Cyber Forensics (Set A)

Q1. Windows Networking: Run the relevant windows command and write the following:

ipconfig

- The IPv4 Address of your system
- The Subnet Mask
- The Default Gateway

Q2. Linux Networking: Use the relevant command for getting information about the domain google.com and write:

whois google.com

- The Creation Date of the domain
- The Registrar name

Q3. Wireshark Analysis: Capture traffic while running ping 8.8.8.8, filter using icmp. Write:

cmd

- The source and destination IP address of any Echo Request
- The source and destination IP address of its matching Echo Reply

Q4. Windows Registry Analysis: Explore Registry Editor and write the following (with the path of the key):

- One typed URL found in the browser's TypedURLs history currentuser\software\Microsoft\Internet Explorer\typedURLs
- One encrypted program name found in UserAssist
  currentuser\Software\Microsoft\Windows\currentVersion\Explorer\UserAssist\{GUID}\Count

Q5. How does the Windows Registry help reconstruct user activity during an investigation? Provide two useful artifacts and their relevance.

TypedURL's key → what user searched
UserAssist key → logs the programs that user ran

Cyber Forensics (Set B)

Q1. Windows Networking: Run a network statistics command with option *-ano* and write:

netstat

- One connection in the ESTABLISHED state
- One port that is LISTENING

Q2. Linux Networking: Run: dig google.com MX and dig google.com TXT. Write:

- Any one MX record listed
- Any one TXT record listed

Q3. Wireshark Analysis: Capture HTTP traffic by visiting http://neverssl.com, apply filter tcp.port == 80 (Relevant Port Number). Write:

- The packet numbers of the SYN, SYN-ACK, and ACK packets forming the TCP handshake

Q4. Windows Registry Analysis: Explore Registry Editor and write the following (with the path of the key):

currentuser\software\Microsoft\windows\CurrentVersion\Explorer\RunMRU

- The latest command listed under Run history (RunMRU)
- One network card description found under the system network interface history
  Local Machine\Software\Microsoft\WindowsNT\CurrentVersion\NetworkCards

Q5. How can the "whois" command help an investigator profile a suspicious domain used in phishing or command-and-control activity? Mention two useful applications.

Cyber Forensics (Set C)

Q1. Windows Networking: Run a windows command to query the domain facebook.com for its IP address. Write: nslookup

- Any one IP address returned for the domain

Q2. Linux Networking: Run: curl -I http://httpforever.com/. Write: HTTP header

- The Server value
- The Content-Type header value

Q3. Wireshark Analysis: Capture traffic and visit - https://tinyurl.com/ymp8znz2 , filter using http.response.code >= 300 && http.response.code < 400. Write:

- The HTTP response code observed
- The value shown in the Location field (redirect destination)

Q4. Windows Registry Analysis: Explore Registry Editor and write the following (with the path of the key):

- The ProductName of the operating system (LocalMachine\SOFTWARE\Microsoft\Windows NT\CurrentVersion)
- The currently configured Time Zone (LocalMachine\SYSTEM\CurrentControlSet\Control\TimeZoneInformation)

Q5. What forensic value does the TCP three-way handshake provide during traffic analysis, and how can abnormalities indicate malicious activity?