015 - Formula 1 - BBC Sport	http://www.bbc.co.uk/sport/0/formula1/results	Link	1	1
02/11/2015 14:39:26	BBC Sport - Formula 1	http://www.bbc.co.uk/sport/0/formula1/	Link	1	1
02/11/2015 14:39:26	BBC Sport - Formula 1	http://www.bbc.co.uk/sport/0/formula1	Link	1	1
02/11/2015 14:39:26	BBC Sport - Formula 1	http://www.bbc.co.uk/sport/formula1	Link	1	1
02/11/2015 14:37:44	Results	https://www.formula1.com/content/fom-website/e	Link	2	2
02/11/2015 14:37:42	Inside F1	https://www.formula1.com/content/fom-website/e	Link	2	2
02/11/2015 14:37:41	Teams	https://www.formula1.com/content/fom-website/e	Link	2	2

Fig. 3 Default view of NetAnalysis Forensic Tool [10]

IV. EVALUATION AND COMPARISON OF THE SELECTED WEB BROWSERS FORENSIC TOOLS

This section critically evaluates the features of the three selected forensic tools chosen in this survey paper, the tools are; Autopsy, Browser History Examiner (BHE) and NetAnalysis forensic tools. The section also makes comparison between the selected tools.

1) *Evaluation of the Web Browsers Forensic Tools*

Nowadays, the rapid development and availability of internet in almost everywhere around the world, people make financial transactions, taking classes on e-learning and so much more, criminals uses the opportunity to make their criminal activities by hacking username and password of some users, scamming, fraud, cyberbullying, cyberstalking and et cetera. With this regard, digital investigators play a vital role in tackling most of the cases. It is advisable for an investigator or forensic examiner to choose a highly recommended tools that can help them make their investigation smoothly. This survey paper selected three web browsers forensic tools and evaluate them in order to guide and help a digital examineror investigator to choose the best among them based on their comparison and potential features.

TABLE I

Evaluation of the Selected Forensic Tools Based on Their Features

S/No.	Features	Web Browser Forensic Tools		
		Autopsy	Browser History Examiner	NetAnalysis
1	Compatible with Mozilla Firefox, Google Chrome and Internet Explorer internet browsers	Yes	Yes	Yes
2	Gathering of log files	Yes	Yes	Yes
3	Extract web browser cache history	Yes	Yes	Yes
4	Multiple users on a single case	Yes	No	No
5	Extract artifact from web browsers	Yes	Yes	Yes
6	Export data in different format e.g. PDF, CSV	Yes	Yes	Yes
7	Timeline analysis	Yes	Yes	Yes
8	Password recovery	Yes	No	Yes
9	Recovery of deleted files	Yes	No	Yes
10.	Perform time zone conversion and selection	Yes	Yes	Yes
11	Bookmarking	Yes	Yes	Yes
12	Extract cookies	Yes	Yes	Yes
13	Download	Yes	Yes	Yes
14	Reviews image galleries	Yes	No	Yes
15	Extracting of email messages	Yes	No	Yes
16	Extraction of data from android smartphones	Yes	No	Yes
17	Search thousands of web pages or URL in a second	Yes	No	Yes
18	Support Keyword Search	Yes	Yes	Yes
29	Easy to install on windows	Yes	Yes	Yes
20	Hash set filtering	Yes	Yes	Yes

With regards to the above evaluation of the three selected forensic tools based on their features. Autopsy seems to be the best forensic tool that is suitable for web browser investigation. Therefore, I recommend Autopsyto be used amidst Browser History Examiner and NetAnalysis because of its robust features. This paper does not need any experiment because it is a survey paper and based on the survey on the selected web browsers, I noticed that Autopsy is the best forensic tool in terms of potability, fast data analysis, less memory and CPU consumption.

V. CONCLUSION

This survey paper focuses on web browsers forensic tools. A web browser is a computer program or application that is use to surf an internet. Nowadays, millions of people use an internet to search an information through web browsers, such information include checking emails, online transactions, downloading educational materials, social networking etc. [2].

Digital forensic usually investigates the collected data from storage media devices such as hard. The main goal of digital forensic investigation is to preserve any evidence found in its most original form and to make sure that the evidence is not tempered. Digital forensic investigators use log files to extract, analyse and present a report based on the criminal activities found on the web browsers, such log files include history, cache, download and cookies.

This survey paper evaluates the features of the three selected browsers forensic tools namely; Browser History Examiner, Autopsy and NetAnalysis and make comparative analysis between them. The findingsbased on the evaluation of the selected tools shows that Autopsy is the best forensic tool among.

REFERENCES

[1] M. R. Jadhav, B. B. Meshram, "Web Browser Forensics for Detecting User Activities*" International Research Journal of Engineering and Technology (IRJET),* Volume: 05 Issue: 07 | July 2018. Accessed on: Mar. 10, 2020. [Online]. Available on: www.irjet.net

[2] D. Rathod, "Web Browser Forensic: Google Chrome" International *Journal of Advanced Research in Computer Science,* Volume 8, No. 7, July – August 2017. Accessed on: Mar. 10, 2020. [Online]. Available DOI:http://dx.doi.org/10.26483/ijarcs.v8i7.4433

[3] Blaine Stephens, "*What is Digital Forensics?",* Feb, 5, 2016. Accessed on: March, 27, 2020. [Online]. Available on: https://interworks.com/blog/bstephens/2016/02/05/what-digital-forensics

[4] Kent, K. and Grance, T.*"Guide to Integrating Forensic Techniques into Incident Response",* 2006. Accessed on Feb, 29, 2020. [Online] Available: http://csrc.nist.gov/publications/nistpubs/800- 86/SP800-86.pdf,

[5] SwetaMahaju and Travis Atkison. "Evaluation of Firefox Browser Forensics Tools" In Proceedings of ACM SE '17, Kenne-saw, GA, USA, April 13-15, 2017, 8 pages. Accessed on: Mar. 10, 2020. [Online]. Available DOI: http://dx.doi.org/10.1145/3077286.3077310

[6] E. Akbal, Futma G. and Ayhan, "Digital Forensic Analyses of Web Browser Records" *Journal of Software,* Volume 11, Number 7, July 2016, Accessed on: Mar. 10, 2020. [Online]. Available DOI: 10.17706/jsw.11.7.631-637

[7] Amor. L, Thabet S. "Forensics Investigation of Web Application Security Attacks" *I.J. Computer Network and Information Security.* Feb, 2015 Accessed on: Mar. 10, 2020. [Online]. Available DOI: 10.5815/ijcnis.2015.03.02

[8] *"Basis Technology Corporation: Autopsy and The Sleuth",* Accessed on: Mar. 14, 2020. [Online] Available http://www.autopsy.com/wp-content/uploads/sites/8/2016/02/Autopsy-4.0-EN-optimized.pdf

[9] Andrew M., Ibrahim B., Talal A. Ali AK., "Portable Web Browser Forensics -A forensic examination of the privacy benefits of portable web browsers", *International Conference on Computer Systems and Industrial Informatics.* 18-20 Dec. 2012. Available DOI: 10.1109/ICCSII.2012.6454516

[10] Craig Wilson *"NetAnalysis and Forensic Internet investigations"* Forensic Internet history Analysis Software, Accessed on: Mar. 14, 2020. [Online] Available On:https://www.digital-detective.net/documents/NetAnalysis-v1.37-Manual.pdf

[11] *Hassan Adamu*,Mansur Alhaji Muhammad, and Sabo Muhammad (2016): Impact of Social Media on Today's Youth in Jigawa State; International Journal of Advanced Engineering and Management Research. Vol. 03 – Issues 04, June 2016. Page 272-279. www.ijaemr.com

[12] Junghoon Oh, Seungbong Lee and Sangjin Lee, "Advanced evidence collection and analysis of web browser activity" *The Digital Forensic Research Conference,* 2001 USA, , Accessed on: Mar. 17, 2020. [Online] Available On DOI:10.1016/j.diin.2011.05.008

[13] Mandeep Kaur1 ,Navreet Kaur2 , SumanKhurana, "A Literature Review on Cyber Forensic and its Analysis tools" *International Journal of Advanced Research in Computer and Communication Engineering* Vol. 5, Issue 1, January 2016, , Accessed on: Mar. 17, 2020. [Online] Available On:DOI 10.17148/IJARCCE.2016.5106 23

[14] E. Oriwoh and G. Williams, ''Internet of Things: The argument for smart forensics,'' in Proc. Handbook Res. Digit. Crime, Cyberspace Secur., Inf. Assurance, 2014, pp. 407–423.

[15] H. Parsonage. (Aug. 4, 2013). Computer Forensics Case Assessment and Triage—Some Ideas for Discussion. [Online]. Available: http://computerforensics.parsonage.co.uk/triage/triage.htm

[16] S. L. Garfinkel, ''Forensic feature extraction and cross-drive analysis,'' Digit. Invest., vol. 3, pp. 71–81, Sep. 2006.

[17] S. Garfinkel, ''Digital media triage with bulk data analysis and bulk_extractor,'' Comput. Secur., vol. 32, pp. 56–72, Feb. 2013.

[18] D. Quick and K.-K. R. Choo, ''Big forensic data management in heterogeneous distributed systems in smart cities: Quick analysis of multimedia forensic data,'' Softw., Pract. Exper., vol. 47, no. 8, pp. 1095–1109, 2016.

[19] D. Quick and K.-K. R. Choo, ''Pervasive social networking forensics: Intelligence and evidence from mobile device extracts,'' J. Netw. Comput. Appl., vol. 86, pp. 24–33, May 2017.

[20] S. Garfinkel, R. Farrell, V. Roussev, and G. Dinolt, Bringing science to digital forensics with standardized forensic corpora. DFRWS, Montreal, QC, Canada, 2009. Accessed: Sep. 9, 2013. [Online]. Available: http://digitalcorpora.org/corpora/disk-images

[21] ***Hassan Adamu,***Abdulkadir A. Shattimahand Musa Aliyu (2016): Role of Information and Communication Technology as a Means of Tackling Corruption in Nigeria; International Journal of Innovative Research and Creative Technology. Vol. 01 – Issues 05, March 2016 (ISSN 2454-5988), Page 478-480. www.ijirct.org

[22] ***Hassan Adamu,*** Musa Aliyu and Ayangbekun O.J. (2015): Impact of Modern Communication Media; International Journal of Innovative Research and Creative Technology. Vol. 01 – Issues 02, September 2015 (ISSN 2454-5988), Page 207-211. www.ijirct.org