Practical 1

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

- Create Forensic Image:

1. Click File, and then Create Disk Image, or click the button on the tool bar.
2. Select the source evidence type you want to make an image of and click Next.
3. Select the source evidence file with path .
4. Click on “add” to add image destination.
5. In the Image Destination Folder field, type the location path where you want to save the image file, or click Browse to find to the desired location.
6. After adding the image destination path click on finish and start the image processing.
7. After the images are successfully created, click Image Summary to view detailed file information, including MD5 and SHA1 checksums.

Analyze Forensic Image:

1. Click on Add Evidence Item to add evidence from disk, image file or folder.
2. Now select the source evidence type as image file.
3. Open the created evidence image file.
4. Now select Evidence Tree and analyze the image file .

PRACTICAL 2

AIM :- Forensics Case Study : Solve the Case study (image file) provide in lab using Encase Investigator or Autopsy.

1. Open Autopsy.
2. Click on new case.
3. Enter details regarding the case and click on next button.
4. Enter further details and click on next button.
5. Now here we have to select Type of data source to add , in our case disk image or VM file and click on next.
6. Now we have to select image file and click on next button.
7. Now click on select all in order to Run ingest modules on: and click on next.
8. Now click on finish
9. Now Autopsy window will appear and it will analyse the disk that we have selected .
10. All image files appears in the Table tab. Select any file to see the data
11. Expand the tree from left side panel to view the document files.
12. To recover the files , go to view code Deleted files node , here select any file and right click on it then select Extract files option
13. Select Path where you want to save extracted file and click on save .
14. Now click on OK
15. Now go to C:\autopsy\case_prac00124\Export folder to see recover file
16. Click on generate report from Autopsy window and select the Excel format and click on next
17. Now report is generated so click on close button. We can see the Report on Report Node.
18. Click on report.

Practical 3

AIM : Capturing and analyzing network packets using Wireshark.

Capturing Packets.

1. Capture traffic on your wireless network, click your wireless interface. You can configure advanced features by clicking Capture > Options, but this isn't necessary for now.

2. As soon as you single-click on your network interface's name, you can see how the packets are working in real time. Wireshark will capture all the packets going in and out of our systems.

3. Promiscuous mode is the mode in which you can see all the packets from other systems on the network and not only the packets send or received from your network adapter.

4. Promiscuous mode is enabled by default. To check if this mode is enabled, go to Capture and Select Options. Under this window check, if the checkbox is selected and activated at the bottom of the window. The checkbox says "Enable promiscuous mode on all interfaces".

5. The red box button "STOP" on the top left side of the window can be clicked to stop the capturing of traffic on the network.

Color Coding

Different packets are seen highlighted in various different colors. This is Wireshark's way of displaying traffic to help you easily identify the types of it. Default colors are:

Light Purple color for TCP traffic.

Light Blue color for UDP traffic.

Black color identifies packets with Errors.

Analyze the captured Packets:

1. First of all, click on a packet and select it. Now, you can scroll down to view all its details.

2. Filters can also be created from here. Right-click on one of any details. From the menu select Apply as Filter drop-down menu so filter based on it can be created.

Display filter command.

1. Display packets based on specific IP-address
ip.addr == 192.0.2.1

2. Display packets which are coming from specific IP-address
ip.src == 192.168.1.3

3. Display packets which are having specific IP-address destination
ip.dst == 192.168.1.1

4. Display packets which are using http protocol
http

5. Display packets which are using http request
http.request

6. Display packets which are using TCP protocol
Tcp

7. Display packets having no error connecting to server
http.response.code==200

8. Display packets having port number 80
tcp.port==80 || udp.port==80

9. Display packets which that contains keyword facebook
Tcp contaion facebook

Practical 4

Aim :- Analyze the packets provided in lab and solve the questions using Wireshark.

How many web servers are running Apache.

Analysis – The web server name can be retrieved from HTTP response header. So will apply filter http. response and we can see all http response packets.

1. Now we will set the server header as column select any packet and right click on it then select Apply as Column.

2. Now can see the server column where all server name is showing.

3. Now we have to check how many Apache packets are there we can't count manually for each packet so we will apply another filter http.server contains "Apache".

4. After applying filter go to Statistics > Endpoints.

5. It will show all connections.

6. Check the limit to display filter then it will show the actual Apache connections. Now there are showing 22 connections but will exclude 192.168.1.71 because it is client's IP not a server IP so there are actual 21 Apache servers.

CONCLUSION: We have successfully analyzed the packets provided and solved the questions using wireshark.

Practical 5

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

Monitor Live Processes : (Tool: ProcMon)

To Do:

1. Filter (Process Name or PID or Architecture, etc)
2. Process Tree
3. Process Activity Summary

Count Occurrences.

Capture TCP/UDP packets (Tool: TcpView) :

To Do:

1. Save to .txt file.
2. Whois

Monitor Virtual Memory (Tool:VNMAP)

To DO:

1. Options – Show Free & Unusable Regions
2. File-> Select Process e.g. chrome.exe
3. Save to .mmp file

Monitor Cache Memory (Tool: TAMMap)

To Do:

1. Save to .RMP file.

Practical 6

Aim: Recovering and Inspecting deleted files.

1. Start Autopsy from Desktop

2. Now create on New Case.

3. Enter the New case Information and click on Next Button.

4. Enter the additional Information and click on Finish.

5. Now Select Source Type as Local disk and Select Local disk form drop down list and click on Next.

6. Click on Next Button.

7. Now click On Finish.

8. Now Autopsy window will appear and it will analyzing the disk that we have selected.

9. All files will appear in table tab select any file to see the data.

10. Expand the tree from left side panel to view the document files.

11. To recover the file, go to view node-> Deleted Files node , here select any file and right click on it than select Extract Files option.

12. By default Export folder is choose to save the recovered file.

13. Now Click on Ok.

14. Now go to the Export Folder to view Recover file.

15. Click on Generate Report from autopsy window and Select the Exce Format and click on next.

16. Now Report is Generated So click on close Button .

17. Now open the Report folder and Open Excel File.

Practical 7

Aim: Web browser forensic.

1. Open BrowserHistoryExaminer.
2. Click on file > Capture History.
3. Select the capture folder and click on next.
4. Enter the destination to capture the data.
5. The History is been extracting.
6. The data has been retrieved.
7. On the left panel click on bookmarks.
8. On the left panel click on cached files.
9. On the left panel click on cached images.
10. On the left panel click on cookies.
11. To Create Reports. Click on file > Report and save the report as pdf or html page.