Secure Coding- Assignment

Name: Ch. Sesha Pranav

Reg.no:19BCN7190

Slot:L39-L40

Date:24.03.2021

KNOWN COMMANDS

```
PS C:\Users\sesha_h2tkg8x> PING WWW.GOOGLE.COM

Pinging WWW.GOOGLE.COM [2404:6800:4009:815::2004] with 32 bytes of data:
Request timed out.
Reply from 2404:6800:4009:815::2004: time=276ms
Reply from 2404:6800:4009:815::2004: time=223ms
Reply from 2404:6800:4009:815::2004: time=272ms

Ping statistics for 2404:6800:4009:815::2004:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 223ms, Maximum = 276ms, Average = 257ms
```

IPCONFIG

```
PS C:\Users\sesha_h2tkg8x> IPCONFIG

Windows IP Configuration


Ethernet adapter Ethernet 2:

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

Wireless LAN adapter Local Area Connection* 3:

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

Wireless LAN adapter Local Area Connection* 6:

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

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c22:b0ed:262:e143%11
   IPv4 Address. . . . . . . . . . . : 192.168.146.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f070:450d:7e45:1644%12
   IPv4 Address. . . . . . . . . . . : 192.168.26.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi 2:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2409:4070:4604:f0b1:1d5e:a1cf:cd2b:45aa
   Temporary IPv6 Address. . . . . . : 2409:4070:4604:f0b1:b056:33df:ee36:5bf8
   Link-local IPv6 Address . . . . . : fe80::1d5e:a1cf:cd2b:45aa%8
   IPv4 Address. . . . . . . . . . . : 192.168.225.50
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::bc5f:a436:2499:8125%8
                                       fe80::dc43:88ff:fecd:2261%8
                                       192.168.225.1


Ethernet adapter Bluetooth Network Connection 3:
```

LS

```
PS C:\Users\sesha_h2tkg8x> LS


    Directory: C:\Users\sesha_h2tkg8x


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         02-11-2020     19:47                .android
d-----         24-07-2020     20:33                .AndroidStudio4.0
d-----         13-08-2020     15:41                .atom
d-----         02-11-2020     19:46                .BigNox
d-----         27-04-2020     18:34                .conda
d-----         13-08-2020     12:23                .config
d-----         13-08-2020     12:23                .eclipse
d-----         22-12-2019     15:33                .gradle
d-----         15-04-2020     11:24                .idlerc
d-----         11-04-2020     21:10                .ipynb_checkpoints
d-----         11-04-2020     21:03                .ipython
d-----         12-04-2020     10:11                .jupyter
d-----         03-11-2020     11:14                .m2
d-----         12-04-2020     12:22                .matplotlib
d-----         03-11-2020     11:10                .nbi
d-----         11-11-2020     20:37                .p2
d-----         13-08-2020     15:41                .platformio
d-----         02-05-2020     13:19                .spyder-py3
d-----         13-08-2020     12:23                .tooling
d-----         11-03-2020     07:20                .ueli
d-----         17-09-2020     18:08                .vscode
d-r---         08-01-2021     04:43                3D Objects
d-----         30-07-2020     20:02                AndroidStudioProjects
d-----         04-04-2020     11:19                Apple
d-----         30-01-2021     16:40                Cisco Packet Tracer 8.0
d-r---         08-01-2021     04:43                Contacts
d-r---         24-03-2021     20:04                Desktop
d-r---         19-03-2021     08:45                Documents
d-r---         24-03-2021     21:28                Downloads
d-----         11-11-2020     19:57                eclipse
d-----         11-11-2020     20:38                eclipse-workspace
d-r---         08-01-2021     04:43                Favorites
d-----         29-04-2020     15:08                HelloNode
d-r---         08-01-2021     04:43                Links
d-r---         08-01-2021     04:43                Music
d-----         11-08-2020     18:02                Nox_share
dar--l         15-03-2021     13:34                OneDrive
d-----         29-01-2021     19:42                Oracle
d-r---         08-01-2021     04:43                Pictures
d-----         24-03-2021     13:43                PycharmProjects
d-r---         08-01-2021     04:43                Saved Games
d-r---         08-01-2021     04:43                Searches
d-r---         08-01-2021     04:43                Videos
d-----         02-11-2020     19:46                vmlogs
-a----         29-04-2020     15:02             13 .bash_history
-a----         13-04-2020     11:50             43 .condarc
-a----         30-07-2020     20:41             16 .emulator_console_auth_token
-a----         17-02-2021     18:40            184 .gitconfig
-a----         29-04-2020     14:52             22 .node_repl_history
-a----         13-03-2021     15:58            184 .packettracer
-a----         07-06-2020     15:29             31 .python_history
-a----         06-03-2020     20:53             15 advanced_ip_scanner_Aliases.bin
```

```
Windows PowerShell

d-----        13-08-2020      12:23                .config
d-----        13-08-2020      12:23                .eclipse
d-----        22-12-2019      15:33                .gradle
d-----        15-04-2020      11:24                .idlerc
d-----        11-04-2020      21:10                .ipynb_checkpoints
d-----        11-04-2020      21:03                .ipython
d-----        12-04-2020      10:11                .jupyter
d-----        03-11-2020      11:14                .m2
d-----        12-04-2020      12:22                .matplotlib
d-----        03-11-2020      11:10                .nbi
d-----        11-11-2020      20:37                .p2
d-----        13-08-2020      15:41                .platformio
d-----        02-05-2020      13:19                .spyder-py3
d-----        13-08-2020      12:23                .tooling
d-----        11-03-2020      07:20                .ueli
d-----        17-09-2020      18:08                .vscode
d-r---        08-01-2021      04:43                3D Objects
d-----        30-07-2020      20:02                AndroidStudioProjects
d-----        04-04-2020      11:19                Apple
d-----        30-01-2021      16:40                Cisco Packet Tracer 8.0
d-r---        08-01-2021      04:43                Contacts
d-r---        24-03-2021      20:04                Desktop
d-r---        19-03-2021      08:45                Documents
d-r---        24-03-2021      21:28                Downloads
d-----        11-11-2020      19:57                eclipse
d-----        11-11-2020      20:38                eclipse-workspace
d-r---        08-01-2021      04:43                Favorites
d-----        29-04-2020      15:08                HelloNode
d-r---        08-01-2021      04:43                Links
d-r---        08-01-2021      04:43                Music
d-----        11-08-2020      18:02                Nox_share
dar--l        15-03-2021      13:34                OneDrive
d-----        29-01-2021      19:42                Oracle
d-r---        08-01-2021      04:43                Pictures
d-----        24-03-2021      13:43                PycharmProjects
d-r---        08-01-2021      04:43                Saved Games
d-r---        08-01-2021      04:43                Searches
d-r---        08-01-2021      04:43                Videos
d-----        02-11-2020      19:46                vmlogs
-a----        29-04-2020      15:02            13 .bash_history
-a----        13-04-2020      11:50            43 .condarc
-a----        30-07-2020      20:41            16 .emulator_console_auth_token
-a----        17-02-2021      18:40           184 .gitconfig
-a----        29-04-2020      14:52            22 .node_repl_history
-a----        13-03-2021      15:58           184 .packettracer
-a----        07-06-2020      15:29            31 .python_history
-a----        06-03-2020      20:53            15 advanced_ip_scanner_Aliases.bin
-a----        06-03-2020      20:53            15 advanced_ip_scanner_Comments.bin
-a----        06-03-2020      20:53           512 advanced_ip_scanner_MAC.bin
-a----        02-08-2020      12:45         67919 battery-report.html
-a----        02-11-2020      20:16           300 d4ac4633ebd6440fa397b84f1bc94a3c.7z
-a----        11-04-2020      21:50          1661 fulfilment_center_info.csv
-a----        11-08-2020      18:02            66 inittk.ini
-a----        11-08-2020      18:01            41 inst.ini
-a----        11-04-2020      21:47          1096 meal_info.csv
-a----        11-08-2020      18:01            45 nuuid.ini
-a----        11-04-2020      21:56      18733819 train.csv
-a----        11-04-2020      21:05           555 Untitled.ipynb
-a----        02-05-2020      10:29           123 untitled0.py
-a----        11-04-2020      21:10            72 Untitled1.ipynb
-a----        11-08-2020      18:01            53 useruid.ini
-a----        13-04-2020      13:06        101263 WEEK 0 CODING ASST.ipynb
```

Get-Alias

```
PS C:\Users\sesha_h2tkg8x> Get-Alias

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Alias           % -> ForEach-Object
Alias           ? -> Where-Object
Alias           ac -> Add-Content
Alias           asnp -> Add-PSSnapin
Alias           cat -> Get-Content
Alias           cd -> Set-Location
Alias           CFS -> ConvertFrom-String                          3.1.0.0    Microsoft.PowerShell.Utility
Alias           chdir -> Set-Location
Alias           clc -> Clear-Content
Alias           clear -> Clear-Host
Alias           clhy -> Clear-History
Alias           cli -> Clear-Item
Alias           clp -> Clear-ItemProperty
Alias           cls -> Clear-Host
Alias           clv -> Clear-Variable
Alias           cnsn -> Connect-PSSession
Alias           compare -> Compare-Object
Alias           copy -> Copy-Item
Alias           cp -> Copy-Item
Alias           cpi -> Copy-Item
Alias           cpp -> Copy-ItemProperty
Alias           curl -> Invoke-WebRequest
Alias           cvpa -> Convert-Path
Alias           dbp -> Disable-PSBreakpoint
Alias           del -> Remove-Item
Alias           diff -> Compare-Object
Alias           dir -> Get-ChildItem
Alias           dnsn -> Disconnect-PSSession
Alias           ebp -> Enable-PSBreakpoint
Alias           echo -> Write-Output
Alias           epal -> Export-Alias
Alias           epcsv -> Export-Csv
Alias           epsn -> Export-PSSession
Alias           erase -> Remove-Item
Alias           etsn -> Enter-PSSession
Alias           exsn -> Exit-PSSession
Alias           fc -> Format-Custom
Alias           fhx -> Format-Hex                                  3.1.0.0    Microsoft.PowerShell.Utility
Alias           fl -> Format-List
Alias           foreach -> ForEach-Object
Alias           ft -> Format-Table
Alias           fw -> Format-Wide
Alias           gal -> Get-Alias
Alias           gbp -> Get-PSBreakpoint
Alias           gc -> Get-Content
Alias           gcb -> Get-Clipboard                               3.1.0.0    Microsoft.PowerShell.Management
Alias           gci -> Get-ChildItem
Alias           gcm -> Get-Command
Alias           gcs -> Get-PSCallStack
Alias           gdr -> Get-PSDrive
Alias           ghy -> Get-History
Alias           gi -> Get-Item
Alias           gin -> Get-ComputerInfo                            3.1.0.0    Microsoft.PowerShell.Management
Alias           gjb -> Get-Job
Alias           gl -> Get-Location
Alias           gm -> Get-Member
```

```
Windows PowerShell
Alias            gp -> Get-ItemProperty
Alias            gps -> Get-Process
Alias            gpv -> Get-ItemPropertyValue
Alias            group -> Group-Object
Alias            gsn -> Get-PSSession
Alias            gsnp -> Get-PSSnapin
Alias            gsv -> Get-Service
Alias            gtz -> Get-TimeZone                     3.1.0.0    Microsoft.PowerShell.Management
Alias            gu -> Get-Unique
Alias            gv -> Get-Variable
Alias            gwmi -> Get-WmiObject
Alias            h -> Get-History
Alias            history -> Get-History
Alias            icm -> Invoke-Command
Alias            iex -> Invoke-Expression
Alias            ihy -> Invoke-History
Alias            ii -> Invoke-Item
Alias            ipal -> Import-Alias
Alias            ipcsv -> Import-Csv
Alias            ipmo -> Import-Module
Alias            ipsn -> Import-PSSession
Alias            irm -> Invoke-RestMethod
Alias            ise -> powershell_ise.exe
Alias            iwmi -> Invoke-WmiMethod
Alias            iwr -> Invoke-WebRequest
Alias            kill -> Stop-Process
Alias            lp -> Out-Printer
Alias            ls -> Get-ChildItem
Alias            man -> help
Alias            md -> mkdir
Alias            measure -> Measure-Object
Alias            mi -> Move-Item
Alias            mount -> New-PSDrive
Alias            move -> Move-Item
Alias            mp -> Move-ItemProperty
Alias            mv -> Move-Item
Alias            nal -> New-Alias
Alias            ndr -> New-PSDrive
Alias            ni -> New-Item
Alias            nmo -> New-Module
Alias            npssc -> New-PSSessionConfigurationFile
Alias            nsn -> New-PSSession
Alias            nv -> New-Variable
Alias            ogv -> Out-GridView
Alias            oh -> Out-Host
Alias            popd -> Pop-Location
Alias            ps -> Get-Process
Alias            pushd -> Push-Location
Alias            pwd -> Get-Location
Alias            r -> Invoke-History
Alias            rbp -> Remove-PSBreakpoint
Alias            rcjb -> Receive-Job
Alias            rcsn -> Receive-PSSession
Alias            rd -> Remove-Item
Alias            rdr -> Remove-PSDrive
Alias            ren -> Rename-Item
Alias            ri -> Remove-Item
Alias            rjb -> Remove-Job
Alias            rm -> Remove-Item
Alias            rmdir -> Remove-Item
Alias            rmo -> Remove-Module
Alias            rni -> Rename-Item
```

```
 Windows PowerShell
Alias           nmo -> New-Module
Alias           npssc -> New-PSSessionConfigurationFile
Alias           nsn -> New-PSSession
Alias           nv -> New-Variable
Alias           ogv -> Out-GridView
Alias           oh -> Out-Host
Alias           popd -> Pop-Location
Alias           ps -> Get-Process
Alias           pushd -> Push-Location
Alias           pwd -> Get-Location
Alias           r -> Invoke-History
Alias           rbp -> Remove-PSBreakpoint
Alias           rcjb -> Receive-Job
Alias           rcsn -> Receive-PSSession
Alias           rd -> Remove-Item
Alias           rdr -> Remove-PSDrive
Alias           ren -> Rename-Item
Alias           ri -> Remove-Item
Alias           rjb -> Remove-Job
Alias           rm -> Remove-Item
Alias           rmdir -> Remove-Item
Alias           rmo -> Remove-Module
Alias           rni -> Rename-Item
Alias           rnp -> Rename-ItemProperty
Alias           rp -> Remove-ItemProperty
Alias           rsn -> Remove-PSSession
Alias           rsnp -> Remove-PSSnapin
Alias           rujb -> Resume-Job
Alias           rv -> Remove-Variable
Alias           rvpa -> Resolve-Path
Alias           rwmi -> Remove-WmiObject
Alias           sajb -> Start-Job
Alias           sal -> Set-Alias
Alias           saps -> Start-Process
Alias           sasv -> Start-Service
Alias           sbp -> Set-PSBreakpoint
Alias           sc -> Set-Content
Alias           scb -> Set-Clipboard                        3.1.0.0    Microsoft.PowerShell.Management
Alias           select -> Select-Object
Alias           set -> Set-Variable
Alias           shcm -> Show-Command
Alias           si -> Set-Item
Alias           sl -> Set-Location
Alias           sleep -> Start-Sleep
Alias           sls -> Select-String
Alias           sort -> Sort-Object
Alias           sp -> Set-ItemProperty
Alias           spjb -> Stop-Job
Alias           spps -> Stop-Process
Alias           spsv -> Stop-Service
Alias           start -> Start-Process
Alias           stz -> Set-TimeZone                         3.1.0.0    Microsoft.PowerShell.Management
Alias           sujb -> Suspend-Job
Alias           sv -> Set-Variable
Alias           swmi -> Set-WmiInstance
Alias           tee -> Tee-Object
Alias           trcm -> Trace-Command
Alias           type -> Get-Content
Alias           wget -> Invoke-WebRequest
Alias           where -> Where-Object
Alias           wjb -> Wait-Job
Alias           write -> Write-Output
```

12 examples:

1)foreach

```
PS C:\Users\sesha_h2tkg8x> 30000,56978,12432 |ForEach-Object -Process{$_/1024}
29.296875
55.642578125
12.140625
```

2) mkdir lol and rmdir lol

```
PS C:\Users\sesha_h2tkg8x> mkdir Lol


    Directory: C:\Users\sesha_h2tkg8x


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        24-03-2021     22:45                Lol
```

```
PS C:\Users\sesha_h2tkg8x> rmdir Lol
```

3) Write-Output

```
PS C:\Users\sesha_h2tkg8x> Write-Output "test ouput"| Get-Member


   TypeName: System.String

Name             MemberType            Definition
----             ----------            ----------
Clone            Method                System.Object Clone(), System.Object ICloneable.Clone()
CompareTo        Method                int CompareTo(System.Object value), int CompareTo(string strB), int IComparable.CompareTo(System.Object obj), int IComparable[string].CompareTo(string other)
Contains         Method                bool Contains(string value)
CopyTo           Method                void CopyTo(int sourceIndex, char[] destination, int destinationIndex, int count)
EndsWith         Method                bool EndsWith(string value), bool EndsWith(string value, System.StringComparison comparisonType), bool EndsWith(string value, bool ignoreCase, cultureinfo culture)
Equals           Method                bool Equals(System.Object obj), bool Equals(string value), bool Equals(string value, System.StringComparison comparisonType), bool IEquatable[string].Equals(string other)
GetEnumerator    Method                System.CharEnumerator GetEnumerator(), System.Collections.IEnumerator IEnumerable.GetEnumerator(), System.Collections.Generic.IEnumerator[char] IEnumerable[char].GetEnumerator()
GetHashCode      Method                int GetHashCode()
GetType          Method                type GetType()
GetTypeCode      Method                System.TypeCode GetTypeCode(), System.TypeCode IConvertible.GetTypeCode()
IndexOf          Method                int IndexOf(char value), int IndexOf(char value, int startIndex), int IndexOf(string value), int IndexOf(string value, int startIndex), int IndexOf(string value, int startIndex, int c...
IndexOfAny       Method                int IndexOfAny(char[] anyOf), int IndexOfAny(char[] anyOf, int startIndex), int IndexOfAny(char[] anyOf, int startIndex, int count)
Insert           Method                string Insert(int startIndex, string value)
IsNormalized     Method                bool IsNormalized(), bool IsNormalized(System.Text.NormalizationForm normalizationForm)
LastIndexOf      Method                int LastIndexOf(char value), int LastIndexOf(char value, int startIndex), int LastIndexOf(string value), int LastIndexOf(string value, int startIndex), int LastIndexOf(string value, i...
LastIndexOfAny   Method                int LastIndexOfAny(char[] anyOf), int LastIndexOfAny(char[] anyOf, int startIndex), int LastIndexOfAny(char[] anyOf, int startIndex, int count)
Normalize        Method                string Normalize(), string Normalize(System.Text.NormalizationForm normalizationForm)
PadLeft          Method                string PadLeft(int totalWidth), string PadLeft(int totalWidth, char paddingChar)
PadRight         Method                string PadRight(int totalWidth), string PadRight(int totalWidth, char paddingChar)
Remove           Method                string Remove(int startIndex), string Remove(int startIndex, int count)
Replace          Method                string Replace(char oldChar, char newChar), string Replace(string oldValue, string newValue)
Split            Method                string[] Split(Params char[] separator), string[] Split(char[] separator, int count), string[] Split(char[] separator, System.StringSplitOptions options), string[] Split(char[] separa...
StartsWith       Method                bool StartsWith(string value), bool StartsWith(string value, System.StringComparison comparisonType), bool StartsWith(string value, bool ignoreCase, cultureinfo culture)
Substring        Method                string Substring(int startIndex), string Substring(int startIndex, int length)
ToBoolean        Method                bool IConvertible.ToBoolean(System.IFormatProvider provider)
ToByte           Method                byte IConvertible.ToByte(System.IFormatProvider provider)
ToChar           Method                char IConvertible.ToChar(System.IFormatProvider provider)
ToCharArray      Method                char[] ToCharArray(), char[] ToCharArray(int startIndex, int length)
ToDateTime       Method                datetime IConvertible.ToDateTime(System.IFormatProvider provider)
ToDecimal        Method                decimal IConvertible.ToDecimal(System.IFormatProvider provider)
ToDouble         Method                double IConvertible.ToDouble(System.IFormatProvider provider)
ToInt16          Method                int16 IConvertible.ToInt16(System.IFormatProvider provider)
ToInt32          Method                int IConvertible.ToInt32(System.IFormatProvider provider)
ToInt64          Method                long IConvertible.ToInt64(System.IFormatProvider provider)
ToLower          Method                string ToLower(), string ToLower(cultureinfo culture)
ToLowerInvariant Method                string ToLowerInvariant()
ToSByte          Method                sbyte IConvertible.ToSByte(System.IFormatProvider provider)
ToSingle         Method                float IConvertible.ToSingle(System.IFormatProvider provider)
ToString         Method                string ToString(), string ToString(System.IFormatProvider provider), string IConvertible.ToString(System.IFormatProvider provider)
ToType           Method                System.Object IConvertible.ToType(type conversionType, System.IFormatProvider provider)
ToUInt16         Method                uint16 IConvertible.ToUInt16(System.IFormatProvider provider)
ToUInt32         Method                uint32 IConvertible.ToUInt32(System.IFormatProvider provider)
ToUInt64         Method                uint64 IConvertible.ToUInt64(System.IFormatProvider provider)
ToUpper          Method                string ToUpper(), string ToUpper(cultureinfo culture)
ToUpperInvariant Method                string ToUpperInvariant()
Trim             Method                string Trim(Params char[] trimChars), string Trim()
TrimEnd          Method                string TrimEnd(Params char[] trimChars)
TrimStart        Method                string TrimStart(Params char[] trimChars)
Chars            ParameterizedProperty char Chars(int index) {get;}
Length           Property              int Length {get;}
```

4) Write-Output 7,8,9 | MeasureObject

```
PS C:\Users\sesha_h2tkg8x> Write-Output 7,8,9 |Measure-Object


Count     : 3
Average   :
Sum       :
Maximum   :
Minimum   :
Property  :
```

5)Get processes based on process name

```
PS C:\Users\sesha_h2tkg8x> Get-Process | Where-Object {$_.ProcessName -Match "^P.*"}

Handles  NPM(K)    PM(K)     WS(K)    CPU(s)     Id  SI ProcessName
-------  ------    -----     -----    ------     --  -- -----------
    169      11     1896      1900      0.13    4544   9 PDStyleAgent
    448      30    18788     20220            5560   0 PEFService
    650      32    61084     76648      1.91  11632   9 powershell
    232      27    27440      3944            5632   0 PresentationFontCache
    331      17     5024      7852            6172   0 ProtectedModuleHost
```

6)Get commands based on properties

```
PS C:\Users\sesha_h2tkg8x> Get-Command |Where OutputType

CommandType     Name                               Version    Source
-----------     ----                               -------    ------
Function        Format-Hex                         3.1.0.0    Microsoft.PowerShell.Utility
Function        Import-PowerShellDataFile          3.1.0.0    Microsoft.PowerShell.Utility
Function        mkdir
Function        New-Guid                           3.1.0.0    Microsoft.PowerShell.Utility
Function        New-TemporaryFile                  3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Add-Computer                       3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Add-History                        3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          Add-PSSnapin                       3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          Add-Type                           3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Clear-Variable                     3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Connect-PSSession                  3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          ConvertFrom-StringData             3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Convert-Path                       3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          ConvertTo-Csv                      3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          ConvertTo-Xml                      3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Disable-PSBreakpoint               3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Disconnect-PSSession               3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          Enable-PSBreakpoint                3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Export-Alias                       3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Export-PSSession                   3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Get-Acl                            3.0.0.0    Microsoft.PowerShell.Security
Cmdlet          Get-Alias                          3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Get-ChildItem                      3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Get-Clipboard                      3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Get-Command                        3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          Get-ComputerRestorePoint           3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Get-Content                        3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Get-ControlPanelItem               3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Get-Culture                        3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Get-Date                           3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Get-Event                          3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Get-EventLog                       3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Get-EventSubscriber                3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Get-FormatData                     3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Get-History                        3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          Get-Host                           3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Get-HotFix                         3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Get-Item                           3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Get-ItemProperty                   3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Get-Job                            3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          Get-Location                       3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Get-Member                         3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Get-Module                         3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          Get-Process                        3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Get-PSBreakpoint                   3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Get-PSCallStack                    3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Get-PSDrive                        3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Get-PSHostProcessInfo              3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          Get-PSProvider                     3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Get-PSReadLineKeyHandler           2.0.0      PSReadline
Cmdlet          Get-PSReadLineOption               2.0.0      PSReadline
Cmdlet          Get-PSSession                      3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          Get-PSSessionCapability            3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          Get-PSSessionConfiguration         3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          Get-PSSnapin                       3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          Get-Random                         3.1.0.0    Microsoft.PowerShell.Utility
```

```
Cmdlet          Get-RunspaceDebug                      3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Get-Service                            3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Get-TraceSource                        3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Get-Transaction                        3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Get-TypeData                           3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Get-UICulture                          3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Get-Variable                           3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Group-Object                           3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Import-Alias                           3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Import-Module                          3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          Import-PSSession                       3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Join-Path                              3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Measure-Command                        3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Measure-Object                         3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          New-Alias                              3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          New-Event                              3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          New-Item                               3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          New-Module                             3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          New-ModuleManifest                     3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          New-PSSession                          3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          New-PSSessionOption                    3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          New-PSTransportOption                  3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          New-Service                            3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          New-TimeSpan                           3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Out-String                             3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Push-Location                          3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Read-Host                              3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Register-EngineEvent                   3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Register-ObjectEvent                   3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Remove-Computer                        3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Remove-Job                             3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          Remove-PSSnapin                        3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          Resolve-Path                           3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Restart-Service                        3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Resume-Job                             3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          Resume-Service                         3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Select-String                          3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Select-Xml                             3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Set-Acl                                3.0.0.0    Microsoft.PowerShell.Security
Cmdlet          Set-Alias                              3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Set-Date                               3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Set-Location                           3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Set-PSBreakpoint                       3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Set-Service                            3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Set-TraceSource                        3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Set-Variable                           3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Split-Path                             3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Start-Job                              3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          Start-Process                          3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Start-Service                          3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Stop-Job                               3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          Stop-Process                           3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Stop-Service                           3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Suspend-Job                            3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          Suspend-Service                        3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Test-ComputerSecureChannel             3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Test-Connection                        3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Test-ModuleManifest                    3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          Test-Path                              3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Test-PSSessionConfigurationFile        3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          Wait-Event                             3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Wait-Job                               3.0.0.0    Microsoft.PowerShell.Core
```

7)LOCATION

```
PS C:\Users\sesha_h2tkg8x> pwd

Path
----
C:\Users\sesha_h2tkg8x
```

8)HISTORY

```
Id CommandLine
-- -----------
 1 PING WWW.GOOGLE.COM
 2 IPCONFIG
 3 LS
 4 Get-Alias
 5 30000,56978,12432 |ForEach-Object -Process{$_/1024}
 6 mkdir Lol
 7 rmdir Lol
 8 Write-Output "test ouput"| Get-Memeber
 9 Write-Output "test ouput"| Get-Member
10 Write-Output 7,8,9 |Measure-Object
11 Get-Process | Where-Object {$_ProcessName -Match "^P.*"}
12 Get-Process | Where-Object {$_.ProcessName -Match "^P.*"}
13 Get-Command |Where OutputType
14 pwd
15 h
```

9) Get-Variable

```
PS C:\Users\sesha_h2tkg8x> gv

Name                            Value
----                            -----
$                               pwd
?                               True
^                               pwd
args                            {}
ConfirmPreference               High
ConsoleFileName
DebugPreference                 SilentlyContinue
Error                           {}
ErrorActionPreference           Continue
ErrorView                       NormalView
ExecutionContext                System.Management.Automation.EngineIntrinsics
false                           False
FormatEnumerationLimit          4
HOME                            C:\Users\sesha_h2tkg8x
Host                            System.Management.Automation.Internal.Host.InternalHost
InformationPreference           SilentlyContinue
input                           System.Collections.ArrayList+ArrayListEnumeratorSimple
Matches                         {0}
MaximumAliasCount               4096
MaximumDriveCount               4096
MaximumErrorCount               256
MaximumFunctionCount            4096
MaximumHistoryCount             4096
MaximumVariableCount            4096
MyInvocation                    System.Management.Automation.InvocationInfo
NestedPromptLevel               0
null
OutputEncoding                  System.Text.ASCIIEncoding
PID                             11632
PROFILE                         C:\Users\sesha_h2tkg8x\Documents\WindowsPowerShell\Microsoft.PowerShell_profile.ps1
ProgressPreference              Continue
PSBoundParameters               {}
PSCommandPath
PSCulture                       en-IN
PSDefaultParameterValues        {}
PSEdition                       Desktop
PSEmailServer
PSHOME                          C:\Windows\System32\WindowsPowerShell\v1.0
PSScriptRoot
PSSessionApplicationName        wsman
PSSessionConfigurationName      http://schemas.microsoft.com/powershell/Microsoft.PowerShell
PSSessionOption                 System.Management.Automation.Remoting.PSSessionOption
PSUICulture                     en-US
PSVersionTable                  {PSVersion, PSEdition, PSCompatibleVersions, BuildVersion...}
PWD                             C:\Users\sesha_h2tkg8x
ShellId                         Microsoft.PowerShell
StackTrace
true                            True
VerbosePreference               SilentlyContinue
WarningPreference               Continue
WhatIfPreference                False
```

10) Get-Module-gmo

```
PS C:\Users\sesha_h2tkg8x> gmo

ModuleType Version   Name                          ExportedCommands
---------- -------   ----                          ----------------
Manifest   3.1.0.0   Microsoft.PowerShell.Management {Add-Computer, Add-Content, Checkpoint-Computer, Clear-Content...}
Manifest   3.0.0.0   Microsoft.PowerShell.Security   {ConvertFrom-SecureString, ConvertTo-SecureString, Get-Acl, Get-AuthenticodeSignature...}
Manifest   3.1.0.0   Microsoft.PowerShell.Utility    {Add-Member, Add-Type, Clear-Variable, Compare-Object...}
Script     2.0.0     PSReadline                      {Get-PSReadLineKeyHandler, Get-PSReadLineOption, Remove-PSReadLineKeyHandler, Set-PSReadLineKeyHandler...}
```

11)python version and java version

```
PS C:\Users\sesha_h2tkg8x> python --version
Python 3.8.3
PS C:\Users\sesha_h2tkg8x> java --version
java 13.0.1 2019-10-15
Java(TM) SE Runtime Environment (build 13.0.1+9)
Java HotSpot(TM) 64-Bit Server VM (build 13.0.1+9, mixed mode, sharing)
PS C:\Users\sesha_h2tkg8x>
```

12) Get-ProcessGps

```
PS C:\Users\sesha_h2tkg8x> gps

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)      Id  SI ProcessName
-------  ------    -----      -----     ------      --  -- -----------
    170       9     2628       3788               4868   0 AdminService
    151      11     2208       1812      0.17    20632   9 amdow
   5405      39   171924      14136      3.22    16736   9 AMDRSServ
    832      47    45772      48004      4.98    14612   9 ApplicationFrameHost
    150       8     1580       6556              17532   0 AppVShNotify
    333      18     4348      16144               5368   0 armsvc
    329      13     2600      11376              18388   9 atieclxx
    184       9     1852       2572               2356   0 atiesrxx
    207      12     2800      10572      0.64    24812   9 atiw
    709      28    29792      36732     31.56     8780   0 audiodg
    242      16     4356      17352      0.20    24096   9 backgroundTaskHost
    573      28    18064       1584      0.41    18980   9 Calculator
   1267      27   159588     148004    100.67     3152   9 chrome
    301      19    18408      38608     21.67     5204   9 chrome
    233      15    70596      96100     19.66     8496   9 chrome
    277      17     7332      18748      1.20    10672   9 chrome
   1606      56   119352     176832    194.34    13056   9 chrome
    186      15    20492      36028      9.83    14784   9 chrome
    209      14    11844      23228      0.14    15464   9 chrome
    209      13     8600      16728      1.08    18052   9 chrome
    224      15    14156      37596      0.89    19136   9 chrome
    272      18    43796      89008     80.89    21468   9 chrome
    234      16    17804      38536      1.11    22324   9 chrome
    193       9     2076       7100      0.22    22816   9 chrome
    223      14    13012      28008      0.47    24804   9 chrome
    142       7     1808       8468      0.17    20084   9 CompPkgSrv
     97       7     6244       2364               6388   0 conhost
    277      14     6636      18616      2.47    12660   9 conhost
    100       7     6348       5804      0.03    21400   9 conhost
    590      31    17660      33240      1.84    25588   9 CredentialUIBroker
   1012      30     2116       3120                888   0 csrss
    848      28     2568       6800              15748   9 csrss
    506      18    51588      52512     78.05    12132   9 ctfmon
    468      21    11768      16116               2964   0 dasHost
    173       9     2068       2668              15412   0 DDVCollectorSvcApi
    408      25    26440      15832              14124   0 DDVDataCollector
    280      18     6552       6956              12060   0 DDVRulesProcessor
    689      41    35876      28620              17228   0 DeliveryService
    886      43    58620      31672              14376   0 DellSupportAssistRemedationService
    213      19     4576       7200               2372   0 dllhost
    121       8     1496       7496      0.09    14856   9 dllhost
    246      15     3700      12292      0.59    23544   9 dllhost
     53       6     1376       4260      0.58     5088   9 dptf_helper
   1734      72   595804      93836              18380   9 dwm
    128       8     1836       3216               4896   0 esif_uf
   4305    1367   127688     140844    288.38    23568   9 explorer
    122       8     1616       7128              13892   0 fodhelper
     39       6     1904       1172               1180   0 fontdrvhost
     39       8     4460       8688              20252   9 fontdrvhost
    467      23    13216      29280      1.94    18636   9 GameBar
    171      10     1600        300              11984   0 GoogleCrashHandler
    154       9     1656        320              18240   0 GoogleCrashHandler64
    866      35    21856       2144      0.78    10168   9 HxCalendarAppImm
    831      40    38608       1628      1.45     5452   9 HxOutlook
    705      29    13012      19400      3.95    11284   9 HxTsr
    436      32   107196      81796              16792   0 IAStorDataMgrSvc
```

Cmdlets

Get-WmiObject -Class Win32_Process

```
OSCreationClassName      : Win32_OperatingSystem
OSName                   : Microsoft Windows 10 Home Single Language|C:\WINDOWS|\Device\Harddisk0\Partition3
OtherOperationCount      : 56
OtherTransferCount       : 1270
PageFaults               : 3401
PageFileUsage            : 1808
ParentProcessId          : 824
PeakPageFileUsage        : 2056
PeakVirtualSize          : 2203424518144
PeakWorkingSetSize       : 11404
Priority                 : 8
PrivatePageCount         : 1851392
ProcessId                : 12412
QuotaNonPagedPoolUsage   : 9
QuotaPagedPoolUsage      : 121
QuotaPeakNonPagedPoolUsage : 10
QuotaPeakPagedPoolUsage  : 123
ReadOperationCount       : 0
ReadTransferCount        : 0
SessionId                : 9
Status                   :
TerminationDate          :
ThreadCount              : 3
UserModeTime             : 312500
VirtualSize              : 2203419799552
WindowsVersion           : 10.0.19042
WorkingSetSize           : 11190272
WriteOperationCount      : 0
WriteTransferCount       : 0
PSComputerName           : PRANAV
ProcessName              : svchost.exe
Handles                  : 138
VM                       : 2203419799552
WS                       : 11190272
Path                     : C:\WINDOWS\system32\svchost.exe


__GENUS                  : 2
__CLASS                  : Win32_Process
__SUPERCLASS             : CIM_Process
__DYNASTY                : CIM_ManagedSystemElement
__RELPATH                : Win32_Process.Handle="22000"
__PROPERTY_COUNT         : 45
__DERIVATION             : {CIM_Process, CIM_LogicalElement, CIM_ManagedSystemElement}
__SERVER                 : PRANAV
__NAMESPACE              : root\cimv2
__PATH                   : \\PRANAV\root\cimv2:Win32_Process.Handle="22000"
Caption                  : rundll32.exe
CommandLine              : "C:\WINDOWS\system32\rundll32.exe" -localserver 22d8c27b-47a1-48d1-ad08-7da7abd79617
CreationClassName        : Win32_Process
CreationDate             : 20210324095542.872544+330
CSCreationClassName      : Win32_ComputerSystem
CSName                   : PRANAV
Description              : rundll32.exe
ExecutablePath           : C:\WINDOWS\system32\rundll32.exe
ExecutionState           :
Handle                   : 22000
HandleCount              : 145
InstallDate              :
KernelModeTime           : 625000
MaximumWorkingSetSize    : 1380
MinimumWorkingSetSize    : 200
Name                     : rundll32.exe
```

Get-Service -by NAME EG-WIN Get-Service -Name "win*" -Exclude "WinRM"

```
PS C:\Users\sesha_h2tkg8x> Get-Service -Name "win*" -Exclude  "WinRm"

Status    Name              DisplayName
------    ----              -----------
Running   WinDefend         Microsoft Defender Antivirus Service
Running   WinHttpAutoProx... WinHTTP Web Proxy Auto-Discovery Se...
Running   Winmgmt           Windows Management Instrumentation
```

Piping Get-process | select ProcessName, ID | Sort ProcessName | FL

```
PS C:\Users\sesha_h2tkg8x> Get-process |SELECT ProcessName,ID|Sort FL

ProcessName                    Id
-----------                    --
svchost                        4328
svchost                        4340
svchost                        4144
svchost                        4160
svchost                        4616
svchost                        4712
svchost                        4452
svchost                        4516
svchost                        3552
svchost                        3584
svchost                        3464
svchost                        3500
svchost                        3824
svchost                        4008
svchost                        3664
svchost                        3744
svchost                        4904
svchost                        5448
svchost                        5760
svchost                        5152
svchost                        5228
svchost                        7580
svchost                        7784
svchost                        6068
svchost                        6092
svchost                        4936
svchost                        4944
svchost                        4912
svchost                        4920
svchost                        4968
svchost                        4980
svchost                        4952
svchost                        4960
svchost                        1920
svchost                        1976
svchost                        1816
svchost                        1912
svchost                        2164
svchost                        2256
svchost                        2056
svchost                        2148
svchost                        1616
svchost                        1672
svchost                        1332
svchost                        1608
svchost                        1740
svchost                        1792
svchost                        1680
svchost                        1700
svchost                        2364
svchost                        2932
svchost                        3008
svchost                        2868
svchost                        2916
svchost                        3316
svchost                        3456
svchost                        3176
```

Script Security Settings

Get-ExecutionPolicy

```
PS C:\Users\sesha_h2tkg8x> Get-ExecutionPolicy
Restricted
```

Examples

- **Pull computer serial number**

```
PS C:\Users\sesha_h2tkg8x> Gwmi  Win32_Bios |select SerialNumber

SerialNumber
------------
CWFTXR2
```

- **Gather Logical Disk Space information**

```
PS C:\Users\sesha_h2tkg8x> Gwmi Win32_LogicalDisk


DeviceID       : C:
DriveType      : 3
ProviderName   :
FreeSpace      : 974179422208
Size           : 1191833497600
VolumeName     : Local Disk C

DeviceID       : E:
DriveType      : 3
ProviderName   :
FreeSpace      : 435854610432
Size           : 524286947328
VolumeName     : local disk e

DeviceID       : F:
DriveType      : 3
ProviderName   :
FreeSpace      : 247637991424
Size           : 268434403328
VolumeName     : local disk f
```

- **Show running processes**

```
OSCreationClassName          : Win32_OperatingSystem
OSName                       : Microsoft Windows 10 Home Single Language|C:\WINDOWS|\Device\Harddisk0\Partition3
OtherOperationCount          : 725
OtherTransferCount           : 10680
PageFaults                   : 18681
PageFileUsage                : 18064
ParentProcessId              : 1124
PeakPageFileUsage            : 20420
PeakVirtualSize              : 4728102912
PeakWorkingSetSize           : 64832
Priority                     : 8
PrivatePageCount             : 18497536
ProcessId                    : 18980
QuotaNonPagedPoolUsage       : 28
QuotaPagedPoolUsage          : 714
QuotaPeakNonPagedPoolUsage   : 29
QuotaPeakPagedPoolUsage      : 727
ReadOperationCount           : 2
ReadTransferCount            : 8192
SessionId                    : 9
Status                       :
TerminationDate              :
ThreadCount                  : 21
UserModeTime                 : 2031250
VirtualSize                  : 4723908608
WindowsVersion               : 10.0.19042
WorkingSetSize               : 1622016
WriteOperationCount          : 0
WriteTransferCount           : 0
PSComputerName               : PRANAV
ProcessName                  : Calculator.exe
Handles                      : 573
VM                           : 4723908608
WS                           : 1622016
Path                         : C:\Program Files\WindowsApps\Microsoft.WindowsCalculator_10.1906.55.0_x64__8wekyb3d8bbwe\Calculator.exe

 GENUS                       : 2
```

• Show Network Adapters

```
PS C:\Users\sesha_h2tkg8x> $NIC =Get-WMIObject Win32_NetworkAdapterConfiguration |where{$_.IPEnabled -eq "TRUE"}
PS C:\Users\sesha_h2tkg8x> $NIC


DHCPEnabled        : True
IPAddress          : {192.168.26.1, fe80::f070:450d:7e45:1644}
DefaultIPGateway :
DNSDomain          :
ServiceName        : VMnetAdapter
Description        : VMware Virtual Ethernet Adapter for VMnet8
Index              : 1

DHCPEnabled        : True
IPAddress          : {192.168.146.1, fe80::c22:b0ed:262:e143}
DefaultIPGateway :
DNSDomain          :
ServiceName        : VMnetAdapter
Description        : VMware Virtual Ethernet Adapter for VMnet1
Index              : 2

DHCPEnabled        : True
IPAddress          : {192.168.225.50, fe80::1d5e:a1cf:cd2b:45aa, 2409:4070:4604:f0b1:b056:33df:ee36:5bf8, 2409:4070:4604:f0b1:1d5e:a1cf:cd2b:45aa}
DefaultIPGateway : {192.168.225.1, fe80::bc5f:a436:2499:8125, fe80::dc43:88ff:fecd:2261}
DNSDomain          :
ServiceName        : Qcamain10x64
Description        : Qualcomm QCA9377 802.11ac Wireless Adapter #2
Index              : 4
```

• Process

```
Windows PowerShell

PS C:\Users\sesha_h2tkg8x> Get-Process |Where {$_.handles -gt 500} |Sort handles |Format-Table

Handles  NPM(K)    PM(K)     WS(K)    CPU(s)     Id  SI ProcessName
-------  ------    -----     -----    ------     --  -- -----------
    501      40    15980     45816      0.53  23032   9 backgroundTaskHost
    508      18    55912     56024     84.17  12132   9 ctfmon
    516      70    16408     26384            13132   0 svchost
    518     192   486716    389040  1,815.92   5468   9 Teams
    528      11     4120      4808             2532   0 svchost
    542      30    20788     35080     48.91  24036   9 ModuleCoreService
    547      26    11012     32228     16.83  14624   9 SystemSettingsBroker
    549      23    14408     20816             8276   0 McCSPServiceHost
    558      22     7828     14684             4340   0 svchost
    558      24   231328     52540             5392   0 SmartByteNetworkService
    568      26     7576     26428      2.84  24024   9 igfxEM
    573      28    18064      1584      0.41  18980   9 Calculator
    576      25     7040     33316      8.86   6776   9 RuntimeBroker
    579      23    14092     22256     10.06   3684   9 TextInputHost
    590      26    27952     32916             4904   0 svchost
    590      31    17660     33244      1.88  25588   9 CredentialUIBroker
    595      33    11836     14228            18044   0 svchost
    639      33    28392     76476      8.58   6780   9 StartMenuExperienceHost
    651      36    21224     21456             7280   0 servicehost
    669      38    15076     43336      6.33  23276   9 McUICnt
    671      29    11464     39856     12.11  22224   9 RuntimeBroker
    684      28   235012    140768            11732   0 MoUsoCoreWorker
    691      40    35732     29112            17228   0 DeliveryService
    699      13     6536      9396             8552   0 svchost
    705      29    13012     11720      3.95  11284   9 HxTsr
    711      28   376460    306120    314.66   8516   0 mcshield
    728      15     6480     12816             3664   0 svchost
    733      75   317000     34996             5580   0 MsMpEng
    738      35    66844     86292     11.20  11632   9 powershell
    740      34    30740     38424     56.58   8780   0 audiodg
    761      18     6832      9372            12372   0 SecurityHealthService
    763      34     9224     34824      4.11  18168   9 svchost
    779      11     3948      9068             2256   0 svchost
    821      29    45136     53976            11636   0 OfficeClickToRun
    831      40    38608      1628      1.45   5452   9 HxOutlook
    832      47    45772     47916      5.02  14612   9 ApplicationFrameHost
    838      47    27608      7300      1.42  15916   9 YourPhone
    839      15    11324     21468             1976   0 svchost
    851      28     2568      6776            15748   9 csrss
    862      25    22788     43332     28.91  23616   9 sihost
    866      35    21856      2144      0.78  10168   9 HxCalendarAppImm
    868      22     8244      9916             5292   0 ModuleCoreService
    878      63    49916     23324     42.02  16088   9 WWAHost
    889      43    57516     29980            14376   0 DellSupportAssistRemedationService
    906      41    24636      1588      0.89    908   9 SystemSettings
    910      39    37624     40004     23.16  21176   9 ShellExperienceHost
    921      13     8976      9872              824   0 services
    934      69    47868      2272      1.73  23028   9 WinStore.App
    990      93   597980     73676            15972   0 SupportAssistAgent
    996      20    42544     19496             1616   0 svchost
   1010      41    15288     35840      5.38  11452   9 RuntimeBroker
   1011      30     2120      3112              888   0 csrss
   1024      59    72552     67984             4296   0 ModuleCoreService
   1099      37    58264     46584             6692   0 MfeAVSvc
   1157      29    11556     45868     28.80   8388   9 svchost
   1179      77    56012     63052             1544   0 SearchIndexer
   1181     893   177032    111436    407.55  13768   9 Teams
```

- **Find the processes in the memory**

```
PS C:\Users\sesha_h2tkg8x> Ps

Handles  NPM(K)    PM(K)     WS(K)    CPU(s)     Id  SI ProcessName
-------  ------    -----     -----    ------     --  -- -----------
    170       9     2628      3784               4868   0 AdminService
    151      11     2208      1812     0.17     20632   9 amdow
   5405      39   171924     14136     3.25     16736   9 AMDRSServ
    832      47    45772     47916     5.02     14612   9 ApplicationFrameHost
    150       8     1580      6560              17532   0 AppVShNotify
    333      18     4348     16140               5368   0 armsvc
    340      13     2600     11380              18388   9 atieclxx
    184       9     1852      2572               2356   0 atiesrxx
    207      12     2800     10452     0.64     24812   9 atiw
    283      26    12216     19208    57.36      8780   0 audiodg
    240      16     4244     17340     0.09     22624   9 backgroundTaskHost
    501      40    15980     44720     0.53     23032   9 backgroundTaskHost
    573      28    18064      1584     0.41     18980   9 Calculator
   1267      27   172888    160640   108.77      3152   9 chrome
    305      19    18644     38664    22.08      5204   9 chrome
    234      15    74848    101356    22.09      8496   9 chrome
    277      17     7332     18744     1.20     10672   9 chrome
   1607      56   134072    191904   208.09     13056   9 chrome
    186      16    22584     38024    11.83     14784   9 chrome
    209      14    11836     23220     0.16     15464   9 chrome
    212      13     8320     16468     1.08     18052   9 chrome
    224      15    14216     37376     1.06     19136   9 chrome
    272      18    43956     89240   105.75     21468   9 chrome
    234      16    17112     37316     1.13     22324   9 chrome
    193       9     2076      7100     0.25     22816   9 chrome
    223      14    13012     27896     0.48     24804   9 chrome
    142       7     1808      8468     0.17     20084   9 CompPkgSrv
     97       7     6244      2364               6388   0 conhost
    279      14     6320     18868    18.45     12660   9 conhost
    100       7     6348      5804     0.03     21400   9 conhost
    590      31    17660     33244     1.88     25588   9 CredentialUIBroker
   1008      30     2120      3108                888   0 csrss
    860      28     2568      6784              15748   9 csrss
    508      18    56244     56360    84.59     12132   9 ctfmon
    456      21    11700     15976               2964   0 dasHost
    173       9     2068      2664              15412   0 DDVCollectorSvcApi
    408      25    26440     15848              14124   0 DDVDataCollector
    280      18     6552      6956              12060   0 DDVRulesProcessor
    691      40    35732     29112              17228   0 DeliveryService
    889      43    57516     29980              14376   0 DellSupportAssistRemedationService
    213      19     4576      7200               2372   0 dllhost
    121       8     1496      7360     0.09     14856   9 dllhost
    248      15     3708     12308     0.67     23544   9 dllhost
     53       6     1376      4260     0.58      5088   9 dptf_helper
   1734      72   599124     90104              18380   9 dwm
    128       8     1836      3216               4896   0 esif_uf
   4341    1387   128256    139212   301.05     23568   9 explorer
    122       8     1616      7128              13892   0 fodhelper
     39       6     1904      1168               1180   0 fontdrvhost
     39       8     4432      8620              20252   9 fontdrvhost
    465      23    13212     29248     1.94     18636   9 GameBar
    171      11     1736      1384              11984   0 GoogleCrashHandler
    154       9     1656       320              18240   0 GoogleCrashHandler64
    866      35    21856      2144     0.78     10168   9 HxCalendarAppImm
    831      40    38608      1628     1.45      5452   9 HxOutlook
    705      29    13012     11720     3.95     11284   9 HxTsr
    436      32   107156     81780              16792   0 IAStorDataMgrSvc
```

• BIOS

```
PS C:\Users\sesha_h2tkg8x> Get-WmiObject  -Class Win32_BIOS -ComputerName .


SMBIOSBIOSVersion : 1.3.1
Manufacturer      : Dell Inc.
Name              : 1.3.1
SerialNumber      : CWFTXR2
Version           : DELL   - 1072009
```

• Current User

```
PS C:\Users\sesha_h2tkg8x> whoami
pranav\sesha_h2tkg8x
```

Get information about the make and model of a computer

```
PS C:\Users\sesha_h2tkg8x> Get-WmiObject -Class Win32_ComputerSystem


Domain              : WORKGROUP
Manufacturer        : Dell Inc.
Model               : Inspiron 5570
Name                : PRANAV
PrimaryOwnerName    :
TotalPhysicalMemory : 8482582528
```

• Get information about the Installed applications


```
Windows PowerShell
PS C:\Users\sesha_h2tkg8x> Get-WmiObject -Class Win32_Product -ComputerName. |Format-Wide -column 1


Python 3.8.3 Core Interpreter (64-bit)
Python 3.8.3 pip Bootstrap (64-bit)
Python 3.8.3 Add to Path (64-bit)
Python 3.8.3 Development Libraries (64-bit)
Python 3.8.3 Test Suite (64-bit)
Python 3.8.3 Executables (64-bit)
Python 3.8.3 Standard Library (64-bit)
GoTo Opener
Python 3.8.3 Utility Scripts (64-bit)
Python 3.8.3 Tcl/Tk Support (64-bit)
Intel(R) Wireless Bluetooth(R)
Office 16 Click-to-Run Extensibility Component
Office 16 Click-to-Run Localization Component
Office 16 Click-to-Run Licensing Component
Splashtop Wired XDisplay Agent
EFH
VMware Player
Microsoft Visual C++ 2005 Redistributable (x64)
Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005
Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005
Oracle Database 11g Express Edition
Dell SupportAssist Remediation
Intel(R) Management Engine Components
Dell Update - SupportAssist Update Plugin
Microsoft Visual C++ 2019 X64 Additional Runtime - 14.24.28127
Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.40660
Dell Update for Windows 10
Dell SupportAssist

Intel(R) Trusted Connect Service Client x86
Intel(R) Trusted Connect Service Client x64
Intel(R) ME UninstallLegacy
Intel(R) Rapid Storage Technology
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161
Adobe Acrobat Reader DC
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.24.28127
Qualcomm Atheros Setup
Microsoft Visual C++ 2012 x64 Additional Runtime - 11.0.61030
Dell Mobile Connect Drivers
AMD Settings
Microsoft Visual C++ 2005 Redistributable (x64)
Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.24.28127
Dell Power Manager Service
AMD Settings
Intel(R) Chipset Device Software

Node.js
Microsoft VC++ redistributables repacked.
Free Cam 8
SmartByte Drivers and Services
Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.61030
Microsoft Visual C++ 2005 Redistributable
Microsoft Visual C++ 2012 x64 Minimum Runtime - 11.0.61030
Network Recording Player
Intel© Optane™ Pinning Explorer Extensions
Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.40660
Intel© Hardware Accelerated Execution Manager
Microsoft VC++ redistributables repacked.
Microsoft Visual C++ 2012 x86 Minimum Runtime - 11.0.61030
```

With format wide =3 col


```
PS C:\Users\sesha_h2tkg8x> Get-WmiObject -Class Win32_Product -ComputerName. |Format-Wide -column 3

Python 3.8.3 Core Interpreter (64-bit)        Python 3.8.3 pip Bootstrap (64-bit)              Python 3.8.3 Add to Path (64-bit)
Python 3.8.3 Development Libraries (64-bit)    Python 3.8.3 Test Suite (64-bit)                 Python 3.8.3 Executables (64-bit)
Python 3.8.3 Standard Library (64-bit)        GoTo Opener                                      Python 3.8.3 Utility Scripts (64-bit)
Python 3.8.3 Tcl/Tk Support (64-bit)          Intel(R) Wireless Bluetooth(R)                   Office 16 Click-to-Run Extensibility Component
Office 16 Click-to-Run Localization Component Office 16 Click-to-Run Licensing Component       Splashtop Wired XDisplay Agent
EFH                                           VMware Player                                    Microsoft Visual C++ 2005 Redistributable (x64)
Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005   Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005   Oracle Database 11g Express Edition
Dell SupportAssist Remediation                Intel(R) Management Engine Components            Dell Update - SupportAssist Update Plugin
Microsoft Visual C++ 2019 X64 Additional Runtime - 14.24.28127   Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.40660   Dell Update for Windows 10
Dell SupportAssist                                                                             Intel(R) Trusted Connect Service Client x86
Intel(R) Trusted Connect Service Client x64   Intel(R) ME UninstallLegacy                      Intel(R) Rapid Storage Technology
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161   Adobe Acrobat Reader DC                         Microsoft Visual C++ 2019 X86 Additional Runtime - 14.24.28127
Qualcomm Atheros Setup                        Microsoft Visual C++ 2012 x64 Additional Runtime - 11.0.61030   Dell Mobile Connect Drivers
AMD Settings                                  Microsoft Visual C++ 2005 Redistributable (x64)   Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.24.28127
Dell Power Manager Service                    AMD Settings                                     Intel(R) Chipset Device Software
                                              Node.js                                          Microsoft VC++ redistributables repacked.
Free Cam 8                                    SmartByte Drivers and Services                   Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.61030
Microsoft Visual C++ 2005 Redistributable     Microsoft Visual C++ 2012 x64 Minimum Runtime - 11.0.61030   Network Recording Player
Intel© Optane™ Pinning Explorer Extensions    Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.40660   Intel© Hardware Accelerated Execution Manager
Microsoft VC++ redistributables repacked.     Microsoft Visual C++ 2012 x86 Minimum Runtime - 11.0.61030   Intel(R) Management Engine Driver
Dell Digital Delivery Service                 Microsoft Update Health Tools                    Python Launcher
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.17   Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.24.28127   AMD WVR64
Intel(R) Management Engine Components         Java(TM) SE Development Kit 13.0.1 (64-bit)
```

• Find the five processes using the most memory

```
PS C:\Users\sesha_h2tkg8x> Get-Process |Sort-Object -Descending WS|select -first 5| select -ExpandProperty ProcessName
Memory Compression
WhatsApp
Teams
WhatsApp
mcshield
```