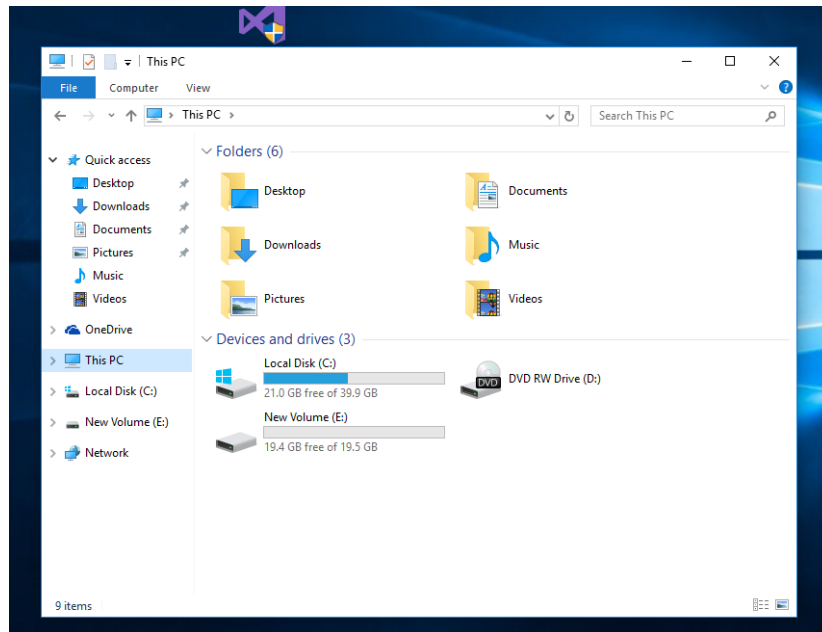


ASSIGNMENT – III

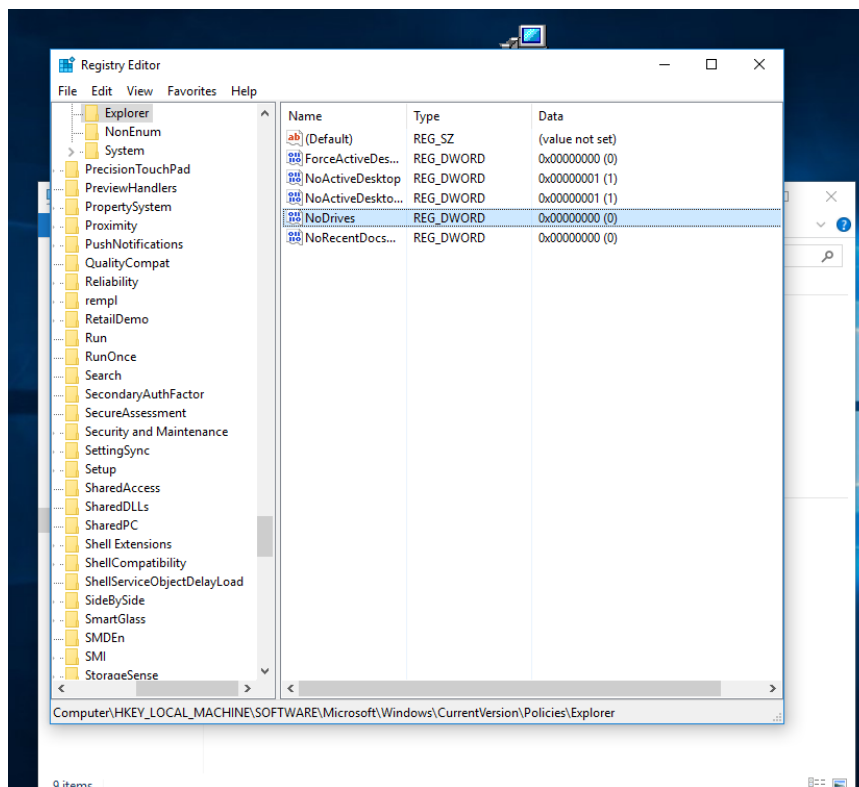
Submitted by: B. Pavan Sai
[mailto:beri_mcs17@diat.ac.in]

Hiding Disk partition by modifying Windows Registry

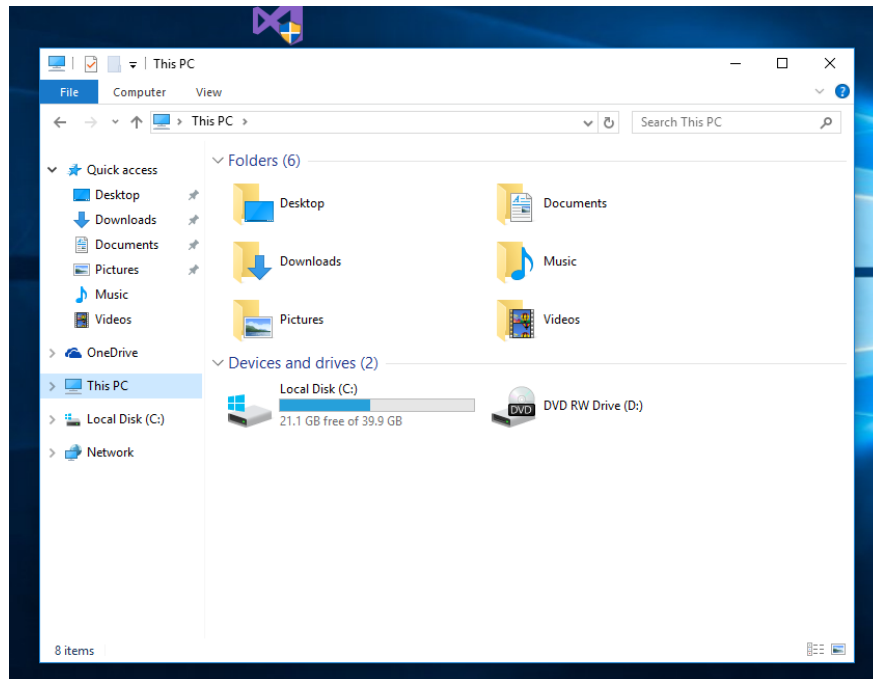
1. Before anything done.



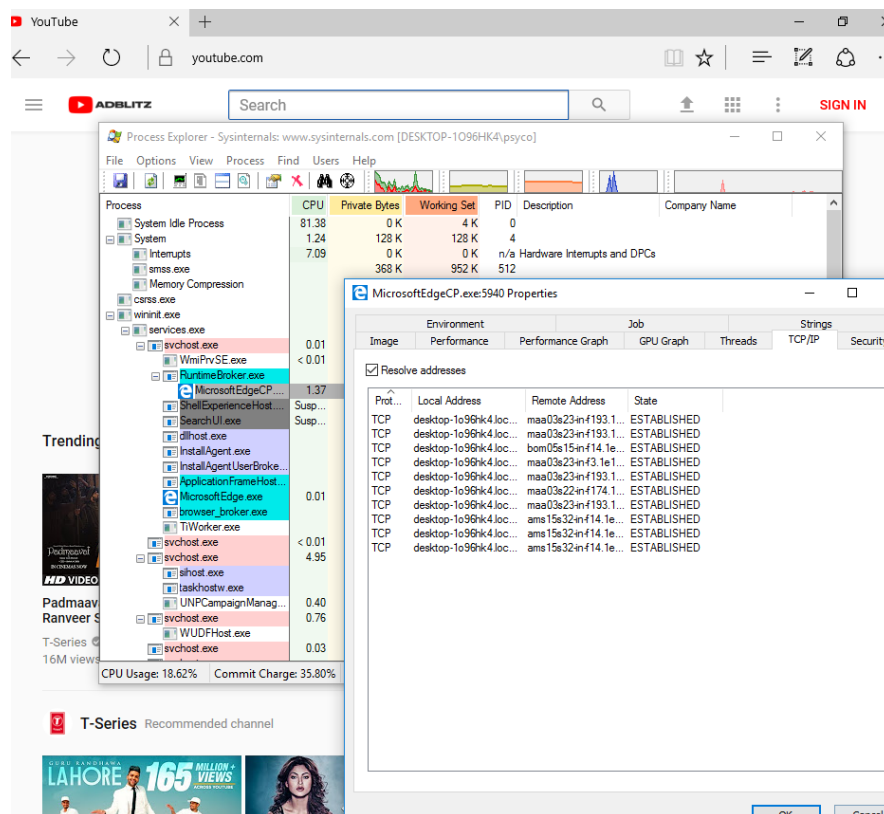
2. Modify the value for NoDrives (create if not available) to 16 (Decimal).



3. Reboot and your E drive is hidden now.



Finding IP address being accessed in browser from ProcExp



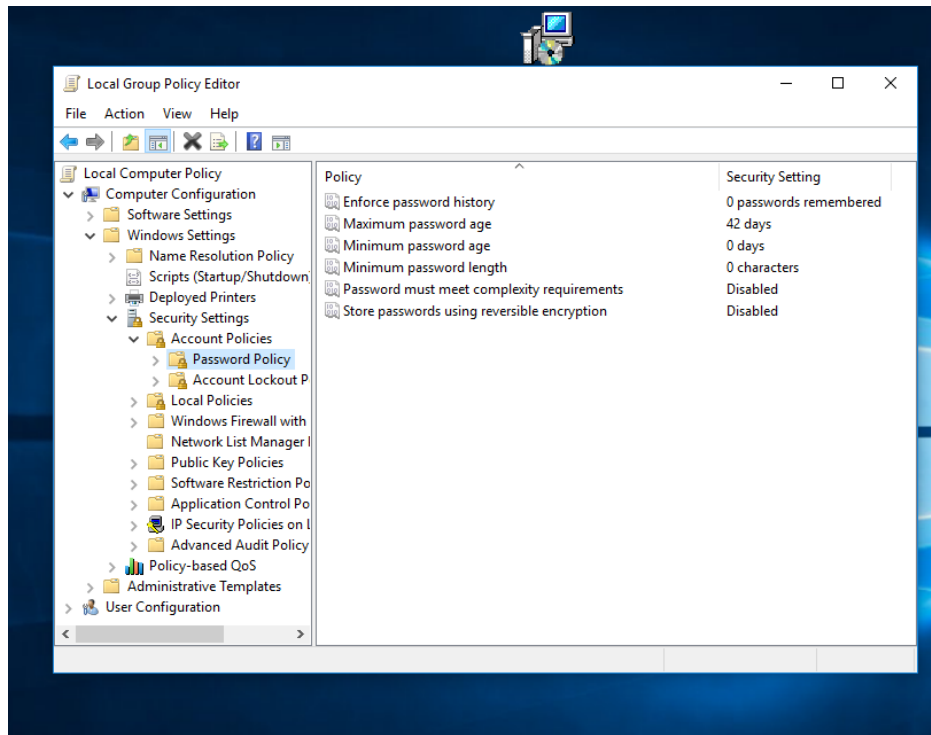
Procedure:

Browse some URL in a browser (say Edge), now open ProcExp from SysInternal tools. Locate that particular browser process and right click to open “Properties”, there select TCP/IP.

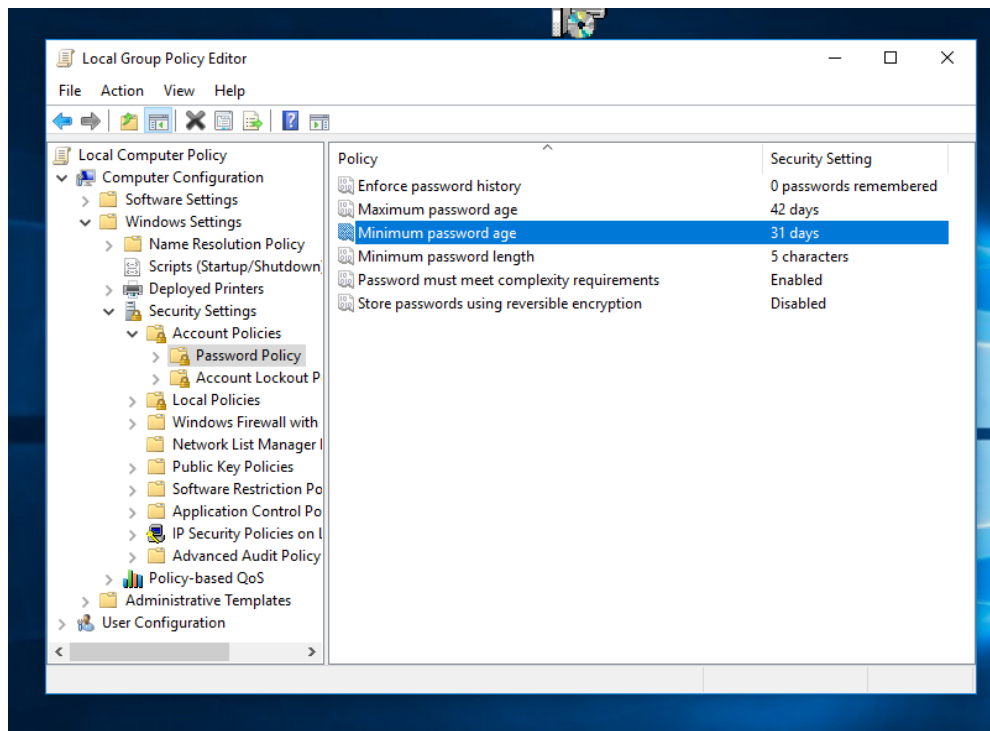
There you can see what are all the IP addresses being accessed by the browser.

Finding IP address being accessed in browser from ProcExp

Run “gpedit.msc” and locate Password Policy as shown in the figure below.



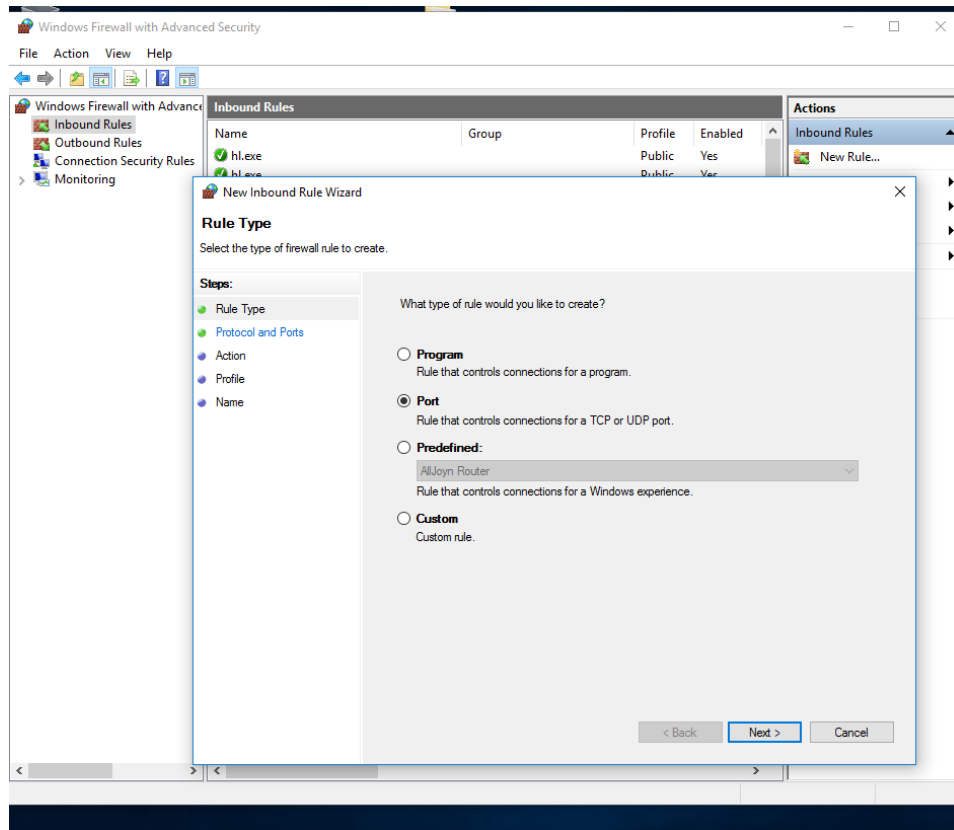
Now modify its contents as per your requirement and reboot the machine.



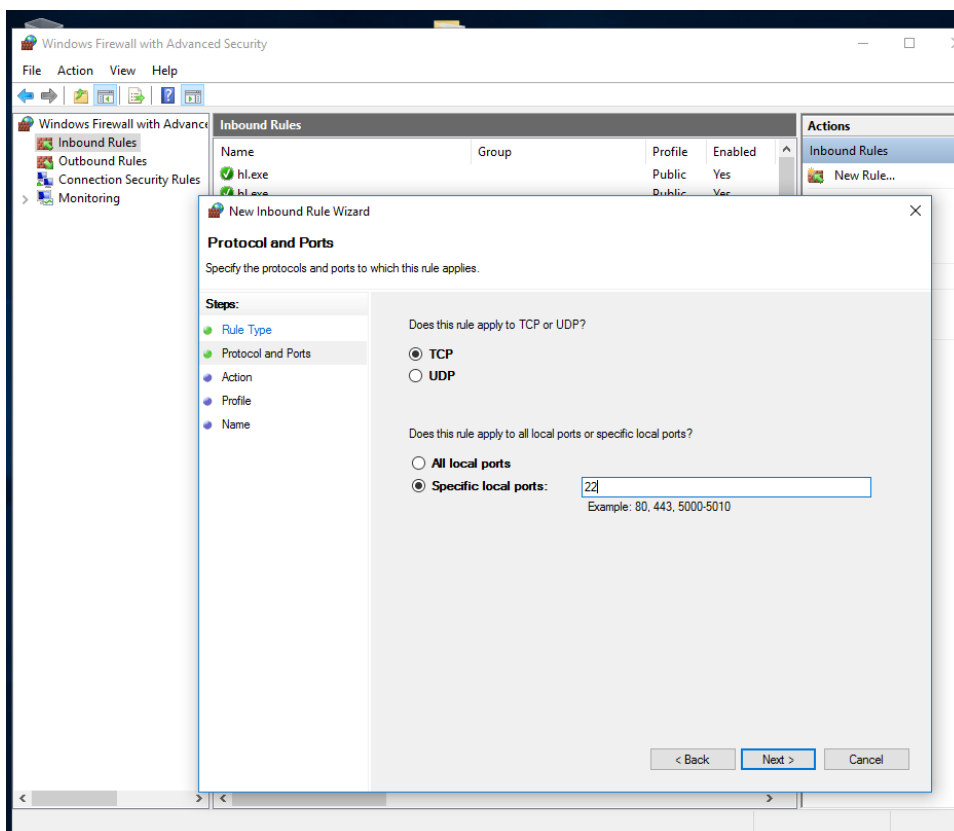
There you have created a new complex password policy using gpedit.

Blocking all incoming SSH traffic in Windows Firewall

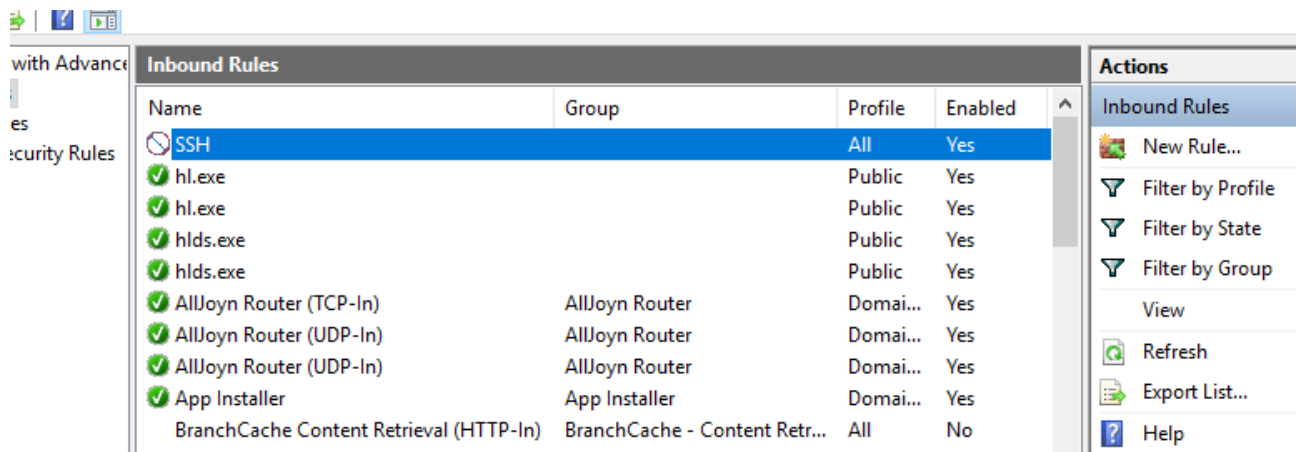
Open Control Panel and goto Firewall settings.
Select “Advanced Features” and click “Inbound Rules”
Select “Add New Rule” and fill all details.



Set blocking port to 22 for TCP



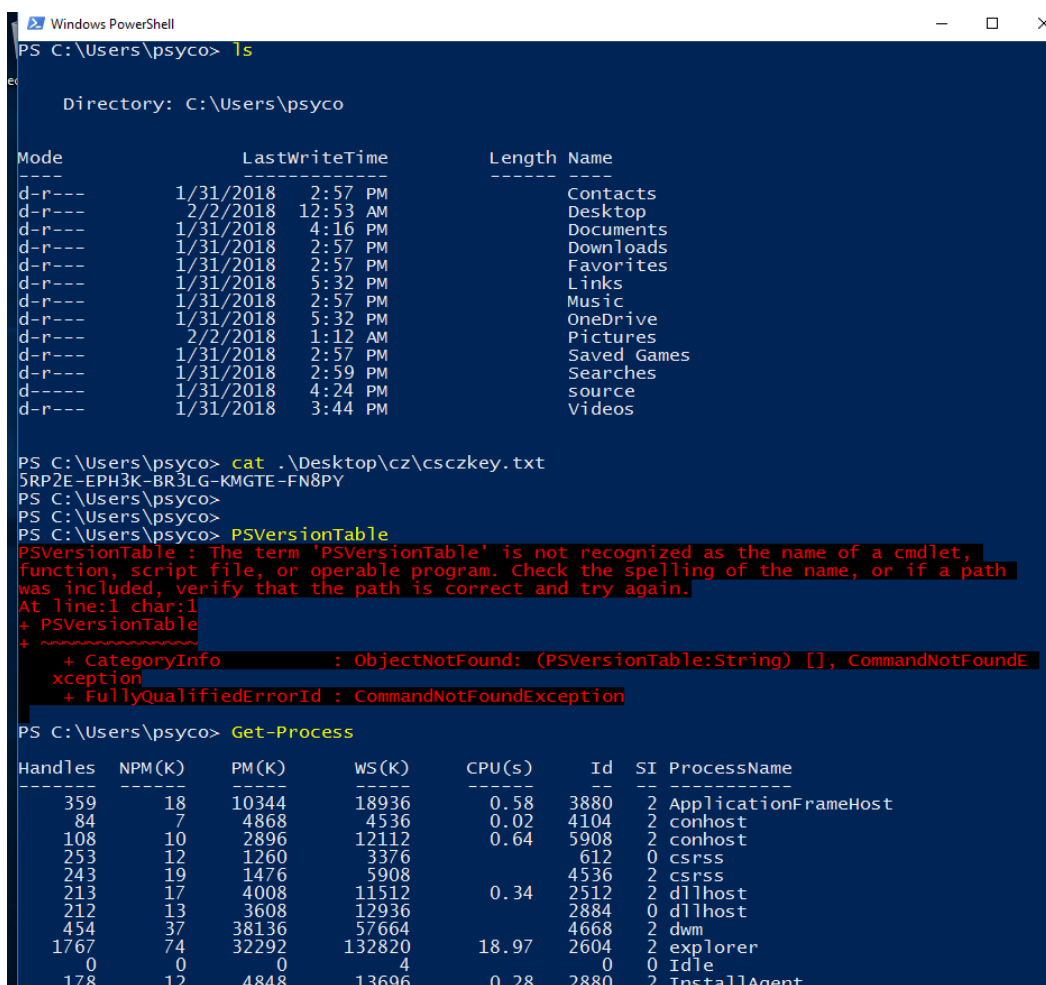
Now you can see that SSH is blocked for incoming traffic.



The screenshot shows the Windows Firewall 'Inbound Rules' list. The 'SSH' rule is highlighted in blue and has a red 'X' icon, indicating it is blocked. Other rules like 'hl.exe', 'hlds.exe', and 'AllJoyn Router' are shown with green checkmarks, indicating they are allowed. The 'Actions' pane on the right shows options like 'New Rule...', 'Filter by Profile', 'Filter by State', 'Filter by Group', 'View', 'Refresh', 'Export List...', and 'Help'.

Name	Group	Profile	Enabled
SSH		All	Yes
hl.exe		Public	Yes
hl.exe		Public	Yes
hlds.exe		Public	Yes
hlds.exe		Public	Yes
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes
App Installer	App Installer	Domai...	Yes
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No

Exploring Windows PowerShell commands



The screenshot shows a Windows PowerShell terminal window. The user runs several commands: 'ls' to list the contents of the current directory, 'cat .\Desktop\cz\csczkey.txt' to display the contents of a file, 'PSVersionTable' to show PowerShell version information (which results in an error), and 'Get-Process' to list running processes.

```
PS C:\Users\psyco> ls

Directory: C:\Users\psyco

Mode                LastWriteTime         Length Name
----                -
d-r---            1/31/2018   2:57 PM             Contacts
d-r---            2/2/2018   12:53 AM             Desktop
d-r---            1/31/2018   4:16 PM             Documents
d-r---            1/31/2018   2:57 PM             Downloads
d-r---            1/31/2018   2:57 PM             Favorites
d-r---            1/31/2018   5:32 PM             Links
d-r---            1/31/2018   2:57 PM             Music
d-r---            1/31/2018   5:32 PM             OneDrive
d-r---            2/2/2018   1:12 AM             Pictures
d-r---            1/31/2018   2:57 PM             Saved Games
d-r---            1/31/2018   2:59 PM             Searches
d-r---            1/31/2018   4:24 PM             source
d-r---            1/31/2018   3:44 PM             Videos

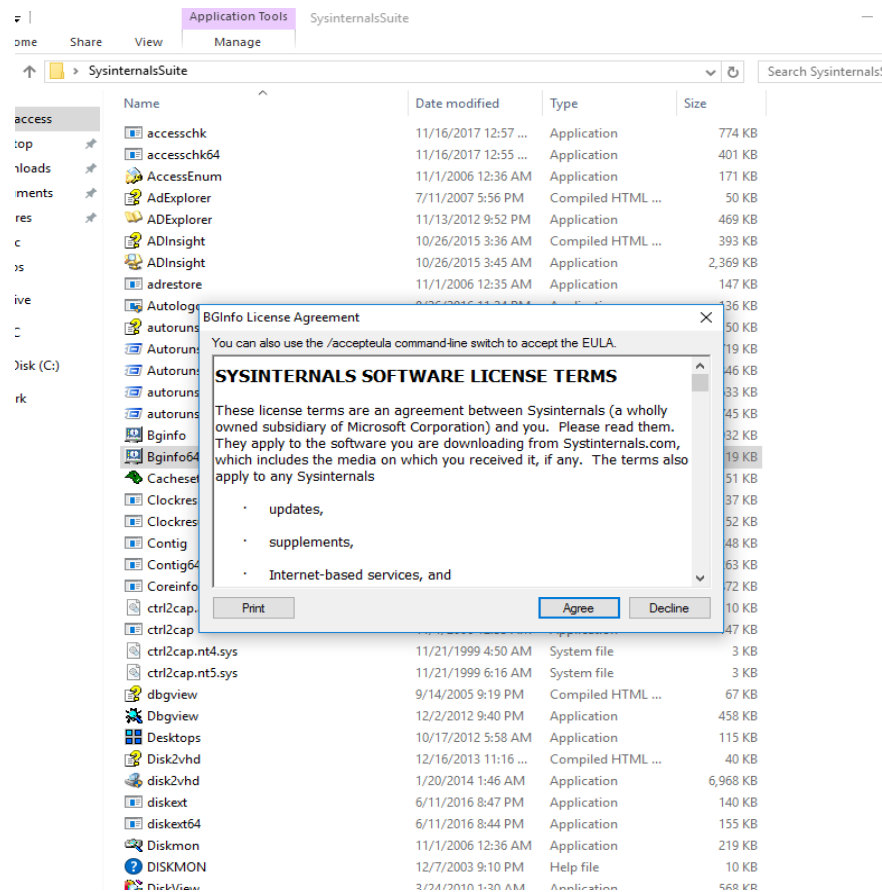
PS C:\Users\psyco> cat .\Desktop\cz\csczkey.txt
5RP2E-EPH3K-BR3LG-KMGTE-FN8PY
PS C:\Users\psyco>
PS C:\Users\psyco> PSVersionTable
PSVersionTable : The term 'PSVersionTable' is not recognized as the name of a cmdlet,
function, script file, or operable program. Check the spelling of the name, or if a path
was included, verify that the path is correct and try again.
At line:1 char:1
+ PSVersionTable
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (PSVersionTable:String) [], CommandNotFounde
xception
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\psyco> Get-Process

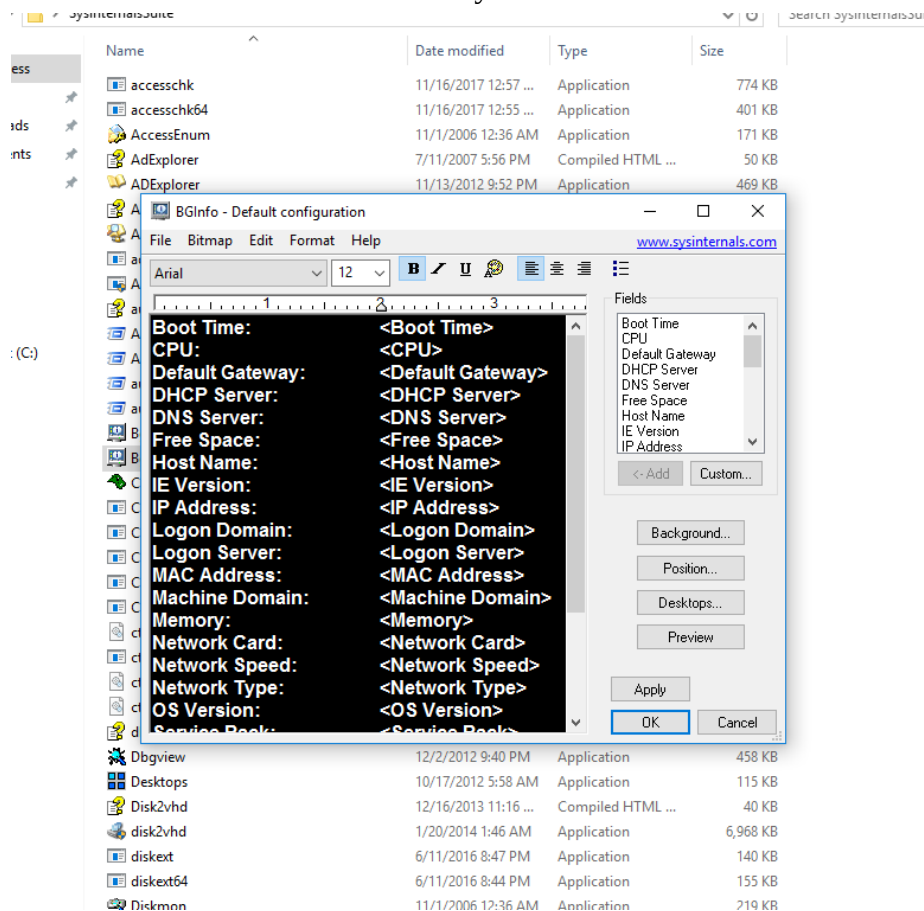
Handles   NPM(K)    PM(K)      WS(K)      CPU(s)     Id  SI ProcessName
-----
359       18     10344     18936      0.58     3880  2 ApplicationFrameHost
84         7       4868       4536      0.02     4104  2 conhost
108        10      2896     12112      0.64     5908  2 conhost
253        12       1260       3376      0.00      612  0 csrss
243        19      1476       5908      0.00     4536  2 csrss
213        17       4008     11512      0.34     2512  2 dllhost
212        13       3608     12936      0.00     2884  0 dllhost
454        37      38136     57664      0.00     4668  2 dwm
1767       74     32292    132820     18.97     2604  2 explorer
0          0         0         4         0.00      0  0 Idle
178        12       4848     13696      0.28     2880  2 InstallAgent
```

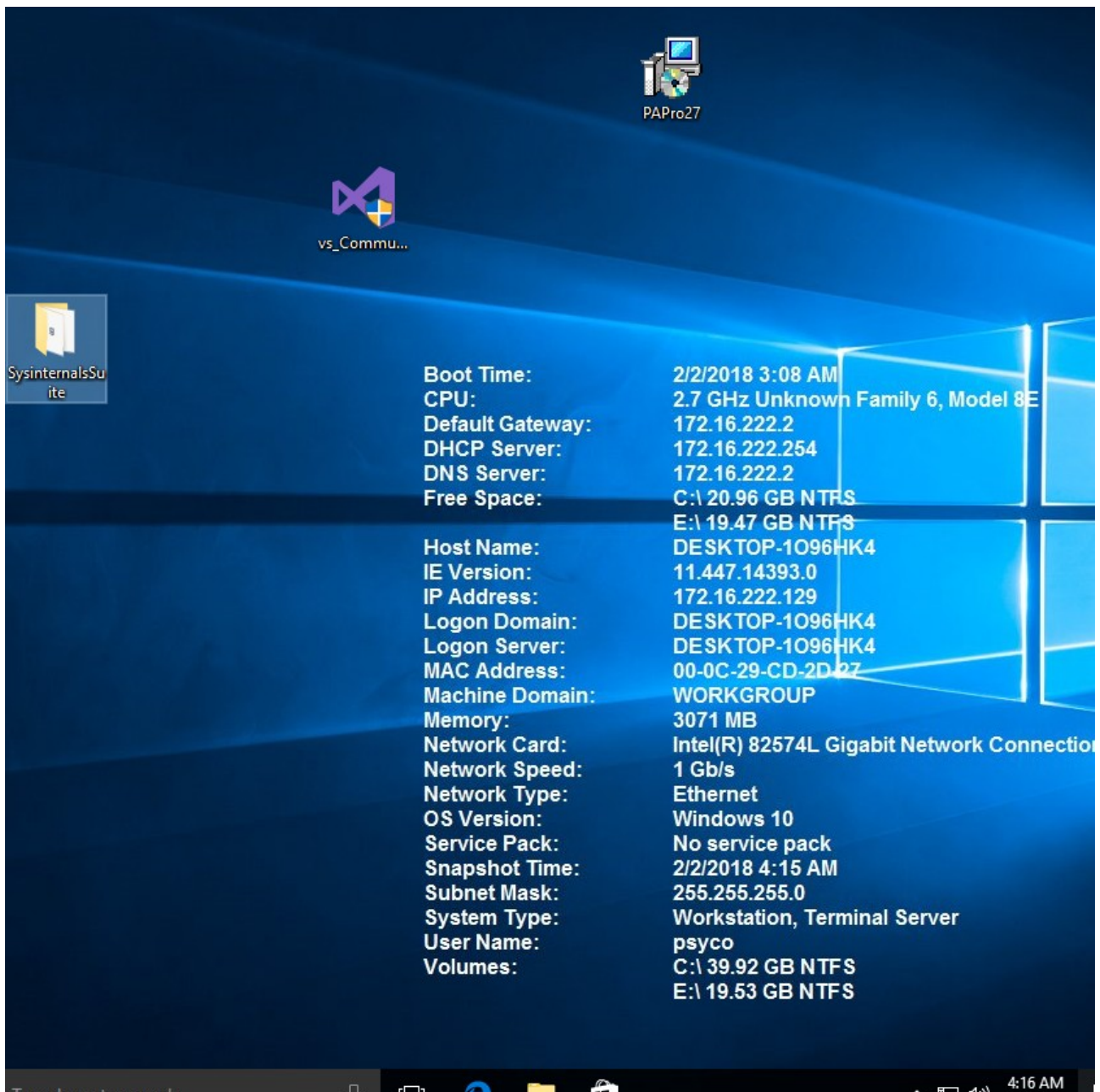
Exploring SysInternalSuite Tools

Download SysInternalSuite tools for your Windows system and try installing them by observing their purpose.



I installed BGInfo and observed what its functionality is...





System Information:

Boot Time:	2/2/2018 3:08 AM
CPU:	2.7 GHz Unknown Family 6, Model 8E
Default Gateway:	172.16.222.2
DHCP Server:	172.16.222.254
DNS Server:	172.16.222.2
Free Space:	C:\ 20.96 GB NTFS
	E:\ 19.47 GB NTFS
Host Name:	DESKTOP-1096HK4
IE Version:	11.447.14393.0
IP Address:	172.16.222.129
Logon Domain:	DESKTOP-1096HK4
Logon Server:	DESKTOP-1096HK4
MAC Address:	00-0C-29-CD-2D-07
Machine Domain:	WORKGROUP
Memory:	3071 MB
Network Card:	Intel(R) 82574L Gigabit Network Connection
Network Speed:	1 Gb/s
Network Type:	Ethernet
OS Version:	Windows 10
Service Pack:	No service pack
Snapshot Time:	2/2/2018 4:15 AM
Subnet Mask:	255.255.255.0
System Type:	Workstation, Terminal Server
User Name:	psyco
Volumes:	C:\ 39.92 GB NTFS
	E:\ 19.53 GB NTFS