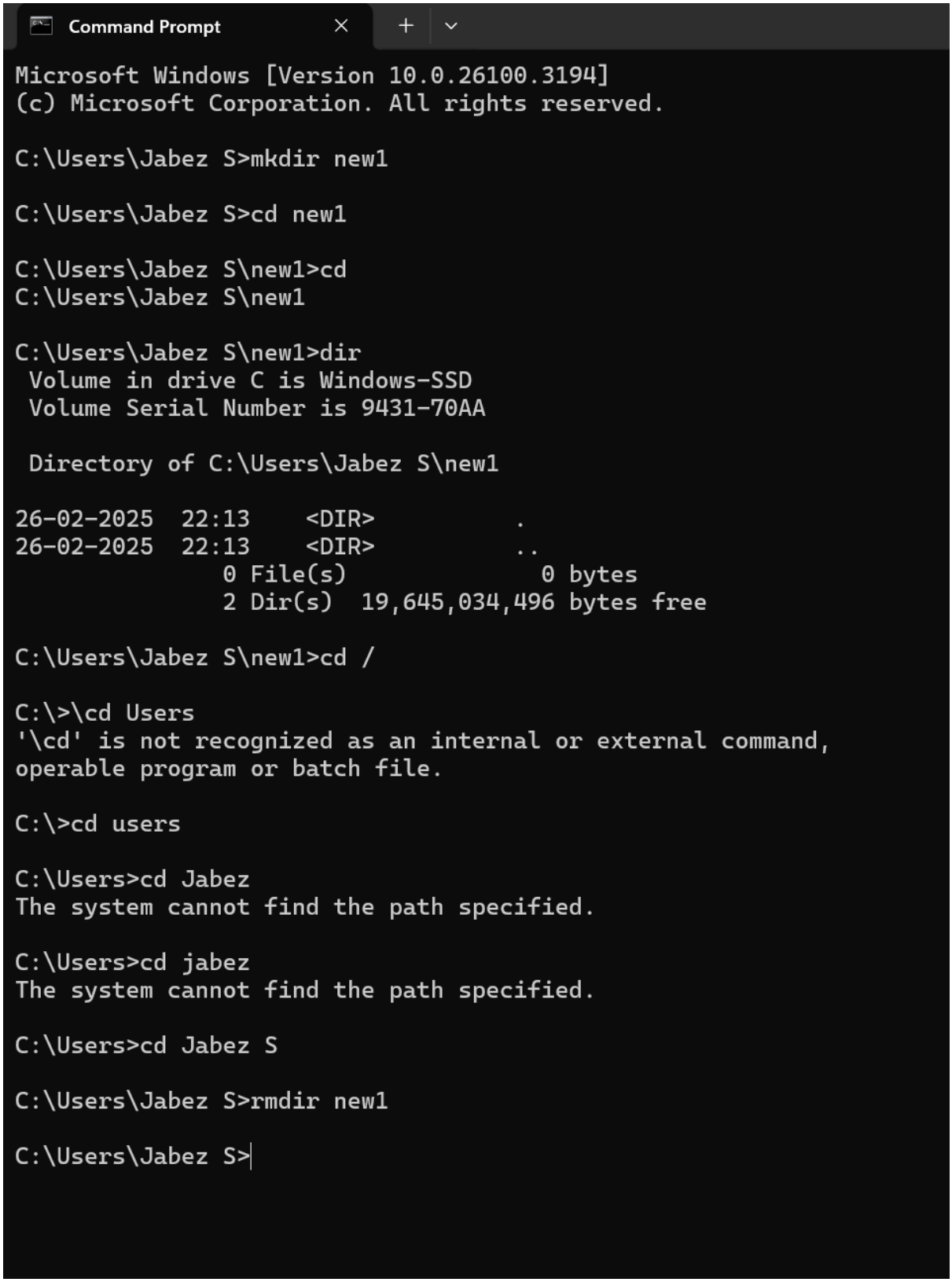
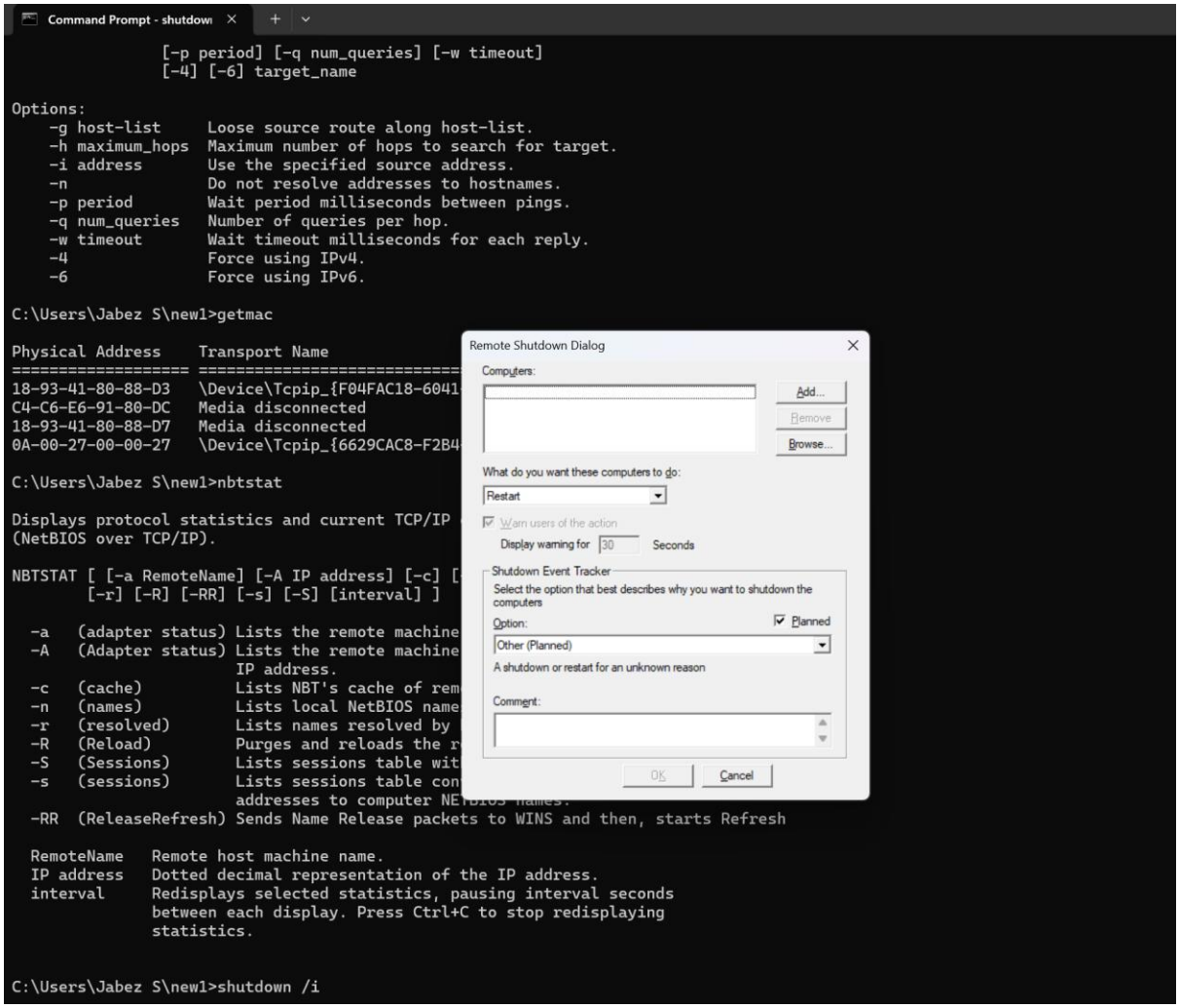
19CS419 – DIGITAL FORENSICS AND DIGITAL INVESTIGATION

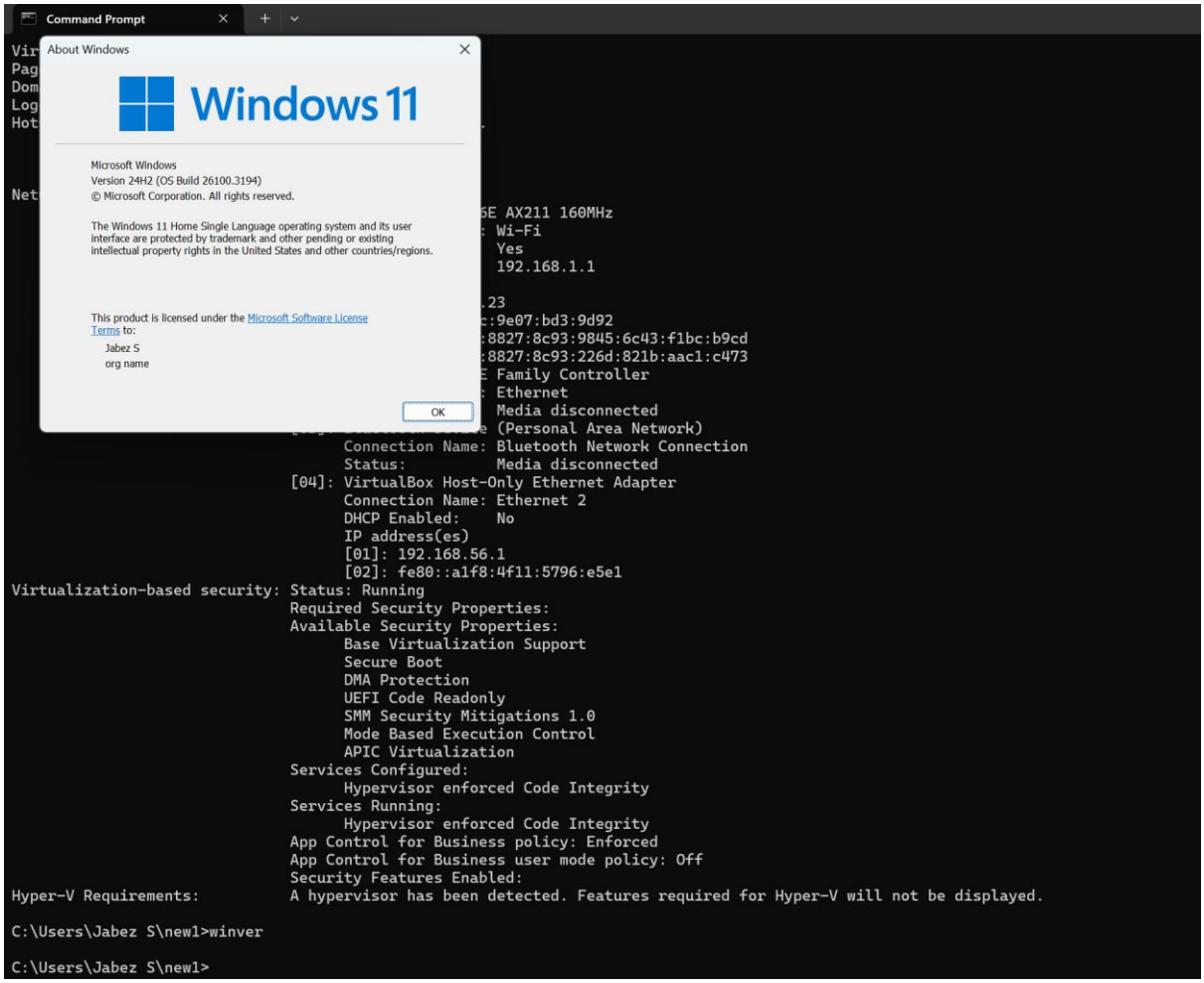
Name : Kamalesh S

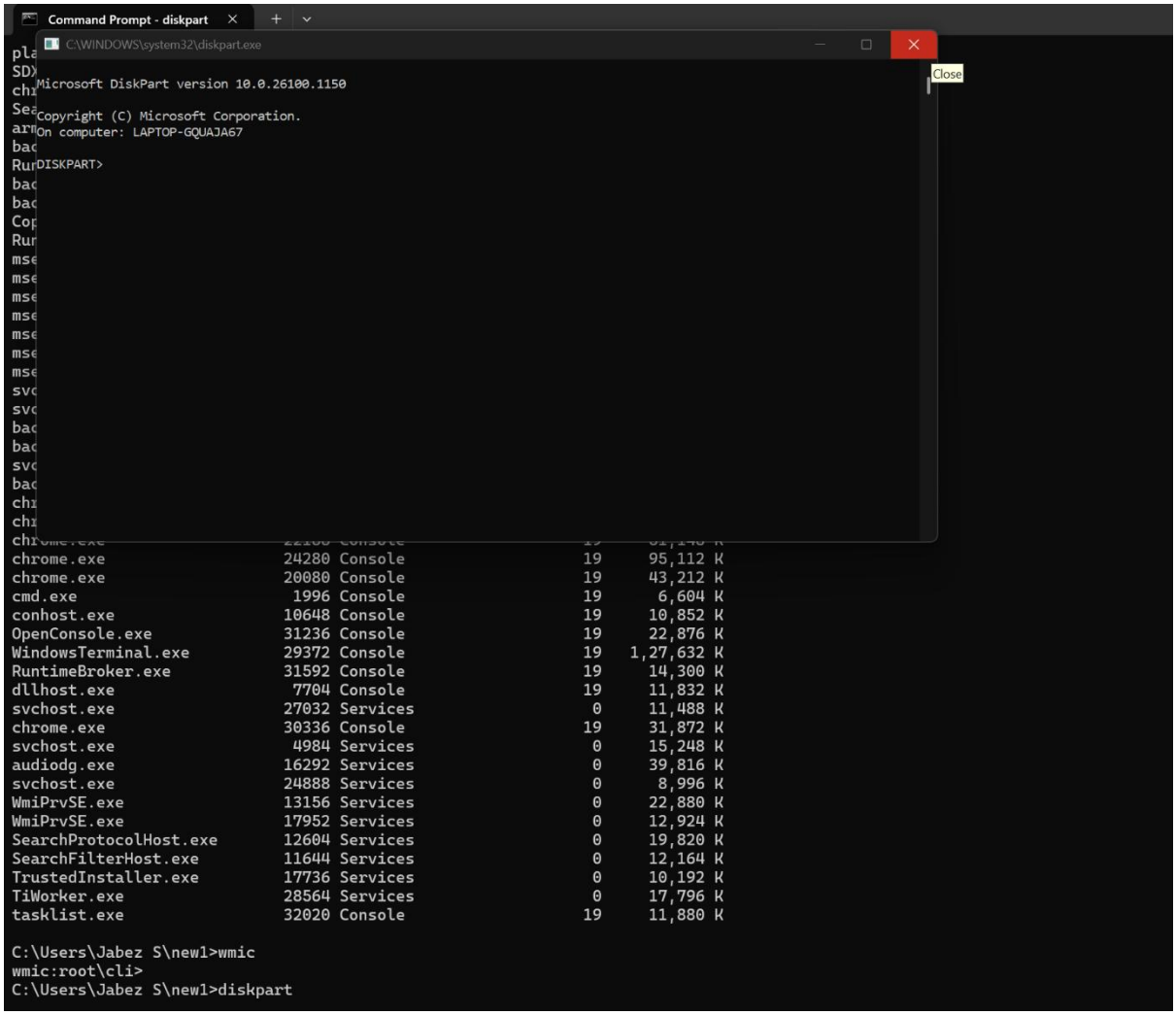
Register : 212223040083

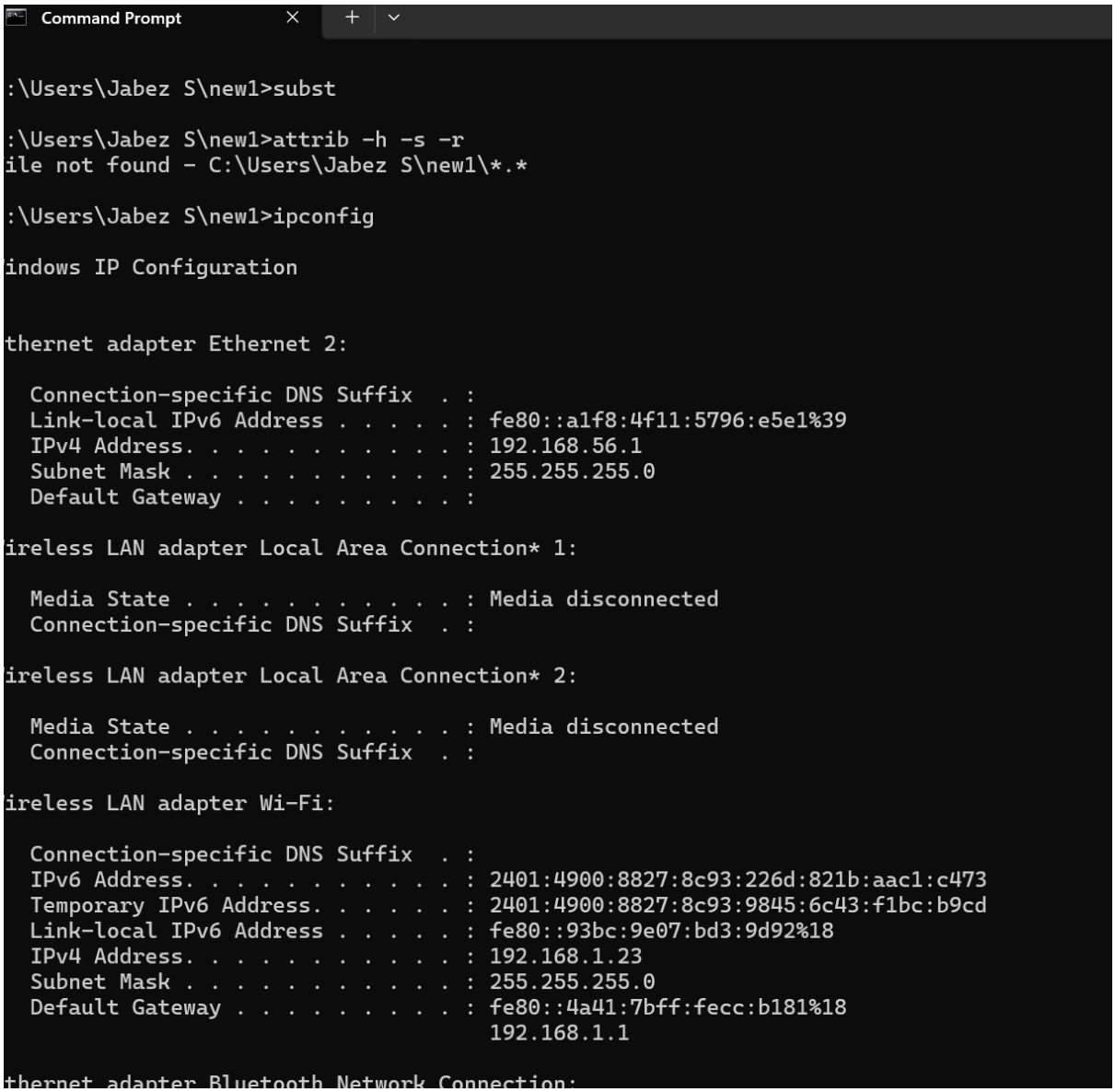
WINDOWS COMMAND

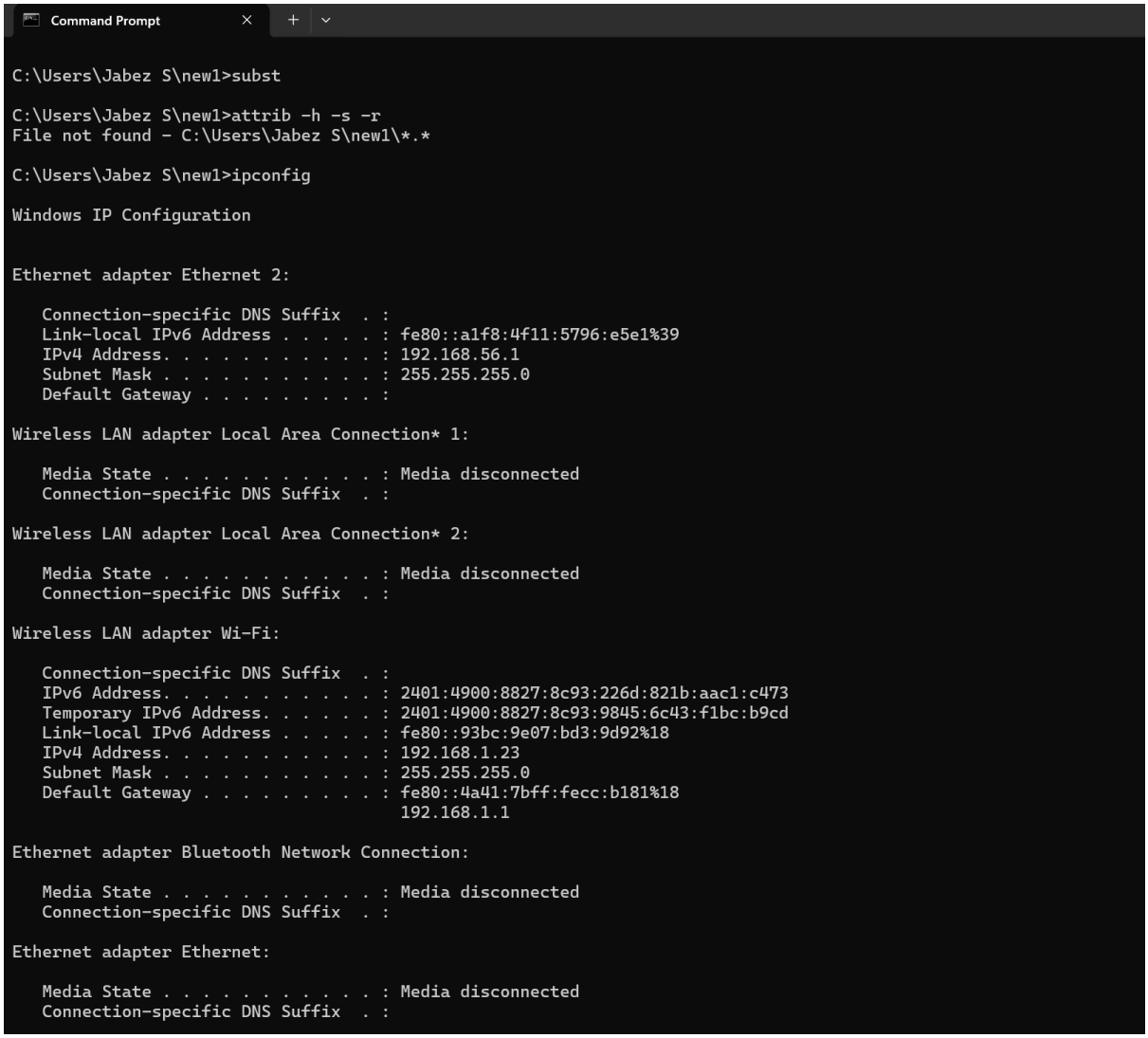


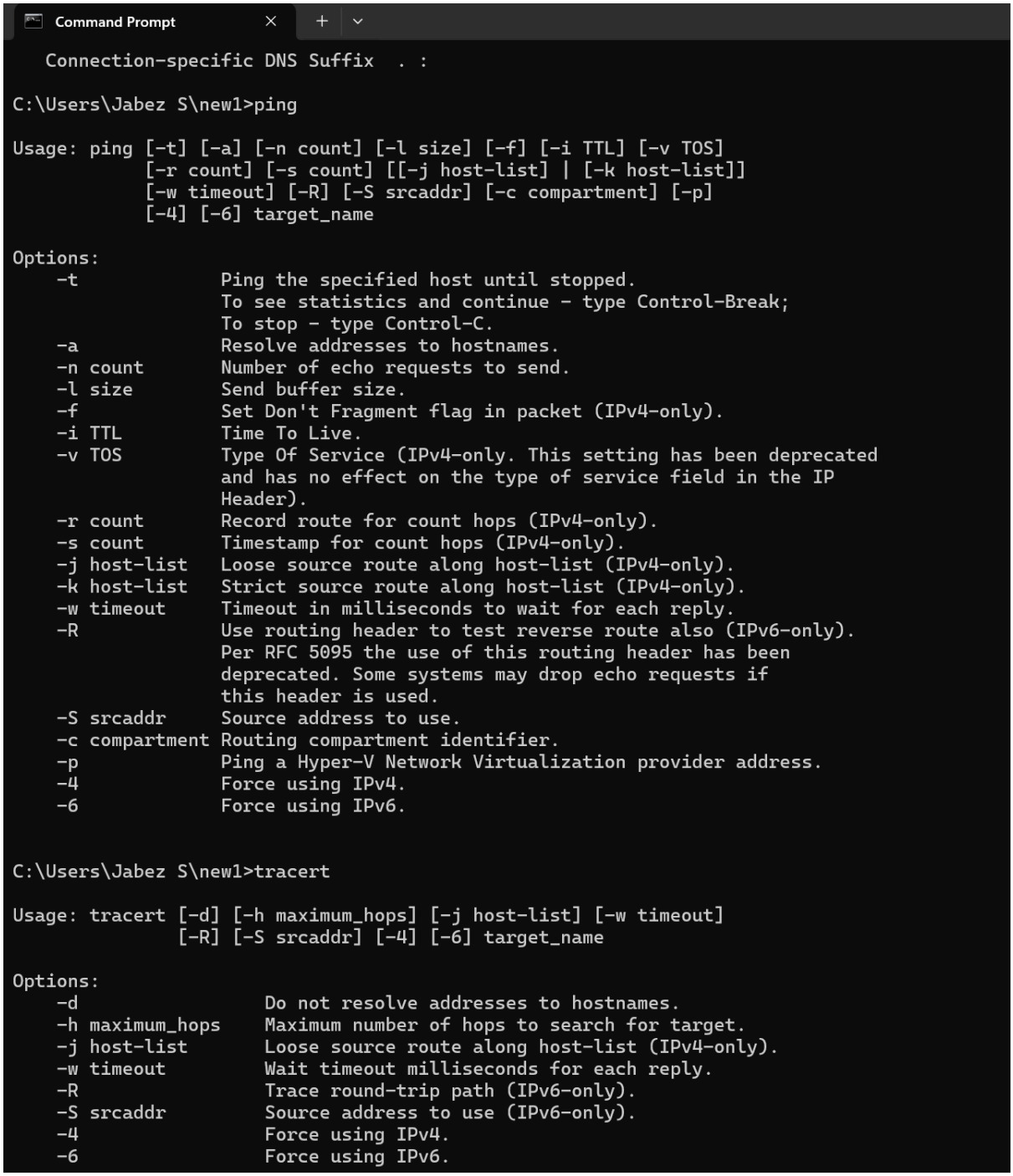

Command Prompt - shutdow
[-p period] [-q num_queries] [-w timeout]
[-4] [-6] target_name
Options:
-g host-list Loose source route along host-list.
-h maximum_hops Maximum number of hops to search for target.
-i address Use the specified source address.
-n Do not resolve addresses to hostnames.
-p period Wait period milliseconds between pings.
-q num_queries Number of queries per hop.
-w timeout Wait timeout milliseconds for each reply.
-4 Force using IPv4.
-6 Force using IPv6.
C:\Users\Jabez S\new1>getmac
Physical Address Transport Name
18-93-41-80-88-D3 \Device\Tcpip_{F04FAC18-6041
C4-C6-E6-91-80-DC Media disconnected
18-93-41-80-88-D7 Media disconnected
0A-00-27-00-00-27 \Device\Tcpip_{6629CAC8-F2B4
C:\Users\Jabez S\new1>nbtstat
Displays protocol statistics and current TCP/IP
(NetBIOS over TCP/IP).
NBTSTAT [[-a RemoteName] [-A IP address] [-c] [
[-r] [-R] [-RR] [-s] [-S] [interval]]
-a (adapter status) Lists the remote machine
-A (Adapter status) Lists the remote machine
IP address.
-c (cache) Lists NBT's cache of rem
-n (names) Lists local NetBIOS name
-r (resolved) Lists names resolved by
-R (Reload) Purges and reloads the r
-S (Sessions) Lists sessions table wit
-s (sessions) Lists sessions table con
addresses to computer NETBIOS names.
-RR (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refresh
RemoteName Remote host machine name.
IP address Dotted decimal representation of the IP address.
interval Redisplays selected statistics, pausing interval seconds
between each display. Press Ctrl+C to stop redisplaying
statistics.
C:\Users\Jabez S\new1>shutdown /i
Remote Shutdown Dialog
Computers:
Add...
Remove
Browse...
What do you want these computers to do:
Restart
Warn users of the action
Display warning for 30 Seconds
Shutdown Event Tracker
Select the option that best describes why you want to shutdown the computers
Option:
Planned
Other (Planned)
A shutdown or restart for an unknown reason
Comment:
OK
Cancel

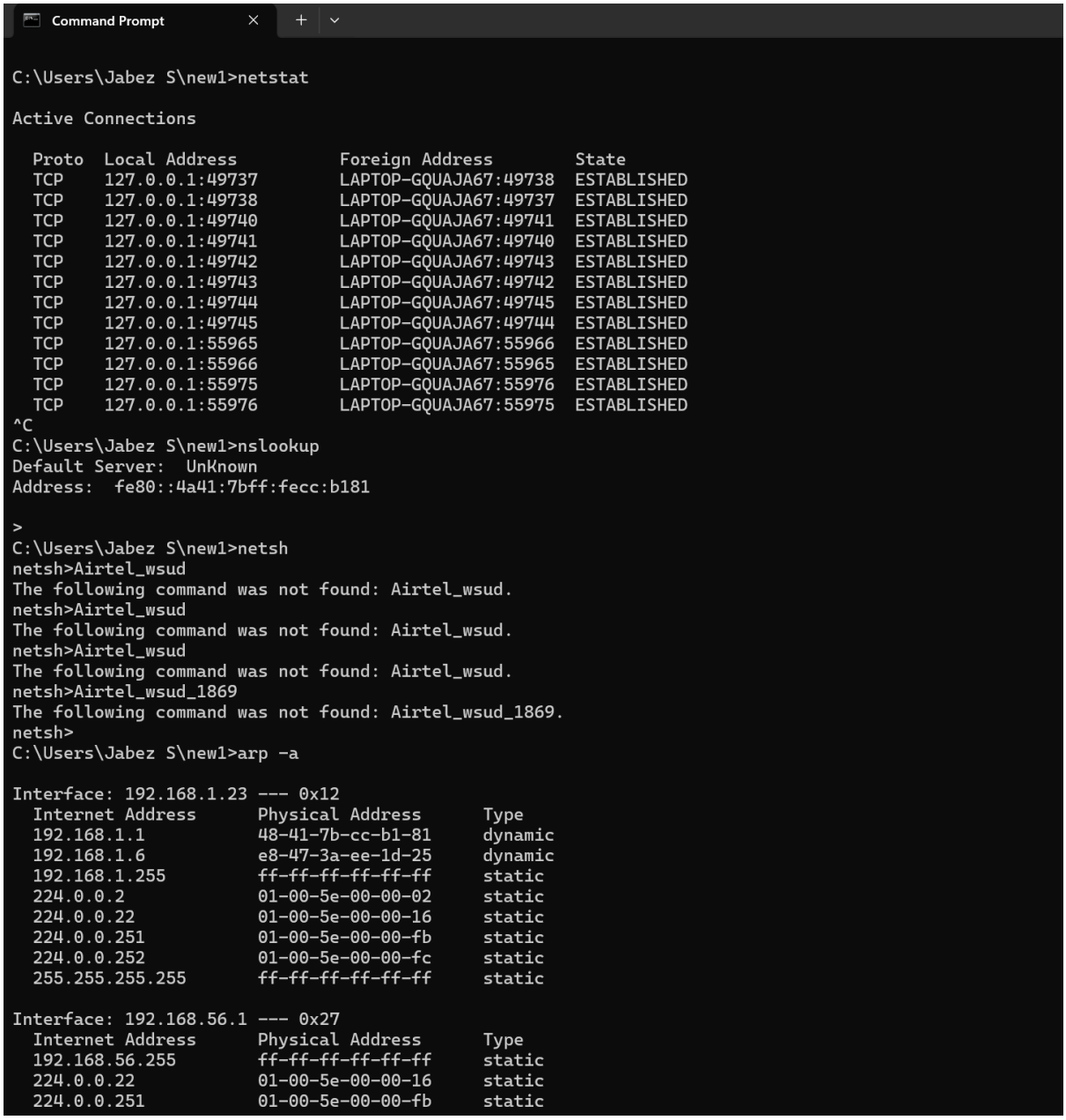

Command Prompt
About Windows
Windows 11
Microsoft Windows
Version 24H2 (OS Build 26100.3194)
© Microsoft Corporation. All rights reserved.
The Windows 11 Home Single Language operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.
This product is licensed under the Microsoft Software License Terms to:
Jabez S
org name
OK
6E AX211 160MHz
: Wi-Fi
Yes
192.168.1.1
.23
c:9e07:bd3:9d92
:8827:8c93:9845:6c43:f1bc:b9cd
:8827:8c93:226d:821b:aac1:c473
E Family Controller
: Ethernet
Media disconnected
e (Personal Area Network)
Connection Name: Bluetooth Network Connection
Status: Media disconnected
[04]: VirtualBox Host-Only Ethernet Adapter
Connection Name: Ethernet 2
DHCP Enabled: No
IP address(es)
[01]: 192.168.56.1
[02]: fe80::a1f8:4f11:5796:e5e1
Virtualization-based security: Status: Running
Required Security Properties:
Available Security Properties:
Base Virtualization Support
Secure Boot
DMA Protection
UEFI Code Readonly
SMM Security Mitigations 1.0
Mode Based Execution Control
APIC Virtualization
Services Configured:
Hypervisor enforced Code Integrity
Services Running:
Hypervisor enforced Code Integrity
App Control for Business policy: Enforced
App Control for Business user mode policy: Off
Security Features Enabled:
Hyper-V Requirements: A hypervisor has been detected. Features required for Hyper-V will not be displayed.
C:\Users\Jabez S\new1>winver
C:\Users\Jabez S\new1>

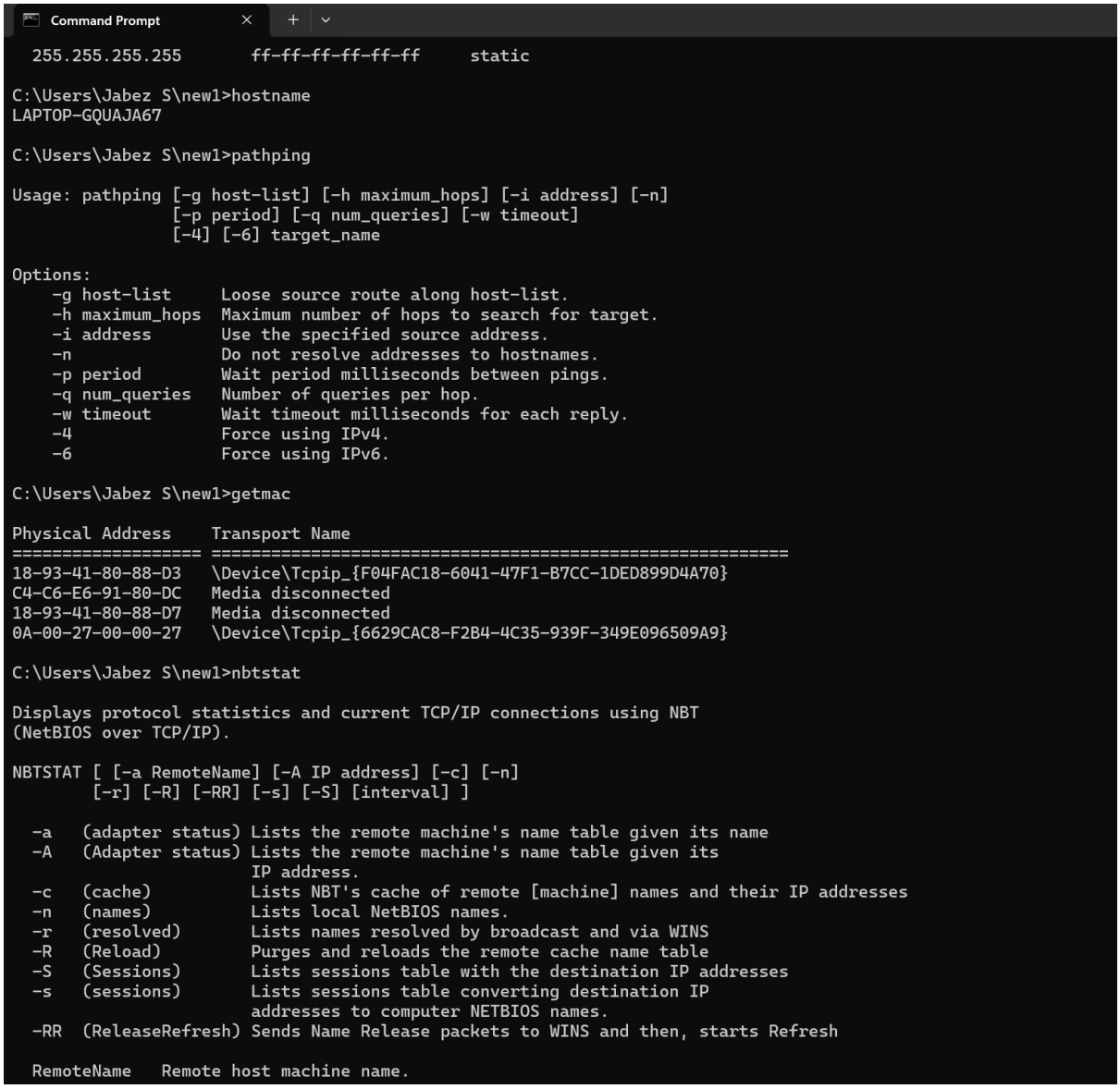

Command Prompt - diskpart
C:\WINDOWS\system32\diskpart.exe
Close
Microsoft DiskPart version 10.0.26100.1150
Copyright (C) Microsoft Corporation.
On computer: LAPTOP-GQUAJA67
DISKPART>
chrome.exe 24280 Console 19 95,112 K
chrome.exe 20080 Console 19 43,212 K
cmd.exe 1996 Console 19 6,604 K
conhost.exe 10648 Console 19 10,852 K
OpenConsole.exe 31236 Console 19 22,876 K
WindowsTerminal.exe 29372 Console 19 1,27,632 K
RuntimeBroker.exe 31592 Console 19 14,300 K
dllhost.exe 7704 Console 19 11,832 K
svchost.exe 27032 Services 0 11,488 K
chrome.exe 30336 Console 19 31,872 K
svchost.exe 4984 Services 0 15,248 K
audiodg.exe 16292 Services 0 39,816 K
svchost.exe 24888 Services 0 8,996 K
WmiPrvSE.exe 13156 Services 0 22,880 K
WmiPrvSE.exe 17952 Services 0 12,924 K
SearchProtocolHost.exe 12604 Services 0 19,820 K
SearchFilterHost.exe 11644 Services 0 12,164 K
TrustedInstaller.exe 17736 Services 0 10,192 K
TiWorker.exe 28564 Services 0 17,796 K
tasklist.exe 32020 Console 19 11,880 K
C:\Users\Jabez S\new1>wmic
wmic:root\cli>
C:\Users\Jabez S\new1>diskpart

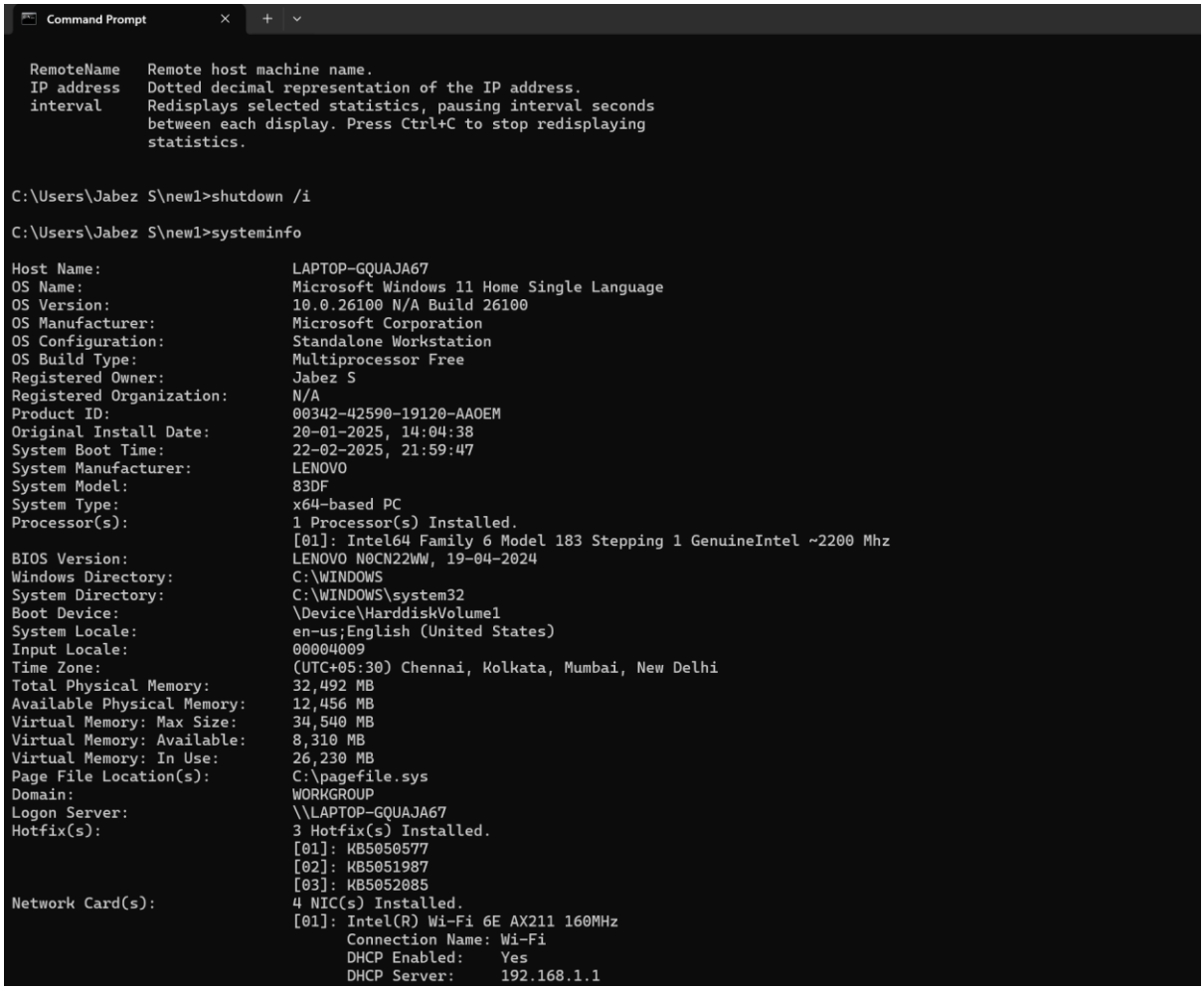

Command Prompt
:\Users\Jabez S\new1>subst
:\Users\Jabez S\new1>attrib -h -s -r
ile not found - C:\Users\Jabez S\new1*.*
:\Users\Jabez S\new1>ipconfig
indows IP Configuration
thernet adapter Ethernet 2:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::a1f8:4f11:5796:e5e1%39
IPv4 Address. . . . . : 192.168.56.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
ireless LAN adapter Local Area Connection* 1:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
ireless LAN adapter Local Area Connection* 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
ireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . : 2401:4900:8827:8c93:226d:821b:aac1:c473
Temporary IPv6 Address. . . . . : 2401:4900:8827:8c93:9845:6c43:f1bc:b9cd
Link-local IPv6 Address . . . . . : fe80::93bc:9e07:bd3:9d92%18
IPv4 Address. . . . . : 192.168.1.23
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::4a41:7bff:fecc:b181%18
192.168.1.1
thernet adapter Bluetooth Network Connection:

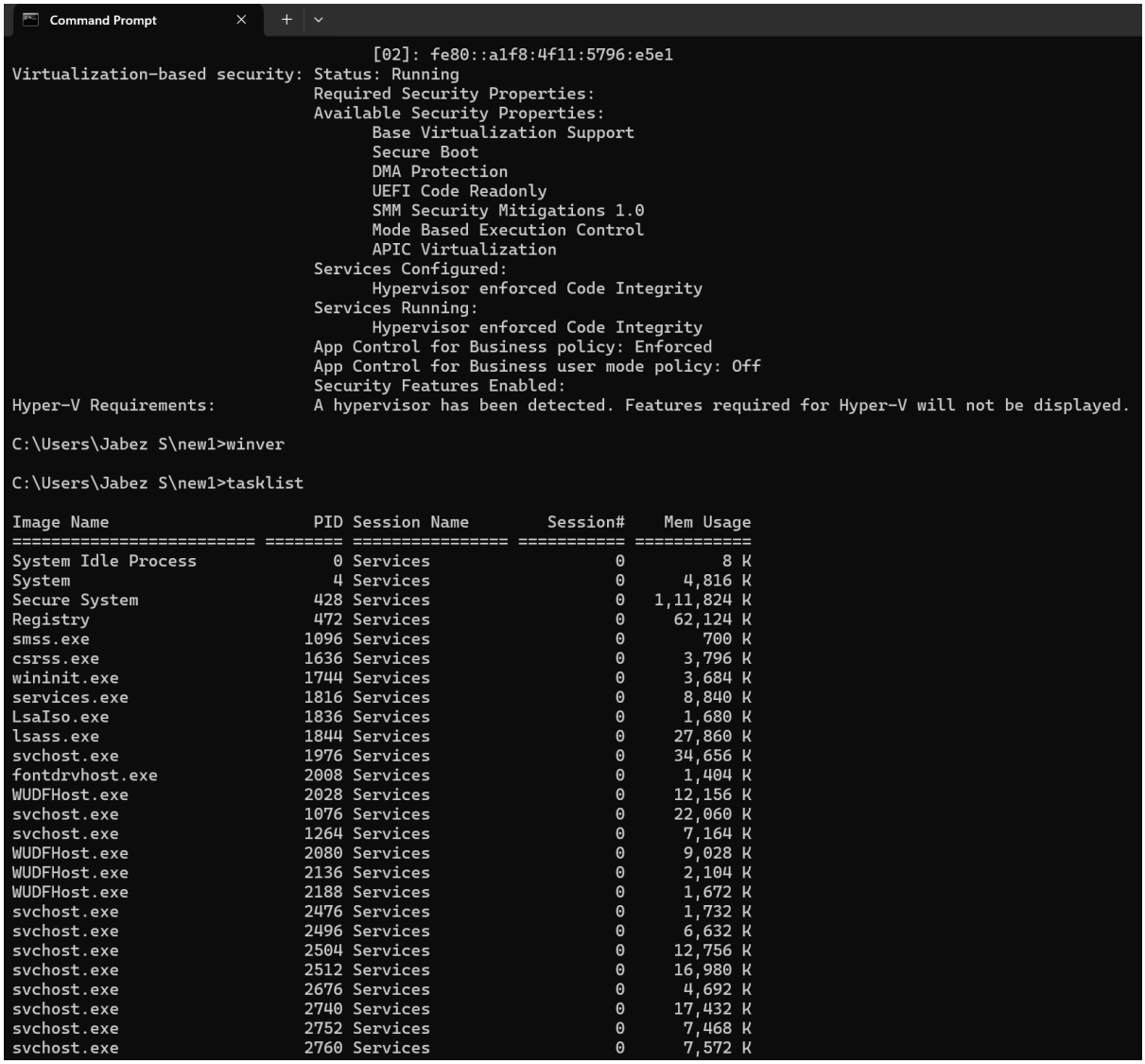

Command Prompt
C:\Users\Jabez S\new1>subst
C:\Users\Jabez S\new1>attrib -h -s -r
File not found - C:\Users\Jabez S\new1*.*
C:\Users\Jabez S\new1>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet 2:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::a1f8:4f11:5796:e5e1%39
IPv4 Address. . . . . : 192.168.56.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
Wireless LAN adapter Local Area Connection* 1:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . : 2401:4900:8827:8c93:226d:821b:aac1:c473
Temporary IPv6 Address. . . . . : 2401:4900:8827:8c93:9845:6c43:f1bc:b9cd
Link-local IPv6 Address . . . . . : fe80::93bc:9e07:bd3:9d92%18
IPv4 Address. . . . . : 192.168.1.23
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::4a41:7bff:fecc:b181%18
192.168.1.1
Ethernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Ethernet adapter Ethernet:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

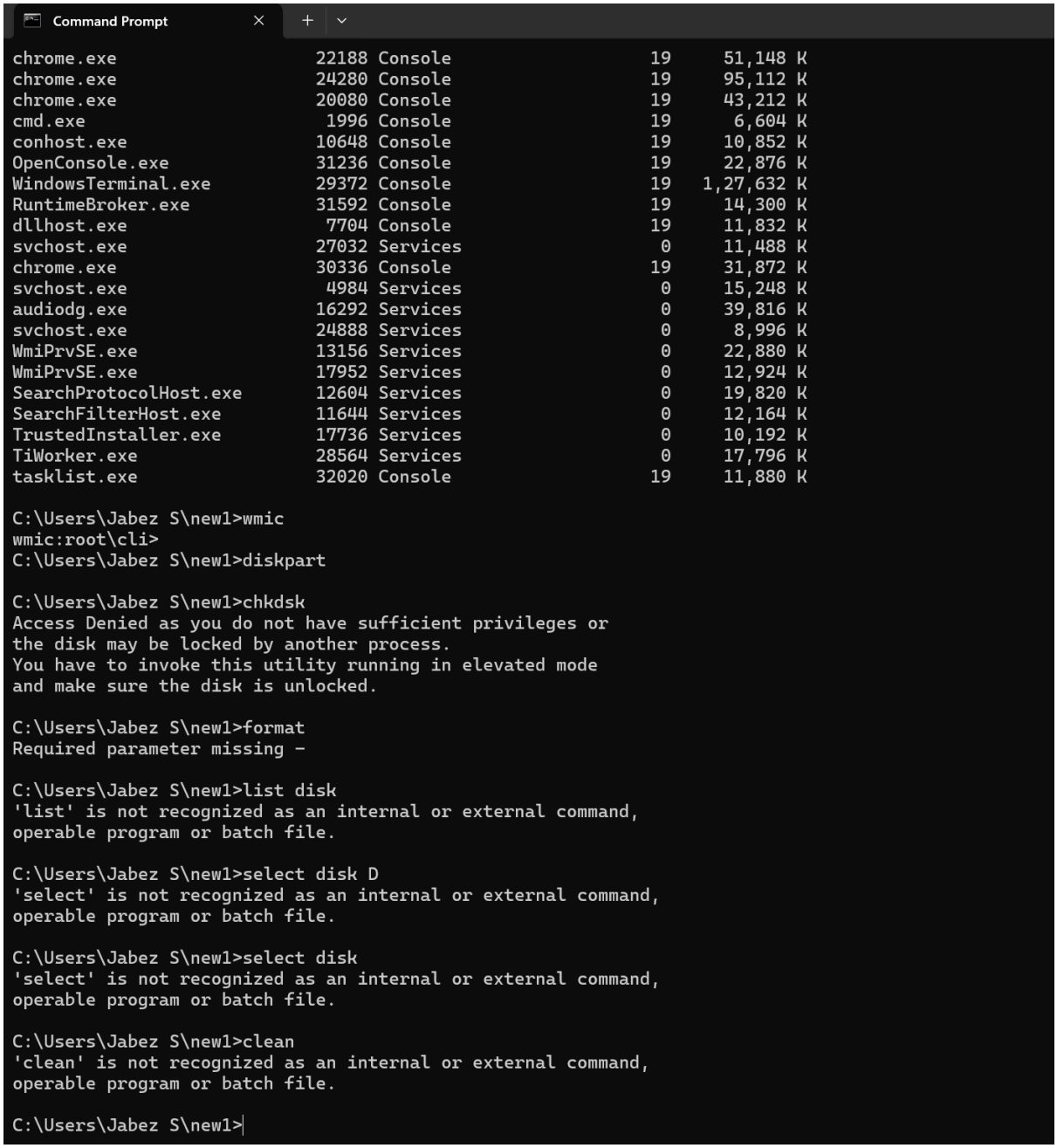

Command Prompt
Connection-specific DNS Suffix . :
C:\Users\Jabez S\new1>ping
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
[-r count] [-s count] [[-j host-list] | [-k host-list]]
[-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
[-4] [-6] target_name
Options:
-t Ping the specified 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 Loose 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\Jabez S\new1>tracert
Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
[-R] [-S srcaddr] [-4] [-6] target_name
Options:
-d Do not resolve addresses to hostnames.
-h maximum_hops Maximum number of hops to search for target.
-j host-list Loose source route along host-list (IPv4-only).
-w timeout Wait timeout milliseconds for each reply.
-R Trace round-trip path (IPv6-only).
-S srcaddr Source address to use (IPv6-only).
-4 Force using IPv4.
-6 Force using IPv6.


Command Prompt
C:\Users\Jabez S\new1>netstat
Active Connections
Proto Local Address Foreign Address State
TCP 127.0.0.1:49737 LAPTOP-GQUAJA67:49738 ESTABLISHED
TCP 127.0.0.1:49738 LAPTOP-GQUAJA67:49737 ESTABLISHED
TCP 127.0.0.1:49740 LAPTOP-GQUAJA67:49741 ESTABLISHED
TCP 127.0.0.1:49741 LAPTOP-GQUAJA67:49740 ESTABLISHED
TCP 127.0.0.1:49742 LAPTOP-GQUAJA67:49743 ESTABLISHED
TCP 127.0.0.1:49743 LAPTOP-GQUAJA67:49742 ESTABLISHED
TCP 127.0.0.1:49744 LAPTOP-GQUAJA67:49745 ESTABLISHED
TCP 127.0.0.1:49745 LAPTOP-GQUAJA67:49744 ESTABLISHED
TCP 127.0.0.1:55965 LAPTOP-GQUAJA67:55966 ESTABLISHED
TCP 127.0.0.1:55966 LAPTOP-GQUAJA67:55965 ESTABLISHED
TCP 127.0.0.1:55975 LAPTOP-GQUAJA67:55976 ESTABLISHED
TCP 127.0.0.1:55976 LAPTOP-GQUAJA67:55975 ESTABLISHED
^C
C:\Users\Jabez S\new1>nslookup
Default Server: UnKnown
Address: fe80::4a41:7bff:fecc:b181
>
C:\Users\Jabez S\new1>netsh
netsh>Airtel_wsud
The following command was not found: Airtel_wsud.
netsh>Airtel_wsud
The following command was not found: Airtel_wsud.
netsh>Airtel_wsud
The following command was not found: Airtel_wsud.
netsh>Airtel_wsud_1869
The following command was not found: Airtel_wsud_1869.
netsh>
C:\Users\Jabez S\new1>arp -a
Interface: 192.168.1.23 --- 0x12
Internet Address Physical Address Type
192.168.1.1 48-41-7b-cc-b1-81 dynamic
192.168.1.6 e8-47-3a-ee-1d-25 dynamic
192.168.1.255 ff-ff-ff-ff-ff-ff static
224.0.0.2 01-00-5e-00-00-02 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
255.255.255.255 ff-ff-ff-ff-ff-ff static
Interface: 192.168.56.1 --- 0x27
Internet Address Physical Address Type
192.168.56.255 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


Command Prompt
255.255.255.255 ff-ff-ff-ff-ff-ff static
C:\Users\Jabez S\new1>hostname
LAPTOP-GQUAJA67
C:\Users\Jabez S\new1>pathping
Usage: pathping [-g host-list] [-h maximum_hops] [-i address] [-n]
[-p period] [-q num_queries] [-w timeout]
[-4] [-6] target_name
Options:
-g host-list Loose source route along host-list.
-h maximum_hops Maximum number of hops to search for target.
-i address Use the specified source address.
-n Do not resolve addresses to hostnames.
-p period Wait period milliseconds between pings.
-q num_queries Number of queries per hop.
-w timeout Wait timeout milliseconds for each reply.
-4 Force using IPv4.
-6 Force using IPv6.
C:\Users\Jabez S\new1>getmac
Physical Address Transport Name
18-93-41-80-88-D3 \Device\Tcpip_{F04FAC18-6041-47F1-B7CC-1DED899D4A70}
C4-C6-E6-91-80-DC Media disconnected
18-93-41-80-88-D7 Media disconnected
0A-00-27-00-00-27 \Device\Tcpip_{6629CAC8-F2B4-4C35-939F-349E096509A9}
C:\Users\Jabez S\new1>nbtstat
Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).
NBTSTAT [[-a RemoteName] [-A IP address] [-c] [-n]
[-r] [-R] [-RR] [-s] [-S] [interval]]
-a (adapter status) Lists the remote machine's name table given its name
-A (Adapter status) Lists the remote machine's name table given its
IP address.
-c (cache) Lists NBT's cache of remote [machine] names and their IP addresses
-n (names) Lists local NetBIOS names.
-r (resolved) Lists names resolved by broadcast and via WINS
-R (Reload) Purges and reloads the remote cache name table
-S (Sessions) Lists sessions table with the destination IP addresses
-s (sessions) Lists sessions table converting destination IP
addresses to computer NETBIOS names.
-RR (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refresh
RemoteName Remote host machine name.


Command Prompt
RemoteName Remote host machine name.
IP address Dotted decimal representation of the IP address.
interval Redisplays selected statistics, pausing interval seconds
between each display. Press Ctrl+C to stop redisplaying
statistics.
C:\Users\Jabez S\new1>shutdown /i
C:\Users\Jabez S\new1>systeminfo
Host Name: LAPTOP-GQUAJA67
OS Name: Microsoft Windows 11 Home Single Language
OS Version: 10.0.26100 N/A Build 26100
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Multiprocessor Free
Registered Owner: Jabez S
Registered Organization: N/A
Product ID: 00342-42590-19120-AAOEM
Original Install Date: 20-01-2025, 14:04:38
System Boot Time: 22-02-2025, 21:59:47
System Manufacturer: LENOVO
System Model: 83DF
System Type: x64-based PC
Processor(s): 1 Processor(s) Installed.
[01]: Intel64 Family 6 Model 183 Stepping 1 GenuineIntel ~2200 Mhz
BIOS Version: LENOVO N0CN22WW, 19-04-2024
Windows Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)
Input Locale: 00004009
Time Zone: (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory: 32,492 MB
Available Physical Memory: 12,456 MB
Virtual Memory: Max Size: 34,540 MB
Virtual Memory: Available: 8,310 MB
Virtual Memory: In Use: 26,230 MB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
Logon Server: \\LAPTOP-GQUAJA67
Hotfix(s): 3 Hotfix(s) Installed.
[01]: KB5050577
[02]: KB5051987
[03]: KB5052085
Network Card(s): 4 NIC(s) Installed.
[01]: Intel(R) Wi-Fi 6E AX211 160MHz
Connection Name: Wi-Fi
DHCP Enabled: Yes
DHCP Server: 192.168.1.1


Command Prompt
[02]: fe80::a1f8:4f11:5796:e5e1
Virtualization-based security: Status: Running
Required Security Properties:
Available Security Properties:
Base Virtualization Support
Secure Boot
DMA Protection
UEFI Code Readonly
SMM Security Mitigations 1.0
Mode Based Execution Control
APIC Virtualization
Services Configured:
Hypervisor enforced Code Integrity
Services Running:
Hypervisor enforced Code Integrity
App Control for Business policy: Enforced
App Control for Business user mode policy: Off
Security Features Enabled:
Hyper-V Requirements: A hypervisor has been detected. Features required for Hyper-V will not be displayed.
C:\Users\Jabez S\new1>winver
C:\Users\Jabez S\new1>tasklist
Image Name PID Session Name Session# Mem Usage
System Idle Process 0 Services 0 8 K
System 4 Services 0 4,816 K
Secure System 428 Services 0 1,11,824 K
Registry 472 Services 0 62,124 K
smss.exe 1096 Services 0 700 K
csrss.exe 1636 Services 0 3,796 K
wininit.exe 1744 Services 0 3,684 K
services.exe 1816 Services 0 8,840 K
LsaIso.exe 1836 Services 0 1,680 K
lsass.exe 1844 Services 0 27,860 K
svchost.exe 1976 Services 0 34,656 K
fontdrvhost.exe 2008 Services 0 1,404 K
WUDFHost.exe 2028 Services 0 12,156 K
svchost.exe 1076 Services 0 22,060 K
svchost.exe 1264 Services 0 7,164 K
WUDFHost.exe 2080 Services 0 9,028 K
WUDFHost.exe 2136 Services 0 2,104 K
WUDFHost.exe 2188 Services 0 1,672 K
svchost.exe 2476 Services 0 1,732 K
svchost.exe 2496 Services 0 6,632 K
svchost.exe 2504 Services 0 12,756 K
svchost.exe 2512 Services 0 16,980 K
svchost.exe 2676 Services 0 4,692 K
svchost.exe 2740 Services 0 17,432 K
svchost.exe 2752 Services 0 7,468 K
svchost.exe 2760 Services 0 7,572 K


Command Prompt
chrome.exe 22188 Console 19 51,148 K
chrome.exe 24280 Console 19 95,112 K
chrome.exe 20080 Console 19 43,212 K
cmd.exe 1996 Console 19 6,604 K
conhost.exe 10648 Console 19 10,852 K
OpenConsole.exe 31236 Console 19 22,876 K
WindowsTerminal.exe 29372 Console 19 1,27,632 K
RuntimeBroker.exe 31592 Console 19 14,300 K
dllhost.exe 7704 Console 19 11,832 K
svchost.exe 27032 Services 0 11,488 K
chrome.exe 30336 Console 19 31,872 K
svchost.exe 4984 Services 0 15,248 K
audiodg.exe 16292 Services 0 39,816 K
svchost.exe 24888 Services 0 8,996 K
WmiPrvSE.exe 13156 Services 0 22,880 K
WmiPrvSE.exe 17952 Services 0 12,924 K
SearchProtocolHost.exe 12604 Services 0 19,820 K
SearchFilterHost.exe 11644 Services 0 12,164 K
TrustedInstaller.exe 17736 Services 0 10,192 K
TiWorker.exe 28564 Services 0 17,796 K
tasklist.exe 32020 Console 19 11,880 K
C:\Users\Jabez S\new1>wmic
wmic:root\cli>
C:\Users\Jabez S\new1>diskpart
C:\Users\Jabez S\new1>chkdsk
Access Denied as you do not have sufficient privileges or
the disk may be locked by another process.
You have to invoke this utility running in elevated mode
and make sure the disk is unlocked.
C:\Users\Jabez S\new1>format
Required parameter missing -
C:\Users\Jabez S\new1>list disk
'list' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\Jabez S\new1>select disk D
'select' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\Jabez S\new1>select disk
'select' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\Jabez S\new1>clean
'clean' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\Jabez S\new1>