# ITFS Practical's

## Practical 1: ----------

**Q. Analyse hard drives or smart phones using forensic tools**

Tools: - **Autopsy: -** Digital forensic tool platform

- used to recover & analyze data
- helps in tracking user activities on a computer (file access, application usage)

Steps: -

- Open Autopsy (dog)
- Create new case
- Add case name, base directory (next)
- Add case no., examiner (next)
- Source image file → **Precious.img**, Time: Asia/ Calcutta
- Tap on keyword search
- Click on advanced
- Create new list (Test)
- Add names in the list (Peter, Sam, movie, etc)
- Click on finish (It will take some time to complete)
- Click on generate report, Results – HTML, All results (Finish)
- Click on the link to view report

## Practical 2: ----------

**Q. Detect OS, hostname, sessions and open ports through packet sniffing.**

Tools: - **CMD prompt, Nmap (Zenmap) & who.is : -**

- used to network discovery i.e. network inventory, port scanning, OS detection, security auditing

Steps: -

Run cmd prompt as administrator and run below codes:

1. systeminfo – information about system
2. hostname – which system is running

3. netstat – network status (Established, Close_wait, time_wait)
4. netstat –ano
5. ipconfig – To check ip address
6. nslookup – to check DNS
7. tracert www.siesascs.edu.in
   First hoop, Second hoop
   Where the packet is travelling (initiation to destination) Traceroot

Now open nmap:

1. Add target (www.youtube.com)
2. Select types of scan (intense scan, regular scan, ping scan, quick scan) & run
3. Below you will find the code as :
4. Nmap -T4 -A -V www.youtube.com
5. Copy and paste the code into cmd prompt and execute
6. Nmap -p22 scanme.nmap.org

Q. Why port is needed?

- It's a virtual point where network connections start & end
- It acts as communication end point for each specific process or service on a device

Now go to web page who.is

- Open browser and enter the url who.is
- Enter the target - www.youtube.com & run
- You will find all the details about youtube

## Practical 3: ----------

**Q. Capture the physical memory of a computer and analyse artifacts in memory.**

Tools: - **FTK (Forensic Toolkit) or AccessData FTK 181: -**

- FTK (Forensic Toolkit) is a comprehensive digital forensics software used for data acquisition, analysis, and reporting in criminal investigations and cybersecurity incidents.

Steps: -

1. Open FTK or Access Data FTK
2. Start a new case > OK
3. Add investigator name, case no., case name, case path (Create a folder cfprac and save this case inside it as **testprac**), description > Next
4. Add Agency, examiner, address, phone, email etc >Next
5. Case Log Options - Tick everything >Next
6. Processes to Perform - Tick everything >Next
7. Data Carving - Tick everything >OK
8. Refine Case – Unconditionally Add - Tick everything >Next
9. Refine Index – Unconditionally Add - Tick everything >Next

- Add Evidence – Click on Add Evidence > **Acquired Image of Drive** >Continue
- Add Evidence location as i.e. Select **sample1.img** (C:\sem4\cfprac\sample1.img)
- Add identification number or name, timezone as Asia/ Calcutta > OK
- Then Next & Finish
- A Overview window will be seen that will have all the analyzed data inside of sample1.img

Now click on Add Evidence:

1. Add investigator name, case no., case name, case path (Create a folder and save this case inside it as testprac), description > Next
2. Add Evidence to case > Select Individual File > Continue
3. Add Evidence location as i.e. Select **testprac.ftk** that you have saved prior (C:\sem4\cfprac\testprac\testprac.ftk) > OK
4. Then a Overview window will be seen will all the analyzed data inside of testprac.ftk
5. Now go to search and search for term ‘peter’ > Add
6. Add filter search hits as all files > OK
7. You will see all the files that contents peter in it

## Practical 4: ----------

**Q. Calculate the MD5 and SHA1 hashes**

Tools: - **CrypTool**

- Cryptool is a tool used for cryptographic analysis tool, i.e. to encrypt plain text into cipher text and decrypt cipher text into plaintext

Steps: -

1. Open CrypTool
2. Add new file > Add pain text for encryption > ETHICAL HACKING
3. Click on Encypt/ Decrypt (Select type of encryption Symmetric, Asymmetric, etc)
4. You will see the encrypted text (cipher text)
5. Now for decrypt encrypted text
6. Click on Encypt/ Decrypt (Select type of decryption Symmetric, Asymmetric, etc)
7. You will see the decrypted text (plain text)

## Practical 5: ----------

**Q. Use tools to collect, preserve and reveal digital evidence without compromising systems and data**

Tools: - **FTK imager**

- FTK Imager is a free forensic imaging software used to create exact copies of storage devices, preview data, recover deleted files, and verify data integrity.

Steps: -

1. Open FTK imager
2. Create new file or case
3. Select Source as Physical Drive > Next
4. Select Drive Selection as default (\\PHYSICALDRIVE0 ...) > Finish
5. Now Create image > In Image Destination > Click on Add
6. Select Raw (dd) > Next

7. Evidence Item Information > Add case no., evidence no., description, examiner > Next
8. Select Image Destination > provide path where it will be saved (C:\sem4\cfprac\ftkimager)
9. Give Image Filename as newimage > Finish
10. Tick on verify images after they are created > Start
11. It will take some time and provide result as Image Summary

## Practical 6: ----------

**Q. Acquire web pages for forensic investigation.**

**Q. Use traffic capturing and analysing tool. Using filters and using test login page.**

Tools: - **Wireshark**

- Wireshark is a network packet analyser that intercepts, captures and logs information about packets passing through a network interface.
- This is useful for analysing network problems, detecting network intrusions, network misuse, and other security problems, monitor usage and gather statistics

Steps: -

1. Open wireshark
2. Double click on Ethernet
3. Now surf on browser to capture packets for some time
4. In Filter type DNS, result will be seen (Analyse menu can also be used)
5. Type tcp, udp, http,https, etc
6. Now open your browser and enter url as http://testphp.vulweb.com
7. Enter username and password as 12345678 and click on login
8. Go back to wireshark and in filter search for http
9. In results find http / PORT (GET), click on the packet
10. Click on HTML Form url encoded (you will see uname & pass as 12345678)

## Practical 7: ----------

**Q. Use tools that scan a hard drive, locate deleted media and scan hard drive.**

Tools: - **FTK (Forensic Toolkit) or AccessData FTK 181 startup: -**

- FTK (Forensic Toolkit) is a comprehensive digital forensics software used for data acquisition, analysis, and reporting in criminal investigations and cybersecurity incidents.

Steps: -

10. Open FTK or Access Data FTK
11. Start a new case > OK
12. Add investigator name, case no., case name, case path (Create a folder cfprac and save this case inside it as **testprac1**), description > Next
13. Add Agency, examiner, address, phone, email etc >Next
14. Case Log Options - Tick everything >Next
15. Processes to Perform - Tick everything >Next
16. Data Carving - Tick everything >OK
17. Refine Case – Unconditionally Add - Tick everything >Next
18. Refine Index – Unconditionally Add - Tick everything >Next

- Add Evidence – Click on Add Evidence > **Acquired Image of Drive** >Continue
- Add Evidence location or Infomation as i.e. Select **sample1.img** (C:\sem4\cfprac\sample1.img)
- Add identification number or name, timezone as Asia/ Calcutta > OK
- Then Next & Finish
- A Overview window will be seen that will have all the analyzed data inside of sample1.img

## Practical 8: ----------

**Q. Use a tool to scan drive and its slack space.**

Tools: - **ProDiscover**

- ProDiscover Basic is a digital forensics tool used to capture and analyze data from storage devices.
- It helps investigators recover deleted files, search for hidden evidence, and create forensic images for legal proceedings.
- Additionally, it includes reporting tools to present findings in a structured manner.

Steps: -

1. Open ProDiscover
2. Create new project > Add case number, Project file name, Description > Open
3. A Capture Image window will pop up
4. Select Destination as the source file you want to analyze i.e. **prodiscover.cmp**
5. (eg. C:\cfprac\pracfiles\prodiscover\prodiscover.cmp) click on Open
6. Now click on password > add new password, confirm password > Ok
7. After that click on Finish, it will take some time and show the results under images menu on left pan.

Note: - Add the prodiscover.cmp file under a new folder and then select it for analysis.

## Practical 9: ----------

**Q. Hide text into image.**

Tools: - **QuickStego**

- QuickStego is a steganography tool that allows users to hide text messages within image files.

- It is used to securely embed secret messages in pictures so that only users with QuickStego can retrieve and read them.
- This tool is particularly useful for covert communication and protecting sensitive information

Steps: -

1. Open QuickStego Application
2. Download an image from browser to use it further (image1)
3. Upload the downloaded Image. This Image is term as Cover, as it will hide the text.
4. Enter the Text you want to hide (“How are you?”) or Upload Text File
5. Click on **Hide Text** button
6. Then **Save Image** Button – (image11_hidden) This Saved Image containing Hidden information is termed as Stego Object.

Recovering Data from Image Steganography using QuickStego:

1. Open QuickStego Application
2. Open the saved image (image11_hidden)
3. Now click on **Get text** Button
4. You will see the hidden content inside the image (“How are you?”)

## Practical 10: ----------

**Q. Use Email Forensic Tools for Email Recovery Mobile Forensics**

Tools: - **FTK (Forensic Toolkit) or AccessData FTK 181: -**

- FTK (Forensic Toolkit) is a comprehensive digital forensics software used for data acquisition, analysis, and reporting in criminal investigations and cybersecurity incidents.

Steps: -

19. Open FTK or Access Data FTK
20. Start a new case > OK
21. Add investigator name, case no., case name, case path (Create a folder cfprac and save this case inside it as **email1**), description > Next

22. Add Agency, examiner, address, phone, email etc >Next
23. Case Log Options - Tick everything >Next
24. Processes to Perform - Tick everything >Next
25. Data Carving - Tick everything >OK
26. Refine Case – Unconditionally Add - Tick everything >Next
27. Refine Index – Unconditionally Add - Tick everything >Next

- Add Evidence to case – **Individual File** >Continue
- Add Evidence as i.e. Select **Jim_shu's.pst** (C:\sem4\cfprac\ Jim_shu's.pst) > Next
- Add identification number or name, timezone as Asia/ Calcutta > OK
- Then Next & Finish
- An Overview window will be seen that will have all the analyzed data inside of Jim_shu's.pst
- Click on E-Mail Tab then click on any email and the content of that email will be seen below it