ST. XAVIER'S COLLEGE
MAITIGHAR, KATHMANDU, NEPAL
Post Box :7437
Contact: 4221365,4244636
Email: ktm@sxc.edu.np

सेन्ट जेभियर्स कलेज
माईतीघर, काठमाडौं, नेपाल
पो.ब.नं. : ७४३७
फोन : ४२२१३६५,४२४४६३६
ईमेल : ktm@sxc.edu.np

DEPARTMENT OF COMPUTER SCIENCE

Bachelor of Information Technology Management

LAB No. #1

Assignment – Basic Windows CMD Networking & Forensic Commands

Submitted By	Submitted To	Signature	Remarks
Babita Khadka 022BIM017 6th Semester - Section A	Mr. Anish Shrestha Computer Department St. Xavier's College		

Student Declaration

I hereby declare that I have completed **Lab 1: Basic Windows CMD Networking & Forensic** Commands under the guidance of **Mr. Anish Shrestha**. This work is my own and has not been submitted elsewhere.

Date:

Name: Babita Khadka

Signature:

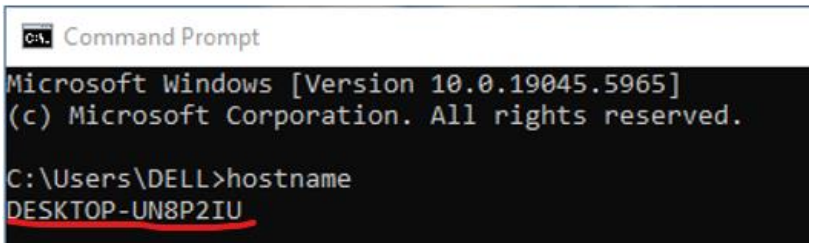
Lab 1: Assignment – Basic Windows CMD Networking & Forensic Commands

Lab Question 1: Network Scanning, Sniffing, and Identification in Windows OS

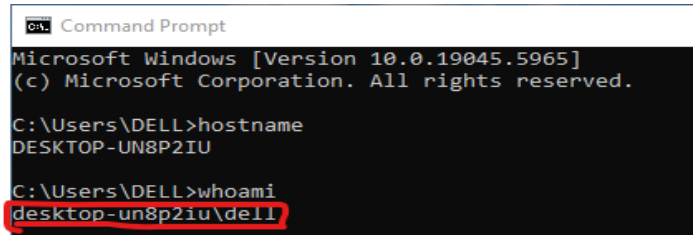
Solution :

1. System Information & Forensic

1. hostname → Display computer name.

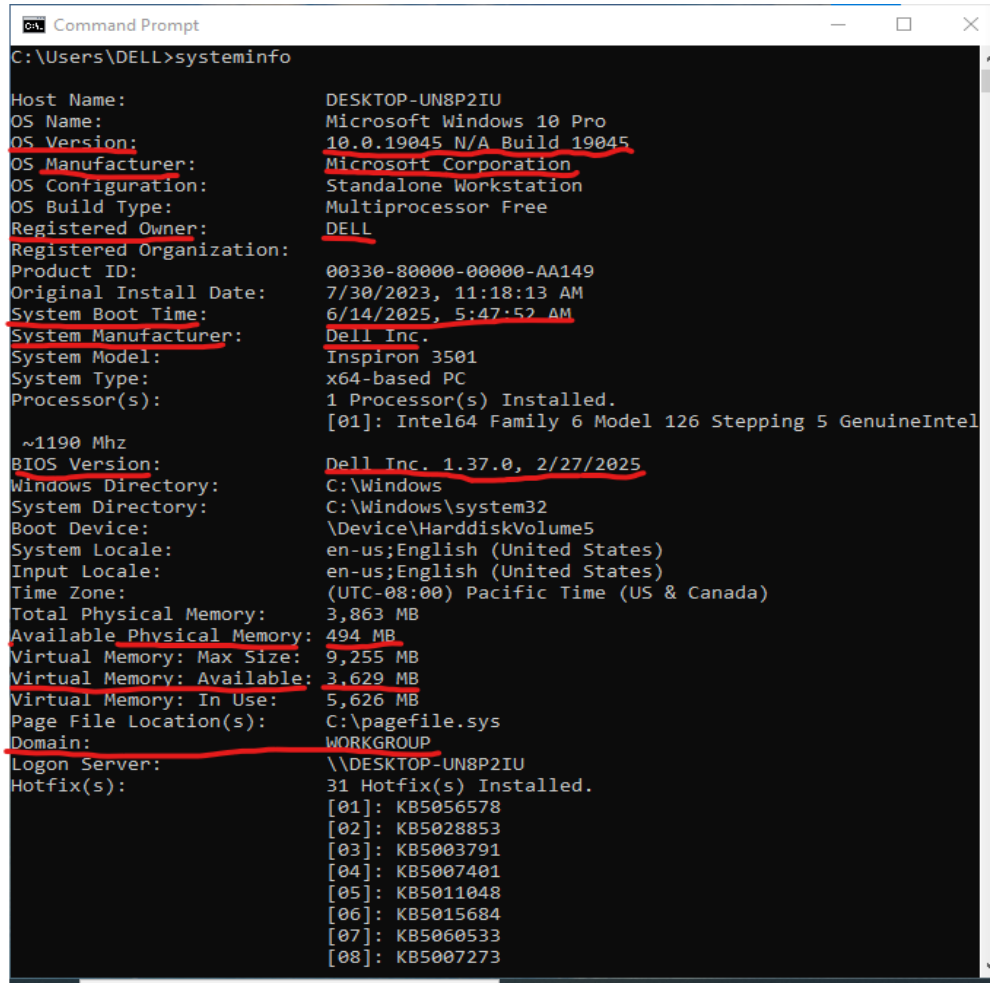
Windows CMD Syntax
• hostname
Screenshot/ Output

Objective/ Use in • Identify the computer name in a network. • Verify which machine you are connected to (useful in remote sessions).
Real world Scenario/ Use Case of this Syntax : • Used when connecting to a remote server or checking which machine you're working on in a network with multiple computers.

2. whoami → Show current logged-in username.

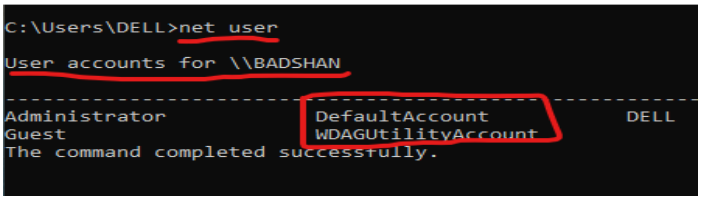
Windows CMD Syntax
• whoami
Screenshot/ Output

Objective/ Use in • Show the currently logged-in user.

• Verify account permissions before executing sensitive commands.
Real world Scenario/ Use Case of this Syntax : • Helpful in shared environments (like servers or corporate PCs) to confirm which user account is active before running commands.

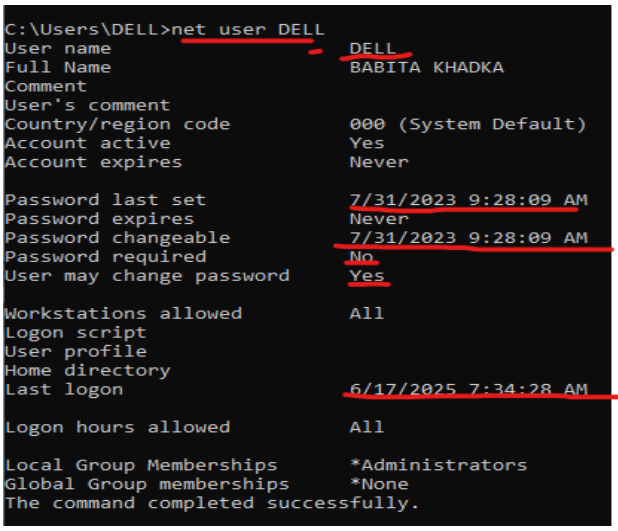
3. systeminfo → Display OS, BIOS, RAM, and boot info.

Windows CMD Syntax
• systeminfo
Screenshot/ Output

Objective/ Use in • Display system specs (OS, BIOS, RAM, updates). • Collect system details for troubleshooting or audits
Real world Scenario/ Use Case of this Syntax : • Useful for troubleshooting, auditing system specs, or verifying requirements before installing software.

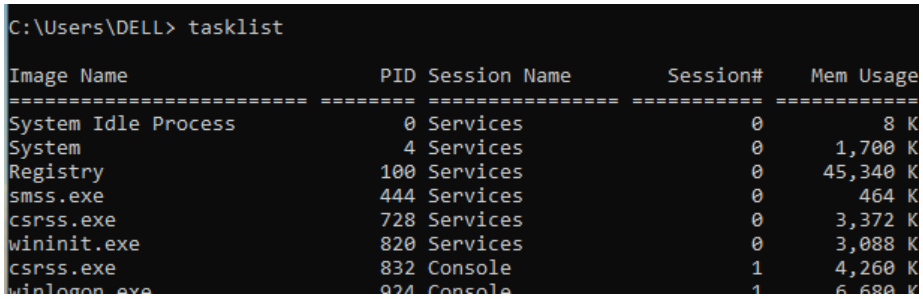
4. net user → List all local users on the system.

Windows CMD Syntax
• net user
Screenshot/ Output

Objective/ Use in • List all local users on a system. • Detect unauthorized or inactive accounts.
Real world Scenario/ Use Case of this Syntax : • Used by IT admins to quickly check which user accounts exist on a system (e.g., finding unused or suspicious accounts).

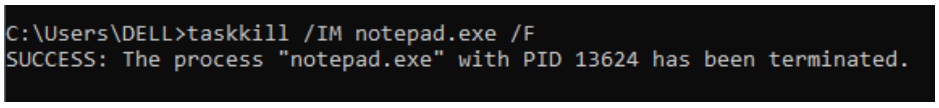
5. net user <username> → Show details of a specific user.

Windows CMD Syntax
• net user DELL
Screenshot/ Output

Objective/ Use in • Show details of a specific account (e.g., last logon, password rules). • Troubleshoot login issues or verify account status.
Real world Scenario/ Use Case of this Syntax : • Helpful for verifying account details like password rules, last logon, or account status when troubleshooting login issues.

6. tasklist → Display all running processes.

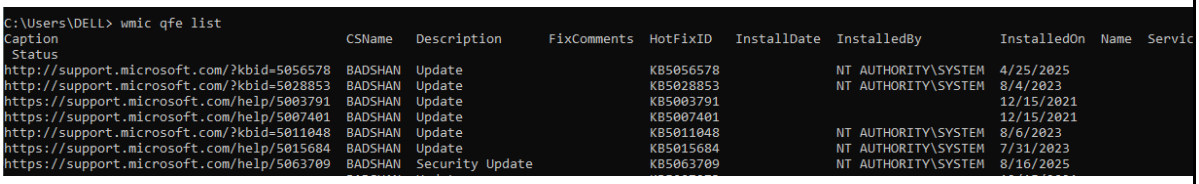
Windows CMD Syntax
• tasklist
Screenshot/ Output

Objective/ Use in • Display all running processes. • Check for resource-heavy or suspicious tasks.
Real world Scenario/ Use Case of this Syntax : • Used to monitor active applications and background services, especially when diagnosing system slowness.

7. taskkill /PID <id> /F → Terminate a running process.

Windows CMD Syntax
• taskkill /IM notepad.exe /F
Screenshot/ Output

Objective/ Use in • Forcefully terminate unresponsive programs. • Stop malware or unauthorized applications.
Real world Scenario/ Use Case of this Syntax : • Helpful to forcefully close frozen or malicious programs that aren't responding through Task Manager.

8. wmic qfe list → Show installed Windows updates (patch history).

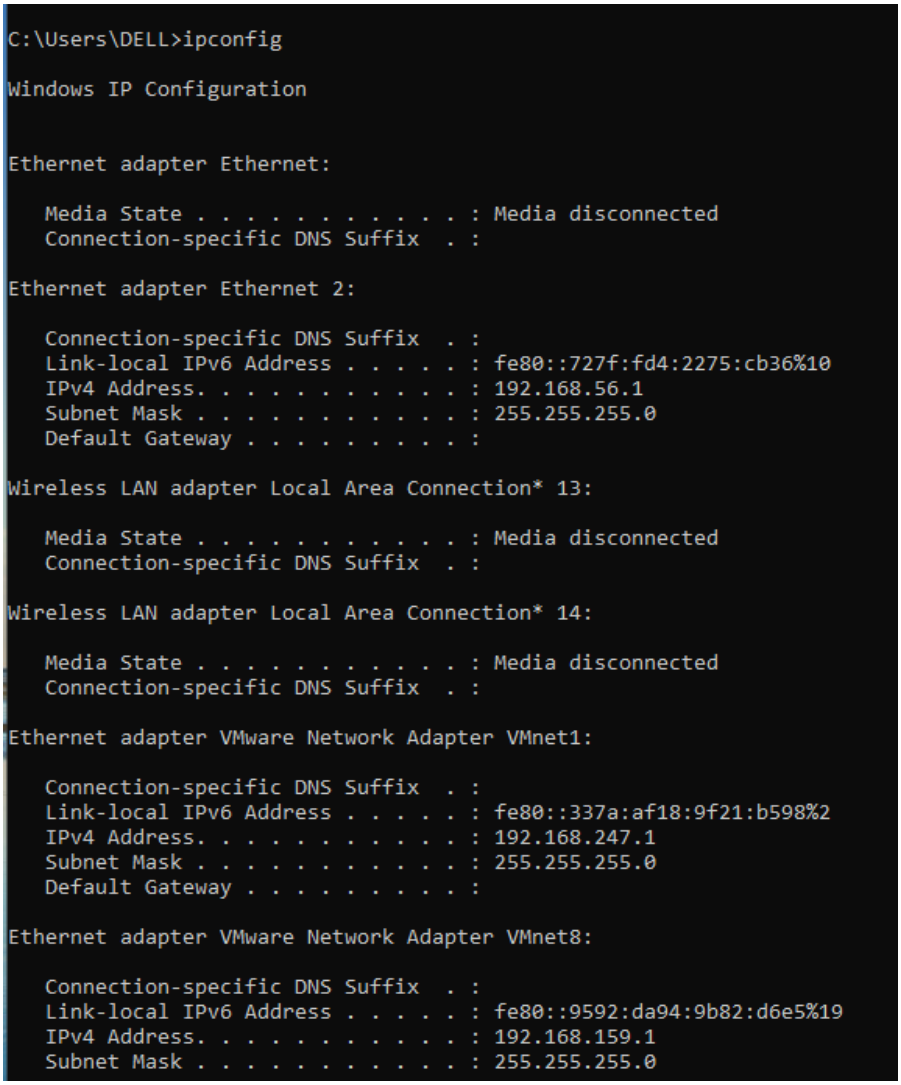
Windows CMD Syntax
• wmic qfe list

Screenshot/ Output

Objective/ Use in ● View installed Windows updates. ● Verify patch history for security compliance.
Real world Scenario/ Use Case of this Syntax : ● Used by admins to check if critical security patches are installed or to confirm update history during troubleshooting.

2. Network Configuration & Troubleshooting

9. ipconfig → Show IP address, subnet, gateway.

Windows CMD Syntax
● ipconfig
Screenshot/ Output



Objective/ Use in

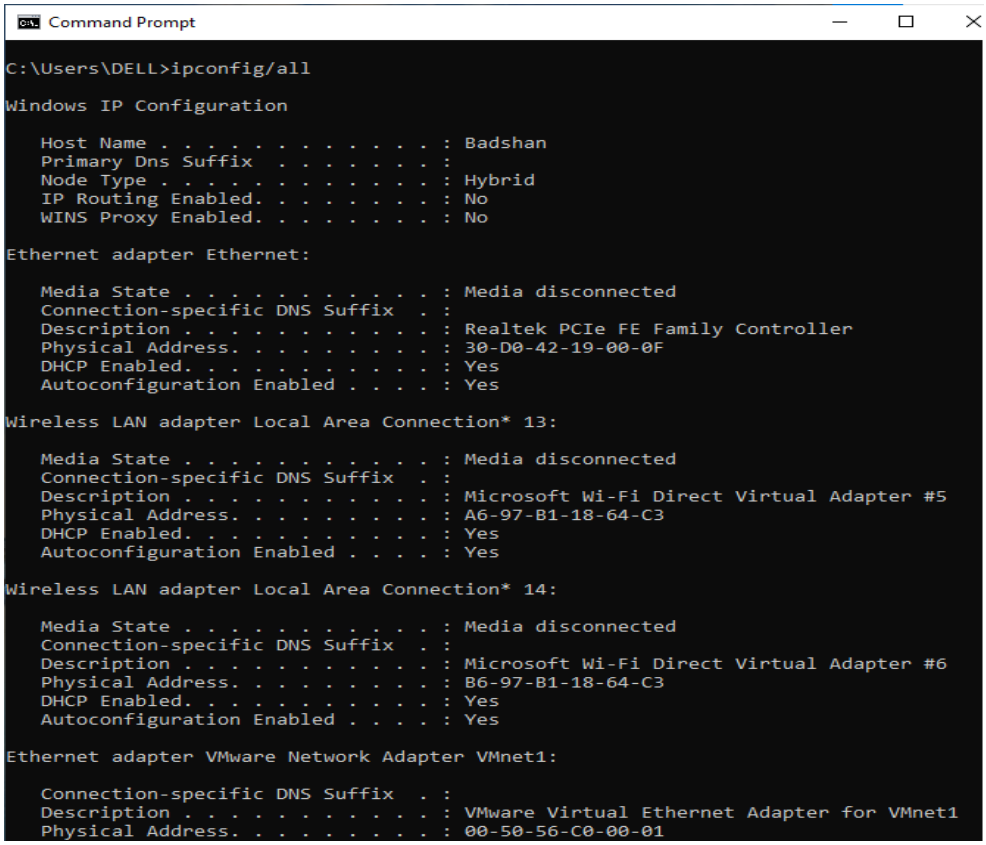
- Show current IP address, subnet, and gateway.
- Quickly check network configuration for troubleshooting.

Real world Scenario/ Use Case of this Syntax :

- Used to quickly check your computer's current network configuration, e.g., when diagnosing internet issues.

10. ipconfig /all → Display full network details (MAC, DNS, DHCP).

Windows CMD Syntax
• ipconfig/all
Screenshot/ Output



Objective/ Use in

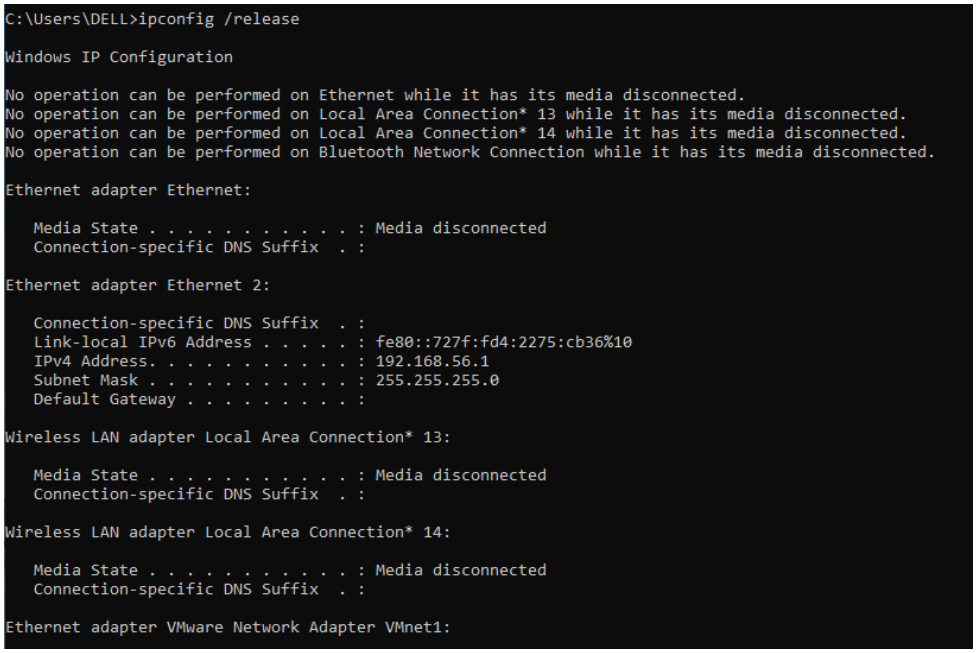
- Display detailed network info (DNS, MAC, DHCP).
- Provide IT support with full adapter configuration.

Real world Scenario/ Use Case of this Syntax :

- Helpful when IT support asks for detailed network info to resolve connection or DNS problems.

11. ipconfig /release → Release the current IP address.

Windows CMD Syntax
• ipconfig /release
Screenshot/ Output



Objective/ Use in

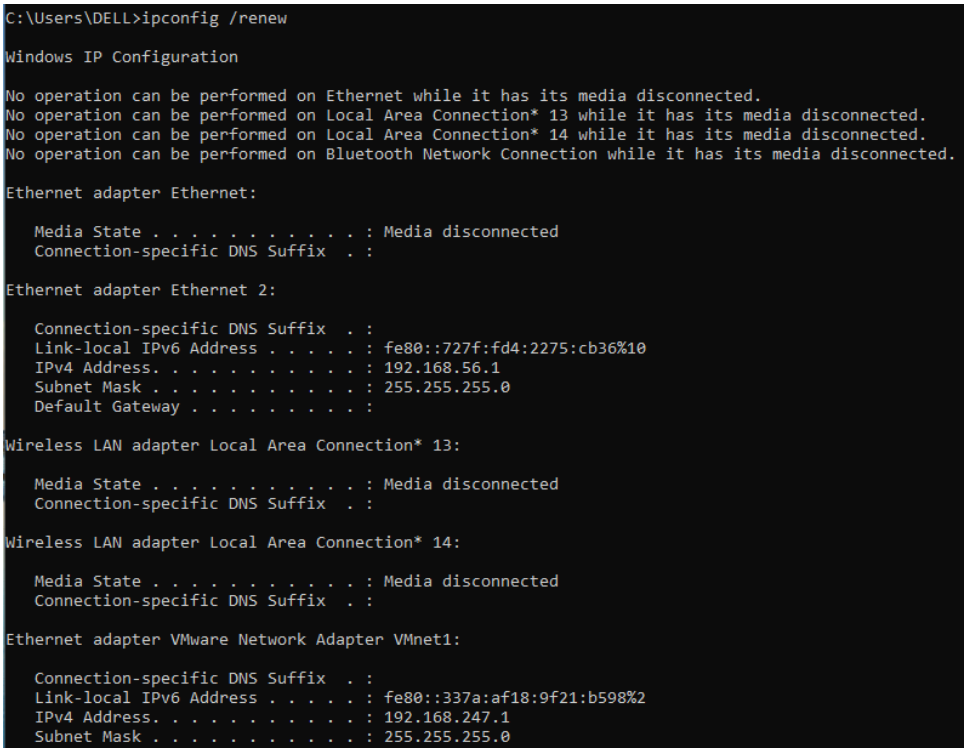
- Release the current IP address.
- Disconnect from network to resolve IP conflicts.

Real world Scenario/ Use Case of this Syntax :

- Used when you want to disconnect from the network or reset your IP address before requesting a new one.

12. ipconfig /renew → Request a new IP from DHCP.

Windows CMD Syntax
• ipconfig /renew
Screenshot/ Output



Objective/ Use in

- Request a new IP from DHCP server.
- Fix “limited/no internet” issues.

Real world Scenario/ Use Case of this Syntax :

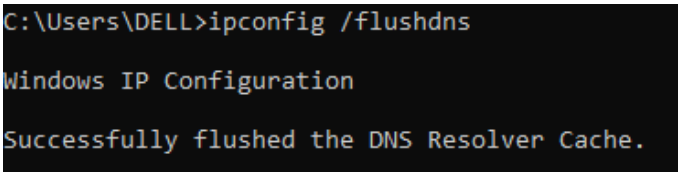
- Commonly used after /release to fix "no internet" issues caused by IP conflicts.

13. ipconfig /flushdns → Clear DNS cache (used to fix DNS errors).

Windows CMD Syntax

- ipconfig /flushdns

Screenshot/ Output



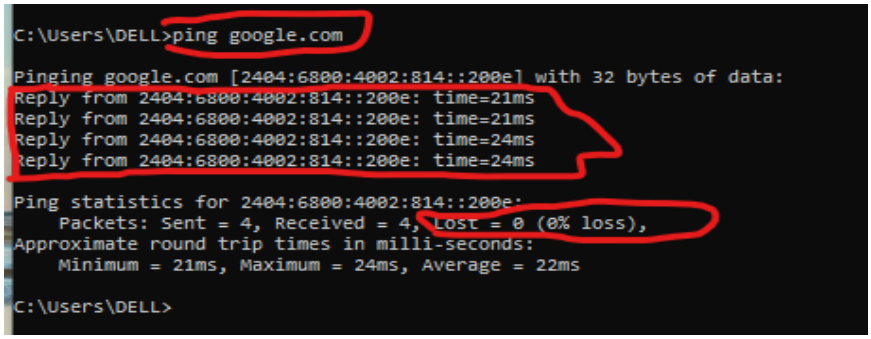
Objective/ Use in

- Clear DNS cache to resolve website loading errors.
- Remove outdated DNS entries for fresh resolution.

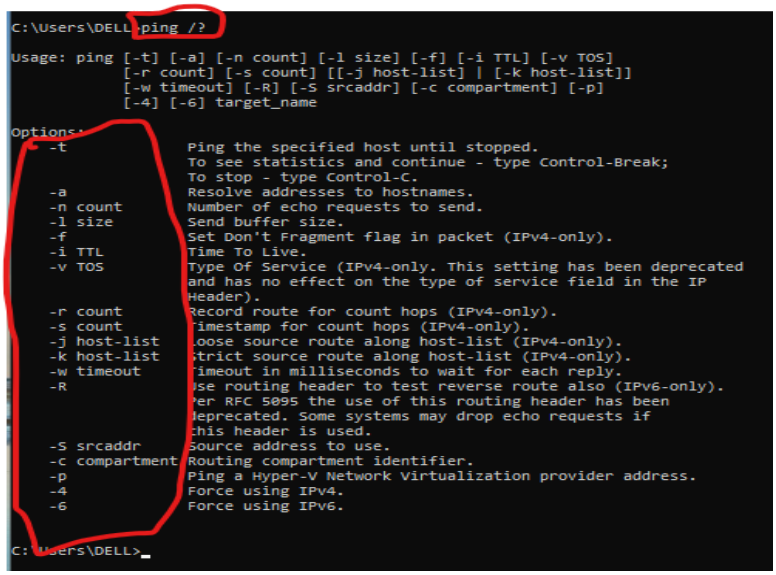
Real world Scenario/ Use Case of this Syntax :

- Useful when websites aren’t loading correctly due to cached DNS errors.

14. ping <IP/hostname> → Test connectivity to another host.

Windows CMD Syntax
• ping google.com
Screenshot/ Output

Objective/ Use in • Test basic connectivity to another host. • Measure response time and detect packet loss.
Real world Scenario/ Use Case of this Syntax : • First step in network troubleshooting to check if another computer, server, or website is reachable.

15. ping /? → Display ping command options.

Windows CMD Syntax
• ping/?
Screenshot/ Output

Objective/ Use in • Display available ping options. • Learn syntax for advanced ping testing.

Real world Scenario/ Use Case of this Syntax :

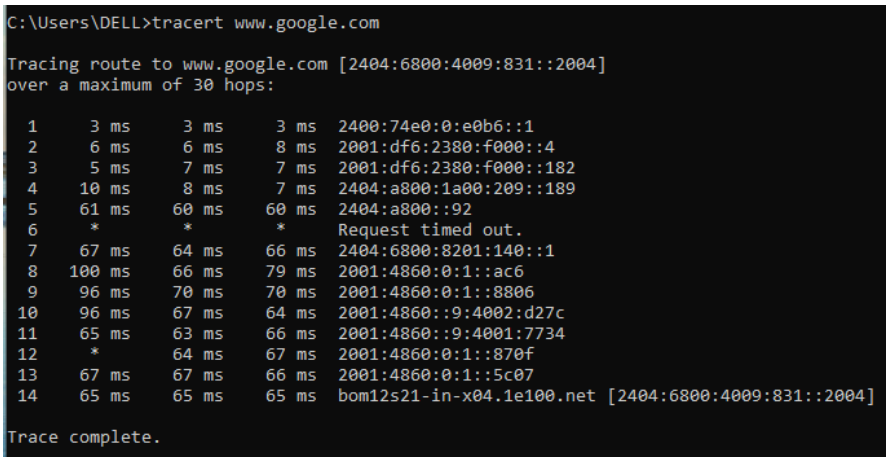
- Used when you forget specific flags (like setting packet count or timeout).

16. tracert <hostname> → Trace the route packets take to reach a host.

Windows CMD Syntax

- tracert www.google.com

Screenshot/ Output



Objective/ Use in

- Trace the route packets take to a destination.
- Identify where delays or failures occur in the path.

Real world Scenario/ Use Case of this Syntax :

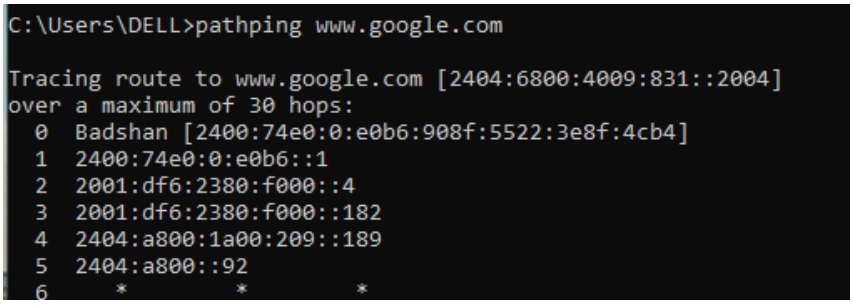
- Helps identify where a connection is slowing or failing between your PC and a remote server.

17. pathping <hostname> → Trace + analyze packet loss on each hop.

Windows CMD Syntax

- pathping www.google.com

Screenshot/ Output



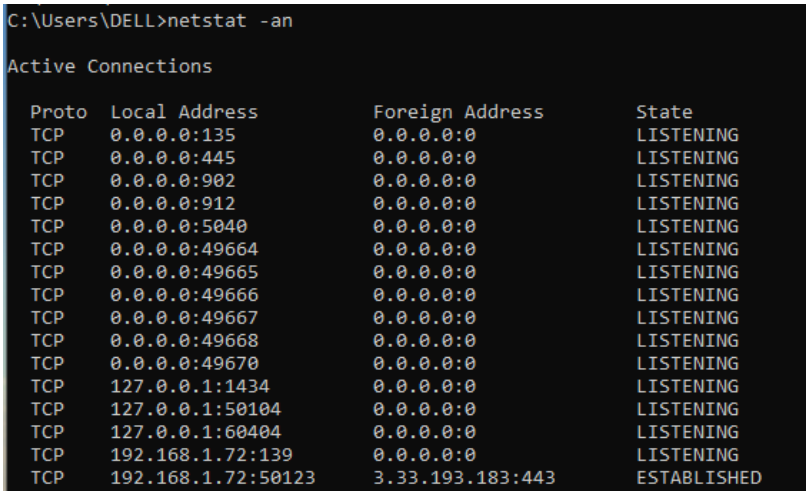
Objective/ Use in

- Trace packet route with additional packet loss analysis.

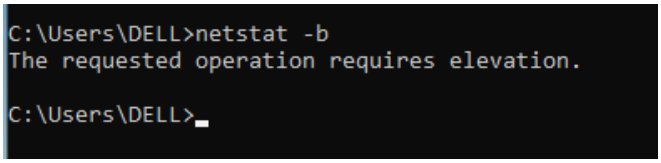
• Troubleshoot unstable or high-latency network connections.
Real world Scenario/ Use Case of this Syntax : • Used for deeper troubleshooting to find out if packet loss occurs at a specific router along the path.

3. Network Scanning & Connections

18. netstat -an → Show all active network connections and ports.

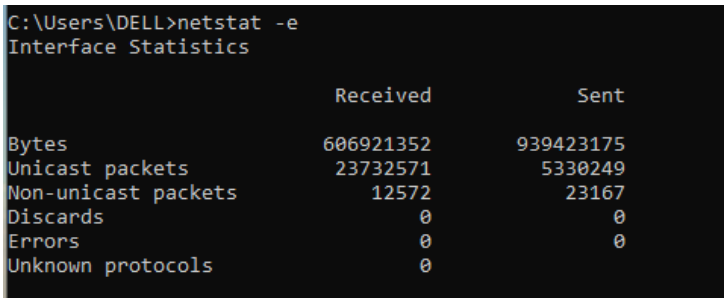
Windows CMD Syntax
• netstat -an
Screenshot/ Output

Objective/ Use in • Show all active network connections and ports. • Detect unusual or unauthorized connections.
Real world Scenario/ Use Case of this Syntax : • Helpful to see if unknown or suspicious connections are open on your system.

19. netstat -b → Show which programs opened connections.

Windows CMD Syntax
• netstat -b
Screenshot/ Output

Objective/ Use in

• Display which programs opened network connections. • Identify malware or suspicious software behavior.
Real world Scenario/ Use Case of this Syntax : • Used in security checks to identify which apps are using the internet, e.g., spotting malware connections.

20. netstat -e → Show Ethernet statistics (packets sent/received).

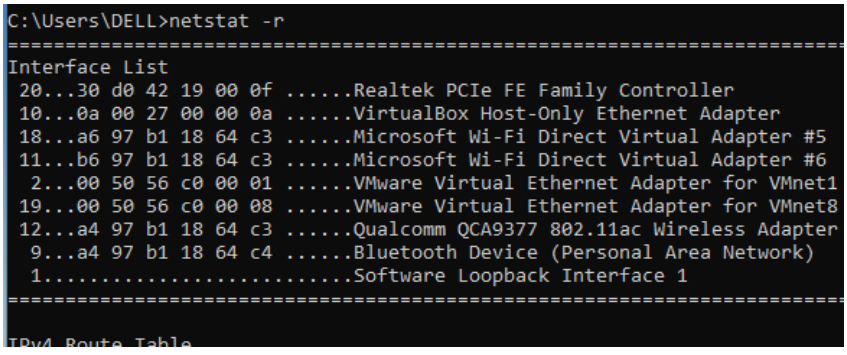
Windows CMD Syntax
• netstat -e
Screenshot/ Output

Objective/ Use in • Show Ethernet stats (packets sent/received). • Monitor network card activity and detect dropped packets.
Real world Scenario/ Use Case of this Syntax : • Useful for monitoring if data is flowing properly over your network card, e.g., checking if packets are being dropped.

```
C:\Users\DELL>netstat -e
Interface Statistics

                           Received            Sent

Bytes                     606921352       939423175
Unicast packets            23732571         5330249
Non-unicast packets           12572           23167
Discards                          0               0
Errors                            0               0
Unknown protocols                 0
```

21. netstat -r or route print → Show routing table of your system.

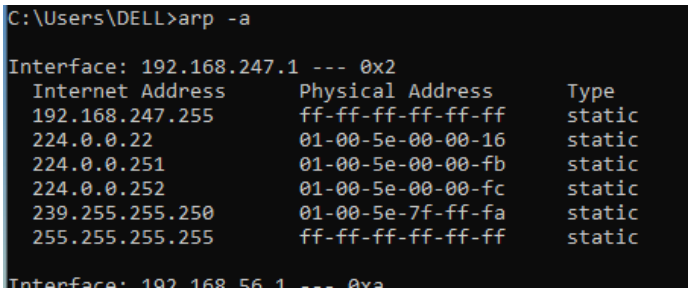
Windows CMD Syntax
• netstat -r
Screenshot/ Output


```
C:\Users\DELL>netstat -r
===========================================================================
Interface List
 20...30 d0 42 19 00 0f ......Realtek PCIe FE Family Controller
 10...0a 00 27 00 00 0a ......VirtualBox Host-Only Ethernet Adapter
 18...a6 97 b1 18 64 c3 ......Microsoft Wi-Fi Direct Virtual Adapter #5
 11...b6 97 b1 18 64 c3 ......Microsoft Wi-Fi Direct Virtual Adapter #6
  2...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 19...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
 12...a4 97 b1 18 64 c3 ......Qualcomm QCA9377 802.11ac Wireless Adapter
  9...a4 97 b1 18 64 c4 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
```

Objective/ Use in ● Display routing table. ● Verify correct gateway and route configurations.
Real world Scenario/ Use Case of this Syntax : ● Helps network admins troubleshoot how traffic is being routed (e.g., verifying default gateway issues).

22. arp -a → Display MAC addresses of devices in the local network.

Windows CMD Syntax
● arp -a
Screenshot/ Output

Objective/ Use in ● Show MAC addresses of local devices. ● Detect unknown devices on LAN for security checks.
Real world Scenario/ Use Case of this Syntax : ● Commonly used to detect devices on the same LAN, useful for network troubleshooting or spotting unknown devices.

4. Wireless & Firewall Investigation

23. netsh wlan show profiles → Show all saved Wi-Fi profiles.

Windows CMD Syntax
● netsh wlan show profiles
Screenshot/ Output

```
C:\Users\DELL>netsh wlan show profiles

Profiles on interface Wi-Fi:

Group policy profiles (read only)
---------------------------------
    <None>

User profiles
-------------
    All User Profile     : St. Xavier
    All User Profile     : Computer
    All User Profile     : mandipkdk1_5
    All User Profile     : potato
    All User Profile     : ALHN-2FEF-5
    All User Profile     : ALHN-2FEF
    All User Profile     : carrot
    All User Profile     : what
    All User Profile     : Big D
    All User Profile     : NTFiber_C4A8_2.4G
```

Objective/ Use in

- Show saved Wi-Fi networks.
- Check history of previously connected networks.

Real world Scenario/ Use Case of this Syntax :

- Handy to see which Wi-Fi networks a laptop has previously connected to.

24. netsh wlan show profile name=<SSID> key=clear → Show Wi-Fi password of a saved profile.

Windows CMD Syntax

- netsh wlan show profile name= ”Big D”key=clear

Screenshot/ Output

```
C:\Users\DELL>netsh wlan show profile name="Big D" key=clear

Profile Big D on interface Wi-Fi:
=======================================================================

Applied: All User Profile

Profile information
-------------------
    Version                : 1
    Type                   : Wireless LAN
    Name                   : Big D
    Control options        :
        Connection mode    : Connect automatically
        Network broadcast  : Connect only if this network is broadcasting
        AutoSwitch         : Do not switch to other networks
        MAC Randomization  : Disabled
```

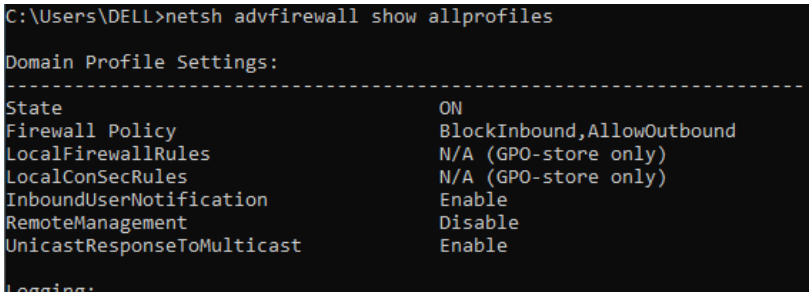
Objective/ Use in

- Display Wi-Fi password for a saved network.
- Recover forgotten Wi-Fi credentials.

Real world Scenario/ Use Case of this Syntax :

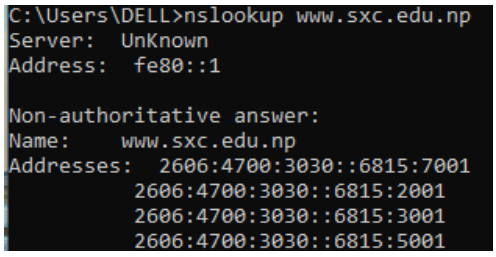
- Useful when you forget your Wi-Fi password but need to share it with someone else.

25. netsh advfirewall show allprofiles → Show firewall status for all profiles.

Windows CMD Syntax
• netsh advfirewall show allprofiles
Screenshot/ Output

Objective/ Use in • Show firewall status for all profiles. • Verify firewall rules and protection state.
Real world Scenario/ Use Case of this Syntax : • Used by admins to check if Windows Firewall is enabled across all profiles (Domain, Private, Public).

5. DNS & Domain Investigation

26. nslookup <domain> → Check DNS resolution of a website.

Windows CMD Syntax
• nslookup www.sxc.edu.np
Screenshot/ Output

Objective/ Use in • Check DNS resolution of a website. • Troubleshoot website access issues.
Real world Scenario/ Use Case of this Syntax : • First step when a website doesn't load — verifies if DNS is resolving the hostname to an IP.

27. nslookup -type=MX <domain> → Find mail server records.

Windows CMD Syntax

- nslookup -type=MX www.google.com

Screenshot/ Output

```
C:\Users\DELL>nslookup -type=MX www.google.com
Server:  UnKnown
Address:  fe80::1

google.com
        primary name server = ns1.google.com
        responsible mail addr = dns-admin.google.com
        serial  = 801461948
        refresh = 900 (15 mins)
        retry   = 900 (15 mins)
        expire  = 1800 (30 mins)
        default TTL = 60 (1 min)
```

Objective/ Use in
- Find mail server records for a domain.
- Verify email configuration during troubleshooting.

Real world Scenario/ Use Case of this Syntax :
- Helpful for IT/email admins when diagnosing email delivery issues.

28. nslookup -type=NS <domain> → Find authoritative name servers.

Windows CMD Syntax

- nslookup -type=NS www.google.com

Screenshot/ Output

```
C:\Users\DELL>nslookup -type=NS www.google.com
Server:  UnKnown
Address:  fe80::1

google.com
        primary name server = ns1.google.com
        responsible mail addr = dns-admin.google.com
        serial  = 801461948
        refresh = 900 (15 mins)
        retry   = 900 (15 mins)
        expire  = 1800 (30 mins)
        default TTL = 60 (1 min)
```

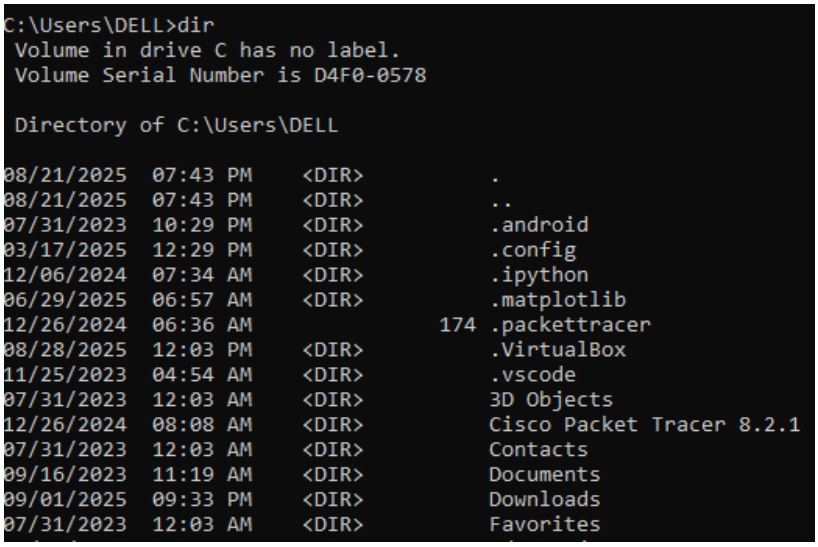
Objective/ Use in
- Show authoritative name servers for a domain.
- Diagnose DNS delegation and configuration problems.

Real world Scenario/ Use Case of this Syntax :
- Used when checking domain configuration or troubleshooting DNS delegation problems.

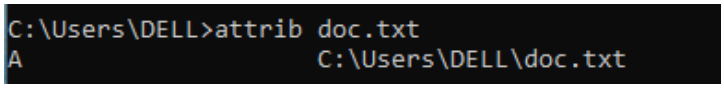
6. File & Disk Forensics

29. dir → List files and directories.

Windows CMD Syntax

• dir
Screenshot/ Output

Objective/ Use in • List files and directories in a folder. • Quickly browse contents without File Explorer.
Real world Scenario/ Use Case of this Syntax : • Everyday use for browsing contents of a folder in Command Prompt.

30. attrib <filename> → Check file attributes (hidden, read-only).

Windows CMD Syntax
• attrib doc.txt
Screenshot/ Output

Objective/ Use in • Display attributes of a file (hidden, read-only, system). • Modify or diagnose file permission issues.
Real world Scenario/ Use Case of this Syntax : • Handy for finding out if a file is hidden, read-only, or system-protected.

31. fsutil fsinfo drives → Show available drives.

Windows CMD Syntax
• fsutil fsinfo drives
Screenshot/ Output

```
C:\Users\DELL>fsutil fsinfo drives

Drives: C:\ D:\ E:\ F:\
```

Objective/ Use in

- List all available drives on the system.
- Check storage device availability before backup or install.

Real world Scenario/ Use Case of this Syntax :

- Useful to quickly list all storage drives connected to the system.

32. chkdsk → Check disk health & errors.

Windows CMD Syntax

- chkdsk

Screenshot/ Output

```
C:\Windows\system32>chkdsk
The type of the file system is NTFS.

WARNING!  /F parameter not specified.
Running CHKDSK in read-only mode.

Stage 1: Examining basic file system structure ...

919552 file records processed.
File verification completed.
 Phase duration (File record verification): 16.78 seconds.

25835 large file records processed.
 Phase duration (Orphan file record recovery): 0.00 milliseconds.

0 bad file records processed.
 Phase duration (Bad file record checking): 0.30 milliseconds.
```

Objective/ Use in

- Scan disk for errors and repair bad sectors.
- Improve performance and prevent data loss.

Real world Scenario/ Use Case of this Syntax :

- Run when a drive is acting slow or showing file corruption to scan and fix errors.

Conclusion

Write *Key learnings from performing the lab.* (*Importance of CMD in networking & forensic investigation.)*