

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

सेन्ट जेमियर्स कलेज
माईतीधर, काठमाडौं, नेपाल
पो.ब.नं. : ७४३७
फोन : ५२२१३६५, ५२४४६३६
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:

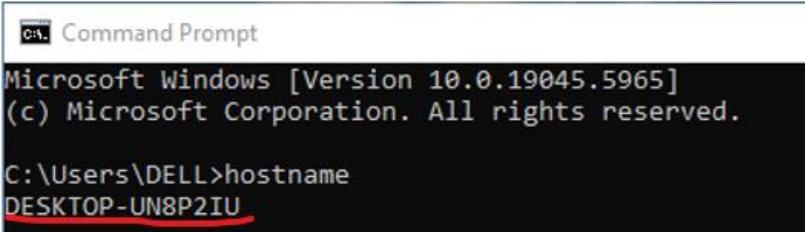
Lab 1: Assignment – Basic Windows CMD Networking & Forensic Commands

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

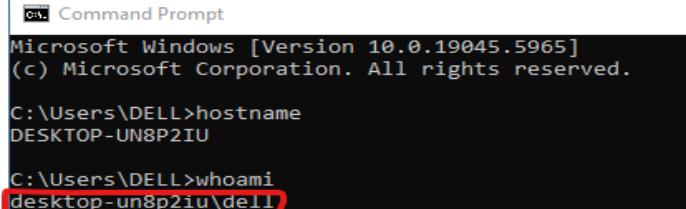
Solution :

1. System Information & Forensic

1. **hostname** → Display computer name.

Windows CMD Syntax
<ul style="list-style-type: none">● hostname
Screenshot/ Output

Objective/ Use in <ul style="list-style-type: none">● 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 : <ul style="list-style-type: none">● 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
<ul style="list-style-type: none">● whoami
Screenshot/ Output

Objective/ Use in <ul style="list-style-type: none">● 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

```

C:\> Command Prompt
C:\Users\DELL>systeminfo

Host Name: DESKTOP-UN8P2IU
OS Name: Microsoft Windows 10 Pro
OS Version: 10.0.19045 N/A Build 19045
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Multiprocessor Free
Registered Owner: DELL
Registered Organization: 00330-80000-00000-AA149
Product ID: 7/30/2023, 11:18:13 AM
Original Install Date: 6/14/2025, 5:47:52 AM
System Boot Time: Dell Inc.
System Manufacturer: Inspiron 3501
System Model: x64-based PC
System Type: 1 Processor(s) Installed.
Processor(s):
~1190 Mhz
Processor(s):
[01]: Intel® Family 6 Model 126 Stepping 5 GenuineIntel
BIOS Version: Dell Inc. 1.37.0, 2/27/2025
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume5
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory: 3,863 MB
Available Physical Memory: 494 MB
Virtual Memory: Max Size: 9,255 MB
Virtual Memory: Available: 3,629 MB
Virtual Memory: In Use: 5,626 MB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
Logon Server: \\DESKTOP-UN8P2IU
Hotfix(s):
31 Hotfix(s) Installed.
[01]: KB5056578
[02]: KB5028853
[03]: KB5003791
[04]: KB5007401
[05]: KB5011048
[06]: KB5015684
[07]: KB5060533
[08]: KB5007273

```

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

```
C:\Users\DELL>net user
User accounts for \\BADSHAN
-----
Administrator          DefaultAccount
Guest                  WDAGUtilityAccount
The command completed successfully.
```

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

```
C:\Users\DELL>net user DELL
User name          DELL
Full Name          BABITA KHADKA
Comment
User's comment
Country/region code    000 (System Default)
Account active      Yes
Account expires     Never
Password last set   7/31/2023 9:28:09 AM
Password expires    Never
Password changeable 7/31/2023 9:28:09 AM
Password required   No
User may change password Yes
Workstations allowed All
Logon script
User profile
Home directory
Last logon          6/17/2025 7:34:28 AM
Logon hours allowed All
Local Group Memberships *Administrators
Global Group memberships *None
The command completed successfully.
```

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
<ul style="list-style-type: none">• <code>tasklist</code>
Screenshot/ Output
<pre>C:\Users\DELL> tasklist Image Name PID Session Name Session# Mem Usage ===== System Idle Process 0 Services 0 8 K System 4 Services 0 1,700 K Registry 100 Services 0 45,340 K smss.exe 444 Services 0 464 K csrss.exe 728 Services 0 3,372 K wininit.exe 820 Services 0 3,088 K csrss.exe 832 Console 1 4,260 K winlogon.exe 924 Console 1 6,680 K</pre>
Objective/ Use in
<ul style="list-style-type: none">• Display all running processes.• Check for resource-heavy or suspicious tasks.
Real world Scenario/ Use Case of this Syntax :
<ul style="list-style-type: none">• 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
<ul style="list-style-type: none">• <code>taskkill /IM notepad.exe /F</code>
Screenshot/ Output
<pre>C:\Users\DELL>taskkill /IM notepad.exe /F SUCCESS: The process "notepad.exe" with PID 13624 has been terminated.</pre>
Objective/ Use in
<ul style="list-style-type: none">• Forcefully terminate unresponsive programs.• Stop malware or unauthorized applications.
Real world Scenario/ Use Case of this Syntax :
<ul style="list-style-type: none">• 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
<ul style="list-style-type: none">• <code>wmic qfe list</code>

Screenshot/ Output

Caption	CSName	Description	FixComments	HotFixID	InstallDate	InstalledBy	InstalledOn	Name	Service
Status									
http://support.microsoft.com/?kbid=5056578	BADSHAN	Update		KB5056578		NT AUTHORITY\SYSTEM	4/25/2025		
http://support.microsoft.com/?kbid=5028853	BADSHAN	Update		KB5028853		NT AUTHORITY\SYSTEM	8/4/2023		
https://support.microsoft.com/help/5003791	BADSHAN	Update		KB5003791			12/15/2021		
https://support.microsoft.com/help/5007401	BADSHAN	Update		KB5007401			12/15/2021		
http://support.microsoft.com/?kbid=5011048	BADSHAN	Update		KB5011048		NT AUTHORITY\SYSTEM	8/6/2023		
https://support.microsoft.com/help/5015684	BADSHAN	Update		KB5015684		NT AUTHORITY\SYSTEM	7/31/2023		
https://support.microsoft.com/help/5063709	BADSHAN	Security Update		KB5063709		NT AUTHORITY\SYSTEM	8/16/2025		

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

```
C:\Users\DELL>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Ethernet adapter Ethernet 2:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::727f:fd4:2275:cb36%10
IPv4 Address. . . . . : 192.168.56.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Wireless LAN adapter Local Area Connection* 13:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 14:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Ethernet adapter VMware Network Adapter VMnet1:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::337a:af18:9f21:b598%2
IPv4 Address. . . . . : 192.168.247.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::9592:da94:9b82:d6e5%19
IPv4 Address. . . . . : 192.168.159.1
Subnet Mask . . . . . : 255.255.255.0
```

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

```

C:\Users\DELL>ipconfig/all
Windows IP Configuration

Host Name . . . . . : Badshan
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : Realtek PCIe FE Family Controller
    Physical Address. . . . . : 30-D0-42-19-00-0F
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Local Area Connection* 13:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #5
    Physical Address. . . . . : A6-97-B1-18-64-C3
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Local Area Connection* 14:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #6
    Physical Address. . . . . : B6-97-B1-18-64-C3
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : VMware Virtual Ethernet Adapter for VMnet1
    Physical Address. . . . . : 00-50-56-C0-00-01

```

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

```
C:\Users\DELL>ipconfig /release

Windows IP Configuration

No operation can be performed on Ethernet while it has its media disconnected.
No operation can be performed on Local Area Connection* 13 while it has its media disconnected.
No operation can be performed on Local Area Connection* 14 while it has its media disconnected.
No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

Ethernet adapter Ethernet:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Ethernet adapter Ethernet 2:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::727f:fd4:2275:cb36%10
  IPv4 Address . . . . . : 192.168.56.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Wireless LAN adapter Local Area Connection* 13:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 14:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Ethernet adapter VMware Network Adapter VMnet1:
```

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

```
C:\Users\DELL>ipconfig /renew

Windows IP Configuration

No operation can be performed on Ethernet while it has its media disconnected.
No operation can be performed on Local Area Connection* 13 while it has its media disconnected.
No operation can be performed on Local Area Connection* 14 while it has its media disconnected.
No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::727f:fd4:2275:cb36%10
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Wireless LAN adapter Local Area Connection* 13:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 14:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::337a:af18:9f21:b598%2
    IPv4 Address. . . . . : 192.168.247.1
    Subnet Mask . . . . . : 255.255.255.0
```

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

```
C:\Users\DELL>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

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

```
C:\Users\DELL>ping google.com

Pinging google.com [2404:6800:4002:814::200e] with 32 bytes of data:
Reply from 2404:6800:4002:814::200e: time=21ms
Reply from 2404:6800:4002:814::200e: time=21ms
Reply from 2404:6800:4002:814::200e: time=24ms
Reply from 2404:6800:4002:814::200e: time=24ms

Ping statistics for 2404:6800:4002:814::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 21ms, Maximum = 24ms, Average = 22ms

C:\Users\DELL>
```

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

```
C:\Users\DELL>ping /?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
           [-r count] [-s count] [[-j host-list] | [-k host-list]]
           [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
           [-4] [-6] target_name

Options:
  -t          Ping the specified host until stopped.
              To see statistics and continue - type Control-Break;
              To stop - type Control-C.
  -a          Resolve addresses to hostnames.
  -n count    Number of echo requests to send.
  -l size     Send buffer size.
  -f          Set Don't Fragment flag in packet (IPv4-only).
  -i TTL      Time To Live.
  -v TOS      Type of Service (IPv4-only. This setting has been deprecated
              and has no effect on the type of service field in the IP
              Header).
  -r count    Record route for count hops (IPv4-only).
  -s count    timestamp for count hops (IPv4-only).
  -j host-list  Choose source route along host-list (IPv4-only).
  -k host-list  Strict source route along host-list (IPv4-only).
  -w timeout   Timeout in milliseconds to wait for each reply.
  -R          Use routing header to test reverse route also (IPv6-only).
              Per RFC 5095 the use of this routing header has been
              deprecated. Some systems may drop echo requests if
              this header is used.
  -S srcaddr   Source address to use.
  -c compartment Routing compartment identifier.
  -p           Ping a Hyper-V Network Virtualization provider address.
  -4           Force using IPv4.
  -6           Force using IPv6.

C:\Users\DELL>
```

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

```
C:\Users\DELL>tracert www.google.com

Tracing route to www.google.com [2404:6800:4009:831::2004]
over a maximum of 30 hops:

 1   3 ms    3 ms    3 ms  2400:74e0:0:e0b6::1
 2   6 ms    6 ms    8 ms  2001:df6:2380:f000::4
 3   5 ms    7 ms    7 ms  2001:df6:2380:f000::182
 4   10 ms   8 ms    7 ms  2404:a800:1a00:209::189
 5   61 ms   60 ms   60 ms  2404:a800::92
 6   *        *        *      Request timed out.
 7   67 ms   64 ms   66 ms  2404:6800:8201:140::1
 8   100 ms  66 ms   79 ms  2001:4860:0:1::ac6
 9   96 ms   70 ms   70 ms  2001:4860:0:1::8806
10   96 ms   67 ms   64 ms  2001:4860::9:4002:d27c
11   65 ms   63 ms   66 ms  2001:4860::9:4001:7734
12   *        64 ms   67 ms  2001:4860:0:1::870f
13   67 ms   67 ms   66 ms  2001:4860:0:1::5c07
14   65 ms   65 ms   65 ms  bom12s21-in-x04.1e100.net [2404:6800:4009:831::2004]

Trace complete.
```

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

```
C:\Users\DELL>pathping www.google.com

Tracing route to www.google.com [2404:6800:4009:831::2004]
over a maximum of 30 hops:
 0  Badshan [2400:74e0:0:e0b6:908f:5522:3e8f:4cb4]
 1  2400:74e0:0:e0b6::1
 2  2001:df6:2380:f000::4
 3  2001:df6:2380:f000::182
 4  2404:a800:1a00:209::189
 5  2404:a800::92
 6  *        *        *
```

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

```
C:\Users\DELL>netstat -an
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135           0.0.0.0:0            LISTENING
  TCP    0.0.0.0:445           0.0.0.0:0            LISTENING
  TCP    0.0.0.0:902           0.0.0.0:0            LISTENING
  TCP    0.0.0.0:912           0.0.0.0:0            LISTENING
  TCP    0.0.0.0:5040          0.0.0.0:0            LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0            LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0            LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0            LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0            LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0            LISTENING
  TCP    0.0.0.0:49670          0.0.0.0:0            LISTENING
  TCP    127.0.0.1:1434          0.0.0.0:0            LISTENING
  TCP    127.0.0.1:50104         0.0.0.0:0            LISTENING
  TCP    127.0.0.1:60484         0.0.0.0:0            LISTENING
  TCP    192.168.1.72:139         0.0.0.0:0            LISTENING
  TCP    192.168.1.72:50123        3.33.193.183:443      ESTABLISHED
```

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

```
C:\Users\DELL>netstat -b
The requested operation requires elevation.

C:\Users\DELL>_
```

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

```
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           0
```

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.

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

```
C:\Users\DELL>arp -a

Interface: 192.168.247.1 --- 0x2
  Internet Address      Physical Address      Type
  192.168.247.255        ff-ff-ff-ff-ff-ff    static
  224.0.0.22              01-00-5e-00-00-16    static
  224.0.0.251             01-00-5e-00-00-fb    static
  224.0.0.252             01-00-5e-00-00-fc    static
  239.255.255.250         01-00-5e-7f-ff-fa    static
  255.255.255.255         ff-ff-ff-ff-ff-ff    static

Interface: 192.168.56.1 --- 0x3
```

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      : mandipdkd1_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

```
C:\Users\DELL>netsh advfirewall show allprofiles

Domain Profile Settings:
-----
State          ON
Firewall Policy    BlockInbound,AllowOutbound
LocalFirewallRules N/A (GPO-store only)
LocalConSecRules   N/A (GPO-store only)
InboundUserNotification Enable
RemoteManagement   Disable
UnicastResponseToMulticast  Enable

Logging:
```

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

```
C:\Users\DELL>nslookup www.sxc.edu.np
Server: UnKnown
Address: fe80::1

Non-authoritative answer:
Name: www.sxc.edu.np
Addresses: 2606:4700:3030::6815:7001
           2606:4700:3030::6815:2001
           2606:4700:3030::6815:3001
           2606:4700:3030::6815:5001
```

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

```
C:\Users\DELL>dir
Volume in drive C has no label.
Volume Serial Number is D4F0-0578

Directory of C:\Users\DELL

08/21/2025  07:43 PM    <DIR>        .
08/21/2025  07:43 PM    <DIR>        ..
07/31/2023  10:29 PM    <DIR>        .android
03/17/2025  12:29 PM    <DIR>        .config
12/06/2024  07:34 AM    <DIR>        .ipython
06/29/2025  06:57 AM    <DIR>        .matplotlib
12/26/2024  06:36 AM    <DIR>        174 .packettracer
08/28/2025  12:03 PM    <DIR>        .VirtualBox
11/25/2023  04:54 AM    <DIR>        .vscode
07/31/2023  12:03 AM    <DIR>        3D Objects
12/26/2024  08:08 AM    <DIR>        Cisco Packet Tracer 8.2.1
07/31/2023  12:03 AM    <DIR>        Contacts
09/16/2023  11:19 AM    <DIR>        Documents
09/01/2025  09:33 PM    <DIR>        Downloads
07/31/2023  12:03 AM    <DIR>        Favorites
07/31/2023  12:03 AM    <DIR>        Pictures
07/31/2023  12:03 AM    <DIR>        Videos
```

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

```
C:\Users\DELL>attrib doc.txt
A                      C:\Users\DELL\doc.txt
```

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 CHDKSK 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.)