Digital Forensic Analyses of Web Browser Records

Erhan Akbal[1*], Fatma Güneş[1], Ayhan Akbal[2]

[1] Department of Digital Forensics Engineering, Fırat University Technology Faculty, 23119, Elazig, Turkey.
[2] Department of Electrical and Electronics Engineering, Fırat University Engineering Faculty, 23119, Elazig, Turkey.

* Corresponding author. Email: erhanakbal@firat.edu.tr
Manuscript submitted January 11, 2016; accepted March 12, 2016.
doi: 10.17706/jsw.11.7.631-637

Abstract: The most used applications by the majority of user of computer are web browsers. Users performs their many activities such as, browsing on the internet, download files, use social media applications, accessing e-mail accounts via web browser. Many of the crimes committed on digital resources must be analyzed user activities by examining the records of web browsers. Especially regarding crimes involving entered the URL, access times, browser type, time, downloaded files, search words, such information must be included in the reports of the examiners will create one of the data obtained. Web browser stores user records in different ways. Also, according to user operating systems differ in the locations for storing data. In this study, it is shown that how it should be done the analysis of web browsers on the digital resources which are subject to criminal, the data of different browsers on different operating systems, storage types and data types that can be obtained. In addition, it is showed that, the tools and features used to examine the records in the web browser.

Key words: URL records, web browser analyses, digital forensic, digital evidence.

1. Introduction

Web browsers are the tools for performing different activities on the Internet by users. Users utilize browsers for many functions such as information search, access to e-mail accounts, e-commerce, making the banking, instant messaging, online blogs, access to social networks Web browser records many data related to user activity. Information such as URLs visited by users, search terms, cookies, cache files, access time, and use time holds in memory on the system [1].

In case of a different user to access the same computer, accessing to this information can be provided in a very easy way. Web browsers are important tools on many of the crimes committed on digital resources. Examining the evidence which is the subject of criminal records is an important step examination of your browser. To uncover offender's profile and connections depends on web registry.

The suspects can use web browsers for activities such as to collect information, to hide the crime, to get in touch with crime partners The evidence obtained from use of the Web browser is a key component of the forensic expert. Suspicious leaves a mark on his computer about every movement as long as the use of web browser [2]. It is possible to analyze evidence like history, cache, cookies, downloads list, entering URL addresses, access time of visit, frequency of visits from the suspect's computer.

In the analysis process should first identify the web browsers. Users can use different processes related offenses in different web browsers. There are many different web browsers can use on the internet today. Utilization ratio of used web browser is shown in Fig. 1 [3]. For doing analysis correctly it is necessary to

examine registry of web browsers on image. The analysis of only a web browser is not enough to obtain the evidence.

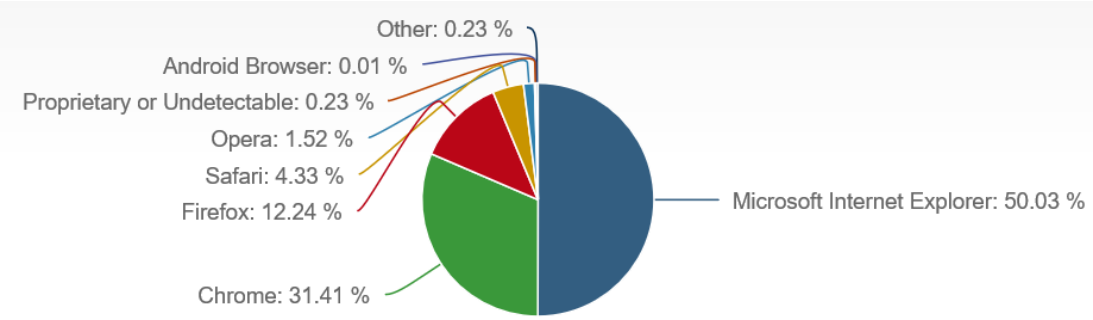

Fig. 1. Utilization ratio of web browsers.

It is very important to be able to analyze evidence with different versions of browsers like Internet Explorer, Google Chrome, Firefox, Safari and Opera for ensuring authenticity of the evidence.

In this paper, it is shown how to obtain user web browser activities from image of an evidence [4]. Usage of applications which are used in this field are shown and compared Processes of getting information like URL, visit date, visit count, web browser type, system user name, browser profile, URL size from web browser files, are demonstrated [5].

2. Analyses of Web Browser Records

Web browsers are one of the most commonly used applications in digital devices. Users perform their internet activities with web browsers in different operating systems. Web browsers are used for many purposes like, searching information, e-mail, e-commerce, news, e-banking, social media and blog writing [6]. For this reason, it is one of the most important parts of evidence analysis. Information like which URLs was visited by the user, which words was searched, when these actions were made, are used by digital forensics experts to determine the crime. Also, usage of different web browsers in the same period must be analyzed. A lot of open source and licensed tools exist for performing analysis. Users often perform activities specified in Table 1 [2] in web browsers.

Table 1. User Activity on Web Browsers

User Activity	Word in URL
Search	Search, word about serch
E-mail	Mail, e-mail
Blog	Blog
Social Media	Facebook, Twitter, Instagram, vb.
News	News
Shopping	Shopping, shop, foni, vb.
Weather Condition	Weather
Game	Game
Video, Visual Content	Video
Music	Music, mp3
Banking	Bank, Credit

2.1. Keeping Records on Computers

Web browsers are stores in different parts of the operating system user activity. To access the user information, analysis is required in various fields. Furthermore, data varies according to web browsers type. Web browsers keep user records on 4 different sections. These are Cache Records, History Records, Cookies

Registry, and Downloaded Files. The locations which are web browsers stores data on operating systems is showed on Table 2.

Table 2. File Location in the Web Browser Operating System

Web Browser	Operating System	File Path
Internet Explorer	Windows 95/98	C:\Temporary Internet Files\Content.ie5 C:\Cookies C:\History\History.ie5
	Windows 2000/XP	C:\Documents and Settings\%username%\Local Settings\Temporary Internet Files\Content.ie5 C:\Documents and Settings\%username%\Cookies C:\Documents and Settings\%username%\Local Settings\History\history.ie5
	Windows Vista, 7 and latest version	C:\Users\%username%\AppData\Local\Microsoft\Windows\Temporary Internet Files\ C:\Users\%username%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\
Firefox	Linux	/home/$USER/.mozilla/firefox/$PROFILE.default/places.sqlite
	MacOS-X	/Users/$USER/Library/Application Support/Firefox/Profiles/$PROFILE.default/places.sqlite
	Windows XP	C:\Documents and Settings\%username%\Application Data\Mozilla\Firefox\Profiles\%PROFILE%.default\places.sqlite
	Windows Vista,7 and latest version	C:\Users\%USERNAME%\AppData\Roaming\Mozilla\Firefox\Profiles\%PROFILE%.default\places.sqlite
Safari	MacOS-X	/Users/$USER/Library/Safari/ /Users/$USER/Library/Caches/com.apple.Safari/
	Windows XP	C:\Documents and Settings\%username%\Application Data\Apple Computer\Safari\ C:\Documents and Settings\%username%\Local Settings\Application Data\Apple Computer\Safari\
	Windows 7	C:\Users\%username%\AppData\Roaming\Apple Computer\Safari\ C:\Users\%username%\AppData\Local\Apple Computer\Safari\
Opera	Linux	/home/$USER/.opera/
	MacOS-X	/Users/$USER/Library/Opera/
	Windows XP	C:\Documents and Settings\%username%\Application Data\Opera\Opera\
	Windows Vista, 7 and latest version	C:\Users\%username%\AppData\Roaming\Opera\Opera\
Google Chrome	Linux	/home/$USER/.config/google-chrome/Default/Preferences
	MacOS-X	/Users/$USER/Library/Application Support/Google/Chrome/Default/Preferences
	Windows XP	C:\Documents and Settings\%username%\Local Settings\Application Data\Google\Chrome\User Data\Default\Preferences
	Windows Vista, 7 and latest version	C:\Users\%username%\AppData\Local\Google\Chrome\User Data\Default\Preferences

According to web browsers system stores data in different folders and locations. In the analysis process it is necessary to examine data in different folders. Folders should be searched for in 4 different record types mentioned above. Types storing of web browser are listed below.

Internet Explorer is a web browser which computer users use commonly. Internet activity records are stored for each user separately under the user profile folder. Data stores in Cookies, Cache, Download History and history folders separately under the locations which is showed in Table 2. Data stores under folders in index.dat or container.dat database files. Data is stored in binary format this file. Safari stores web browser data in file which is named History.plist in binary format under the web browser data locations. It stores the information of URL addresses, date of visit, time, and the number of visits for each website Firefox stores web browsers data in a file which is named places.sqlite. File uses the SQLite database format. Opera keeps data in different files with the extension .dat. These files are cookies4.dat, download.dat, global_history.dat,

search_field_history.dat. Google Chrome stores data in the preferences file. There is separate file for each user. There is information about user policies, master preferences, and local locations data.

2.2. Time Formats Used by the Web Browser

It is necessary to analyze the user behavior in a given time period for demonstrating crime in forensic examination. In order to determine the offender's activities, a time schedule should be formed and followed. [4]. Thereby it can uncover about relationships with other websites which are related crime visited by suspects in same time. Time format which is used by web browsers given Table III [2]. The expert who analyzes must take into account the time format that has been used by the web browser. Otherwise the time of suspect use cannot determine. Therefore, the expert who examine must do time correction. The time format of the data obtained from the evidence must be consistent with the user's examination of his time format.

Table 3. Time Format Used by Web Browser

Web Browser	Time Format
İnternet Explorer	FILETIME:100-ns(10-9) Since January 1, 1601 00:00:00 (UTC)
Firefox	PRTime:microsecond (10-6) Since January 1, 1970 00:00:00 (UTC)
Google Chrome	WEBKIT Time: microsecond (10-6) Since January 1, 1601 00:00:00 (UTC)
Safari	CF Absolute Time: second Since January 1, 2001 00:00:00 (UTC)
Opera	UNIX Time : second ince January 1, 1970 00:00:00 (UTC

2.3. Clearing the Web Browser History

The analysis process of web browsers record, suspicious could have deleted browsers data. Many web browsers offer options for delete cache, cookies, history, download files to users. When this information is deleted, users will destroy that can be obtained in the examination by using function of browser. There are two ways for deleting records. [2], [4]. First method, by overwriting the existing data with the launch of applications, the old data is lost. Second method, deleting data from the browser menu or the index by users voluntarily. After first method, accessing old data is very hard. After second method accessing data is possible by recovering and disk scratching actions. Choice and access roads allowing the deletion of records by users of the browser is given in Table IV.

Table 4. Locations of Deleting Data According to the Type of Browser

Web Browser	Delete Options Path
İnternet Explorer	Settings/ Internet Options/ / Deletes
Firefox	Settings /Privacy/History about:preferences#privacy
Google Chrome	Settings /History/Search Data chrome://settings/clearBrowserData
Safari	Settings / Privacy / Delete All Web Site Data Settings/History
Opera	Settings /History/Privacy and Security/Delete All Search Data opera://settings/clearBrowserData

3. Tools for Analysis

Commonly WEFA, NetAnalaysis, Browser History Examiner, FTK and Encase are software used for analyzing web browsers in digital forensics examinations. In this chapter features of specified web browser analyze tools are demonstrated [7].

3.1. IEF (Internet Evidence Finder)

IEF is a software with license fee produced by Magnet forensics company. Personal computers are used in the process of examinations of smart phones and tablets by experts. With its different models, it presents the characteristics like examining internet TV series, analysis of traces obtained from mobile applications. It is used on Windows and MacOs operating systems.

3.2. WEFA

WEFA is a free web browser analyze tool. It runs on Windows NT and later versions. Supports Internet Explorer(~11),Mozilla Firefox, Apple Safari, Opera, Chromium, Google Chrome, Google Chrome Canary, Comodo Dragon, CoolNovo(ChromePlus), Swing browsers. For these browsers WEFA offers various methods to perform analysis from an active system or an image disk. These methods include gathering the web browser's cache, cookies, internet history, download history, session data, temporary internet files, and the timesheet data information. The obtained data can be displayed in timeline view, HTML view or URL parameters view Searches can be made in obtained data by date, key word or regular expressions. Also deleted data can be recovered, index.dat file can be analyzing in detail and classification and analysis of user behaviors can be made. CSV formatted reports can be generated according to these data.

3.3. NetAnalysis

NetAnalysis is a licensed tool developed by Digital Detective company for digital examining of web browsers. And supports Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari and Opera bowsers. It allows the examination of Internet history, cache, cookies and other components. And it has an effective reporting feature that allows quickly gathering evidence according to user behavior. Also this software has effective analytical tools for decoding and understanding data. At the same time, it has ability to use SQL queries to identify related evidence. Also it can be used to recover deleted web browser components

3.4. Browser History Examiner

Browser History Examiner is a licensed tool developed by Foxton Forensics Company and it extracts and analyzes web history It supports Chrome, Firefox, Internet Explorer and Edge web browsers. And it can analyze a lot of data type as downloads, cache data and visited URL files.

Internet activities in a specific timeline can be traced with web site timeline feature. Data can be analyzed by using various filters like key word list and time-date range with advanced filtering feature. Image files saved in the browser cache can be easily shown in thumbnail galleries with cache image viewer feature. Web sites stored in browser cache can be reconstructed and analyzed with cache web page viewer feature. Different time zone conversions can be performed with Time Zone and DST Configuration feature. And all obtained data from these features are reported.

3.5. FTK

FTK is one of the tools developed to analyze systems entirely. It enables to analyze web browser data with its features. Web browser history is virtualized in detail. Internet Explorer, Firefox, Chrome, Safari and Opera browsers are supported. Also, deleted web browser data can be recovered by FTK. This software also has a feature to report analysis results.

3.6. Encase

Encase system is an analysis tool developed to examine systems entirely. It enables to examine web browser data with its features. With the help of a simple script, all browser history, cookies and cache files are copied into

a file by using 3rd party software. Internet explorer, Firefox, Chrome / Chromium, Opera and Safari are supported in Windows, UNIX and Mac operating systems. Also it enables to recover deleted internet components. Obtained data can be analyzed by filtering according to key word and time parameters.

WEFA, NetAnalysis and History Examiner are developed especially for performing digital analysis of web browsers. But, FTK and EnCase applications are developed to examine files and systems. This software also has features as analyzing web history and holistic analysis.

4. Conclusion

Web browser analysis is one of the most important processes in digital forensics. Most of the crimes committed through computer systems is performed via a web browsers and a lot of crimes are revealed by this analysis. Digital forensics experts must know how web browsers save data in different operating systems to be able to collect evidence from web browsers. Obtaining search history of the suspect, search words, visited URLs, download history and cache data is very important for gathering evidence. Information which obtained from user files reveals whether the offense occurred or not. Therefore, experts must analyze browser data correctly.

In this paper it is shown how most commonly used web browsers store data, what information can be recover or analyze and how different operating systems store records. Besides, applications which can be used by experts who perform analysis in this field, are introduced. Thus, it is put forward which data will be obtained and analyzed by expert in this field.

References

[1] Murilo, T. P. (2009). Forensic analysis of the Firefox 3 internet history and recovery of deleted SQLite records. *Digital Investigation*, *5,* 93-103.

[2] Junghoon, O., Seungbong, L., & Sangjin, L. (2011). Advanced evidence collection and analysis of web browser activity. *Digital Investigation, 8,* 62-70.

[3] Net application. Browser market share. Retrieved from https://marketshare. hitslink.com/browser-market-share.aspx

[4] Said, H., Mutawa, N. A., Awadhi, I. A., & Guimaraes, M. (2011). Forensic analysis of private browsing artifacts. *Proceedings of International Conference on Innovations in Information Technology* (pp. 198-202). Abu Dhabi: IEEE.

[5] Zsolt, N. (2012). Using forensic techniques for internet activity reconstruction. *Proceedings of the 16th WSEAS International Conference on Computers* (pp. 248–253).

[6] Keith, J. J., & Rohyt, B. (2005). *Web Browser Forensics, Part 1.* Retrieved from *http://www.securityfocus.com/infocus/1827*

[7] Eckersley, P. (2009). *How unique is your web browser?* Electronic Frontier Foundation. Retrieved, from https://panopticlick.eff.org/ browser-uniqueness.pdf

Erhan Akbal is currently working as an assistant professor at Digital Forensics Engineering Department of Firat University, He received his Ph.D. degree in electrical and electronics engineering in 2012, the M.S. degree in computer engineering in 2007, from Firat University, Turkey. His research interests include computer network security, wireless sensor network, intrusion detection and digital forensics.

Fatma Gunes is currently working as a research assistant at Digital Forensics Engineering Department of Firat University, Turkey. She received her bachelor degree in computer science in 2013, Kocaeli University, Turkey. Her research interests include computer network security, wireless network, information security and digital forensics.

Ayhan Akbal was born in 1977 in Elazig, Turkey. He is currently working as an assistant professor at Electrical-Electronics Engineering Department of Firat University. He received his Ph.D. degree in electrical and electronics engineering in 2008, the M.S. degree in computer engineering in 2001, from Firat University, Turkey. His research interests include communication, network, wireless, FPGA security, wireless sensor network.