Cyber Forensics

Pract 1:- Ftk imager

Creating a forensic image using

Ftk imager/encase imager:-

-Creating forensic image

- check integrity of data

- Analyze forensic image

1)Ftk imager – file – create disk image – content of the file/folder – next – browse any file(select) – ok – finish.

2)Add – case no: 1 – evidence no:1 – unique description : pract 1 – next

3)Image destination folder – browse – desktop – image file name :ftk 1 – finish

4)Start – close the window that will appear – close

5)File – add evidence item – image file – next – enter Sourcepath (browse) – desktop -

ftk1.ad1(type: AD1 file***) – select – open – finish

6)+ ftkad1 expand – click on path – c:\user… ..

Pract 2 :- autopsy

Forensic case study:- solve the case study (image file) provide in lab using encase investigation or autopsy

1. Open – add new case – case name: 123 – base directory: browse – download – next
2. Case no :123 examiner: pooja – finish
3. Add data source – select source type to add – logical files – add – select any file- select – add – next – select all – next - finish
4. Open file come on screen(logical file set1) – select file - output

Pract 3 :- wire shark

Capturing and analyzing network packets using wireshark (fundamentals)

- Identification of live network
- Capture packets

- Analyze
    1. Capture – interface – select what having more packets – start
    2. Filter – following commands
       ip.addr == any one
       ip.src==
       ......

Pract 4 :- wire shark

Analyze the packets provided in lab and solve the question using wireshark

- What web server software is used by rrcbj…
- About what cell phone problem is that clients concerned…
    1. Wireshsrk – capture – start
    2. Chrome – rrcpryj.org just open – wireshark
    3. Filter – http – apply
    4. Down there will be Hypertext Transfer Protocol expand – right click on Host:rrcpryj.org\r\n – apply as column

5. Right click on blue line in filters (http) – follow tcp stream – output

Pract 5 :- sysinternals

To download sysinternals tools :- live.sysinternals.com-/(procmon diskmon rammap tcpview vmmap

1. Procmon.exe – open – tools – process tree (output) – tools - process activity summary (output)– tools - count occurance(output)
2. Rammap.exe- output
3. Tcpview.exe- chrome.exe – right click – whois – output
4. Vmmap.exe - ok- output

Cloud computing

Pract 1 :- owncloud

To study and implementation of identity management.

1. Chrome – demo.OwnCl
2. oud.org – fill details - + - new folder- tycd create – open tycs - + - upload – any image – open – click on share symbol – public links – create public link – share – copy to clipboard (small symbol in public link line)
3. Open new tab in chrome – demo.owncloud.org- output.

Pract 2:- google form

To study and implementation of storage as service

Google Drive- +new- new folder – google forms – now design.

Pract 3 :- infrastructures as a service theory

Pract 4 :- case study on google cloud platform theory

Pract 5 :- kvm

Pract 6:- usb server

File manager – this pc – local disk D – usb server – usb webserver –(if not opening down there will be sysmbol… . Hidden icons open from there) (***yoh have to find usb web server on pc)

New screen will open – setting – port apache change to 8085 – save – ok .

Again open web server – general – localhost – output.