Web Forensics

GRADUATE PROJECT PROPOSAL

Submitted to the Faculty of
The Department of Computing Sciences
Texas A&M University-Corpus Christi
Corpus Christi, Texas

In Partial Fulfillment of Requirements for the Degree of Masters of Science in Computer Science

By

Sandeep Kumar Khanikekar
Fall 2010

Committee Members

Dr. Mario García
Committee Chairperson

Dr. Ajay Katangur
Committee Member

Dr. Hongyu Guo
Committee Member
ABSTRACT

Cyber-crimes are increasing rapidly and the people who do such things try to leave no forensic evidence. Cyber-crimes range from piracy to identity theft and beyond. Sometimes the criminals make use of the Internet which makes tracking the users of a Web page complex and difficult. Evidence of digital crime includes network traffic, network devices, storage devices, mobile devices etc. The Browser history, registry entries and cookies on the client side and the log files on the server side are some of the potential sources where one can track the user’s actions and find evidence of occurrence of a particular event. This project focuses on the forensic analysis of Web Browsers particularly Internet Explorer, Safari, Google Chrome and Mozilla Firefox on Windows 7.

The project also includes examination of the various changes in the system configuration, browser data and registry when “private browsing” is enabled and disabled in the browsers which offer this option.
# TABLE OF CONTENTS

Abstract ................................................................................................................................. i

Table of Contents .................................................................................................................. ii

List of Figures ....................................................................................................................... iv

List of Tables ......................................................................................................................... vi

1. Background and Rationale ............................................................................................. 1
   1.1 Introduction .................................................................................................................. 1
   1.2 Types of Browsers ..................................................................................................... 3
   1.3 Previous Work on Web Forensics .............................................................................. 5

2. Web Forensics ................................................................................................................. 11
   2.1 Definitions ................................................................................................................. 11
   2.2 Server side Forensics .............................................................................................. 15
   2.3 Obtaining Information from the Registry .............................................................. 18
   2.4 Other forms of Forensic Evidence .......................................................................... 19

3. System Design ................................................................................................................. 30
   3.1 Overview of the system ......................................................................................... 30
   3.2 Information Analyzed ........................................................................................... 31
4. Testing and Evaluation ................................................................. 39

4.1 Fresh Installation ........................................................................ 39

4.2 Browser Installation ..................................................................... 40

4.3 Flash Cookies ............................................................................. 48

5. Conclusion and Future work .......................................................... 49

Bibliography and References ............................................................. 53

Appendix A. Starting Private Browsing ............................................... 56

Appendix B. Looking for Cookies ....................................................... 62

Appendix C. Program to visit Websites ............................................. 66
LIST OF FIGURES

Figure 2.1 Displaying Firewall Rules ......................................................... 15
Figure 2.2 Temporary files stored in Low Privilege mode of IE. ......................... 26
Figure 2.3 Temporary files and Cookies stored in IE ...................................... 27
Figure 2.4 Browser specific files stored in Safari ......................................... 28
Figure 3.1 User Data .................................................................................... 37
Figure 4.1 Flash Player initial preview ....................................................... 40
Figure 4.2 Mozilla plugin preview ............................................................. 42
Figure 4.3 Main Folder of IECookies.plist .................................................. 43
Figure 4.4 Cookies.plist ............................................................................. 44
Figure 4.5 Cookies.plist tree view ............................................................. 46
Figure 4.6 Typed URLs shown in registry .................................................... 47
Figure 4.7 Recovery of deleted files failed using FTK .................................... 48
Figure 5.1 Cookies stored in Chrome on the test system ............................... 52
Figure 5.2 Screenshots of websites stored in Safari .................................... 53
Figure A.1 Starting Private Browsing in IE .................................................. 57
Figure A.2 Private Browsing window in IE .................................................. 58
Figure A.3 Starting Private Browsing in Mozilla Firefox .............................. 59
Figure A.4 Starting Private Browsing in Mozilla Firefox .............................. 59
Figure A.5 Private Browsing window in Google Chrome .............................. 60
Figure A.6 Private Browsing window in Google Chrome .............................. 61
Figure A.7 Private Browsing window in Apple Safari………………………………………………62
Figure A.8 Private Browsing window in Apple Safari………………………………………………62
Figure B.1 Cookies in IE – 1 .................................................................................................63
Figure B.2 Cookies in IE – 2 .................................................................................................64
Figure B.3 Cookies in Firefox.................................................................................................65
Figure B.4 Cookies in Chrome.................................................................................................66
Figure C.1 Setting Environmental variables I ........................................................................67
Figure C.2 Setting Environmental variables II .........................................................................64
Figure B.3 Cookies in Firefox.................................................................................................65
Figure B.4 Cookies in Chrome.................................................................................................66
1. BACKGROUND AND RATIONALE

1.1 Introduction

The Internet is a very easy way to reach any system. If confidential data is not properly protected, then it becomes opens to vulnerable access and misuse. Cyber-crime can cause varying degrees of damage by hackers. So, detailed forensic analysis is required to come to a conclusion about an incident and to prove or disprove someone’s guilt.

Web forensics relates to cyber-crime on the Internet. Some criminal activities like child pornography, hacking, and identity theft can be traced and the criminals can be punished if proper evidence is found against them. Web forensic analysis brings out some details like when and in what sequence did somebody access a Web page. Cross-site request forgery (CSRF) can be used by an attacker to force the victim’s Browser to perform searches and all forms of illegal actions for the attacker. The victim is eventually discovered by the firms monitoring the inappropriate users of systems. The US Secret Service and the San Francisco Electronic Crimes Task Force report that approximately 30 attack sites are detected each day [Chou 2004].

The victims of Web attacks are clients and Web servers. Both clients and server side protection is necessary. The attacks can be performed by using false URLs and redirects to malicious sites. The medium of attack on the Internet are Web Browser, database servers and application servers. On the client side, forensic analysis is done to find out if a user has been involved or has been a victim of the crime. Potential evidence
can be found in the Browser history, registry entries, temporary files, index.dat, cookies, favorites, html pages in unallocated space, emails sent and received by the user and the cache etc. On the server side, forensic analysis can be done by examining access logs, error logs and FTP log files and network traffic. The intermediate site logs such as antivirus server logs, Web filter logs, spam filter logs and firewall logs also help in tracking an incident.

There are five basic steps to computer forensics [Ashcroft 2001]:

1. Preparation (of the investigator, not the data)

   The investigator should be aware of the problem fully. He/she should have a proper (could be abstract) plan for investigation. Acquire permissions to access the information that investigation process may need.

2. Collection (of the data)

   Collect the data required for the investigation. Proper precautions need to be taken while collecting the information. Safety devices like write blockers should be used. All the data should be collected according to a plan of investigation.

3. Examination

   A careful examination of data should be done. Sophisticated tools should be used to make sure the tests give accurate results. All the possible
scenarios should be taken into consideration while an investigation is being carried out.

4. Analysis

Analysis of results to reach a conclusion should be transparent. Analyzing could not lead to the actual facts. If possible an interview should be conducted to backup the results.

5. Reporting

Reports should be reported to the concerned authority with utmost security and integrity. The reports should be archived and saved for future references.

1.2 Types of Browsers

Web Browsers can be classified based on the layout engines or the technology used in the development. Some of the kinds of Browsers are [Browsers 2010]:

- KHTML and WebKit based Browsers
- Gecko-based Browsers
- Trident based Browsers
- Specialty Browsers
- Text based Browsers
• Other Browsers

A brief overview of these Browsers follows [Browsers 2010]:

1.2.1 KHTML and WebKit based Browsers Developed by the KDE project (a free software community which produces cross platform applications for Linux, Windows, Solaris, FreeBSD, Mac OS X), KHTML is an HTML layout engine written in which C++ supports good Web standards. Browsers like ABrowse, Safari, Konqueror were developed based on this layout engine. Safari is an Apple Web Browser that comes pre-installed with the Macintosh operating system. WebKit is another layout which was initially developed by Apple Inc. and later Google Inc. also developed this layout to develop Google Chrome Browser.

1.2.2 Gecko-based Browsers Mozilla Corporation developed this layout engine and many more like this, for example Mozilla Application Suite, Nvu, Mozilla Thunderbird etc. It is written in C++ and is cross-platform and offers a rich programming API that makes it suitable for a variety of applications to run in the Browser.

1.2.3 Trident based Browsers These Browsers use Microsoft’s Trident engine. Some of the Browsers using this layout engine are AOL Explorer, Enigma, and Yahoo! Browser etc. The Add/Remove Programs tool in Windows is an HTML application based on Trident to display the list of programs installed on the computer. Appropriate adjustments were made to use Trident for the layout of the newer versions of IE.

1.2.4 Specialty Browsers These Browsers are designed for special purposes to give specific intended content. Ghostzilla is used to hide the Internet use and HeatSeek is the
Browser to seek online porn. Some of the other specialties Browsers include Flock, Wyzo and Songbird.

1.2.5 **Text based Browser** These Browsers only use text. Some of the Browsers like Alynx, Elink, w3m, and Lynx are developed using this approach.

Other Browsers like Emacs, IBrowse and PlanetWeb are also available on the Internet.

The focus of this project is on the Internet Explorer, a Trident based Browser, and Mozilla Firefox, a Gecko based Browser, Google Chrome, a WebKit based browser and Apple, KHTML based browser.

1.3 **Previous Work on Web Forensics**

It is well known fact that it is difficult to find criminals online based on previous experiences. The lessons learned from previous criminal cases involving computers can be used to assist with current investigations. The difference in skill sets within computer forensics and Web forensics not only refer to the characteristics of the investigator, but also to the criminal as well [Berghel 2003]. Berghel emphasizes that in most cases computer forensics criminals are not that computer savvy and have only the basic fundamental skill level of a typical end user. There is an advanced skill set required for Web and Internet related crimes and the author mentions that criminals tend to rely on the same tools that they are most likely being investigated with. Berghel references the application NetScanTools Pro as a forensic tool which is used for forensic analysis within a legal fashion yet can also be manipulated by hackers for the purpose of misuse and
illegal activity. The difference in use of the applications within the Web forensics environment is one of ethics and not skill.

Martellaro discusses the role of the ping command in a forensics investigation, which is used in finding out the IP addresses of a known domain name [Martellaro 2009]. While the icmp (Internet Control Message Protocol) may be disabled on some networks, the IP address of a site is returned right away. On a Windows computer launching the command prompt application and typing `ping <domain name>` gets the IP address. For a Mac the Network Utility found in the Application/Utilities folder is invoked and there are multiple information gathering tools like ping, lookup, traceroute and whois. The interesting part is that IP addresses are generally assigned by country, and there are databases of IP addresses versus geolocation. That's how an iPhone uses location services [Martellaro 2009].

IE is a browser that is pre-installed on a Windows computer, stores all Internet browsing activity under a user’s Windows profile. According to Jones, the directory closely matching the path “C:\Documents and Settings\<user>\Local Settings\Temporary Internet Files\Content.IE5” in Windows XP, this directory stores the cached pages and images that a user may have accessed through their Web Browser [Jones 2010]. The purpose of this cache is for the Browsers not re-download information that has been previously viewed. Other two directories of interest as Jones et al [Jones 2010] point out are: “C:\Documents and Settings\<user>\Local Settings\History\History.IE5” and “C:\Documents and Settings\<user>\Cookies” [Jones 2010]. The locally cached Web page and the URL has to be correctly located to rebuild a Web page a user had visited.
and the corresponding URL the user visited. The authors assert that the difference between the index.dat and history.dat file is that a history.dat file is saved in an ASCII format rather than binary [Jones 2010].

The other difference being that the history.dat file does not link Website activity with cached Web pages. This is a drawback for the investigator because views of the visited Web pages cannot be readily assembled.

To overcome this limitation with investigating Internet activity as used in Firefox Browser, they proposed using Cache View, which is a shareware tool that provides access to several Browsers. “For each cached page, Cache View provides the URL from which the page was retrieved, the name of the cached file as stored on the local system, the file size, file type, the time it was last modified, the download date and its expiry (if applicable)” [Jones 2010]. File type definitely includes HTML Web pages for which Cache View digs down to some interesting information about email addresses as stored.

Web-based e-mail content and persistent Browser cookies are important things in the analysis and reconstruction of the subject's Internet activity. There are many Web browsing forensic tools an investigator can choose. Forensic tools FTK, SQLitebrowser, Cache Viewer, Registrar Registry manager, plist Editor Pro and IECacheView are the tools used in the project.

According to the recently (June 2010) NIST (National Institute of Standards & Technology) released an Inter agency Report, a design and architecture of a forensic Web service (FWS) that would securely maintain transactional records between other Web
services is proposed. The secure records can be re-linked to reproduce the transactional history by an independent agency. The report then is used to show the necessary components of a forensic framework for Web services and its success through a case study. The challenges that need to be overcome in regards to Web forensics were mentioned in the report. As opposed to traditional forensics implementation, applying forensics to Web service infrastructures introduces novel problems such as a need for impartiality and comprehensiveness. The primary purpose of digital forensics is to present digital evidence in legal proceedings. Therefore, the techniques used to extract digital evidence from devices must comply with legal standards. Reliability is another important issue for forensic examinations.

There are many approaches or measures to help the forensic analysis of an incident to prove or disprove the occurrence of a crime. Seunghee et al [Seunghee 2008] makes use of image files of Web URL pages of the same time that is recorded in the log files and made to properly document the evidence of a crime. These log entries serve as traces of digital evidence of the crime. Ahmed and Hussain proposed [Ahmed 2009] an automated approach to log Web URLs for forensic analysis using a user transparent approach to log the Web URLs visited by the user. Storing the log activity to a hidden default location which is defined by the system variables and storing on a logging server helps maintain the log of the visited URLs even if the user deletes the local log activity. The approach proposed by Lin et al [Lin 2008] is a forensic system that extracts timestamps and any other clue of the events that can be found in the log file.
Commercial ware is software that is the property of the producers and can be bought for use and such products are considerably safe and virus free to use, in most cases. Freeware or shareware are free to use software but may have bugs in them or unchecked dependencies. Security is the responsibility of the user in this case. The piracy of files has become a threat to the copyrights and confidentiality of information on the Internet. Campidoglio et al [Campidoglio 2009] describe the problem and suggest Digital Rights Management (DRM) systems to protect the legal rights of the information. The authors further explained the various rights, laws against piracy and effects of piracy. Campidoglio et al are confident that the DRM systems surely helps support the legal rights associated with the digital content.

The hackers and phish try to circumvent the preventive measures taken by the client side defensive software. There are many software’s which detect malicious sites and report that to the user. One such approach is proposed by Chou et al by using the usage and history of the user [Chou 2004]. Chou et al say that the hackers and phish overcome the measures to protect a client side system; hence a detailed study in the field is necessary to find a way to get a permanent solution for hacking and phishing.

In Web forensics, new techniques are developed by structuring and analyzing the existing techniques and using the overlooked content in the Web data [Sen 2006]. A well-structured hierarchical methodology is proposed. The click records are analyzed and integrated with the Web data warehousing. These data used to study the visit behavior and track and understand the user’s decision on buying a product. Hence loyal customers can be identified [Sen 2006].
Michael et al [Micheal 2009] proposed a tool to reconstruct the browsing activity like a slideshow unlike some of the tools which parse the cache into URLs. Web Cache Illuminator and IE History & Cache Viewer are the tools which can parse the cache to URLs. This tool can effectively show the intension of the user because the investigator can visually inspect the activity and help in deeper understanding of the activity and specific intensions of the user. But the drawbacks of this tool are that the client side scripting interaction is totally lost. Whenever the URL is accessed, the older version of Web page is lost and is overwritten. There are some compatibility problems with the CSS and AJAX technology files. [Micheal 2009]

Murillo et al explains how IE Browser deletes the history and ways to recover the deleted history. A detailed Firefox forensic analysis is also presented using forensic utility tools. Murillo et al proposes an algorithm to recover deleted SQLite entries based on known internal record structures. [Murillo 2009]
2 WEBFORENSICS

The port number 80 is the standard port for Websites and is open for lot of security issues. This is the port which listens to requests from a Web Client. The potential attacks enter into the system through this port. Web forensics is carried out on both client side and server side. While the server side forensic evidence helps an investigator progress towards a conclusion, the client side evidence provides potentially very strong and detailed evidence. Both server side and client side forensic evidence are sometimes insufficient for ascertaining the occurrence of an activity. Intermediate logging locations like application server logs play a crucial role in proving someone’s guilt. A personal interview of the accused helps to carry out investigation more effectively.

2.1 Definitions:

2.1.1 Activity

Activity is any event which involves human intervention in changing, adding or deleting system variables and system state. An activity can be requesting a Web page, downloading a file from Internet, changing the preferences of a Browser etc. An activity can be represented (and/or results in) by a change in the system state. Not all the activity is logged.

2.1.2 Cross Site Request Forgery

This is a one click access given to the requesting software which could potentially be an attack. This type of attack can happen because of the trust the user has in the Website or the trust the Website has in the user. This trust can be easily misused to attack the machine.
2.1.3 Cross Site Scripting

This kind of an attack is basically due to the addition of client side script in to the Web page to attack on a server to put the server’s security at risk.

2.1.4 Poison Null Byte

This is a kind of attack where the hacker passes the null character in the places where the null character is not valid through applications which allow null characters.

2.1.5 SQL Injection

This kind of an attack exploits the vulnerability in the database. The SQL query to the database is manipulated in such a way so that the result is not the intended result but the other data is also retrieved.

2.1.6 Trip Wires

These are a kind of alerting strategy that some of the firms use for detecting the hackers and their activity. An alert is sent to the security agency whenever some suspicious activity occurs.

2.1.7 Honeypots

This is a tricky trap set by the software firms to attract the hackers. The honeypot is a system that appears to be in network but actually it is not a part of the network. The system has superficial information which seems to be very attracting to the hackers. More than one honeypot makes a honeynet. The spammers or hackers use honeypot detection systems as tools against the honeypots and honeynets.

2.1.8 Access Control System

This is another layer of security restricting the illegal entry of any unauthorized user. It restricts the entry of unauthorized requests from malicious sources.
2.1.9 Encryption

Encryption is needed for securing the privacy and integrity of the authorized user. There are various methods of encryption in the field of computer security.

2.1.10 Forensic Utilities

These are the tools available for forensic analysis and investigation of the digital evidence. These forensic tools are used to recover deleted files and folders, create image of the disk, have a closer look at the registry entries etc. Examples of forensic utility are FTK, Encase, Prodiscover etc.

2.1.11 Digital Finger Print

This is a binary string in the coded format to identify the data files uniquely. The encryption algorithms, hashing algorithms are used to generate such digital finger prints. Each finger print generated by for files is unique and refers to single file. Hence any change in the file can be known by just generating a finger print and comparing it to the original finger print.

2.1.12 Suspicious Character/ Hazardous character

This is the character which is identified to be suspicious meaning not the general one but might be a foreign character generally introduced by the software accessing the files. Generally these characters can be identified not easily but finding it becomes more complicated when such strings are used along with encryption technologies.

2.1.13 Automated CGI scanning utilities

These are the utilities used by the hackers to scan the cgiscript on the server to hack the confidential information on the server. This can give access to the confidential information stored on the server.
2.1.14 Digital Evidence

Digital evidence involves taking an image of the suspect’s computer and investigating it. But for security reasons, the total computer may not be accessible to the investigator. So, one has to intelligently take the images of the necessary files and areas of the suspect’s computer.

2.1.15 FTK (Forensic Tool Kit)

Forensic tool kit is a software which is used for forensic analysis of files and folders. It is distributed by the AccessData. There are many components in this product each offering excellent forensic tools for investigating a case. FTK supports the files from Encase.

2.1.16 Encase

Encase is a forensic software to analyze the digital evidence. Encase is used for data procurement, data recovery, searching and parsing the files and indexes.

2.1.17 Prodiscover

Prodiscover is a very dominant security tool that empowers the investigators to locate data on a computer disk and help generate reports for concluding about the occurrence of a crime. It cross examines the files recovered using hashing techniques.

2.1.18 Registrar Registry Manager
This is a forensic tool used to view and edit registry. It also has the capability of comparing the registry keys. It is safer than regedit and offers registry defragmenter. All the registry keys and their descriptions are very nicely displayed. The Figure 2.1 shows the registrar registry manager displaying Firewall Rules.

![Figure 2.1 Displaying Firewall Rules](image)

2.2 Server Side Forensics:

Some of the information is found on the Webserver logs and Application Server logs. But most of these don’t grant access to the HTTP information like headers and requests. For example “POST”. The hackers may also try to hack the source code for server side scripts.
To know if the attack was done by an application, the following information is needed.

(i) Date

(ii) Time

(iii) IP Address of the client

(iv) HTTP method used

(v) URL

(vi) HTTP Query used to retrieve the information from the server

(vii) A total set of headers (HTTP headers)

(viii) The full body of the request

But most of the times the full data is not obtained to ascertain the happening of the crime.

“Following a standard methodology is crucial to successful and effective computer forensics. Just as professional programmers use a thorough programming methodology, computer forensic professionals should use a thorough investigative methodology.” [Jim 2000].

Methodology to be followed when carrying out the forensic investigation:

(1) Protect the system during forensic investigation from possible data corruption/ alteration

(2) Discover all files needed for the forensic investigation
a. Web server and application server logs

b. Server side scripts

c. Configuration files of Application server and Webserver

d. Third party installed software logs and important files

e. OS logs and registry entries

The ways to acquire this evidence effectively and sufficiently is described by Seunghee et al. On an abstract view, the methodology is described in following four steps [Seunghee 2009]:

1. Selection and Pre-investigation: Only file system metadata is collected to judge if forensic investigation is necessary.

2. Tracing the recent computer usage: The cache files or the prefetch files from the applications, registry and Web Browser are examined

3. Analysis of computer usage pattern: The computer usage pattern is studied on daily and hourly usage.

4. Investigation of user files: The files that need to be extracted are known and those files are investigated to see if the suspect had tried to modify the content or extensions or he/she has tried to delete or encrypt the files.

(3) After collecting evidence group them according to the timestamp. This helps in recreating the user sessions flow. The grouping could also be conveniently done based on the user profile, browser, operating system etc.
(4) Analyze the collected data and try to recreate the activity or chain of events

(5) Summarize the findings

2.3 Obtaining Information from the Registry

Windows registry is a central hierarchical database used to store information that is necessary to configure the system for one or more users, applications and hardware devices [Microsoft 2010]. The Registry has the information which is continually referenced by Windows during operation, such as profiles for each user, the applications installed on the computer and the types of documents that each can create, hardware existing on the system, and the ports in use. A registry hive is a group of keys, subkeys, and values in the registry that has a set of supporting files that contain backups of its data [Microsoft 2010].

Examining the Windows registry reveals the operations done by the user. The Windows registry has keys which are similar to folders and values which are name/data pairs. One such entry to be examined is the

\texttt{HKEY\_CURRENT\_USER\Software\Microsoft\Internet\Explorer\TypedURLs} key which obtains all of the URLs that were typed into Internet Explorer by the current user during their Website surfing. However, it does not provide a full history on the user’s browsing, such as what links were clicked on within a Web page or what queries were made where the searches were made on a search engine Website. [Skoudias 2008]. The

\texttt{HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\UBSTOR/s} key obtains the history on every USB device that was ever plugged into the user’s system. When, the
The `/s` parameter is specified following the key, all information is recursively pulled from all items in the registry below the registry branch that was specified in the query. The `HK\EY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces` key does not only obtain the current IP address but all recently used IP configurations. Some of the forensic tools such as the FTK (Forensic Tool Kit) provide a closer look to the Windows registry entries. Such data is not accessible to Windows regedit [Farmer 2007].

Browsers don’t utilize the Registry in the way that Internet Explorer does. In Internet Explorer, the history of visited sites is maintained in a file called `index.dat`, which is referenced in the Windows Registry database. That is the reason why one can see the history contents in the `TypedURLs` key. Firefox keeps limited information in the registry. It stores its history in ASCII format in a `history.dat` file located at `C:\Documents and Settings\<user>\Application Data\Mozilla\Firefox\Profiles\x.default` in Windows XP and `C:\Documents and Settings\<user>\AppData\Roaming\Mozilla\Firefox\Profiles\clfzo15s.default`.

### 2.4 Other forms of Forensic Evidence

Cookies are files containing date, time and leaving Website information. In the case of Internet Explorer, the cookie folder contains an `index.dat` file which tracks the cookie files in the folder. Cache has the information like key or the URL, data size, last modified, expiring date and time. History tracks the Websites in folders representing weekly/daily history visited by the user and includes date/time info in the `index.dat` file.
Each day a new folder is created and each week on Sunday (i.e.; 23:59 hours) a new
text data: generated and all daily folders get merged into this folder. Each of these folders
contain index.dat file that has details like URL, Filename, Username and content. Internet
Explorer also leaves some temporary files in cache. When FTK (Forensic Tool Kit) is
used, FTK lists all these files under the “Unknown Type:” button on the overview tab
[Farmer 2007]. Temporary files and deleted files also form a strong digital forensic
evidence.

2.4.1 Cookies

HTTP protocol is a stateless protocol. Every time a request is sent to the server,
the server behaves as if it was the first time the request was made from that client. The
most common way of performing session management is via the Set-Cookie directive of
HTTP which stores a token on the client. Cookies are useful for storing small amounts of
information on the client. Cookies can be used for personalizing the page when users
browse a Web site. Either the direct information can be used, or a reference to a database
on the server can be made. Cookies are also used for storing the session information that
just lasts a session. Technically a session starts when a client accesses a particular domain
and ends when the Browser is closed. There are First party cookies and Third party
cookies depending upon which website sets the cookie. The cookie set by the site visited
by the user intentionally is called First party cookie. I an intermediate site sets the cookie
then it is called Third party cookie.

If a client requests a Web page that allows cookies, then the system checks to see
if there is a cookie already set from this Website. It then sends the cookies in the HTTP
headers. Cookies can be set to exist for a variable amount of time. It can be set to expire
within a specified amount of time or can be set to expire immediately with the session. Whenever a client requests a Webpage from a domain, it first looks for any already set cookies in its cookies jar. If any cookies are already set, then the list of cookies is sent back in the HTTP headers. $HTTP_COOKIE_VAR$ array is used to access the list. [Benson 2008]. Generally the browsers have a limit to number cookies accepted per domain. Cookies are of different types classified based on the type of information they store and their life period (the time period of its existence). They are explained as follows.

**Session Cookies**

Cookies which expire with the closing of the browser. These cookies store data specific to a user’s session and gets deleted when the session ends in other words, when the browser is closed.

**Permanent/Persistent/Stored Cookies**

Cookies that retain the user preferences and can be used to get statistical information like the amount of time spent on each website and website performance etc.

**Flash Cookies**

Flash cookies are also known as Local Shared Objects. Flash cookies are used to store a lot of information about the user activity. Comparatively, the flash cookies store more information than the normal cookies. This information is used to trace the client’s movement. Flash cookie on a client’s machine cannot be located either in a Browser or in the list of saved visible cookies saved on a client’s machine.
2.4.2 Contents of a Cookie

The cookie contains all or some of the attributes viz. Name, Value, Expiry Date, Path, Domain and Security Code. The name is a custom name, value is the value returned for name. The expiry date specifies when the cookie expires. The path is the directory under which the cookies are stored under. Generally the same domain is allowed access to the cookie but one can specify grants to two different sites from same server using the domain attribute. Security is to the number 1 if only the cookie is to be sent when requesting an SSL encrypted page.

Generally only few of the fields are present in the cookies. All fields are not mandatory but it is very helpful to have all the fields in a forensic analysis. So it depends on the Website how strongly it supports forensics.

2.4.3 Setting cookies using PHP and JavaScript

`setcookie()` function is used to set cookie. It takes all the 6 parameters described above.

```
setcookie([name string],[value string],[expires UNIX time stamp],[path string],[domain string],[name integer])
```

Example: `setcookie("fname","Frank",time()+3600,"/",boumphrey.com",1)`

Setting Cookies using JavaScript

JavaScript uses `document.cookie` property to access the cookie. It is similar to the cookie created using PHP

Example: `document.cookie = ’[cookie name]=[value]; expires=[Date (format :DY,DD MON YYYY HH24:MM:SS) UTC; path=[pathname]’`
The cookie can be rewritten by using same command keeping the cookie name for which it has to be changed and varying other parameters. The cookie is overwritten and hence called resetting a cookie.

### 2.4.4 Retrieving Cookies

Retrieving cookies in PHP is done by referring to the associative array $HTTP_COOKIE_VARS[]. The array is referenced by using the following commands:

```
echo $HTTP_COOKIE_VARS["cookiename"]; and
```

In JavaScript, the cookies are referred to by the `document.cookie` attribute.

The cookies can be edited, deleted and read to further process the client’s request. The documents in the folder which created the cookie and the subfolders in that directory can access the cookie. Apart from these the documents in the PATH variable can access the cookie.

### 2.4.5 Limitations

1. No more than 300 cookies can the Browsers can retain
2. For a particular domain, only 20 cookies can be retained.
3. Only maximum of 4K of Data can be contained by cookies
4. Cookies can be blocked by the clients

For details about how to view the cookies in each of these browsers, refer to Appendix 2. View Cookies.

### 2.4.6 Flash Cookies
Flash Cookies are stored in directories depending on the OS. In Windows, the Flash cookies are stored at `C:\Documents and Settings\<user>\Application Data\Macromedia\Flash Player` in Windows XP and in Windows 7 its stored at . Flash Cookies are files with a `.SOL` extension. The settings can be viewed only from the Adobe Macromedia Website. To edit a flash cookie, there are special editors available out there which can be used to customize what the flash cookie can store and delete the ones which the client doesn’t prefer to put on the client’s machine.

The potential security threat is posed by these flash cookies for the matter of fact that they are the sources from where a hacker can get personal data from. Customized information for many social networking Websites and personal information like login details, sometimes credit card details, game specific data for the flash games are stored in the flash cookies and are vulnerable to get disclosed to any hacker. The main drawback is that the modifications done from the Adobe Website are uncertain about the time they reflect these modifications. The settings can be reset instantly or after a cookie resetting program is run. The protective cookie of Adobe also gets deleted and the client’s computer returns the point where it actually started. There are special add-ons developed for Mozilla Firefox which can delete the Flash cookies created by any Browser. Many sites use normal cookies as a backup for the Flash cookies. This allows the flash cookies get created and retain data on a revisit to that particular Website. A sound knowledge of the flash cookies and their attributes can know all the information stored on the client’s flash cookies and the privacy of the client is at risk. The design of Websites should be in
such a way that the normal functioning/behavior of the Website should not change when these cookies are blocked.

2.4.7 Protected Mode

'Protected Mode' Internet Explorer, runs as a 'Low Privilege' process. This prevents the Internet Explorer from writing to areas of the File System or the Registry that require a higher privilege. One can read the cookies with notepad, or use WinPatrol for reading and managing them. Vista creates a set of folders and files, for use with Protected Mode' Internet Explorer. These files and folders share the same Low Privilege level as Internet Explorer. The low privilege folders have cache, history and Temp files at C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Cookies\Low. If the protected mode is turned off then these files are stored in a higher privilege location in the C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Cookies folder [Technet 2010]. Figure 2.2 shows the temp files stored in Private mode. The InPrivate Browsing is indicated by a bar saying “InPrivate” is displayed to the left of the address bar.
Figure 2.2 Temporary files stored in Low Privilege mode of IE

Figure 2.3 shows the Temporary files and cookies stored in normal mode. Both Temporary and cookies are stored in the same location as shown in the figure.

Figure 2.3 Temporary files and Cookies stored in IE
Firefox has the “Protected mode” as “Private Browsing” to hide the activity on the user’s machine. In private browsing, the visited pages history is not retained. Apart from this, downloaded items list, passwords, cookies and the form data and search bar entries are not stored for facility of form autocomplete. Temporary cache is maintained until the session of Private browsing lasts. The only things which are retained are the bookmarks during the private browsing and the downloaded files. The cookies are stored in C:\Users\<user>\AppData\Roaming\Mozilla\Firefox\Profiles\<some text>.default location.

Google Chrome also has this protected browsing and this is called the “incognito mode”. This helps the user to browse in stealth mode. Similar to Firefox, no history, no downloaded file list, no cookies etc. are stored. The cookies are stored in the C:\Users\<user>\AppData\Local\Google\Chrome\User Data\Default folder in the cookies file. The only stored items are the downloaded files. Also the changes to settings and bookmarks are stored. When the private browsing is turned on, there appears a little detective icon in the left top corner of the browser window indicating the private browsing is turned on. Figure shows the location of Cookies folder for Google chrome browser.

Safari remember the visited pages and all events in history, bookmarks etc. To enable privacy, the browser has a “Private Browsing” facility which helps the users to keep their activity undisclosed to any other user using the same system later. In other words, the browsing activity is not documented anywhere to help user’s privacy. C:\Users\<user>\AppData\Roaming\Apple Computer\Safari\Cookies\Cookies.plist is the
location for storing cookies in Safari. A sample preview of the cookie is shown in the Figure 2.4.
The private browsing is indicated by an icon saying “PRIVATE” is displayed in the address bar.

The protected browsing or the private browsing is helpful to the users to conceal the details of their browsing activity. Because the browser in Protected Browsing runs as a low priority or a low privileged process, no activity is being logged into the Registry. The browsers however don’t store any footprints of the activity in this mode. So it is a security bottleneck in the browsers. This creates serious problems for the forensic investigators trying to trace the activity. However the Downloaded files are not deleted. So if there are any files which are created in that period of time can be considered for potentially being forensic evidence.
3 SYSTEM DESIGN

3.1 Overview of the system

The file formats and the relevant file paths for IE, Mozilla Firefox, Chrome and Safari Internet activity files are studied in the Windows 7 operating system and those results are documented.

A fresh or wiped system was taken for study and a basic installation of Windows 7 was done on the machine. The directory structure and contents of files after the installation were examined. After installation, the changes in the directory structure and the changes in content of files were noted for a very detailed investigation. The registry changes were also noted as this is a potential source of evidence. The Browsers Internet Explorer, Chrome, Safari and Mozilla Firefox were installed and again the changes in the system were noted.

The Browsers were used to browse top 100 Websites according to quantcast.com. Some of these top 100 Websites store cookies. The history, cache and cookies were examined for changes. The changes were noted and cross examined with those of the new installation. Traitorous activity was simulated by deleting files and folders. The state of the system was again noted and examined for changes. The deleted files and folders were subjected to recovering attempts.

The project finds a way to reconstruct all the activity. This helps in proving the malicious activity on the very popular Web Browsers namely Internet Explorer, Firefox, Google Chrome, and Apple Safari. Each of these Browsers uses a different way of maintaining the history or the user activity. As the user specific data stored in Browsers
is reflected in some folders and files, a detailed study was performed on these as listed below.

3.2 Information Analyzed

3.2.1 Internet Explorer

The Temporary Files folder at the location

\( C:\Users\<user>\AppData\Local\Microsoft\Windows\Temporary Internet Files \)

has the temporary files. The cookies stored using Internet Explorer is also stored at the same location. The cookies have their names in a special format. IECache Viewer can be used to view the cookies and other cached files. Counting cookies can be done by filtering the list of files based on the type of name they are given.

3.2.2 Firefox

The default location for cookies associated with Firefox for Windows is stored in profile folders at the following location

\( C:\Users\<user>\AppData\Roaming\Mozilla\Firefox\Profiles\<profile folder> \)

[Mozillazine 2010]. Some files and folders which store or reveal the user data are as follows [Mozillazine 2010]:

3.2.2.1 bookmarkbackups:

The bookmarkbackups folder contains bookmarks-(date).json files in Firefox 3.0 and above versions. Bookmark Backup is a simple extension that keeps bookmarks and optionally other Firefox settings safe. Each time Firefox is closed, a copy of the bookmarks file was made to a backup location. When Firefox's bookmarks became corrupted or lost, the most recent uncorrupted backup copied into the profile folder.
helped in retaining the bookmarks. Daily rotating backups of bookmarks are stored in
places.sqlite. places.sqlite is created using bookmarkbackups in Firefox 3.0 and above
versions. In the older versions, bookmarks.html is used to create places.sqlite.

3.2.2.2 Cache:

Firefox maintains a cache where it stores temporary files such as Web pages and
other online media downloaded from the Internet. It can be seen in a browser by just
typing about:cache in the address bar.

3.2.2.3 Offline Cache:

It is a Second disk cache for off-line usage. The locations which have custom
profile folders had this folder. The location can be found out by looking at the cache.

3.2.2.4 Extensions:

All the installed extensions were stored here. Inside the extensions folder, there
were folders for each extension and theme installed for the Browser. The removal of
extensions did not have an effect on the regular operation of the browser. Some of the
extensions (like Adblock Plus) were not possible to be removed manually. These
extensions were removed only with the help of the application which added the
extension. These extensions were flexible to be disabled when desired.

3.2.2.5 Microsummary-generators:

Microsummaries are regularly-updated short summaries of Web pages. They
provided more useful information about pages than static page titles, and they got
regularly updated as new information became available. Microsummary generators are firefox addons which can generate microsummaries for those sites which don’t provide them by default. This was identified by the <Link> tag having rel attribute set to “microsummary” and the matter in the href attribute is used to generate microsummaries.

3.2.2.6 Minidump:

The minidump file format contained the data about crash on Windows. It had a .dmp extension. It contained a dump of values on the stack of the crashing thread.

3.2.2.7 profiles.ini:

This file contained information which was used to keep track of Firefox and profiles. Deleting this file created a new profiles.ini the next time when Firefox application was started. The old profiles were not visible in the profile Manager. This file along with the profile settings was shifted to another system and an identical user was created.

Table 3.1 shows a tabular representation of the list of folders used to review the user data. It clearly shows the description of each folder.

<table>
<thead>
<tr>
<th>Name</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bookmarkbackups</td>
<td>1.5 and</td>
<td>Daily rotating backups of bookmarks.</td>
</tr>
<tr>
<td></td>
<td>above</td>
<td></td>
</tr>
<tr>
<td>Cache</td>
<td>Linux - all versions.</td>
<td>Temporary storage for the recently used URLs</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>OfflineCache</td>
<td>3.0 and above, as noted</td>
<td>Second disk cache for off-line usage. Note: Only profiles in custom locations on Windows include the OfflineCache folder. about:cache was typed in the browser to find the location and view the list of entries.</td>
</tr>
<tr>
<td>extensions</td>
<td></td>
<td>Installed extensions/addons</td>
</tr>
<tr>
<td>microsummary-generators</td>
<td>2.0 and above</td>
<td>Regularly-updated brief compilations of the most important information on Web pages.</td>
</tr>
<tr>
<td>minidumps</td>
<td></td>
<td>For Crash Reporter</td>
</tr>
<tr>
<td>profiles.ini</td>
<td></td>
<td>Keeps track of profile location. This folder was edited to point to a moved profile folder. When deleted, it regenerated along with a new default profile folder upon program restart.</td>
</tr>
</tbody>
</table>

Some files and folders which can be examined for user activity are as follows

[Mozillazine 2010]

3.2.2.8 .autoreg:
When changes are made to the Extensions datasource - new items are installed, old items uninstalled, enabled or disabled, a .autoreg file is written to the profile directory as well. This tells the startup code that the system has been modified, so that it destroys the component registries, finishes pending transactions and regenerates metadata appropriately.

3.2.2.9 blocklist.xml:

blocklist.xml contains a list of add-ons that Mozilla considers to be harmful to the user. The add-ons already installed and are on the block list are disabled and any attempt to install any add-on on the block list result in an error. This can be managed from time to time according to user preferences also.

3.2.2.10 bookmarks.html:

bookmarks.html and bookmarks.bak In earlier versions of Firefox, bookmarks are stored by the bookmarks.htm and the latest versions use places.sqlite to store bookmarks. When Firefox is started and bookmarks.html is either missing or reduced to "0", bookmarks.bak is used, if present, instead of the default set of bookmarks.

3.2.2.11 bookmarks.html.moztmp:

bookmarks.html.moztmp is a temporary file used when writing bookmarks. The presence of this file indicates that writing to the bookmarks file has failed and can also cause the creation of multiple bookmarks-(number).html files.

3.2.2.12 cookies.sqlite:
It has the cookies but not the history. It contains the information like the login information, session data and preferences. This is a replacement for the cookies.txt in the Firefox 2.0 and earlier versions of Firefox.

3.2.2.13 downloads.rdf and downloads.sqlite:

This is a place where the information about the downloaded files is stored. Deleting downloads.rdf clears the download history and a new file is created on start up or when the application first needs to write to the file. Download history is stored in downloads.sqlite instead of downloads.rdf.

3.2.2.14 Crash Reports:

The Crash Reports folder contains two subfolders: pending and submitted. submitted contains reports that have been submitted, while pending contains reports that have not. Each file in these folders represents one report.

Firefox also supports installation on a small drives like thumb drives. Firefox unlike Internet Explorer, stores much of its tracking information in files instead of registry.

3.2.3 Safari

Safari stores the user's browsing history in .plist files. There are three files of interest in Safari:

1. version.plist which contains detailed information about the installed Safari version;
2. *info.plist* which contains system wide configuration information and records downloaded files; and

3. *Cookies.plist* stores cookie information provided by Websites. [Jones 2010]

Cookies can be counted by counting the number of files in this folder. The browser offers a directory structured representation of cookies.

### 3.2.4 Google Chrome

Google Chrome stores the user data at

*C:\Users\<user>\AppData\Local\Google\Chrome\User Data\*. Figure 3.1 shows the structure of the User Data folder. This is pictorial representation of the UserData in Google Chrome.

![Figure 3.1 User Data](image)

The User Data folder has the Local State, Safe Browsing, Safe Browsing filter used to filter the type of content the user would not like to view and has a Default folder that has all the Cache information, Cookies, History and Plug-in Data. The User Data
folder is used by chrome to maintain session information so it identifies a person based on the information in the folder. This is a security threat as the User Data folder can be copied and hence the identity is replicated. This is a potential threat in the form of identity theft. On the other hand, Internet Explorer has a security setting that allows the browser specific settings to be copied when the profile folder is copied. But while copying the profile folder to another system, the validations are not copied over. The cookies can be counted by counting the number of files in the cookies folder.

Google Chrome has two files for ensuring safe browsing. The Safe Browsing Bloom and Safe Browsing Bloom Filter 2 files are responsible for storing the malicious Websites information. The malicious website URL is converted into a canonical form/s. Each URL entered is checked against these set of malicious Website URLs and filtered. Long hash is computed \( N \) number of times and the value is multiplied by a scale factor. \( N \) addresses of bits are computed in a bit array. If all the bits are set then the site is malicious. So logically it can store about 1 million malicious Websites.
4. TEST EVALUATION AND RESULTS

Forensic tools FTK (Forensic Tool Kit), Registrar Registry Manager, Cookie Editors and Cache viewers like plist Editor Pro, IECacheView were used to help reconstruct all the activity done by the user. The project is carried out on a fresh installation of Windows 7 Professional edition on a virtual machine running in VM player. The host system is Windows Vista Home Premium edition.

4.1 Fresh Installation

The evidence of an activity is stored in various places in the system and those locations are discussed in the later part of this chapter. The registry entries get automatically modified, history, cache and cookies stored can reveal the details of an activity. Initially with the default installation the Cookies folder at 

C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Cookies was empty. The C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Cookies\Low had some cookies which represents the low privilege browsing done before the report was carried out. There are no Flash cookie files in the default installation. The recently used IP configurations and the download register key did not change after installing the browsers. In other words, the installation of browsers did not have much effect on the registry. The temporary files were not many and no cookies were stored. The Cache and History had the recently visited Website URLs in the browsers.
4.2 After Browser Installation

After the installation of all other browsers (viz Firefox, Chrome and Safari), the Macromedia Flash was also installed. As a result *Macromedia* folder was created under *AppData*. Subfolder Flash player has *#SharedObjects* and *macromedia.com* folders both of which have cookies in their subfolders. The flash cookies are stored in a `.sol` format.

A program to open all the top 100 websites according to quancast.com

The registry preview is shown in Figure 4.1

![Figure 4.1 Flash Player initial preview](image)

4.2.1 Internet Explorer

The data of Internet Explorer Web Browser was stored in the

*HKEY_CURRENT_USER\Software\Microsoft\InternetExplorer* key [Farmer 2007]. This key contains three sub keys within it. Among which the

*HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main* is the key that was
analyzed for obtaining user’s settings in Internet Explorer such as search bars, start page and form settings [Farmer 2007]. The HKEY_CURRENT_USER\Software\Microsoft \Internet Explorer\Download Directory key demonstrates the last directory where a downloaded file was stored. This was a result of index.dat in which the Web history was stored. There are several index.dat files stored at different locations in Windows 7. These locations are C:\Documents and Settings\<user>\Cookies\index.dat, C:\Documents and Settings\<user>\Local Settings\History\History.IE5\MSHistXXXXXXXXXXX\index.dat, C:\Documents and Settings\<user>\Local Settings\Temporary Internet Files\Content.IE5\index.dat. Similarly, Netscape and Firefox use history.dat to store the Web history. The HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List key was examined to know the list of applications that accessed outside the firewall [Farmer 2007]. Figure 4.2 shows the User preferences stored by Internet Explorer.
4.2.2 Firefox

Firefox also supports installation on a small drives like thumb drives. Firefox unlike Internet Explorer, stores much of its tracking information in files instead of registry. Individual folders are used to store user data, so it’s easy for the user to totally wipe out the folders without leaving any traces. The history was stored in 2 SQL tables: "moz_history" and "moz_historyvisit" [Mozilla 2010]. Firefox files are located in the following directory [Jones 2010]: \Documents and Settings\<user>\Application Data\Mozilla\Firefox\Profiles\<random text>\history.dat.

Flash player installation also added a Firefox plug-in to support the flash objects. A preview is shown in Figure 4.3

Figure 4.3 Mozilla plugin preview
This is an example of changing the registry by another program. A potential attack can be to just change the registry value as some virus infected site’s URL.

Example; [HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main] "Start Page"="http://www.somecrazyvirus.com/"

The sites like https://www.blogspot.com have both secure and insecure data. The insecure data does not comply with the security of HTTPS. Whenever there is any insecure content on the requested page, the Firefox browser prompts the user and asks if the user want to proceed.

4.2.3 Safari

The default Web Browser in Mac OS X is Safari. The Safari Web cache is located at ~/Library/Caches/Safari. There are a large number of other folders contained within the ~/Users/"USER"/Library/Cache folder that can be of interest for investigators to look at. ~/Library/Preferences/com.apple.finder.plist. Within that file is "FXConnectToLastURL". This entry shows the last file servers the suspect connected to. The entry "CFURLAliasData" has the names of file servers accessed, disk images mounted, and sometimes names of DVDs (although they seem to be Apple authored only) that have been mounted on within the Finder. The entry "recent-folders" shows the last batch of folders that were accessed [Mac Forensic Lab 2010]. Tools like Pasco and FTK are suggested by Jones and Belani to do forensic analysis of Browsers [Jones 2010].

In Safari for Windows, the History, cache and bookmarks are stored at

C:\Users\<user>\AppData\Roaming\Apple Computer\Safari\History.plist,
C:\Users\<user>\AppData\Roaming\Apple Computer\Safari\Bookmarks.plist,
C:\Users\<user>\AppData\Roaming\Apple Computer\Safari\Downloads.plist,
C:\Users\<user>\AppData\Roaming\Apple Computer\Safari\LastSession.plist,
C:\Users\<user>\AppData\Roaming\Apple Computer\Safari\TopSites.plist and the form values are stored in C:\Users\<user>\AppData\Roaming\Apple Computer\Safari\Form Values.plist.

The cookies are stored in the C:\Users\Laxmi Narsimha\AppData\Roaming\Apple Computer\Safari\Cookies/Cookies.plist file.

4.2.3.1 Cookies.plist:

A sample entry in the Cookies.plist looks as shown in Figure 4.4

It has sections which states different tags and corresponding information is stored in a metadata format.
The tree structure of the cookies folder is shown in the Figure 4.5.

![Figure 4.5 Cookies.plist tree view](image_url)

The nice thing about Safari is that it also maintains the feeds for the bookmarks in metadata documents which are used for quick view of the feeds when a user is looking for.

### 4.2.3.2 Google Chrome

The cached website address entries and history is stored in the

\[ HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs \]

The addresses in the key are listed as Ur11, Ur12, Ur13 and so on. These URLs are numbered in a consecutive manner. Below is list of URLs shown in registry in the Figure 4.6
While investigation on the test system it was observed that the user data deleted from the Google chrome was recovered but Safari or Mozilla files were not totally recovered by the FTK. This is illustrated in Figure 4.7
The reason for this is that the temporary files are stored at a memory location is reused to store other temporary files if there is space contention and/or the temporary file becomes unimportant. Whenever there is a rewriting of the same memory location it is impossible to recover the erased data. The modern hard disks are having great bit density and the very small track sizes. So, overwritten parts of hard disk cannot be recovered using the forensic tools. Even the sophisticated procedure used to recover such data will be able to partially recover it. This procedure requires physical damage to the hard drive under very controlled atmospheric conditions. Hence the FTK was unsuccessful in retrieving the temporary files.
4.3 Flash Cookies

The websites which have flash objects running sends flash cookies to the user’s system. For example youtube.com stored cookies in high privilege cookies folder

C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Cookies and also stored flash cookie on the system C:\Users\<user>\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\AJYRWPL\www.youtube.com folder. Websites like youtube.com, hulu.com, imdb.com and amazon.com etc. save a normal cookie and a flash cookie. In case of any missing flash cookie, the normal cookie is helpful in building the flash cookie.

This was simulated by deleting the flash cookie and tried to recover it. But FTK could not identify it to recover. Such flash cookies were rebuilt once the Website was revisited. Using successfully recovered results one can partially show the proof/disproof of a certain activity. So further investigation should be interviewing and common sense must be applied to take a decision on the occurrence of the crime.
5. CONCLUSION AND FUTURE WORK

An activity on a system is recorded in various locations in several forms. When closely observed, the activity done by the user is understood. The digital evidence is used for forensic investigations and to undo some activities which are offensive or malicious or improperly terminated (for example System Restore). The Registry is a very potential place to look at when a forensic investigator is trying to trace the evidences of any activity. To trace an activity with respect to Web, the areas that were looked for evidences are history, cache, cookies, browser specific data, browser specific preferences and the registry. All these areas reflected the expected changes in the system state and hence were helpful in reconstructing the whole activity. But deleting any of the evidences would seriously disturb the process of investigation.

Mozilla Firefox has the portability of user profile. Copying the profile folder creates a user. When the profile folder was deleted, then a new user profile folder was created. So the investigators should check the timestamp the profile folder to know when it was created.

The Apple Safari stores all its data in totally different format which is not easily editable. Mozilla Firefox has some security add-ons but they have very frequent updates. Apple Safari is slower than the other browsers as it has very complex JavaScript code running in the background. Not all applications and websites support Safari. Google chrome is a light weight browser. It was found that chrome is very good for regular browsing. It has become popular very soon after it came into existence. The most
vulnerable Web Browser is Internet Explorer. This browser supports many applications and is most widely used browser. Some of the websites like blogspot.com and others have secure and insecure data on the same page giving the user an option to take the risk or just avoid. But the user preferences made on these websites are saved in the user's profile. This can be vulnerable as most of the users generally forget their settings. So browser specific choices should be made wisely and any preferences that would involve any security issue should be avoided. For example allowing a plugin to run in the browser can be vulnerable. Such preferences should not be saved and the plugins should be allowed to run only when it originates from a trusted source. This ensures safe browsing.

IE and Firefox prompt about the insecure content but the chrome and safari do not indicate the presence of insecure content. However it is preferable to have a warning before attempting to view insecure content.

The different ways of storing various cookies by the top 100 Websites was studied. Figure 5.1 shows the cookies from various Websites stored on the test system.
Cookies help the websites learn more about the user preferences and their behavior. Cookies also help in knowing the user's opinion on certain products or page. This information is used to enhance their services.

Sometimes the firewall may block a Website if the certificate is not verified properly. The reliable sites need to be added to the trusted Websites to access the site. This generally happens with the customized Websites in professional environments where sensitive scripts run on the website.

The activity done on a system was successfully reconstructed using various logs and internet footprints (evidences) left on the user's system. An efficient way of recording the activity is to maintain the screenshots of the Web pages and keep them very safely. Mapping these screenshots to the URLs in the history can help visualize the activity.
better. Safari maintains the screen shots of the Web pages from time to time. The location where it stores these screen shots is 
\( C:\Users\<user>\AppData\Local\Apple Computer\Safari\Webpage Previews \). Figure 5.2 shows the screenshots of websites saved by Apple Safari whenever the site was visited.

![Figure 5.2 Screenshots of websites stored in Safari](image)

This project can be used to develop a tool that can give a sequence of client’s activity taking the server side logs, locally stored screenshots and the Web history. This can be consistent only if no files are deleted. This can be a great contribution to the Internet community.
BIBLIOGRAPHY AND REFERENCES


[Murillo 2009] Murillo Tito Pereira; "Forensic analysis of the Firefox 3 Internet history and recovery of deleted SQLite records, Digital Investigation" Volume 5, Issues 3-4, March 2009, Pages 93-103 (Feb 2009)


[Seunghee 2009] SeungBong, Lee; Jewan, Bang; KyungSoo, Lim; Jongsung, Kim; Sangjin, Lee; "A Stepwise Methodology for Tracing Computer Usage", Fifth


APPENDIX A. STARTING PRIVATE BROWSING

Internet Explorer

1. Open the Internet Explorer

2. From the Tools menu, select InPrivate Browsing option

Figure A.1 shows how to select the Private Browsing mode in IE

Figure A.1 Starting Private Browsing in IE

4. Figure A.2 shows the Private browsing window in IE.
Firefox

1. Open the Firefox Browser.

2. Select the Tools menu and from the dropdown list, select Start Private Browsing option.

The figure A.3 explains steps to start Private Browsing in Firefox
Figure A.3 Starting Private Browsing in Mozilla Firefox

3. The figure A.4 shows the Private Browsing Window
Chrome

1. Open the Chrome browser

2. In the right corner adjacent to the address bar, there is a wrench shaped small icon. Clicking the icon lists various options.

3. Select “New incognito window”

The figure A.5 shows the way to access this option.

4. The incognito window or the Protected mode of browsing in Chrome looks as shown in the figure.
Safari

1. Start the Safari Browser

2. On the rightmost corner in the browser, there appears a small icon depicting gear. This represents setting option which can be used to customize the toolbar. Clicking on that lists a number of options.

3. Select “Private Browsing…”

Here is the figure A.7 showing the option in the browser.
Figure A.7 Private Browsing window in Apple Safari

4. Private browsing window looks like similar to the Figure A.8

Figure A.8 Private Browsing window in Apple Safari
APPENDIX B. LOOKING FOR COOKIES

Internet Explorer

1. Open the Internet Explorer.

2. Click on the wrench icon and select Options → Under the Hood (tab)

→ Click Content settings → Cookies → Show Cookies and other site data. Figure B.1 and B.2 shows the illustration of these steps.

Figure B.1 Cookies in IE – 1
3. This pops out another window showing the list of cookies.

Figure B.2 Cookies in IE – 2

**FireFox**

1. From the select Tools Menu → Options

2. Go to the Privacy tab → Show Cookies

3. Figure B.3 shows the process to look at the cookies in firefox
Google Chrome

1. From the select Customize and control Menu \(\rightarrow\) Options (like a wrench symbol)

2. Go to the Under the Hood tab \(\rightarrow\) Find Content settings \(\rightarrow\) Cookies

3. Click on “Show cookies and other site data” as Figure B.4 below shows the process to look at the cookies in Chrome.
Figure B.4 Cookies in Chrome
APPENDIX C. PROGRAM TO VISIT WEBSITES

Here is a small program written for cmd for windows 7. Preliminary requirement is that the environmental PATH variable must be set to include all the paths for the browser executable files on the system. There are four scripts written for each of the four browsers (viz. Internet Explorer, Mozilla Firefox, Google Chrome and Apple Safari). There are 10 input files each containing a list of 10 websites.

The steps to set the environmental variables in Windows 7 are shown below.

Windows→Computer→ (right click) Properties . Refer to Figure C.1

Figure C.1 Setting Environmental variables I

The system window comes up. Click on the Advanced system settings. This pops up the system properties window. Under the Advanced tab find and click the button Environment Variables. Here the PATH variable needs to be set. If there is no PATH variable then a new one needs to be created and the address where the browsers are located should be set. For Windows 7, the paths for each browser is listed in the Table C.1
Table C.1 Locations of Browsers in Windows 7

<table>
<thead>
<tr>
<th>Browser</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer</td>
<td>C:\Program Files\Internet Explorer\</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>C:\Program Files\Mozilla Firefox\</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>C:\Users&lt;user&gt;\AppData\Local\Google\Chrome\Application\</td>
</tr>
<tr>
<td>Apple Safari</td>
<td>C:\Program Files\Safari\</td>
</tr>
</tbody>
</table>

These values need to be semicolon delimited refer to the Figure C.2. Click ‘OK’ on the three windows and the system is then ready to run the script. Go to the directory where all the files are stored and execute each script with each of the inputfiles which have urls of the websites that needs to be visited.

Figure C.2 Setting Environmental variables II
How to Run

Edit each script using notepad to give input file name. Save the script with .bat extension.

Double click the batch file and the browsers open in new windows/tabs depending upon their settings. After all the windows are opened, the command prompt prompts the user to input so that the program can terminate.

------------------------------------------------------------------------------------------------------------

Batch file for Internet Explorer

------------------------------------------------------------------------------------------------------------

:: Batch file for Internet Explorer
@echo off
:: Turn off the output on command line
for /f %%i in (list10.txt) do iexplore %%i
:: Iterate through the list of websites in the list<number>.txt file
echo closing the IE.....
pause
:: Wait for the user input to close the Browser
taskkill /F /FI "imagename eq iexplore*"
:: Kill the Browser process
pause
Batch file for Mozilla Firefox

:: Batch file for Mozilla Firefox
@echo off
:: Turn off the output on command line
for /f %%i in (list4.txt) do firefox %%i
:: Iterate through the list of websites in the list<number>.txt file
echo closing the Firefox.....
pause
:: Wait for the user input to close the Browser
taskkill /F /FI "imagename eq firefox*"
:: Kill the Browser process
pause

Batch file for Google Chrome

:: Batch file for Google Chrome
@echo off
:: Turn off the output on command line

for /f %%i in (list7.txt) do chrome %%i

:: Iterate through the list of websites in the list<number>.txt file

echo closing the Chrome.....

pause

:: Wait for the user input to close the Browser

taskkill /F /FI "imagename eq chrome*"

:: Kill the Browser process

pause

------------------------------------------------------------------------------------------------------------

Batch file for Apple Safari

------------------------------------------------------------------------------------------------------------

:: Batch file for Apple Safari

@echo off

:: Turn off the output on command line

for /f %%i in (list5.txt) do safari %%i

:: Iterate through the list of websites in the list<number>.txt file

echo closing the Safari.....

pause
:: Wait for the user input to close the Browser

taskkill /F /FI "imagename eq safari*"

:: Kill the Browser process

pause

List of top 100 Websites according to quantcast.com

List1.txt

http://www.google.com

http://www.facebook.com

http://www.yahoo.com

http://www.youtube.com

http://www.msn.com

http://www.live.com

http://www.amazon.com

http://www.wikipedia.org

http://www.microsoft.com

http://www.ebay.com

List2.txt

http://www.blogspot.com
http://www.aol.com
http://www.blogger.com
http://www.answers.com
http://www.twitter.com
http://www.craigslist.org
http://www.ask.com
http://www.ehow.com
http://www.bing.com
http://www.about.com

List3.txt

http://www.myspace.com
http://www.weather.com
http://www.mapquest.com
http://www.wordpress.com
http://www.adobe.com
http://www.photobucket.org
http://www.reference.com
http://www.godaddy.com
http://www.paypal.com
http://www.walmart.com

List4.txt
http://www.go.com

http://www.att.com

http://www.hulu.com

http://www.huffingtonpost.com

http://www.comcast.com

http://www.windows.org

http://www.imdb.com

http://www.break.com

http://www.monster.com

http://www.linkedin.com

List5.txt

http://www.webmd.com

http://www.pandora.com

http://www.stumbleupon.com

http://www.match.com

http://www.cnn.com

http://www.whitepages.org

http://www.flickr.com

http://www.target.com

http://www.associatedconnect.com

http://www.bankofamerica.com
List6.txt

http://www.manta.com
http://www.chase.com
http://www.apple.com
http://www.hubpages.com
http://www.mybloglog.com
http://www.chinaontv.org
http://www.digg.com
http://www.cnet.com
http://www.filmanx.com
http://www.thefind.com

List7.txt

http://www.yellowpages.com
http://www.local.com
http://www.careerbuilder.com
http://www.nytimes.com
http://www.tripadvisor.com
http://www.bbc.co.uk
http://www.tumblr.com
http://www.accuweather.com
http://www.evite.com
http://www.legacy.com

List8.txt

http://www.comcast.com
http://www.washingtonpost.com
http://www.hp.com
http://www.tmz.com
http://www.chacha.com
http://www.searchassist.com
http://www.dailymotion.com
http://www.drudgereport.com
http://www.mtv.com
http://www.people.com

List9.txt

http://www.netflix.com
http://www.suite101.com
http://www.yelp.com
http://www.usps.com
http://www.wellsfargo.com
http://www.typepad.com
http://www.simplyhired.com
http://www.squidoo.com

http://www.ap.org

http://www.merriam-webster.com

List10.txt

http://www.bestbuy.com

http://www.bizrate.com

http://www.wikia.com

http://www.zynga.com

http://www.weatherbug.com

http://www.wunderground.com

http://www.examiner.com

http://www.jcpenny.com

http://www.merchantarticle.org

http://www.twitpic.com