Evaluation of Firefox Browser Forensics Tools

Sweta Mahaju
University of Alabama
P.O. Box 870290
Tuscaloosa, Alabama 35487
smahaju@crimson.ua.edu

Travis Atkison[*]
University of Alabama
P.O. Box 870290
Tuscaloosa, Alabama 35487
atkison@cs.ua.edu

ABSTRACT

Web browsers store web surfing data and history to facilitate the users ease of operation such as instant website recommendations or quicker access to previously visited sites. Since cyber-criminals or suspects, in general, may use the browser to search for any number of crime methods or visit different websites to collect information, this is a good source of electronic evidence used in lawsuits and other crime related investigations. For this reason, web browser forensics is an important field of Digital Forensics. It is crucial to know about the different web browsing analysis tools that are available and have a clear understanding of which tool would be more productive and suitable for which cases and situations. Therefore, this paper presents a survey of web browser forensics analysis tools for Firefox, as well as evaluates the performance of the tools and the system while the tool is being run. These tools are tested against different criteria such as time constraints, memory consumption, and availability. The evaluation result is varied with respect to different sets of criteria. Each of the tools in this survey had their own strengths and weaknesses. However, if one is to be chosen which could be suitable enough for all the jobs, then FoxAnalysis would be the choice.

KEYWORDS

Digital Forensics, Web Browsers, Survey

ACM Reference format:
Sweta Mahaju and Travis Atkison. 2017. Evaluation of Firefox Browser Forensics Tools. In *Proceedings of ACM SE '17, Kennesaw, GA, USA, April 13-15, 2017,* 8 pages.
DOI: http://dx.doi.org/10.1145/3077286.3077310

1 INTRODUCTION

Internet is used by almost every one today; around 3.5 billion, as of the most recent report according to Statista [16]. Among those billions of Internet users are a number of suspects who will use the Internet for any help or information to assist with their criminal activities. These could be activities they either intend to commit or have already committed in the past; whether it be web searching, visiting different websites or deleting browsing history of the web browser, accessing emails or online storage, or downloading files and so on. Therefore, considering web browsers for evidence searching could be a crucial part of a digital forensic investigation, as critical electronic evidence is usually found in a suspect's web browsing history in the form of above mentioned logs.

There are several numbers of web browsers that a user can use to access the Internet. Among them, Mozilla Firefox, Google Chrome, Internet Explorer, Safari and Opera are known as web browsing giants of today's age. Each of them has their own significance. However, this paper will focus on the Firefox web browser as it is OS independent, i.e., it is compatible to several operating systems like MAC, Windows, Linux, etc. [17]. Moreover, it is highly customizable with a simple layout and easier to use, which could be one of the reasons making it many users' first choice [17]. Web browsers save traces and logs, such as cache, history, cookies, login credentials, and a download list. Similarly, Firefox stores browsing logs in an SQLite database from which data can be extracted during an investigation. The Firefox browser and its log data files and formats are described in detail in the upcoming section.

Web browsing evidence recognition is one of the most significant parts of a digital forensic investigation [13]. However, a forensic investigation is not limited to collecting logs and evidence. After gathering evidence, the next step is the analysis phase in which the forensic investigators begin by reconstructing the web browsing events and activities. As the process is quite complicated, it calls for the need of different forensics analysis tools. There are several browser specific and browser independent analysis tools available. However, not every tool exhibits all the features that a particular investigation scenario may require. Hence evaluation of the analysis tools with respect to the set of features they provide would be beneficial, especially for forensics investigation. Therefore, this paper includes a section which evaluates different web browser forensic tools for the Firefox browser on the basis of different features they provided which may be helpful during forensics investigations.

Additionally, performance of a tool is one of the key factors to be considered. Speed, ease of use, availability, memory utilization and CPU consumption, etc., are some of the performance matrices on the basis of which the tools could be tested against, so that forensic investigation could get a

[*] Corresponding author.

ACM SE '17, April 13-15, 2017, Kennesaw, GA, USA
© 2017 ACM. ISBN 978-1-4503-5024-2/17/04...$15.00
DOI: http://dx.doi.org/10.1145/3077286.3077310

performance-wise better tool among all the available tools exhibiting the common feature sets. Considering the same logic, this paper also focuses on benchmarking the tools as well as the system on which the tools are to be run, on the basis of mentioned performance matrices to compare the results among themselves and find out the best tool of the chosen set.

This paper contains five sections. Section II discusses the different early works that were related to the work proposed in this paper. Section III describes the Firefox web browser and the log files it stores. Section IV presents the different web browser forensics tools. Section V provides an evaluation of web browser forensics tools with subsections that categorizes the evaluation into feature set evaluation and performance evaluation of the tools. Section VI discusses the accuracy of the idea the paper presents along with the comparison of the tools on the basis of the evaluation result. Finally, section VII summarizes the concept of evaluation of web browser analysis tools and conclude with its importance on the field of digital forensics investigation.

2 RELATED WORKS

In [7], Lowman focuses on the topic of web history visualization and compares the work of a visual web browser tool, 'Webscavator,' with that of one of the non-visual web browser tool, 'NetAnalysis'. The paper shows the evaluation of the visual browser forensic tool and explains the importance of data visualization in the field of digital forensics by comparing its features set with those of a non-visual browser forensic tools. Haggerty and Taylor [4] focus on web log analysis in which the author proposes a methodology for data visualization of search strings in web browser log files, so as to summarize a suspect's interest, intentions and actions over a period of time.

In [12], Pereira points out the change in the structure of web history log when the web browser Firefox shifted from version 2 to version 3, explaining the new structure. Furthermore, the author proposes the methodologies to recover the deleted history files from the SQLite databases explaining that the traces of deleted records could be found in the unallocated spaces.

In [1], Akbal et al. presents a nice methodology for the forensic analysis to be carried out on the digital resources related to the suspect's web browser data. The data could be of any of the different web browsers and on any of the different operating system. With regards to the same, the author includes a section that introduces some of the web forensics tools and describes their features in brief.

In [11], Oh et al. proposes a new methodology for web browser log file analysis and evidence gathering. The paper explains in detail a few of the important functionalities that a web browser forensics tool should have; introduces a new tool, WEFA (Web Browser Forensic Analyzer), which exhibits functionalities of advance evidence collection and integrated analysis; and finally, performs functional comparison of the same tool with existing tools.

Most of the above mentioned research works are focused on web log file structures and analysis. Some of them include comparisons of different web browser forensics tools. However, those papers show the limitations of the tools or introduce a new tool and compare and contrast the features of those existing tools with respect to extra features the new tools provides. Furthermore, almost all of the related research mentioned above are out of date as their discussions focus either on older tool versions or are superfluous in analysis of appropriate tools for Firefox log files. With the demand of upgrading technologies, the research needs to be updated to include the newer version of the tools that may provide more features.

Hence, this paper focuses on the web browser forensics tools and different features they provide for browser forensic data analysis; evaluation of the tools based on those features as well as different performance matrices; simultaneously comparing the results in a motive to help the forensic investigators to find out the best suited tool for a given forensic case.

3 FIREFOX WEB BROWSER AND LOG FILES

Firefox is one of the predominant web browsers today. It supports web standards such as HTML, XHTML, CSS, DOMs, XML and plugins such as Java, Flash, Acrobat Reader as well as millions of non-standard web pages that can be found in the Internet today [3].

Firefox uses an SQLite database to record browser information and log files. It stores everything in separate SQLite files. There are a total of 12 SQLite files maintained corresponding to the different functions like cookies, web searches, website visited, etc. These SQLite files contain various tables to store user profile data. The data is stored in a protective way so that it is still saved in the tables even after deletion by user. From a forensic point of view, these SQLite files are considered helpful to extract the digital evidence. Table 1 describes the different SQLite log files used by Firefox to store the web browsing information and their importance [2].

4 WEB BROWSER FORENSICS TOOLS

The forensic analysis phase is an important phase of a digital forensic investigation as the forensic investigator reaches a result based on the analysis done on the collected evidence. For a web browser investigation, the process begins with event reconstruction of the web browsing history. However, there are several tools available now that could considerably accommodate contouring the procedure [5].

Web browser forensics tools, among different computer forensic tools, are those which are specifically related to Internet browsing activities of the suspect's system. Different web browsing analysis tools are browser specific. However, there are some that may be compatible with more than one browser. As this paper is concerned with the Firefox web browser, below are some of the top web browsing history analysis tools which support Firefox log files format as input mentioned and described briefly below:

Table 1: Firefox log Files

S. No.	Firefox Log Files	Description
1	content-prefs.sqlite	This file is used to set user specific preferences for browser and content setting that persist throughout the user browsing session along with browsing history. content-prefs.sqlite contains 3 tables - namely groups, prefs, and settings which give the information about preferably visited sites during forensic investigation [2]
2	extensions.sqlite	This file contains seven different tables which are used to store information about different extensions installed in Firefox browser. Among these tables, 'addon' could be considered as an important one according to Forensics point of view as it stores information like "descriptor", "installDate", and "sourceURL" [2]
3	places.sqlite	This file is probably one of the most significant files in Firefox forensics. It maintains the records of all the Firefox bookmarks and lists of all the files downloaded and websites visited; and all the related information are considerably important for forensic investigation to pursue the suspect [6]
4	addons.sqlite	This file contains the table that stores all the information related to browser add-ons - such as name of add-on, version number, description, developer notes, support URL, creator and creator's URL, homepage URL and total number of downloads. Therefore, a forensic investigator can use this file to retrieve the details of all the installed add-ons while analyzing the browsing activities of the suspect [2]
5	cookies.sqlite	Firefox uses a table named "moz_cookies" to store all the information related to the browser cookies. Not all the cookies are relevant to forensic analysis, as cookies are generated for two purposes - one to create a user profile and other for advertisement purposes. Hence, the columns like baseDomain, host, lastAccessed, and creationTime are the important ones from a forensic point of view which can be used to extract the relevant information [2]
6	formhistory.sqlite	This file contains a table named "moz_formhistory" which stores all the data used for filling web forms. Additionally, the data related to web searching using search bar as well as the search keywords used for the same are also stored in the table. The important columns are "value", "fieldname", "firstUsed" and "lastUsed". The search keywords are stored in "fieldname" and data related to search and other forms data are stored in "value" column whereas the other two columns give the information about the time related to the records [2]
7	search.sqlite	The search.sqlite file stores the lists of all the available search engines such as - google, bing, yahoo, wikipedia, etc., that can be used by Firefox browser [2]
8	signons.sqlite	When the user logs in to any website, their user credentials (username and password) are stored in this file in encrypted forms under the columns "encryptedUsername" and "encryptedPassword". Along with these, there is also the information related to timestamps such as - created time, last used time, password last changed time. Site visit count is also stored as data under "timeUsed" column. Hence, this file is one of the important files for investigators to retrieve information which could be decisive and pivotal during evidence searching [2]
9	permissions.sqlite	This file consists of a table named "moz_hosts" whose column "host" stores the name of the sites for which permission such as allow pop ups, allow adobe flash, etc., are set [2]
10	downloads.sqlite	This file consists of the table named "moz_downloads" which saves all the information about past downloads such as files downloaded, destination, sources, time, etc., which can be crucial to forensic investigation [2]
11	webappstore.sqlite	The information about software methodology and protocols used in a web browser is stored in this file. Along with these, the table in the file also contains information about the web storage types. Moreover, even after the user deletes the browser history, cookies, or other browsing information, the data still remains in the table [2]
12	chromeappsstore.sqlite	This file stores the information related to a search engine in the table named "webappstore2" [2]

4.1 NetAnalysis V2

NetAnalysis v2 is a web browser forensic application which allows the user to retrieve the logged web browsing history and perform forensic analysis on it. Digital Detective Group Ltd introduced this application along with HstEx v4 which is an advanced data recovery solution designed to recover deleted browser history and other browsing data. The NetAnalysis tool provides the features of web browser forensics, filtering and searching, cache export and page rebuilding, and reporting, all of which are meant to be useful for digital forensic analysis and investigation [8].

4.2 FoxAnalysis V1.6.0

FoxAnalysis is a web browser forensics tool developed by Foxton Software Limited that helps with retrieving recorded bookmarks, cookies, downloads, form histories, web histories, logins, saved sessions, and website visits within the Firefox browser. All of these are equally important data for the forensics investigations. Some of the features it provides are web history timeline and analysis, filtering, create and open case files, exporting and reporting, etc. [10].

4.3 PasswordFox

PasswordFox gives the investigators the privilege of retrieving the login credentials saved by the Firefox browser. The program is developed by Nir Sofer, which introduced it as a portable program. It does not need to be installed and can also be transported via portable devices. PasswordFox retrieves the records related to the current user profile by default. However, any location can be given which selects any other Firefox user profile. The application allows you to extract the information specifically related to the website, user name, password, user name field, password field, sign-on file, HTTP realm, password strength and Firefox version. Another feature of the application is that the list of the records can be exported to a TXT, HTML, XML or KeePass CSV file [15].

4.4 Browser History Examiner

Browser History Examiner is also one of the products of Foxton Software Limited. It is a browser forensic tool used for capturing, extracting and analyzing the web browsing history data of the Firefox web browser. It stores logs of bookmarks, cached data, cookies, downloads, favicons, form history, web searches, website visits, login credentials, etc., which are almost all the type of data relevant for web browser forensics investigation. [9].

4.5 MZ History Viewer

MZ History Viewer is a simple web browser forensic tool to view the browsing history of the Firefox browser. It provides the user with several simple features. These features include displaying the browsing history in a grid view with columns for First Visit time, Last visit time, Visit Count, Url, Visit Length, etc., searching the history, properties window, navigating to the displayed history urls, and reporting, etc.

This is the common information necessary for a forensics investigation. [14].

5 EVALUATION OF WEB BROWSER FORENSICS TOOLS

The importance of forensics tools call forth the need to assure that the tools are well tested against their features and performance level. The paper provides an evaluation of the tools listed above based on the features they provide and performance matrices which will show at what level processing of the tools may affect the machine on which they are run.

5.1 Evaluation based on Feature Sets

There may be various scenarios and cases the forensics investigators need to work on which call for the use of web browser forensics tools. Having the knowledge about what tools are suitable for which case and what relevant features the tool provides might play a crucial role on minimizing the workload of the investigator. Therefore, this paper lists out a set of most important features a tool should have as the evaluation matrix and summarizes the availabilities of the same in the five tools mentioned in Section IV in a tabular format, see Table 2.

Table 2: Feature Set Evaluation

S. No.	Features	NetAnalysis	PasswordFox	MZ History Viewer	Browser History Examiner	FoxAnalysis
1	Websites Visits	Y	Y	Y	Y	Y
2	Form History	Y	Y	Y	Y	Y
3	Visit Count	Y	N	Y	Y	Y
4	First Accessed Time	Y	Y	Y	Y	Y
5	Last Accessed Time	Y	Y	Y	Y	Y
6	Firefox Version	Y	Y	N	N	N
7	Parent Page	N (Not in Evaluation Version)	N	Y	Y	N
8	Bookmarks	Y	N	N	Y	Y
9	Cookies	Y	N	N	Y	Y
10	Downloads	Y	N	Y	Y	Y
11	Logins	Y	Y	N	Y	Y
12	Session	N	N	N	Y	Y
13	Favicon	Y	N	N	Y	Y
14	Filtering	Y	N	Y	Y	Y
15	Search by Keyword	Y	Y	Y	Y	Y
16	Sorting	Y	Y	Y	Y	Y
17	Select Column to Display	Y	Y	Y	N	N
18	Time Zone Selection	Y	N	N	Y	Y
19	Preview	Y	N	N	Y	N (Not in Trial Version)
20	Classification of browsing activities	N	N	N	Y	Y
21	Deleted Information Recovery	Y	Y	N	N	N
22	Timeline Generation	N	N	N	Y	Y
23	Web page reconstruction	N	N	N	N	N (Not in Trial Version)
24	Open selected link in web browser	Y	N	Y	N	N
25	Password Recovery	N	Y	N	N	N
26	Exporting	Y	N	N	Y	Y
27	Reporting	Y	Y	Y	Y	N (Not in Trial Version)

With reference to Table 2, the participated tools can be compared with respect to the features they provide which will help the investigators to select the best suited tool for their case. It can be seen that all of the five browser tools provide the most necessary and basic features that are crucial for browser forensics; however, some of the tools exhibit more features than the others.

With web browser history analysis, the basic information that is considered relevant and important would be 'Websites Visits', 'Form History', 'Visit Count', 'First Accessed Time', 'Last Accessed Time', 'Bookmarks', 'Cookies', 'Downloads', 'Logins', 'Keywords Used' and 'Reporting'. Advanced feature would comprise of 'Content Preview', 'Time-line Generation', 'Web Page Reconstruction' while 'Password Recovery' would be specific features. Other features such as 'Sorting', 'Filtering', 'Column to Display', 'link to the history url', 'Exporting' could be categorized as features based on ease of use.

According to the feature evaluation result from the table above, we see that:

1. Almost all the tools exhibit the basic features to provide user browsing history information.
2. Advanced functionalities are lacking on almost all of the tools; however, the paid version of Fox Analysis, Browser History Examiner and NetAnalysis provide some of these or other features.
3. As PasswordFox is a specific password recovery tool, it lacks most of the features mentioned above. However, it is a worthy tool to use when the case calls for recovering the saved password of any login page. Furthermore, along with the password recovery feature, it provides the user with basic forensic information about the user login page, making the case easier to an extent.
4. MZ History Viewer, which is a small tool with a simple interface, provides the least features from which basic information about the web browsing history could be extracted.
5. NetAnalysis, Browser Examiner and Fox Analysis exhibit almost all the features listed in the table. However, due to the availability of only a trial version of tools for the evaluation purpose, many functionalities they provide could not be tested in this project.

5.2 Evaluation Based on Performance Matrices

In addition to knowledge of different features that the tools provide, it is essential that a forensic investigator know how well the tools, and the system on which the tools are to be run as a whole, work when tested against some of the performance constraints. Performance evaluation will decide if the system will be satisfactorily stable and function without any measure impact due to the processing of the tools.

The configuration of the system on which the performance evaluation was done is described below:

Windows Edition:

Windows 8.1

System:

Processor: Intel(R) Core(TM) i5-4200U CPU @ 1.60GHz 2.30 GHz

Installed Memory (RAM): 12.0 GB (11.8 GB Usable)

System Type: 64-bit Operating System, x64-based processor

To benchmark the system, the built-in application 'Task Manager' has been used to record the memory utilization and CPU consumption measurement for all of the five candidate tools against a dataset of 108 MB. Other criteria are set considering human to machine interaction.

Below performance matrices are used to evaluate the tools in system processing as well as a user's friendliness point of view.

5.2.1 Memory Utilization. According to the evaluation done, the following results could be drawn out for the five web browser forensic tools:

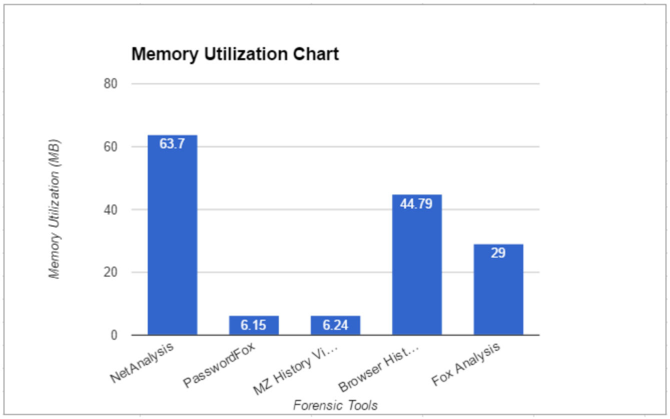


Figure 1: Performance Evaluation: Memory Utilization

We can see in Figure 1 that Netanalysis utilizes the largest memory among all the tested tools, i.e., 63.7 MB. Next is Browser History Examiner with 44.79 MB. FoxAnalysis utilizes 29 MB whereas the remaining other two tools consume around 6 MB of the system memory. Analyzing the data, it seems that the tools with more features consume more memory than the simple tools such as MZ History Viewer and PasswordFox. However, forensics investigation requires further criteria to be considered including the feature set, rather than only memory consumption. Hence, relatively logical decision needs to be made to choose a better tool.

5.2.2 CPU Consumption. CPU consumption could be another matrix that needs to be considered when benchmarking the tools as it could be one of the reasons that might make the system processing slow. Slow processing is not a good thing considering the need for urgency during an investigation.

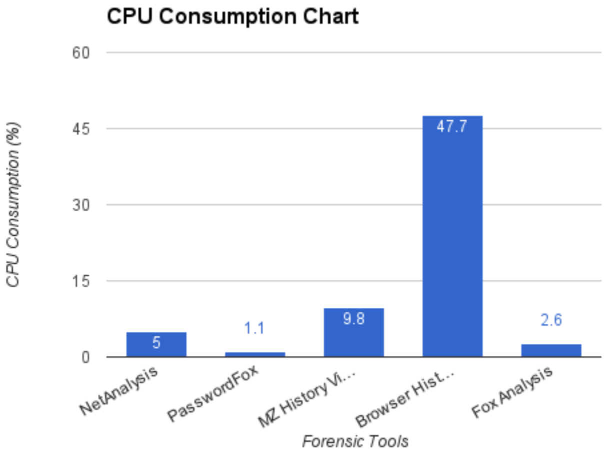


Figure 2: Performance Evaluation: CPU Consumption

Figure 2 provides results of evaluating the tools against the CPU consumption constraint:

Figure 2 shows that Browser History Examiner consumes the greatest percentage of CPU among the five tools, i.e., maximum of 47.7%. Analyzing the overall result, NetAnalysis and FoxAnalysis could be considered as better tools considering low CPU consumption and more of the features privileges.

5.2.3 Speed of processing. Some cases in forensic investigation need urgent analysis of the information. Hence, the speed of the tools matter for those cases. The five browser forensics tools were tested against the time constraint and evaluated based on speed of their processing. The following bar chart (Figure 3) shows the results based on processing speed:

From the evaluation result, it has been found that PasswordFox and MZ History Viewer do their job faster than the other three tools. It is understandable because PasswordFox is only concerned about the password recovery process and retrieves basic browsing information of those login pages. MZ History Viewer is also the same as PasswordFox in retrieving only basic web browsing activities of the users. NetAnalysis shows the longest processing time of all. Browser History Examiner has around the same time as NetAnalysis. And FoxAnalysis shows has around an average of all the processing times. Browser History Examiner and FoxAnalysis could be taken as considerably better tools if tested on the basis of time constraint that have good features set.

5.2.4 Availability. This matrix considers if the tools are easily available to the user or must be paid for. Rating values are Free-ware or Paid. PasswordFox and MZ History Viewer, both produced by NirSofer, are completely free-ware. On the other hand, FoxAnalysis and Browser History Examiner,

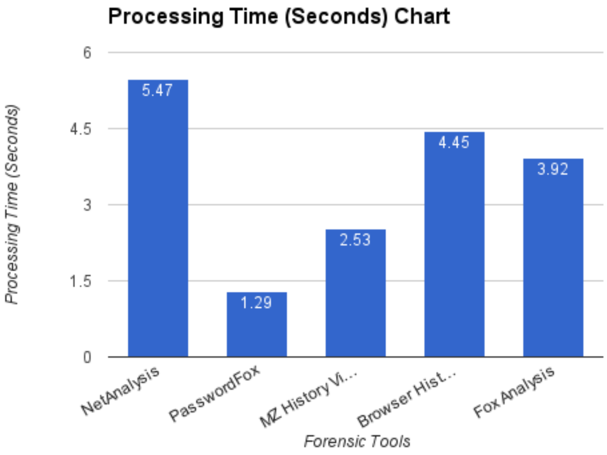


Figure 3: Performance Evaluation: Speed of Processing

both produced by Foxton Software Ltd., are paid products. However, trial packages could be found in the Internet. These trial versions limited how long they could be used. They also allowed the user access to only a limited number of available features and limited the number of records that could be fetched from the web history to 25 records. In order to access all available product features, FoxAnalysis and Browser History Examinermust be paid for. NetAnalysis is another paid software that belongs to Digital Detective Group Ltd. An evaluation package could be downloaded on request.

5.2.5 Ease of use. Finally, 'Ease of Use' of the tools for the users is one of the important criteria that needs to be taken into consideration while evaluating the tools. There are many functionalities such as classification of feature set, user friendly layout, preview function, etc, that determine ease of use. In the tools like FoxAnalysis and Browser History Viewer, different categories of user browsing activities like website visits, bookmarks, cookies, form histories, etc., are classified into tabs or a left sub menu bar which makes it easier for the users to view the desired category of browsing information. On the other hand, NetAnalysis does not provide this type of ease in the user interface. All the browsing information is displayed in the single grid. However, users have been provided with filter functionality in the each of the grid columns. MZ History View and PasswordFox are very easy to use because of their limited features. Both of them shows a grid of browsing history information and a property window for more details for each of the information.

With respect to user friendliness of the interface, Browser history Examiner was the easier tool to use, as everything would be visible in the same layout. The left navigation bar contains all the categories of the user browser activities while the right side of the screen shows the filter functionalities. The resulting information is displayed in the center. FoxAnalysis could also be considered user friendly as it also provides different categories of user activities. Plus, it shows a time-line of those activities in the website visits screen. The filter menu is easily detectable in the menu-bar. These tools are rated on the scale of 0 to 10 for this performance matrix. For ease of use, NetAnalysis gets 6 out of 10; PasswordFox and MZ History Viewer both get 9 out of 10 because of their easy interface; and Browser History Examiner and FoxAnalysis are both rated as 7 out of 10 considering the user-friendly interface together with a better set of features.

Table 3 sums up the evaluation results:

Table 3: Performance Evaluation

S. No.	Performance Matrices	NetAnalysis	PasswordFox	MZ History Viewer	Browser History Examiner	FoxAnalysis
1	Memory Utilization (MB)	63.7	6.15	6.24	44.79	29
2	CPU Consumption (Max. Percent)	5	1.1	9.8	47.7	2.6
3	Speed of Processing (Secs)	5.47	1.29	2.53	4.45	3.92
4	Availability	Paid	Freeware	Freeware	Paid	Paid
5	Ease of Use (Out of 10)	6	9	9	7	7

Considering both the evaluations and analyzing the result, it can be summarized that NetAnalysis and FoxAnalysis could be considered as the contenders, as both of them provide the users with more features helping in better and easier investigation and both of them performs considerably better based on performance criteria. PasswordFox could be considered when it is specifically a call for a password recovery job. However, though it performs well in performance evaluation case, it provides less features for investigation purpose. Similarly, MZ History Viewer should be used only for the cases when basic information retrieval is enough as it will perform faster and easily than other tools. Finally, Browser History Examiner is the last pick in this evaluation as we can see that even though it provides better features for investigation, it shows the largest CPU consumption (even for a dataset of merely 108 MB). Hence, it is ranked in the lower place in this evaluation.

6 ACCURACY AND COMPARISON OF THE BROWSER FORENSIC TOOLS

6.1 Accuracy

The evaluation has been performed on a personal dataset of 108 MB and the accuracy of the data retrieval could be done by comparing the browsing history in the Browser History Library with that of the tools. Check these attributes:

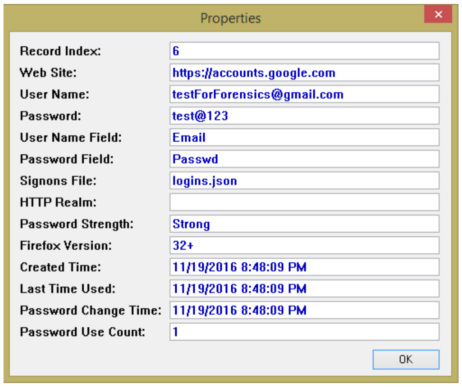
6.1.1 Website Visits. From Firefox browser history window, the browsing history related to the website visits could be used to compare and verify those retrieved by the tools. All of the tools show the browsing history. However, as Browser History Examiner and FoxAnalysis were trial version packages, they retrieved only 25 of the total records on the display.

Table 4: Forensic Tools Comparison Chart

Attributes	NetAnalysis	PasswordFox	MZ History Viewer	Browser History Examiner	FoxAnalysis	Guidelines and Suggestion
Portability and Simplicity	Not portable and complex	Portable and simple	Portable and Simple	Not portable and Complex	Not portable and Complex	Nir Sofer introduces the products like PasswordFox and MZ History Viewer keeping in mind the simplicity of the interface and portability of the products. They would be the best tool to use if these attributes are considered to be important.
Speed	Slow	Fast	Fast	Fast	Considerably Fast	The scenario when the forensic investigators have to deal with a large dataset could be troublesome to get the result in a short period of time. Speed of the tool is obviously desirable. Hence, FoxAnalysis would be the best tool which processes the data in comparatively faster time than other tools relatively similar in other attributes.
Classification of user Activities	Not Classified	Not Classified	Not Classified	Classified	Classified	FoxAnalysis would be the best tool to use which provides the user with an easy access to the desired category of the user activities in their browsing history. This would help the investigators to get the relevantly smaller list of the user browsing information making the investigation relatively faster and easier.
Memory and CPU Consumption	High	Low	Low	Very High	Considerably low	Browser History Examiner is not preferable considering the highest memory and CPU exploitation in average. PasswordFox and MZ History Viewer with low CPU and memory consumption are preferred for basic history retrieval job. NetAnalysis is a good tool with a variety of feature set and low CPU consumption. However, FoxAnalysis would be best preferred considering comparatively lower average CPU and memory consumption and having a similar set of features.

NetAnalysis and MZ History Viewer retrieve all the history records whereas PasswordFox does not retrieve the website visit record unless it is related to logins.

6.1.2 Bookmarks. We can view the user created bookmarks in the browser's bookmark toolbar. In more detail, they can be viewed in the browser history library window where the screen provides a tab for the bookmark section. The information retrieved by the tools that are related to the bookmarks could be verified from here. As a result, it has been known that the tools FoxAnalysis and Browser History Examiner fetch all the bookmark data correctly whereas PasswordFox and MZ History Viewer do not exhibit the feature to retrieve the bookmarks of a user profile. NetAnalysis on the other hand consists of a column Bookmark in its grid view. However, the evaluation version does not retrieve the information related to the bookmarks.



Record Index: 6
Web Site: https://accounts.google.com
User Name: testForForensics@gmail.com
Password: test@123
User Name Field: Email
Password Field: Passwd
Signons File: logins.json
HTTP Realm:
Password Strength: Strong
Firefox Version: 32+
Created Time: 11/19/2016 8:48:09 PM
Last Time Used: 11/19/2016 8:48:09 PM
Password Change Time: 11/19/2016 8:48:09 PM
Password Use Count: 1

Figure 4: PasswordFox: Properties Window

6.1.3 Password Recovery. The personal Firefox user profile contains login information, one of which is a test Gmail account. The evaluation result shows that PasswordFox retrieves the saved password in a decrypted form along with the other relevant information such as 'Created Time', 'Last Time Used', 'Password Change Time', etc., as shown in Figure 4.

NetAnalysis gives the login information for the login page. However, the password is displayed in encrypted form in the evaluation version. FoxAnalysis and Browser History Examiner gives all other information related to the login page. But the password recovery feature does not exist on them. MZ History viewer does not have the feature either.

6.1.4 Downloads. Firefox browser history window gives the information about the list of downloads which could be used to verify the data retrieval using the tools that are related to download history. We see that NetAnalysis accurately retrieves the information related to the user download history. Browser History Examiner does not retrieve this information in the trial version while FoxAnalysis trial version shows 25 records of the download history. MZ History Viewer shows the download information in the grid with Visit type value 'Downloads'. On the other hand, PasswordFox does not exhibit the feature to retrieve download history.

6.2 Comparison Chart

Based on both the feature evaluation as well as performance evaluation, the tools could be compared on the basis on following attributes described in Table 4.

7 CONCLUSION

Web browser forensics is an important part of digital forensics. It is extremely important as the Internet has become an avenue for criminals to commit or cover up their crimes, and web browsers are the gateway for humans to interact with the Internet. Crucial evidence can be collected while investigating the suspect's web browsers. Mozilla Firefox is one of the most popular web browsers currently available, and can be considered as an important source of information.

To analyze the web browsing history related information, different forensics tools are available. Some tools give the functionality of web browsing activities analysis as an extra feature whereas some tools are especially developed for those jobs. As different tools provide different or same sets of features presented in different ways, it is essential for an investigator to know which tool could be most suited for a particular case. Moreover, knowing the impact of the tools in the system they are run on is also equally important. Hence, the paper presents the evaluation of five of the web browser forensic tools based on the features they provide. It also examines how well they work on the system on which they are running. Various performance matrices were used when evaluating the 5 tools.

The evaluation result is varied with respect to different sets of criteria. However, if one is to be chosen which could be suitable enough for all the jobs, then FoxAnalysis would be the choice. Though the evaluation is done in the trial version, the complete package gives the user the privilege of retrieving all the basic and important information, generating a time-line of the user browsing activities, reconstructing the web pages, plus the availability of a simple and user friendly interface as well as being performance-wise considerably better.

REFERENCES

[1] Erhan Akbal, Fatma Günes, and Ayhan Akbal. 2016. Digital Forensic Analyses of Web Browser Records. *JSW* 11, 7 (2016), 631–637.

[2] Acquire Forensics. 2016. *Mozilla Firefox Forensics Usage of Sqlite File in Investigation.* http://www.acquireforensics.com/services/tech/mozilla-firefox.html.

[3] Ann Fry. 2011. *A Forensic web Log Analysis Tool: Techniques and implementation.* Ph.D. Dissertation. Concordia University Montréal, Québec, Canada.

[4] J Haggerty and MJ Taylor. 2014. Retrieval and Analysis of Web Search Narratives for Digital Investigations. In *Proceedings of the Tenth International Network Conference (INC 2014).* Lulu. com, 153.

[5] K. Jones and R. Belani. 2005. *Web Browser Forensics, Part 1.* http://www.symantec.com/connect/articles/web-browser-forensics-part-1.

[6] D. Koepi. 2010. *Firefox Forensics.* https://davidkoepi.wordpress.com/2010/11/27/firefoxforensics/.

[7] Sarah Lowman and Ian Ferguson. 2010. Web history visualisation for forensic investigations. *Msc Forensic Informatics Dissertation, Department of Computer and Information Sciences, University of Strathclyde* (2010).

[8] Digital Detective Group Ltd. 2016. NetAnalysis. (2016). http://www.digital-detective.net/digital-forensic-software/netanalysis/.

[9] Foxton Software Ltd. 2011. Browser History Examiner. (2011). https://www.foxtonforensics.com.

[10] Foxton Software Ltd. 2011. FoxAnalysis. (2011). https://www.foxtonforensics.com.

[11] Junghoon Oh, Seungbong Lee, and Sangjin Lee. 2011. Advanced evidence collection and analysis of web browser activity. *digital investigation* 8 (2011), S62–S70.

[12] Murilo Tito Pereira. 2009. Forensic analysis of the Firefox 3 Internet history and recovery of deleted SQLite records. *Digital Investigation* 5, 3 (2009), 93–103.

[13] Marcus K Rogers, James Goldman, Rick Mislan, Timothy Wedge, and Steve Debrota. 2006. Computer forensics field triage process model. In *Proceedings of the conference on Digital Forensics, Security and Law.* Association of Digital Forensics, Security and Law, 27.

[14] Nir Sofer. 2015. Mozilla History Viewer. (2015). http://www.nirsoft.net/.

[15] Nir Sofer. 2016. Password Fox. (2016). http://www.nirsoft.net/.

[16] Statista. 2016. *Number of internet users worldwide from 2005 to 2016.* https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/.

[17] B. Widder. 2016. *Battle of the browsers: Edge vs. Chrome vs. Firefox vs. Safari vs. Opera vs. IE vs. Vivaldi.* http://www.digitaltrends.com/computing/best-browser-internet-explorer-vs-chrome-vs-firefox-vs-safari-vs-edge/.