Unit II

CHAPTER 5

E-mail Forensics

Introduction

- Email is used to communicate with the two parties. Where file transfer taken place between the two servers on a particular port number. A client side application is required to compose an e-mail.
- The examples of client side application are yahoo mail, Web Client, MS Outlook, hotmail. It requires a Sender's identity, stores it as a file and then delivered to a destination user address through one or more number of servers.
- The Email communication makes the things simple, powerful and efficient. Email writing and communication have been under the focus of malicious intruders over the last few decades. Emails can be forged easily.
- Email abuse is also increasing day by day. Email crimes like spam, threatening mails, narcotic trafficking etc are also increased.

5.1 Email Clients and Servers

Q. 5.1.1 Write a short note on email forensics? *(Ref. Secs. 5.1 and 5.2)* **(5 Marks)**

- Email client message is made up of two parts that are header and the body. The header contains the information about the email origin, like the address from where it comes, how it reached to the destination and who send it. The body contains the message and attachment if any.
- Many organizations have their own mail server. Some Users dials for the internet service provider. When this user sends the mail that mail first go to the ISP server then ISP send that mail to receivers mail server.
- The message stays on the receiver server till the recipient retrieve it. An email server is a computer which runs on Unix, Windows or any other operating system. The server contains the software to manage the transmission and holds the messages.

- When we investigate the email crime, the internal corporate emails are easy to trace. They use Universal Naming Conventions (UNC) coupled with central authentication and controls. So it makes easy to find the sender and receiver of email.
- The email client performs task like listing all the messages in mailbox by displaying message header as well as the time and date of the messages. It also tells the senders and the size of the message. The client can view, compose or delete the message.
- The email server is having the list of all the accounts. It have text file for each account. When a person click the send button to send the mail. It passes the mail to the mail server with sender and receiver name and message. The server formats this information and appends it to the bottom of the recipients text file. To interact with the server the following email protocols are required.
  - **Post Office Protocol (POP) :** It stores only incoming messages. Investigation is done at the workstation.
  - **Internet Message Access Protocol (IMAP) :** This protocol stores all the messages. Copies of incoming and the outgoing messages are stored on the server or workstation or both.
  - **Microsoft's Mail API (MAPI) :** This protocol also work same as IMAP.
  - **HTTP :** This protocol is used for web based send and receives.
  - **Simple mail transfer protocol (SMTP) :** It is responsible for sending and receiving the email. It uses TCP port 25. It is easy to spoof SMTP and send the fake mail.

Syllabus Topic : E-mail Analysis

5.2 E-mail Analysis

Q. 5.2.1 Write a short note on email forensics? *(Ref. Secs. 5.1 and 5.2)* **(5 Marks)**

Q. 5.2.2 Explain the steps involved in email analysis/investigation? *(Ref. Sec. 5.2)* **(5 Marks)**

Email crime investigation or analysis contains the following steps:

1. Examine the email message	2. Copy the email message
3. Print the email message	4. View the mail headers
5. Examine the email headers	6. Examine attachment if it is there in email
7. Trace the Email.	

➜ **1. Examine the email**

When it is come into the light that email crime has happened then it is necessary to collect the evidence which is required to prove the crime in the court of law. Evidence may be gathers from the victim's computer. Evidence is the mail which the victim received.

- First take the image of machines hard drive.
- Obtain the victims machine password to open the encrypted file.
- Take the printed copy of the crime mail (including header).
- Examine the IP address of the sender's server.

➜ **2. Copy the email message into the USB key.**

➜ **3. Take the printout of the email message by using the print option available in the mail program.**

➜ **4. View the mail header**

- To check the mail header
- Open your mail.
- Right click on your mail.
- After right click menus will display. Click on view full header.
- The file header will get opened.

➜ **5. Examine the email header**

The email header contains the message header and the subject body. The email header contains the information of the email origin. You can see in the given message that the IP address of the sender's machine is sent i.e. X-originating- IP: [200.85.213.54]. It also gives the return path, and the receiver mail id.

From Suvarna Pansambal Tue Feb 2 12:16:14 2016

X-Apparently-To : suvarnashirke@yahoo.com; Tue, 02 Feb 2016 12:16:15 +0000

Return-Path : <suvarna.atharv@gmail.com>

Received-SPF : pass (domain of gmail.com designates 209.85.213.54 as permitted sender)

X-Originating-IP : [209.85.213.54]

Authentication-Results : mta1073.mail.gq1.yahoo.com from=gmail.com; domainkeys=neutral (no sig); from=gmail.com; dkim=pass (ok)

Received : from 127.0.0.1 (EHLO mail-vk0-f54.google.com) (209.85.213.54) by mta1073.mail.gq1.yahoo.com with SMTPS; Tue, 02 Feb 2016 12:16:15 + 0000

Received : by mail-vk0-f54.google.com with **SMTP id** n1so95500114vkb.3 for <suvarnashirke@yahoo.com>; Tue, 02 Feb 2016 04:16:14 -0800 (PST)

DKIM-Signature : v=1; a=rsa-sha256; c=relaxed/relaxed; d=gmail.com; s=20120113;

h=mime-version:date:message-id:subject:from:to:content-type;

bh=7AWYrxUKcsQ8uhNfa2cJrervIPR8oNJDId+M28otZas=;

b=TFIL3/WMYu9aLdGKBoSoYoWqerdG+Wjmmckw/kKA7tNfNncm1xvyqlRpOYMIO05LIq

X-Google-DKIM-Signature : v=1; a=rsa-sha256; c=relaxed/relaxed;

d=1e100.net; s=20130820;

h=x-gm-message-state:mime-version:date:message-id:subject:from:to:content-type;

bh=7AWYrxUKcsQ8uhNfa2cJrervIPR8oNJDId+M28otZas=;-Gm-Message-State: AG10YOT91xCYmn4COfUybd9MEb6HEtEU+MiOY99sDZQ6PbFlgE09G/boN2F9x MBQSk6aAFVx74W0+hLMbo5SJg==

MIME-Version : 1.0

X-Received : by 10.31.16.197 with SMTP id 66mr16543831vkq.41.1454415374794; Tue, 02 Feb 2016 04:16:14 -0800 (PST)

Received : by 10.31.151.147 with HTTP; Tue, 2 Feb 2016 04:16:14 -0800 (PST)

Date : Tue, 2 Feb 2016 17:46:14 +0530

Message-ID : <CAL1VNuOeJv075FDfSN=ENDdg_KhGNmQGizVsi9y9eA8OcX401w@mail.gmail.com>

Subject : Threat mail

From : Suvarna Pansambal suvarna.atharv@gmail.com

To : suvarnashirke suvarnashirke@yahoo.com

Content-Type : multipart/alternative; boundary=001a11436378c545c7052ac877ff

Content-Length : 542

Fig. 5.2.1 : Email Message header

6. Examine the attachments

If the mail contains any attachment then copy that attachment and also take the print of the attachment.

7. Trace the Email

- The IP address of the origination computer machine tells the owner of the email address which has been used in the possible crime that is being investigated. It may be possible that this information may be fake. So it's important to validate the evidence which you uncover. There are many sites which tell the owner associated with the domain name. For example: suvarna@yahoo.com , everything after the @ sign is the domain name.
- The examples of the site which tells the owner of the mail associated with the sites are :

1. www.arin.net

The ARIN (American Registry for Internet Numbers) is used to find the domain name from the IP addresses. It also gives the contact personal listed against the domain name.

2. www.freeality.com

This website provides many different searching options like names, phone number and mail address. This websites permit the users to reverse email searches. This may help to reveal the subjects original identity.

Syllabus Topic : e-Mail Headers and Spoofing

5.3 e-mail Headers and Spoofing

We have studied the E-mail headers in the previous section. Email spoofing is the forgery of an email header. The message which you receive is actually originated from someone else than the actual user.

Email Spoof with PHP function mail ()

The mail () function allows you to send mail.

- Bool mail (string $to, string $subject, string $message [, string $additional_headers [, string $additional parameters]])

- Example: www.rootspot.com/jose/mai

Email Spoof with telnet

- Open command prompt and type telnet 25
- mail from: your email id @ blah.com
- rcpt to: recipient email id @ blah.com

Email Recovery Tools

The list of the email recovery tools is as follows:

- FINALeMAIL
- Email Examiner
- Network E-mail Examiner
- R-mail

Syllabus Topic : Laws against e-mail Crime

5.4 Laws Against e-mail Crime

Q. 5.4.1 Write short note on CAN-SPAM act. *(Ref. Sec. 5.4)* **(5 Marks)**

Q. 5.4.2 Explain the Law against email crimes? *(Ref. Sec. 5.4)* **(5 Marks)**

1. The CAN-SPAM Act

- The CAN-SPAM Act, a law that sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have you stop emailing them, and spells out tough penalties for violations.
- Despite its name, the CAN-SPAM Act doesn't make a difference just to mass email. It covers every single business message, which the law characterizes as "any electronic mail message the basic role of which is the business ad or advancement of a business item or administration," including email that advances content on business sites.
- The law makes no special case for business-to-business email. That implies all email – for instance, a message to previous clients declaring another product offering – must obey the rules to the law.

- Each separate email infringing upon the CAN-SPAM Act is liable to penalties of upto $16,000, so rebelliousness can be expensive. In any case, following the law isn't confounded.

Here's a rundown of CAN-SPAM's main requirements :

1. Try not to utilize false or deceiving header data. Your "From," "To," "ReplyTo," and directing data – including the beginning space name and email address – must be exact and distinguish the individual or business who initiated the message.
2. Try not to utilize tricky titles. The headline should precisely reflect the content of the message.
3. Recognize the message as a promotion. The law gives you a great deal of space in how to do this; however you should reveal unmistakably and prominently that your message is an ad.
4. Tell recipients where you are located. Your message must incorporate your substantial physical postal address. This can be your present street address, a post office box you have registered with the Postal Service, or a private mailbox you have registered with a business mail accepting office set up under Postal Service directions
5. Advise recipients how to quit accepting future email from you. Your message must incorporate a reasonable and prominent clarification of how the recipients can quit getting email from you later on. Specialty the notice in a way that is simple for a customary individual to perceive, read, and get it. Innovative utilization of sort size, shading, and area can enhance lucidity. Give an arrival email address or another simple Internet based approach to enable individuals to impart their decision to you. You may make a menu to enable a recipients to quit specific sorts of messages, however you should incorporate the choice to prevent every single business message from you. Ensure your spam channel doesn't shut these quit requests.
6. Respect quit asks for immediately. Any quit component you offer must have the capacity to process quit demands for no less than 30 days after you send your message. You should respect a recipient's quit demand inside 10 business days. You can't charge an expense, require the recipient to give you any specifically recognizing data past an email address, or make the recipient make any stride other than sending an answer email or visiting a solitary page on an Internet site as a condition for respecting a quit demand. When individuals have revealed to you they would prefer not to get more messages from you, you can't move or exchange their email addresses, even as a mailing list.

   The main special case is that you may exchange the addresses to an organization you have procured to enable you to conform to the CAN-SPAM Act.

7. Monitor what others are doing on your behalf. The law clarifies that regardless of whether you employ another organization to deal with your email advertising, you can't contract away your lawful duty to conform to the law.

   Both the organization whose item is advanced in the message and the organization that really sends the message might be considered lawfully dependable.

5.5 Section 66A

- Sending offensive messages through communication service, causing irritation etc through an electronic communication or sending an email to mislead or deceive the recipient about the origin of such messages (commonly known as IP or email spoofing) are all covered here.
- Punishment for these acts is imprisonment upto three years or fine. If anyone get booked under Section 66A, then that person has to face upto 3 years of imprisonment along with a fine.

Syllabus Topic : Messenger Forensics : Yahoo Messenger

5.6 Messenger Forensics : Yahoo Messenger

Q. 5.6.1 Write a short note on messenger forensics? *(Ref. Sec. 5.6)* **(5 Marks)**

Yahoo Messenger Overview

- Yahoo! Messenger is one of the popular instant messaging clients from Yahoo. By using the yahoo messenger you can send messages, photos, videos, files. You can do video chat as well as internet phone calls.
- Yahoo messenger has some default preferences such as alerts, sounds and signing into Yahoo Messenger. In yahoo messenger by default chat messages are archived and saved but these messages are cleared out once the user signs out of Yahoo Messenger. If you do not log out then it is possible to view these archived messages.
- One can also change the default setting option. If user wants to Yahoo messenger chat sessions then they can do it.

Data Analysis

- Investigation of the evidence start from the registry structure for Windows Vista and Windows 7 using the built in registry editor for Windows. The registry is examined with respect to the Yahoo Messenger files.

- Windows registry structure is quite similar to Yahoo Messenger registry structure for Windows XP. The data is found in the given locations as shown in Table 5.6.1.

Table 5.6.1 : Yahoo registry evidence for Windows XP, Windows Vista and Windows 7.

File	Location	Description	XP	Vista	Windows 7
HKEY_CURRENT_USER	Software\yahoo\Pager	Gives user ID	Yahoo User ID	Yahoo User ID	Yahoo User ID
		Gives the Installed Version	N/A	Version	Version
		Gives the version revisions	N/A	VersionRev	VersionRev
		Show if the password is saved		Save password	Save password
		Shows if auto sign in is on or off	N/A	Auto login	Auto login
		Number of P2P users	N/A	P2P count	N/A
HKEY_CURRENT_USER	Software\yahoo\Pager\Profiles\screenname\Chat		Chat(rooms visited or created)	Chat	chat
HKEY_CURRENT_USER	Software\yahoo\Pager\Profiles\screenname\Chat\FavoriteRooms		N/A	Favorite rooms	Favorite rooms
HKEY_CURRENT_USER	Software\yahoo\Pager\Profiles\screenname\FT	Location of last received file and last sent transferred file.	File transfer	FT	FT
HKEY_CURRENT_USER	Software\yahoo\Pager\Profiles\screenname\FriendIcons	Location of user icon displayed to friends.	N/A	Friend Icons	Friend Icons

- The investigator try to find out the Yahoo user ID of the person who is using the account, version of the Yahoo Messenger installed on the computer, all the revisions made to the YM version, if the save password option is turned on and also if the Auto sign in has been enabled. There is one extra feature in Windows Vista that is P2P count. P2P count is the number of allowed P2P users who can send huge data among each other.
- **User\Software\Yahoo\Pager\profiles\profile_name\chat** location shows the last selected chat room category, but not essentially the correct chat room entered. Y using this information investigator can understand chat room category that the predators potentially use. **User\Software\Yahoo\Pager\profiles\profile_name\chat\favorite_rooms** location provides the list of saved favourite rooms for the user. This information is important to understand the different chat rooms that the predator uses.
- **User\Software\Yahoo\Pager\profiles\profile name\FT** location provides the last saved location of a received file as well the last sent location of a transferred file, that is, the location from where the last sent file was uploaded. This information is useful when validating whether a user has been sharing or receiving files. Please refer to Table 5.6.1 for further detail. **User\Software\Yahoo\Pager\profiles\profile_name\FriendIcons** location provides the icon that the user has set for himself, that is displayed to the user's friends. The name of the file used will be visible in the path as well as where it is located on the hard drive.
- Photo Sharing: Creation of the "S" folder

In the Yahoo Messenger whenever a photo sharing session is initiated r from a Vista machine, a photo sharing folder starting with the letter "S" is created in the Program Data folder. In addition random assigned numbers and alphanumeric characters are appended to the end of the naming structure. The following is the path for the created "S" folder:

C:\ProgramData\Yahoo!\Messenger\PhotoSharing\Sc8b0

- The "S" folder is created when the user initiates the photo sharing session. Once the session is initiated, immediately the other yahoo user accepts the photo sharing invite, the "S" folder is created in the Photo Sharing folder on the initiator's side.
- The "S" folder is empty until a picture is shared. As soon as an image is shared or sent, a thumbs file '_t.jpg' is created followed by the image file '_m.jpg'. The name of this file is displayed as randomly assigned series of alphanumeric characters.
- If there are multiple chat sessions and photo sharing sessions open on users machine then at the same time with different users, a different "S" folder is created for each chat session.

5.6.1 File Transfer

- Yahoo Messenger has two ways of sharing a photo:
  1. Yahoo Photo Sharing
  2. File transfer option.
- For the photo sharing the "S" folder creation is applicable but it is not applicable to file transfer. If the user wants to save the photos through Photo Sharing, the default folder where these pictures will be saved is in the 'Picture' folder.
- The 'Picture' folder is a shortcut located under 'Libraries'. The full path is **'C:\Users\UserName\Pictures'**. The user can save the photos to any location they wish on the computer.
- The file transfer is used to transfer all types of media such as, photos, music, documents etc. The default location for saving a file during a file transfer is "Documents". The Documents folder is a shortcut located under 'Libraries'.
- The full path is **'C:\Users\UserName\Documents'**. The user can save the file anywhere on the computer as per his wish. The default file name and the original file is same. The date-time stamp of the saved file is same as local machine when the file was saved.

Syllabus Topic : Social Media Forensics: Social Media Investigations

5.7 Social Media Forensics : Social Media Investigations

Q. 5.7.1 Write a short note on social media forensics? *(Ref. Sec. 5.7)* **(5 Marks)**

- Social Media Investigations is now a days is a common feature of any investigation effort. The police uses social media to collect the evidences and build cases. Investigators use photos posted on the social media. The personal information on social media helps the investigator to ascertain someone's character, check for illegal or wrong behavior, to find someone, or to prove (or disprove) an explanation.
- Social media investigation is powerful as more that 80% people is using social media and people are posting to much information online. There are many popular social media sites, few are listed below.
  - Facebook
  - LinkedIn

  - Twitter
  - Youtube
  - Instagram
  - LinkedIn
  - Tumblr
  - Reddit
- Social media is a rich wellspring of data for pretty much any examination. In the event that your objectives incorporate get-together data about somebody's developments, partners, or character, social media investigations are an incredible fit.

5.7.1 Gathering Evidence for Court

- For court cases social media is a great source. Evidences are collected to prove someone's character, prove or disprove defense, or collect other various supporting evidence. Investigator collects the more information from statuses, photos, tweets from social media.
- The metadata attached with the post is used to determine where someone was at a given time. It also provides information about someone's behaviours and habits over time. This sort of evidence can discredit or support someone's claims, or even establish their reliability as a witness.
- Social media evidences should be collected methodologically, with proper metadata and other validating information intact. If the evidence is not collected properly then it won't be considered in the court.

Types of Evidence Typically Collected for Court Cases

- Relevant statements or comments.
- Metadata from posts establishing time and location of posting.
- Posts relating to past illegal activity.
- Photos.
- Content establishing character (for example, attitudes to police, past sentiments, racist or sexist content etc).
- List of social media profiles and screen names associated with target individual.

Employment Checks

- The social media is also used in employment where the employer can assess your character, work experience, and education.

- Social media investigations helps to find the past illegal behaviour, provide evidence to support or discredit claims about education and employment, and assess whether they are probable to conduct themselves in a manner befitting your organization. Before conducting a social media investigation on an employee , you should know that these types of background checks are subject to the Fair Credit Reporting Act. It means applicants consent is needed.

Types of Evidence Typically Collected

- Posts and photos relating to illegal activity or **drug use.**
- Posts relating to objectionable content (e.g. **racist or sexist** content).
- Posts supporting or discrediting past **education and employment.**
- Relevant statements and comments.
- List of social media profiles and screen names associated with target individual.

Person Location

Social media posts contains location data. It will be helpful you to find your long lost friend then social media is useful. Social media investigations merge social connections and biographical information to find people.

Types of Evidence Typically Collected

- Location metadata from posts.
- Location metadata from images.
- Relevant statements and claims.
- Photo analysis.
- Leads from interviews and social connections.

The same way social media is used in custody cases, divorce cases.

Tools used for Social Media Investigation

Screencast-O-Matic

Screencast-O-Matic tool is used to record the screen. This tool record the social media screen as evidence. It record the posts, comments, photos and videos posted on the social media.

5.8 Browser Forensics

Q. 5.8.1 Write a short note on browser forensics ? (Ref. Sec. 5.8) (5 Marks)

Web browsers overview

- Nowadays there are many web browsers available in the market like Internet Explorer, Google Chrome, and Mozilla etc.
- These all web browsers are slightly different in web services. To display the same website faster on future occasions, web browsers maintain the Downloaded web site data, so that it remains available on the computer even if the user closes the browser or shuts down the machine. This is a useful feature.
- The downloaded web files are known as caches, cached history or temporary files. Based on the operating system and browser applications they are in different locations.

Internet Explorer

The most famous web browser is Internet Explorer (IE) as it is a component of the Windows operating system. IE is very and is frequently used as a default web browser. In windows 10 IE is replaced with Microsoft EDGE (ME).IE and ME both work in InPrivate mode, without storing information about web resources visited by the user.

Google Chrome

- Google Chrome is browser by provided by Google. It has incorporation with Google services. It allows the Synchronization of user passwords between devices. One can use the extensions and plug-in. Google Chrome performs fast operations and collects user data but it Consumes large amounts of memory.
- The important feature of google chrome is that it works in Incognito mode, which prevents the browser from permanently storing any history information, cookies, site data or form inputs.
- There are many web browsers created by the third party developers based on Chrome Engine, like Chromodo, Amigo, Sputnik, Uran, Epic Browser, SafeZone, Comodo Dragon, Flock, Rockmelt, Sleipnir SRWare Iron, Titan Browser, Torch Browser, 360 Extreme Explorer, Avast Chromium, CoolNovo, Cốc Cốc, Vivaldi, Yandex.Browser, Opera, Orbitum, Breach, Nihrome, Perk, QIP Surf, Baidu Spark, etc. All of these borrowers function like Google Chrome and create web browser artifacts like Google Chrome and also support most of Google Chrome's extensions and plugins.

Opera

The Opera web browser is also a famous web browser. It was the first web browser to introduce features that other web browsers adopted, like; pop-up blocking, Speed Dial, private browsing and tabbed browsing re-opening recently closed pages. Opera have a free Virtual Private Network (VPN) service, which permits users to surf the web incognito.

Firefox

Firefox is also one of the popular web browsers. It is more secure as compare to other browsers. It has advanced Incognito mode, disabling tracking of user's locations and advertisements. Firefox has its own extensions.

Difficulties of web browsers forensic analysis

There are following difficulties faced by the forensic examiner while analyzing the web browsers :

- Many web browsers are available with lots of data. Different data.
- To protect the data Encryption is used.
- If the user is using the Incognito mode (private mode) then computer do not contain the browser artifacts.

Web browser forensic artifacts

Each web browser has its own artifacts in operating system. The artefacts are depend on the version of the web browser. Usually one can get the following artefacts:

- History
- Cache
- Cookies
- Typed URLs
- Sessions
- Most visited sites
- Screenshots
- Financial info
- Form values (Searches, Autofill)
- Downloaded files (Downloads)
- Favorites.

Syllabus Topic : Browser Forensics : Cookie Storage and Analysis

5.8.1 Cookie Storage and Analysis

- Cookies are the text files. These files are used to feedback from the user to the server. When performing some actions with a web resource like viewing web links, downloading files, etc, these actions are registered in a cookie that is secretly sent by the server to the user's computer. By using this web resource, the server can find out what actions the user has taken on previous visits to this web resource.
- The cookies are stored in cookies folder, but the location of the cookies folder is based on the web browser and the operating system .The following table illustrate the location of the cookies based on the browser and operating system.

Browser	Operating System	location
Internet Explorer	Windows 98	\Windows\Cookies\
	Windows 2000, Windows XP	\Documents and Settings\Administrator\Cookies
	Windows 7	\Users\%userprofile%\AppData\Roaming\Microsoft\Windows\Cookies
	Windows 7	\Users\Default\AppData\Roaming\Microsoft\Windows\Cookies
Firefox, Windows		\Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\cookies.sqlite
Google Chrome, Windows		\Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\Cookies.db

Syllabus Topic : Browser Forensics : Analyzing Cache and Temporary Internet Files

5.8.2 Analyzing Cache and Temporary Internet Files

Cache Files

- The cache folder contains the browser history and it automatically creates the profile folder at start. This folder is the storage place for the browsing history.

- The following table shows the cache locations of the different browsers :

Firefox	Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\cache2\entries
Google Chrome, Windows	\Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\Cache\ \Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\GPUCache\ \Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\Media Cache\
Opera	\Users\%userprofile%\AppData\Roaming\Opera Software\Opera Stable\ShaderCache\GPUCache\data_3
Safari, MacOS	\Users\%userprofile%\Library\Caches\com.apple.Safari\Cache.db

Windows Temporary Internet Files

- Temporary Internet Files (C:\Windows\Temporary Internet Files) are immediate downloads from the Internet, more often than not containing realistic pictures in Windows bitmap (bmp), jpeg, gif, or .art format. There will likewise be html and htm files for website home page components, and so forth. Approaching Yahoo and Hotmail messages may likewise exist as files in the Temporary Internet Files folder.
- Downloaded movies, mpegs, avi files, and Adobe PDF files will be found in Temporary Internet Files.

Temporary files

- Windows Temp files (C:\Windows\Temp) are temporary files made by Windows as different programs are running and diverse processes are occurring. They are regularly exact copy of files put away somewhere else on the PC. At different occasions they are exact duplicates of files which are waiting to be handled by the PC.
- For instance, a print work heading off to a laser printer will make a temporary document called an EMF (enhanced windows metafiles). EMF's (smaller than normal photos of the original) can frequently be found in the Temp index a very long time after laser printer was utilized.
- Numerous different sorts of files can be found in the Temp registry too (e.g., programmed report recuperation files).

How is the data stored?

- Internet Explorer and Windows Explorer store most of the data in index.dat files. INDEX.DAT files are used by Internet Explorer to store information about visited pages, cookies and the time they are used.
- To this end, Internet Explorer indexes files that are located in folders that are browser caches and maps these files to the network resource from which these files were downloaded. In addition, INDEX.DAT files contain such information as the decryption of HTTP-header packets, in which the file was transferred, the date of creation and last access to the file, the number of calls to it, and much more.
- The following are the locations for index.dat file.

1	\Documents and Settings\%userprofile%\Local Settings\Temporary Internet Files\Content.IE5\index.dat
2	\Users\%userprofile%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
3	\Documents and Settings\%userprofile%\Cookies\
4	\Documents and Settings\%userprofile%\Local Settings\History\History.IE
5	\Documents and Settings\%userprofile%\Local Settings\History\History.IE\MSHist[timestamps]

Syllabus Topic : Browser Forensics : Web Browsing Activity Reconstruction

5.8.3 Web Browsing Activity Reconstruction

- To reconstruct the web browsing activity, you have to reconstruct it from cached file in users computer. Examine Cached files created by web browsers.
- The browsing activities are internet shopping, downloading, browsing and searching etc. you can perform web browsing activity reconstruction using any open source or freeware tool.
- The following are the steps to reconstruct the web browsing activity :

1. **First check the cookies folder, here we are considering browser Firefox, and operating system is windows xp. So you get the cache file at the location given below:**

   \Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\cookies.sqlite

2. Check the cache file at the given location

Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\cache2\entries)

3. Check the favorites at the given location

Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\places.sqlite

4. For session recover check the following location

\Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\sessionstore.js

5. Check the downloaded file given at the following location

\Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\places.sqlite

6. Check the URL's visited in the location given below

\Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\places.sqlite

7. Check the form value

\Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\formhistory.sqlite (Firefox, Windows)

8. Check the typed URL's

\Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\places.sqlite

9. Check the session restore artifacts

\Users\%userprofile%\Library\Safari\Local Storage\

\Users\%userprofile%\AppData\Roaming\Opera Software\Opera Stable\Last Tabs (Opera, Windows)

- Google Chrome, Safari, Firefox, Opera store most of the data in SQLite databases. Manual analysis of these databases and carving will allow you to extract the maximum amount of data.

When analyzing SQLite data bases, remember :

- Some deleted records can be found in Freelist – unused tables that can contain deleted data.

Where can I find the Web Browsers artifacts?

- Physical dumps of mobile devices.
- File systems of mobile devices.
- Backups of mobile devices.
- Data, which can be extracted from Clouds.
- Hard drives.
- Images of hard drives.
- Memory dumps.
- Hibernation and page files.

5.9 Exam Pack (Review Questions)

Syllabus Topic : E-mail Analysis

Q. 1 Write a short note on email forensics ? *(Refer sections 5.1 and 5.2)* **(5 Marks)**

Q. 2 Explain the steps involved in email analysis/investigation. *(Refer section 5.2)* **(5 Marks)**

Syllabus Topic : Laws against e-mail Crime

Q. 3 Write short note on CAN-SPAM act ? *(Refer section 5.4)* **(5 Marks)**

Q. 4 Explain the Law against email crimes ? *(Refer section 5.4)* **(5 Marks)**

Syllabus Topic : Messenger Forensics : Yahoo Messenger

Q. 5 Write a short note on messenger forensics ? *(Refer section 5.6)* **(5 Marks)**

Syllabus Topic : Social Media Forensics : Social Media Investigations

Q. 6 Write a short note on social media forensics ? *(Refer section 5.7)* **(5 Marks)**

Q. 7 Write a short note on browser forensics ? *(Refer section 5.8)* **(5 Marks)**

□□□

Chapter Ends...