SECURE CODING LAB-6

NISHANK VERMA
SLOT-L39+L40

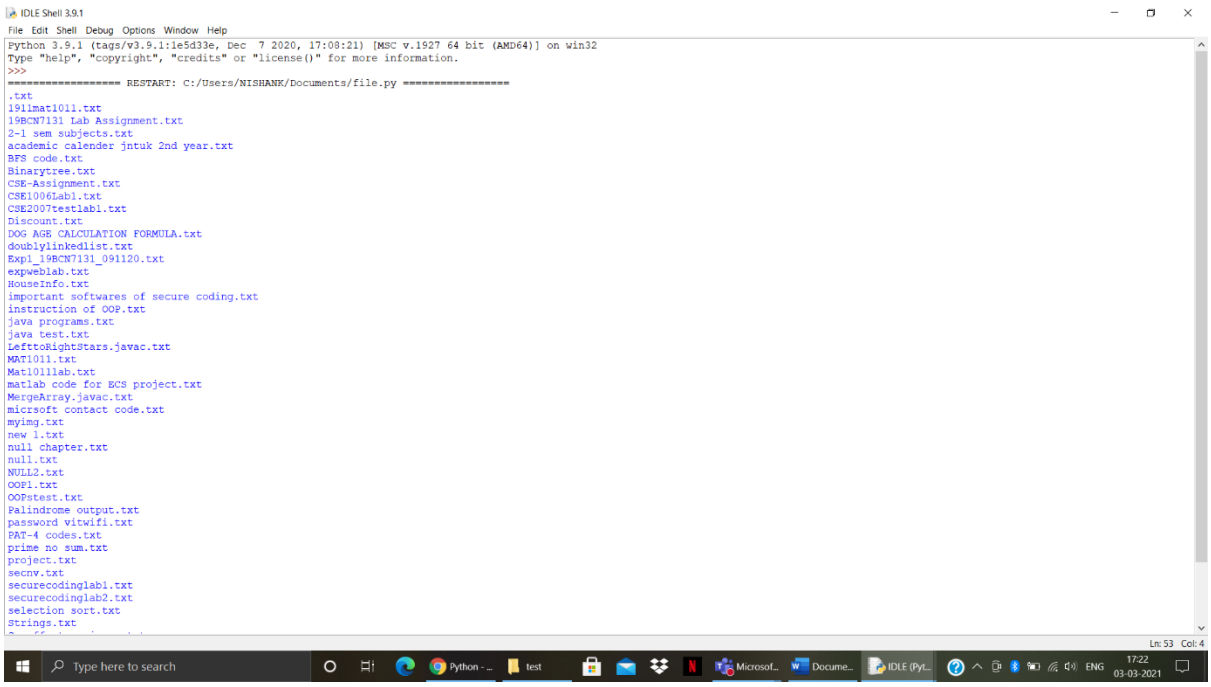
19BCN7131

POWER SHELL AND AUTOMATION

Assignment:

1)Write a python script to get all the file names in the current directory

```
import os


for x in os.listdir():
    if x.endswith(".txt"):
        print(x)
```

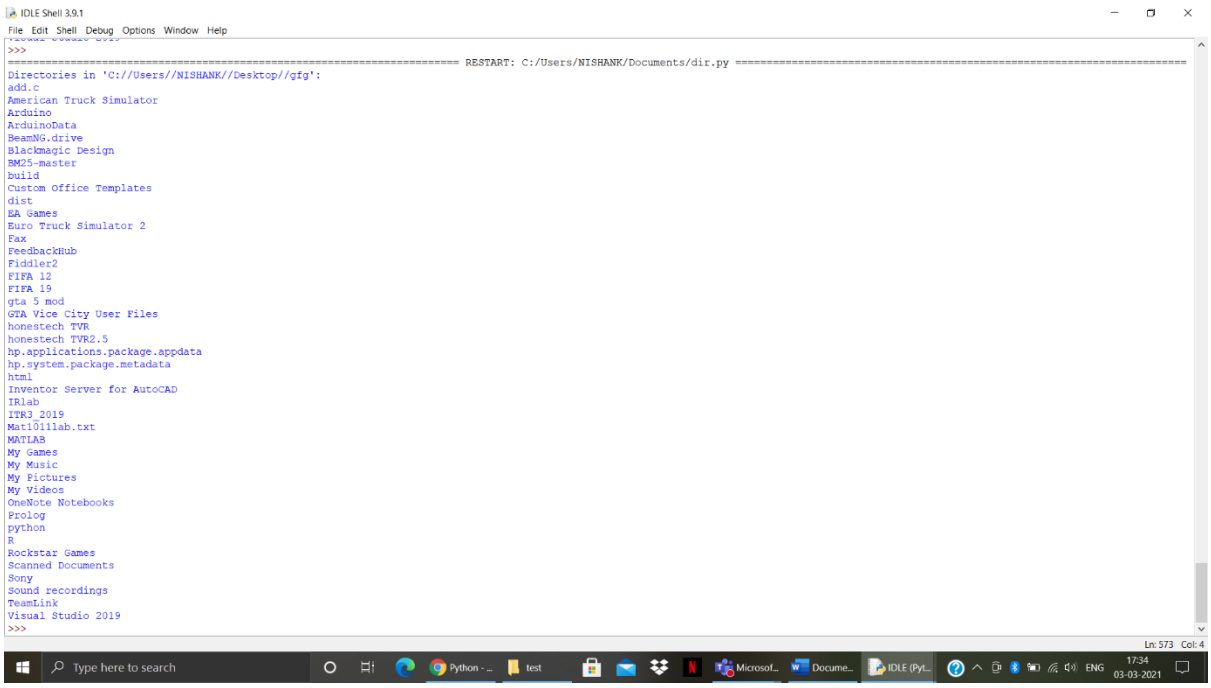


2)Write a python script to get all the directory names in the current directory

```
import os


for x in os.listdir():
    print(x)
```

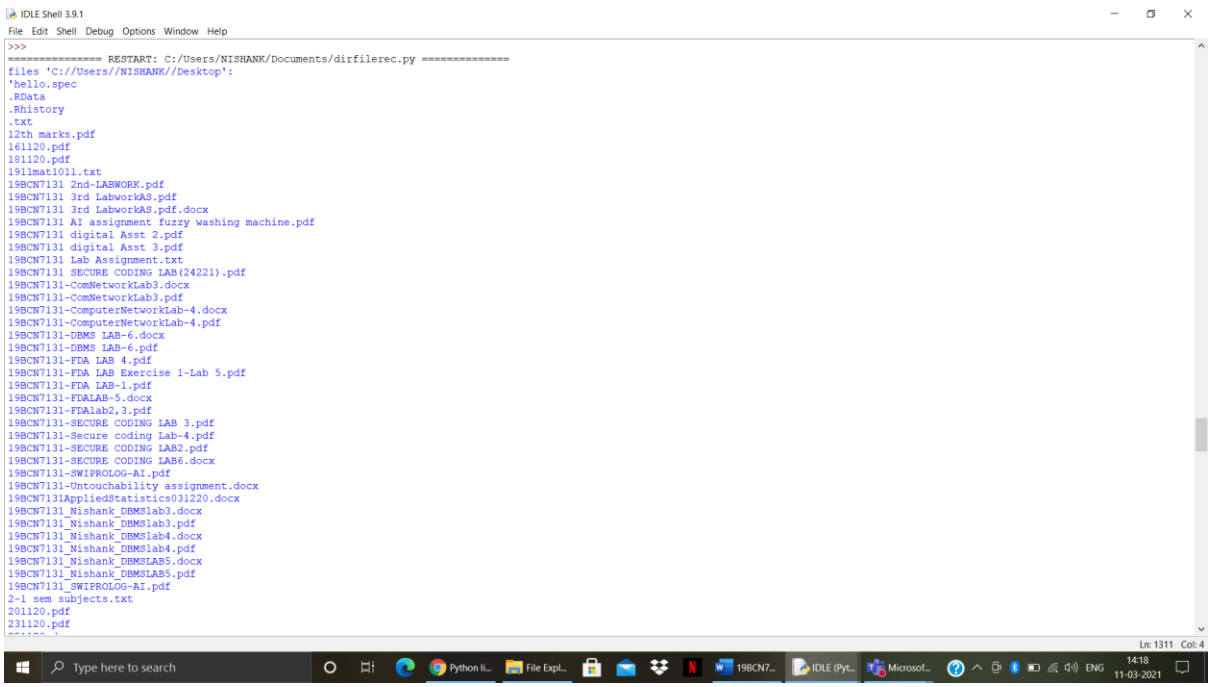
3)Write a python script to get all the directory and subdirectory names in the current directory

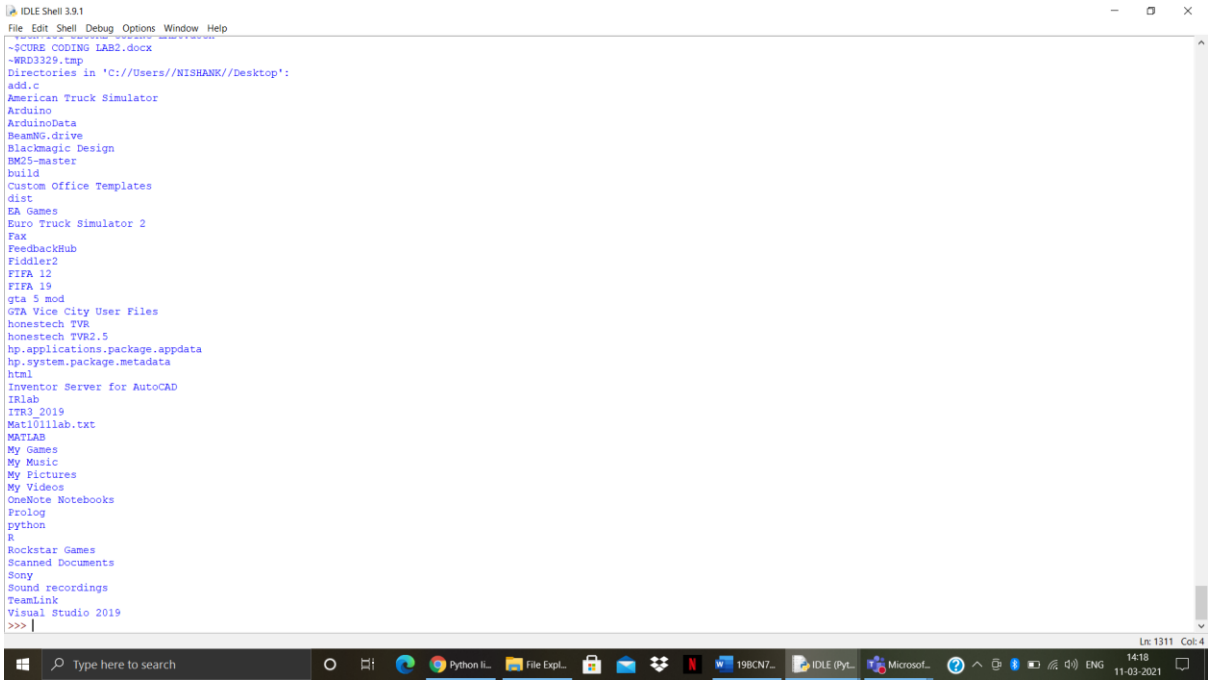
```
import os
path="C://Users//NISHANK//Desktop//gfg"
obj = os.scandir()
print("Directories in '% s':" % path)
for entry in obj:
    if entry.is_dir():
        print(entry.name)
```



4) Write a python script to get all the file name, directory and all the subdirectory names (recursively) in the current directory

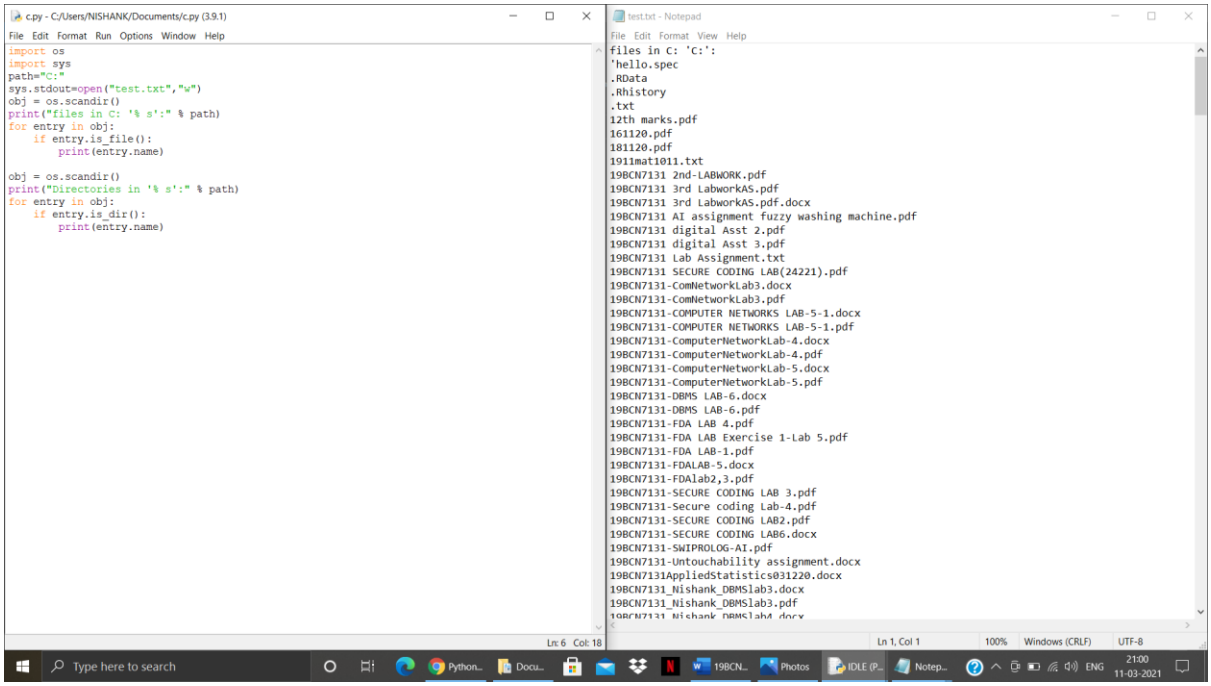
```
import os

path="C://Users//NISHANK//Desktop"

obj = os.scandir()

print("files '% s':" % path)

for entry in obj:

    if entry.is_file():

        print(entry.name)


obj = os.scandir()

print("Directories in '% s':" % path)

for entry in obj:

    if entry.is_dir():

        print(entry.name)
```



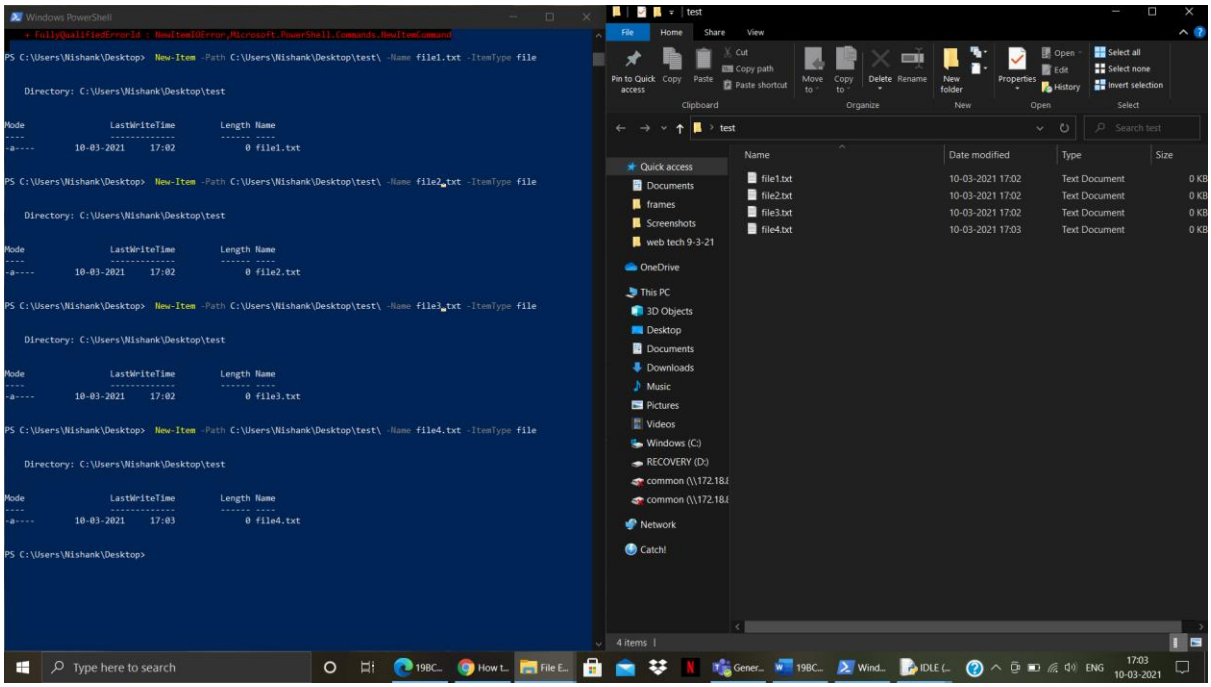


5)Write a python script to get all the file name, directory and all the subdirectory names (recursively) in the current drive and write it to a text file.

```
import os

import sys

path="C:"

sys.stdout=open("test.txt","w")

obj = os.scandir()

print("files in C: '% s':" % path)

for entry in obj:

    if entry.is_file():

        print(entry.name)


obj = os.scandir()

print("Directories in '% s':" % path)

for entry in obj:

    if entry.is_dir():

        print(entry.name)
```



6)Write a python script which creates four new files in the current directory using Powershell.



Get-Alias will list the preloaded Alias's and will show you what Cmdiet they are mapped to

PS C:\Users\NISHANK> 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	gci -> Get-ChildItem		
Alias	gcm -> Get-Command		
Alias	gcs -> Get-PSCallStack		
Alias	gdr -> Get-PSDrive		
Alias	ghy -> Get-History		
Alias	gi -> Get-Item		
Alias	gjb -> Get-Job		
Alias	gl -> Get-Location		
Alias	gm -> Get-Member		
Alias	gmo -> Get-Module		
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	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

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 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       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
```

Get-Process command

```
PS C:\Users\NISHANK> Get-Process

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)      Id  SI ProcessName
-------  ------    -----      -----     ------      --  -- -----------
    285      18     7364      24608       2.63    3720   1 ApplicationFrameHost
    386      22    17536      20000     328.05    9904   0 audiodg
     97       7     6220       4352                4060   0 conhost
     97       7     6348        116       0.03    5840   1 conhost
    275      14     4736      17192       2.75    6452   1 conhost
    711      51    28648      57260       1.08   11044   1 Cortana
    813      25     1956       5200                 728   0 csrss
    743      19     2768       6868                 840   1 csrss
    571      18    30300      24524      74.14    7756   1 ctfmon
    329      15     3636       8520                4936   0 dasHost
    307      16     4132      12968                8392   0 DiscSoftBusServiceLite
    203      16     3328      10440                3200   0 dllhost
    333      38    10188      18944       1.50    4708   1 dllhost
    165      10     3576       9720       5.69    6556   1 dllhost
```

217	13	6092	14192	9.63	8928	1	DTShellHlp
1759	45	116864	99676		1376	1	dwm
526	20	8196	24840	203.19	8904	1	ETDCtrl
1092	10	2796	9636	8.27	14976	1	ETDCtrlHelper
110	7	1236	4968		4468	0	ETDService
122	9	2096	6932	0.02	11652	1	ETDTouch
4784	140	152492	185560	1,442.92	7316	1	explorer
39	9	4704	8256		332	1	fontdrvhost
32	8	3888	4756		1028	0	fontdrvhost
564	23	45040	37984		1364	0	HPSupportSolutionsFrameworkService
427	34	67424	31312		3520	0	IAStorDataMgrSvc
89	6	1216	4756		4508	0	ibtsiva
0	0	60	8		0	0	Idle
270	12	3568	12408	0.11	11660	1	IESettingSync
174	10	2044	8376		2000	0	igfxCUIService
151	8	1624	7028		4608	0	IntelCpHDCPSvc
139	7	1644	6704		5184	0	IntelCpHeciSvc
136	8	1300	5676		5176	0	jhi_service
553	27	12668	45500	2.41	12896	1	LockApp
44	6	1208	2644		1000	0	LsaIso
1549	27	9292	20816		1008	0	lsass
0	0	1208	212664		2944	0	Memory Compression
366	20	40180	31840		6496	0	MoUsoCoreWorker
470	26	9160	21876		4520	0	nvcontainer
380	57	30000	35120	21.13	13088	1	nvcontainer
341	27	5536	16248		2340	0	NVDisplay.Container
680	30	33080	37352		12716	1	NVDisplay.Container
560	72	35924	1436	14.02	13996	1	NVIDIA Web Helper
256	16	4940	13216		4900	0	NvTelemetryContainer
809	28	36560	47156		4908	0	OfficeClickToRun
612	58	770528	118548		4700	0	oracle
612	30	70692	83572	3.55	5676	1	powershell
252	28	24788	16416		8672	0	PresentationFontCache
0	18	8372	56416		132	0	Registry
184	10	2140	9056		4588	0	RegSrvc

```
 191     9    2240      7652           3136   0 RtkAudioService64
 142    10    2412      8876      0.05 9988   1 rundll32
 844    35   17076     46036     18.17 6924   1 RuntimeBroker
 462    25    8316     29324     13.02 8388   1 RuntimeBroker
 457    24   10464     34280     21.58 8644   1 RuntimeBroker
 358    19    6572     25704      2.41 8720   1 RuntimeBroker
 501    23    7840     29072      3.17 10056  1 RuntimeBroker
 194    12    2960     15228      0.17 10416  1 RuntimeBroker
1868   155  215132    104060     72.86 9032   1 SearchApp
 910    82   81008     63268           1276   0 SearchIndexer
   0     0     184     22912             72   0 Secure System
 398    17    4756     14972          10480   0 SecurityHealthService
 814    12    6220      9196            956   0 services
 654    31   14884      5412     12.52 1492   1 SettingSyncHost
 116     7    7736      7600           4332   0 SgrmBroker
 896    36   31304     58512      6.81 9936   1 ShellExperienceHost
 761    26   13856     40368     22.14 2596   1 sihost
  53     3    1092      1128            512   0 smss
 506    29    6052     13500           3988   0 spoolsv
 757    37   41500     87868     26.50 8356   1 StartMenuExperienceHost
 222    12    2656     10900            664   0 svchost
1250    25   15932     34332            732   0 svchost
 184    10    2296      7772            980   0 svchost
1427    22   11084     17208           1204   0 svchost
 306    12    2880      8132           1268   0 svchost
 150    24    5956      7136           1400   0 svchost
 256    13    2640      9540           1484   0 svchost
 334    10    2916      7152           1564   0 svchost
 155     9    2068     11036           1572   0 svchost
 299    10    2260      7876           1620   0 svchost
 880    21    5668     19616           1640   0 svchost
 181     9    1992      7396           1664   0 svchost
 100     9    1256      4792           1792   0 svchost
 436    13   14596     14692           1828   0 svchost
 421    20    7520     15256           1872   0 svchost
```

245	16	38340	12012		1940	0	svchost
179	13	2048	7872		1976	0	svchost
288	10	2876	9544		2080	0	svchost
403	16	5216	9892		2180	0	svchost
443	12	3420	9128		2276	0	svchost
228	13	3292	11580		2392	0	svchost
309	11	3368	9652		2448	0	svchost
312	16	3904	8448		2476	0	svchost
250	15	103764	104188		2536	0	svchost
199	7	1316	5456		2544	0	svchost
166	7	1608	5616		2564	0	svchost
264	10	2236	7844		2652	0	svchost
145	11	1816	8420		2664	0	svchost
137	9	1596	6236		2816	0	svchost
441	32	11908	13404		2888	0	svchost
128	9	1444	5884		2964	0	svchost
184	11	2124	7564		3048	0	svchost
530	15	4604	18436		3088	0	svchost
151	10	1824	7812		3164	0	svchost
213	10	8260	15644		3172	0	svchost
123	8	1684	7564		3272	0	svchost
144	11	1896	6272		3368	0	svchost
387	16	3132	9548		3376	0	svchost
126	8	1552	6292		3448	0	svchost
530	25	7168	18188		3620	0	svchost
226	13	2536	9296		3636	0	svchost
514	24	16776	24652	28.58	3732	1	svchost
245	15	2956	13552		3868	0	svchost
199	11	2368	8580		3984	0	svchost
240	12	2484	9928		4164	0	svchost
569	28	23416	28816		4172	0	svchost
232	10	2700	7912		4180	0	svchost
416	21	25936	29636		4188	0	svchost
324	30	6584	15608		4196	0	svchost
264	14	2796	7116		4212	0	svchost

436	15	7772	16236		4224	0	svchost
132	7	1296	5160		4232	0	svchost
132	9	1636	5640		4240	0	svchost
207	12	2488	8984		4248	0	svchost
315	14	4244	17332		4256	0	svchost
202	12	1788	6536		4268	0	svchost
239	17	2156	6488		4432	0	svchost
631	25	9752	37180	25.45	4580	1	svchost
369	17	2868	10052		4748	0	svchost
105	7	1332	4984		4812	0	svchost
326	17	4160	23680	8.75	4820	1	svchost
212	12	2396	8672		5136	0	svchost
393	25	3620	11816		5224	0	svchost
365	20	5732	21084		5748	0	svchost
590	74	22516	26640		6204	0	svchost
220	12	2796	10860		6396	0	svchost
198	13	3228	15812		6804	0	svchost
408	29	5380	19140		6932	0	svchost
248	11	2468	7852		6936	0	svchost
280	34	2316	9532		7048	0	svchost
232	13	3016	11576		7484	0	svchost
442	16	6696	14840		7504	0	svchost
353	20	6792	19652	3.36	7632	1	svchost
180	9	1844	7452		7704	0	svchost
383	15	5000	21424		7716	0	svchost
174	201	2364	6488		7960	0	svchost
332	16	4268	16216		8536	0	svchost
467	25	5504	18820	2.22	8584	1	svchost
289	20	3032	11964		8828	0	svchost
262	32	2332	12624		10256	0	svchost
529	32	11208	19444		11204	0	svchost
119	8	1460	6144		11228	0	svchost
111	7	1344	5352		11568	0	svchost
137	8	1668	6728	0.11	12052	1	svchost
149	9	1860	8668	0.05	13196	1	svchost

193	15	6420	8960		13644	0	svchost
197	11	2052	8724		14672	0	svchost
4609	0	224	14124		4	0	System
571	27	8800	29500	4.94	12804	1	SystemSettingsBroker
315	16	4048	15772	6.81	13860	1	TabTip
305	63	16400	25856	11.05	7348	1	taskhostw
352	19	6056	17624	1.22	15244	1	taskhostw
519	190	418084	472952	267.80	436	1	Teams
514	121	243924	302800	159.53	6416	1	Teams
494	29	18708	44164	14.11	7224	1	Teams
322	26	27108	48832	0.45	9180	1	Teams
1524	64	190164	178696	455.67	10400	1	Teams
333	20	11564	58260	0.77	12960	1	Teams
1189	68	174868	139840	64.31	13304	1	Teams
1217	36	505776	402456	181.27	14244	1	Teams
397	104	205444	233576	206.86	14332	1	Teams
305	22	23840	77292	0.17	15248	1	Teams
557	23	11544	42600	13.67	9124	1	TextInputHost
99	7	1216	4728		4528	0	tmGAInstall
256	25	16348	13704		4564	0	TNSLSNR
133	9	2148	7736		5632	0	unsecapp
133	10	2168	8932	0.98	14432	1	UserOOBEBroker
170	11	1472	6056		832	0	wininit
292	14	3120	12320		904	1	winlogon
1253	53	68360	161284	65.02	12064	1	WINWORD
411	19	5304	16228		4044	0	wlanext
233	14	4292	12332		5996	0	WmiPrvSE
316	14	4284	10856		824	0	WUDFHost
602	18	7740	10824		1136	0	WUDFHost
287	18	7416	18728	1,205.83	9312	1	xampp-control
349	20	5572	17416		4620	0	ZeroConfigService

Piping-One of the time savers in power Shell is giving the user the ability to pip commands together :

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

ProcessName : ApplicationFrameHost
Id          : 3720

ProcessName : audiodg
Id          : 9904

ProcessName : conhost
Id          : 6452

ProcessName : conhost
Id          : 5840

ProcessName : conhost
Id          : 4060

ProcessName : Cortana
Id          : 11044

ProcessName : csrss
Id          : 840

ProcessName : csrss
Id          : 728

ProcessName : ctfmon
Id          : 7756

ProcessName : dasHost
Id          : 4936

ProcessName : DiscSoftBusServiceLite
Id          : 8392
```

ProcessName : dllhost

Id : 6556

ProcessName : dllhost

Id : 4708

ProcessName : dllhost

Id : 3200

ProcessName : DTShellHlp

Id : 8928

ProcessName : dwm

Id : 1376

ProcessName : ETDCtrl

Id : 8904

ProcessName : ETDCtrlHelper

Id : 14976

ProcessName : ETDService

Id : 4468

ProcessName : ETDTouch

Id : 11652

ProcessName : explorer

Id : 7316

ProcessName : fontdrvhost

Id : 1028

ProcessName : fontdrvhost

Id : 332

ProcessName : HPSupportSolutionsFrameworkService

Id : 1364

ProcessName : IAStorDataMgrSvc

Id : 3520

ProcessName : ibtsiva

Id : 4508

ProcessName : Idle

Id : 0

ProcessName : IESettingSync

Id : 11660

ProcessName : igfxCUIService

Id : 2000

ProcessName : IntelCpHDCPSvc

Id : 4608

ProcessName : IntelCpHeciSvc

Id : 5184

ProcessName : jhi_service

Id : 5176

ProcessName : LockApp

Id : 12896

ProcessName : LsaIso

Id : 1000

ProcessName : lsass

Id : 1008

ProcessName : Memory Compression

Id : 2944

ProcessName : MoUsoCoreWorker

Id : 6496

ProcessName : nvcontainer

Id : 13088

ProcessName : nvcontainer

Id : 4520

ProcessName : NVDisplay.Container

Id : 12716

ProcessName : NVDisplay.Container

Id : 2340

ProcessName : NVIDIA Web Helper

Id : 13996

ProcessName : NvTelemetryContainer

Id : 4900

ProcessName : OfficeClickToRun

Id : 4908

ProcessName : oracle

Id : 4700

ProcessName : powershell

Id : 5676

ProcessName : PresentationFontCache

Id : 8672

ProcessName : Registry

Id : 132

ProcessName : RegSrvc

Id : 4588

ProcessName : RtkAudioService64

Id : 3136

ProcessName : rundll32

Id : 9988

ProcessName : RuntimeBroker

Id : 8720

ProcessName : RuntimeBroker

Id : 10056

ProcessName : RuntimeBroker

Id : 10416

ProcessName : RuntimeBroker

Id : 6924

ProcessName : RuntimeBroker

Id : 8388

ProcessName : RuntimeBroker

Id : 8644

ProcessName : SearchApp

Id : 9032

ProcessName : SearchIndexer

Id : 1276

ProcessName : Secure System

Id : 72

ProcessName : SecurityHealthService

Id : 10480

ProcessName : services

Id : 956

ProcessName : SettingSyncHost

Id : 1492

ProcessName : SgrmBroker

Id : 4332

ProcessName : ShellExperienceHost

Id : 9936

ProcessName : sihost

Id : 2596

ProcessName : smss

Id : 512

ProcessName : spoolsv

Id : 3988

ProcessName : StartMenuExperienceHost

Id : 8356

ProcessName : svchost

Id : 4748

ProcessName : svchost

Id : 4812

ProcessName : svchost

Id : 4580

ProcessName : svchost

Id : 4268

ProcessName : svchost

Id : 4432

ProcessName : svchost

Id : 5748

ProcessName : svchost

Id : 6204

ProcessName : svchost

Id : 5224

ProcessName : svchost

Id : 4820

ProcessName : svchost

Id : 5136

ProcessName : svchost

Id : 4256

ProcessName : svchost

Id : 4188

ProcessName : svchost

Id : 4196

ProcessName : svchost

Id : 4180

ProcessName : svchost

Id : 4164

ProcessName : svchost

Id : 4172

ProcessName : svchost

Id : 4240

ProcessName : svchost

Id : 4248

ProcessName : svchost

Id : 4232

ProcessName : svchost

Id : 4212

ProcessName : svchost

Id : 4224

ProcessName : svchost

Id : 6396

ProcessName : svchost

Id : 11204

ProcessName : svchost

Id : 11228

ProcessName : svchost

Id : 10256

ProcessName : svchost

Id : 8584

ProcessName : svchost

Id : 8828

ProcessName : svchost

Id : 13644

ProcessName : svchost

Id : 14672

ProcessName : svchost

Id : 13196

ProcessName : svchost

Id : 11568

ProcessName : svchost

Id : 12052

ProcessName : svchost

Id : 8536

ProcessName : svchost

Id : 7048

ProcessName : svchost

Id : 7484

ProcessName : svchost

Id : 6936

ProcessName : svchost

Id : 6804

ProcessName : svchost

Id : 6932

ProcessName : svchost

Id : 7716

ProcessName : svchost

Id : 7960

ProcessName : svchost

Id : 7704

ProcessName : svchost

Id : 7504

ProcessName : svchost

Id : 7632

ProcessName : svchost

Id : 3984

ProcessName : svchost

Id : 1872

ProcessName : svchost

Id : 1940

ProcessName : svchost

Id : 1828

ProcessName : svchost

Id : 1664

ProcessName : svchost

Id : 1792

ProcessName : svchost

Id : 2276

ProcessName : svchost

Id : 2392

ProcessName : svchost

Id : 2180

ProcessName : svchost

Id : 1976

ProcessName : svchost

Id : 2080

ProcessName : svchost

Id : 1640

ProcessName : svchost

Id : 1204

ProcessName : svchost

Id : 1268

ProcessName : svchost

Id : 980

ProcessName : svchost

Id : 664

ProcessName : svchost

Id : 732

ProcessName : svchost

Id : 1572

ProcessName : svchost

Id : 1620

ProcessName : svchost

Id : 1564

ProcessName : svchost

Id : 1400

ProcessName : svchost

Id : 1484

ProcessName : svchost

Id : 2448

ProcessName : svchost

Id : 3368

ProcessName : svchost

Id : 3376

ProcessName : svchost

Id : 3272

ProcessName : svchost

Id : 3164

ProcessName : svchost

Id : 3172

ProcessName : svchost

Id : 3732

ProcessName : svchost

Id : 3868

ProcessName : svchost

Id : 3636

ProcessName : svchost

Id : 3448

ProcessName : svchost

Id : 3620

ProcessName : svchost

Id : 3088

ProcessName : svchost

Id : 2564

ProcessName : svchost

Id : 2652

ProcessName : svchost

Id : 2544

ProcessName : svchost

Id : 2476

ProcessName : svchost

Id : 2536

ProcessName : svchost

Id : 2964

ProcessName : svchost

Id : 3048

ProcessName : svchost

Id : 2888

ProcessName : svchost

Id : 2664

ProcessName : svchost

Id : 2816

ProcessName : System

Id : 4

ProcessName : SystemSettingsBroker

Id : 12804

ProcessName : TabTip

Id : 13860

ProcessName : taskhostw

Id : 15244

ProcessName : taskhostw

Id : 7348

ProcessName : Teams

Id : 13304

ProcessName : Teams

Id : 12960

ProcessName : Teams

Id : 14244

ProcessName : Teams

Id : 15248

ProcessName : Teams

Id : 14332

ProcessName : Teams

Id : 6416

ProcessName : Teams

Id : 436

ProcessName : Teams

Id : 7224

ProcessName : Teams

Id : 10400

ProcessName : Teams

Id : 9180

ProcessName : TextInputHost

Id : 9124

ProcessName : tmGAInstall

Id : 4528

ProcessName : TNSLSNR

Id : 4564

ProcessName : unsecapp

Id : 5632

ProcessName : UserOOBEBroker

Id : 14432

ProcessName : wininit

Id : 832

ProcessName : winlogon

Id : 904

ProcessName : WINWORD

Id : 12064

ProcessName : wlanext

Id : 4044

ProcessName : WmiPrvSE

Id : 5996

ProcessName : WUDFHost

Id : 1136

ProcessName : WUDFHost

Id : 824

ProcessName : xampp-control

Id : 9312

ProcessName : ZeroConfigService

Id : 4620

Pull computer serial number

PS C:\Users\NISHANK> Gwmi Win32_Bios | select SerialNumber

SerialNumber

5CD8080G0Z

Reboot a machine

(Gwmi win32_OperatingSystem –comp | server).reboot()

Gather Logical Disk Space information

PS C:\Users\NISHANK> Gwmi Win32_LogicalDisk

DeviceID : C:

DriveType : 3

ProviderName :

FreeSpace : 1055100841984

Size : 1981152227328

VolumeName : Windows

DeviceID : D:

DriveType : 3

ProviderName :

FreeSpace : 2099453952

Size : 17922256896

VolumeName : RECOVERY

DeviceID : E:

DriveType : 5

ProviderName :

FreeSpace :

Size :

VolumeName :

Show running processes

PS C:\Users\NISHANK> Gwmi Win32_Process

Show Network Adapters

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

PS C:\Users\NISHANK> $NIC

DHCPEnabled : True

IPAddress : {192.168.1.6, fe80::49c8:728e:e6c1:54e4}

DefaultIPGateway : {192.168.1.1}

DNSDomain :

ServiceName : Netwtw04

Description : Intel(R) Dual Band Wireless-AC 7265

Index : 2

DHCPEnabled : False

IPAddress : {192.168.56.1, fe80::84b7:924e:f036:b859}

DefaultIPGateway :

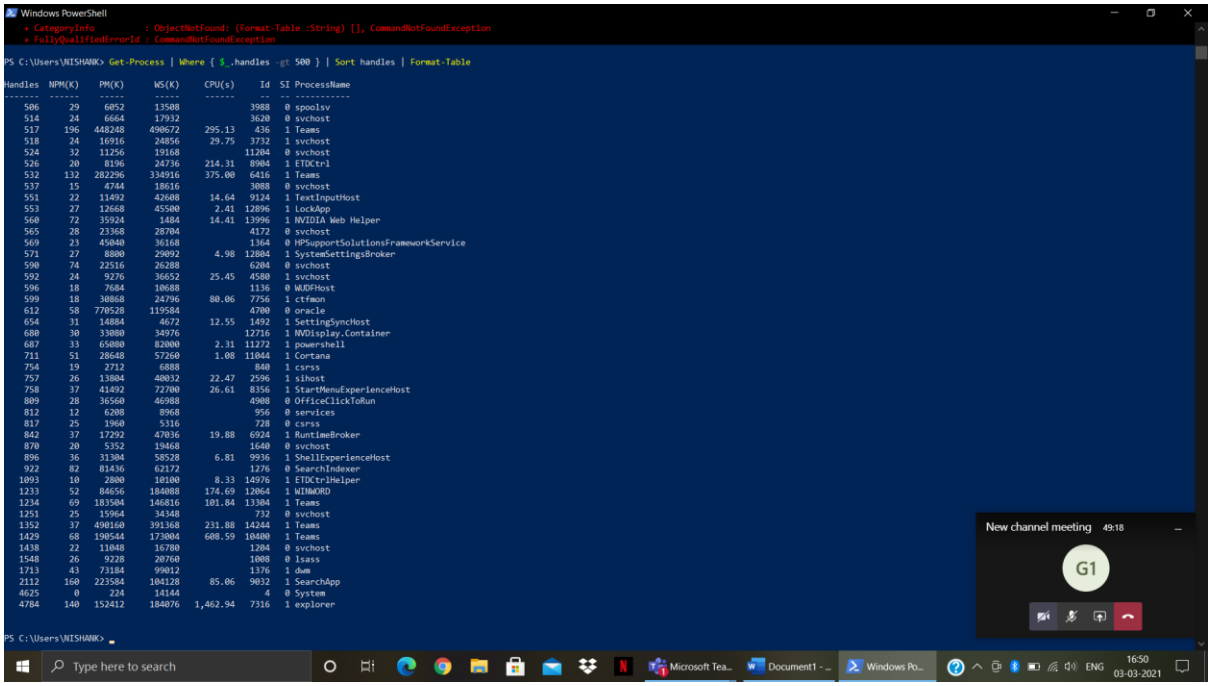
DNSDomain :

ServiceName : VBoxNetAdp

Description : VirtualBox Host-Only Ethernet Adapter

Index : 14

Process



Find the processes in the memory

PS C:\Users\NISHANK> ps

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
287	18	7392	24756	2.63	3720	1	ApplicationFrameHost
388	22	17828	20408	469.73	9904	0	audiodg
97	7	6220	4352		4060	0	conhost
97	7	6348	116	0.03	5840	1	conhost
273	14	5808	17916	2.70	6720	1	conhost
711	51	28648	57260	1.08	11044	1	Cortana
823	26	1960	5324		728	0	csrss
760	19	2716	6892		840	1	csrss
605	18	30888	24884	81.05	7756	1	ctfmon
329	15	3636	8612		4936	0	dasHost
307	16	4132	12836		8392	0	DiscSoftBusServiceLite
203	16	3328	10144		3200	0	dllhost
345	40	10892	19496	2.38	4708	1	dllhost
176	10	3788	14184	5.86	6556	1	dllhost

217	13	6092	13676	9.63	8928	1	DTShellHlp
1706	43	73664	99736		1376	1	dwm
526	20	8196	24736	215.77	8904	1	ETDCtrl
1105	10	2800	10120	8.55	14976	1	ETDCtrlHelper
110	7	1236	4968		4468	0	ETDService
122	9	2096	6932	0.02	11652	1	ETDTouch
5179	152	159400	201528	1,470.75	7316	1	explorer
39	8	5120	8140		332	1	fontdrvhost
32	8	3888	4756		1028	0	fontdrvhost
569	23	45040	36168		1364	0	HPSupportSolutionsFrameworkService
427	34	67424	30672		3520	0	IAStorDataMgrSvc
89	6	1216	4392		4508	0	ibtsiva
0	0	60	8		0	0	Idle
270	12	3568	11956	0.11	11660	1	IESettingSync
174	10	2044	8176		2000	0	igfxCUIService
151	8	1624	6756		4608	0	IntelCpHDCPSvc
139	7	1644	6432		5184	0	IntelCpHeciSvc
136	8	1300	5676		5176	0	jhi_service
553	27	12668	45500	2.41	12896	1	LockApp
44	6	1208	2644		1000	0	LsaIso
1559	26	9232	20976		1008	0	lsass
0	0	1212	273248		2944	0	Memory Compression
353	20	40440	31968		6496	0	MoUsoCoreWorker
468	26	9132	21796		4520	0	nvcontainer
372	56	29780	34960	21.34	13088	1	nvcontainer
341	27	5536	15716		2340	0	NVDisplay.Container
680	30	33080	34976		12716	1	NVDisplay.Container
560	72	35924	1484	14.50	13996	1	NVIDIA Web Helper
245	16	4712	13120		4900	0	NvTelemetryContainer
809	28	36560	47044		4908	0	OfficeClickToRun
612	58	770528	119584		4700	0	oracle
769	33	67360	85024	2.78	11272	1	powershell
252	28	24788	16416		8672	0	PresentationFontCache
0	18	8776	57116		132	0	Registry
184	10	2140	8688		4588	0	RegSrvc

191	9	2240	7608		3136	0	RtkAudioService64
142	10	2412	8572	0.05	9988	1	rundll32
842	37	17292	47044	19.89	6924	1	RuntimeBroker
431	24	7568	28396	13.38	8388	1	RuntimeBroker
453	24	10328	34044	21.64	8644	1	RuntimeBroker
358	19	6556	25316	2.44	8720	1	RuntimeBroker
496	22	7700	29020	3.20	10056	1	RuntimeBroker
194	12	2960	15236	0.17	10416	1	RuntimeBroker
2112	160	223584	104128	85.06	9032	1	SearchApp
177	10	1992	9180		11564	0	SearchFilterHost
943	82	82912	63620		1276	0	SearchIndexer
365	13	2572	13972		12020	0	SearchProtocolHost
0	0	184	22912		72	0	Secure System
398	17	4756	14948		10480	0	SecurityHealthService
812	12	6268	8996		956	0	services
654	31	14884	5444	12.56	1492	1	SettingSyncHost
116	7	7296	7292		4332	0	SgrmBroker
896	36	31304	58528	6.81	9936	1	ShellExperienceHost
757	26	13804	40080	22.50	2596	1	sihost
410	23	8256	23964	0.30	3664	1	smartscreen
53	3	1092	1128		512	0	smss
506	29	6052	13516		3988	0	spoolsv
758	37	41496	72708	26.63	8356	1	StartMenuExperienceHost
355	13	3420	12652		664	0	svchost
1245	25	15912	34328		732	0	svchost
177	10	2132	7732		980	0	svchost
1444	22	11052	16900		1204	0	svchost
306	12	2888	8116		1268	0	svchost
151	25	5952	6636		1400	0	svchost
256	13	2640	9252		1484	0	svchost
332	10	2852	7056		1564	0	svchost
155	9	2068	10808		1572	0	svchost
299	10	2260	7728		1620	0	svchost
870	20	5352	19468		1640	0	svchost
181	9	1992	6924		1664	0	svchost

100	9	1256	4792		1792	0	svchost
434	13	14104	13852		1828	0	svchost
417	19	7448	15716		1872	0	svchost
247	16	38396	13216		1940	0	svchost
179	13	2048	7516		1976	0	svchost
289	10	2920	9616		2080	0	svchost
403	16	5216	9320		2180	0	svchost
434	12	3360	9080		2276	0	svchost
219	13	3064	11504		2392	0	svchost
309	11	3364	9584		2448	0	svchost
310	17	4036	8632		2476	0	svchost
246	15	109744	110276		2536	0	svchost
201	7	1316	5456		2544	0	svchost
166	7	1608	5588		2564	0	svchost
264	10	2236	7592		2652	0	svchost
145	11	1792	8448		2664	0	svchost
137	9	1596	6236		2816	0	svchost
439	32	11848	13376		2888	0	svchost
128	9	1444	5884		2964	0	svchost
187	11	2144	7596		3048	0	svchost
534	15	4692	18604		3088	0	svchost
151	10	1824	7484		3164	0	svchost
237	11	15104	23124		3172	0	svchost
142	11	1812	6232		3368	0	svchost
383	15	2820	9380		3376	0	svchost
126	8	1552	6292		3448	0	svchost
514	24	6660	17928		3620	0	svchost
230	13	2704	9328		3636	0	svchost
518	24	16924	24880	29.86	3732	1	svchost
245	15	2956	13492		3868	0	svchost
200	11	2440	8648		3984	0	svchost
240	12	2484	9564		4164	0	svchost
565	28	23344	28804		4172	0	svchost
232	10	2716	7908		4180	0	svchost
417	21	26052	28268		4188	0	svchost

320	29	6520	15044		4196	0	svchost
264	14	2796	6856		4212	0	svchost
452	15	8392	17352		4224	0	svchost
132	7	1296	5212		4232	0	svchost
132	9	1636	5640		4240	0	svchost
207	12	2488	8548		4248	0	svchost
315	14	4244	16540		4256	0	svchost
202	12	1788	6328		4268	0	svchost
239	17	2156	6104		4432	0	svchost
592	24	9224	36640	25.45	4580	1	svchost
369	17	2920	9800		4748	0	svchost
105	7	1332	4892		4812	0	svchost
330	17	4256	23744	9.22	4820	1	svchost
210	12	2420	8772		5136	0	svchost
393	25	3620	11732		5224	0	svchost
368	19	5676	20972		5748	0	svchost
586	74	22460	26308		6204	0	svchost
220	12	2796	10896		6396	0	svchost
197	13	3260	15824		6804	0	svchost
412	30	5448	19108		6932	0	svchost
248	11	2468	7780		6936	0	svchost
280	34	2316	9484		7048	0	svchost
232	13	3016	11524		7484	0	svchost
441	15	6588	14388		7504	0	svchost
353	20	6792	19484	3.38	7632	1	svchost
180	9	1844	7484		7704	0	svchost
364	14	4604	17436		7716	0	svchost
174	201	2364	6360		7960	0	svchost
329	16	4188	16128		8536	0	svchost
467	25	5504	18416	2.22	8584	1	svchost
289	20	3048	11968		8828	0	svchost
262	32	2332	12392		10256	0	svchost
524	32	11256	19168		11204	0	svchost
134	9	1620	6800		11228	0	svchost
111	7	1344	5248		11568	0	svchost

137	8	1668	6740	0.11	12052	1	svchost
149	9	1860	8428	0.05	13196	1	svchost
193	15	6420	8960		13644	0	svchost
197	11	2052	8396		14672	0	svchost
168	9	1796	7364		15648	0	svchost
4673	0	224	14144		4	0	System
571	27	8800	29092	4.98	12804	1	SystemSettingsBroker
321	17	4112	16052	8.00	13860	1	TabTip
308	63	16512	26456	11.30	7348	1	taskhostw
367	21	6276	18336	1.25	15244	1	taskhostw
520	196	448304	491064	296.31	436	1	Teams
304	22	23496	77236	0.05	5776	1	Teams
535	135	287068	344096	398.56	6416	1	Teams
496	29	18644	43980	22.55	7224	1	Teams
322	26	27108	48724	0.45	9180	1	Teams
327	26	31688	85952	1.02	9624	1	Teams
1447	65	190800	173724	622.73	10400	1	Teams
336	21	11600	58252	0.78	12960	1	Teams
1234	69	183536	146704	106.31	13304	1	Teams
1354	38	504192	405548	235.95	14244	1	Teams
385	110	223624	244472	242.94	14332	1	Teams
555	23	11552	42636	14.86	9124	1	TextInputHost
99	7	1216	4668		4528	0	tmGAInstall
256	25	16348	13708		4564	0	TNSLSNR
133	9	2120	7704		5632	0	unsecapp
138	10	2208	8964	1.02	14432	1	UserOOBEBroker
170	11	1472	6056		832	0	wininit
296	14	3196	12384		904	1	winlogon
1603	65	110380	225852	192.86	12064	1	WINWORD
407	19	5240	16124		4044	0	wlanext
233	14	4208	12296		5996	0	WmiPrvSE
171	11	3336	11008		13080	0	WmiPrvSE
316	14	4284	10460		824	0	WUDFHost
596	18	7684	10688		1136	0	WUDFHost
287	18	7416	18432	1,242.73	9312	1	xampp-control

337 20 5448 17288 4620 0 ZeroConfigService

BIOS

CURRENT USER

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


SMBIOSBIOSVersion : F.35
Manufacturer      : Insyde
Name              : F.35
SerialNumber      : 5CD8080G0Z
Version           : HPQOEM - 0



PS C:\Users\NISHANK> Get-WmiObject -Class Win32_ComputerSystem -Property UserName -ComputerName .


__GENUS          : 2
__CLASS          : Win32_ComputerSystem
__SUPERCLASS     :
__DYNASTY        :
__RELPATH        :
__PROPERTY_COUNT : 1
__DERIVATION     : {}
__SERVER         :
__NAMESPACE      :
__PATH           :
UserName         : LAPTOP-G637AG3U\NISHANK
PSComputerName   :
```

Get Information about the make and model of a computer

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


Domain               : WORKGROUP
Manufacturer         : HP
Model                : HP Pavilion Laptop 15-cc1xx
Name                 : LAPTOP-G637AG3U
PrimaryOwnerName     : HP
TotalPhysicalMemory : 8470630400
```

Get information about the installed applications

PS C:\Users\NISHANK> Get-WmiObject -Class Win32_Product -ComputerName . | Format-Wide -Column 1

Python 3.9.1 Core Interpreter (64-bit)

Python 3.9.1 Tcl/Tk Support (64-bit)

Autodesk App Manager 2020

Autodesk Genuine Service

Python 3.9.1 Standard Library (64-bit)

DaVinci Resolve

Autodesk Featured Apps 2020

Python 3.9.1 pip Bootstrap (64-bit)

Autodesk Save to Web and Mobile

GoTo Opener

Python 3.9.1 Utility Scripts (64-bit)

Python 3.9.1 Test Suite (64-bit)

Python 3.9.1 Add to Path (64-bit)

Python 3.9.1 Executables (64-bit)

Python 3.9.1 Development Libraries (64-bit)

Python 3.9.1 Documentation (64-bit)

Office 16 Click-to-Run Extensibility Component

Office 16 Click-to-Run Localization Component

Office 16 Click-to-Run Licensing Component

Intel(R) Wireless Bluetooth(R)

HP Recovery Manager

EFH

Java 9.0.4 (64-bit)

Autodesk Material Library 2020

Update for Windows 10 for x64-based Systems (KB4023057)

Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219

HP ePrint SW

Microsoft Visual C++ 2005 Redistributable (x64)

Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219

Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005

Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005

HP Support Solutions Framework

Oracle Database 11g Express Edition

Bonjour

Java(TM) SE Development Kit 9.0.4 (64-bit)

Intel(R) Rapid Storage Technology

vs_FileTracker_Singleton

Intel(R) Management Engine Components

Microsoft Visual C++ 2005 Redistributable

Intel(R) Management Engine Driver

HP ePrint SW

Python Launcher

Microsoft Visual Studio Setup Configuration

Java 8 Update 271 (64-bit)

Java SE Development Kit 8 Update 271 (64-bit)

Intel(R) Trusted Connect Service Client x86

Intel(R) Trusted Connect Service Client x64

HP ePrint SW

Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29325

Xperia Companion

HP Customer Experience Enhancements

Intel(R) ME UninstallLegacy

Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29325

Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005

Oracle VM VirtualBox 6.1.18

vs_minshellmsires

Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161

Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161

Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005

Microsoft Visual C++ 2008 Redistributable - x86 9.0.21022

Microsoft Visual C++ 2019 X86 Additional Runtime - 14.24.28127

HP Support Assistant

vs_filehandler_amd64

DaVinci Resolve Panels

Microsoft Visual C++ 2012 x64 Additional Runtime - 11.0.61030

Intel(R) Chipset Device Software

Microsoft Visual C++ 2005 Redistributable (x64)

Microsoft Xbox 360 Accessories 1.2

Autodesk Material Library Base Resolution Image Library 2020

HP 3D DriveGuard

HP Audio Switch

Autodesk Single Sign On Component

Xperia Companion Service

HP ePrint SW

HP System Event Utility

vs_filehandler_x86

Microsoft VC++ redistributables repacked.

HP ePrint SW

HP ePrint SW

HP Registration Service

Microsoft VC++ redistributables repacked.

HP JumpStart Bridge

Intel(R) PRO/Wireless Driver

Intel® PROSet/Wireless WiFi Software

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

HP PC Hardware Diagnostics UEFI

Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148

Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.17

Microsoft Visual C++ 2012 x86 Minimum Runtime - 11.0.61030

vs_minshellmsi

HP JumpStart Launch

HP CoolSense

Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.17

Microsoft Update Health Tools

Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.24.28127

Java Auto Updater

Intel(R) Management Engine Components

AutoCAD 2020

ACAD Private

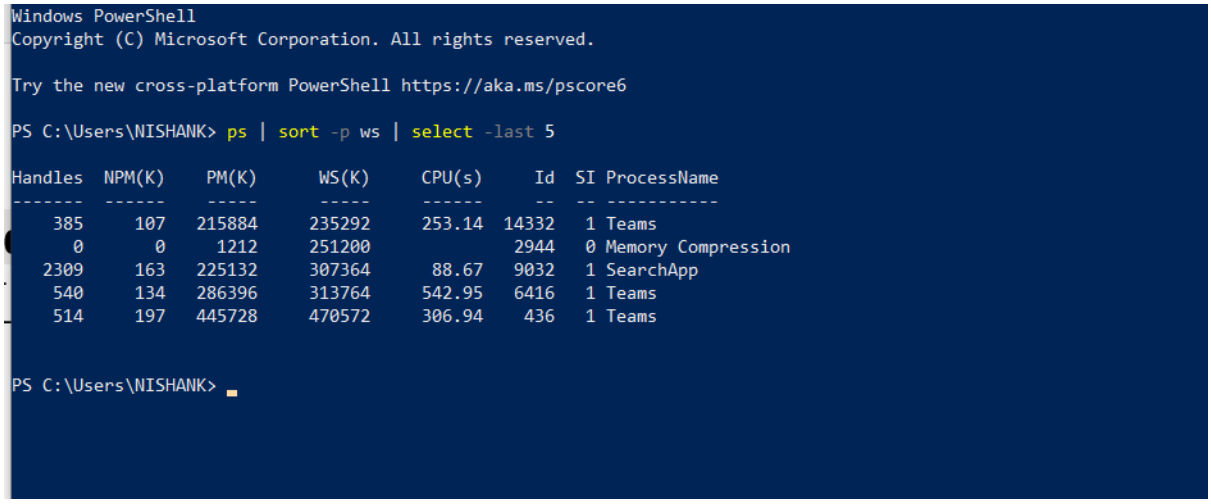
AutoCAD 2020 Language Pack - English

AutoCAD 2020 - English

ACA & MEP 2020 Object Enabler

Find the five processes using the most memory

1)Ps – process
2)Ws –working set (Working set is a concept in computer science which defines the amount of memory that a process requires in a given time interval.)


Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Users\NISHANK> ps | sort -p ws | select -last 5
Handles NPM(K) PM(K) WS(K) CPU(s) Id SI ProcessName
385 107 215884 235292 253.14 14332 1 Teams
0 0 1212 251200 2944 0 Memory Compression
2309 163 225132 307364 88.67 9032 1 SearchApp
540 134 286396 313764 542.95 6416 1 Teams
514 197 445728 470572 306.94 436 1 Teams
PS C:\Users\NISHANK>