Module 7 (Case Study)

Objective are :-

1) Understanding of internet resources
2) Web Browser
3) Email Header policy Forensic
4) Social Networking Service

* Network

The internet is based on the network which follows are iso or OSI model. As per OSI model network is divided into seven layers.

a) Application layer : It is the highest level in Network Stack and represents the language used by programs to communicate with each other. It used several protocols such HTTP (Hyper text transfer protocol, FTP (File transfer protocol), SMTPP (Simple mail transfer protocol) etc.

b) presentation layer : It defines the network equivalent on the alphabet to be used for communication It is responsible for translating between different character sets and may also be responsible for implementing the Encryption

c) session layer : It is responsible for maintaining a dialogue between two pecies of a software

d) Transport layer : It deals with end node to end node communication and responsible for combining multiple sessions into a format suitable for transmission between machines ~~In this layer Internet protocol runs (IPv4, IPv6)~~

~~In this layer we use routers and routing algorithm~~

In this layer TCP (Transport control protocol) , UDP (User Datagram protocol) runs

e) Network layer : It is the route planner of the network stack. It identifies the most efficient way of getting the transport layers data from the point of orgin to destination.

In this layer Internet protocol runs (IPv4, IPv6)

In this layer we use routers and routing algorithm

f) Data link layer : It is responsible for implementing the network box HOPS used by the network layer and deals with adjacent node to node communication.

It checks the data with the help of some technique such as cyclic redundancy coding such as CRC It uses several network protocol such as Aloha, Slotted Aloha, CSMA/CD CSMA-CA etc.

d) Physical layer: It is the lowest layer in the network stack the frames of data link layer are converted into signals and transported to a medium and reaches to the destination It deals with wires, wireless, optical fibers, Coaxial cables, radio frequency signals etc.

Internet protocol suite

An Internet protocol suite is a standard or method which helps to divide the network into 5 layers

a) Application layer: Application layer of IP suite model is constructed by application and presentation layer of OSI it deals with HTTP, SMTP, FTP, BOBS etc protocols

b) transport layer: the transport layer of IP suite model is constituted by the session and transport layer of the OSI model. It deals with several protocols such TCP, UDP etc.

c) Internet layer: the internet layer of IP suite model is constituted by the network layer of the OSI module. It deals with IP address. Which may be catagories into several types such as IPv4, IPv6, IPv4 is of 32 bits and IPv6 is of 128 bits. IP address are divided into 4 classes

class A : 0 to 127
class B : 128 to 191
class C : 192 to 223
class D : 224 to 255

This layer uses classless and classful addressing scheme and uses classless inter domain routing

d) Data link layer: It is responsible for node to node communication

e) Physical layer: It is responsible for converting data link layer frames into appropriate signals

And transport them through a transporting medium (wire or wireless)

* DNS (Domain Name Server) or (Domain Name System/Service)

Internet release on IP address which may not be secure and practically useless for humans to solve this problem a system allows humans to refer to machines by name. this name is known as domain name system or service.

* WWW (world wide web)

It is a collection of services, setting on top of the wider internet and accessible through a unified interface it deals with two components HTML and HTTP

* Web Browser

a) when a web client connects to a server to retrieve a web page it typically starts by issuing get command to retrieve the main HTML page

b) once the HTML has been received the browser will then issue a series of get's and or POSTS to retrieve the enabled resources identified by the HTML

c) In this way a single web page which is constituted by multiple files will be loaded on the internet or web client or web browser

d) Web Browser contains stored copies of previously used resources in an local area which is known as Browser cache.

e) Web Browser access the data from the server using a ~~secure~~ secure HTTPS connection

f) Most Web Browsers give a history of recently visited resources

g) Web Browsers accepts and store cookies which are small chunks of data and holds the information of the recently visited web sites and others. A cookie contains following information such as created, domain, expired, name, path and value. created indicates time and date of cookie creation. domain denotes a place ~~where~~ where the cookie should be returned name denotes the name of the cookie as it is known to the server. path it denotes the starting point in the resource path for the server. value it denotes the data to be stored in the cookie

* Email

a) Electronic mail or Email is a popular application on the internet to sent and receive information

b) sending email: a) to send an email we use SMTP or simple mail transfer protocol. To send an email b) we also use a standard definition of the format of mail messages

c) SMTP defines a technique which allows an email software to deliver the messages directly to the receiving system

~~d) Collecting~~

e) Collecting Email: *) With advancement of personal computers, we face a situation where delivery to a local server was no longer sufficient to allow users to work with email efficient

*) Either of desktop machines must be capable of receiving SMTP or we will not be able to receive or collect any email.

*) During earlier times, if the PC of the receiver is switched off for a prolong period of time then the receivers are allowed to collect there emails on demand. So in order to collect the emails by a receiver software, from there mail box a new protocol is established which is known as POP3 (Post office protocol)

*) Internet message access protocol (IMAP) help us to collect ~~data~~ and delete data from an email stored on the server.

This protocol allows the clients to create and manipulate with folders which are inserted to be used for mail storage on the server

4) From an investigating point of view receiving collecting email and retrieving information has little or no effect on the content of the messages retrived but this procedure may be used to, If we need to examine a mailbox, which is still active on the server If we know, which retrival protocol was in use then we can ensure that checks are carried out for all features supported by the protocol

Email Header Forensics

1) the email header provides a record of the path the message took ~~for~~ from ~~to~~ sender to receiver
2) Email Headers should be read from the bottom to the top
3) If any sender sends an email to a receiver then the email Header contains following information
   a) Delivered to : It denotes at which email address the email message is delivered.

b) Received: It denotes date, time, Id and protocol used

c) Returned path: It denotes an URL through which the mail will come back to the sender if anything goes wrong during the transport

d) Received From: It denotes the email id, protocol, date and time and other information of the sender

e) Message ID: It denotes an unique ID to identify an email

f) From an investigating point of view. If a digital forensic expert can email header he or she will come to know about all these facts. What are associated with an email Header. (Refer to pic pg 129 & 5 samson)

Social networking sites

1) Law enforcement officer and several other investigating organisation and prospective employer are used to search the social networking sites, and practitioner. to learn more about suspect, prospective employee and other

2) Several social networking sites are now under consideration such as FB, Twitter linkedin, whatsapp, Instagram and others

3) these sites are routinely investigated.

4) the objectives of this investigation are
a) understanding the user associated with this site
b) security c) To maintain integrity d) to identify frauds e) to identify misleading

Social media evidence can be found in several places such as suspects computer, smart phone, provider network and others. As provider only retains the valuable information for a certain amount of time - hence getting evidence from the provider requires quick action.

* Recording evidence on the local machine is a challenging task we may search page file or swap space or index.dat file which may hold multiple of artifacts
* The confirmation email found in the history.if file holds some useful information
* contact.ief file directly holds profile realted item file which holds information about the user facebook profile.
* History.ief directly holds index.dat file which can contain information about all the FB friend searches.