---PRACTICAL 1---

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

a) Creating Forensic Image

b) Check Integrity of Data

c) Analyze Forensic Image

Note:- Before creating the disk image you need to create Two folders on the the system and Name them as Input and Output Respectively

Steps :

a) Creating 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 (Select Content of a folder)and click Next.
3. Select the source evidence file with path .(Select the input Folder which you created)
4. Click on "add" to add image destination

a. In the Image Destination Folder field, type the location path where you want to savethe image file, or click Browse to find to the desired location.

Note: If the destination folder you select is on a drive that does not have sufficient free space to store the entire image file, FTK Imager prompts for a new destination folderwhen all available space has been used in the first location.

5. In the Image Filename field, specify a name for the image file but do not specify a fileextension.
6. After adding the image destination path click on finish and start the image processing. (Here Select the output folder path to Store the recovery file in it)
7. After the images are successfully created, click Image Summary to view detailed file information, including MD5 and SHA1 checksums.

b) Analyze Forensic Image:

a) Click on Add Evidence Item to add evidence from disk, image file or folder.

b) Now select the source evidence type as image file.

c) Open the created evidence image file

d) Now select Evidence Tree and analyze the image file.

---Practical 2---

Aim : Data Acquisition Perform data acquisition using:

• USB Write Blocker + FTK Imager

Steps :   Enable USB Write Block in Windows 10, 8 and 7 using registry

1. Press the Windows key + R to open the Run box. Type regedit and press Enter.
2. This will open the Registry Editor. Navigate to the following key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control

3. Right-click on the Control key in the left pane, select New -> Key.
4. Name it as StorageDevicePolicies
5. Select the StorageDevicePolicies key in the left pane, then right-click on any empty spacein the right pane and select New -> DWORD (32-bit) Value. Name it WriteProtect
6. Double-click on WriteProtect and then change the value data from 0 to 1.
7. The new setting takes effect immediately. Every user who tries to copy / move data toUSB devices or format USB drive will get the error message "The disk is write protected".
8. We can only open the file in the USB drive for reading, but it's not allowed to modifyand save the changes back to USB drive. So this is how you can enable write protection to all connected USB drives. If you want to disable write protection at a later time, just open Registry Editor and set the WriteProtect value to 0.
9. Now Create image of the USB drive using FTK imager
10. Select the USB drive folder by browsing and click next & Finish.
11. In the Create Image dialog, click Add.

• You can compare the stored hashes of your image content by checking theVerify images after they are created box. If a file doesn't have a hash, thisoption will generate one.

• You can list the entire contents of your images with path, creation dates, whether files were deleted, and other metadata. The list is saved in a tab-separated value format

12. Select the type of image you want to create, and then click Next

---PRACTICAL 3---

Aim : Capturing and analyzing network packets using Wireshark.

a) Identification the live network

b) Capture Packets

c) Analyze the captured packets

Steps : 1. Open Wireshark and click on Ethernet.

2. Now go on browser and open any unsecured website i.e and perform some activity on thewebsite.
3. Now come back to Wireshark and enter http in the search bar
4. Now click on the get request and see the details.

---PRACTICAL 4---

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

a)Check Sysinternals tools

b) Monitor Live Processes

c) Capture RAM

d) Capture TCP/UDP packets

e) Monitor Hard Disk

f) Monitor Virtual Memory

g) Monitor Cache Memory

Steps :

a) Check Sysinternals tools: Windows Sysinternals tools are utilities to manage, diagnose, troubleshoot, and monitor a Microsoft Windows environment. The following are the categories of Sysinternals Tools:

1. File and Disk Utilities
2. Networking Utilities
3. Process Utilities
4. Security Utilities
5. System Information Utilities
6. Miscellaneous Utilities

b) Monitor Live Process:(Tool: ProMon)

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

4. Count Occurrences

Output:

1. Click on Tools → Select Process tree → Close
2. Tools → Count Occurance → Click on Count

c) Capture RAM(Tools: RAMCapture):

To Do:

1. Click Capture
2. Creates a .mem file of the system memory (RAM) utilized.
3. Process Activity SummaryCount Occurrences

Output:

d) Capture TCP/UDP packets (Tool; TCPview):

To Do:

1. Save to .txt file.
2. Whois

Output:

e) Monitor Virtual Memory (Tools: VMMAP):

To Do:

1. Options – Show Free & UnusableRegions Check operations performed in thedisk as per time and sectors affected.
2. File → Select Process e.g. chrome.exe
3. Save to .mmp file.

Output:

f) Monitor Cache Memory (Tools: RAMMap):

To Do: 1. Save to .RMP file

Output:

---PRACTICAL 5---

Aim : Recovering & Inspecting Deleted files.

a) Check for Deleted Files b) Recover the Deleted Files c) Analyzing & Inspecting the recovered files Steps :

a) Creating Forensic Image

1. In CS server Create a new Folder → Copy Paste some file in it → Delete that filepermanently.
2. Open AccessData FTK Imager. Click on File → Add evidence item → PhysicalDrive → next → Keep Selected 'Physical Drive' → Finish
3. Evidence Tree appears and hash values

• Now Expand evidence Tree → Then select Volume on which you have savethe folder and File.

• Now Expand (+) New Volume (NTFS) → Click on bar like loading appears & certain options appears

4. Now expand (+) root ◊ Select the Folder from where you have deleted file
5. Right Click on the file which you want to recover → Click on Export file → Give Destination Path from Which you have deleted the file → save and Recover file → ok
6. Now browse the Folder to the folder where you saved recovered file you will file find the 'file' our file got recover.

---PRACTICAL 6---

Aim : Mobile Device Forensics:

a) Perform a forensic analysis of a mobile device, such as a smartphone ortablet.

b) Retrieve call logs, text messages, and other relevant data for investigativepurposes.

Steps :-   1. Perform a forensic analysis of a mobile device, such as a smartphone or tablet.

1. Download mobiledit forensic tool in mobile.
2. Open Mobileit tool in PC
3. Click on connect.
4. Connect your mobile device to the system. Click on phone → Next
5. Click the Connection.
6. Open the mobiledit tool in phone and click on the type of connection (i.e Wifi) → Copy the IP address and enter it in the PC and click next.
7. It shows the phone which is connected. Click on Next.

2. Retrieve call logs, text messages, and other relevant data for investigative purposes.

8. Click on Next.
9. Click on Whole system and click Next.
10. Click on case and click next.
11. Click on your device in the left panel.
12. You can see all the files.

---PRACTICAL 8--

Aim : Web Browser Forensics:

a) Analyze browser artifacts, including history files, bookmarks, and downloadrecords.

b) Analyze cache and cookies data to reconstruct user-browsing history and identifyvisited websites or online activities.

c) Extract the relevant log or timestamp file, analyze its contents and interpret thetimestamp data to determine the user'slast internet activity and associated details.

Steps :

1. Open Browser History Examiner.
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

---PRACTICAL 7--

Aim : Email Forensics:

a) Analyze email headers & content to trace the origin of suspicious emails.

b) Identify potential email forgeries or tampering.

Steps :

Recovering Email

1. Start AccessData FTK and click Start a new case, then click OK.
2. Click Next until you reach the Refine Case - Default dialog box Click the EmailEmphasis button, and then click Next
3. Create a new File.
4. Fill the details of the Examiner.
5. Click on all the options and Click Next
6. Select all the options.
7. Now we have reached the Email Emphasis section.
8. Click Next until you reach the Add Evidence to Case dialog box, and then click the AddEvidence button. In the Add Evidence to Case dialog box, click the Individual File option button, and then click Continue.
9. In the Select File dialog box, navigate to your work folder, click the Jim_shu's.pstfile, and then click Open.
10. Give some data.
11. Complete the steps and Click on Next.
12. Click on finish and see the data.
13. When the Add Evidence to Case dialog box opens, click Next. In the Case summary dialogbox, click Finish. When FTK finishes processing the file, in the main FTK window, click the Email Messages button, and then click the Full Path column header to sort the records.
14. For email recovery follow following steps: Click the E-Mail tab. In the tree view, click to expand all folders, and then click the Deleted Items folder.
15. Select any message say Message0001 right click and select option Launch DetachedViewer and you can see detail of deleted message.
16. For analyzing header follow following steps: Click the E-Mail tab. In the tree view, clickto expand all folders, and then click the Inbox folder. In the File List pane at the upper right, click Message0003; as shown in the pane at the bottom, it's from Sam and is addressed to Jim_shu@comcast.net.
17. Right-click on any message say Message0003 in the File List pane and click Export File. In the Export Files dialog box, click OK.
18. FTK saves exported files in the HTML format with no extension.
19. Right-click the Message0003 file and click Rename. Type Message0003.html and pressEnter.
20. Double-click Message0003.html to view it in a Web browser.