Forensic analysis on Windows System for Internet Evidences

SILPA M L
M.Tech in Computer Science
With specialization in Cyber Forensics and Information Security ER&DCI Institute of Technology
CDAC, Trivandrum
Kerala, India
silpaml.vlnd@gmail.com

Abstract-- **Internet has become essential for everyday tasks and it is being used to commit a lot of criminal acts. Users perform various activities with a Web browser, such as information retrieval, e-mail, shopping, news, online banking, blogging, and SNS. Therefore, the forensic investigator should be able to analyze the user's activities when performing the investigation. Accessing the Internet leaves a wide variety of information in a computer system. Those information from the system may help the investigators to a great extend to their investigation. This paper is a study on the locations of various internet related artifacts available on a windows system and the tools available to retrieve those information.**

I. INTRODUCTION

Internet is an essential tool for everyday tasks. Its usage is growing day by day. Users perform various activities with a Web browser, such as information retrieval, e-mail, shopping, news, online banking, blogging, and SNS. Those information from the system may help the investigators to a great extend to their investigation. Searching for evidence left by web browsing activity is typically a crucial component of digital investigation. Web browser history, cache, cookies, preferences and the registry are the areas commonly searched for evidence. There are so many tools exist to collect internet related evidences.

Most common Internet browsers are today Mozilla's Firefox, Internet Explorer developed by Microsoft and Chrome from Google. The typical computer forensics process examines and analyses all possible information located on the computer or other digital devices related to the incident. But as mentioned earlier, a big amount of information exchange and access is done over the World Wide Web and hence some kind of Internet browsing software is needed. All Internet browsers have once in common, as all of them save some information about the user browsing behavior for the reason of user convenience and speed which was a big topic in the beginning of the Internet. These savings offer a big benefit for computer forensics and hence forensic professionals are able to reconstruct parts of the users browsing history. They are able to determine visited URL's, even sometimes when they were visited years ago, discover bookmarks and cookies and find out searches and downloads.

II. RELATED WORKS

In 2011, Junghoon Oh et al presented a paper 'Advanced evidence collection and analysis of web browser activity' describes users perform various activities with a Web browser, such as information retrieval, e-mail, shopping, news, online banking, blogging, and SNS. Therefore, the forensic investigator should be able to analyze the user's activities when performing the investigation. Search word information, which can be used to analyze information retrieval activity, is especially important.

The paper "Forensic analysis of residual artifacts from private and portable web browsing sessions" describes the private browsing [2] modes of commonly used web browsers and the traces that left on the system during private browsing session. Microsoft IE offers users a private browsing feature called InPrivate Browsing. Browsing enables users to surf the Internet without leaving a trace on their computer. However, while using InPrivate Browsing, some information such as cookies and temporary files are temporarily stored so that webpages will work correctly. Once the browsing session is ended, all of that data is discarded. In regards to browser extensions, IE disables all toolbars and extensions during InPrivate Browsing sessions to ensure better privacy.

The paper "Study on Pagefile.sys in Windows System" describes the structure of a pagefile [1] and the various artifacts present in it. Paging is a memory management scheme used by the operating system to store and retrieve data from secondary storage for use in main memory. Paging is an important part of virtual memory implementation in

most currently available operating systems, allowing them to use disk storage for data that does not fit into physical memory. When the physical memory is full and has no more space for the incoming processes then the memory management swaps out pages to an area on the hard disk and retrieve them when needed. Pagefile.sys is a file that is used by Microsoft Windows to store frames of memory that do not currently fit into physical memory. It means Windows uses a page file to store data that can't be held by the computers random-access memory when it fills up. Analysis of the Pagefile.sys gives the information of which events were done on PC. Analysis of Pagefile.sys can give the sensitive information such as User Ids, Passwords, Hidden Processes, Download info, Search Activity of Browser etc.

III. INTERNET HISTORY LOCATIONS

This section describes the various internet artifact location on a windows system.

A. Browser Cache

The browser cache saves parts of any visited website. If the user attempts to visit a website the browser checks first if some information is already stored in the cache directory before fetching the URL. If content from the requested URL is already stored in cache and still valid, the browser will automatically uses that information rather than downloading the page content again, which speeds up the browsing performance. The location of cache files of various browsers are the following:

Firefox: %USERPROFILE%\ AppData\ Local\ Mozilla\Firefox\Profiles\<randomtext>.default\ Cache

Internet Explorer: %USERPROFILE%\ AppData\ Local\ Microsoft\ Windows\ Temporary Internet Files\ Content.IE5

Google Chrome: %USERPROFILE%\ AppData\ Local\ Google\ Chrome\ User Data\ Default\ Cache\ - data_# and f_######

B. Cookies

Cookies are used to store session information sent by the web server to the Internet browser which then stores it on the client's disk. The information within a cookie is therefore useful for computer forensics to determine visited websites, maybe the user identifier (ID), access time or what a user has chosen or selected on the website. The range of possible information stored within a cookie is obviously very broad and hence it can be a goldmine for forensic professionals.

Mozilla Firefox: C:\Users\ <*username*> \AppData\ Roaming\ Mozilla\ Firefox\ Profiles\ code.default\

Internet Explorer: C:\Users\<*username*>\ AppData\ Roaming\ Microsoft\ Windows\ Cookies\ Low\

Google Chrome: C:\ Users\ <*username*>\ AppData\Local\Google\Chrome\User Data\Default\

C. Downloads

The 'downloads' are the files a user downloaded from the internet. These can be of any data type and each browser handles downloads differently. All versions of Firefox and Chrome and Internet Explorer present downloads a user made in a download list which can be opened from inside the browser. If a user did not clear this list then it can show all downloads made in the past and hence provide some evidence.

D. Restore Points

Windows creates automatically restore points which allows the user in case of a system failure or other reasons to reset the system to a certain configuration point in the past. Christo Ananth et al. [4] proposed a secure hash message authentication code. A secure hash message authentication code to avoid certificate revocation list checking is proposed for vehicular ad hoc networks (VANETs). The group signature scheme is widely used in VANETs for secure communication, the existing systems based on group signature scheme provides verification delay in certificate revocation list checking. In order to overcome this delay this paper uses a Hash message authentication code (HMAC). It is used to avoid time consuming CRL checking and it also ensures the integrity of messages. The Hash message authentication code and digital signature algorithm are used to make it more secure . In this scheme the group private keys are distributed by the roadside units (RSUs) and it also manages the vehicles in a localized manner. Finally, cooperative message authentication is used among entities, in which each vehicle only needs to verify a small number of messages, thus greatly alleviating the authentication burden.These points contain a copy of the system and applications, hence includes all browsing history data no matter which Internet browser was in use. Such restore points are not accessible in a live system and therefore it is nearly impossible for a user to tamper the data within it. A forensic professional can create a bit image of the disk, accessing the restore points and trust the data to be authentic. A restore point is very useful for a forensic investigation as it shows the past states of a system and all related data to that state.

E. Hiberfile

The Windows hibernation file, called 'hiberfil.sys', is stored as a hidden file in the root folder of the OS which is usually the C drive. This file is always in use by the OS itself and hence not accessible while the system is running. Therefore an image of the disk is required before it can be accessed.

F. Pagefile

Pagefile.sys is a windows system files, acts as swap file and was designed to improve performance. The size of the pagefile is around 1.5 to 3 times the size of the RAM. It is located in the C drive. Pagefile.sys is a file that is used by Microsoft Windows to store frames of memory that do not currently fit into physical memory. It means Windows uses a page file to store data that can't be held by the random access memory when it fills up. This files may contain live memory artifacts written to a disk as a part of operation system's working routine.

Capturing the page-file is difficult on a live system as traditional file copying utilities cannot open them. When the system is running the files are in use by the operating system and may not be opened by another process. To acquire the page-file mount the drive in a guest operating system and copy the page-file.

Analysis of the pagefile.sys gives the information of which events were done on PC and can give the sensitive information such as user ids, passwords, hidden Processes, download information, search activity of browser etc.

IV. TOOLS FOR INTERNET EVIDENCE COLLECTION

There are so many tools exist to collect internet related evidences. Most of the tools are developed to perform log analysis.

A. Pasco

Pasco is an open-source tool that can be used to reconstruct browser use from Microsoft Internet Explorer's (IE's) index.dat files. The files contain data such as which URLs were visited and when. Pasco is a command-line tool that creates a text-based output file.

B. Galleta

Galleta is an Internet Explorer Cookie Forensic Analysis Tool that was also developed by Keith J. Jones, a Principal Computer Forensic Consultant at Foundstone, Inc. Many computer crime investigations require the reconstruction of a subject's Internet Explorer Cookie files and since this analysis technique is executed regularly, Galleta analyses the structure of the data found in the cookie files. It is an open source browser forensics CLI tool for Internet Explorer and collect evidences from index.dat file and gives a text based output file.

C. NetAnalysis

NetAnalysis is the industry leading software for the extraction and analysis of data from Internet browsers. It is a software for the extraction of Internet browser trace evidence. It collect information from browser history and cookies.

D. Cacheback

It is possible to perform an integrated analysis of different Web browsers, but this tool uses a simple parsing process to analyze cache and history files. Cacheback is an offline, Window based Internet evidence extraction tool that is designed to analyze Internet browser related artifacts. Cacheback is the only Internet forensic tool on the market today that supports all five top browsers (IE, Firefox, Google Chrome, Opera and Safari). They further claims that Cacheback is the preferred Net analysis tool for forensic investigations. It is also the leading finder of Internet evidence and related artifacts that consolidates everything into a single, comprehensive user interface. Cacheback was not able to scan the evidence image without third party tool intervention, other tools such as FTK imager has to be used in conjunction with the CacheBack tool.

E. Internet Evidence Finder

Internet Evidence Finder (IEF) is a computer forensics product that can search a live RAM for Internet-related evidence. It is a software application that can search a hard drive or files for Internet related artifacts. It can be used as a data recovery tool that is geared towards digital forensics examiners. IEF works with Windows operating system. IEF provides a user-friendly interface for the digital forensic investigator.

The Table I how the list of open source utilities to collect browsing information from a system. For each of the browser, variety of tools exists to retrieve the information regarding the users browsing activity.

Table I: List of open source utilities to collect browser records

Software	Purpose
IE History View	To count the number of histories made using Internet Explorer
IE Cache View .	To count the number of files currently stored in the Internet Explorer cache
IE Cookies View	To count the number of cookies that Internet Explorer stores on target computer.
Mozilla History View	To count history data file (history.dat) of Firefox Web browsers.

Mozilla Cache View	To count the number of cached items from cache folder of Firefox Web browser.
Mozilla Cookies View	To count the number of cookies stored inside the cookies file.
Chrome History View	To count the list of all visited Web pages in Chrome web browser.
Chrome Cache View	To count the list of all files currently stored in the cache in Chrome browser.
Chrome Cookie View	To count the list of all cookies stored by Google Chrome Web browser.

VI. CONCLUSION

Retrieving internet evidences from a suspect's system is a crucial activity during digital investigation. Users browsing information can be collected from various locations in a windows system. During investigation, the first thing is to identify the locations where the artifacts are available and which tools can be used to retrieve those artifacts. This paper describes the various artifact location and the tools available to collect the browser related information.

V. REFERENCES

[1] Nisarg Trivedi, "Study on Pagefile.sys in Windows System" IOSR Journal of Computer Engineering, April 2014

[2] Donny J Ohana, Narasimha Shashidhar, "Forensic analysis of residual artifacts from private and portable web browsing sessions," EURASIP Journal on Information Security, June 2013

[3] E. Schaap, I. Hoogendoorn, "Reconstructing web pages from browser cache," University of Amsterdam July 5, 2013

[4] Christo Ananth, M.Danya Priyadharshini, "A Secure Hash Message Authentication Code to avoid Certificate Revocation list Checking in Vehicular Adhoc networks", International Journal of Applied Engineering Research (IJAER), Volume 10, Special Issue 2, 2015,(1250-1254)

[5] J. Oh, S. Lee, and S. Lee, "Advanced evidence collection and analysis of web browser activity," Digital Investigation: The International Journal of Digital Forensics & Incident Response archive, vol. 8, pp. S62–S70, August 2011.

[6] Kris Harms, "Forensic analysis of windows system restore point", 2007

[7] Keith J. Jones, "Forensic Analysis of Internet Explorer Activity Files," 2003

[8] Belani, R., Jones, K., Web browser forensics. Retrieved from http:// www.symantec.com/ connect/ articles/ web-browser-forensics-part-1