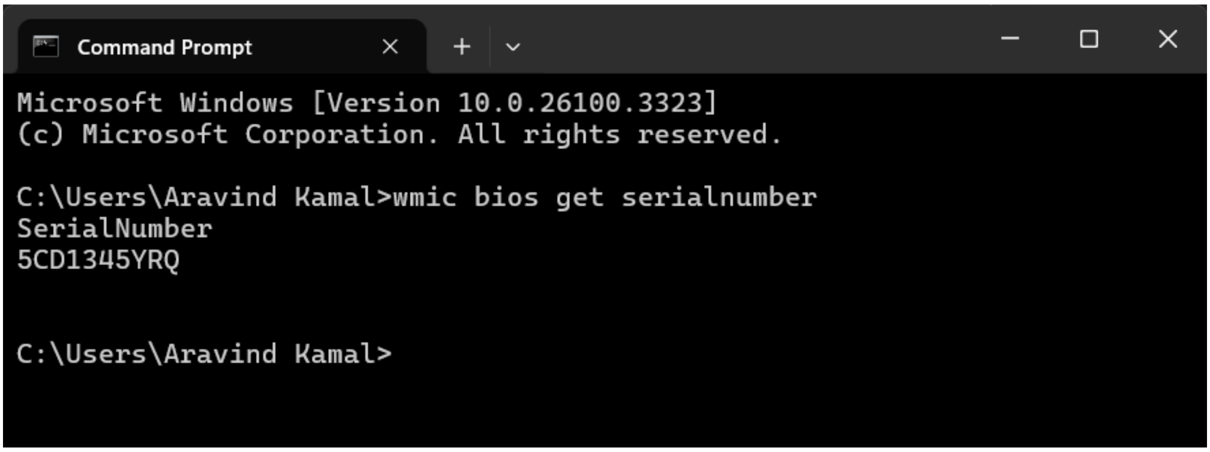
LAB 8

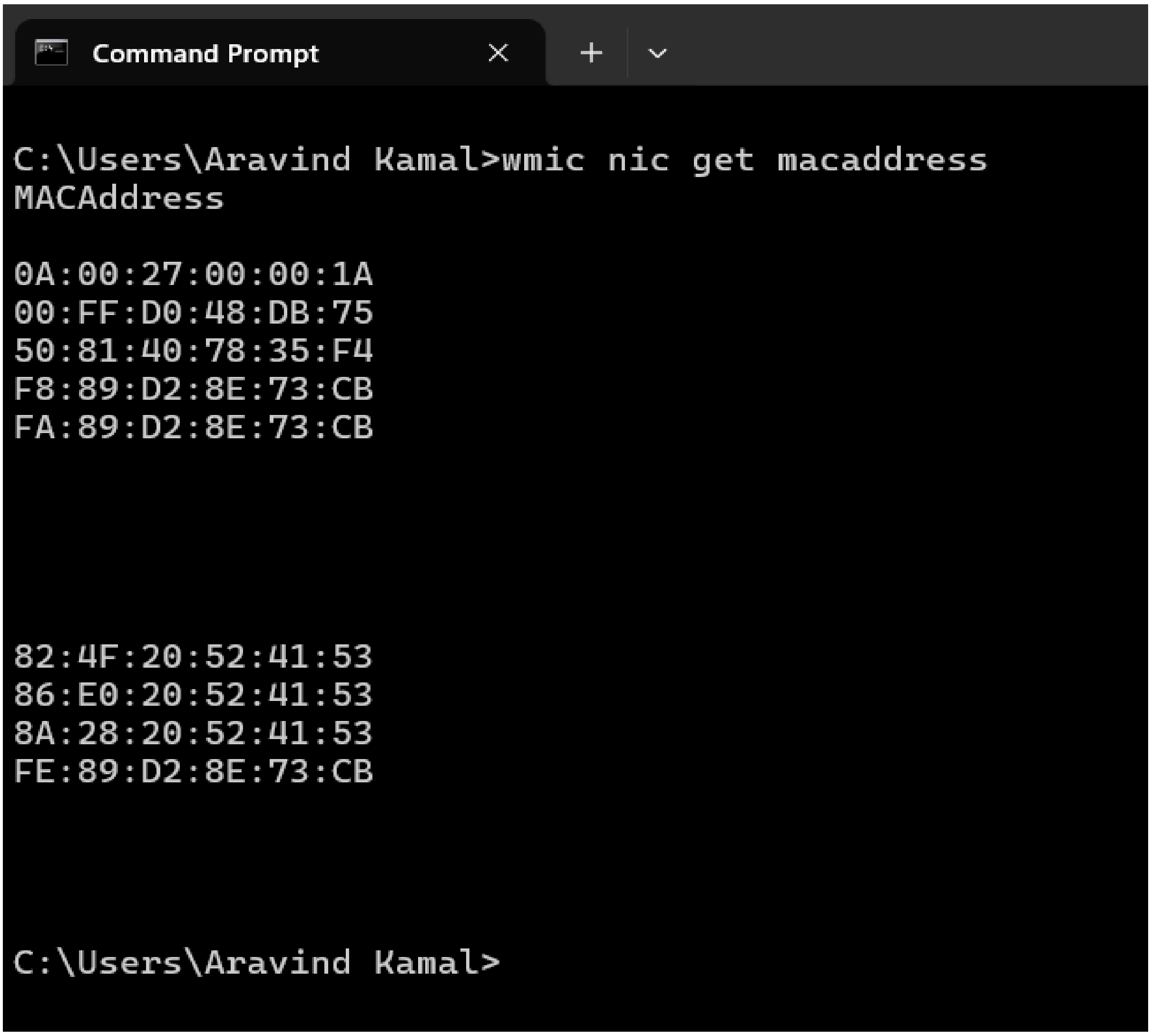
Name : ARAVINDHAN.K ROLLNO:CH.EN.U4CYS22001

SUBJECT : Cyber Forensics **CODE: 20CYS311**

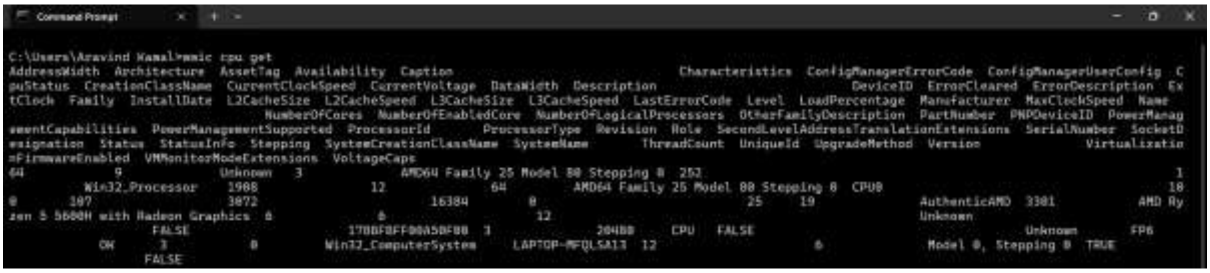
1)Windows management Interface command(WMIC)



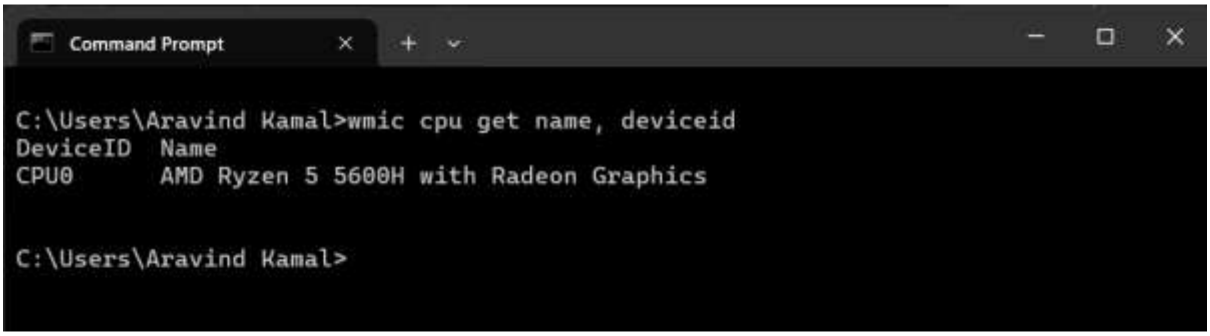
```
Microsoft Windows [Version 10.0.26100.3323]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Aravind Kamal>wmic bios get serialnumber
SerialNumber
5CD1345YRQ


C:\Users\Aravind Kamal>
```



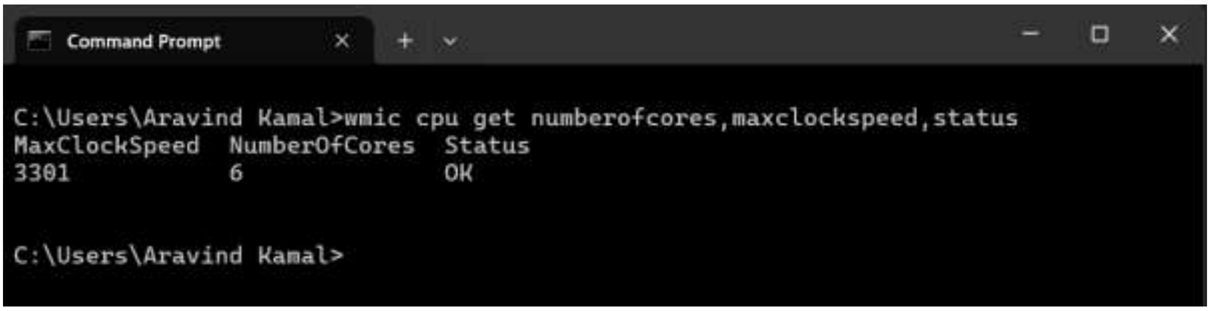
```

C:\Users\Aravind Kamal>wmic nic get macaddress
MACAddress

0A:00:27:00:00:1A
00:FF:D0:48:DB:75
50:81:40:78:35:F4
F8:89:D2:8E:73:CB
FA:89:D2:8E:73:CB





82:4F:20:52:41:53
86:E0:20:52:41:53
8A:28:20:52:41:53
FE:89:D2:8E:73:CB




C:\Users\Aravind Kamal>
```



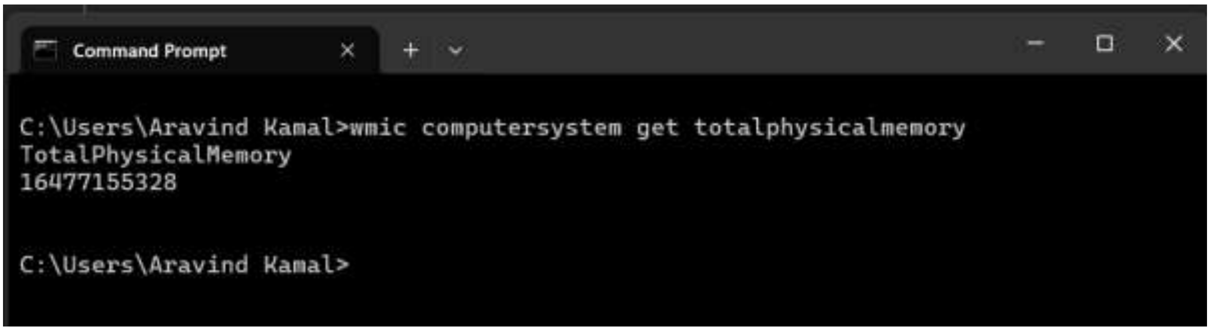
```
C:\Users\Aravind Kamal>wmic cpu get
AddressWidth  Architecture  AssetTag  Availability  Caption                                Characteristics  ConfigManagerErrorCode  ConfigManagerUserConfig  C
puStatus  CreationClassName  CurrentClockSpeed  CurrentVoltage  DataWidth  Description                               DeviceID  ErrorCleared  ErrorDescription  Ex
tClock  Family  InstallDate  L2CacheSize  L2CacheSpeed  L3CacheSize  L3CacheSpeed  LastErrorCode  Level  LoadPercentage  Manufacturer  MaxClockSpeed  Name
                                   NumberOfCores  NumberOfEnabledCore  NumberOfLogicalProcessors  OtherFamilyDescription  PartNumber  PNPDeviceID  PowerManag
ementCapabilities  PowerManagementSupported  ProcessorId       ProcessorType  Revision  Role  SecondLevelAddressTranslationExtensions  SerialNumber  SocketD
esignation  Status  StatusInfo  Stepping  SystemCreationClassName  SystemName        ThreadCount  UniqueId  UpgradeMethod  Version                 Virtualizatio
nFirmwareEnabled  VMMonitorModeExtensions  VoltageCaps
64            9                 Unknown   3             AMD64 Family 25 Model 80 Stepping 0  252                                                          1
          Win32_Processor    1908             12            64         AMD64 Family 25 Model 80 Stepping 0  CPU0                                         18
0       107                  3072                16384       0                              25     19             AuthenticAMD  3301           AMD Ry
zen 5 5600H with Radeon Graphics  6                 6                 12                                        Unknown
                   FALSE                    178BFBFF00A50F00  3                20480     CPU   FALSE                                Unknown        FP6
                OK      3            0        Win32_ComputerSystem     LAPTOP-MFQLSA13  12                      6               Model 0, Stepping 0  TRUE
                  FALSE
```



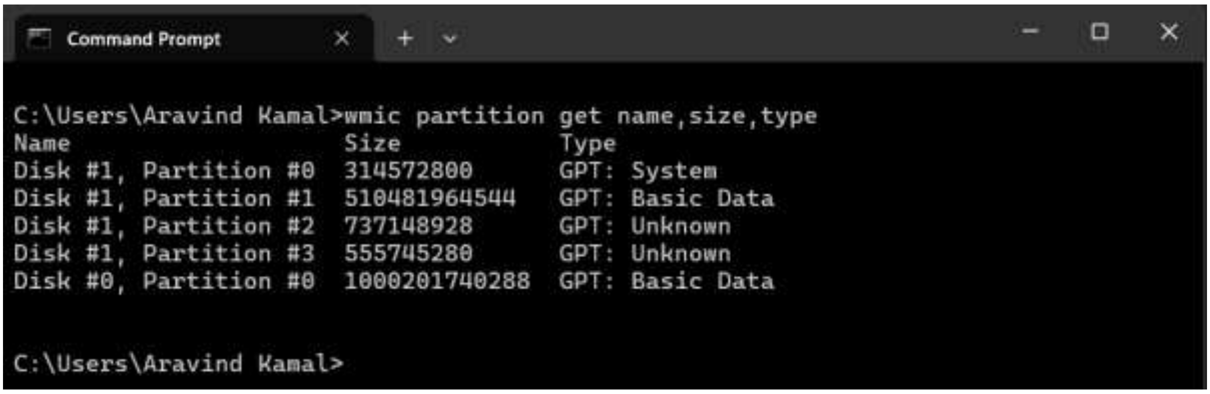
```
C:\Users\Aravind Kamal>wmic cpu get name, deviceid
DeviceID  Name
CPU0      AMD Ryzen 5 5600H with Radeon Graphics


C:\Users\Aravind Kamal>
```



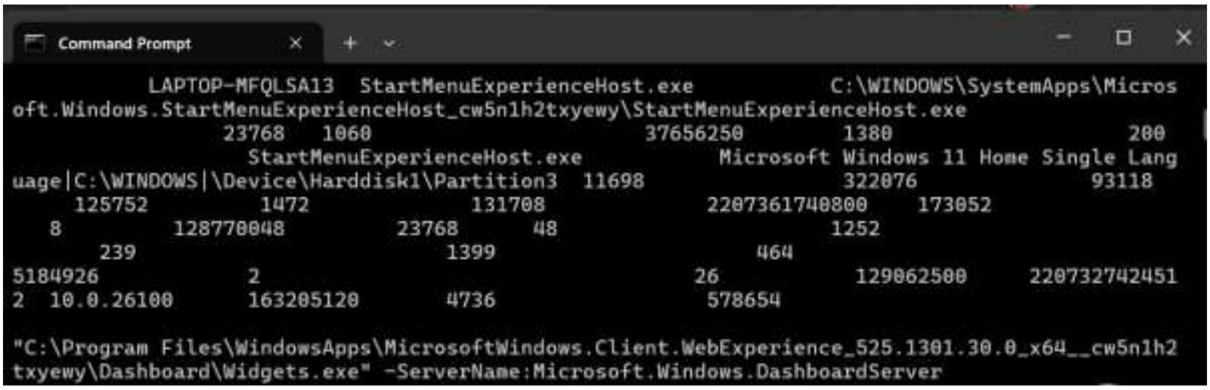
```
C:\Users\Aravind Kamal>wmic cpu get numberofcores,maxclockspeed,status
MaxClockSpeed  NumberOfCores  Status
3301           6              OK


C:\Users\Aravind Kamal>
```



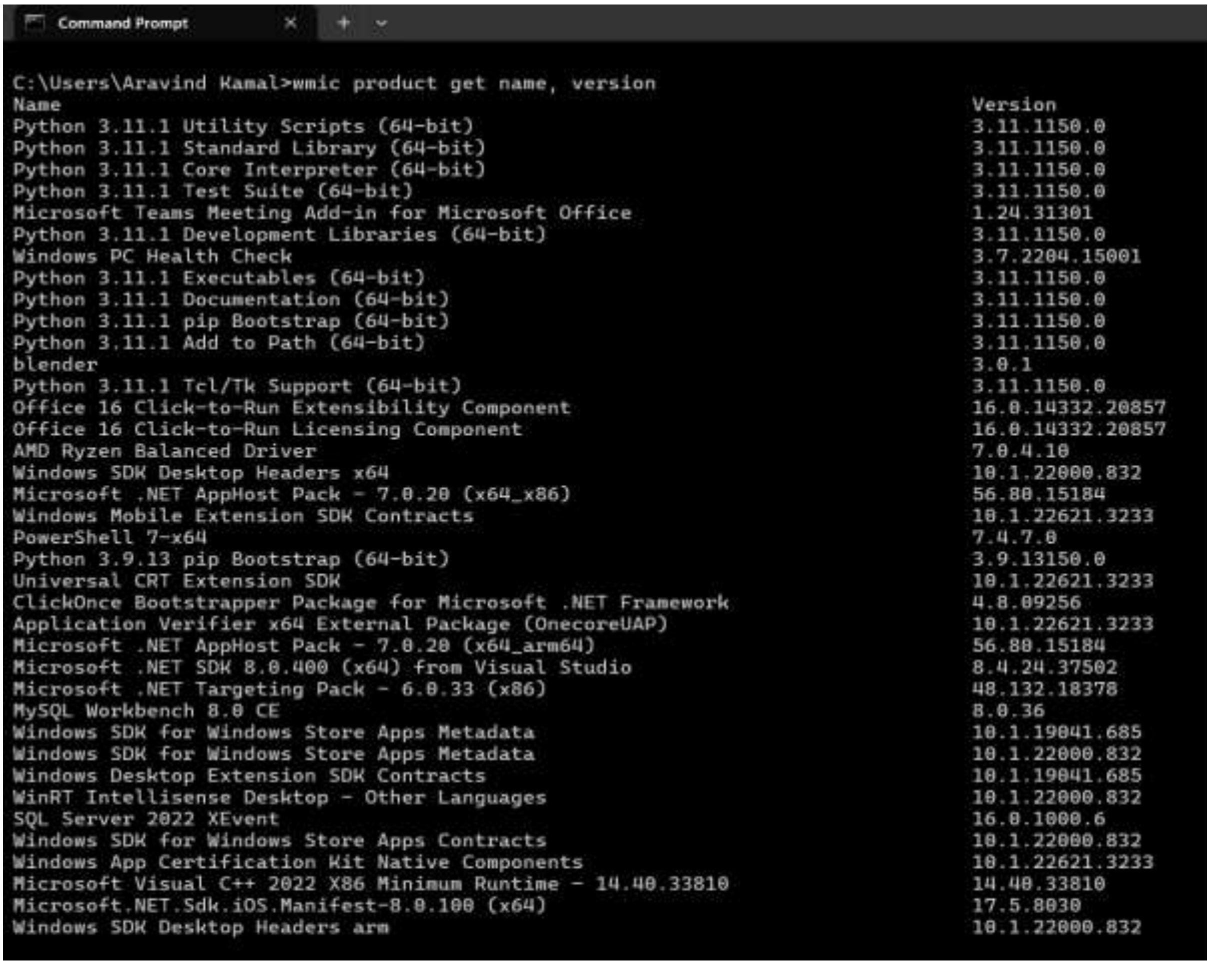
```
C:\Users\Aravind Kamal>wmic computersystem get totalphysicalmemory
TotalPhysicalMemory
16477155328


C:\Users\Aravind Kamal>
```



```
C:\Users\Aravind Kamal>wmic partition get name,size,type
Name                   Size           Type
Disk #1, Partition #0  314572800      GPT: System
Disk #1, Partition #1  510481964544   GPT: Basic Data
Disk #1, Partition #2  737148928      GPT: Unknown
Disk #1, Partition #3  555745280      GPT: Unknown
Disk #0, Partition #0  1000201740288  GPT: Basic Data

C:\Users\Aravind Kamal>
```

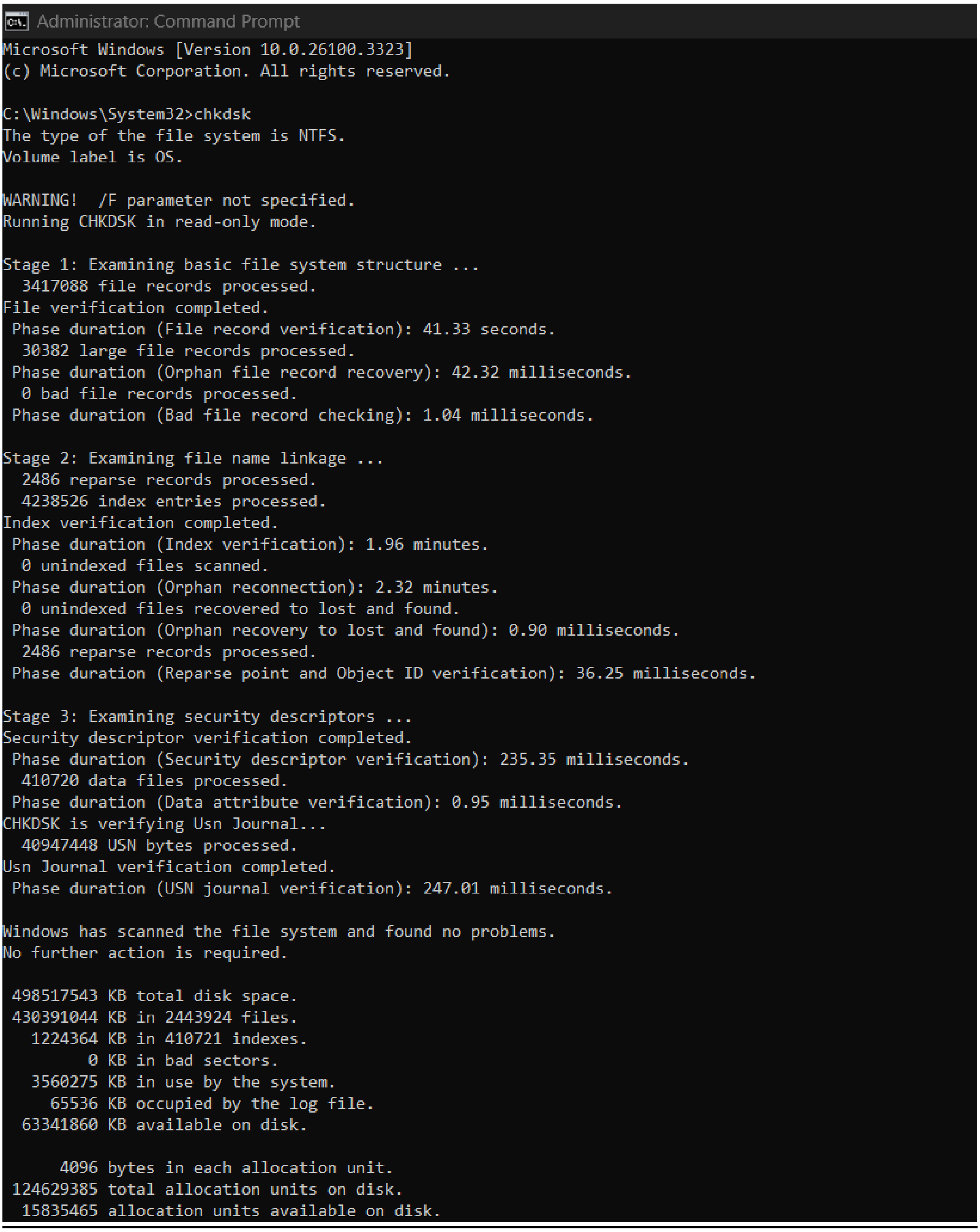


```
           LAPTOP-MFQLSA13  StartMenuExperienceHost.exe          C:\WINDOWS\SystemApps\Micros
oft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe
                 23768   1060                     37656250        1380                   200
                   StartMenuExperienceHost.exe          Microsoft Windows 11 Home Single Lang
uage|C:\WINDOWS|\Device\Harddisk1\Partition3  11698               322076              93118
     125752         1472             131708            2207361740800    173052
   8         128770048        23768     48                      1252
       239                         1399                    464
5184926            2                                  26           129062500     220732742451
2  10.0.26100      163205120       4736                578654

"C:\Program Files\WindowsApps\MicrosoftWindows.Client.WebExperience_525.1301.30.0_x64__cw5n1h2
txyewy\Dashboard\Widgets.exe" -ServerName:Microsoft.Windows.DashboardServer
```



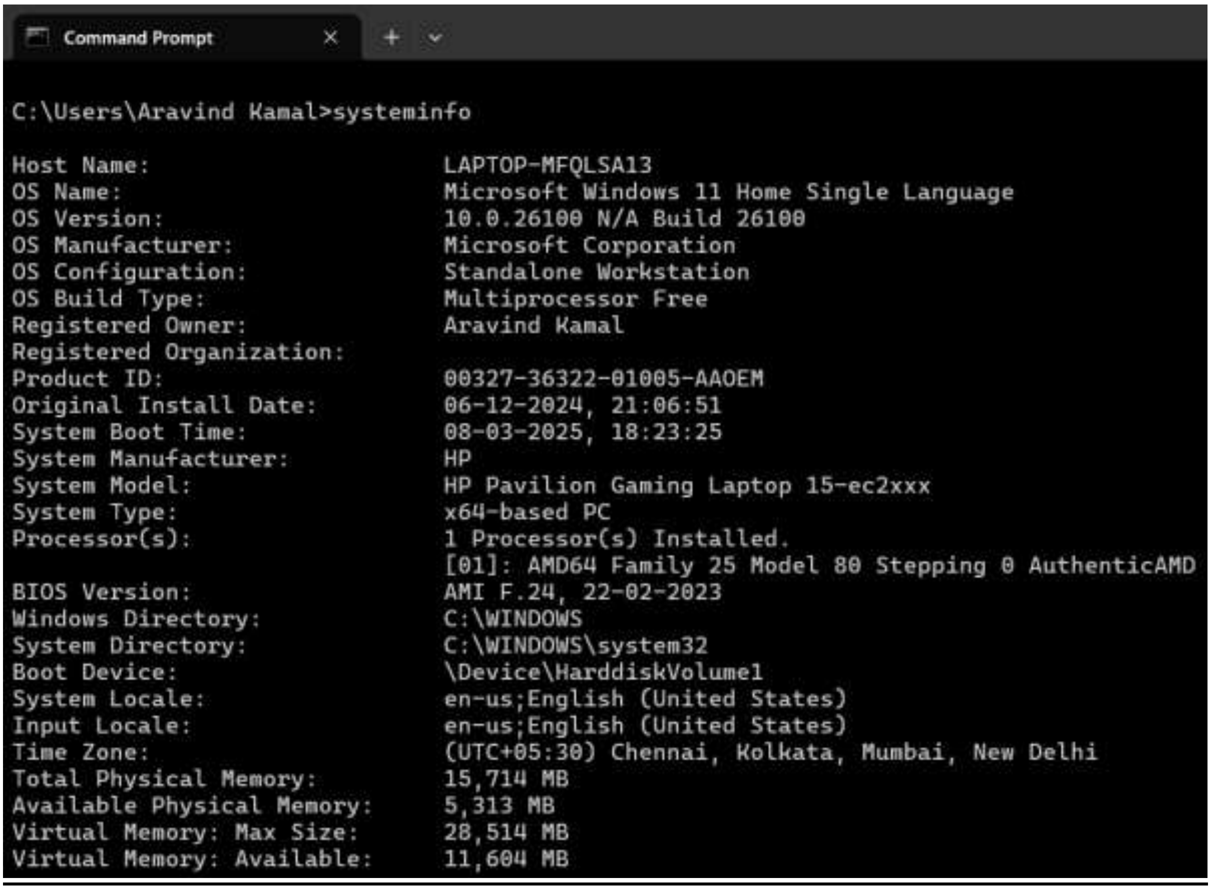
```
C:\Users\Aravind Kamal>wmic product get name, version
Name                                                                           Version
Python 3.11.1 Utility Scripts (64-bit)                                         3.11.1150.0
Python 3.11.1 Standard Library (64-bit)                                        3.11.1150.0
Python 3.11.1 Core Interpreter (64-bit)                                        3.11.1150.0
Python 3.11.1 Test Suite (64-bit)                                              3.11.1150.0
Microsoft Teams Meeting Add-in for Microsoft Office                            1.24.31301
Python 3.11.1 Development Libraries (64-bit)                                   3.11.1150.0
Windows PC Health Check                                                        3.7.2204.15001
Python 3.11.1 Executables (64-bit)                                             3.11.1150.0
Python 3.11.1 Documentation (64-bit)                                           3.11.1150.0
Python 3.11.1 pip Bootstrap (64-bit)                                           3.11.1150.0
Python 3.11.1 Add to Path (64-bit)                                             3.11.1150.0
blender                                                                        3.0.1
Python 3.11.1 Tcl/Tk Support (64-bit)                                          3.11.1150.0
Office 16 Click-to-Run Extensibility Component                                 16.0.14332.20857
Office 16 Click-to-Run Licensing Component                                     16.0.14332.20857
AMD Ryzen Balanced Driver                                                      7.0.4.10
Windows SDK Desktop Headers x64                                                10.1.22000.832
Microsoft .NET AppHost Pack - 7.0.20 (x64_x86)                                 56.80.15184
Windows Mobile Extension SDK Contracts                                         10.1.22621.3233
PowerShell 7-x64                                                               7.4.7.0
Python 3.9.13 pip Bootstrap (64-bit)                                           3.9.13150.0
Universal CRT Extension SDK                                                    10.1.22621.3233
ClickOnce Bootstrapper Package for Microsoft .NET Framework                    4.8.09256
Application Verifier x64 External Package (OnecoreUAP)                         10.1.22621.3233
Microsoft .NET AppHost Pack - 7.0.20 (x64_arm64)                               56.80.15184
Microsoft .NET SDK 8.0.400 (x64) from Visual Studio                            8.4.24.37502
Microsoft .NET Targeting Pack - 6.0.33 (x86)                                   48.132.18378
MySQL Workbench 8.0 CE                                                         8.0.36
Windows SDK for Windows Store Apps Metadata                                    10.1.19041.685
Windows SDK for Windows Store Apps Metadata                                    10.1.22000.832
Windows Desktop Extension SDK Contracts                                        10.1.19041.685
WinRT Intellisense Desktop - Other Languages                                   10.1.22000.832
SQL Server 2022 XEvent                                                         16.0.1000.6
Windows SDK for Windows Store Apps Contracts                                   10.1.22000.832
Windows App Certification Kit Native Components                                10.1.22621.3233
Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.40.33810                    14.40.33810
Microsoft.NET.Sdk.iOS.Manifest-8.0.100 (x64)                                   17.5.8030
Windows SDK Desktop Headers arm                                                10.1.22000.832
```

Chkdsk



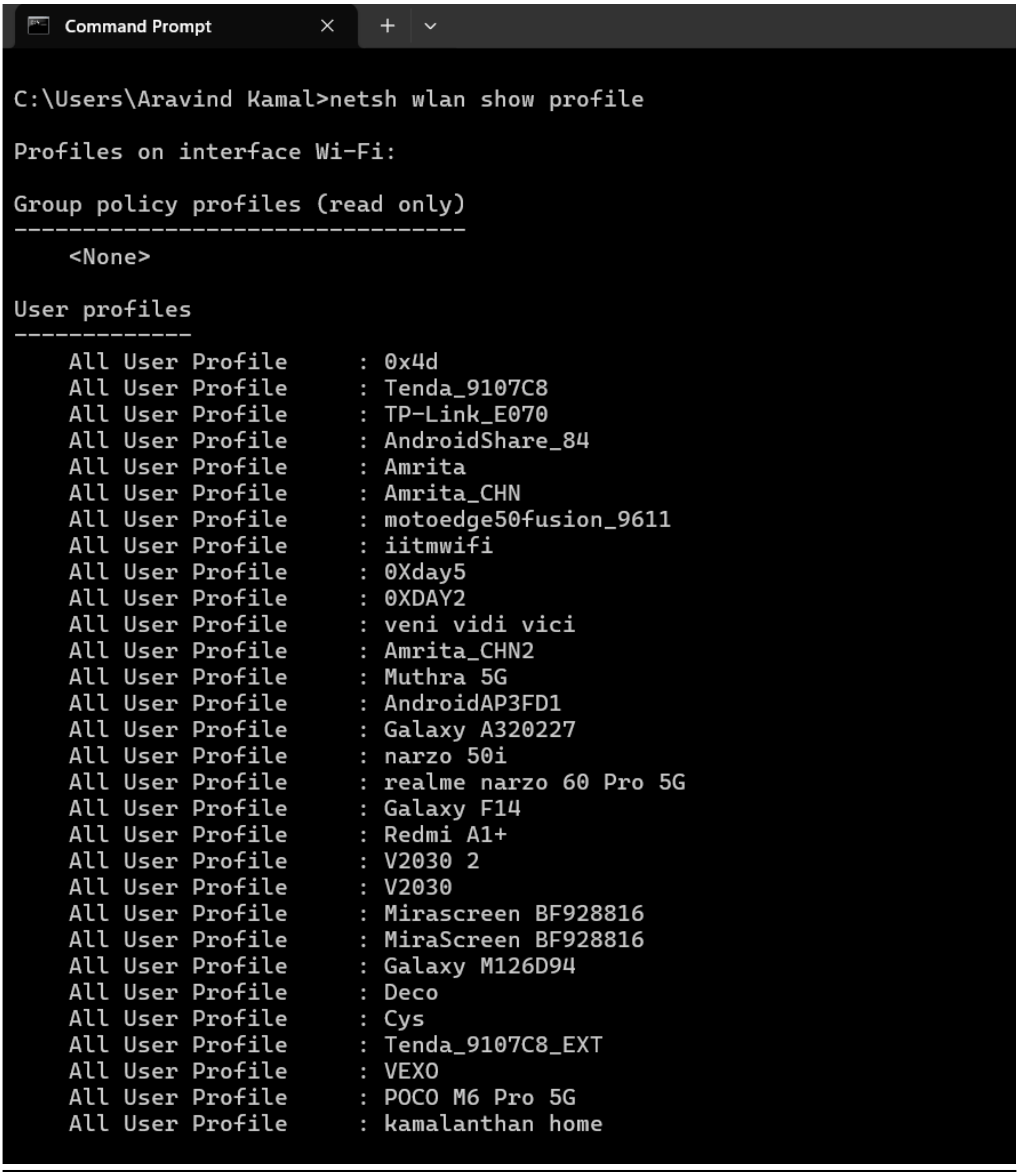
```
Microsoft Windows [Version 10.0.26100.3323]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>chkdsk
The type of the file system is NTFS.
Volume label is OS.

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

Stage 1: Examining basic file system structure ...
  3417088 file records processed.
File verification completed.
 Phase duration (File record verification): 41.33 seconds.
  30382 large file records processed.
 Phase duration (Orphan file record recovery): 42.32 milliseconds.
  0 bad file records processed.
 Phase duration (Bad file record checking): 1.04 milliseconds.

Stage 2: Examining file name linkage ...
  2486 reparse records processed.
  4238526 index entries processed.
Index verification completed.
 Phase duration (Index verification): 1.96 minutes.
  0 unindexed files scanned.
 Phase duration (Orphan reconnection): 2.32 minutes.
  0 unindexed files recovered to lost and found.
 Phase duration (Orphan recovery to lost and found): 0.90 milliseconds.
  2486 reparse records processed.
 Phase duration (Reparse point and Object ID verification): 36.25 milliseconds.

Stage 3: Examining security descriptors ...
Security descriptor verification completed.
 Phase duration (Security descriptor verification): 235.35 milliseconds.
  410720 data files processed.
 Phase duration (Data attribute verification): 0.95 milliseconds.
CHKDSK is verifying Usn Journal...
  40947448 USN bytes processed.
Usn Journal verification completed.
 Phase duration (USN journal verification): 247.01 milliseconds.

Windows has scanned the file system and found no problems.
No further action is required.

 498517543 KB total disk space.
 430391044 KB in 2443924 files.
   1224364 KB in 410721 indexes.
         0 KB in bad sectors.
   3560275 KB in use by the system.
     65536 KB occupied by the log file.
  63341860 KB available on disk.

      4096 bytes in each allocation unit.
 124629385 total allocation units on disk.
  15835465 allocation units available on disk.
```

SystemInfo

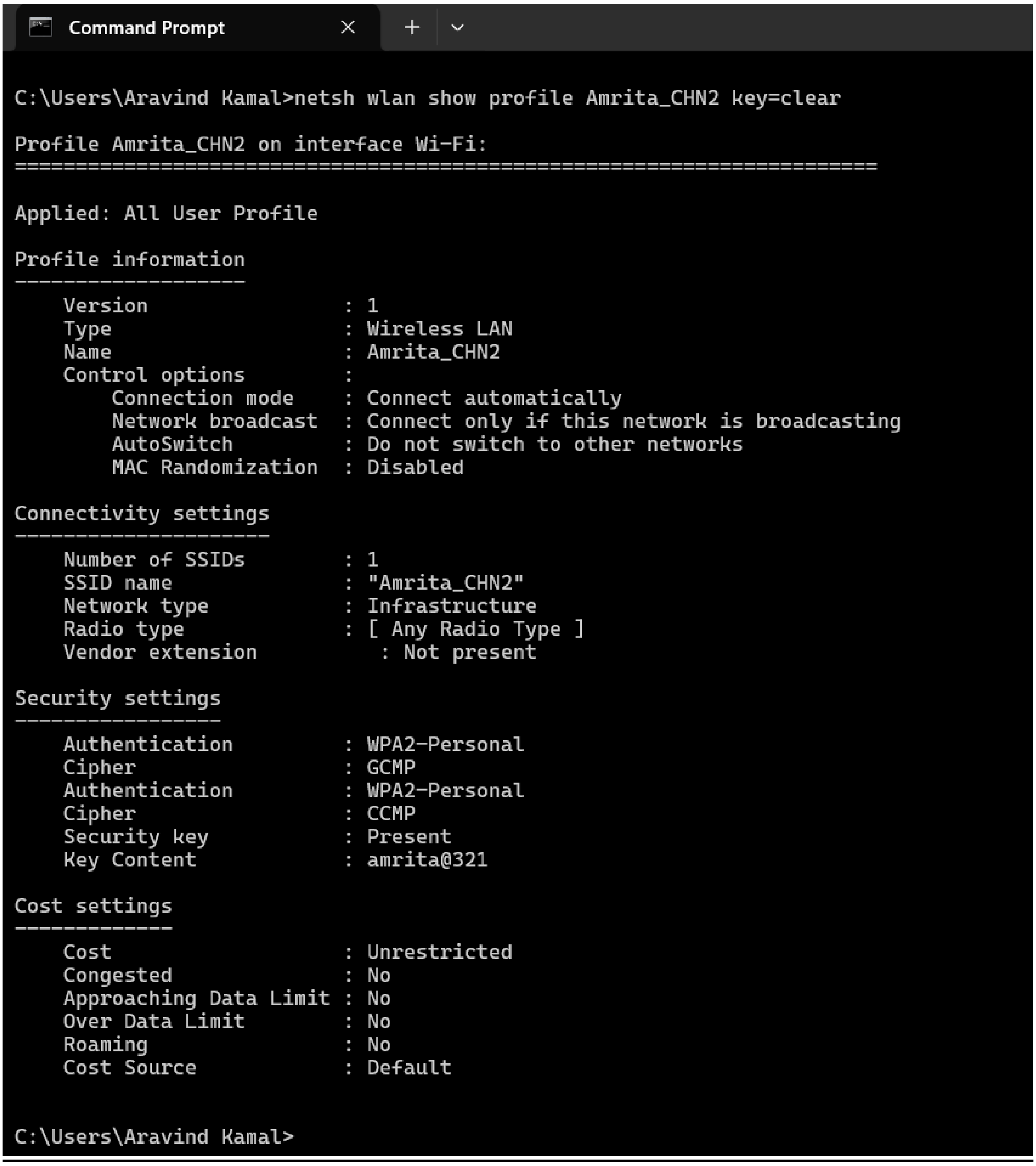


```
C:\Users\Aravind Kamal>systeminfo

Host Name:                 LAPTOP-MFQLSA13
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:          Aravind Kamal
Registered Organization:
Product ID:                00327-36322-01005-AAOEM
Original Install Date:     06-12-2024, 21:06:51
System Boot Time:          08-03-2025, 18:23:25
System Manufacturer:       HP
System Model:              HP Pavilion Gaming Laptop 15-ec2xxx
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 25 Model 80 Stepping 0 AuthenticAMD
BIOS Version:              AMI F.24, 22-02-2023
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     15,714 MB
Available Physical Memory: 5,313 MB
Virtual Memory: Max Size:  28,514 MB
Virtual Memory: Available: 11,604 MB
```

Netsh

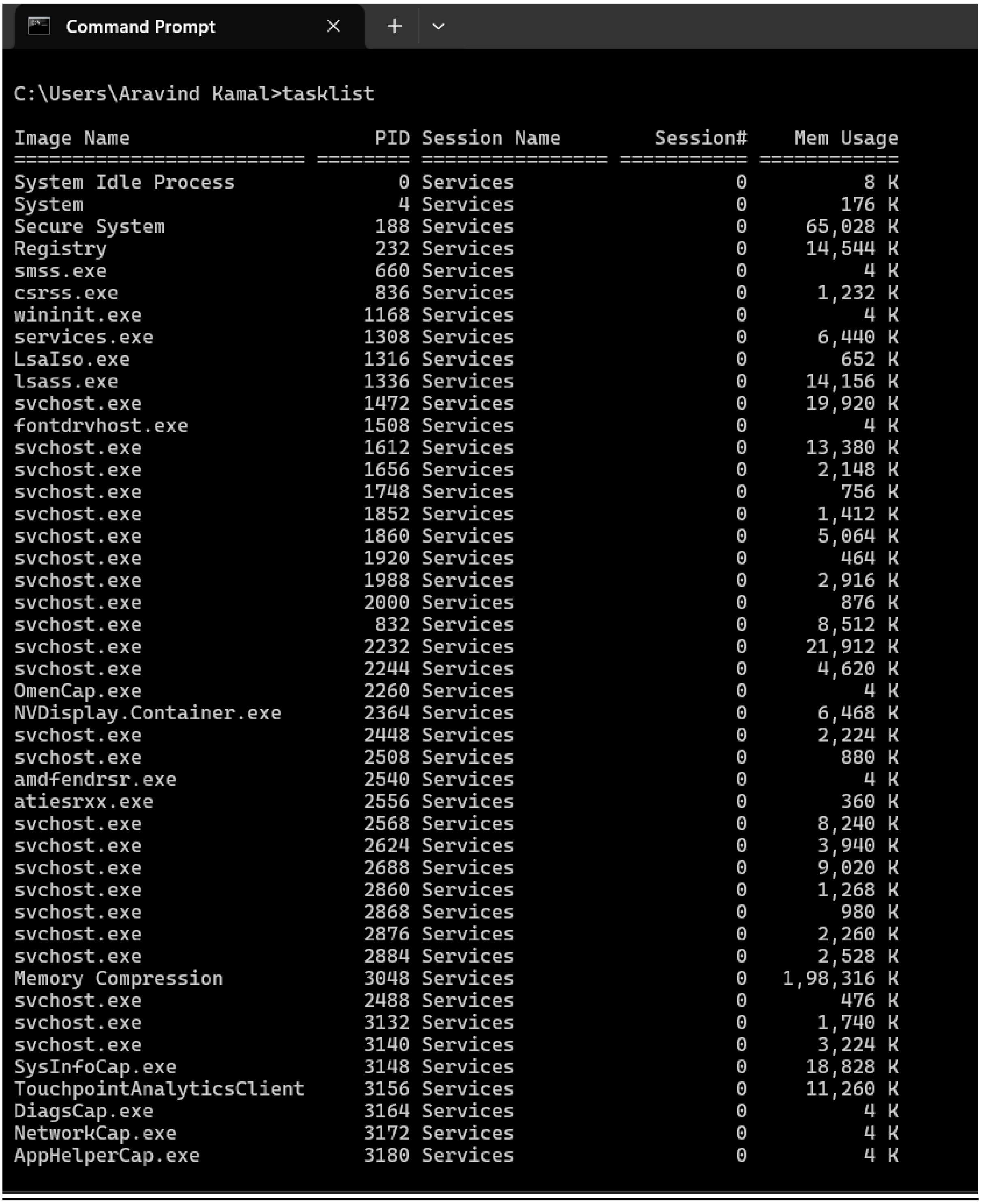


```
C:\Users\Aravind Kamal>netsh wlan show profile

Profiles on interface Wi-Fi:

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

User profiles
-------------
    All User Profile     : 0x4d
    All User Profile     : Tenda_9107C8
    All User Profile     : TP-Link_E070
    All User Profile     : AndroidShare_84
    All User Profile     : Amrita
    All User Profile     : Amrita_CHN
    All User Profile     : motoedge50fusion_9611
    All User Profile     : iitmwifi
    All User Profile     : 0Xday5
    All User Profile     : 0XDAY2
    All User Profile     : veni vidi vici
    All User Profile     : Amrita_CHN2
    All User Profile     : Muthra 5G
    All User Profile     : AndroidAP3FD1
    All User Profile     : Galaxy A320227
    All User Profile     : narzo 50i
    All User Profile     : realme narzo 60 Pro 5G
    All User Profile     : Galaxy F14
    All User Profile     : Redmi A1+
    All User Profile     : V2030 2
    All User Profile     : V2030
    All User Profile     : Mirascreen BF928816
    All User Profile     : MiraScreen BF928816
    All User Profile     : Galaxy M126D94
    All User Profile     : Deco
    All User Profile     : Cys
    All User Profile     : Tenda_9107C8_EXT
    All User Profile     : VEXO
    All User Profile     : POCO M6 Pro 5G
    All User Profile     : kamalanthan home
```



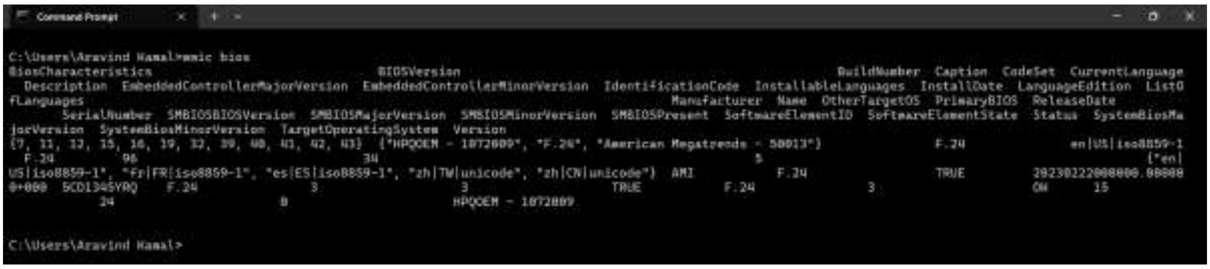
```
C:\Users\Aravind Kamal>netsh wlan show profile Amrita_CHN2 key=clear

Profile Amrita_CHN2 on interface Wi-Fi:
=======================================================================

Applied: All User Profile

Profile information
-------------------
    Version                : 1
    Type                   : Wireless LAN
    Name                   : Amrita_CHN2
    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

Connectivity settings
---------------------
    Number of SSIDs        : 1
    SSID name              : "Amrita_CHN2"
    Network type           : Infrastructure
    Radio type             : [ Any Radio Type ]
    Vendor extension          : Not present

Security settings
-----------------
    Authentication         : WPA2-Personal
    Cipher                 : GCMP
    Authentication         : WPA2-Personal
    Cipher                 : CCMP
    Security key           : Present
    Key Content            : amrita@321

Cost settings
-------------
    Cost                   : Unrestricted
    Congested              : No
    Approaching Data Limit : No
    Over Data Limit        : No
    Roaming                : No
    Cost Source            : Default


C:\Users\Aravind Kamal>
```

Tasklist



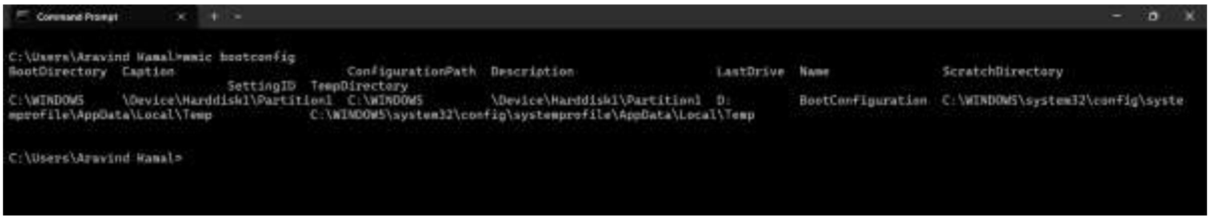
```
C:\Users\Aravind Kamal>tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0        176 K
Secure System                  188 Services                   0     65,028 K
Registry                       232 Services                   0     14,544 K
smss.exe                       660 Services                   0          4 K
csrss.exe                      836 Services                   0      1,232 K
wininit.exe                   1168 Services                   0          4 K
services.exe                  1308 Services                   0      6,440 K
LsaIso.exe                    1316 Services                   0        652 K
lsass.exe                     1336 Services                   0     14,156 K
svchost.exe                   1472 Services                   0     19,920 K
fontdrvhost.exe               1508 Services                   0          4 K
svchost.exe                   1612 Services                   0     13,380 K
svchost.exe                   1656 Services                   0      2,148 K
svchost.exe                   1748 Services                   0        756 K
svchost.exe                   1852 Services                   0      1,412 K
svchost.exe                   1860 Services                   0      5,064 K
svchost.exe                   1920 Services                   0        464 K
svchost.exe                   1988 Services                   0      2,916 K
svchost.exe                   2000 Services                   0        876 K
svchost.exe                    832 Services                   0      8,512 K
svchost.exe                   2232 Services                   0     21,912 K
svchost.exe                   2244 Services                   0      4,620 K
OmenCap.exe                   2260 Services                   0          4 K
NVDisplay.Container.exe       2364 Services                   0      6,468 K
svchost.exe                   2448 Services                   0      2,224 K
svchost.exe                   2508 Services                   0        880 K
amdfendrsr.exe                2540 Services                   0          4 K
atiesrxx.exe                  2556 Services                   0        360 K
svchost.exe                   2568 Services                   0      8,240 K
svchost.exe                   2624 Services                   0      3,940 K
svchost.exe                   2688 Services                   0      9,020 K
svchost.exe                   2860 Services                   0      1,268 K
svchost.exe                   2868 Services                   0        980 K
svchost.exe                   2876 Services                   0      2,260 K
svchost.exe                   2884 Services                   0      2,528 K
Memory Compression            3048 Services                   0   1,98,316 K
svchost.exe                   2488 Services                   0        476 K
svchost.exe                   3132 Services                   0      1,740 K
svchost.exe                   3140 Services                   0      3,224 K
SysInfoCap.exe                3148 Services                   0     18,828 K
TouchpointAnalyticsClient     3156 Services                   0     11,260 K
DiagsCap.exe                  3164 Services                   0          4 K
NetworkCap.exe                3172 Services                   0          4 K
AppHelperCap.exe              3180 Services                   0          4 K
```

- **Bios – Gives the details of the bios vendor**
  - **C:wmic bios**



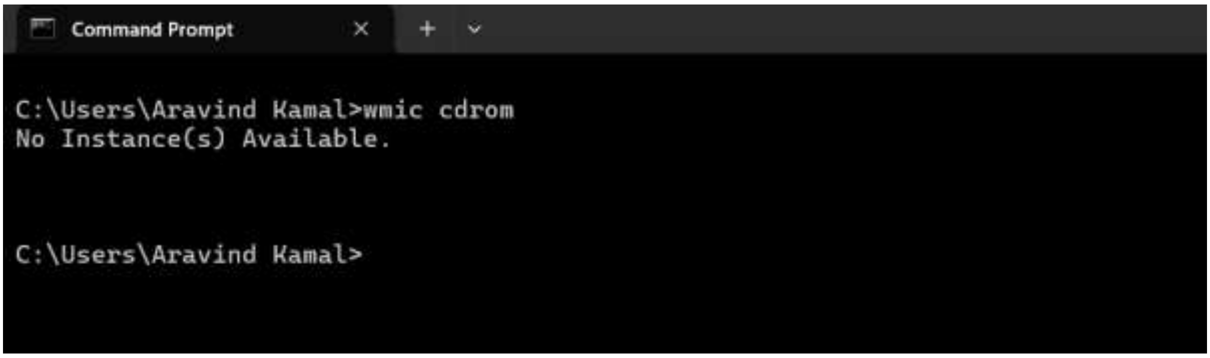
```
C:\Users\Aravind Kamal>wmic bios
BiosCharacteristics                               BIOSVersion                                                 BuildNumber  Caption  CodeSet  CurrentLanguage
  Description  EmbeddedControllerMajorVersion  EmbeddedControllerMinorVersion  IdentificationCode  InstallableLanguages  InstallDate  LanguageEdition  ListO
fLanguages                                                                                          Manufacturer  Name  OtherTargetOS  PrimaryBIOS  ReleaseDate
       SerialNumber  SMBIOSBIOSVersion  SMBIOSMajorVersion  SMBIOSMinorVersion  SMBIOSPresent  SoftwareElementID  SoftwareElementState  Status  SystemBiosMa
jorVersion  SystemBiosMinorVersion  TargetOperatingSystem  Version
{7, 11, 12, 15, 16, 19, 32, 39, 40, 41, 42, 43}  {"HPQOEM - 1072009", "F.24", "American Megatrends - 50013"}                  F.24                 en|US|iso8859-1
  F.24          96                          34                                              5                                                  {"en|
US|iso8859-1", "fr|FR|iso8859-1", "es|ES|iso8859-1", "zh|TW|unicode", "zh|CN|unicode"}  AMI             F.24                    TRUE          20230222000000.000000
0+000  5CD1345YRQ    F.24                3                     3                   TRUE            F.24               3                   ON       15
           24                   0                         HPQOEM - 1072009


C:\Users\Aravind Kamal>
```

- **Bootconfig – displays the bootpartition and related data**
  - **C:wmic bootconfig**



```
C:\Users\Aravind Kamal>wmic bootconfig
BootDirectory  Caption                     ConfigurationPath  Description                     LastDrive  Name               ScratchDirectory
                         SettingID  TempDirectory
C:\WINDOWS     \Device\Harddisk1\Partition1  C:\WINDOWS         \Device\Harddisk1\Partition1  D:         BootConfiguration  C:\WINDOWS\system32\config\syste
mprofile\AppData\Local\Temp              C:\WINDOWS\system32\config\systemprofile\AppData\Local\Temp


C:\Users\Aravind Kamal>
```

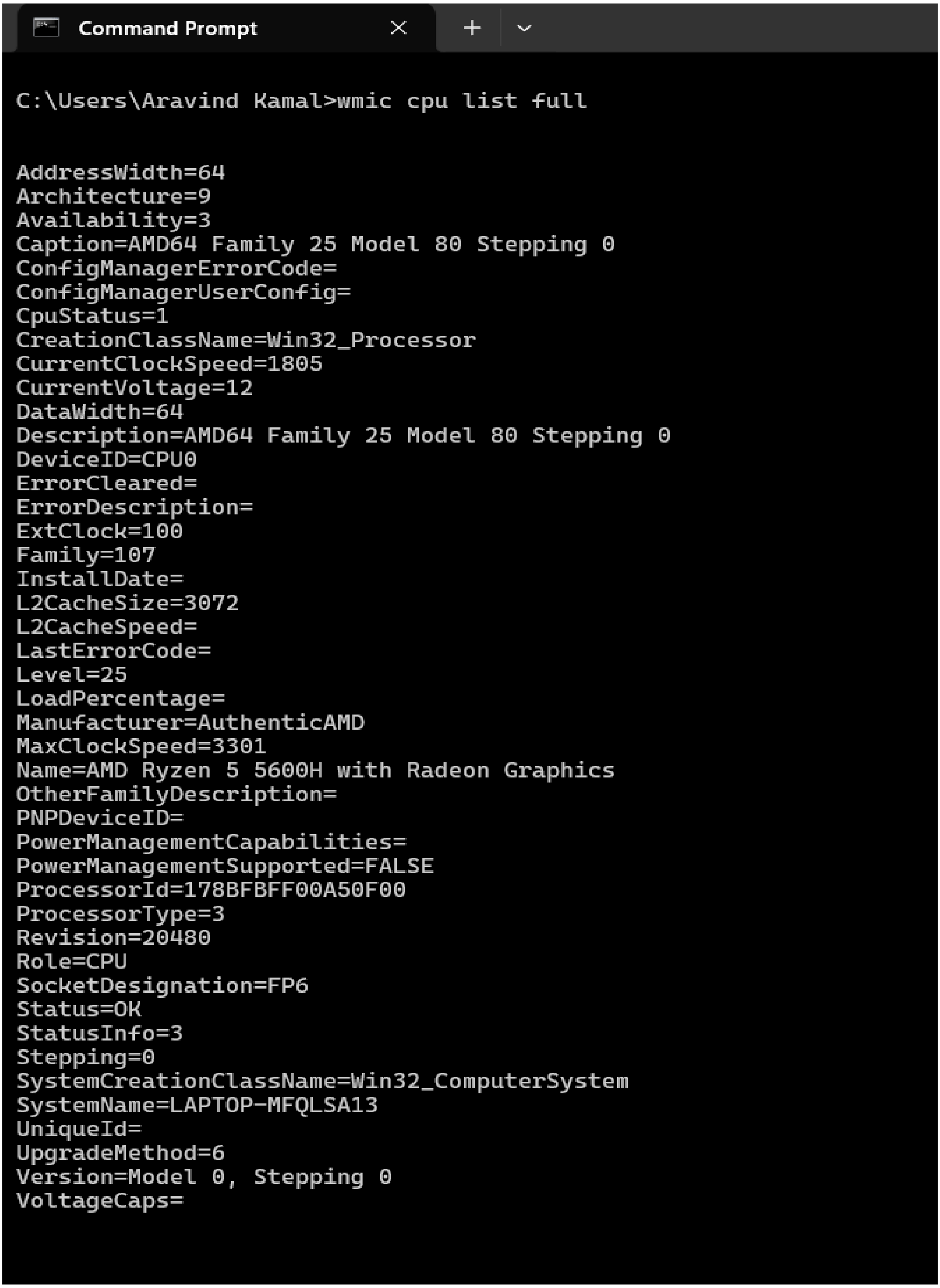
- **Cdrom – displays the details of any optical disc hardware or virtual optical drives (daemon tools, gamedrive) as well.**
  - **C:wmic cdrom**



```
C:\Users\Aravind Kamal>wmic cdrom
No Instance(s) Available.


C:\Users\Aravind Kamal>
```

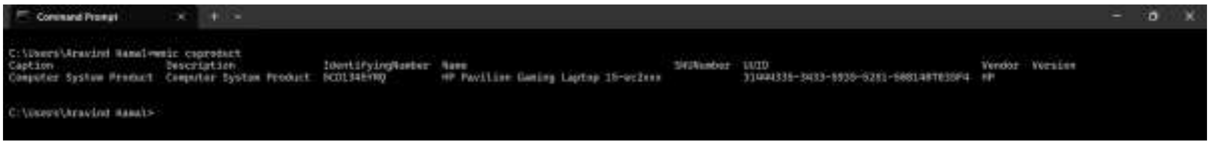
CPU – lists the properties of the microprocessor(s) installed.

- C:wmic cpu list full



```
C:\Users\Aravind Kamal>wmic cpu list full


AddressWidth=64
Architecture=9
Availability=3
Caption=AMD64 Family 25 Model 80 Stepping 0
ConfigManagerErrorCode=
ConfigManagerUserConfig=
CpuStatus=1
CreationClassName=Win32_Processor
CurrentClockSpeed=1805
CurrentVoltage=12
DataWidth=64
Description=AMD64 Family 25 Model 80 Stepping 0
DeviceID=CPU0
ErrorCleared=
ErrorDescription=
ExtClock=100
Family=107
InstallDate=
L2CacheSize=3072
L2CacheSpeed=
LastErrorCode=
Level=25
LoadPercentage=
Manufacturer=AuthenticAMD
MaxClockSpeed=3301
Name=AMD Ryzen 5 5600H with Radeon Graphics
OtherFamilyDescription=
PNPDeviceID=
PowerManagementCapabilities=
PowerManagementSupported=FALSE
ProcessorId=178BFBFF00A50F00
ProcessorType=3
Revision=20480
Role=CPU
SocketDesignation=FP6
Status=OK
StatusInfo=3
Stepping=0
SystemCreationClassName=Win32_ComputerSystem
SystemName=LAPTOP-MFQLSA13
UniqueId=
UpgradeMethod=6
Version=Model 0, Stepping 0
VoltageCaps=
```

- **Gives a view of the column headers line by line**
    - **Csproduct list full – Gives the serial number and vendor name of the laptop/desktop system as well as the UUID and version number. Very useful for viewing this information without opening your laptop.**
- **C:wmic csproduct**



```
C:\Users\Aravind Kamal>wmic csproduct
Caption                 Description             IdentifyingNumber  Name                                 SKUNumber  UUID                                  Vendor  Version
Computer System Product  Computer System Product  5CD1348YRQ         HP Pavilion Gaming Laptop 15-ec1xxx             31444336-3433-5935-5251-5881487E35F4  HP

C:\Users\Aravind Kamal>
```