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 for a 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 banking and 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 make a comparison 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, preserve and 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 business transactions, 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. Atkinson 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.

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 and 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.

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.

![Default view of NetAnalysis Forensic Tool](image)

**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 examiner or investigator to choose the best among them based on their comparison and potential features.

<table>
<thead>
<tr>
<th>S/No.</th>
<th>Features</th>
<th>Autopsy</th>
<th>Browser History Examiner</th>
<th>NetAnalysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Compatible with Mozilla Firefox, Google Chrome and Internet Explorer internet browsers</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>2</td>
<td>Gathering of log files</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>Extract web browser cache history</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>4</td>
<td>Multiple users on a single case</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>5</td>
<td>Extract artifact from web browsers</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6</td>
<td>Export data in different format e.g. PDF, CSV</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>7</td>
<td>Timeline analysis</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>8</td>
<td>Password recovery</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>9</td>
<td>Recovery of deleted files</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>10</td>
<td>Perform time zone conversion and selection</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>11</td>
<td>Bookmarking</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>12</td>
<td>Extract cookies</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>13</td>
<td>Download</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>14</td>
<td>Reviews image galleries</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>15</td>
<td>Extracting of email messages</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>16</td>
<td>Extraction of data from android smartphones</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>17</td>
<td>Search thousands of web pages or URL in a second</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>18</td>
<td>Support Keyword Search</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>19</td>
<td>Easy to install on windows</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>20</td>
<td>Hash set filtering</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
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 Autopsy to 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 used 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 forensic tools namely; Browser History Examiner, Autopsy and NetAnalysis and make comparative analysis between them. The findningsbased on the evaluation of the selected tools shows that Autopsy is the best forensic tool among.

REFERENCES


