Practical : 1

Aim: Creating a Forensic Image using FTK Imager/Encase Imager:

CREATE A NEW DISK IMAGE

SELECT CONTENTS OF A FOLDER

BROWSE THE FOLDER

ENTER THE FOLLOWING FIELDS

ENTER DESTINATION

THIS IS HOW THE OUTPUT FILE WILL LOOK LIKE

ADD EVIDENCE

SELECT IMAGE FILE

SELECT OUTPUT FILE

YOU CAN SEEE THE OUTPUT FILE IN EVIDENCE TREE

Practical:2

Aim:

Open win registory editor using run>regedit

Go to Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\ and create new key

Name this key “StorageDevicePolicies”

Make New Dword name it “WriteProtect”

Enter Hexa value as 1

THE SPELLING IS VERY IMPORTANT RENAME IF YOU ENTERED WRONG

“StorageDevicePolicies”

“WriteProtect”

We can only open the file in the USB drive for reading, but it’s not allowed to modify and

save the changes back to USB drive.

Now Create image of the USB drive using FTK imager

Enter data into the required fields. Select the destination folder.

Image file is created and you can verify it.

Practical No – 3

Aim: Forensics Case Study:

- Solve the Case study (image file) provide in lab using Autopsy

Install autopsy software and select new data source, select disk image or utf file

Browse and select the image of the pendrive made by ftk imager, enter the optional values if needed

Configure ingest elect all options and add data source

On the left hierarchy lookup for deleted files

Expand it and click on All

Right click on the table view and select Extract files

Select the export folder

Now click on generate report and select excel report

Click all results and select finish

You can view the folders in generated base directory

Practical:4

Aim: Capturing and analyzing network packets using Wireshark (Fundamentals):

- Identification the live network

- Capture Packets

- Analyze the captured packets

1. Open Wireshark

TCP package: search TCP package

Analysis youtube data

Now go on browser and open youtube and perform some activity on the youtube

Now come back to Wireshark and enter udp contains youtube in the search bar.

search

udp contains user:

Now go on browser, login in any secured website and Now come back to Wireshark and enter udp contains user in the search bar.

http website: go on browser, login in any unsecured website and Now come back to Wireshark and enter

http.request.method==POST

testphp.vulnweb.com

in the search bar.You can view the username and password because it is http website

filter with ip: ip.addr==192.168.0.104

filter udp package with length : udp.length==100

Many other filter expression

Practical-5

AIM: Analyze the packets provided in lab and solve the questions using Wireshark :

- What web server software is used by www.snopes.com?

- About what cell phone problem is the client concerned?

- According to Zillow, what instrument will Ryan learn to play?

- How many web servers are running Apache?

- What hosts (IP addresses) think that jokes are more entertaining when they are explained?

What webserver is this website using?

ANS-

Server is Microsoft iis server

About what cell phone problem is the client concerned with?

-Search for a keyword cell in all cell packets using regex

-frame matches ”(?)cell”

ANS-

Client had searched for cell charge problem

How many webservers?

Into the filter type “ http.server contains "Apache" ” and search. Now click on Statistics – Endpoints.

Move to Ipv4. Check the Limit to display filter at the bottom and you can see that 22 servers are

running Apach

What hosts think Jokes are more entertaining when they are explained?

Search in filter: frame matches”(?)jokes”

To begin firstly search the keyword jokes into the filter type “frame matches"(?)jokes"” and click on the

first row of result. Now move to the second frame, where you will find Hypertext Transfer Protocol

expand it to see the GET method where you’ll see what query the user has searched for i.e. jokes are

more entertaining when they are explained . The IP address for the same is 173.241.244.99

Practical:6

Aim: Using Sysinternals tools for Network Tracking and Process Monitoring:

-Check Sysinternals tools

-Monitor Live Processes

-Capture RAM-Capture

-TCP/UDP packets

-Monitor Hard Disk

-Monitor Virtual Memory

-Monitor Cache Memory

Sysinternal tools

The SysInternals suite of tools is simply a set of Windows applications that can be downloaded for free from their section of the Microsoft Technet web site. They are all portable, which means that not only do you not have to install them, you can stick them on a flash drive and use them from any PC

The Sysinternals tools are divided into six categories: File and Disk Utilities, Networking Utilities, Processes Utilities, Security Utilities, System Information and Miscellaneous Utilities. There are many tools, but the widely known are AutoRuns, Process Monitor, Process Explorer, TCPView and RootkitRevealer.

Tcp -udp packets

Diskmonitoring

Practical 7

Aim: Recovering and Inspecting the recovered files.

I) Check for deleted files.

II) Recover the Deleted Files.

Steps:

1) First, create a text file and paste some data in it and store it in a folder.

2) Open AccessData FTK Imager then click on file and select “Create Disk image”.

3) Select source as Content of a folder and click on next.

4) Then browse the source evidence that we created previously as a text file then click on finish.

5) Enter the evidence item information and click on next.

6) Then browse the image destination folder and name the image file and click on finish.

7) For creating and image, click on start.

8) As we get the result, we can verify by looking at the verify result of both the hashing functions.

9) Atlast, we get the status of the creation and we can also view image summary.

10) For adding an evidence, select “Add evidence item”.

11) Select source as image file and click on next.

12) Then browse the path of the evidence source and click on finish.

13) In the evidence tree we can see the image file that we created.

III) Analyzing and inspecting the recovered files.

Perform this using recovery option in ENCASE and also Perform manually through command line.

Steps:

1) Download TestDisk zip file.

2) Extract the downloaded file in a folder.

3) In that file, open “photorec\_win” application.

4) Then select the pen drive that you attached to your PC and proceed.

5) Then select the drive with the name of your pen drive and proceed.

6) Then select on Other and proceed.

7) Select “Whole” for extracting files from whole partition and proceed.

8) Then for going to another directory or drive use left arrow key on your keyboard, then select the pen drive to store the deleted data.

9) After reaching the destination, press C key on the keyboard. After that the process will start.

10) Atlast, we can see that the files that were deleted are successfully retrieved.

Practical:8

Aim: Acquisition of Cell phones and Mobile devices

MOBILE:

Download and install mobile edit on your android phone and connect to your pc

PC: Pair / connect with your pc using usb, Bluetooth or Wifi,

Then open MobileEdit in your pc

Find your Device and select next

Set a Name for your device

Get device Info

Get Phonebook Directory

Get Files and messages

Practical 9

Aim: Email Forensics

- Mail Service Providers

- Email protocols

- Recovering emails

- Analyzing email header

click Start a new case, and then click OK.

Type case Information and examiner information

Select case log options and all processes to perform

Select these options and add evidence information

New case setup is complete

Export case information

Part2

Launch detached information

View message headers and body

PRACTICAL 10

Aim :- Web Browser Forensics

- Web Browser working

Google Chrome

Microsoft Edge

Firefox

- Forensics activities on browser

Go to File Menu > Capture History

Click Next

Give the path of folder in which you want to save your captured data and click on capture

All the captured details are listed below

Downloads

Searches

Website Visits

Bookmarks

- Cache / Cookies analysis

Number of cache files and cookies gets captured

- Last Internet activity

Generating Report

Right Click on the content and click Add to report

Go to File menu and then Report>Save as PDF

Report gets generated

Exporting Report

Go to File Menu Export > Export to Html

Click on Export

Report gets exported into html

Last Internet Activity gets listed below in the exported report