PRACTICAL 7

MIHIR DEVGHARE (20162171006)

NETWORK SECURITY

Windows Sysinternals is a website that offers technical resources and utilities to manage, diagnose, troubleshoot, and monitor a Microsoft Windows environment.Originally, the Sysinternals website was created in 1996 and was operated by the company Winternals Software LP, which was located in Austin, Texas. It was started by software developers Bryce Cogswell and Mark Russinovich. On July 18, 2006, Microsoft Corporation acquired the company and its assets. Russinovich explained that Sysinternals will remain active until Microsoft agrees on a method of distributing the tools provided there. So it provides multiple tools which help to better analyze and test the current health of a network, device, application and services. Different tools are provided to get different kinds of such information.

If any suspicious activity is encountered in those tools, then the sample can be submitted to the scanning sites to get the details of the same. So as a network administrator, specify 3 such tools in each category (i.e network, process, files etc) which you think is essential for your network and device maintenance. And which can be used for troubleshooting later. Mention the details about those tools and why it is important to use in your organization. Mention the additional features that are supported by those tools.

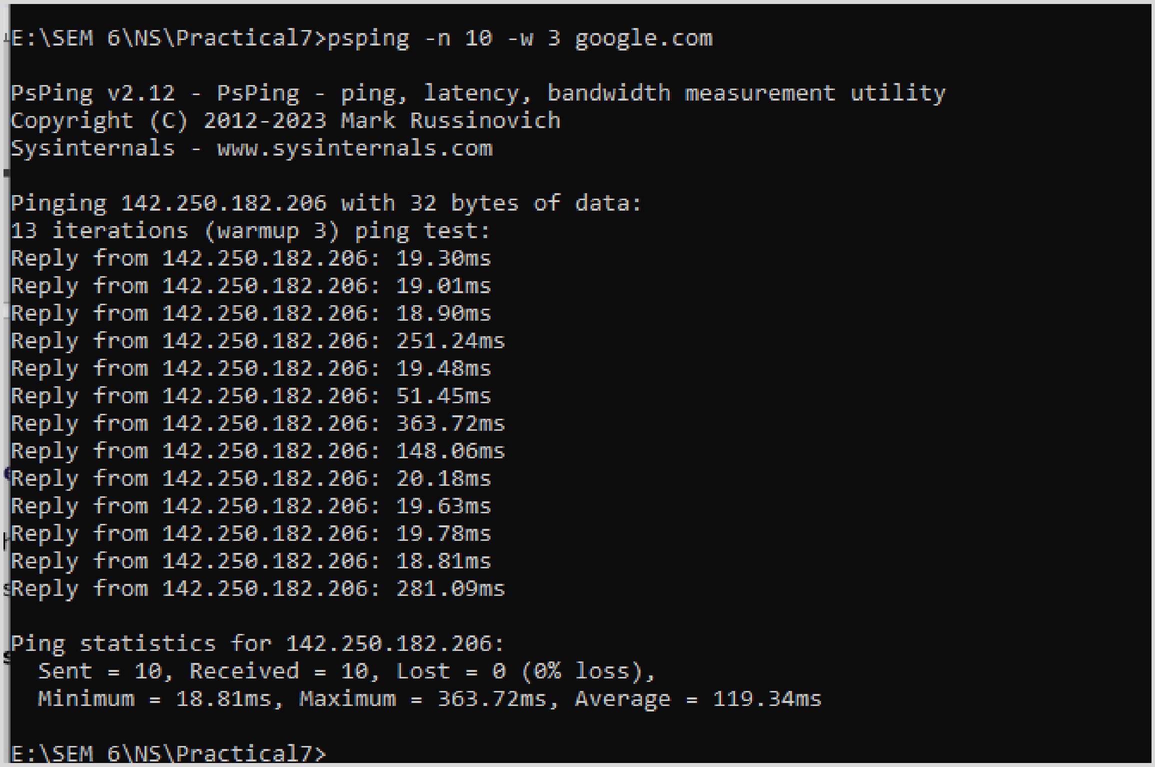
Networking Utilities

Networking utilities are useful for network administrators and IT professionals to troubleshoot the network issues, monitor network performance and manage network resources.

Following are some of tools which I have used:

PsPing: It measures network performance by sending ping requests to a target server and measuring the response time, as well as measuring TCP throughput.

Advantage: To test the latency and bandwidth of a network connection between two servers to ensure that it meets your organization's requirements. Also helpful to diagnose network issues and identify areas where performance could be improved.



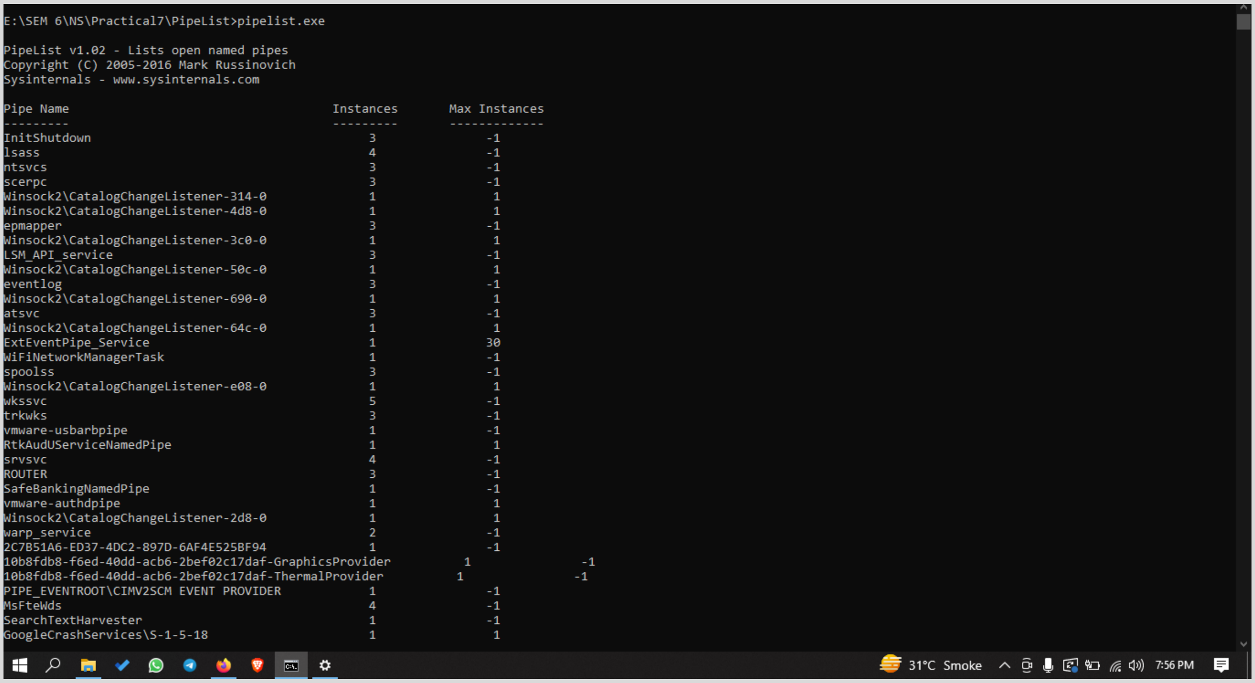
```
E:\SEM 6\NS\Practical7>psping -n 10 -w 3 google.com

PsPing v2.12 - PsPing - ping, latency, bandwidth measurement utility
Copyright (C) 2012-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

Pinging 142.250.182.206 with 32 bytes of data:
13 iterations (warmup 3) ping test:
Reply from 142.250.182.206: 19.30ms
Reply from 142.250.182.206: 19.01ms
Reply from 142.250.182.206: 18.90ms
Reply from 142.250.182.206: 251.24ms
Reply from 142.250.182.206: 19.48ms
Reply from 142.250.182.206: 51.45ms
Reply from 142.250.182.206: 363.72ms
Reply from 142.250.182.206: 148.06ms
Reply from 142.250.182.206: 20.18ms
Reply from 142.250.182.206: 19.63ms
Reply from 142.250.182.206: 19.78ms
Reply from 142.250.182.206: 18.81ms
Reply from 142.250.182.206: 281.09ms

Ping statistics for 142.250.182.206:
  Sent = 10, Received = 10, Lost = 0 (0% loss),
  Minimum = 18.81ms, Maximum = 363.72ms, Average = 119.34ms

E:\SEM 6\NS\Practical7>
```

Above, I have used the **PsPing** utility to measure the network performance, response time and the TCP throughput.

PipeList: Pipelist can display information about active named pipes, including their name, size, and the processes that are using them. It can also be used to monitor named pipe activity on a system in real-time.

Advantage: To diagnose issues related to IPC, such as deadlocks or blocked pipes, which can impact the performance of your applications.

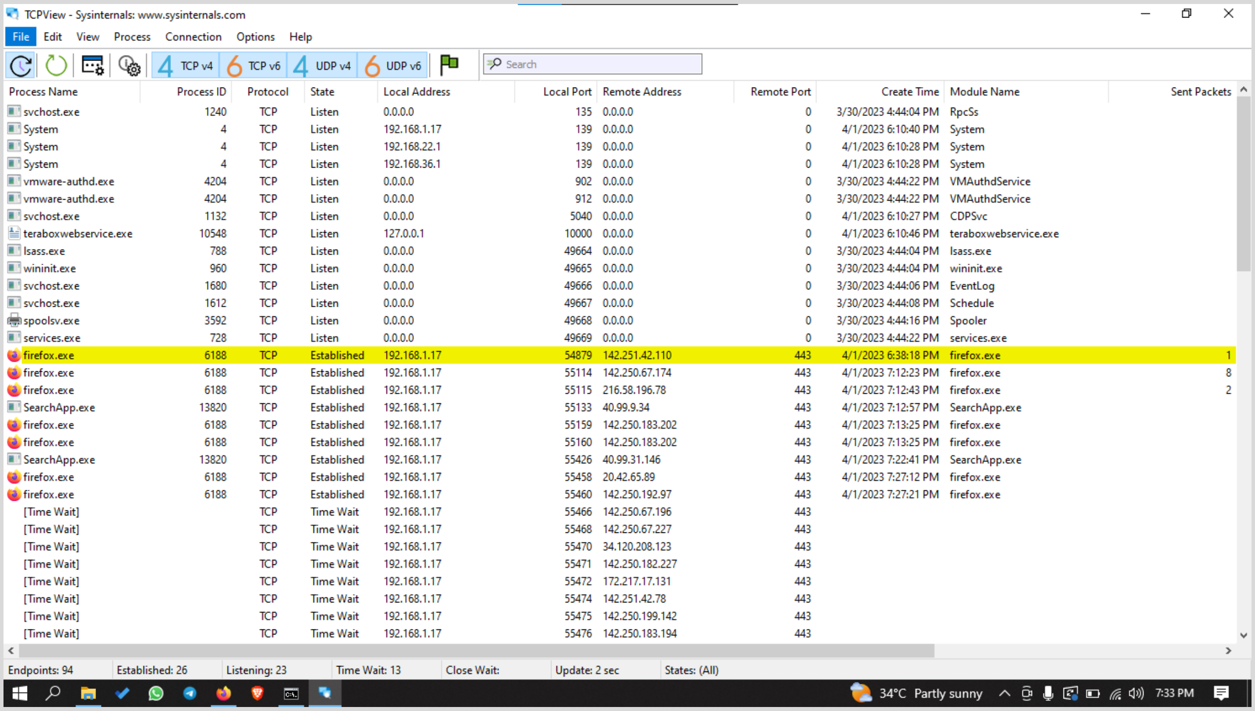
Following are the activated pipes in my system along with their names, instances used.



```
E:\SEM 6\NS\Practical7\PipeList>pipelist.exe

PipeList v1.02 - Lists open named pipes
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Pipe Name                                    Instances       Max Instances
---------                                    ---------       -------------
InitShutdown                                      3               -1
lsass                                             4               -1
ntsvcs                                            3               -1
scerpc                                            3               -1
Winsock2\CatalogChangeListener-314-0              1                1
Winsock2\CatalogChangeListener-4d8-0              1                1
epmapper                                          3               -1
Winsock2\CatalogChangeListener-3c0-0              1                1
LSM_API_service                                   3               -1
Winsock2\CatalogChangeListener-50c-0              1                1
eventlog                                          3               -1
Winsock2\CatalogChangeListener-690-0              1                1
atsvc                                             3               -1
Winsock2\CatalogChangeListener-64c-0              1                1
ExtEventPipe_Service                              1               30
WiFiNetworkManagerTask                            1               -1
spoolss                                           3               -1
Winsock2\CatalogChangeListener-e08-0              1                1
wkssvc                                            5               -1
trkwks                                            3               -1
vmware-usbarbpipe                                 1               -1
RtkAudUServiceNamedPipe                           1                1
srvsvc                                            4               -1
ROUTER                                            3               -1
SafeBankingNamedPipe                              1               -1
vmware-authdpipe                                  1                1
Winsock2\CatalogChangeListener-2d8-0              1                1
warp_service                                      2               -1
2C7B51A6-ED37-4DC2-897D-6AF4E525BF94              1               -1
10b8fdb8-f6ed-40dd-acb6-2bef02c17daf-GraphicsProvider          1               -1
10b8fdb8-f6ed-40dd-acb6-2bef02c17daf-ThermalProvider          1               -1
PIPE_EVENTROOT\CIMV2SCM EVENT PROVIDER            1               -1
MsFteWds                                          4               -1
SearchTextHarvester                               1               -1
GoogleCrashServices\S-1-5-18                      1                1
```

TCPView: This application displays the real-time information about active TCP and UDP connections on a Windows Computer. The information provided is detailed [PID, Process name, local and remote IP Address, port number and status of connection]. TCPView also allows you to close individual connections, as well as terminate the process that is associated with a particular connection. This tool can be useful for troubleshooting network connectivity issues and identifying network-related performance problems.

Advantage: To identify suspicious network activity or connections that could be causing performance degradation.

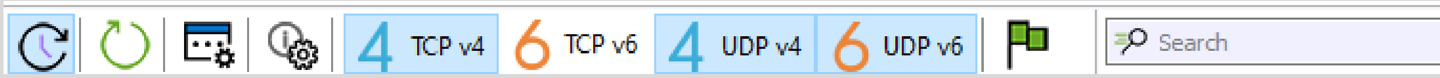

TCPView - Sysinternals: www.sysinternals.com
File Edit View Process Connection Options Help
4 TCP v4
6 TCP v6
4 UDP v4
6 UDP v6
Search

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets
svchost.exe	1240	TCP	Listen	0.0.0.0	135	0.0.0.0	0	3/30/2023 4:44:04 PM	RpcSs	
System	4	TCP	Listen	192.168.1.17	139	0.0.0.0	0	4/1/2023 6:10:40 PM	System	
System	4	TCP	Listen	192.168.22.1	139	0.0.0.0	0	4/1/2023 6:10:28 PM	System	
System	4	TCP	Listen	192.168.36.1	139	0.0.0.0	0	4/1/2023 6:10:28 PM	System	
vmware-authd.exe	4204	TCP	Listen	0.0.0.0	902	0.0.0.0	0	3/30/2023 4:44:22 PM	VMAuthdService	
vmware-authd.exe	4204	TCP	Listen	0.0.0.0	912	0.0.0.0	0	3/30/2023 4:44:22 PM	VMAuthdService	
svchost.exe	1132	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	4/1/2023 6:10:27 PM	CDPSvc	
teraboxwebservice.exe	10548	TCP	Listen	127.0.0.1	10000	0.0.0.0	0	4/1/2023 6:10:46 PM	teraboxwebservice.exe	
lsass.exe	788	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	3/30/2023 4:44:04 PM	lsass.exe	
wininit.exe	960	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	3/30/2023 4:44:04 PM	wininit.exe	
svchost.exe	1680	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	3/30/2023 4:44:06 PM	EventLog	
svchost.exe	1612	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	3/30/2023 4:44:08 PM	Schedule	
spoolsv.exe	3592	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	3/30/2023 4:44:16 PM	Spooler	
services.exe	728	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	3/30/2023 4:44:22 PM	services.exe	
firefox.exe	6188	TCP	Established	192.168.1.17	54879	142.251.42.110	443	4/1/2023 6:38:18 PM	firefox.exe	1
firefox.exe	6188	TCP	Established	192.168.1.17	55114	142.250.67.174	443	4/1/2023 7:12:23 PM	firefox.exe	8
firefox.exe	6188	TCP	Established	192.168.1.17	55115	216.58.196.78	443	4/1/2023 7:12:43 PM	firefox.exe	2
SearchApp.exe	13820	TCP	Established	192.168.1.17	55133	40.99.9.34	443	4/1/2023 7:12:57 PM	SearchApp.exe	
firefox.exe	6188	TCP	Established	192.168.1.17	55159	142.250.183.202	443	4/1/2023 7:13:25 PM	firefox.exe	
firefox.exe	6188	TCP	Established	192.168.1.17	55160	142.250.183.202	443	4/1/2023 7:13:25 PM	firefox.exe	
SearchApp.exe	13820	TCP	Established	192.168.1.17	55426	40.99.31.146	443	4/1/2023 7:22:41 PM	SearchApp.exe	
firefox.exe	6188	TCP	Established	192.168.1.17	55458	20.42.65.89	443	4/1/2023 7:27:12 PM	firefox.exe	
firefox.exe	6188	TCP	Established	192.168.1.17	55460	142.250.192.97	443	4/1/2023 7:27:21 PM	firefox.exe	
[Time Wait]		TCP	Time Wait	192.168.1.17	55466	142.250.67.196	443			
[Time Wait]		TCP	Time Wait	192.168.1.17	55468	142.250.67.227	443			
[Time Wait]		TCP	Time Wait	192.168.1.17	55470	34.120.208.123	443			
[Time Wait]		TCP	Time Wait	192.168.1.17	55471	142.250.182.227	443			
[Time Wait]		TCP	Time Wait	192.168.1.17	55472	172.217.17.131	443			
[Time Wait]		TCP	Time Wait	192.168.1.17	55474	142.251.42.78	443			
[Time Wait]		TCP	Time Wait	192.168.1.17	55475	142.250.199.142	443			
[Time Wait]		TCP	Time Wait	192.168.1.17	55476	142.250.183.194	443			

Endpoints: 94 Established: 26 Listening: 23 Time Wait: 13 Close Wait: Update: 2 sec States: (All)

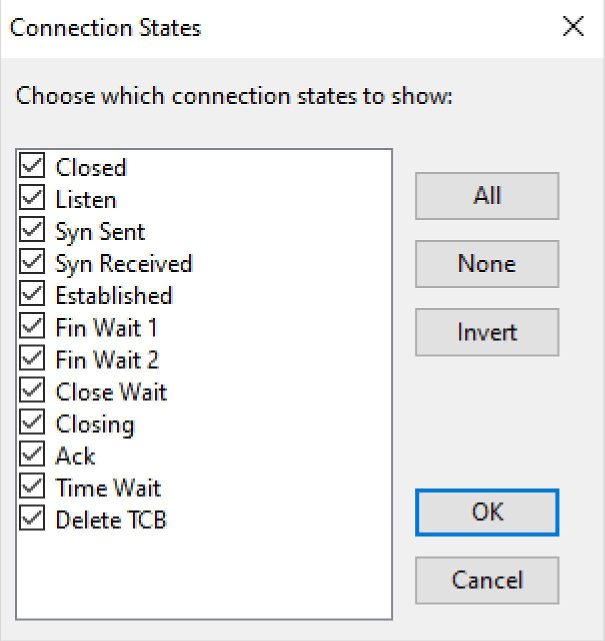
Above we can see the processes name, process ID, Protocol Used, State, Local Address, Local Port, Remote Address, Remote port, Create Time, Send and Receive Packets and Bytes.

Above, we can see the firefox.exe having PID is highlighted with yellow color. Here color plays some role. Yellow means the endpoint has changed its state from one update to another, Red means the endpoints have been deleted and Green means new endpoints.



Above are the options via which we can filter content.

1. Pause/resume the monitoring
2. Refresh the content
3. Resolve Address
4. Properties of process
5. There are 4 options, we can choose which protocol and version packet we need to capture and monitor
6. Then there is a green flag which states the filter. By selecting it we can customize the content:

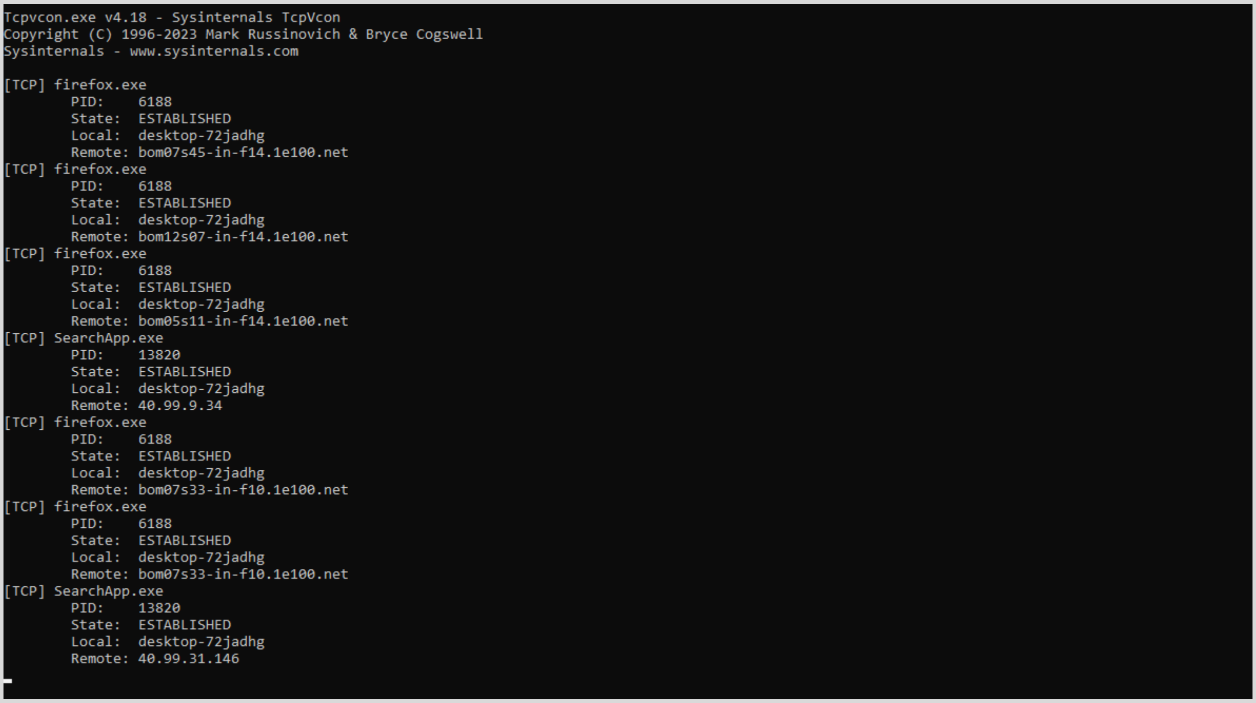

Connection States

Choose which connection states to show:

☑ Closed
☑ Listen
☑ Syn Sent
☑ Syn Received
☑ Established
☑ Fin Wait 1
☑ Fin Wait 2
☑ Close Wait
☑ Closing
☑ Ack
☑ Time Wait
☑ Delete TCB

7. Then there comes the search option.

Below is the CLI view.

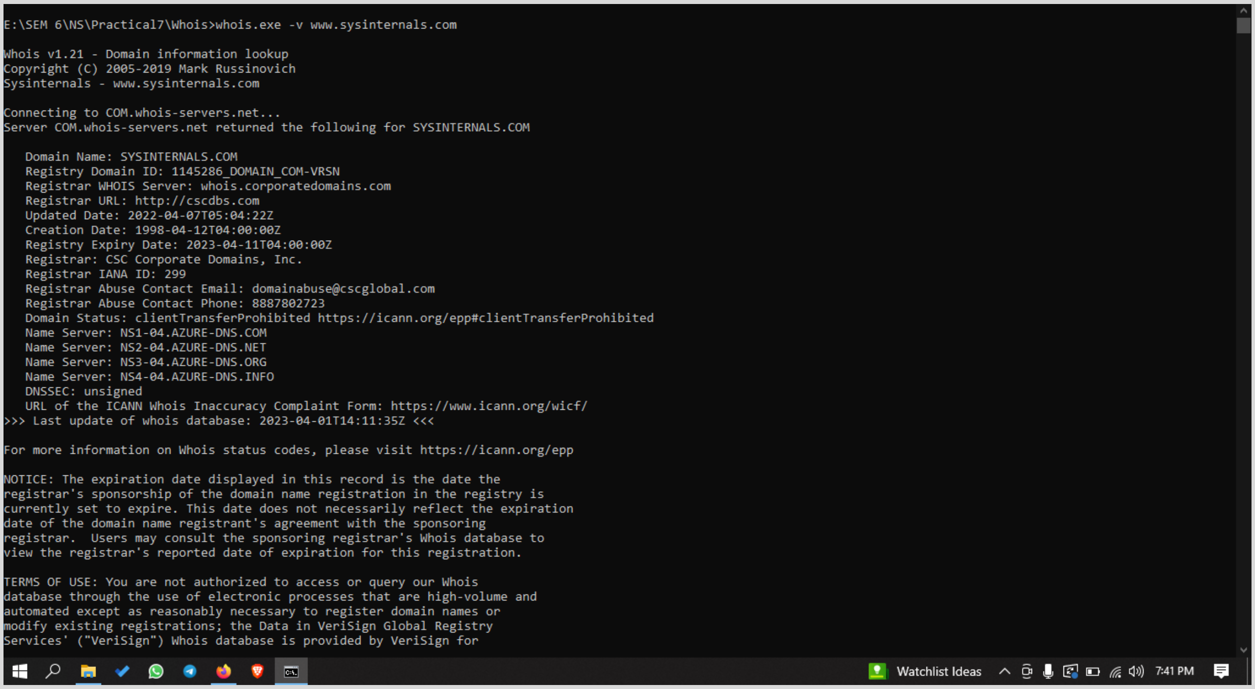


```
Tcpvcon.exe v4.18 - Sysinternals TcpVcon
Copyright (C) 1996-2023 Mark Russinovich & Bryce Cogswell
Sysinternals - www.sysinternals.com

[TCP] firefox.exe
        PID:    6188
        State:  ESTABLISHED
        Local:  desktop-72jadhg
        Remote: bom07s45-in-f14.1e100.net
[TCP] firefox.exe
        PID:    6188
        State:  ESTABLISHED
        Local:  desktop-72jadhg
        Remote: bom12s07-in-f14.1e100.net
[TCP] firefox.exe
        PID:    6188
        State:  ESTABLISHED
        Local:  desktop-72jadhg
        Remote: bom05s11-in-f14.1e100.net
[TCP] SearchApp.exe
        PID:    13820
        State:  ESTABLISHED
        Local:  desktop-72jadhg
        Remote: 40.99.9.34
[TCP] firefox.exe
        PID:    6188
        State:  ESTABLISHED
        Local:  desktop-72jadhg
        Remote: bom07s33-in-f10.1e100.net
[TCP] firefox.exe
        PID:    6188
        State:  ESTABLISHED
        Local:  desktop-72jadhg
        Remote: bom07s33-in-f10.1e100.net
[TCP] SearchApp.exe
        PID:    13820
        State:  ESTABLISHED
        Local:  desktop-72jadhg
        Remote: 40.99.31.146
```

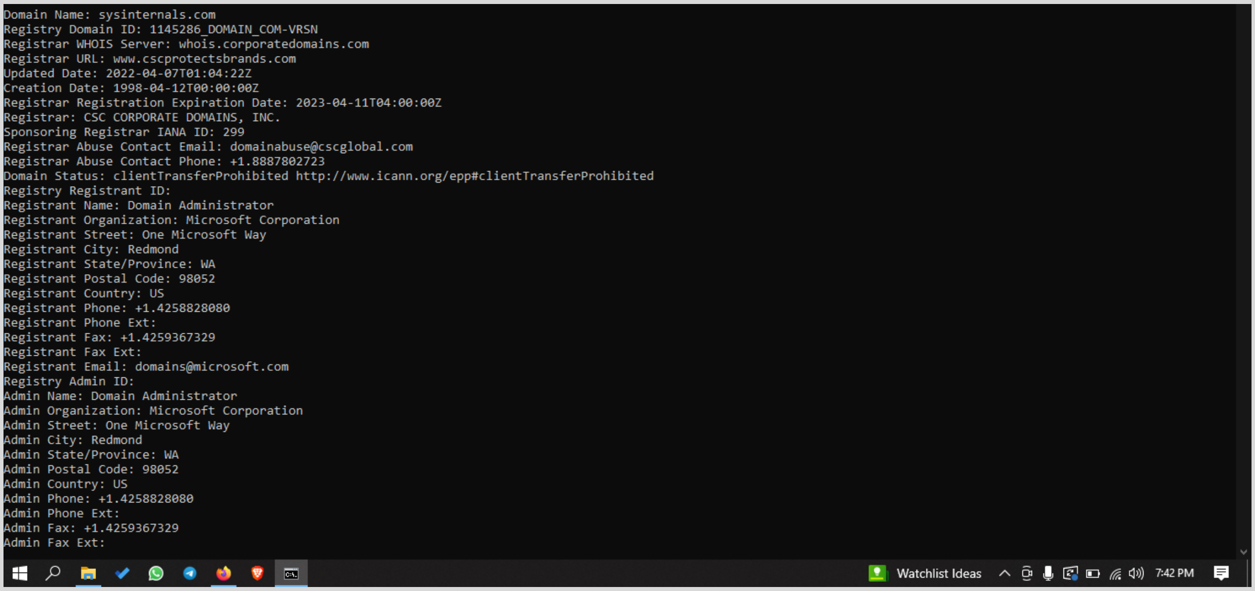
Whois: Whois is a networking utility available in Sysinternals, which allows you to look up information about a domain name or an IP address. It queries the appropriate WHOIS server to retrieve the registration information for the domain or IP address, such as the name and contact information of the owner, the registration date, and the expiration date.

Whois can also be used for troubleshooting network problems, such as identifying the owner of a suspicious domain name or tracking down the source of spam or phishing emails.

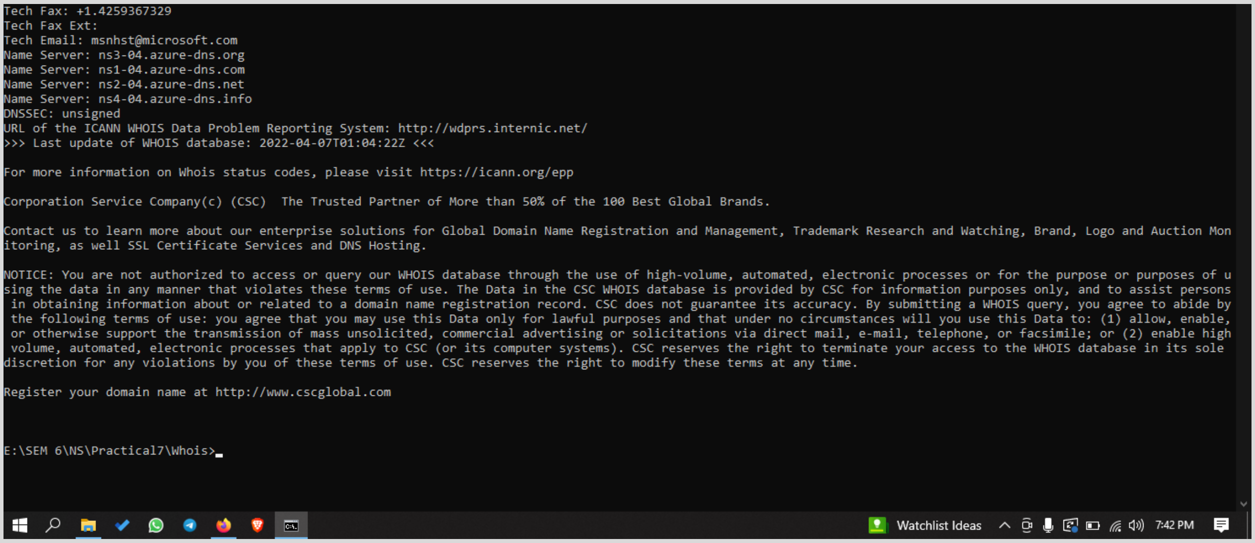
Advantage: Useful for identifying the owner of a domain, verifying the domain's registration status, and identifying the domain's name servers. For example, you could use Whois to investigate a domain name associated with suspicious network activity to identify its owner and contact them to address the issue.



```
E:\SEM 6\NS\Practical7\Whois>whois.exe -v www.sysinternals.com

Whois v1.21 - Domain information lookup
Copyright (C) 2005-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting to COM.whois-servers.net...
Server COM.whois-servers.net returned the following for SYSINTERNALS.COM

   Domain Name: SYSINTERNALS.COM
   Registry Domain ID: 1145286_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.corporatedomains.com
   Registrar URL: http://cscdbs.com
   Updated Date: 2022-04-07T05:04:22Z
   Creation Date: 1998-04-12T04:00:00Z
   Registry Expiry Date: 2023-04-11T04:00:00Z
   Registrar: CSC Corporate Domains, Inc.
   Registrar IANA ID: 299
   Registrar Abuse Contact Email: domainabuse@cscglobal.com
   Registrar Abuse Contact Phone: 8887802723
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: NS1-04.AZURE-DNS.COM
   Name Server: NS2-04.AZURE-DNS.NET
   Name Server: NS3-04.AZURE-DNS.ORG
   Name Server: NS4-04.AZURE-DNS.INFO
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-04-01T14:11:35Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
```



```
Domain Name: sysinternals.com
Registry Domain ID: 1145286_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2022-04-07T01:04:22Z
Creation Date: 1998-04-12T00:00:00Z
Registrar Registration Expiration Date: 2023-04-11T04:00:00Z
Registrar: CSC CORPORATE DOMAINS, INC.
Sponsoring Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Microsoft Corporation
Registrant Street: One Microsoft Way
Registrant City: Redmond
Registrant State/Province: WA
Registrant Postal Code: 98052
Registrant Country: US
Registrant Phone: +1.4258828080
Registrant Phone Ext:
Registrant Fax: +1.4259367329
Registrant Fax Ext:
Registrant Email: domains@microsoft.com
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: Microsoft Corporation
Admin Street: One Microsoft Way
Admin City: Redmond
Admin State/Province: WA
Admin Postal Code: 98052
Admin Country: US
Admin Phone: +1.4258828080
Admin Phone Ext:
Admin Fax: +1.4259367329
Admin Fax Ext:
```



```
Tech Fax: +1.4259367329
Tech Fax Ext:
Tech Email: msnhst@microsoft.com
Name Server: ns3-04.azure-dns.org
Name Server: ns1-04.azure-dns.com
Name Server: ns2-04.azure-dns.net
Name Server: ns4-04.azure-dns.info
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2022-04-07T01:04:22Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

Corporation Service Company(c) (CSC)  The Trusted Partner of More than 50% of the 100 Best Global Brands.

Contact us to learn more about our enterprise solutions for Global Domain Name Registration and Management, Trademark Research and Watching, Brand, Logo and Auction Mon
itoring, as well SSL Certificate Services and DNS Hosting.

NOTICE: You are not authorized to access or query our WHOIS database through the use of high-volume, automated, electronic processes or for the purpose or purposes of u
sing the data in any manner that violates these terms of use. The Data in the CSC WHOIS database is provided by CSC for information purposes only, and to assist persons
 in obtaining information about or related to a domain name registration record. CSC does not guarantee its accuracy. By submitting a WHOIS query, you agree to abide by
 the following terms of use: you agree that you may use this Data only for lawful purposes and that under no circumstances will you use this Data to: (1) allow, enable,
 or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via direct mail, e-mail, telephone, or facsimile; or (2) enable high
 volume, automated, electronic processes that apply to CSC (or its computer systems). CSC reserves the right to terminate your access to the WHOIS database in its sole
discretion for any violations by you of these terms of use. CSC reserves the right to modify these terms at any time.

Register your domain name at http://www.cscglobal.com


E:\SEM 6\NS\Practical7\Whois>
```

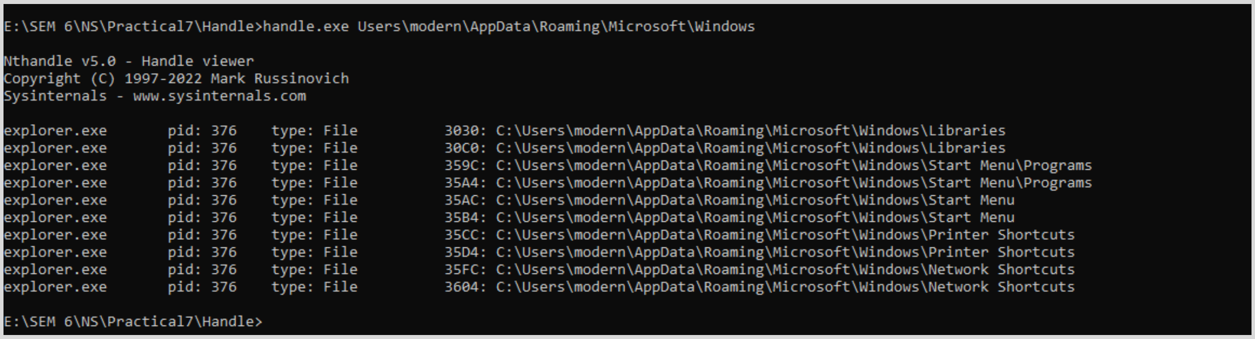
Process Utilities

Process Utilities are useful for system administrators, developers, and security professionals to troubleshoot performance issues, identify process-related problems and diagnose system crashes.

Following are some of the tools which I have used:

Handle: Handle is used to view and manage all open handles (or file references) for any process running in the system. A handle is a unique identifier assigned by the operating system to any file or object that is opened by a process.

Advantages: Tracking down file and registry leaks, as well as diagnosing handle leaks in a particular process. This can help organizations identify potential security vulnerabilities and optimize system performance.

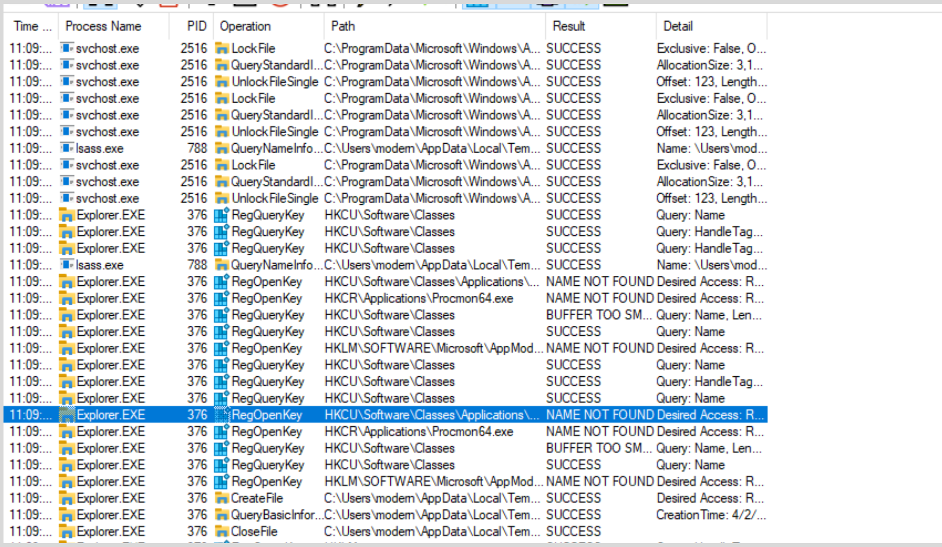


```
E:\SEM 6\NS\Practical7\Handle>handle.exe Users\modern\AppData\Roaming\Microsoft\Windows

Nthandle v5.0 - Handle viewer
Copyright (C) 1997-2022 Mark Russinovich
Sysinternals - www.sysinternals.com

explorer.exe       pid: 376    type: File          3030: C:\Users\modern\AppData\Roaming\Microsoft\Windows\Libraries
explorer.exe       pid: 376    type: File          30C0: C:\Users\modern\AppData\Roaming\Microsoft\Windows\Libraries
explorer.exe       pid: 376    type: File          359C: C:\Users\modern\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
explorer.exe       pid: 376    type: File          35A4: C:\Users\modern\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
explorer.exe       pid: 376    type: File          35AC: C:\Users\modern\AppData\Roaming\Microsoft\Windows\Start Menu
explorer.exe       pid: 376    type: File          35B4: C:\Users\modern\AppData\Roaming\Microsoft\Windows\Start Menu
explorer.exe       pid: 376    type: File          35CC: C:\Users\modern\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
explorer.exe       pid: 376    type: File          35D4: C:\Users\modern\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
explorer.exe       pid: 376    type: File          35FC: C:\Users\modern\AppData\Roaming\Microsoft\Windows\Network Shortcuts
explorer.exe       pid: 376    type: File          3604: C:\Users\modern\AppData\Roaming\Microsoft\Windows\Network Shortcuts

E:\SEM 6\NS\Practical7\Handle>
```

Above, we can see the handles [files here] which are opened in **C:\Users\modern\AppData\Roaming\Microsoft\Windows** along with their process id, type, location etc.

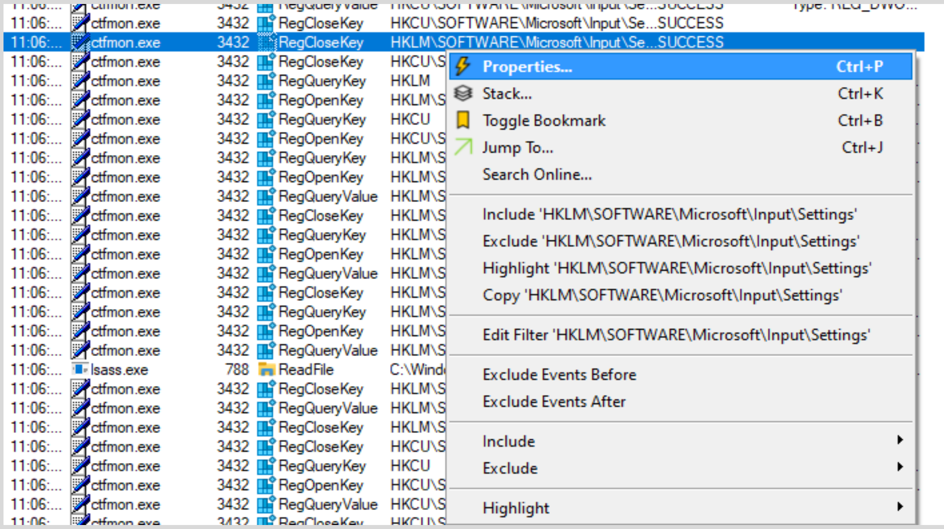
Process Monitor: It is a real-time monitoring tool that captures and displays all the system events and process-related activities, including file system and registry changes, network activity, and process information

Advantages: Troubleshooting issues with application or system performance and security, as well as detecting malware and other malicious activity.



Time ...	Process Name	PID	Operation	Path	Result	Detail
11:09:...	svchost.exe	2516	LockFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
11:09:...	svchost.exe	2516	QueryStandardI...	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	AllocationSize: 3,1...
11:09:...	svchost.exe	2516	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 123, Length...
11:09:...	svchost.exe	2516	LockFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
11:09:...	svchost.exe	2516	QueryStandardI...	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	AllocationSize: 3,1...
11:09:...	svchost.exe	2516	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 123, Length...
11:09:...	lsass.exe	788	QueryNameInfo...	C:\Users\modem\AppData\Local\Tem...	SUCCESS	Name: \Users\mod...
11:09:...	svchost.exe	2516	LockFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
11:09:...	svchost.exe	2516	QueryStandardI...	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	AllocationSize: 3,1...
11:09:...	svchost.exe	2516	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 123, Length...
11:09:...	Explorer.EXE	376	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
11:09:...	Explorer.EXE	376	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
11:09:...	Explorer.EXE	376	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
11:09:...	lsass.exe	788	QueryNameInfo...	C:\Users\modem\AppData\Local\Tem...	SUCCESS	Name: \Users\mod...
11:09:...	Explorer.EXE	376	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: R...
11:09:...	Explorer.EXE	376	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
11:09:...	Explorer.EXE	376	RegQueryKey	HKCU\Software\Classes	BUFFER TOO SM...	Query: Name, Len...
11:09:...	Explorer.EXE	376	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
11:09:...	Explorer.EXE	376	RegOpenKey	HKLM\SOFTWARE\Microsoft\AppMod...	NAME NOT FOUND	Desired Access: R...
11:09:...	Explorer.EXE	376	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
11:09:...	Explorer.EXE	376	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
11:09:...	Explorer.EXE	376	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
11:09:...	Explorer.EXE	376	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: R...
11:09:...	Explorer.EXE	376	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
11:09:...	Explorer.EXE	376	RegQueryKey	HKCU\Software\Classes	BUFFER TOO SM...	Query: Name, Len...
11:09:...	Explorer.EXE	376	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
11:09:...	Explorer.EXE	376	RegOpenKey	HKLM\SOFTWARE\Microsoft\AppMod...	NAME NOT FOUND	Desired Access: R...
11:09:...	Explorer.EXE	376	CreateFile	C:\Users\modem\AppData\Local\Tem...	SUCCESS	Desired Access: R...
11:09:...	Explorer.EXE	376	QueryBasicInfor...	C:\Users\modem\AppData\Local\Tem...	SUCCESS	CreationTime: 4/2/...
11:09:...	Explorer.EXE	376	CloseFile	C:\Users\modem\AppData\Local\Tem...	SUCCESS	

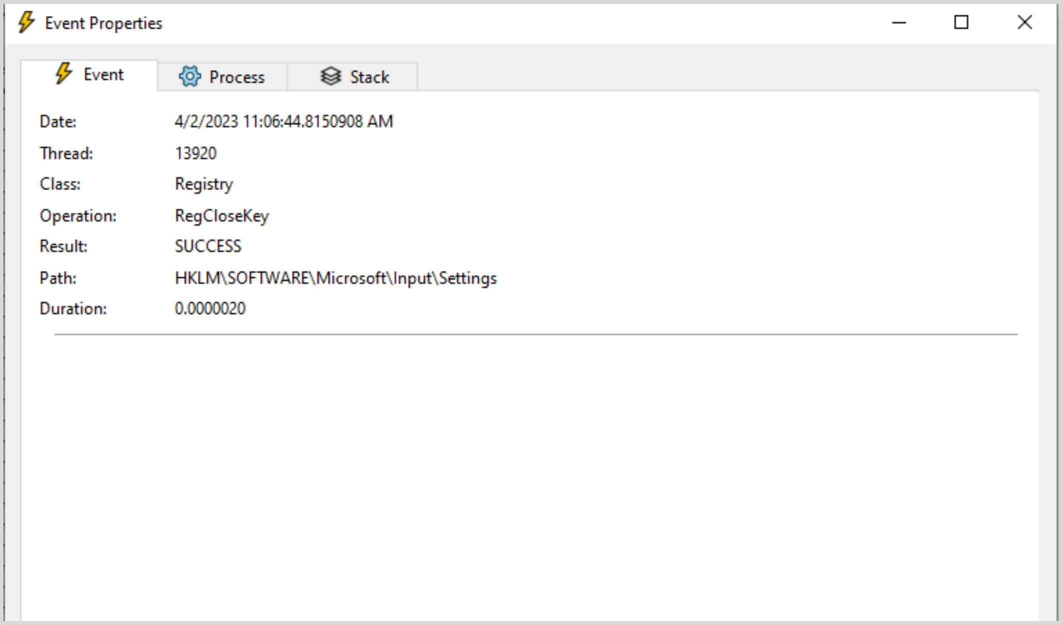
Above we can see the information which is related to the real-time process of my system. We can see the time, name, ID, path, result and all the details.



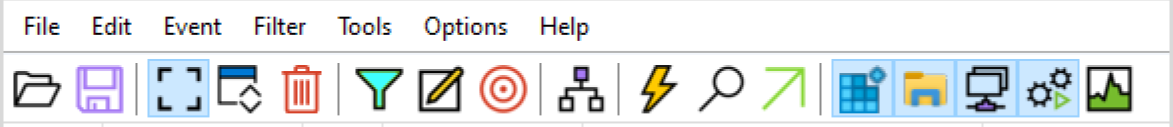
11:06:...	ctfmon.exe	3432	RegCloseKey	HKCU\SOFTWARE\Microsoft\Input\Se...	SUCCESS
11:06:...	ctfmon.exe	3432	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS
11:06:...	ctfmon.exe	3432	RegCloseKey	HKCU\S	
11:06:...	ctfmon.exe	3432	RegQueryKey	HKLM	
11:06:...	ctfmon.exe	3432	RegOpenKey	HKLM\S	
11:06:...	ctfmon.exe	3432	RegQueryKey	HKCU	
11:06:...	ctfmon.exe	3432	RegOpenKey	HKCU\S	
11:06:...	ctfmon.exe	3432	RegQueryKey	HKLM\S	
11:06:...	ctfmon.exe	3432	RegOpenKey	HKLM\S	
11:06:...	ctfmon.exe	3432	RegQueryValue	HKLM\S	
11:06:...	ctfmon.exe	3432	RegCloseKey	HKLM\S	
11:06:...	ctfmon.exe	3432	RegQueryKey	HKLM\S	
11:06:...	ctfmon.exe	3432	RegOpenKey	HKLM\S	
11:06:...	ctfmon.exe	3432	RegQueryValue	HKLM\S	
11:06:...	ctfmon.exe	3432	RegCloseKey	HKLM\S	
11:06:...	ctfmon.exe	3432	RegQueryKey	HKLM\S	
11:06:...	ctfmon.exe	3432	RegOpenKey	HKLM\S	
11:06:...	ctfmon.exe	3432	RegQueryValue	HKLM\S	
11:06:...	lsass.exe	788	ReadFile	C:\Wind	
11:06:...	ctfmon.exe	3432	RegCloseKey	HKLM\S	
11:06:...	ctfmon.exe	3432	RegQueryValue	HKLM\S	
11:06:...	ctfmon.exe	3432	RegCloseKey	HKLM\S	
11:06:...	ctfmon.exe	3432	RegCloseKey	HKCU\S	
11:06:...	ctfmon.exe	3432	RegQueryKey	HKCU	
11:06:...	ctfmon.exe	3432	RegOpenKey	HKCU\S	
11:06:...	ctfmon.exe	3432	RegQueryValue	HKCU\S	

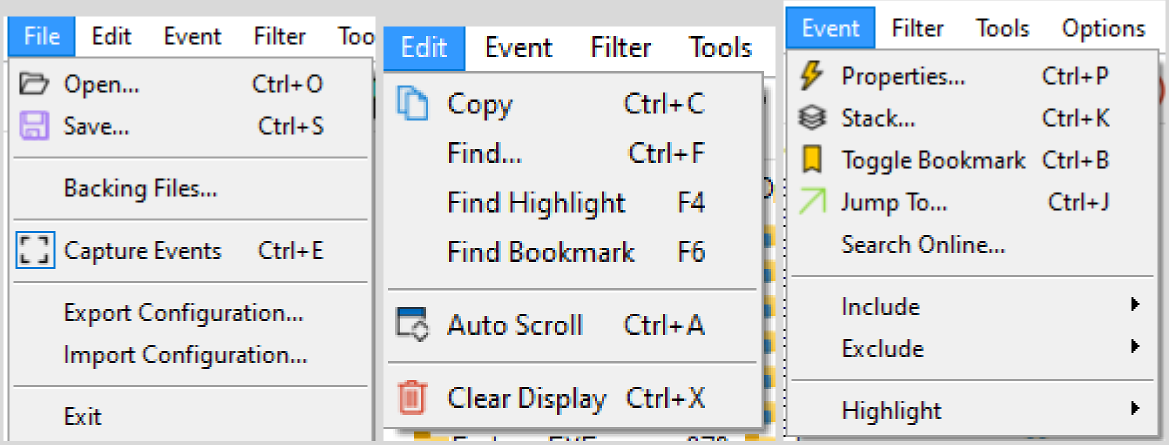
Properties... Ctrl+P
Stack... Ctrl+K
Toggle Bookmark Ctrl+B
Jump To... Ctrl+J
Search Online...
Include 'HKLM\SOFTWARE\Microsoft\Input\Settings'
Exclude 'HKLM\SOFTWARE\Microsoft\Input\Settings'
Highlight 'HKLM\SOFTWARE\Microsoft\Input\Settings'
Copy 'HKLM\SOFTWARE\Microsoft\Input\Settings'
Edit Filter 'HKLM\SOFTWARE\Microsoft\Input\Settings'
Exclude Events Before
Exclude Events After
Include
Exclude
Highlight

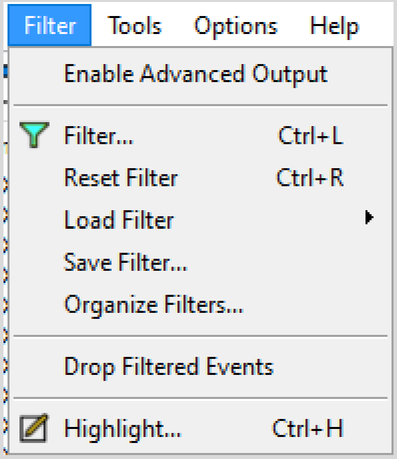
On right clicking any process, we get various options which we can see in the above screenshot. And in the below screenshot, we can see the properties of that event. Similarly, on clicking the process tab we get the information about the process like PID, user who owns that process etc and the Stack tab shows the call stack for the process, including all the functions that were called and their parameters

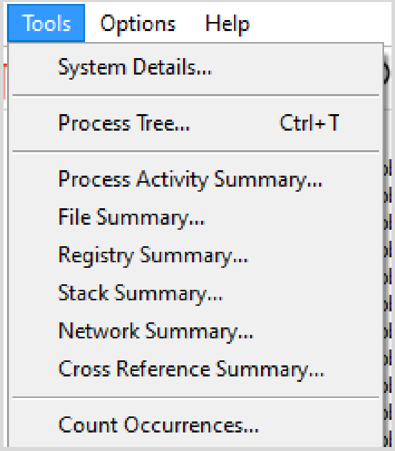


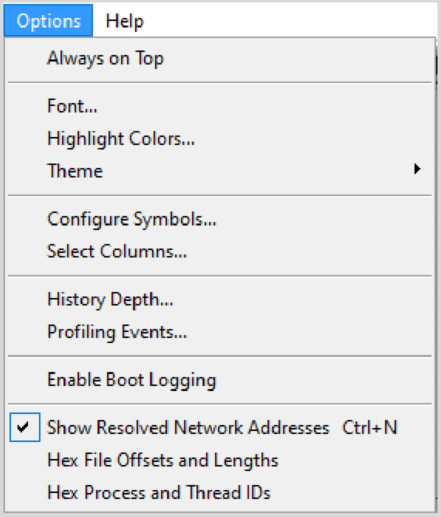
Date: 4/2/2023 11:06:44.8150908 AM
Thread: 13920
Class: Registry
Operation: RegCloseKey
Result: SUCCESS
Path: HKLM\SOFTWARE\Microsoft\Input\Settings
Duration: 0.0000020











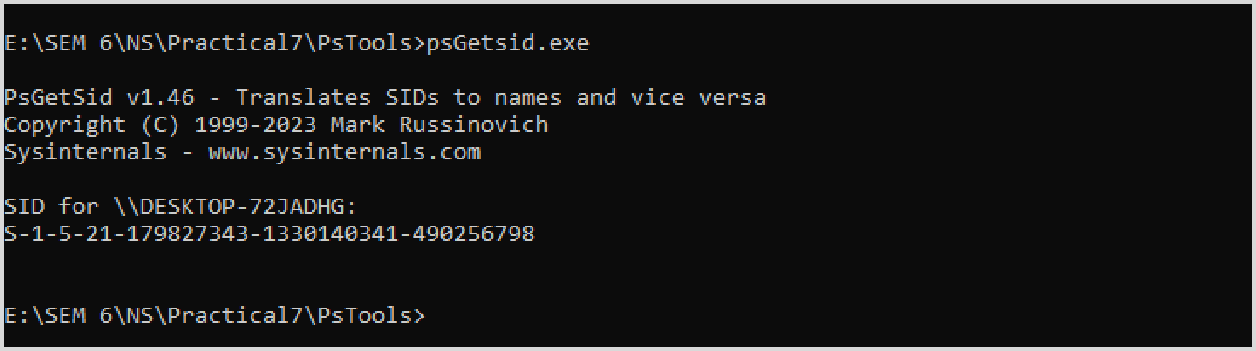
Include Process from Windows

Process Tree

We can filter what we want to see like to see only registry Activity or File system or network or process and thread activity or profiling events respectively.

PsGetSid: It is a tool that displays the SID (Security Identifier) of a local or remote machine or a user account. The SID is a unique identifier for security principals, including users, groups, and computers, that is used in Windows security and access control mechanisms.

Advantages: For auditing and managing security permissions on a network.

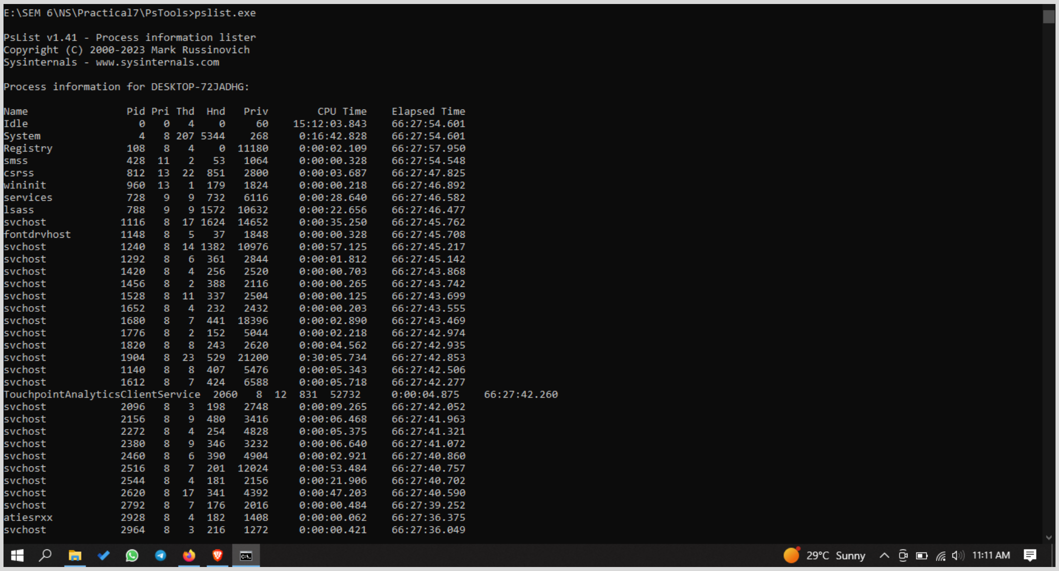


```
E:\SEM 6\NS\Practical7\PsTools>psGetsid.exe

PsGetSid v1.46 - Translates SIDs to names and vice versa
Copyright (C) 1999-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

SID for \\DESKTOP-72JADHG:
S-1-5-21-179827343-1330140341-490256798


E:\SEM 6\NS\Practical7\PsTools>
```

In the above screenshot we can see the SID number of my machine.

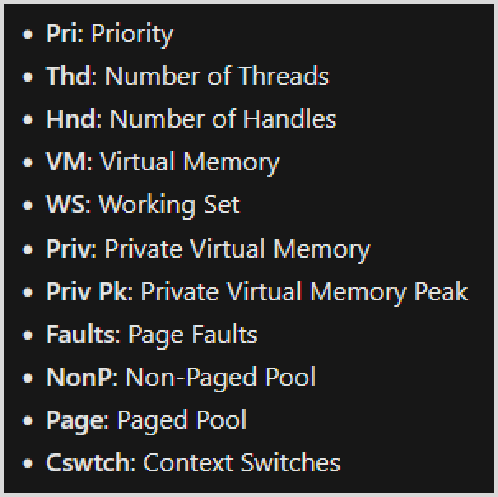
PsList: It is used to display detailed information about processes running on a system. It can display the processes running in real-time, including their process ID (PID), the amount of CPU and memory they are using and other information.

Advantages: It can be used to identify resource-intensive processes, detect rogue or malicious processes, and monitor system performance. It can also be used to terminate processes and threads that are causing problems.



```
E:\SEM 6\NS\Practical7\PsTools>pslist.exe

PsList v1.41 - Process information lister
Copyright (C) 2000-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

Process information for DESKTOP-72JADHG:

Name                Pid Pri Thd  Hnd   Priv        CPU Time    Elapsed Time
Idle                  0   0   4    0     60    15:12:03.843    66:27:54.601
System                4   8 207 5344    268     0:16:42.828    66:27:54.601
Registry            108   8   4    0  11180     0:00:02.109    66:27:57.950
smss                428  11   2   53   1064     0:00:00.328    66:27:54.548
csrss               812  13  22  851   2800     0:00:03.687    66:27:47.825
wininit             960  13   1  179   1824     0:00:00.218    66:27:46.892
services            728   9   9  732   6116     0:00:28.640    66:27:46.582
lsass               788   9   9 1572  10632     0:00:22.656    66:27:46.477
svchost            1116   8  17 1624  14652     0:00:35.250    66:27:45.762
fontdrvhost        1148   8   5   37   1848     0:00:00.328    66:27:45.708
svchost            1240   8  14 1382  10976     0:00:57.125    66:27:45.217
svchost            1292   8   6  361   2844     0:00:01.812    66:27:45.142
svchost            1420   8   4  256   2520     0:00:00.703    66:27:43.868
svchost            1456   8   2  388   2116     0:00:00.265    66:27:43.742
svchost            1528   8  11  337   2504     0:00:00.125    66:27:43.699
svchost            1652   8   4  232   2432     0:00:00.203    66:27:43.555
svchost            1680   8   7  441  18396     0:00:02.890    66:27:43.469
svchost            1776   8   2  152   5044     0:00:02.218    66:27:42.974
svchost            1820   8   8  243   2620     0:00:04.562    66:27:42.935
svchost            1904   8  23  529  21200     0:30:05.734    66:27:42.853
svchost            1140   8   8  407   5476     0:00:05.343    66:27:42.506
svchost            1612   8   7  424   6588     0:00:05.718    66:27:42.277
TouchpointAnalyticsClientService  2060   8  12  831  52732     0:00:04.875    66:27:42.260
svchost            2096   8   3  198   2748     0:00:09.265    66:27:42.052
svchost            2156   8   9  480   3416     0:00:06.468    66:27:41.963
svchost            2272   8   4  254   4828     0:00:05.375    66:27:41.321
svchost            2380   8   9  346   3232     0:00:06.640    66:27:41.072
svchost            2460   8   6  390   4904     0:00:02.921    66:27:40.860
svchost            2516   8   7  201  12024     0:00:53.484    66:27:40.757
svchost            2544   8   4  181   2156     0:00:21.906    66:27:40.702
svchost            2620   8  17  341   4392     0:00:47.203    66:27:40.590
svchost            2792   8   7  176   2016     0:00:00.484    66:27:39.252
atiesrxx           2928   8   4  182   1408     0:00:00.062    66:27:36.375
svchost            2964   8   3  216   1272     0:00:00.421    66:27:36.049
```

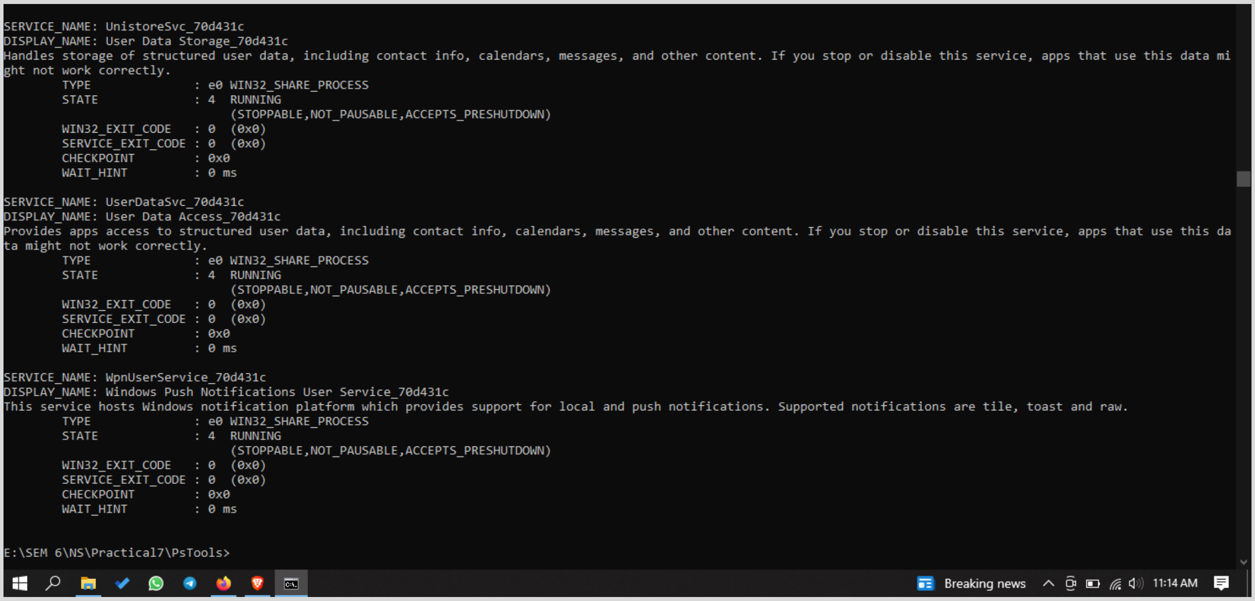
The terms in the screenshot indicate the following thing for a particular process.



- **Pri:** Priority
- **Thd:** Number of Threads
- **Hnd:** Number of Handles
- **VM:** Virtual Memory
- **WS:** Working Set
- **Priv:** Private Virtual Memory
- **Priv Pk:** Private Virtual Memory Peak
- **Faults:** Page Faults
- **NonP:** Non-Paged Pool
- **Page:** Paged Pool
- **Cswtch:** Context Switches

PsService: It allows users to view and control services on a local or remote computer. It provides various functions to manipulate services, such as starting, stopping, and querying their status.

Advantages: To troubleshoot service-related issues, such as identifying services that are causing high CPU or memory usage, and managing services across a network of computers. It can also be used to create scripts for managing services or automate service-related tasks.



```
SERVICE_NAME: UnistoreSvc_70d431c
DISPLAY_NAME: User Data Storage_70d431c
Handles storage of structured user data, including contact info, calendars, messages, and other content. If you stop or disable this service, apps that use this data mi
ght not work correctly.
        TYPE               : e0 WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE,NOT_PAUSABLE,ACCEPTS_PRESHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0 ms

SERVICE_NAME: UserDataSvc_70d431c
DISPLAY_NAME: User Data Access_70d431c
Provides apps access to structured user data, including contact info, calendars, messages, and other content. If you stop or disable this service, apps that use this da
ta might not work correctly.
        TYPE               : e0 WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE,NOT_PAUSABLE,ACCEPTS_PRESHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0 ms

SERVICE_NAME: WpnUserService_70d431c
DISPLAY_NAME: Windows Push Notifications User Service_70d431c
This service hosts Windows notification platform which provides support for local and push notifications. Supported notifications are tile, toast and raw.
        TYPE               : e0 WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE,NOT_PAUSABLE,ACCEPTS_PRESHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0 ms


E:\SEM 6\NS\Practical7\PsTools>
```

Above is the information gathered about the services on the system. We can see the service name, name which is being displayed, then the type, state, and much more information.

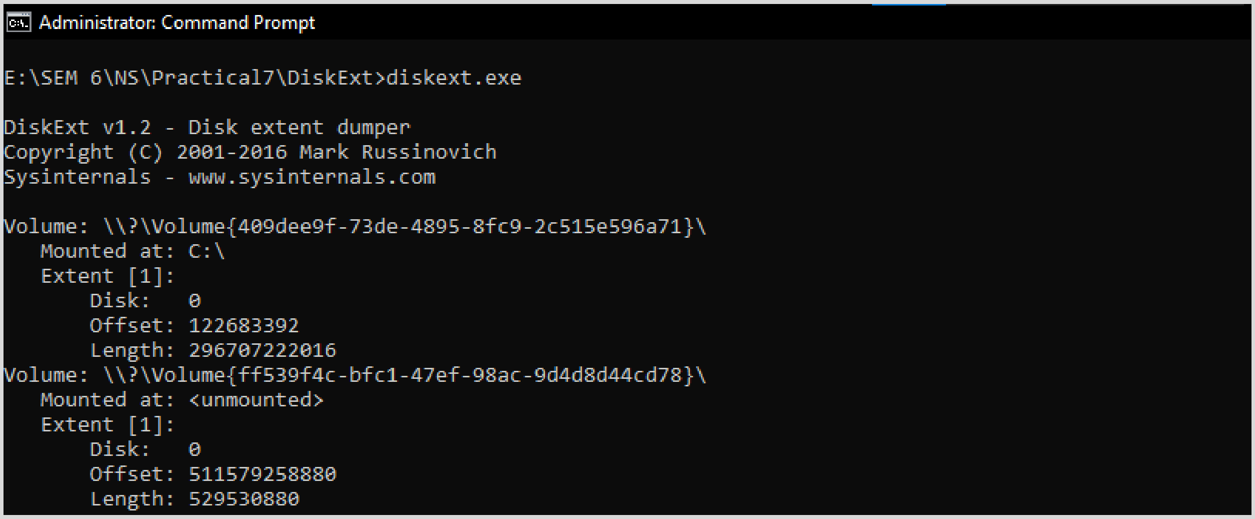
Files and Disk Utilities

File and disk related utilities in Sysinternals are a set of tools designed to help manage and troubleshoot file and disk-related issues in Windows systems. These tools provide administrators with a deep understanding of how files and disks are used by the system and can help identify issues and performance bottlenecks.

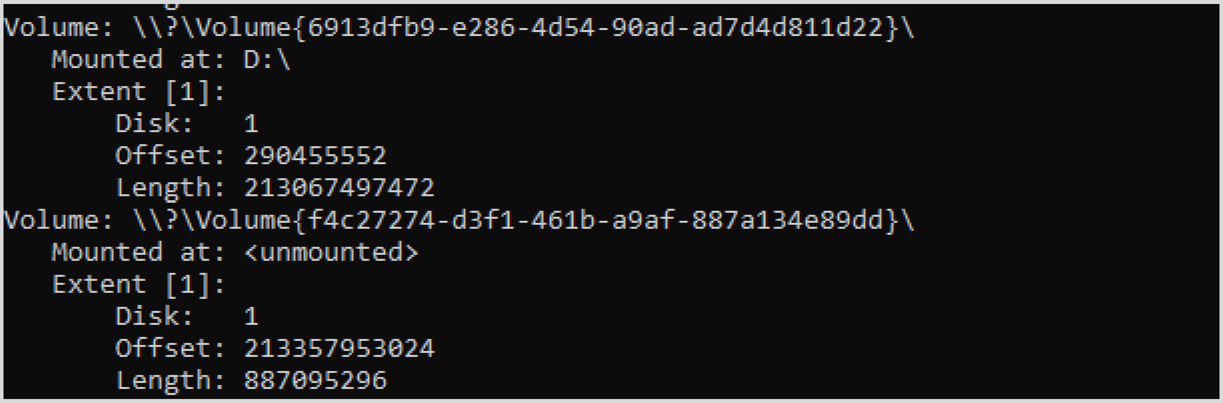
Following are some of the tools which I have used:

DiskExt: It can be used to display information about the file system on a given volume, including the volume's size, cluster size, total number of clusters, number of free clusters, and the amount of free space. Diskext can also be used to display detailed information about individual files and directories on the volume, including the file's size, creation and modification dates, and attributes

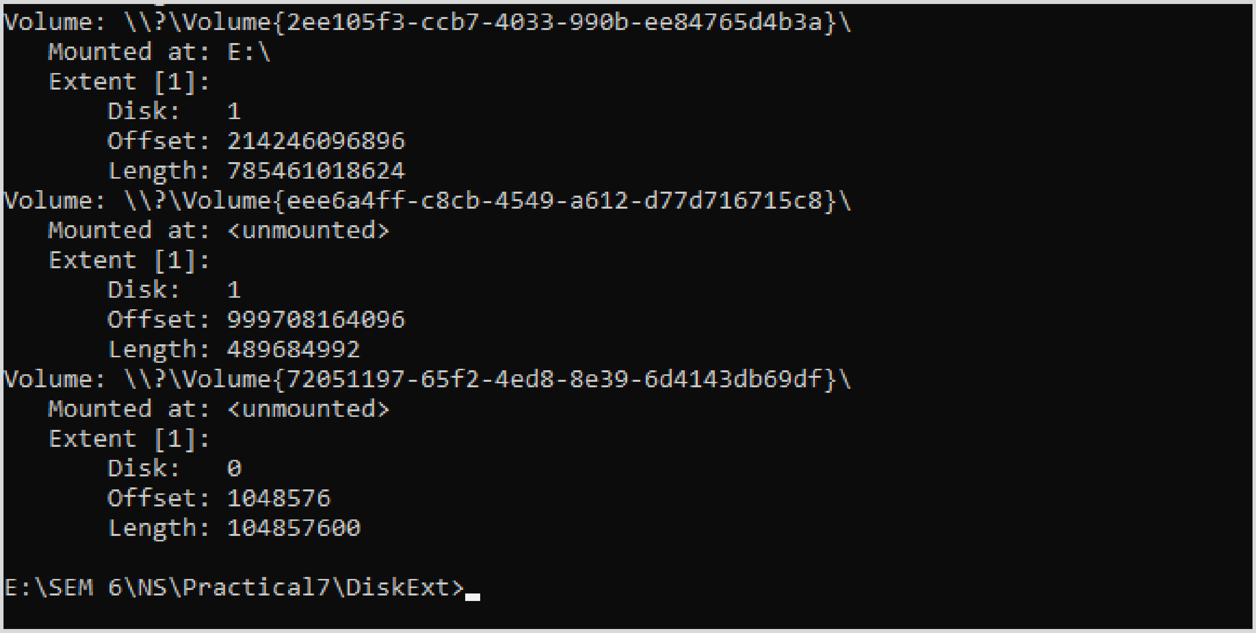
Advantages: Useful for IT administrators to troubleshoot disk-related issues.



```
E:\SEM 6\NS\Practical7\DiskExt>diskext.exe

DiskExt v1.2 - Disk extent dumper
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Volume: \\?\Volume{409dee9f-73de-4895-8fc9-2c515e596a71}\
   Mounted at: C:\
   Extent [1]:
       Disk:   0
       Offset: 122683392
       Length: 296707222016
Volume: \\?\Volume{ff539f4c-bfc1-47ef-98ac-9d4d8d44cd78}\
   Mounted at: <unmounted>
   Extent [1]:
       Disk:   0
       Offset: 511579258880
       Length: 529530880
```



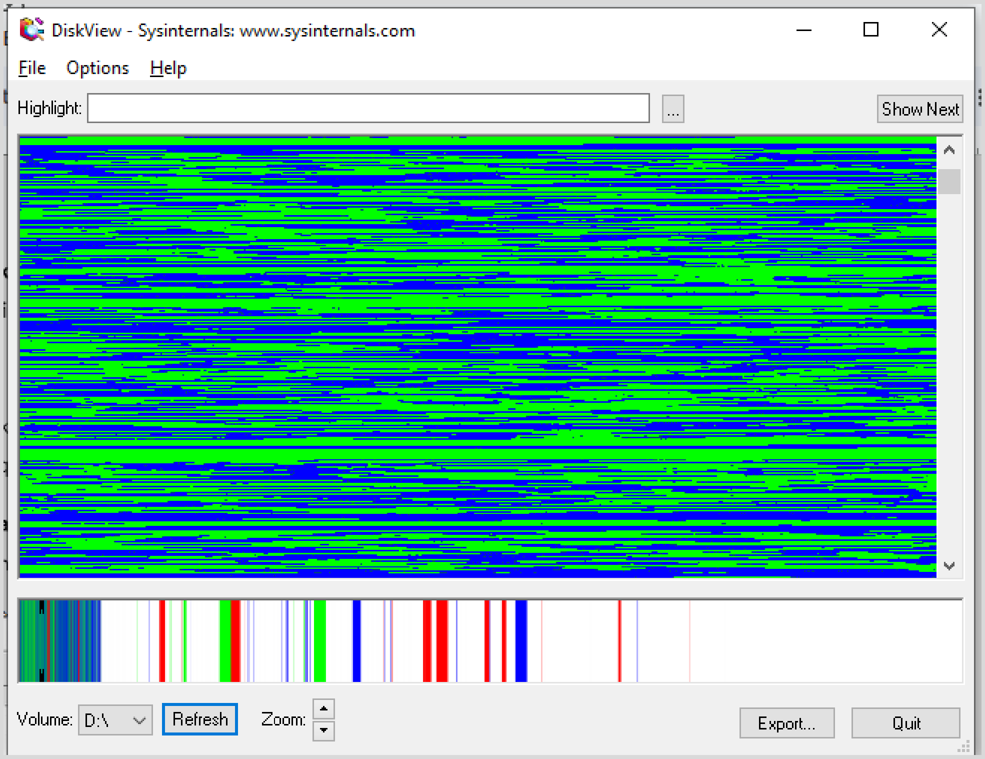
```
Volume: \\?\Volume{6913dfb9-e286-4d54-90ad-ad7d4d811d22}\
   Mounted at: D:\
   Extent [1]:
       Disk:   1
       Offset: 290455552
       Length: 213067497472
Volume: \\?\Volume{f4c27274-d3f1-461b-a9af-887a134e89dd}\
   Mounted at: <unmounted>
   Extent [1]:
       Disk:   1
       Offset: 213357953024
       Length: 887095296
```



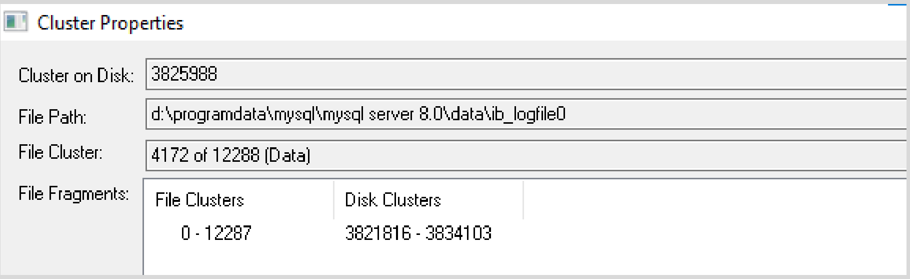
```
Volume: \\?\Volume{2ee105f3-ccb7-4033-990b-ee84765d4b3a}\
   Mounted at: E:\
   Extent [1]:
       Disk:   1
       Offset: 214246096896
       Length: 785461018624
Volume: \\?\Volume{eee6a4ff-c8cb-4549-a612-d77d716715c8}\
   Mounted at: <unmounted>
   Extent [1]:
       Disk:   1
       Offset: 999708164096
       Length: 489684992
Volume: \\?\Volume{72051197-65f2-4ed8-8e39-6d4143db69df}\
   Mounted at: <unmounted>
   Extent [1]:
       Disk:   0
       Offset: 1048576
       Length: 104857600

E:\SEM 6\NS\Practical7\DiskExt>
```

DiskView: It provides a graphical representation of the distribution of files and folders on the hard drive, allowing users to easily identify large files and folders that are taking up valuable disk space. DiskView also allows users to drill down into individual folders and files to see detailed information about their size and location on the hard drive.

Advantages: Used to identify large files and folders that are taking up too much space, and help optimize disk usage.



On double clicking the random part, I got the detail about the file which is shown below: [Cluster → basic unit of allocation of file system]



Cluster Properties

Cluster on Disk: 3825988

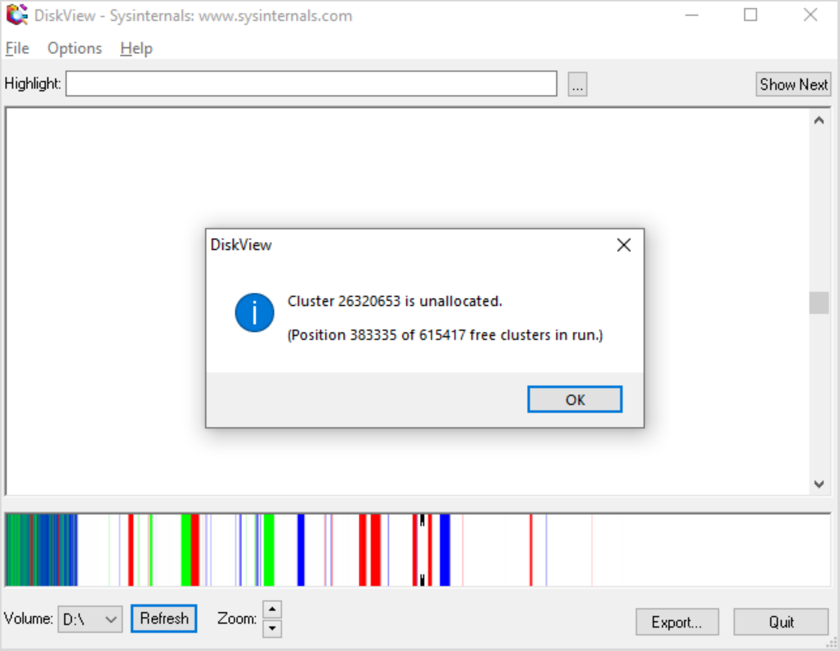
File Path: d:\programdata\mysql\mysql server 8.0\data\ib_logfile0

File Cluster: 4172 of 12288 (Data)

File Fragments:

File Clusters	Disk Clusters
0 - 12287	3821816 - 3834103

On clicking on the white part, I got the following popup saying the cluster is unallocated

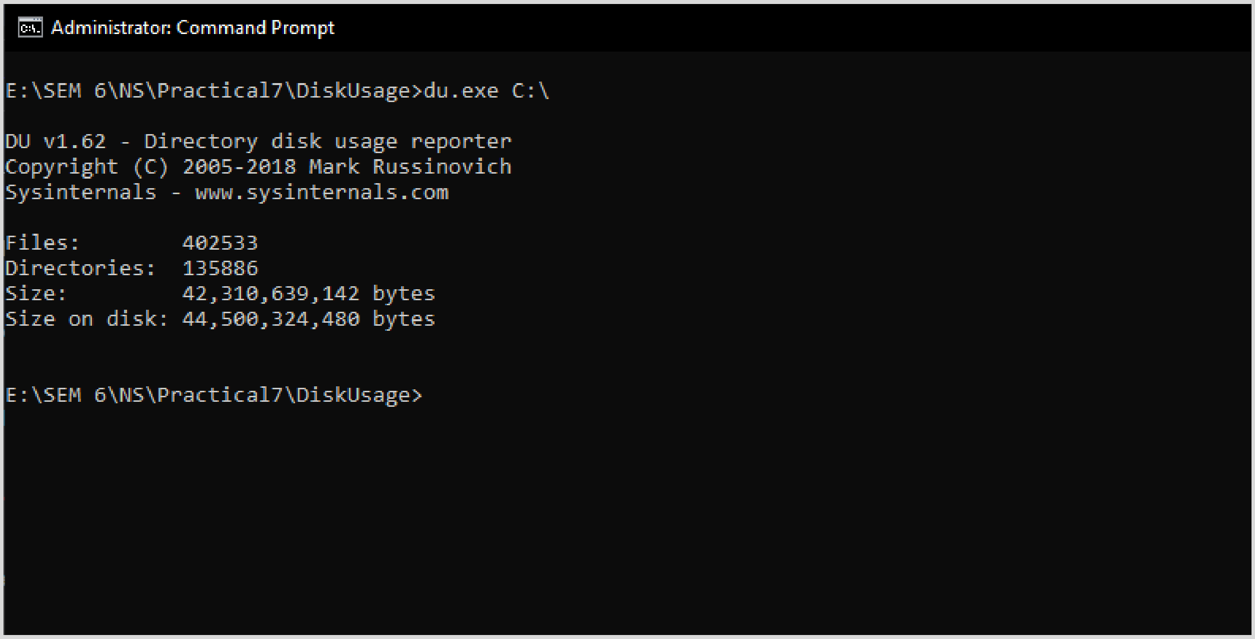


Cluster 26320653 is unallocated.

(Position 383335 of 615417 free clusters in run.)

DiskUsage: Determine the space used by directories and files on an NTFS volume. It can display the size of each folder and file, and also provides a summary of the total size occupied by the entire directory tree.

Advantages: Used to find out which files and folders are taking up the most space, and help optimize disk usage.

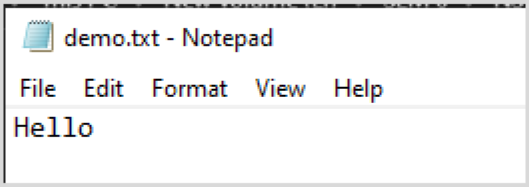


```
E:\SEM 6\NS\Practical7\DiskUsage>du.exe C:\

DU v1.62 - Directory disk usage reporter
Copyright (C) 2005-2018 Mark Russinovich
Sysinternals - www.sysinternals.com

Files:        402533
Directories:  135886
Size:         42,310,639,142 bytes
Size on disk: 44,500,324,480 bytes


E:\SEM 6\NS\Practical7\DiskUsage>
```

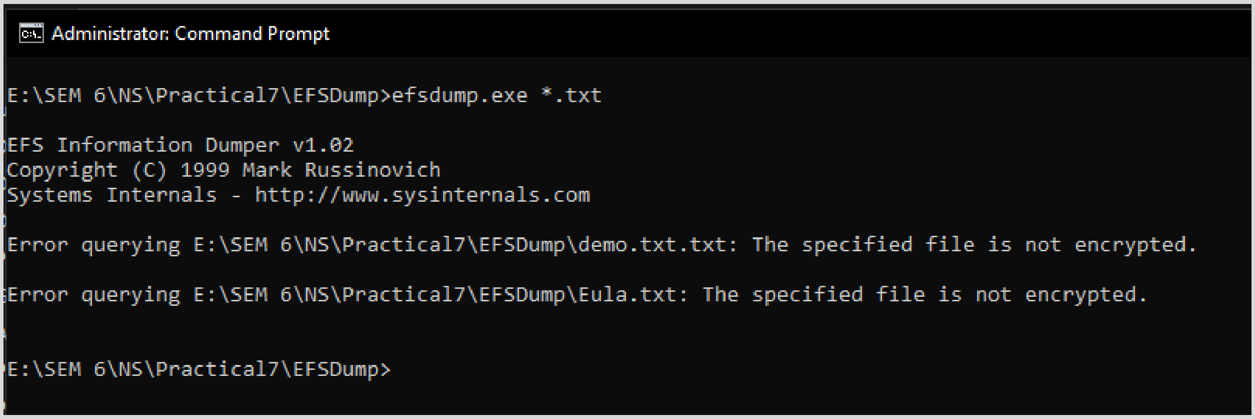
We can see in the screenshot the amount of space occupied by the files, directories.

EFSDump: To extract and analyze the encrypted file system (EFS) certificates and private keys that are used to protect files on a Windows file system. EFS is a feature in Windows that provides encryption for files and folders to protect data from unauthorized access.

Advantages: It can be used to recover data from encrypted files and folders.

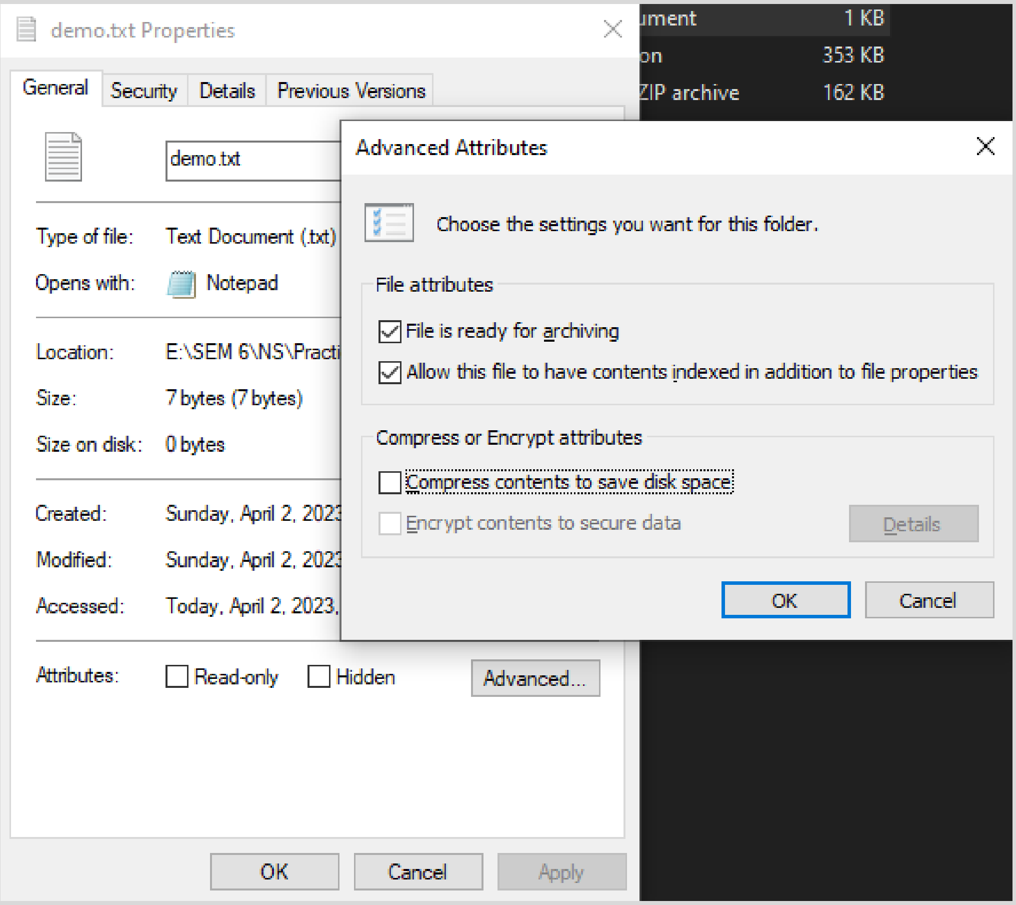


Hello



```
E:\SEM 6\NS\Practical7\EFSDump>efsdump.exe *.txt

EFS Information Dumper v1.02
Copyright (C) 1999 Mark Russinovich
Systems Internals - http://www.sysinternals.com

Error querying E:\SEM 6\NS\Practical7\EFSDump\demo.txt.txt: The specified file is not encrypted.

Error querying E:\SEM 6\NS\Practical7\EFSDump\Eula.txt: The specified file is not encrypted.


E:\SEM 6\NS\Practical7\EFSDump>
```

In my system I dont have any encrypted file so it is showing me the file is not encrypted. If there would be any then it would have shown me the name of the user who has access to that encrypted file.



demo.txt

Type of file: Text Document (.txt)

Opens with: Notepad

Location: E:\SEM 6\NS\Practi

Size: 7 bytes (7 bytes)

Size on disk: 0 bytes

Created: Sunday, April 2, 2023

Modified: Sunday, April 2, 2023

Accessed: Today, April 2, 2023,

Attributes: □ Read-only □ Hidden

Choose the settings you want for this folder.

File attributes

☑ File is ready for archiving

☑ Allow this file to have contents indexed in addition to file properties

Compress or Encrypt attributes

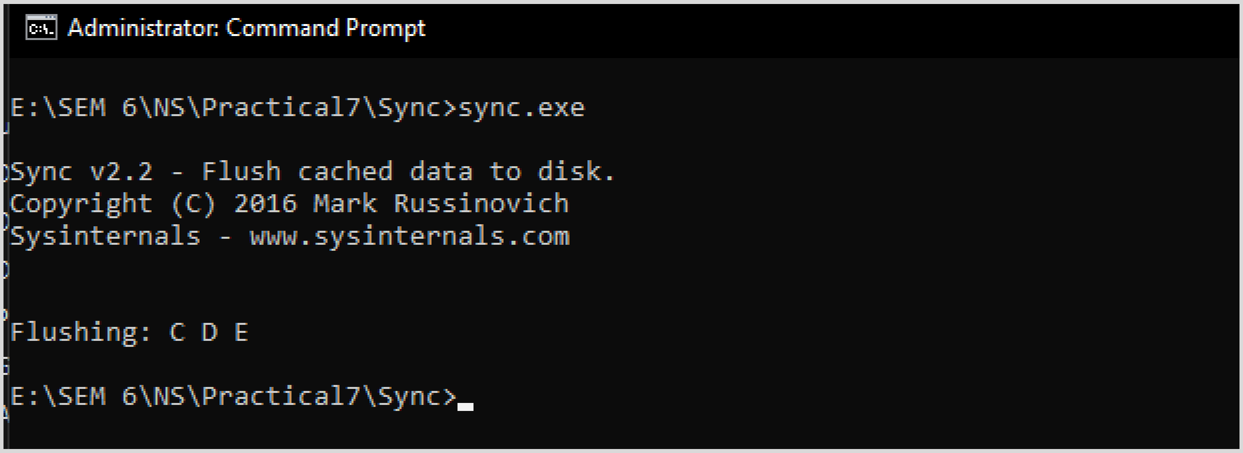
□ Compress contents to save disk space

□ Encrypt contents to secure data

I tried to encrypt the file but I dont have the pro version and so I am not able to encrypt the file.

Sync: It provides a way to flush the file system buffer cache. This cache can cause problems when data is not written to the disk immediately, such as when power is lost or the system crashes.

Advantages: , administrators can ensure that all file system data is written to the disk and the cache is cleared, which can help to avoid data loss or corruption in the event of a power failure or system crash. Useful for IT administrators to keep important files and data in sync across multiple devices.

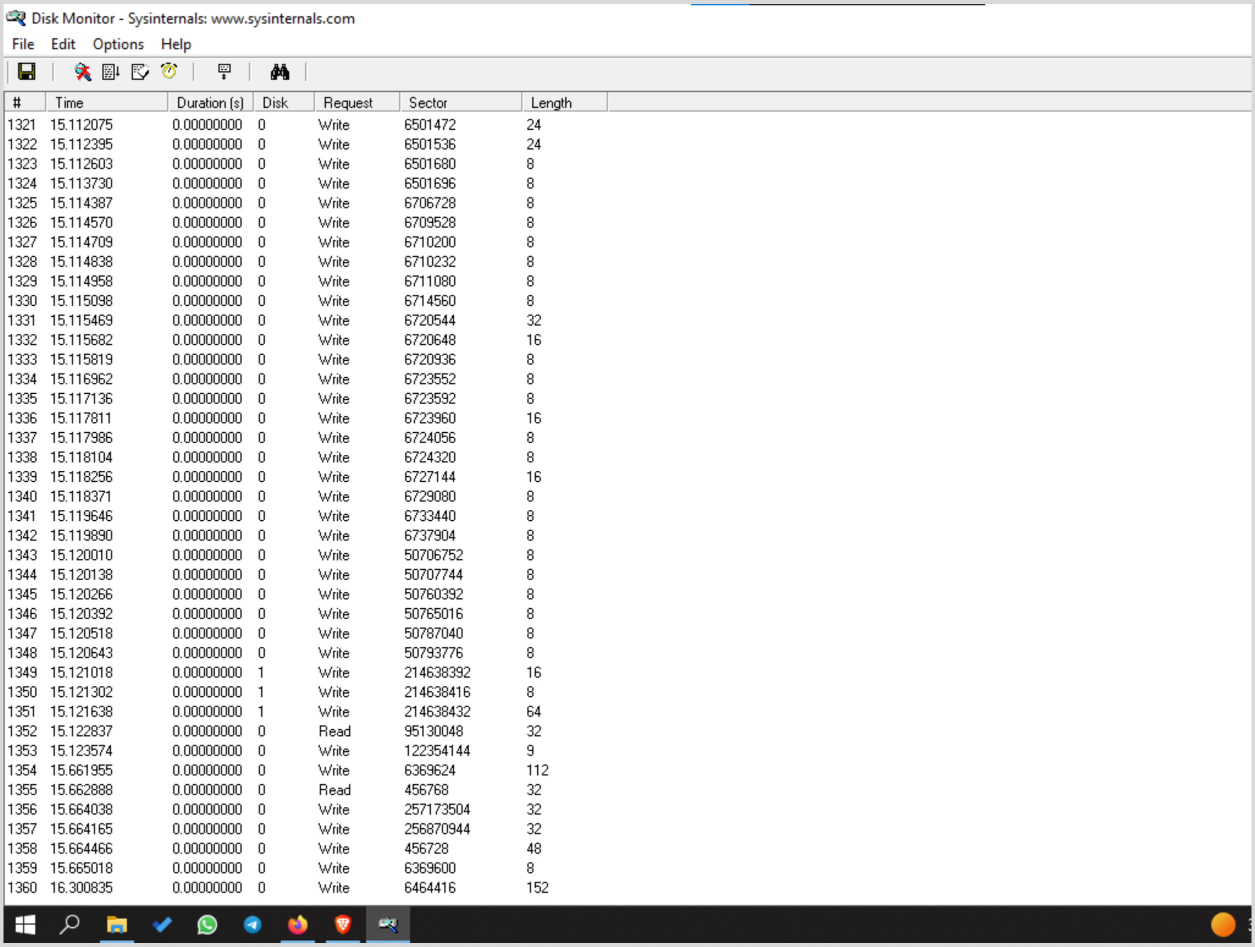


```
E:\SEM 6\NS\Practical7\Sync>sync.exe

Sync v2.2 - Flush cached data to disk.
Copyright (C) 2016 Mark Russinovich
Sysinternals - www.sysinternals.com


Flushing: C D E

E:\SEM 6\NS\Practical7\Sync>
```

The cache from all the drives, C, D and E has been flushed.

DiskMon: DiskMon is a disk activity monitoring tool provided by Sysinternals, which captures all hard disk activity or I/O operations taking place on a system in real-time.

Advantages: Useful for troubleshooting disk performance problems and identifying processes that are generating a high volume of disk activity, which may be affecting overall system performance



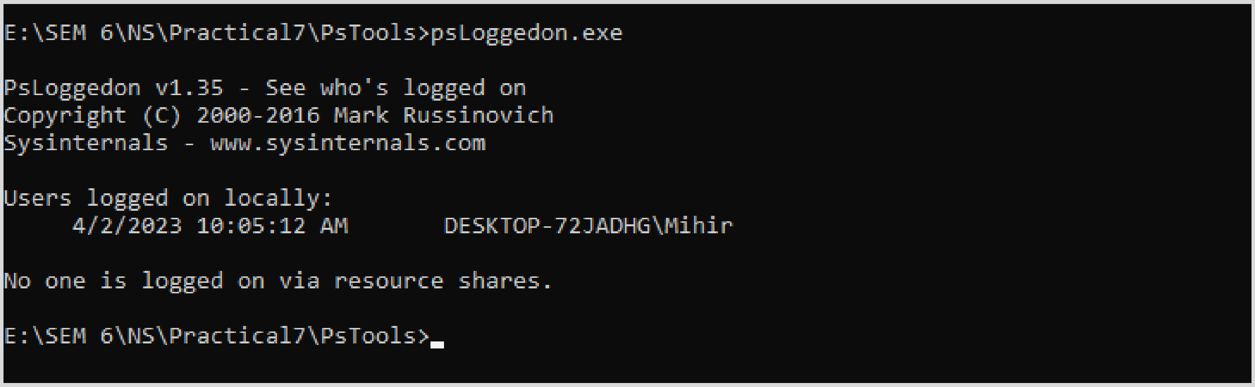
#	Time	Duration (s)	Disk	Request	Sector	Length
1321	15.112075	0.00000000	0	Write	6501472	24
1322	15.112395	0.00000000	0	Write	6501536	24
1323	15.112603	0.00000000	0	Write	6501680	8
1324	15.113730	0.00000000	0	Write	6501696	8
1325	15.114387	0.00000000	0	Write	6706728	8
1326	15.114570	0.00000000	0	Write	6709528	8
1327	15.114709	0.00000000	0	Write	6710200	8
1328	15.114838	0.00000000	0	Write	6710232	8
1329	15.114958	0.00000000	0	Write	6711080	8
1330	15.115098	0.00000000	0	Write	6714560	8
1331	15.115469	0.00000000	0	Write	6720544	32
1332	15.115682	0.00000000	0	Write	6720648	16
1333	15.115819	0.00000000	0	Write	6720936	8
1334	15.116962	0.00000000	0	Write	6723552	8
1335	15.117136	0.00000000	0	Write	6723592	8
1336	15.117811	0.00000000	0	Write	6723960	16
1337	15.117986	0.00000000	0	Write	6724056	8
1338	15.118104	0.00000000	0	Write	6724320	8
1339	15.118256	0.00000000	0	Write	6727144	16
1340	15.118371	0.00000000	0	Write	6729080	8
1341	15.119646	0.00000000	0	Write	6733440	8
1342	15.119890	0.00000000	0	Write	6737904	8
1343	15.120010	0.00000000	0	Write	50706752	8
1344	15.120138	0.00000000	0	Write	50707744	8
1345	15.120266	0.00000000	0	Write	50760392	8
1346	15.120392	0.00000000	0	Write	50765016	8
1347	15.120518	0.00000000	0	Write	50787040	8
1348	15.120643	0.00000000	0	Write	50793776	8
1349	15.121018	0.00000000	1	Write	214638392	16
1350	15.121302	0.00000000	1	Write	214638416	8
1351	15.121638	0.00000000	1	Write	214638432	64
1352	15.122837	0.00000000	0	Read	95130048	32
1353	15.123574	0.00000000	0	Write	122354144	9
1354	15.661955	0.00000000	0	Write	6369624	112
1355	15.662888	0.00000000	0	Read	456768	32
1356	15.664038	0.00000000	0	Write	257173504	32
1357	15.664165	0.00000000	0	Write	256870944	32
1358	15.664466	0.00000000	0	Write	456728	48
1359	15.665018	0.00000000	0	Write	6369600	8
1360	16.300835	0.00000000	0	Write	6464416	152

Security Utilities

Following are some of the tools which I have used:

PsLoggedOn: It displays logged-on user information for a local or remote machine. It shows the users logged on to a system, whether they are currently active or not, and their login times. The utility can also show logon session information for remote systems, including the user account name, the computer name, and the session ID.

Advantages: Useful for system administrators who need to monitor user activity on a network, especially in cases where there may be security concerns and also to troubleshoot issues related to user login and authentication



```
E:\SEM 6\NS\Practical7\PsTools>psLoggedon.exe

PsLoggedon v1.35 - See who's logged on
Copyright (C) 2000-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Users logged on locally:
     4/2/2023 10:05:12 AM       DESKTOP-72JADHG\Mihir

No one is logged on via resource shares.

E:\SEM 6\NS\Practical7\PsTools>
```