Practical – 2

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 analyse and test the current health of 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.

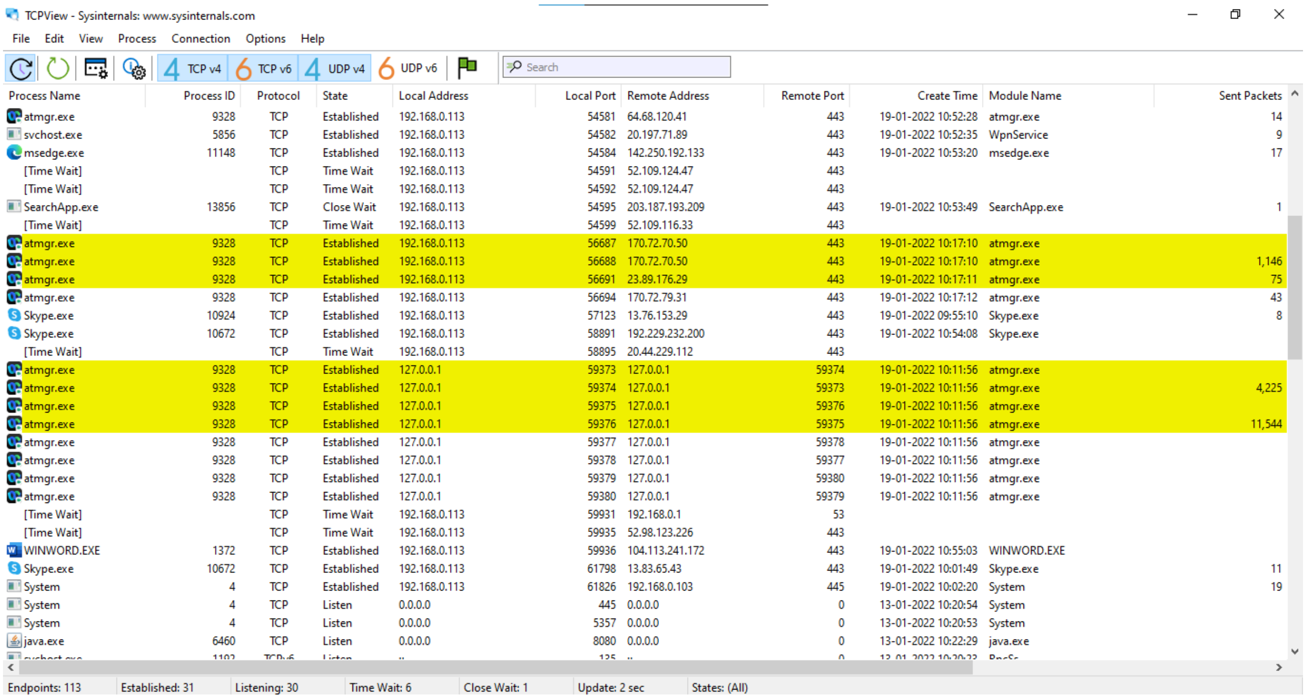
Website: live.sysinternals.com

Network:

1. TCPView.exe

This tool gives us the information of all the current connections with their port number, service name, address and type (TCP/ UDP).

We can use this tool to easily monitor and manage ongoing connections of our system.

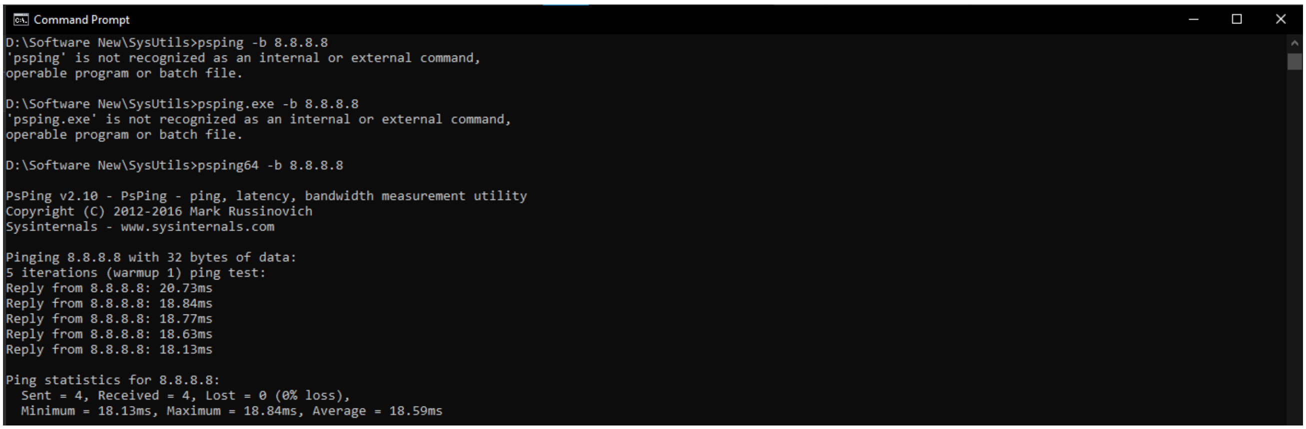


Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets
atmgr.exe	9328	TCP	Established	192.168.0.113	54581	64.68.120.41	443	19-01-2022 10:52:28	atmgr.exe	14
svchost.exe	5856	TCP	Established	192.168.0.113	54582	20.197.71.89	443	19-01-2022 10:52:35	WpnService	9
msedge.exe	11148	TCP	Established	192.168.0.113	54584	142.250.192.133	443	19-01-2022 10:53:20	msedge.exe	17
[Time Wait]		TCP	Time Wait	192.168.0.113	54591	52.109.124.47	443			
[Time Wait]		TCP	Time Wait	192.168.0.113	54592	52.109.124.47	443			
SearchApp.exe	13856	TCP	Close Wait	192.168.0.113	54595	203.187.193.209	443	19-01-2022 10:53:49	SearchApp.exe	1
[Time Wait]		TCP	Time Wait	192.168.0.113	54599	52.109.116.33	443			
atmgr.exe	9328	TCP	Established	192.168.0.113	56687	170.72.70.50	443	19-01-2022 10:17:10	atmgr.exe	
atmgr.exe	9328	TCP	Established	192.168.0.113	56688	170.72.70.50	443	19-01-2022 10:17:10	atmgr.exe	1,146
atmgr.exe	9328	TCP	Established	192.168.0.113	56691	23.89.176.29	443	19-01-2022 10:17:11	atmgr.exe	75
atmgr.exe	9328	TCP	Established	192.168.0.113	56694	170.72.79.31	443	19-01-2022 10:17:12	atmgr.exe	43
Skype.exe	10924	TCP	Established	192.168.0.113	57123	13.76.153.29	443	19-01-2022 09:55:10	Skype.exe	8
Skype.exe	10672	TCP	Established	192.168.0.113	58891	192.229.232.200	443	19-01-2022 10:54:08	Skype.exe	
[Time Wait]		TCP	Time Wait	192.168.0.113	58895	20.44.229.112	443			
atmgr.exe	9328	TCP	Established	127.0.0.1	59373	127.0.0.1	59374	19-01-2022 10:11:56	atmgr.exe	
atmgr.exe	9328	TCP	Established	127.0.0.1	59374	127.0.0.1	59373	19-01-2022 10:11:56	atmgr.exe	4,225
atmgr.exe	9328	TCP	Established	127.0.0.1	59375	127.0.0.1	59376	19-01-2022 10:11:56	atmgr.exe	
atmgr.exe	9328	TCP	Established	127.0.0.1	59376	127.0.0.1	59375	19-01-2022 10:11:56	atmgr.exe	11,544
atmgr.exe	9328	TCP	Established	127.0.0.1	59377	127.0.0.1	59378	19-01-2022 10:11:56	atmgr.exe	
atmgr.exe	9328	TCP	Established	127.0.0.1	59378	127.0.0.1	59377	19-01-2022 10:11:56	atmgr.exe	
atmgr.exe	9328	TCP	Established	127.0.0.1	59379	127.0.0.1	59380	19-01-2022 10:11:56	atmgr.exe	
atmgr.exe	9328	TCP	Established	127.0.0.1	59380	127.0.0.1	59379	19-01-2022 10:11:56	atmgr.exe	
[Time Wait]		TCP	Time Wait	192.168.0.113	59931	192.168.0.1	53			
[Time Wait]		TCP	Time Wait	192.168.0.113	59935	52.98.123.226	443			
WINWORD.EXE	1372	TCP	Established	192.168.0.113	59936	104.113.241.172	443	19-01-2022 10:55:03	WINWORD.EXE	
Skype.exe	10672	TCP	Established	192.168.0.113	61798	13.83.65.43	443	19-01-2022 10:01:49	Skype.exe	11
System	4	TCP	Established	192.168.0.113	61826	192.168.0.103	445	19-01-2022 10:02:20	System	19
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	13-01-2022 10:20:54	System	
System	4	TCP	Listen	0.0.0.0	5357	0.0.0.0	0	13-01-2022 10:20:53	System	
java.exe	6460	TCP	Listen	0.0.0.0	8080	0.0.0.0	0	13-01-2022 10:22:29	java.exe	

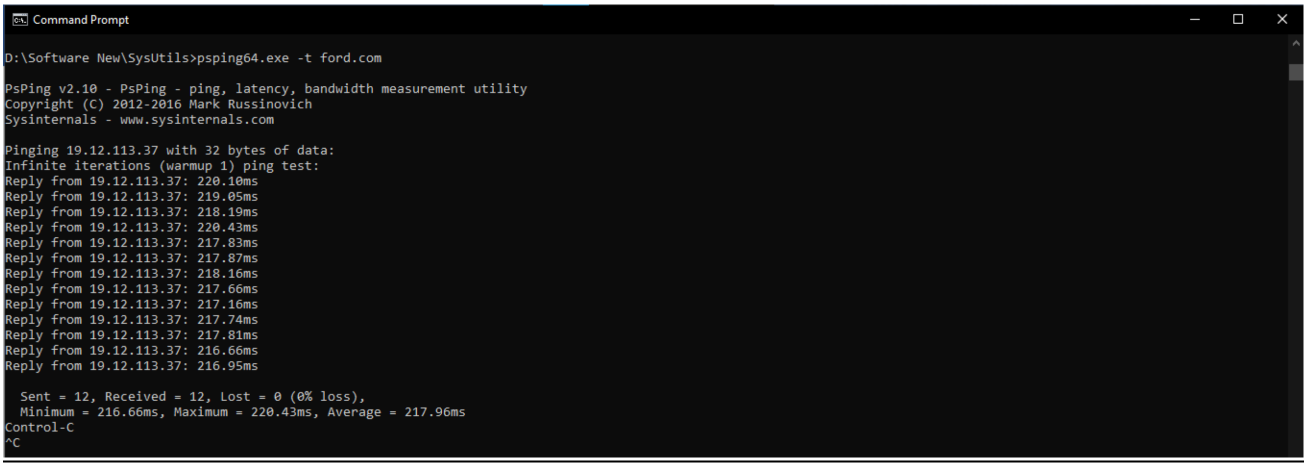
Endpoints: 113 | Established: 31 | Listening: 30 | Time Wait: 6 | Close Wait: 1 | Update: 2 sec | States: (All)

2. Psping.exe

This tool helps us in checking the ports and services of other devices by sending packets and pinging them. It also gives us different pinging options and option to check latency and bandwith.



```
D:\Software New\SysUtils>psping -b 8.8.8.8
'psping' is not recognized as an internal or external command,
operable program or batch file.

D:\Software New\SysUtils>psping.exe -b 8.8.8.8
'psping.exe' is not recognized as an internal or external command,
operable program or batch file.

D:\Software New\SysUtils>psping64 -b 8.8.8.8

PsPing v2.10 - PsPing - ping, latency, bandwidth measurement utility
Copyright (C) 2012-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Pinging 8.8.8.8 with 32 bytes of data:
5 iterations (warmup 1) ping test:
Reply from 8.8.8.8: 20.73ms
Reply from 8.8.8.8: 18.84ms
Reply from 8.8.8.8: 18.77ms
Reply from 8.8.8.8: 18.63ms
Reply from 8.8.8.8: 18.13ms

Ping statistics for 8.8.8.8:
  Sent = 4, Received = 4, Lost = 0 (0% loss),
  Minimum = 18.13ms, Maximum = 18.84ms, Average = 18.59ms
```



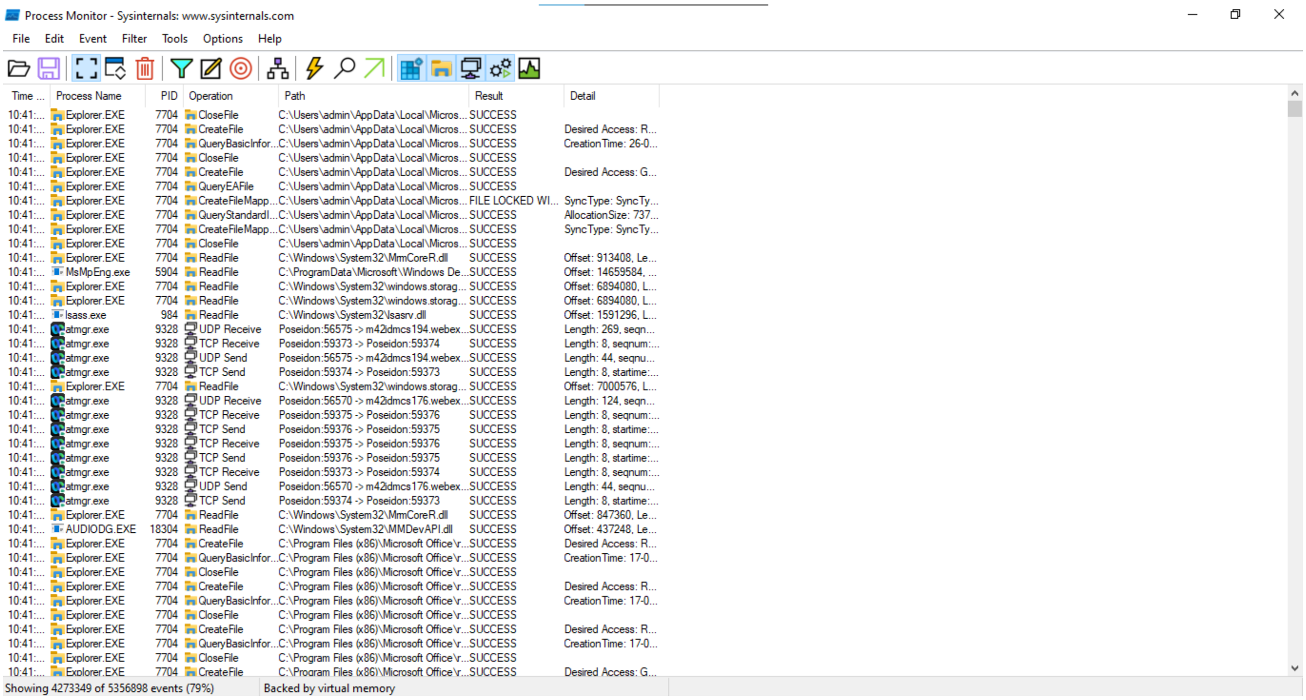
```
D:\Software New\SysUtils>psping64.exe -t ford.com

PsPing v2.10 - PsPing - ping, latency, bandwidth measurement utility
Copyright (C) 2012-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Pinging 19.12.113.37 with 32 bytes of data:
Infinite iterations (warmup 1) ping test:
Reply from 19.12.113.37: 220.10ms
Reply from 19.12.113.37: 219.05ms
Reply from 19.12.113.37: 218.19ms
Reply from 19.12.113.37: 220.43ms
Reply from 19.12.113.37: 217.83ms
Reply from 19.12.113.37: 217.87ms
Reply from 19.12.113.37: 218.16ms
Reply from 19.12.113.37: 217.66ms
Reply from 19.12.113.37: 217.16ms
Reply from 19.12.113.37: 217.74ms
Reply from 19.12.113.37: 217.81ms
Reply from 19.12.113.37: 216.66ms
Reply from 19.12.113.37: 216.95ms

  Sent = 12, Received = 12, Lost = 0 (0% loss),
  Minimum = 216.66ms, Maximum = 220.43ms, Average = 217.96ms
Control-C
^C
```

Process:

1. ProcMon.exe

This tool gives us the information of all the current running processes in our system. It also has options to give further details of processes like PID, TID Architecture, etc.

We can use this tool to monitor and manage processes on our system.

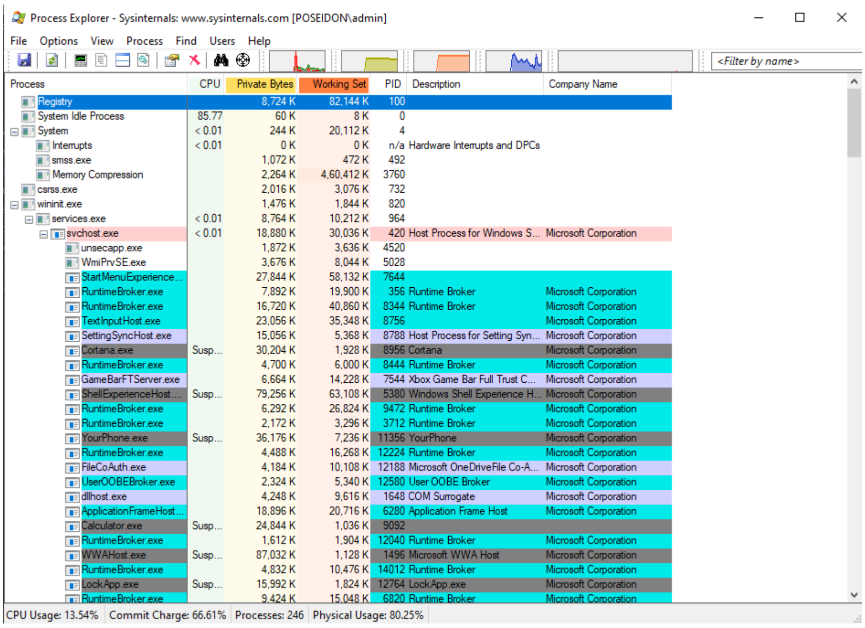


Time ...	Process Name	PID	Operation	Path	Result	Detail
10:41:...	Explorer.EXE	7704	CloseFile	C:\Users\admin\AppData\Local\Micros...	SUCCESS	
10:41:...	Explorer.EXE	7704	CreateFile	C:\Users\admin\AppData\Local\Micros...	SUCCESS	Desired Access: R...
10:41:...	Explorer.EXE	7704	QueryBasicInfor...	C:\Users\admin\AppData\Local\Micros...	SUCCESS	CreationTime: 26-0...
10:41:...	Explorer.EXE	7704	CloseFile	C:\Users\admin\AppData\Local\Micros...	SUCCESS	
10:41:...	Explorer.EXE	7704	CreateFile	C:\Users\admin\AppData\Local\Micros...	SUCCESS	Desired Access: G...
10:41:...	Explorer.EXE	7704	QueryEAFile	C:\Users\admin\AppData\Local\Micros...	SUCCESS	
10:41:...	Explorer.EXE	7704	CreateFileMapp...	C:\Users\admin\AppData\Local\Micros...	FILE LOCKED WI...	SyncType: SyncTy...
10:41:...	Explorer.EXE	7704	QueryStandardI...	C:\Users\admin\AppData\Local\Micros...	SUCCESS	AllocationSize: 737...
10:41:...	Explorer.EXE	7704	CreateFileMapp...	C:\Users\admin\AppData\Local\Micros...	SUCCESS	SyncType: SyncTy...
10:41:...	Explorer.EXE	7704	CloseFile	C:\Users\admin\AppData\Local\Micros...	SUCCESS	
10:41:...	Explorer.EXE	7704	ReadFile	C:\Windows\System32\MrmCoreR.dll	SUCCESS	Offset: 913408, Le...
10:41:...	MsMpEng.exe	5904	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 14659584, ...
10:41:...	Explorer.EXE	7704	ReadFile	C:\Windows\System32\windows.storag...	SUCCESS	Offset: 6894080, L...
10:41:...	Explorer.EXE	7704	ReadFile	C:\Windows\System32\windows.storag...	SUCCESS	Offset: 6894080, L...
10:41:...	lsass.exe	984	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1591296, L...
10:41:...	atmgr.exe	9328	UDP Receive	Poseidon:56575 -> m42idmcs194.webex...	SUCCESS	Length: 269, seqn...
10:41:...	atmgr.exe	9328	TCP Receive	Poseidon:59373 -> Poseidon:59374	SUCCESS	Length: 8, seqnum:...
10:41:...	atmgr.exe	9328	UDP Send	Poseidon:56575 -> m42idmcs194.webex...	SUCCESS	Length: 44, seqnu...
10:41:...	atmgr.exe	9328	TCP Send	Poseidon:59374 -> Poseidon:59373	SUCCESS	Length: 8, startime:...
10:41:...	Explorer.EXE	7704	ReadFile	C:\Windows\System32\windows.storag...	SUCCESS	Offset: 7000576, L...
10:41:...	atmgr.exe	9328	UDP Receive	Poseidon:56570 -> m42idmcs176.webex...	SUCCESS	Length: 124, seqn...
10:41:...	atmgr.exe	9328	TCP Receive	Poseidon:59375 -> Poseidon:59376	SUCCESS	Length: 8, seqnum:...
10:41:...	atmgr.exe	9328	TCP Send	Poseidon:59376 -> Poseidon:59375	SUCCESS	Length: 8, startime:...
10:41:...	atmgr.exe	9328	TCP Receive	Poseidon:59375 -> Poseidon:59376	SUCCESS	Length: 8, seqnum:...
10:41:...	atmgr.exe	9328	TCP Send	Poseidon:59376 -> Poseidon:59375	SUCCESS	Length: 8, startime:...
10:41:...	atmgr.exe	9328	TCP Receive	Poseidon:59373 -> Poseidon:59374	SUCCESS	Length: 8, seqnum:...
10:41:...	atmgr.exe	9328	UDP Send	Poseidon:56570 -> m42idmcs176.webex...	SUCCESS	Length: 44, seqnu...
10:41:...	atmgr.exe	9328	TCP Send	Poseidon:59374 -> Poseidon:59373	SUCCESS	Length: 8, startime:...
10:41:...	Explorer.EXE	7704	ReadFile	C:\Windows\System32\MrmCoreR.dll	SUCCESS	Offset: 847360, Le...
10:41:...	AUDIODG.EXE	18304	ReadFile	C:\Windows\System32\MMDevAPI.dll	SUCCESS	Offset: 437248, Le...
10:41:...	Explorer.EXE	7704	CreateFile	C:\Program Files (x86)\Microsoft Office\r...	SUCCESS	Desired Access: R...
10:41:...	Explorer.EXE	7704	QueryBasicInfor...	C:\Program Files (x86)\Microsoft Office\r...	SUCCESS	CreationTime: 17-0...
10:41:...	Explorer.EXE	7704	CloseFile	C:\Program Files (x86)\Microsoft Office\r...	SUCCESS	
10:41:...	Explorer.EXE	7704	CreateFile	C:\Program Files (x86)\Microsoft Office\r...	SUCCESS	Desired Access: R...
10:41:...	Explorer.EXE	7704	QueryBasicInfor...	C:\Program Files (x86)\Microsoft Office\r...	SUCCESS	CreationTime: 17-0...
10:41:...	Explorer.EXE	7704	CloseFile	C:\Program Files (x86)\Microsoft Office\r...	SUCCESS	
10:41:...	Explorer.EXE	7704	CreateFile	C:\Program Files (x86)\Microsoft Office\r...	SUCCESS	Desired Access: R...
10:41:...	Explorer.EXE	7704	QueryBasicInfor...	C:\Program Files (x86)\Microsoft Office\r...	SUCCESS	CreationTime: 17-0...
10:41:...	Explorer.EXE	7704	CloseFile	C:\Program Files (x86)\Microsoft Office\r...	SUCCESS	
10:41:...	Explorer.EXE	7704	CreateFile	C:\Program Files (x86)\Microsoft Office\r...	SUCCESS	Desired Access: G...

Showing 4273349 of 5356898 events (79%) | Backed by virtual memory

2. Procexp64.exe

This tool helps us displaying and managing all the running processes and subprocesses and set properties like priority and affinity.


Process Explorer - Sysinternals: www.sysinternals.com [POSEIDON\admin]
File
Options
View
Process
Find
Users
Help
<Filter by name>

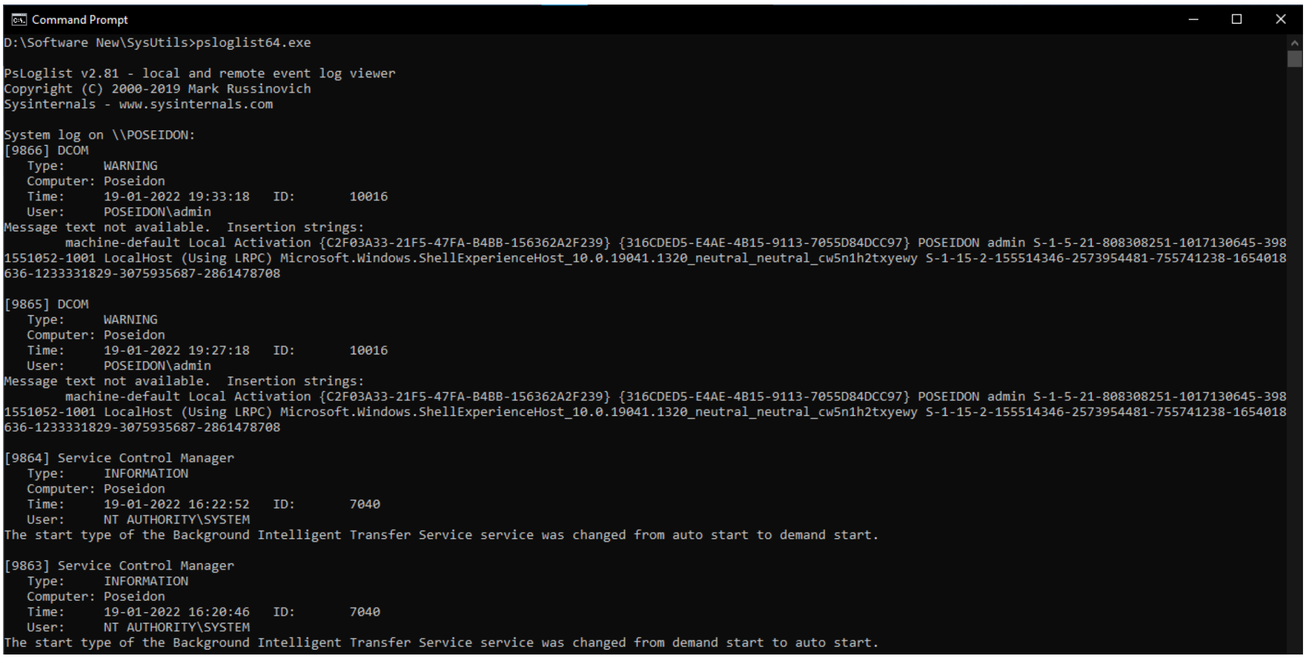
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		8,724 K	82,144 K	100		
System Idle Process	85.77	60 K	8 K	0		
System	< 0.01	244 K	20,112 K	4		
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1,072 K	472 K	492		
Memory Compression		2,264 K	4,60,412 K	3760		
csrss.exe		2,016 K	3,076 K	732		
wininit.exe		1,476 K	1,844 K	820		
services.exe	< 0.01	8,764 K	10,212 K	964		
svchost.exe	< 0.01	18,880 K	30,036 K	420	Host Process for Windows S...	Microsoft Corporation
unsecapp.exe		1,872 K	3,636 K	4520		
WmiPrvSE.exe		3,676 K	8,044 K	5028		
StartMenuExperience...		27,844 K	58,132 K	7644		
RuntimeBroker.exe		7,892 K	19,900 K	356	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		16,720 K	40,860 K	8344	Runtime Broker	Microsoft Corporation
TextInputHost.exe		23,056 K	35,348 K	8756		Microsoft Corporation
SettingSyncHost.exe		15,056 K	5,368 K	8788	Host Process for Setting Syn...	Microsoft Corporation
Cortana.exe	Susp...	30,204 K	1,928 K	8956	Cortana	Microsoft Corporation
RuntimeBroker.exe		4,700 K	6,000 K	8444	Runtime Broker	Microsoft Corporation
GameBarFTServer.exe		6,664 K	14,228 K	7544	Xbox Game Bar Full Trust C...	Microsoft Corporation
ShellExperienceHost....	Susp...	79,256 K	63,108 K	5380	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		6,292 K	26,824 K	9472	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		2,172 K	3,296 K	3712	Runtime Broker	Microsoft Corporation
YourPhone.exe	Susp...	36,176 K	7,236 K	11356	YourPhone	Microsoft Corporation
RuntimeBroker.exe		4,488 K	16,268 K	12224	Runtime Broker	Microsoft Corporation
FileCoAuth.exe		4,184 K	10,108 K	12188	Microsoft OneDriveFile Co-A...	Microsoft Corporation
UserOOBEBroker.exe		2,324 K	5,340 K	12580	User OOBE Broker	Microsoft Corporation
dllhost.exe		4,248 K	9,616 K	1648	COM Surrogate	Microsoft Corporation
ApplicationFrameHost...		18,896 K	20,716 K	6280	Application Frame Host	Microsoft Corporation
Calculator.exe	Susp...	24,844 K	1,036 K	9092		
RuntimeBroker.exe		1,612 K	1,904 K	12040	Runtime Broker	Microsoft Corporation
WWAHost.exe	Susp...	87,032 K	1,128 K	1496	Microsoft WWA Host	Microsoft Corporation
RuntimeBroker.exe		4,832 K	10,476 K	14012	Runtime Broker	Microsoft Corporation
LockApp.exe	Susp...	15,992 K	1,824 K	12764	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		9,424 K	15,048 K	6820	Runtime Broker	Microsoft Corporation

CPU Usage: 13.54% | Commit Charge: 66.61% | Processes: 246 | Physical Usage: 80.25%

Security:

1. Psloglist.exe

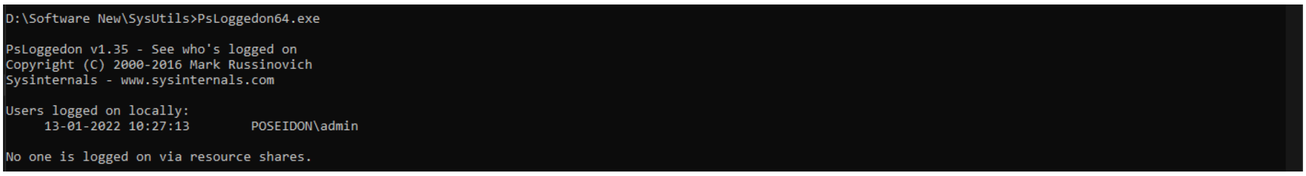
This tool helps us display all the system logs which contains the events performed by the user. It helps us in identifying any suspicious activity.



```
D:\Software New\SysUtils>psloglist64.exe

PsLoglist v2.81 - local and remote event log viewer
Copyright (C) 2000-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

System log on \\POSEIDON:
[9866] DCOM
   Type:     WARNING
   Computer: Poseidon
   Time:     19-01-2022 19:33:18   ID:       10016
   User:     POSEIDON\admin
Message text not available.  Insertion strings:
        machine-default Local Activation {C2F03A33-21F5-47FA-B4BB-156362A2F239} {316CDED5-E4AE-4B15-9113-7055D84DCC97} POSEIDON admin S-1-5-21-808308251-1017130645-398
1551052-1001 LocalHost (Using LRPC) Microsoft.Windows.ShellExperienceHost_10.0.19041.1320_neutral_neutral_cw5n1h2txyewy S-1-15-2-155514346-2573954481-755741238-1654018
636-1233331829-3075935687-2861478708

[9865] DCOM
   Type:     WARNING
   Computer: Poseidon
   Time:     19-01-2022 19:27:18   ID:       10016
   User:     POSEIDON\admin
Message text not available.  Insertion strings:
        machine-default Local Activation {C2F03A33-21F5-47FA-B4BB-156362A2F239} {316CDED5-E4AE-4B15-9113-7055D84DCC97} POSEIDON admin S-1-5-21-808308251-1017130645-398
1551052-1001 LocalHost (Using LRPC) Microsoft.Windows.ShellExperienceHost_10.0.19041.1320_neutral_neutral_cw5n1h2txyewy S-1-15-2-155514346-2573954481-755741238-1654018
636-1233331829-3075935687-2861478708

[9864] Service Control Manager
   Type:     INFORMATION
   Computer: Poseidon
   Time:     19-01-2022 16:22:52   ID:       7040
   User:     NT AUTHORITY\SYSTEM
The start type of the Background Intelligent Transfer Service service was changed from auto start to demand start.

[9863] Service Control Manager
   Type:     INFORMATION
   Computer: Poseidon
   Time:     19-01-2022 16:20:46   ID:       7040
   User:     NT AUTHORITY\SYSTEM
The start type of the Background Intelligent Transfer Service service was changed from demand start to auto start.
```

2. Psloggedon.exe

This tool shows the currently logged in users, and whether they are locally or remotely.

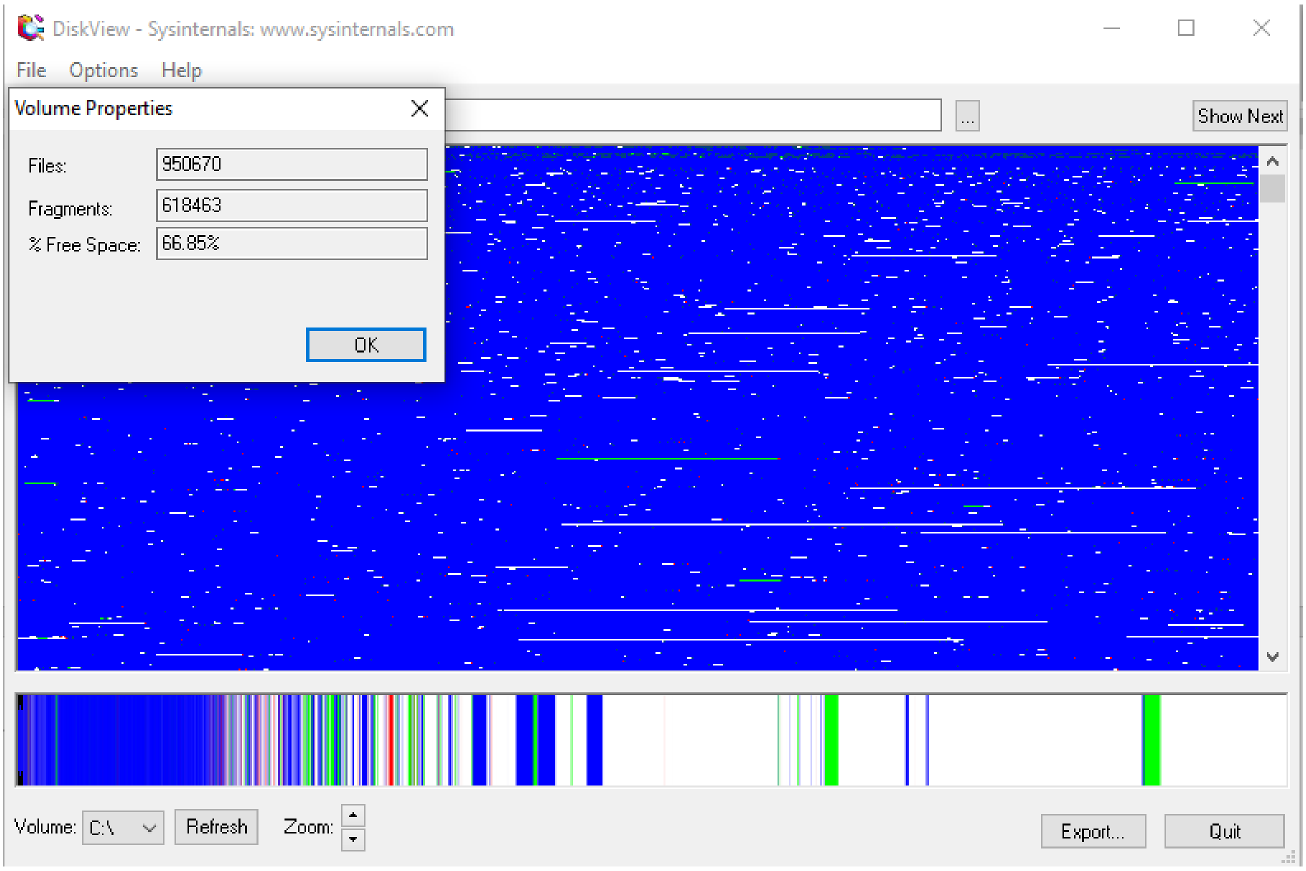


```
D:\Software New\SysUtils>PsLoggedon64.exe

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

Users logged on locally:
     13-01-2022 10:27:13        POSEIDON\admin

No one is logged on via resource shares.
```

Files:

1. Diskview.exe

This tool helps us scan our system volumes and displays information like files, fragments, free space and overall disk health.



Files: 950670

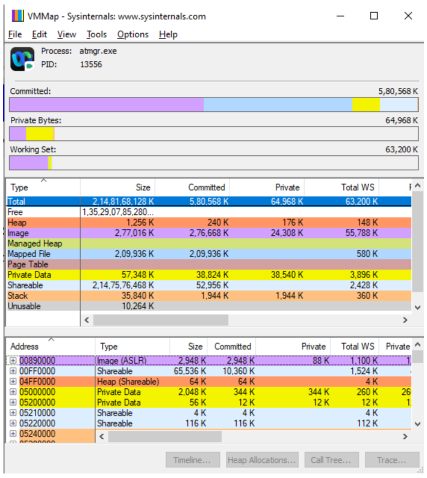
Fragments: 618463

% Free Space: 66.85%

Volume: C:\

2. Vmmap.exe (Memory)

This tool gives us a detailed information on memory usage of each application.

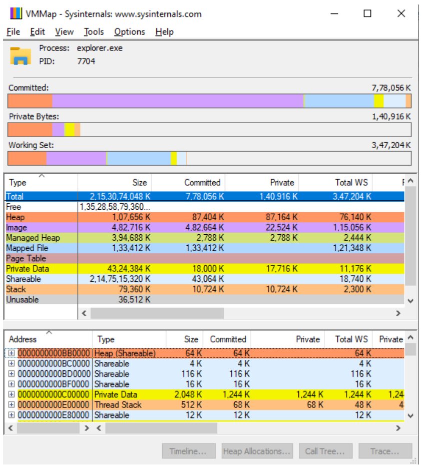

VMMap - Sysinternals: www.sysinternals.com
File Edit View Tools Options Help
Timeline...
Heap Allocations...
Call Tree...
Trace...

Process: atmgr.exe
PID: 13556

Committed: 5,80,568 K
Private Bytes: 64,968 K
Working Set: 63,200 K

Type	Size	Committed	Private	Total WS
Total	2,14,81,68,128 K	5,80,568 K	64,968 K	63,200 K
Free	1,35,29,07,85,280...			
Heap	1,256 K	240 K	176 K	148 K
Image	2,77,016 K	2,76,668 K	24,308 K	55,788 K
Managed Heap				
Mapped File	2,09,936 K	2,09,936 K		580 K
Page Table				
Private Data	57,348 K	38,824 K	38,540 K	3,896 K
Shareable	2,14,75,76,468 K	52,956 K		2,428 K
Stack	35,840 K	1,944 K	1,944 K	360 K
Unusable	10,264 K			

Address	Type	Size	Committed	Private	Total WS	Private
00890000	Image (ASLR)	2,948 K	2,948 K	88 K	1,100 K	1.
00FF0000	Shareable	65,536 K	10,360 K		1,524 K	
04FF0000	Heap (Shareable)	64 K	64 K		4 K	
05000000	Private Data	2,048 K	344 K	344 K	260 K	26
05200000	Private Data	56 K	12 K	12 K	12 K	1.
05210000	Shareable	4 K	4 K		4 K	
05220000	Shareable	116 K	116 K		112 K	
05240000						


VMMap - Sysinternals: www.sysinternals.com
File Edit View Tools Options Help
Timeline...
Heap Allocations...
Call Tree...
Trace...

Process: explorer.exe
PID: 7704

Committed: 7,78,056 K
Private Bytes: 1,40,916 K
Working Set: 3,47,204 K

Type	Size	Committed	Private	Total WS
Total	2,15,30,74,048 K	7,78,056 K	1,40,916 K	3,47,204 K
Free	1,35,28,58,79,360...			
Heap	1,07,656 K	87,404 K	87,164 K	76,140 K
Image	4,82,716 K	4,82,664 K	22,524 K	1,15,056 K
Managed Heap	3,94,688 K	2,788 K	2,788 K	2,444 K
Mapped File	1,33,412 K	1,33,412 K		1,21,348 K
Page Table				
Private Data	43,24,384 K	18,000 K	17,716 K	11,176 K
Shareable	2,14,75,15,320 K	43,064 K		18,740 K
Stack	79,360 K	10,724 K	10,724 K	2,300 K
Unusable	36,512 K			

Address	Type	Size	Committed	Private	Total WS	Private
0000000000BB0000	Heap (Shareable)	64 K	64 K		64 K	
0000000000BC0000	Shareable	4 K	4 K		4 K	
0000000000BD0000	Shareable	116 K	116 K		116 K	
0000000000BF0000	Shareable	16 K	16 K		16 K	
0000000000C00000	Private Data	2,048 K	1,244 K	1,244 K	1,244 K	1,24
0000000000E00000	Thread Stack	512 K	68 K	68 K	48 K	4
0000000000E80000	Shareable	12 K	12 K		12 K	