CYBER FORENSICS

Write protected cables → used to only Read not write purpose.

beat stream copy → every bit will copy.

hash value →

presentation -
Acquisition -
Analysis -
Discovery -
Documentation -
presentation -

preservation ⇒ making sure that evidence is un-tampered with and continues to be in the same state in which it is found

Acquisition → The process of aquiring or gaining evidance. (Evidence collection Form

Analysis (Identification) → going through and discovering what type of information and evidence that we have acquired.

Discovery (Extraction) → Breaking down the acquired evidence and identifying the interested information with the use of tools and techniques.

Documentation → Mostly used For litigation (to file a ~~case~~ case - a controversy before a court or a 'lawsuit') purpose. serve to prove that we followed due diligence (due-care) when performing the investigations from biginning to the end

presentation of Evidence (Interpretation) → coverts everything that we have learned into understandable terms when conveyed to an interesting party.

Ctrl + shift + ++++ → zoom in
Ctrl + shift + ---- → zoom out

start Machine kali
HD - 200 GB
(actual size 25 GB) → compressed (10 GB)

1st connect pendrive → ~ sudo lsblk
~ sudo fdisk -l ← shows pendrive connected
~ what is dd ← convert and copy file
# zeroisation → run when dont want to hold data so used to wipe out data

~ sudo dd if=/dev/zero of=/dev/sdb
↑ disk

~ sudo dd if=/dev/zero | pv | sudo dd of=/dev/~~zero~~sdb

pv → monitor the progress of data through a pipe

~ sudo dd if=/dev/zero | pv | sudo dd of=/dev/~~zero~~sdb bs=16384
↑ bike size
16 mb size because pendrive size is 16 Mb

#

~ xxd abc.txt
→ prints hexadecimal val of text inside file

~ sudo xxd -a /dev/sdb
→ checks disk is empty or not
if it shows only 0000 then consider empty
if it shows any bit val then consider some data available inside disk

1 disk attach
2 disk partition
3 format
4 mount (mnt/disk) → Data copy → Data delete → Disk img create

hashval → Hard disk — dev/sdb } must same
evidence

dd if=/dev/zero | pv | sudo dd of=/dev/sdb bs=16384

- above cmd used to completely wipe (zero out) storage device (/dev/sdb) by overwriting it with 0x00 (null bytes)

- Erase all existing data from a drive by overwriting every sector with zeros.

- used with pv to observe real-time speed during a large write operation.

- prepare a disk for reuse by wiping old partitions and data.

dd - command line utility used for low-level copying and converting raw data

if=/dev/zero → if option specifies input file. /dev/zero is special file in linux that provides and endless stream of null characters.

| → pipe char connects ~~input~~ output of the first cmd (dd if=/dev/zero) to input of nex cmd pv.

pv → pipe viewer cmd.
visually monitors the data flowing through a pipe, displaying metrics like time elapsed, percentage complete, transfer speed.

dd → 2nd dd cmd takes output from pv command as its input

-R - used it to give permission to all files and also folder.

of=/dev/sdb → of option specifies the output file / device. The output is directed to the raw block device /dev/sdb, overwriting all existing data.

bs → option sets the block size for both the input and output operations
using large blocks size can significantly increase the speed of data transfer.

e.g bs 16384
bs 65536

after applying above cmd pendrive doesn't have any kind of data and no expert can get data back from this pendrive.
Now save any kind of data to pendrive and delete it and connect pendrive and run below commands

~ fdisk -l ← shows pendrive
~ sudo sha1sum /dev/sdb >> hash.txt
~ ~~dd if=/dev/sdb of=evidence.img bs=16384~~
~ sudo dd if=/dev/sdb | pv | sudo dd of=evidence.img bs=16384

→ create image

above cmd stores the img which was previously deleted.

~ ls
→ we can see our deleted file

~ sudo sha1sum evidence.img
~ sudo sha1sum evidence.img >> hash.txt
↑ this hash

through disk → do partition
mnt/ photo / panda.png

home/ star/ recover_data/ panda.png ← give permission chmod 777 panda.png

~ cat hash.txt

→ /dev/sdb
evidence.img } if the both hash val same then

1) # data Recovery Tool → Foremost

~ sudo apt install Foremost

~ mkdir recover_data ← create folder to store

~ sudo foremost -t all evidence.img -o recover_data/
(-o: output; evidence.img: data goes from; recover_data/: to)

~ sudo cd recover_d
~ chmod 777 /home/star/
~ ls
~ sudo sha1sum evidence.img >> hash.txt

} 4 same

2) # data Recovery Tool → bulk_extractor.
} scans a disk img for regular expressions and other content }

~ bulk_extractor -o recover_data
~ ls

Digital Forensics :-

- process of investigating computer equipment and associated storage media to determine if it has been used in the commision of a crime or unauthorized activities.
- It is the collection of techniques and tools used to find the evidence in a computer.

- What is a crime?
To breaks a law.

- What is the unauthorized Activity?
Generally related to organization. Un-authorized access / tried to access unauthorized resource. (breach of policy) -ex Accessing social media or Not safe For work content.

- What is cyber / digital crime?
Any crimindl activity that uses a computer either as an instrument or tool, target or.
as a means / incidental to crime For commiting crimes.

- Digital Forensic Investigatator
- skilled professionals - specialy trained
- produce repeatable results.
-Two opposing computer forensic experts work at the same information; they should come to the same conclusion, as far as the facts are concerned
skills required
- database
- cloud

- Firewall
- operating system
- Web servers
- logs generated by all of the above.
- Mobile
- virtualization
- forensic Tools
- How attacker works?
- how attacker penetrate systems

-professional skills -
written, verbal and presentation skills (Good communication).

- Types of investigation
- criminal (Law Enforcement)
- corporate (E-commerce sites, credit/debit card frauds, Insurance companies)
- private/civil (mainly in European countries).

Due-Diligence
- performing reasonable examination of and research before commiting to a course of action.
- Example - researching the terms of a contract before signing it.
- opposite of due-digigance is 'haphazard' or not doing your homework.
- ex. before taking an admission in DTISS you have performed an initial research.

Due-care
- performing the ongoing maintenance necessary to keep something in proper working order.
- The opposition of due care is 'negligence'

Evidence

4 types of evidences are there.

- Real (Real evidence that we can carry to court)
- Documentary (Documentary like attendance sheet, logbooks)
- Demonstrative (real demonstration like CCTV camera or the things can happen)
- Testimonial (Gawahi)

Locard's Exchange principle

Anyone or Anything, entering a crime scene takes something of the scene with them, and leaves something of them behind when they leave.

The Role of digital evidence -

is to establish credible link between the attacker, victim and the crime scene.

Characteristics of Digital Evidence -

- Admissible
- Authentic
- Complete
- Reliable
- Believeable

Fragility

the quality of being easily broken / damaged.

Anti-Digital Forensics (ADF) / Anti forensics :-

- ADF is an approach to manipulate, erase or obfuscate the digital data.
- Makes forensic examination difficult, time consuming, or impossible.

- some of the ADF methodologys
  - overwriting data and metadata(wiping)
  - obfusation of data (Encryption, Data masking, Tokenaization)
  - Hiding data (steganography)

~ sudo apt install exif ← used to read metadata shows info in jpg file

~ ls

~ exif img.jpg

Latitude 18, 38, 46.58
East or West longitude E
73 45 29.86
Altit.

osforensic tool

Steganography :- (add msg into photo and check it on notepad)

copy /b panda.jpg

```
#!/bin/bash
function sum()
{
    read -p "Enter two values: " num1 num2
    ans=$((num1+num2))
    echo "sum of $num1 and $num2 is $ans"
}
function mul()
    read -p "Enter two values: " num1 num2
    ans=$((num1*num2))
    echo "sum of $num1
}
echo "Welcome $USER"
echo "_____"
echo "1. Addition"
echo "2. Multiplication"
read -p "Enter a choice" choice
case $choice in
    1)
        sum
    ;;
    2)
        mul
    ;;
    *)
        cowsay "MB HE HE"
    ;;
```

esac

google logs :-
google →
Manage google account

bitrot (data decay)
gradual degradation and corruption of digital data stored on digital media over the time, leading to errors, unreadability or complete data loss

It occurs when individual bits, the fundamental bits of data (0s and 1s), flip (rotate) their state due to factors like environmental factors, physical wear, magnetic interferences radiation and even the leakage of electrical charges in solid-state drive.

this silent process can affect any storage medium including hard drives, SSD's, flash drives and optical discs

hack

~~set~~ password of physical machine :-

press shift key and Restart Machine

Troubleshout → command promt

> c
> cd windows
> cd system32
> copy sethc.exe tinku.exe
> del sethc.exe
> copy cmd.exe sethc.exe
> reboot
> exit

write password →

hold shift key
it will open cmd
> net users

> net user diksa *
→ write pass
→ Retype pass

Now
type pass to window → #
then we can able to open window.

~~Now~~ ~~open cmd run as administrator - copy tinku.exe.~~
~~c drive - windo - system32 →~~
Now recover machine as it is

c - win - system32 → seth.exe (delete it)

c - win - system32 → tinku.exe (rename to seth.exe)

go to cmd
> net user diliss *
→ pass
→ Retype pass

MAC Binding

DHCP
→ IP and MAC binding
Access Rules →
give access and deny to specific IP
content filter →
e.g chatgpt, instagram } we can block it by adding into content filter