Practical 7

Aim:- Tools to perform Behavioural Analysis of Malware:-

1.Process Hackers

Description:-

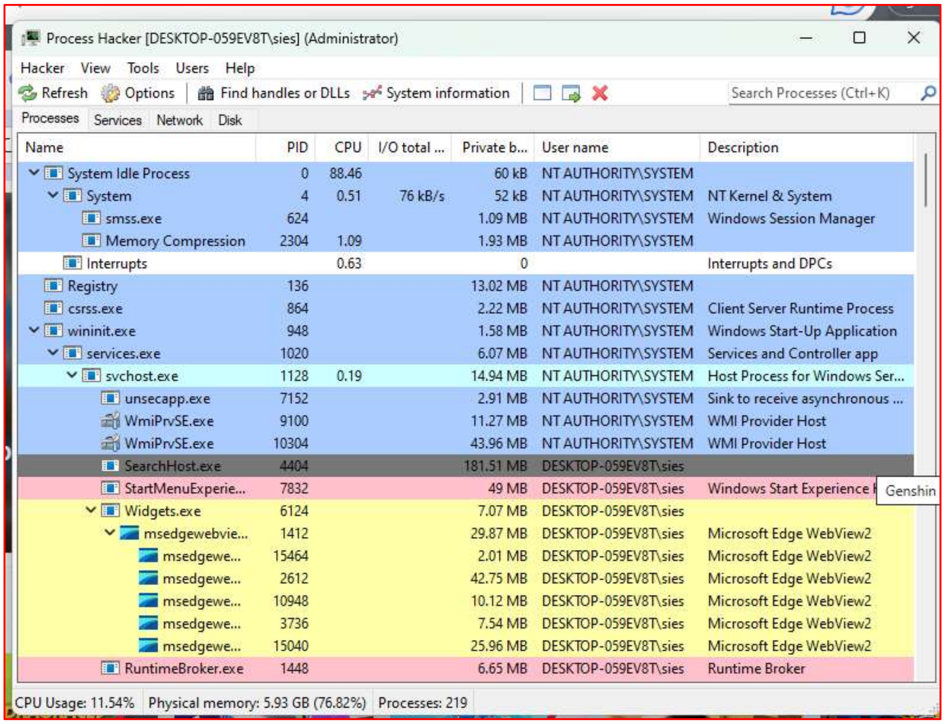
Process Hacker is an open-source tool that will allow you to see what processes are running on a device, identify programs that are eating up CPU resources and identify network connections that are associated with a process.

These types of features make Process Hacker an ideal tool for monitoring malware on a device. By seeing what processes are created and being able to identify network connections and interesting strings from memory means that valuable indicators of compromise (IOC's) can be gathered when triaging a malware infection.

Steps:-

Download process hacker from google then,

Below is the default display shown for Process Hacker when it is launched on a device:



Process Hacker [DESKTOP-059EV8T\sies] (Administrator)
Hacker View Tools Users Help
Refresh Options Find handles or DLLs System information
Search Processes (Ctrl+K)
Processes Services Network Disk
Genshin

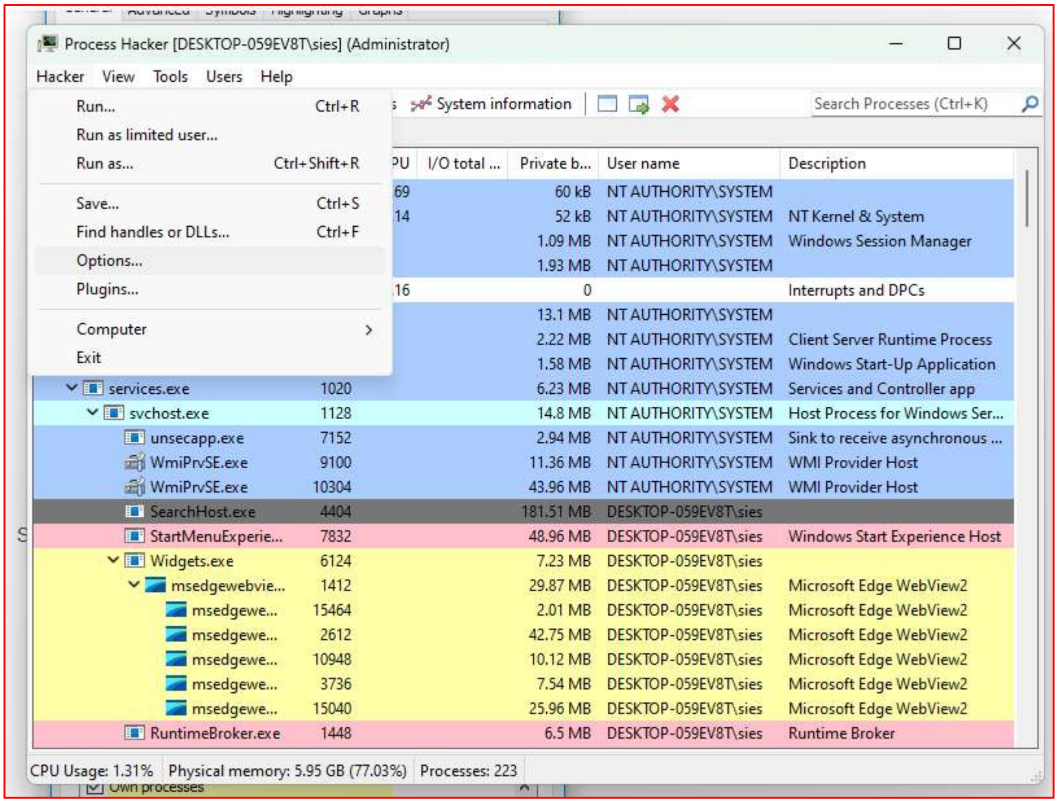
Name	PID	CPU	I/O total ...	Private b...	User name	Description
System Idle Process	0	88.46		60 kB	NT AUTHORITY\SYSTEM	
System	4	0.51	76 kB/s	52 kB	NT AUTHORITY\SYSTEM	NT Kernel & System
smss.exe	624			1.09 MB	NT AUTHORITY\SYSTEM	Windows Session Manager
Memory Compression	2304	1.09		1.93 MB	NT AUTHORITY\SYSTEM	
Interrupts		0.63		0		Interrupts and DPCs
Registry	136			13.02 MB	NT AUTHORITY\SYSTEM	
csrss.exe	864			2.22 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process
wininit.exe	948			1.58 MB	NT AUTHORITY\SYSTEM	Windows Start-Up Application
services.exe	1020			6.07 MB	NT AUTHORITY\SYSTEM	Services and Controller app
svchost.exe	1128	0.19		14.94 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
unsecapp.exe	7152			2.91 MB	NT AUTHORITY\SYSTEM	Sink to receive asynchronous ...
WmiPrvSE.exe	9100			11.27 MB	NT AUTHORITY\SYSTEM	WMI Provider Host
WmiPrvSE.exe	10304			43.96 MB	NT AUTHORITY\SYSTEM	WMI Provider Host
SearchHost.exe	4404			181.51 MB	DESKTOP-059EV8T\sies	
StartMenuExperie...	7832			49 MB	DESKTOP-059EV8T\sies	Windows Start Experience H
Widgets.exe	6124			7.07 MB	DESKTOP-059EV8T\sies	
msedgewebvie...	1412			29.87 MB	DESKTOP-059EV8T\sies	Microsoft Edge WebView2
msedgewe...	15464			2.01 MB	DESKTOP-059EV8T\sies	Microsoft Edge WebView2
msedgewe...	2612			42.75 MB	DESKTOP-059EV8T\sies	Microsoft Edge WebView2
msedgewe...	10948			10.12 MB	DESKTOP-059EV8T\sies	Microsoft Edge WebView2
msedgewe...	3736			7.54 MB	DESKTOP-059EV8T\sies	Microsoft Edge WebView2
msedgewe...	15040			25.96 MB	DESKTOP-059EV8T\sies	Microsoft Edge WebView2
RuntimeBroker.exe	1448			6.65 MB	DESKTOP-059EV8T\sies	Runtime Broker

CPU Usage: 11.54% Physical memory: 5.93 GB (76.82%) Processes: 219

The first tab named 'Processes' gives an overview of what processes are running on the device which contains the following information:

- **Name** of the running process
- **The PID** is the process ID, this is a unique number assigned to the process
- **The CPU** tab displays the amount of CPU being consumed by the process
- **The I/O total output** tab
- **The Private bytes** tab
- **The User name** tab displays which account was used to launch the process
- **The Description** tab displays information relating to what the process is

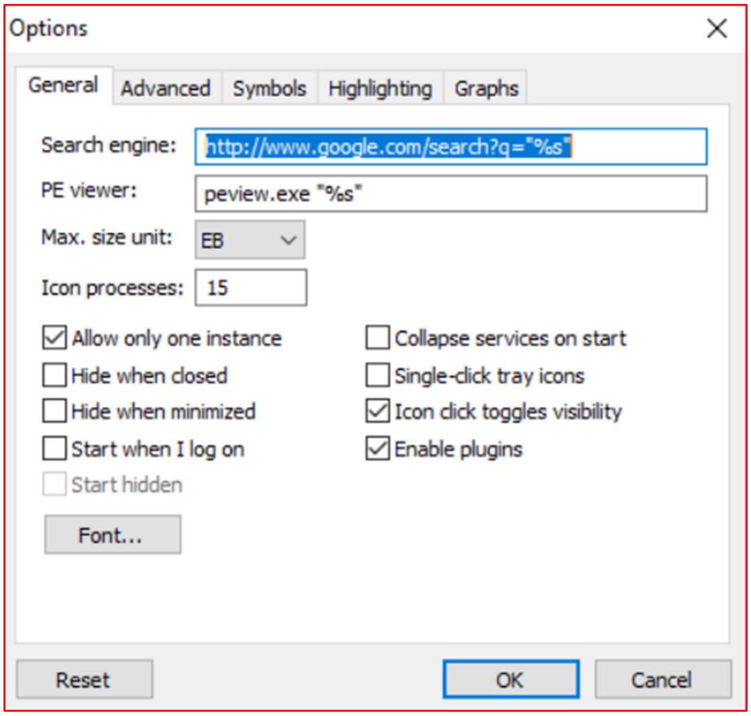
The ‘Processes’ tab also color codes the listed processes. By navigating to ‘Hacker’ and then ‘Options’ menu you can identify what each color represents in Process Hacker.



		PU	I/O total ...	Private b...	User name	Description
		69		60 kB	NT AUTHORITY\SYSTEM	
		14		52 kB	NT AUTHORITY\SYSTEM	NT Kernel & System
				1.09 MB	NT AUTHORITY\SYSTEM	Windows Session Manager
				1.93 MB	NT AUTHORITY\SYSTEM	
		16		0		Interrupts and DPCs
				13.1 MB	NT AUTHORITY\SYSTEM	
				2.22 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process
				1.58 MB	NT AUTHORITY\SYSTEM	Windows Start-Up Application
services.exe	1020			6.23 MB	NT AUTHORITY\SYSTEM	Services and Controller app
svchost.exe	1128			14.8 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
unsecapp.exe	7152			2.94 MB	NT AUTHORITY\SYSTEM	Sink to receive asynchronous ...
WmiPrvSE.exe	9100			11.36 MB	NT AUTHORITY\SYSTEM	WMI Provider Host
WmiPrvSE.exe	10304			43.96 MB	NT AUTHORITY\SYSTEM	WMI Provider Host
SearchHost.exe	4404			181.51 MB	DESKTOP-059EV8T\sies	
StartMenuExperie...	7832			48.96 MB	DESKTOP-059EV8T\sies	Windows Start Experience Host
Widgets.exe	6124			7.23 MB	DESKTOP-059EV8T\sies	
msedgewebvie...	1412			29.87 MB	DESKTOP-059EV8T\sies	Microsoft Edge WebView2
msedgewe...	15464			2.01 MB	DESKTOP-059EV8T\sies	Microsoft Edge WebView2
msedgewe...	2612			42.75 MB	DESKTOP-059EV8T\sies	Microsoft Edge WebView2
msedgewe...	10948			10.12 MB	DESKTOP-059EV8T\sies	Microsoft Edge WebView2
msedgewe...	3736			7.54 MB	DESKTOP-059EV8T\sies	Microsoft Edge WebView2
msedgewe...	15040			25.96 MB	DESKTOP-059EV8T\sies	Microsoft Edge WebView2
RuntimeBroker.exe	1448			6.5 MB	DESKTOP-059EV8T\sies	Runtime Broker

CPU Usage: 1.31% Physical memory: 5.95 GB (77.03%) Processes: 223

This then opens the ‘Options’ menu.



Options

General | Advanced | Symbols | Highlighting | Graphs

Search engine: http://www.google.com/search?q="%s"

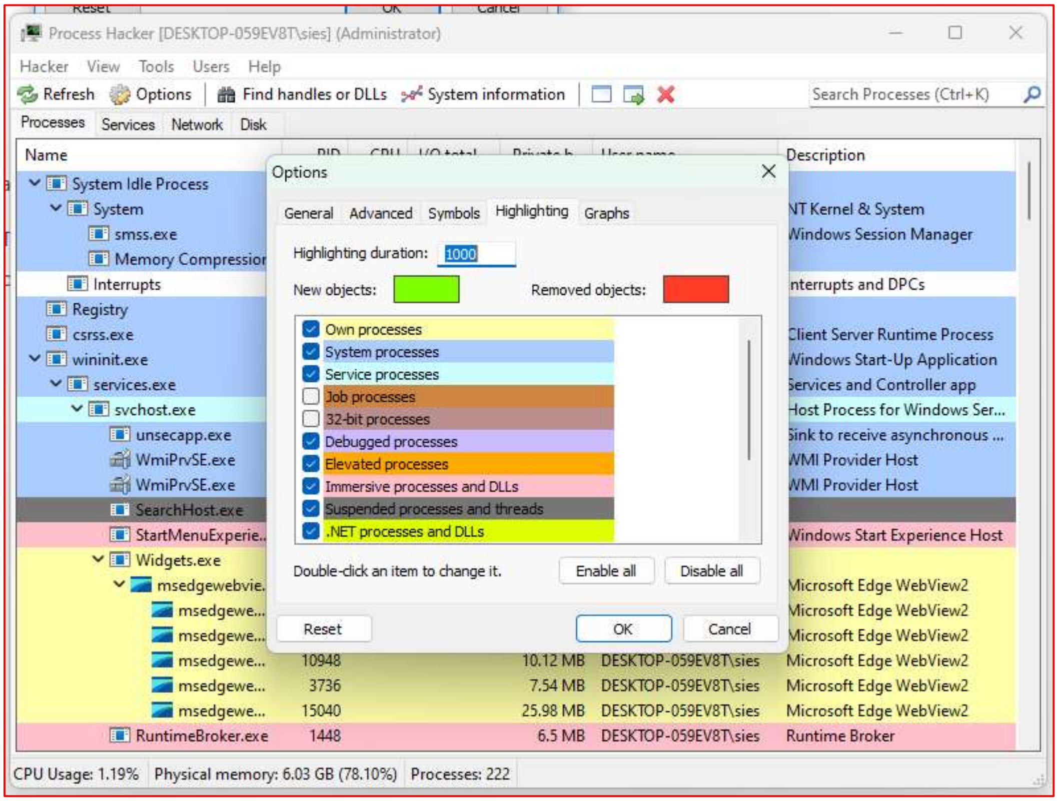
PE viewer: peview.exe "%s"

Max. size unit: EB

Icon processes: 15

- ☑ Allow only one instance
- ☐ Hide when closed
- ☐ Hide when minimized
- ☐ Start when I log on
- ☐ Start hidden
- ☐ Collapse services on start
- ☐ Single-click tray icons
- ☑ Icon click toggles visibility
- ☑ Enable plugins

Select the 'Highlighting' tab to view what each color represents:



Process Hacker [DESKTOP-059EV8T\sies] (Administrator)

Hacker View Tools Users Help
Refresh Options Find handles or DLLs System information
Search Processes (Ctrl+K)
Processes Services Network Disk

Options

General | Advanced | Symbols | Highlighting | Graphs

Highlighting duration: 1000

New objects: 🟩 Removed objects: 🟥

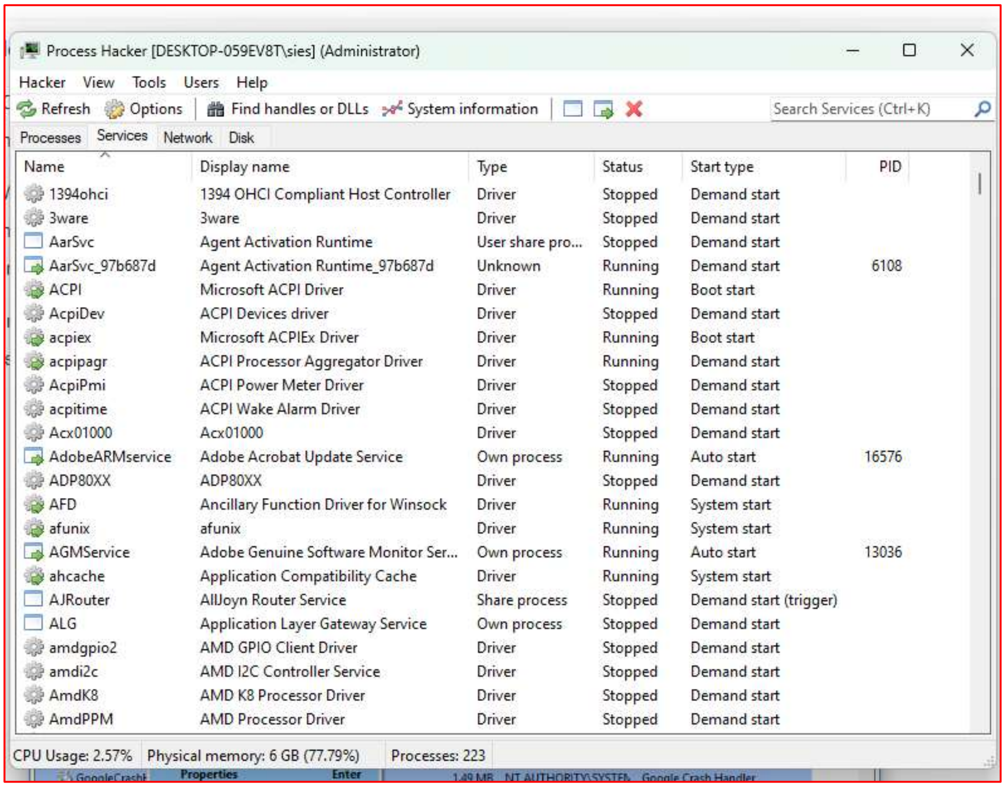
- ☑ Own processes
- ☑ System processes
- ☑ Service processes
- ☐ Job processes
- ☐ 32-bit processes
- ☑ Debugged processes
- ☑ Elevated processes
- ☑ Immersive processes and DLLs
- ☑ Suspended processes and threads
- ☑ .NET processes and DLLs

Double-click an item to change it.

Name	PID	Private b...	User name	Description
System Idle Process				
System				NT Kernel & System
smss.exe				Windows Session Manager
Memory Compression				
Interrupts				Interrupts and DPCs
Registry				
csrss.exe				Client Server Runtime Process
wininit.exe				Windows Start-Up Application
services.exe				Services and Controller app
svchost.exe				Host Process for Windows Ser...
unsecapp.exe				Sink to receive asynchronous ...
WmiPrvSE.exe				WMI Provider Host
WmiPrvSE.exe				WMI Provider Host
SearchHost.exe				
StartMenuExperie...				Windows Start Experience Host
Widgets.exe				
msedgewebvie...				Microsoft Edge WebView2
msedgewe...				Microsoft Edge WebView2
msedgewe...				Microsoft Edge WebView2
msedgewe...	10948	10.12 MB	DESKTOP-059EV8T\sies	Microsoft Edge WebView2
msedgewe...	3736	7.54 MB	DESKTOP-059EV8T\sies	Microsoft Edge WebView2
msedgewe...	15040	25.98 MB	DESKTOP-059EV8T\sies	Microsoft Edge WebView2
RuntimeBroker.exe	1448	6.5 MB	DESKTOP-059EV8T\sies	Runtime Broker

CPU Usage: 1.19% | Physical memory: 6.03 GB (78.10%) | Processes: 222

The image below displays the **services** identified by Process Hacker, services run in the background and don't interact with the desktop.



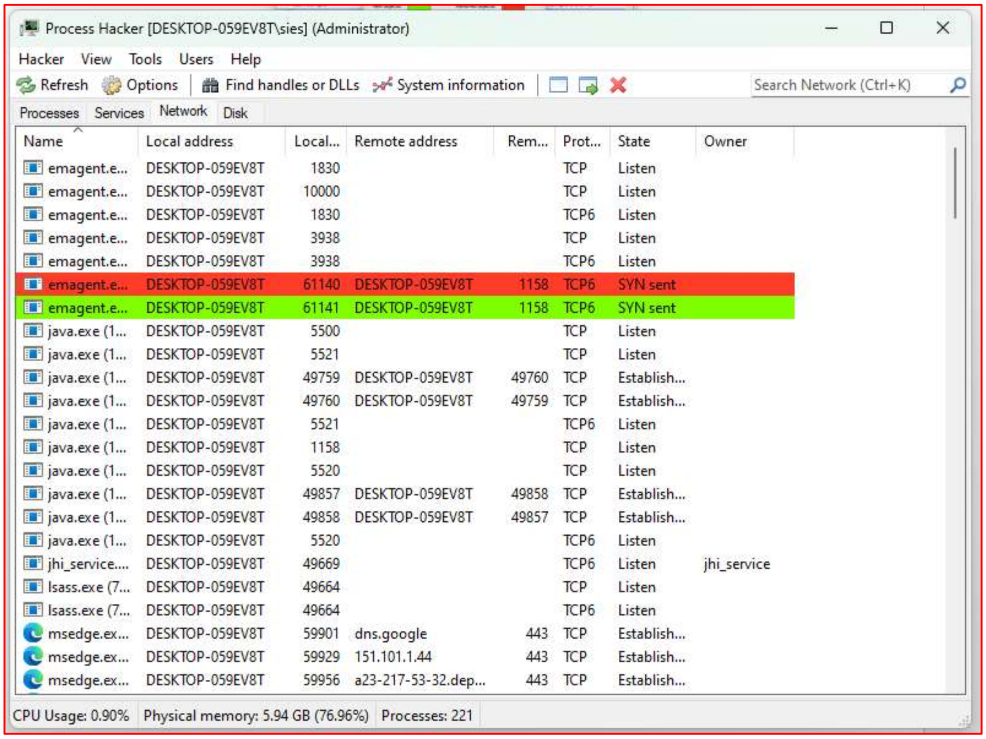
Name	Display name	Type	Status	Start type	PID
1394ohci	1394 OHCI Compliant Host Controller	Driver	Stopped	Demand start	
3ware	3ware	Driver	Stopped	Demand start	
AarSvc	Agent Activation Runtime	User share pro...	Stopped	Demand start	
AarSvc_97b687d	Agent Activation Runtime_97b687d	Unknown	Running	Demand start	6108
ACPI	Microsoft ACPI Driver	Driver	Running	Boot start	
AcpiDev	ACPI Devices driver	Driver	Stopped	Demand start	
acpiex	Microsoft ACPIEx Driver	Driver	Running	Boot start	
acpipagr	ACPI Processor Aggregator Driver	Driver	Running	Demand start	
AcpiPmi	ACPI Power Meter Driver	Driver	Stopped	Demand start	
acpitime	ACPI Wake Alarm Driver	Driver	Stopped	Demand start	
Acx01000	Acx01000	Driver	Stopped	Demand start	
AdobeARMservice	Adobe Acrobat Update Service	Own process	Running	Auto start	16576
ADP80XX	ADP80XX	Driver	Stopped	Demand start	
AFD	Ancillary Function Driver for Winsock	Driver	Running	System start	
afunix	afunix	Driver	Running	System start	
AGMService	Adobe Genuine Software Monitor Ser...	Own process	Running	Auto start	13036
ahcache	Application Compatibility Cache	Driver	Running	System start	
AJRouter	AllJoyn Router Service	Share process	Stopped	Demand start (trigger)	
ALG	Application Layer Gateway Service	Own process	Stopped	Demand start	
amdgpio2	AMD GPIO Client Driver	Driver	Stopped	Demand start	
amdi2c	AMD I2C Controller Service	Driver	Stopped	Demand start	
AmdK8	AMD K8 Processor Driver	Driver	Stopped	Demand start	
AmdPPM	AMD Processor Driver	Driver	Stopped	Demand start	

CPU Usage: 2.57% | Physical memory: 6 GB (77.79%) | Processes: 223

The 'Services' tab displays the following information:

- **Name** of identified service
- **Display name** of service
- **Type** of service identified i.e. Driver
- **Status** of service i.e. Running
- **Start type** i.e. Boot start
- **Process** identifier of service if available

The '**Network**' tab is useful for malware analysis as malware will often try to call home to the bad guy's command and control (c2) infrastructure.



Process Hacker [DESKTOP-059EV8T\sies] (Administrator)
Hacker View Tools Users Help
Refresh Options Find handles or DLLs System information
Search Network (Ctrl+K)
Processes Services Network Disk

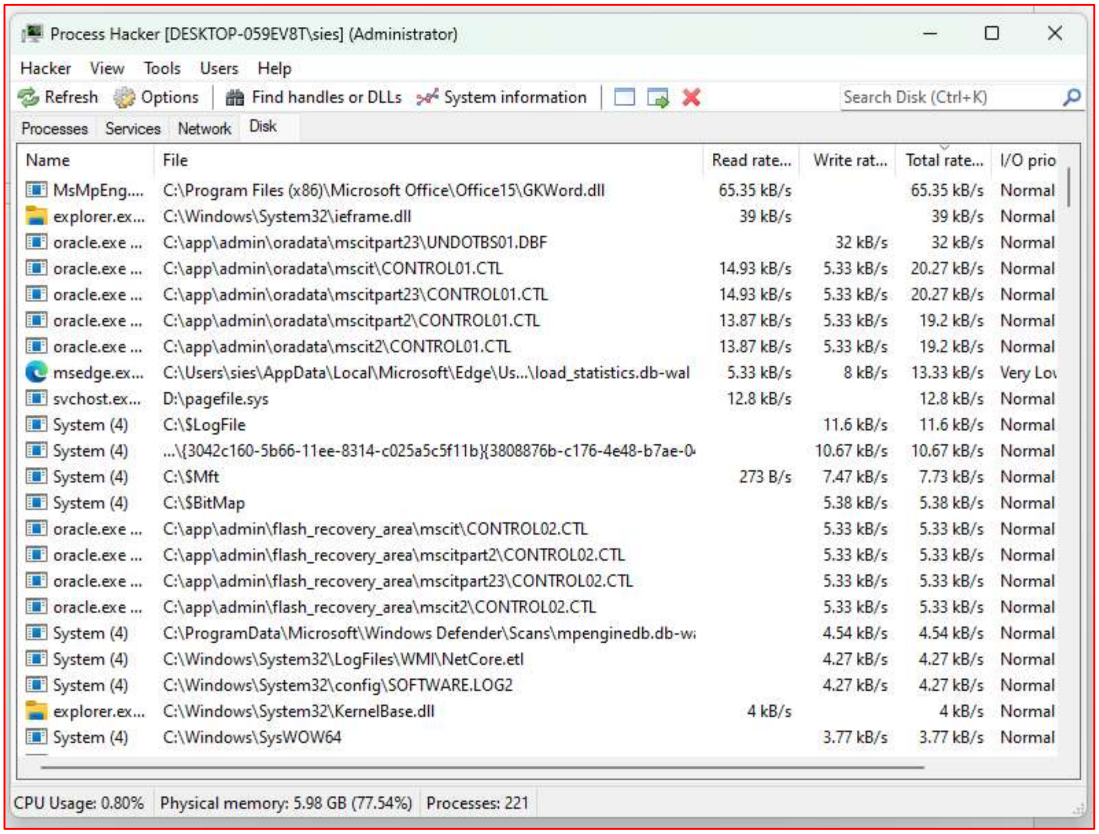
Name	Local address	Local...	Remote address	Rem...	Prot...	State	Owner
emagent.e...	DESKTOP-059EV8T	1830			TCP	Listen	
emagent.e...	DESKTOP-059EV8T	10000			TCP	Listen	
emagent.e...	DESKTOP-059EV8T	1830			TCP6	Listen	
emagent.e...	DESKTOP-059EV8T	3938			TCP	Listen	
emagent.e...	DESKTOP-059EV8T	3938			TCP6	Listen	
emagent.e...	DESKTOP-059EV8T	61140	DESKTOP-059EV8T	1158	TCP6	SYN sent	
emagent.e...	DESKTOP-059EV8T	61141	DESKTOP-059EV8T	1158	TCP6	SYN sent	
java.exe (1...	DESKTOP-059EV8T	5500			TCP	Listen	
java.exe (1...	DESKTOP-059EV8T	5521			TCP	Listen	
java.exe (1...	DESKTOP-059EV8T	49759	DESKTOP-059EV8T	49760	TCP	Establish...	
java.exe (1...	DESKTOP-059EV8T	49760	DESKTOP-059EV8T	49759	TCP	Establish...	
java.exe (1...	DESKTOP-059EV8T	5521			TCP6	Listen	
java.exe (1...	DESKTOP-059EV8T	1158			TCP	Listen	
java.exe (1...	DESKTOP-059EV8T	5520			TCP	Listen	
java.exe (1...	DESKTOP-059EV8T	49857	DESKTOP-059EV8T	49858	TCP	Establish...	
java.exe (1...	DESKTOP-059EV8T	49858	DESKTOP-059EV8T	49857	TCP	Establish...	
java.exe (1...	DESKTOP-059EV8T	5520			TCP6	Listen	
jhi_service....	DESKTOP-059EV8T	49669			TCP6	Listen	jhi_service
lsass.exe (7...	DESKTOP-059EV8T	49664			TCP	Listen	
lsass.exe (7...	DESKTOP-059EV8T	49664			TCP6	Listen	
msedge.ex...	DESKTOP-059EV8T	59901	dns.google	443	TCP	Establish...	
msedge.ex...	DESKTOP-059EV8T	59929	151.101.1.44	443	TCP	Establish...	
msedge.ex...	DESKTOP-059EV8T	59956	a23-217-53-32.dep...	443	TCP	Establish...	

CPU Usage: 0.90% Physical memory: 5.94 GB (76.96%) Processes: 221

The ‘Network’ tab displays the following information:

- **Process name** and PID
- **Local address**
- **Local port** used by the process
- **Remote address** the process is connecting to
- **Remote port** of network connection
- **Protocol** used by the process
- **State** of identified network connection
- **Owner**

The ‘Disk’ tab displays information relating to files on the device hard drive which are being used:


Process Hacker [DESKTOP-059EV8T\sies] (Administrator)
Hacker View Tools Users Help
Refresh Options Find handles or DLLs System information
Search Disk (Ctrl+K)
Processes Services Network Disk

Name	File	Read rate...	Write rat...	Total rate...	I/O prio
MsMpEng....	C:\Program Files (x86)\Microsoft Office\Office15\GKWord.dll	65.35 kB/s		65.35 kB/s	Normal
explorer.ex...	C:\Windows\System32\ieframe.dll	39 kB/s		39 kB/s	Normal
oracle.exe ...	C:\app\admin\oradata\mscitpart23\UNDOTBS01.DBF		32 kB/s	32 kB/s	Normal
oracle.exe ...	C:\app\admin\oradata\mscit\CONTROL01.CTL	14.93 kB/s	5.33 kB/s	20.27 kB/s	Normal
oracle.exe ...	C:\app\admin\oradata\mscitpart23\CONTROL01.CTL	14.93 kB/s	5.33 kB/s	20.27 kB/s	Normal
oracle.exe ...	C:\app\admin\oradata\mscitpart2\CONTROL01.CTL	13.87 kB/s	5.33 kB/s	19.2 kB/s	Normal
oracle.exe ...	C:\app\admin\oradata\mscit2\CONTROL01.CTL	13.87 kB/s	5.33 kB/s	19.2 kB/s	Normal
msedge.ex...	C:\Users\sies\AppData\Local\Microsoft\Edge\Us...\load_statistics.db-wal	5.33 kB/s	8 kB/s	13.33 kB/s	Very Lov
svchost.ex...	D:\pagefile.sys	12.8 kB/s		12.8 kB/s	Normal
System (4)	C:\$LogFile		11.6 kB/s	11.6 kB/s	Normal
System (4)	...\{3042c160-5b66-11ee-8314-c025a5c5f11b}{3808876b-c176-4e48-b7ae-0		10.67 kB/s	10.67 kB/s	Normal
System (4)	C:\$Mft	273 B/s	7.47 kB/s	7.73 kB/s	Normal
System (4)	C:\$BitMap		5.38 kB/s	5.38 kB/s	Normal
oracle.exe ...	C:\app\admin\flash_recovery_area\mscit\CONTROL02.CTL		5.33 kB/s	5.33 kB/s	Normal
oracle.exe ...	C:\app\admin\flash_recovery_area\mscitpart2\CONTROL02.CTL		5.33 kB/s	5.33 kB/s	Normal
oracle.exe ...	C:\app\admin\flash_recovery_area\mscitpart23\CONTROL02.CTL		5.33 kB/s	5.33 kB/s	Normal
oracle.exe ...	C:\app\admin\flash_recovery_area\mscit2\CONTROL02.CTL		5.33 kB/s	5.33 kB/s	Normal
System (4)	C:\ProgramData\Microsoft\Windows Defender\Scans\mpenginedb.db-wa		4.54 kB/s	4.54 kB/s	Normal
System (4)	C:\Windows\System32\LogFiles\WMI\NetCore.etl		4.27 kB/s	4.27 kB/s	Normal
System (4)	C:\Windows\System32\config\SOFTWARE.LOG2		4.27 kB/s	4.27 kB/s	Normal
explorer.ex...	C:\Windows\System32\KernelBase.dll	4 kB/s		4 kB/s	Normal
System (4)	C:\Windows\SysWOW64		3.77 kB/s	3.77 kB/s	Normal

CPU Usage: 0.80% | Physical memory: 5.98 GB (77.54%) | Processes: 221

The ‘Disk’ tab displays the following information:

- **Process name** and PID
- **File** location on disk
- **Read rate average** in realtime of the hard drive
- **Write rate average** in realtime of the hard drive
- **Total rate average** of read and write output
- **I/O priority**
- **Response time**

2.Process Monitor (ProcMon)

Description:-

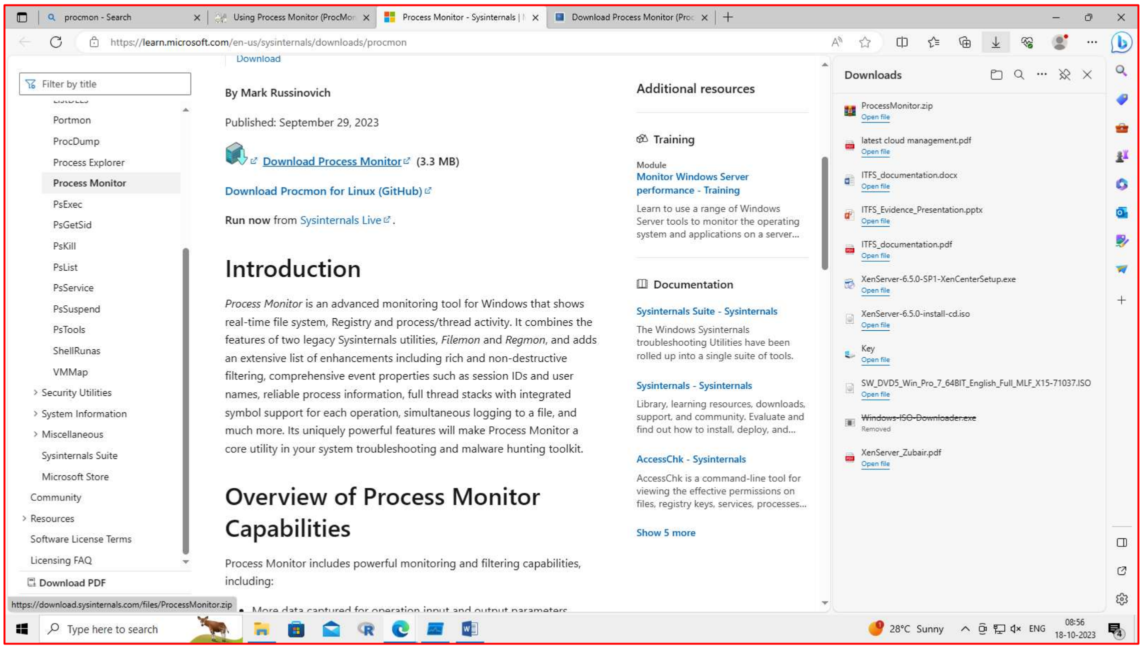
The **Process Monitor (ProcMon)** tool is used to track the various processes activity in the Windows operating system. This utility allows you to show how processes access files on disk, registry keys, remote resources, etc. in real-time. The ProcMon combines the capabilities of two legacy Sysinternals utilities at once — **FileMon** and **RegMon**.

With Process Monitor, you can:

- Track the startup and shutdown events of processes and threads, including information about the exit code;
- Collect data on the parameters of input and output operations;
- Set filters to display only the necessary information. For example, about the actions of a specific process, access to a specific file or a registry key;
- Log all operations during system boot (starting processes, services). This is useful for diagnosing slow Windows boot.

Steps:-

Download the ProcMon tool from google.



https://learn.microsoft.com/en-us/sysinternals/downloads/procmon

By Mark Russinovich

Published: September 29, 2023

Download Process Monitor (3.3 MB)

Download Procmon for Linux (GitHub)

Run now from Sysinternals Live.

Introduction

Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity. It combines the features of two legacy Sysinternals utilities, *Filemon* and *Regmon*, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such as session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more. Its uniquely powerful features will make Process Monitor a core utility in your system troubleshooting and malware hunting toolkit.

Overview of Process Monitor Capabilities

Process Monitor includes powerful monitoring and filtering capabilities, including:

- More data captured for operation input and output parameters

Additional resources

Training

Module

Monitor Windows Server performance - Training

Learn to use a range of Windows Server tools to monitor the operating system and applications on a server...

Documentation

Sysinternals Suite - Sysinternals

The Windows Sysinternals troubleshooting Utilities have been rolled up into a single suite of tools.

Sysinternals - Sysinternals

Library, learning resources, downloads, support, and community. Evaluate and find out how to install, deploy, and...

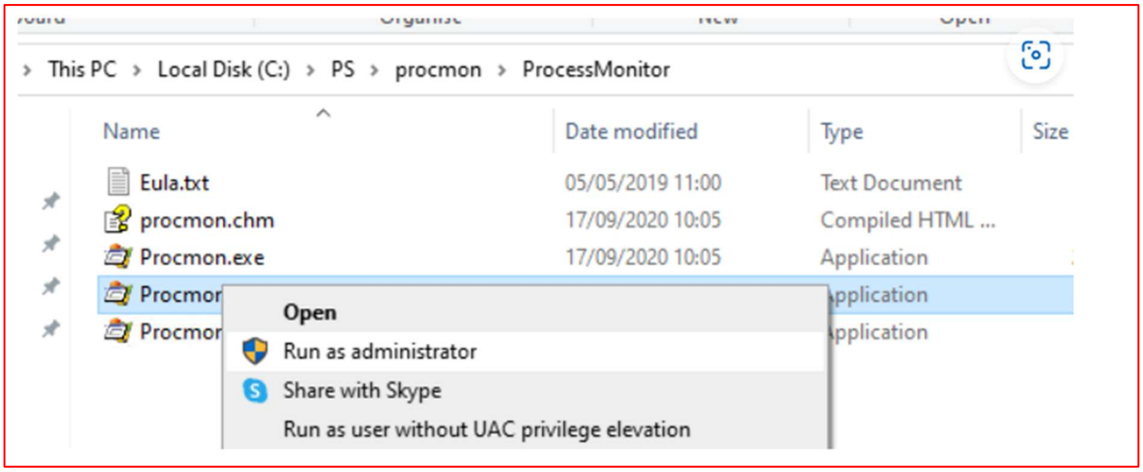
AccessChk - Sysinternals

AccessChk is a command-line tool for viewing the effective permissions on files, registry keys, services, processes...

Show 5 more

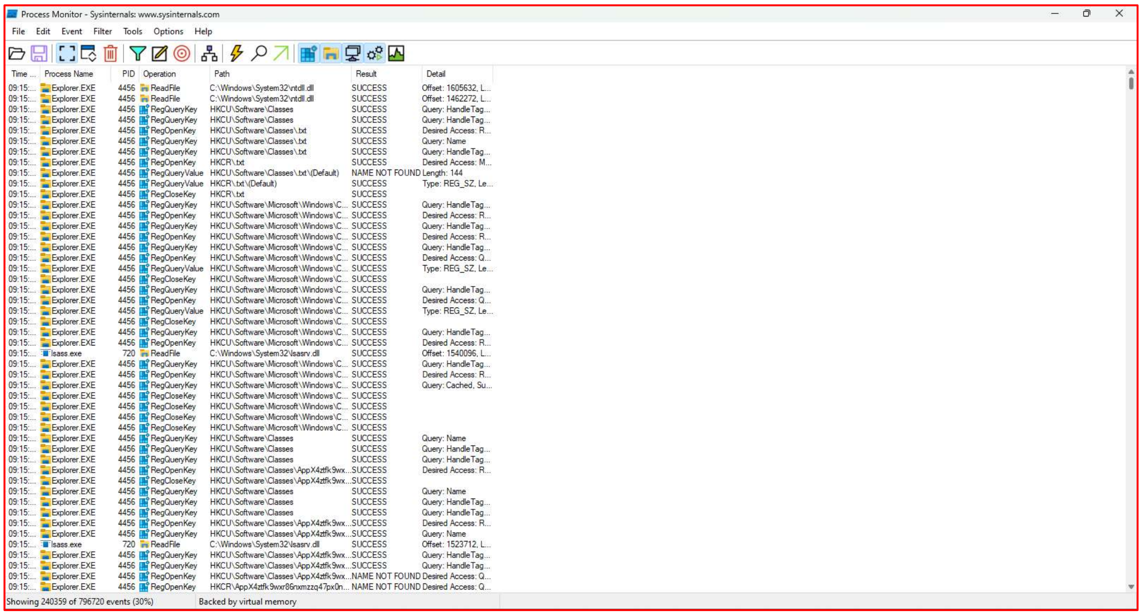
https://download.sysinternals.com/files/ProcessMonitor.zip

Extract the zip file and open the Procmon.exe (Application) any one file to be installed.


This PC › Local Disk (C:) › PS › procmon › ProcessMonitor
Open
Run as administrator
Share with Skype
Run as user without UAC privilege elevation

Name	Date modified	Type	Size
Eula.txt	05/05/2019 11:00	Text Document	
procmon.chm	17/09/2020 10:05	Compiled HTML ...	
Procmon.exe	17/09/2020 10:05	Application	
Procmor		pplication	
Procmor		pplication	

The moment you run procmon, it begins capturing many different kinds of Windows events.



Time ...	Process Name	PID	Operation	Path	Result	Detail
09:15:...	Explorer.EXE	4456	ReadFile	C:\Windows\System32\ntdll.dll	SUCCESS	Offset: 1605632, L...
09:15:...	Explorer.EXE	4456	ReadFile	C:\Windows\System32\ntdll.dll	SUCCESS	Offset: 1462272, L...
09:15:...	Explorer.EXE	4456	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
09:15:...	Explorer.EXE	4456	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
09:15:...	Explorer.EXE	4456	RegOpenKey	HKCU\Software\Classes\.txt	SUCCESS	Desired Access: R...
09:15:...	Explorer.EXE	4456	RegQueryKey	HKCU\Software\Classes\.txt	SUCCESS	Query: Name
09:15:...	Explorer.EXE	4456	RegQueryKey	HKCU\Software\Classes\.txt	SUCCESS	Query: HandleTag...
09:15:...	Explorer.EXE	4456	RegOpenKey	HKCR\.txt	SUCCESS	Desired Access: M...
09:15:...	Explorer.EXE	4456	RegQueryValue	HKCU\Software\Classes\.txt\(Default)	NAME NOT FOUND	Length: 144
09:15:...	Explorer.EXE	4456	RegQueryValue	HKCR\.txt\(Default)	SUCCESS	Type: REG_SZ, Le...
09:15:...	Explorer.EXE	4456	RegCloseKey	HKCR\.txt	SUCCESS	
09:15:...	Explorer.EXE	4456	RegQueryKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Query: HandleTag...
09:15:...	Explorer.EXE	4456	RegOpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Desired Access: R...
09:15:...	Explorer.EXE	4456	RegQueryKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Query: HandleTag...
09:15:...	Explorer.EXE	4456	RegOpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Desired Access: R...
09:15:...	Explorer.EXE	4456	RegQueryKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Query: HandleTag...
09:15:...	Explorer.EXE	4456	RegOpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Desired Access: Q...
09:15:...	Explorer.EXE	4456	RegQueryValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Type: REG_SZ, Le...
09:15:...	Explorer.EXE	4456	RegCloseKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	
09:15:...	Explorer.EXE	4456	RegQueryKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Query: HandleTag...
09:15:...	Explorer.EXE	4456	RegOpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Desired Access: Q...
09:15:...	Explorer.EXE	4456	RegQueryValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Type: REG_SZ, Le...
09:15:...	Explorer.EXE	4456	RegCloseKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	
09:15:...	Explorer.EXE	4456	RegQueryKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Query: HandleTag...
09:15:...	Explorer.EXE	4456	RegOpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Desired Access: R...
09:15:...	lsass.exe	720	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1540096, L...
09:15:...	Explorer.EXE	4456	RegQueryKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Query: HandleTag...
09:15:...	Explorer.EXE	4456	RegOpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Desired Access: R...
09:15:...	Explorer.EXE	4456	RegQueryKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Query: Cached, Su...
09:15:...	Explorer.EXE	4456	RegCloseKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	
09:15:...	Explorer.EXE	4456	RegCloseKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	
09:15:...	Explorer.EXE	4456	RegCloseKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	
09:15:...	Explorer.EXE	4456	RegCloseKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	
09:15:...	Explorer.EXE	4456	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
09:15:...	Explorer.EXE	4456	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
09:15:...	Explorer.EXE	4456	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
09:15:...	Explorer.EXE	4456	RegOpenKey	HKCU\Software\Classes\AppX4ztfk9wx...	SUCCESS	Desired Access: R...
09:15:...	Explorer.EXE	4456	RegCloseKey	HKCU\Software\Classes\AppX4ztfk9wx...	SUCCESS	
09:15:...	Explorer.EXE	4456	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
09:15:...	Explorer.EXE	4456	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
09:15:...	Explorer.EXE	4456	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
09:15:...	Explorer.EXE	4456	RegOpenKey	HKCU\Software\Classes\AppX4ztfk9wx...	SUCCESS	Desired Access: R...
09:15:...	Explorer.EXE	4456	RegQueryKey	HKCU\Software\Classes\AppX4ztfk9wx...	SUCCESS	Query: Name
09:15:...	lsass.exe	720	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1523712, L...
09:15:...	Explorer.EXE	4456	RegQueryKey	HKCU\Software\Classes\AppX4ztfk9wx...	SUCCESS	Query: HandleTag...
09:15:...	Explorer.EXE	4456	RegQueryKey	HKCU\Software\Classes\AppX4ztfk9wx...	SUCCESS	Query: HandleTag...
09:15:...	Explorer.EXE	4456	RegOpenKey	HKCU\Software\Classes\AppX4ztfk9wx...	NAME NOT FOUND	Desired Access: Q...
09:15:...	Explorer.EXE	4456	RegOpenKey	HKCR\AppX4ztfk9wxr86nxmzzq47px0n...	NAME NOT FOUND	Desired Access: Q...

Showing 240359 of 796720 events (30%)   Backed by virtual memory

As you can see in the screenshot above under the **Operation** column, there are various icons each representing different classes of Windows events. Procmon captures events from five different classes:

- Registry
- Filesystem
- Network
- Processes
- Profiling events

Each event in all classes is represented in a single list pane of seven columns:

Time of day – The time the event occurred.

Process name – The name of the process that triggered the event.

PID – The process identifier.

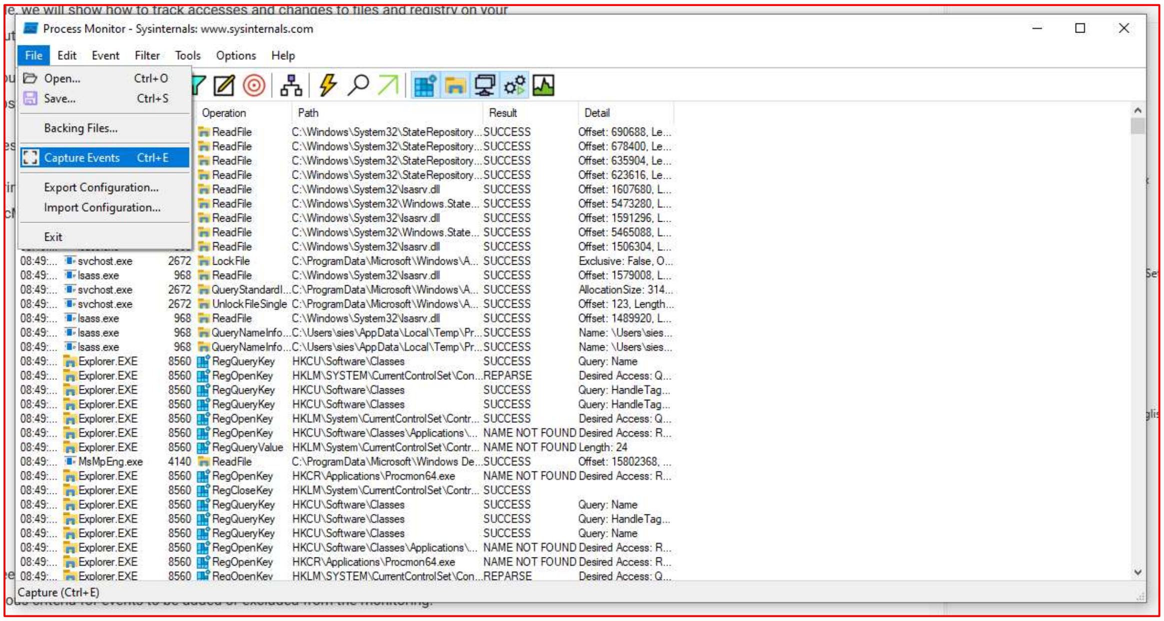
Operation – The type of event like if the process opened a file, changed a registry key value, etc.

Path – The path to the object the event interacted with like a file path, registry path, etc.

Result – This column will contain numerous values to indicate the result of the event. This value can be as simple as SUCCESS or specific to the event like REPARSE, BUFFER OVERFLOW, NAME NOT FOUND, etc.

Detail – This column contains all of the nitty-gritty detail once you pinpoint an event you'd like to see.

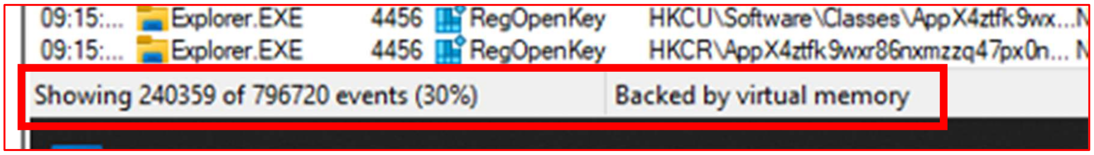
To capture events, go to file > Capture events



			Operation	Path	Result	Detail
			ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 690688, Le...
			ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 678400, Le...
			ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 635904, Le...
			ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 623616, Le...
			ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1607680, L...
			ReadFile	C:\Windows\System32\Windows.State...	SUCCESS	Offset: 5473280, L...
			ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1591296, L...
			ReadFile	C:\Windows\System32\Windows.State...	SUCCESS	Offset: 5465088, L...
			ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1506304, L...
08:49:...	svchost.exe	2672	LockFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
08:49:...	lsass.exe	968	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1579008, L...
08:49:...	svchost.exe	2672	QueryStandardI...	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	AllocationSize: 314...
08:49:...	svchost.exe	2672	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 123, Length...
08:49:...	lsass.exe	968	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1489920, L...
08:49:...	lsass.exe	968	QueryNameInfo...	C:\Users\sies\AppData\Local\Temp\Pr...	SUCCESS	Name: \Users\sies...
08:49:...	lsass.exe	968	QueryNameInfo...	C:\Users\sies\AppData\Local\Temp\Pr...	SUCCESS	Name: \Users\sies...
08:49:...	Explorer.EXE	8560	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
08:49:...	Explorer.EXE	8560	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
08:49:...	Explorer.EXE	8560	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
08:49:...	Explorer.EXE	8560	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
08:49:...	Explorer.EXE	8560	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
08:49:...	Explorer.EXE	8560	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: R...
08:49:...	Explorer.EXE	8560	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 24
08:49:...	MsMpEng.exe	4140	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 15802368, ...
08:49:...	Explorer.EXE	8560	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
08:49:...	Explorer.EXE	8560	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
08:49:...	Explorer.EXE	8560	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
08:49:...	Explorer.EXE	8560	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
08:49:...	Explorer.EXE	8560	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
08:49:...	Explorer.EXE	8560	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: R...
08:49:...	Explorer.EXE	8560	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
08:49:...	Explorer.EXE	8560	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...

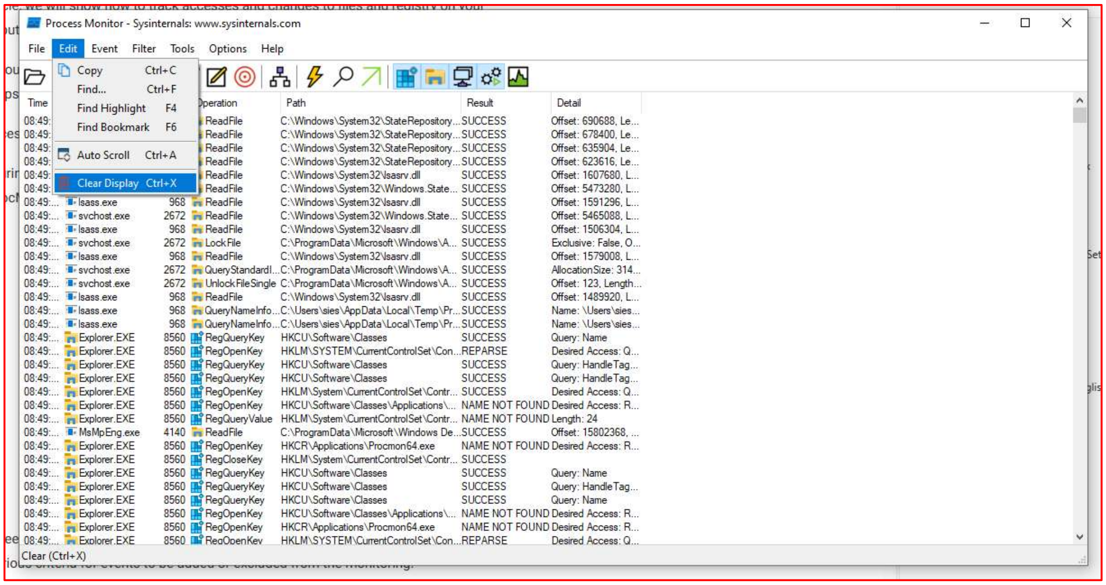
Capture (Ctrl+E)

Number of Events in the Window seen at the bottom:



```
09:15:...  Explorer.EXE    4456  RegOpenKey   HKCU\Software\Classes\AppX4ztfk9wx...N
09:15:...  Explorer.EXE    4456  RegOpenKey   HKCR\AppX4ztfk9wxr86nxmzzq47px0n... N
Showing 240359 of 796720 events (30%)          Backed by virtual memory
```

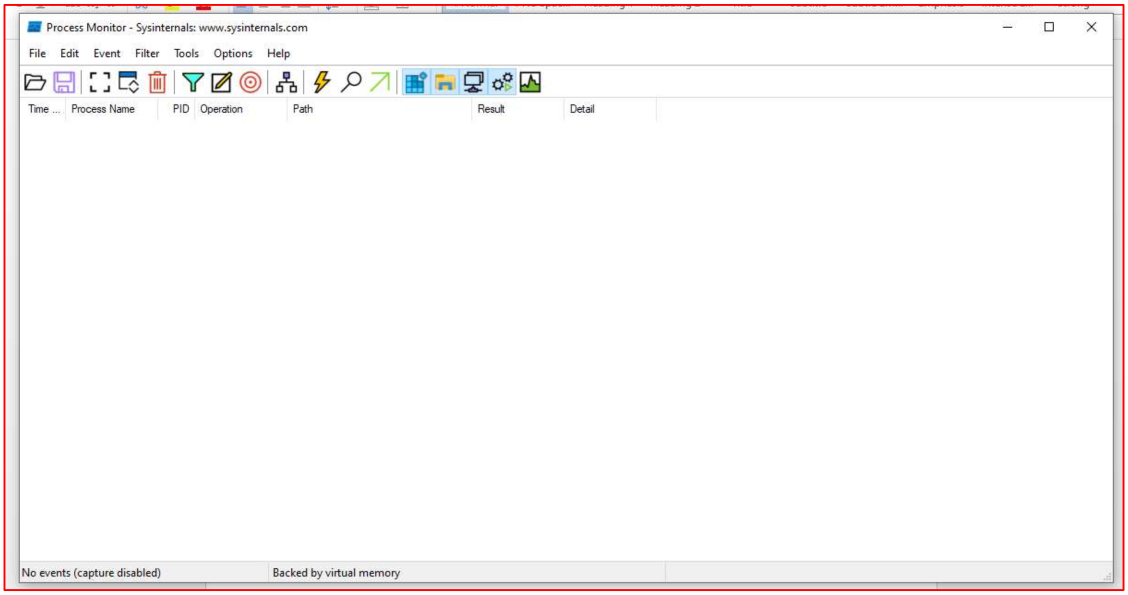
To Clear Display, go to file > Clear Display (Don’t perform until practical is completed)



Time			Operation	Path	Result	Detail
08:49:			ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 690688, Le...
08:49:			ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 678400, Le...
08:49:			ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 635904, Le...
08:49:			ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 623616, Le...
08:49:			ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1607680, L...
08:49:			ReadFile	C:\Windows\System32\Windows.State...	SUCCESS	Offset: 5473280, L...
08:49:...	lsass.exe	968	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1591296, L...
08:49:...	svchost.exe	2672	ReadFile	C:\Windows\System32\Windows.State...	SUCCESS	Offset: 5465088, L...
08:49:...	lsass.exe	968	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1506304, L...
08:49:...	svchost.exe	2672	LockFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
08:49:...	lsass.exe	968	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1579008, L...
08:49:...	svchost.exe	2672	QueryStandardI...	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	AllocationSize: 314...
08:49:...	svchost.exe	2672	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 123, Length...
08:49:...	lsass.exe	968	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1489920, L...
08:49:...	lsass.exe	968	QueryNameInfo...	C:\Users\sies\AppData\Local\Temp\Pr...	SUCCESS	Name: \Users\sies...
08:49:...	lsass.exe	968	QueryNameInfo...	C:\Users\sies\AppData\Local\Temp\Pr...	SUCCESS	Name: \Users\sies...
08:49:...	Explorer.EXE	8560	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
08:49:...	Explorer.EXE	8560	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
08:49:...	Explorer.EXE	8560	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
08:49:...	Explorer.EXE	8560	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
08:49:...	Explorer.EXE	8560	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
08:49:...	Explorer.EXE	8560	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: R...
08:49:...	Explorer.EXE	8560	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 24
08:49:...	MsMpEng.exe	4140	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 15802368, ...
08:49:...	Explorer.EXE	8560	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
08:49:...	Explorer.EXE	8560	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
08:49:...	Explorer.EXE	8560	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
08:49:...	Explorer.EXE	8560	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
08:49:...	Explorer.EXE	8560	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
08:49:...	Explorer.EXE	8560	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: R...
08:49:...	Explorer.EXE	8560	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
08:49:...	Explorer.EXE	8560	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...

Clear (Ctrl+X)

After Display is cleared.



Time ...	Process Name	PID	Operation	Path	Result	Detail

No events (capture disabled)

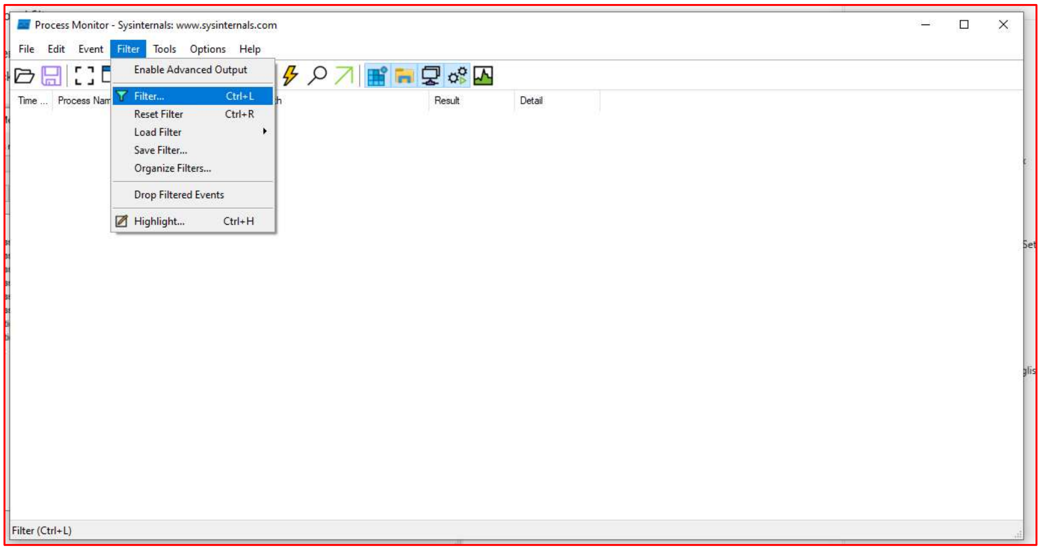
Backed by virtual memory

Events Filter:-

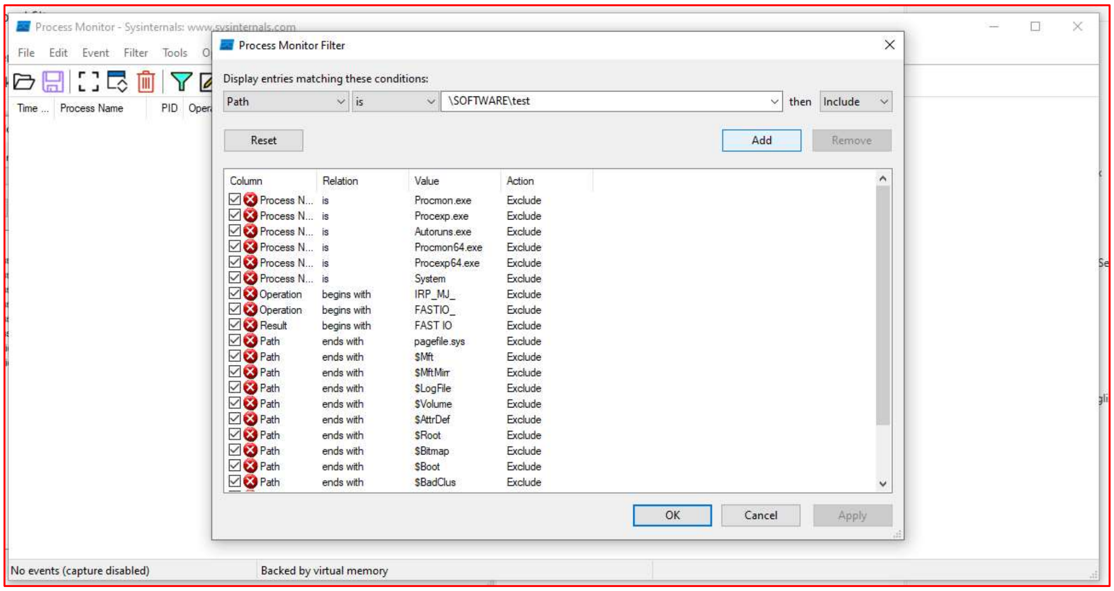
The filters allow you to specify various criteria for events to be added or excluded from the monitoring.

The default filter already excludes events of a standard Windows system activity and the procmon.exe process itself. In most cases, you don’t need to remove these filters. We’ll add some additional filters.

To access Event Filters, Go to Filter > Click on Filter



Create a filter for monitoring access to the registry key: Path > contains > \SOFTWARE\test > Include. Click Add to add a new filter to the list.

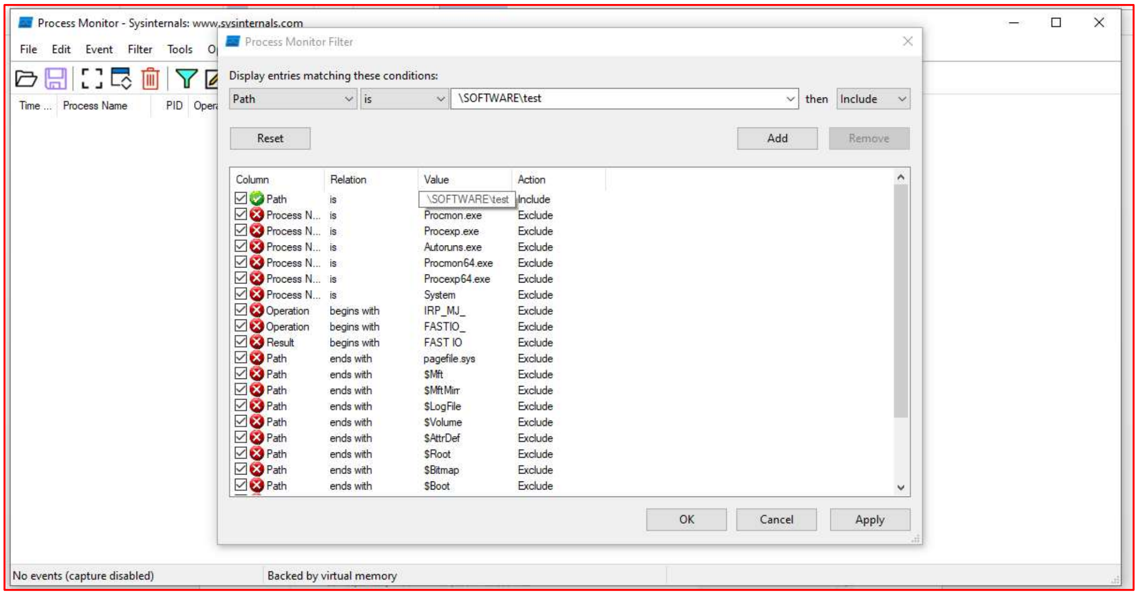


Display entries matching these conditions:

Path | is | \SOFTWARE\test | then | Include

Column	Relation	Value	Action
☑ Process N...	is	Procmon.exe	Exclude
☑ Process N...	is	Procexp.exe	Exclude
☑ Process N...	is	Autoruns.exe	Exclude
☑ Process N...	is	Procmon64.exe	Exclude
☑ Process N...	is	Procexp64.exe	Exclude
☑ Process N...	is	System	Exclude
☑ Operation	begins with	IRP_MJ_	Exclude
☑ Operation	begins with	FASTIO_	Exclude
☑ Result	begins with	FAST IO	Exclude
☑ Path	ends with	pagefile.sys	Exclude
☑ Path	ends with	$Mft	Exclude
☑ Path	ends with	$MftMirr	Exclude
☑ Path	ends with	$LogFile	Exclude
☑ Path	ends with	$Volume	Exclude
☑ Path	ends with	$AttrDef	Exclude
☑ Path	ends with	$Root	Exclude
☑ Path	ends with	$Bitmap	Exclude
☑ Path	ends with	$Boot	Exclude
☑ Path	ends with	$BadClus	Exclude

Path added successfully


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools O
Time ... Process Name PID Opera
Process Monitor Filter
Reset
Add
Remove
OK
Cancel
Apply
No events (capture disabled)
Backed by virtual memory

Display entries matching these conditions:

Path | is | \SOFTWARE\test | then | Include

Column	Relation	Value	Action
☑ ✓ Path	is	\SOFTWARE\test	Include
☑ ✗ Process N...	is	Procmon.exe	Exclude
☑ ✗ Process N...	is	Procexp.exe	Exclude
☑ ✗ Process N...	is	Autoruns.exe	Exclude
☑ ✗ Process N...	is	Procmon64.exe	Exclude
☑ ✗ Process N...	is	Procexp64.exe	Exclude
☑ ✗ Process N...	is	System	Exclude
☑ ✗ Operation	begins with	IRP_MJ_	Exclude
☑ ✗ Operation	begins with	FASTIO_	Exclude
☑ ✗ Result	begins with	FAST IO	Exclude
☑ ✗ Path	ends with	pagefile.sys	Exclude
☑ ✗ Path	ends with	$Mft	Exclude
☑ ✗ Path	ends with	$MftMirr	Exclude
☑ ✗ Path	ends with	$LogFile	Exclude
☑ ✗ Path	ends with	$Volume	Exclude
☑ ✗ Path	ends with	$AttrDef	Exclude
☑ ✗ Path	ends with	$Root	Exclude
☑ ✗ Path	ends with	$Bitmap	Exclude
☑ ✗ Path	ends with	$Boot	Exclude

3.Microsoft Network Monitor

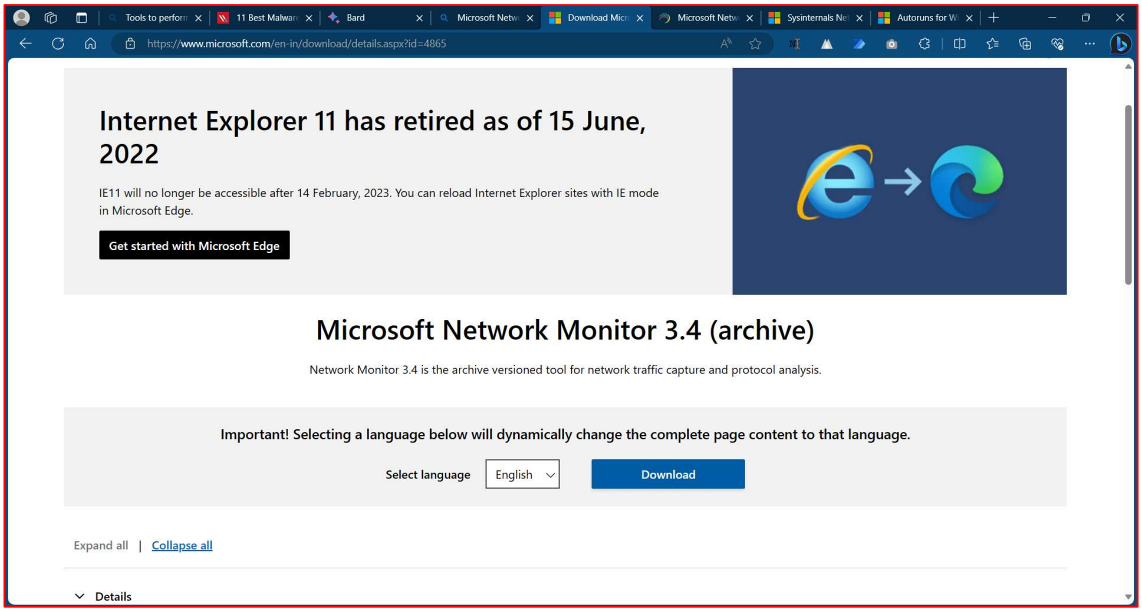
Description:-

It is a software utility designed to help users capture network traffic and analyze incoming and outgoing packets. The packet analyzer is included in a user-friendly interface, bundled with intuitive options.

A packet sniffer can be used to troubleshoot application connectivity issues. For example, you can detect programs that use a lot of traffic, which is often a sign of malware activity. Packet analyzers are also great for security analysis, whether you're an expert or not.

Steps:-

Download Microsoft Network Monitor (3.4) by searching it on google.



https://www.microsoft.com/en-in/download/details.aspx?id=4865

Internet Explorer 11 has retired as of 15 June, 2022

IE11 will no longer be accessible after 14 February, 2023. You can reload Internet Explorer sites with IE mode in Microsoft Edge.

Get started with Microsoft Edge

Microsoft Network Monitor 3.4 (archive)

Network Monitor 3.4 is the archive versioned tool for network traffic capture and protocol analysis.

Important! Selecting a language below will dynamically change the complete page content to that language.

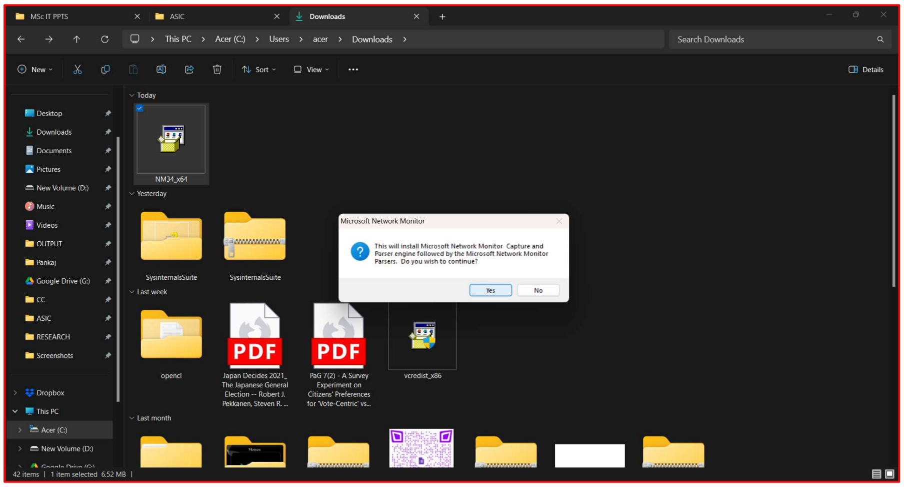
Select language: English

Download

Expand all | Collapse all

Details

Click on the downloaded file (NM34_x64) > A pop up will appear, tap yes.

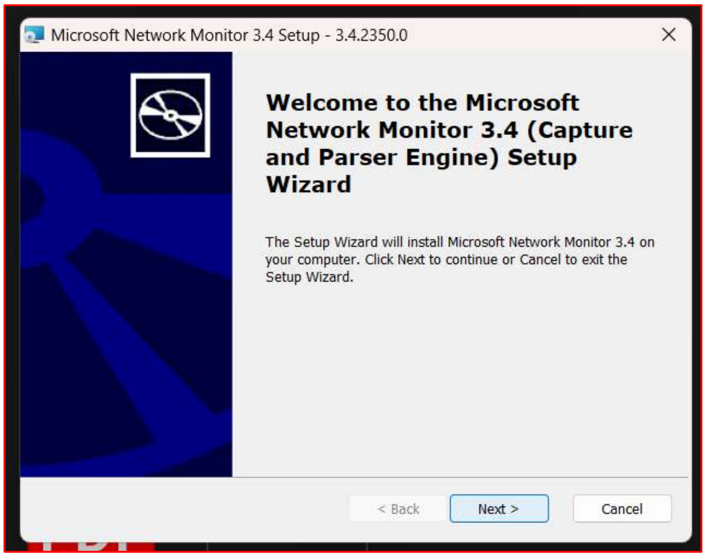


Microsoft Network Monitor

This will install Microsoft Network Monitor Capture and Parser engine followed by the Microsoft Network Monitor Parsers. Do you wish to continue?

Yes No

Click next

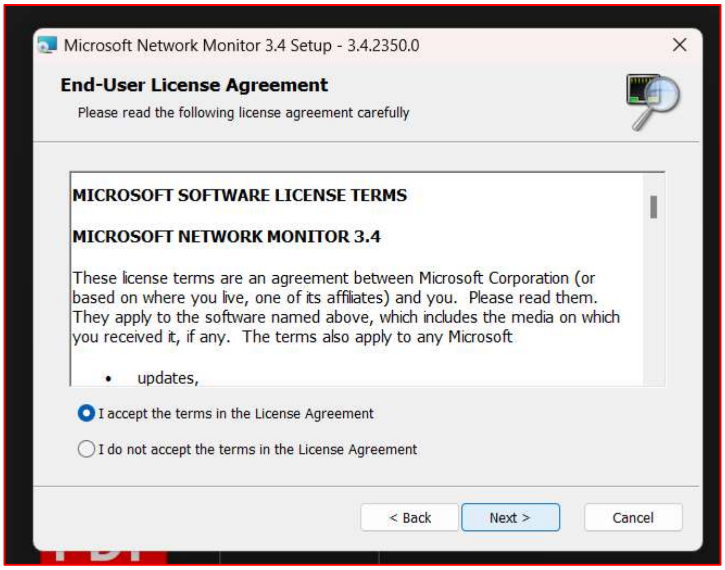


Microsoft Network Monitor 3.4 Setup - 3.4.2350.0

Welcome to the Microsoft Network Monitor 3.4 (Capture and Parser Engine) Setup Wizard

The Setup Wizard will install Microsoft Network Monitor 3.4 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Accept the terms and conditions and click on next



Microsoft Network Monitor 3.4 Setup - 3.4.2350.0

End-User License Agreement

Please read the following license agreement carefully

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT NETWORK MONITOR 3.4

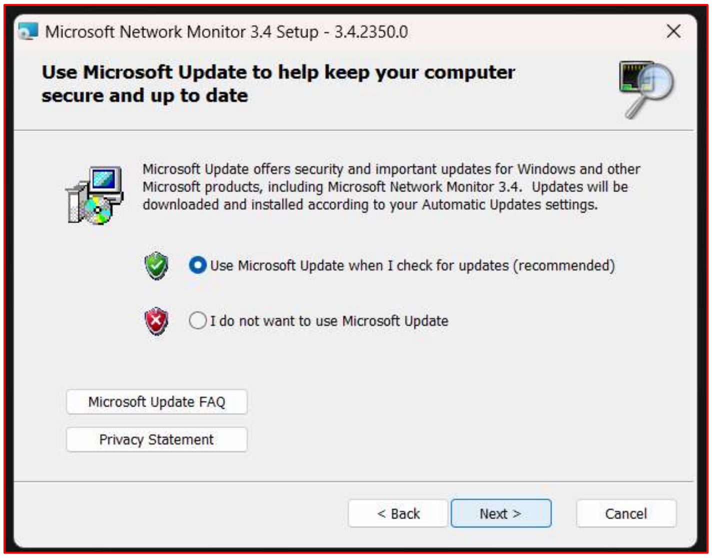
These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

- updates,

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

Choose, use Microsoft Update and click on next



Microsoft Network Monitor 3.4 Setup - 3.4.2350.0

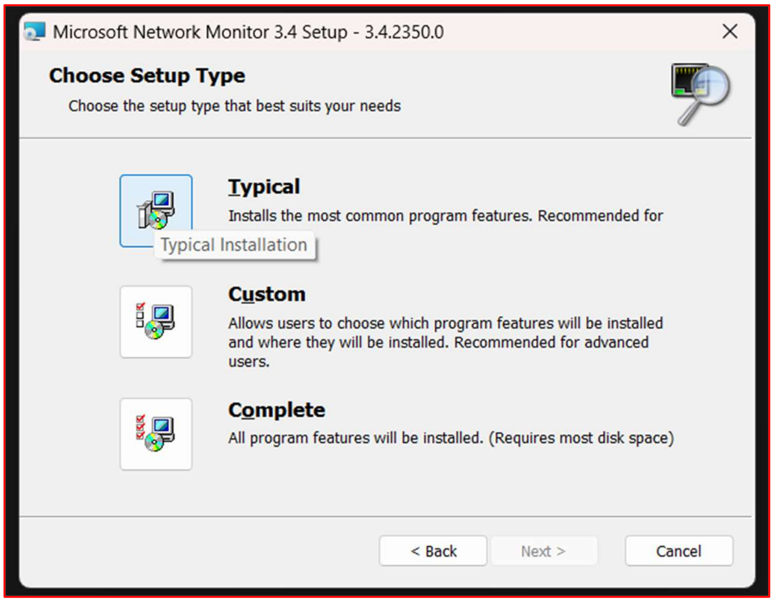
Use Microsoft Update to help keep your computer secure and up to date

Microsoft Update offers security and important updates for Windows and other Microsoft products, including Microsoft Network Monitor 3.4. Updates will be downloaded and installed according to your Automatic Updates settings.

● Use Microsoft Update when I check for updates (recommended)

○ I do not want to use Microsoft Update

Click on Typical



Microsoft Network Monitor 3.4 Setup - 3.4.2350.0

Choose Setup Type

Choose the setup type that best suits your needs

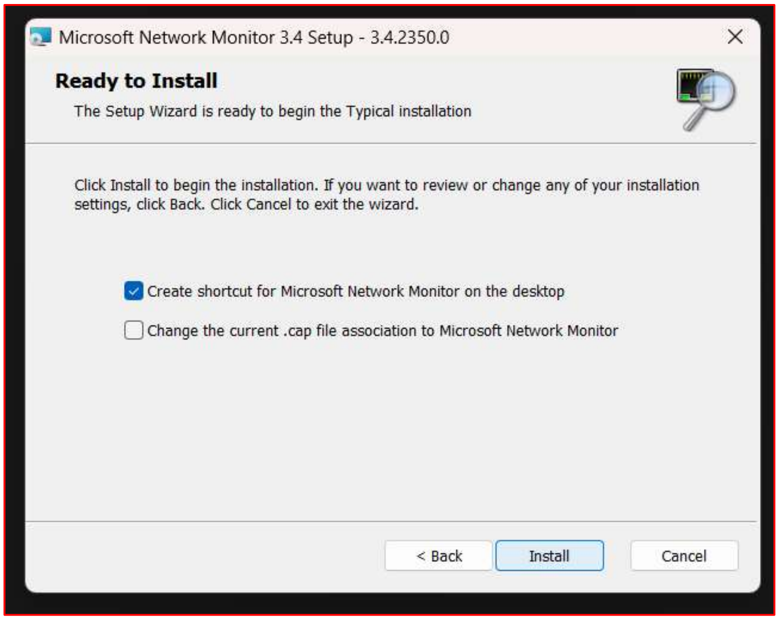
Typical
Installs the most common program features. Recommended for

Typical Installation

Custom
Allows users to choose which program features will be installed and where they will be installed. Recommended for advanced users.

Complete
All program features will be installed. (Requires most disk space)

Click on Install



Microsoft Network Monitor 3.4 Setup - 3.4.2350.0

Ready to Install

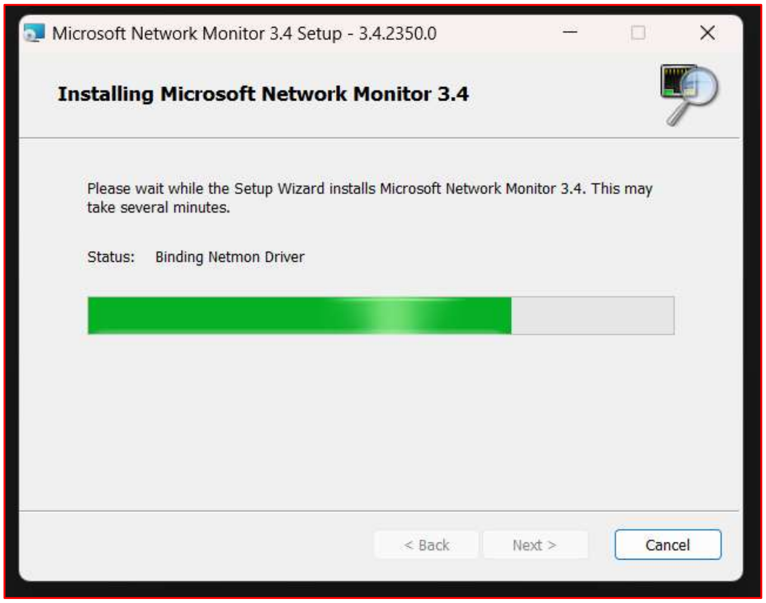
The Setup Wizard is ready to begin the Typical installation

Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

☑ Create shortcut for Microsoft Network Monitor on the desktop

□ Change the current .cap file association to Microsoft Network Monitor

Installing….



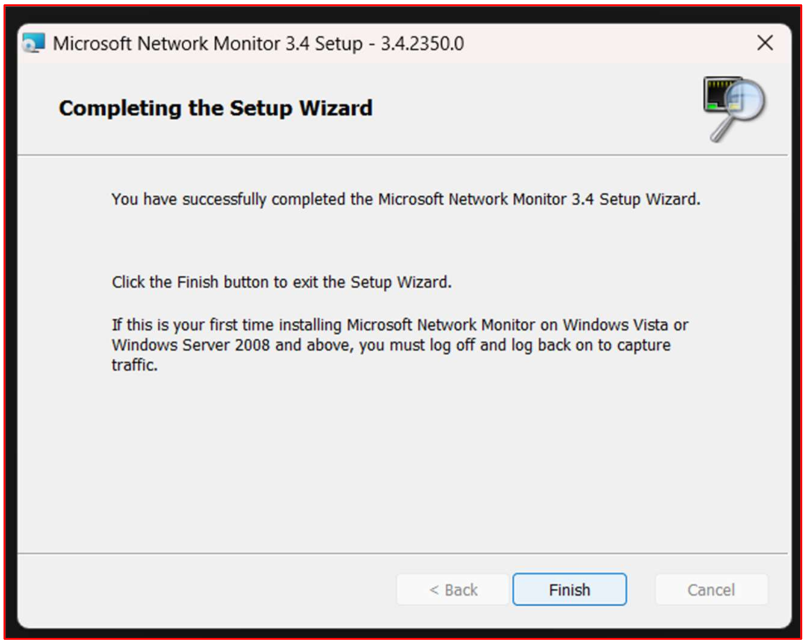
Microsoft Network Monitor 3.4 Setup - 3.4.2350.0

Installing Microsoft Network Monitor 3.4

Please wait while the Setup Wizard installs Microsoft Network Monitor 3.4. This may take several minutes.

Status: Binding Netmon Driver

Tap on Finish



Microsoft Network Monitor 3.4 Setup - 3.4.2350.0

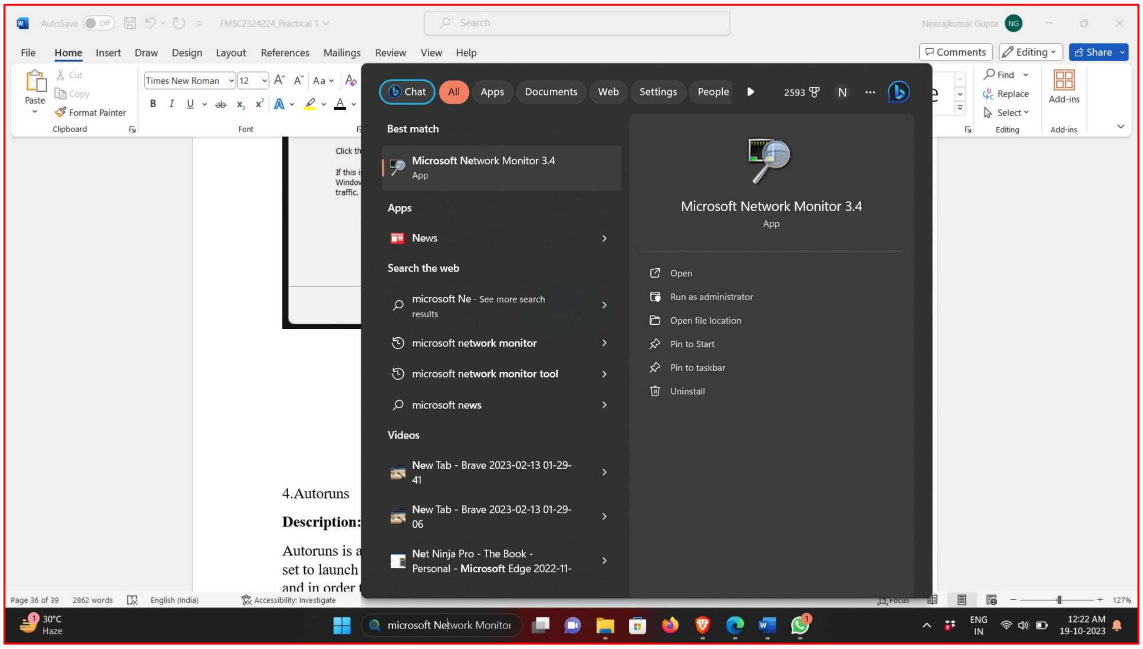
Completing the Setup Wizard

You have successfully completed the Microsoft Network Monitor 3.4 Setup Wizard.

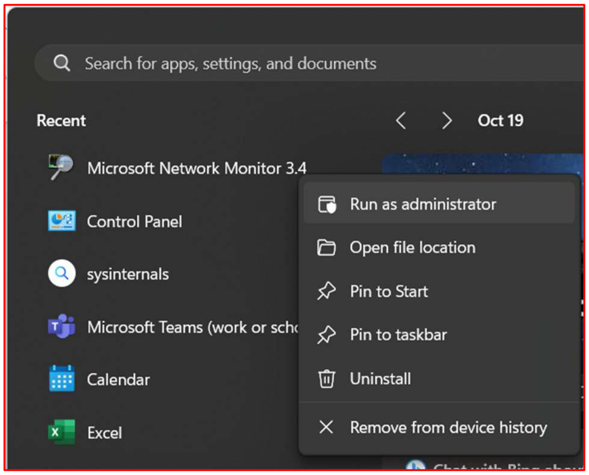
Click the Finish button to exit the Setup Wizard.

If this is your first time installing Microsoft Network Monitor on Windows Vista or Windows Server 2008 and above, you must log off and log back on to capture traffic.

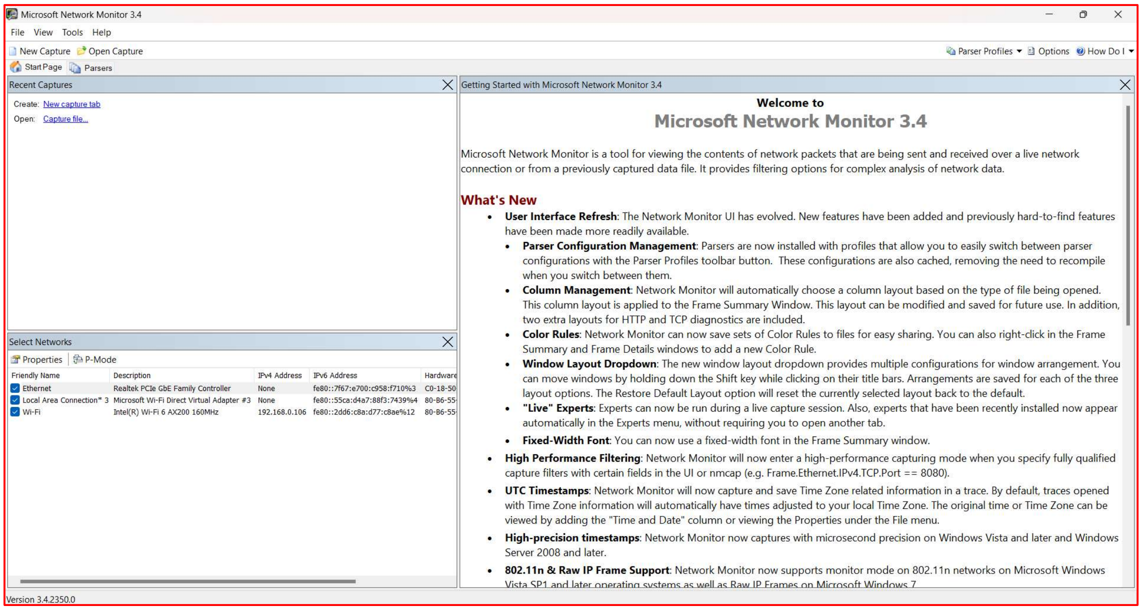
Now search for Microsoft Network Monitor in windows and Run it as Administrator & open it.



Chat
All
Apps
Documents
Web
Settings
People
2593
Best match
Microsoft Network Monitor 3.4
App
Apps
News
Search the web
microsoft Ne - See more search results
microsoft network monitor
microsoft network monitor tool
microsoft news
Videos
New Tab - Brave 2023-02-13 01-29-41
New Tab - Brave 2023-02-13 01-29-06
Net Ninja Pro - The Book - Personal - Microsoft Edge 2022-11-
Microsoft Network Monitor 3.4
App
Open
Run as administrator
Open file location
Pin to Start
Pin to taskbar
Uninstall
microsoft Network Monitor
4.Autoruns
Description:
30°C
Haze
ENG
IN
12:22 AM
19-10-2023



Default start page



Create: New capture tab

Open: Capture file...

Select Networks

Friendly Name	Description	IPv4 Address	IPv6 Address	Hardware
☑ Ethernet	Realtek PCIe GbE Family Controller	None	fe80::7f67:e700:c958:f710%3	C0-18-50
☑ Local Area Connection* 3	Microsoft Wi-Fi Direct Virtual Adapter #3	None	fe80::55ca:d4a7:88f3:7439%4	80-B6-55
☑ Wi-Fi	Intel(R) Wi-Fi 6 AX200 160MHz	192.168.0.106	fe80::2dd6:c8a:d77:c8ae%12	80-B6-55

Welcome to

Microsoft Network Monitor 3.4

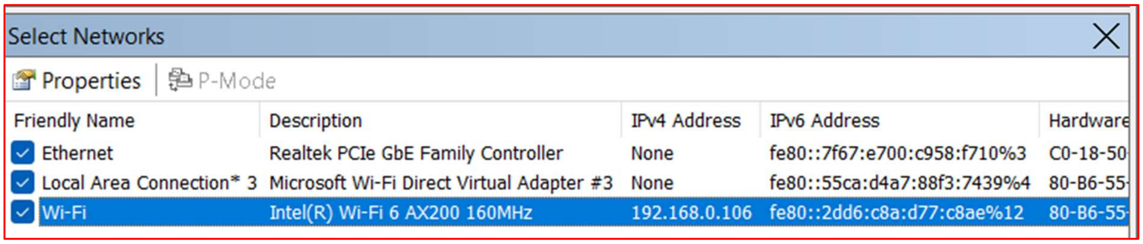
Microsoft Network Monitor is a tool for viewing the contents of network packets that are being sent and received over a live network connection or from a previously captured data file. It provides filtering options for complex analysis of network data.

What's New

- **User Interface Refresh**: The Network Monitor UI has evolved. New features have been added and previously hard-to-find features have been made more readily available.
    - **Parser Configuration Management**: Parsers are now installed with profiles that allow you to easily switch between parser configurations with the Parser Profiles toolbar button. These configurations are also cached, removing the need to recompile when you switch between them.
    - **Column Management**: Network Monitor will automatically choose a column layout based on the type of file being opened. This column layout is applied to the Frame Summary Window. This layout can be modified and saved for future use. In addition, two extra layouts for HTTP and TCP diagnostics are included.
    - **Color Rules**: Network Monitor can now save sets of Color Rules to files for easy sharing. You can also right-click in the Frame Summary and Frame Details windows to add a new Color Rule.
    - **Window Layout Dropdown**: The new window layout dropdown provides multiple configurations for window arrangement. You can move windows by holding down the Shift key while clicking on their title bars. Arrangements are saved for each of the three layout options. The Restore Default Layout option will reset the currently selected layout back to the default.
    - **"Live" Experts**: Experts can now be run during a live capture session. Also, experts that have been recently installed now appear automatically in the Experts menu, without requiring you to open another tab.
    - **Fixed-Width Font**: You can now use a fixed-width font in the Frame Summary window.
- **High Performance Filtering**: Network Monitor will now enter a high-performance capturing mode when you specify fully qualified capture filters with certain fields in the UI or nmcap (e.g. Frame.Ethernet.IPv4.TCP.Port == 8080).
- **UTC Timestamps**: Network Monitor will now capture and save Time Zone related information in a trace. By default, traces opened with Time Zone information will automatically have times adjusted to your local Time Zone. The original time or Time Zone can be viewed by adding the "Time and Date" column or viewing the Properties under the File menu.
- **High-precision timestamps**: Network Monitor now captures with microsecond precision on Windows Vista and later and Windows Server 2008 and later.
- **802.11n & Raw IP Frame Support**: Network Monitor now supports monitor mode on 802.11n networks on Microsoft Windows Vista SP1 and later operating systems as well as Raw IP Frames on Microsoft Windows 7

Version 3.4.2350.0

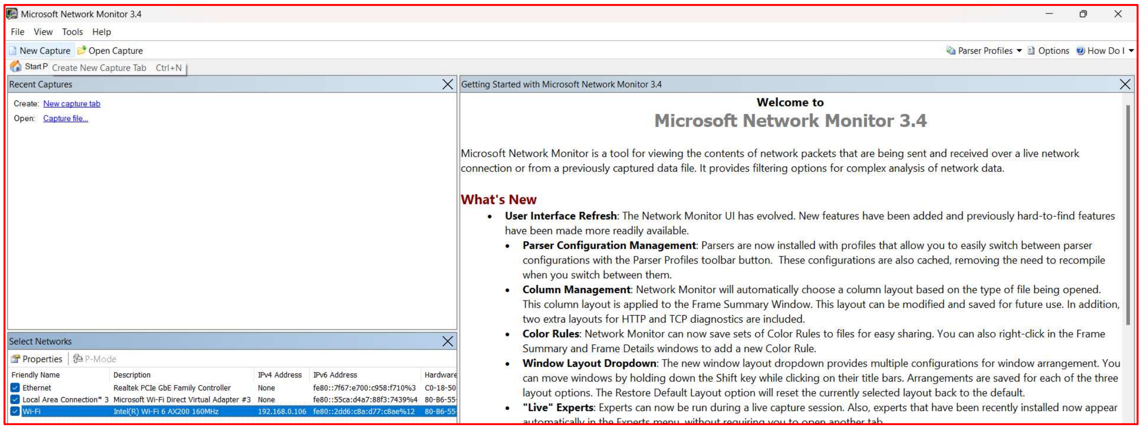
Select your device connected network or your preferred network



Select Networks

Friendly Name	Description	IPv4 Address	IPv6 Address	Hardware
☑ Ethernet	Realtek PCIe GbE Family Controller	None	fe80::7f67:e700:c958:f710%3	C0-18-50
☑ Local Area Connection* 3	Microsoft Wi-Fi Direct Virtual Adapter #3	None	fe80::55ca:d4a7:88f3:7439%4	80-B6-55
☑ Wi-Fi	Intel(R) Wi-Fi 6 AX200 160MHz	192.168.0.106	fe80::2dd6:c8a:d77:c8ae%12	80-B6-55

After Selecting the Network, click on New Capture



Friendly Name	Description	IPv4 Address	IPv6 Address	Hardware
☑ Ethernet	Realtek PCIe GbE Family Controller	None	fe80::7f67:e700:c958:f710%3	C0-18-50
☑ Local Area Connection* 3	Microsoft Wi-Fi Direct Virtual Adapter #3	None	fe80::55ca:d4a7:88f3:7439%4	80-B6-55
☑ Wi-Fi	Intel(R) Wi-Fi 6 AX200 160MHz	192.168.0.106	fe80::2dd6:c8a:d77:c8ae%12	80-B6-55

Welcome to

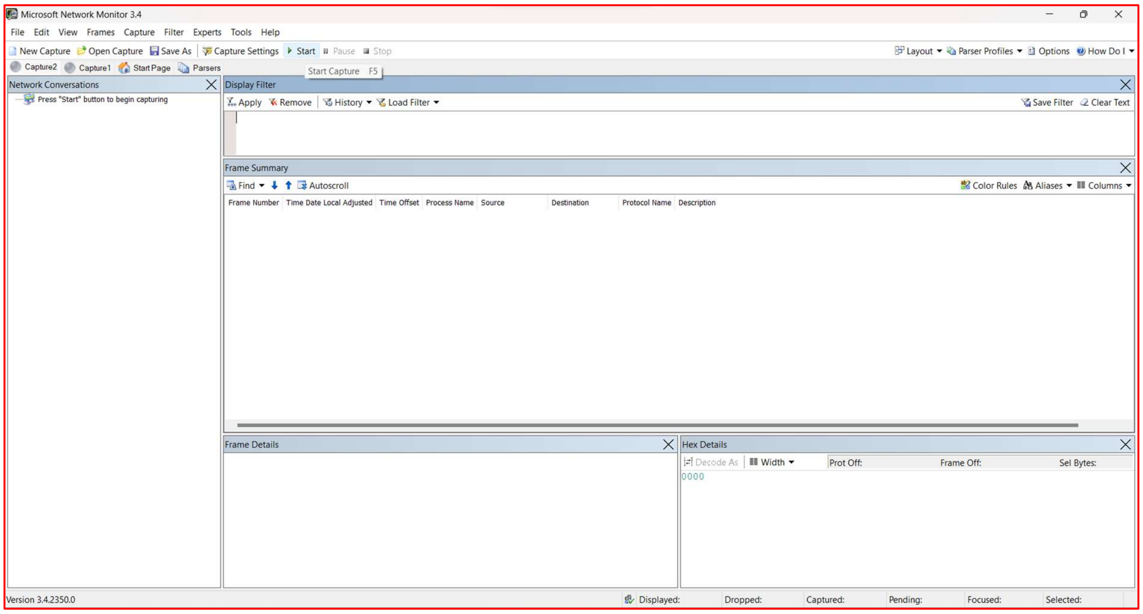
Microsoft Network Monitor 3.4

Microsoft Network Monitor is a tool for viewing the contents of network packets that are being sent and received over a live network connection or from a previously captured data file. It provides filtering options for complex analysis of network data.

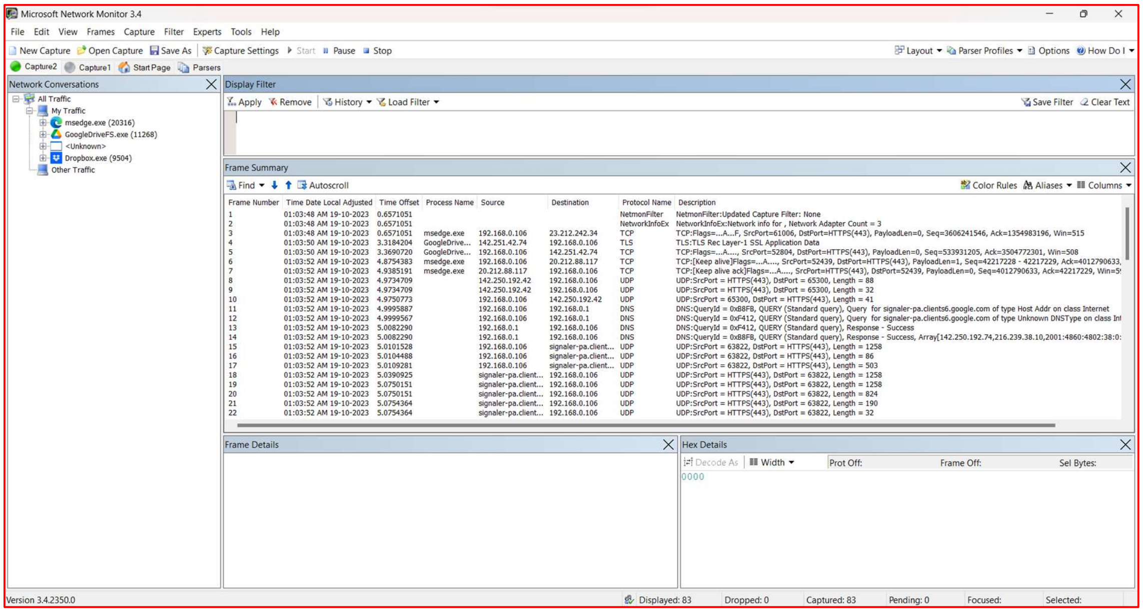
What's New

- **User Interface Refresh**: The Network Monitor UI has evolved. New features have been added and previously hard-to-find features have been made more readily available.
  - **Parser Configuration Management**: Parsers are now installed with profiles that allow you to easily switch between parser configurations with the Parser Profiles toolbar button. These configurations are also cached, removing the need to recompile when you switch between them.
  - **Column Management**: Network Monitor will automatically choose a column layout based on the type of file being opened. This column layout is applied to the Frame Summary Window. This layout can be modified and saved for future use. In addition, two extra layouts for HTTP and TCP diagnostics are included.
  - **Color Rules**: Network Monitor can now save sets of Color Rules to files for easy sharing. You can also right-click in the Frame Summary and Frame Details windows to add a new Color Rule.
  - **Window Layout Dropdown**: The new window layout dropdown provides multiple configurations for window arrangement. You can move windows by holding down the Shift key while clicking on their title bars. Arrangements are saved for each of the three layout options. The Restore Default Layout option will reset the currently selected layout back to the default.
  - **"Live" Experts**: Experts can now be run during a live capture session. Also, experts that have been recently installed now appear automatically in the Experts menu, without requiring you to open another tab.

Now click on Start



Captured networks all that are running and present


Microsoft Network Monitor 3.4
File Edit View Frames Capture Filter Experts Tools Help
New Capture Open Capture Save As Capture Settings Start Pause Stop
Layout Parser Profiles Options How Do I
Capture2 Capture1 Start Page Parsers
Network Conversations
Display Filter
Apply Remove History Load Filter
Save Filter Clear Text
Frame Summary
Find Autoscroll
Color Rules Aliases Columns
Frame Details
Hex Details
Decode As Width

- All Traffic
  - My Traffic
    - msedge.exe (20316)
    - GoogleDriveFS.exe (11268)
    - <Unknown>
    - Dropbox.exe (9504)
  - Other Traffic

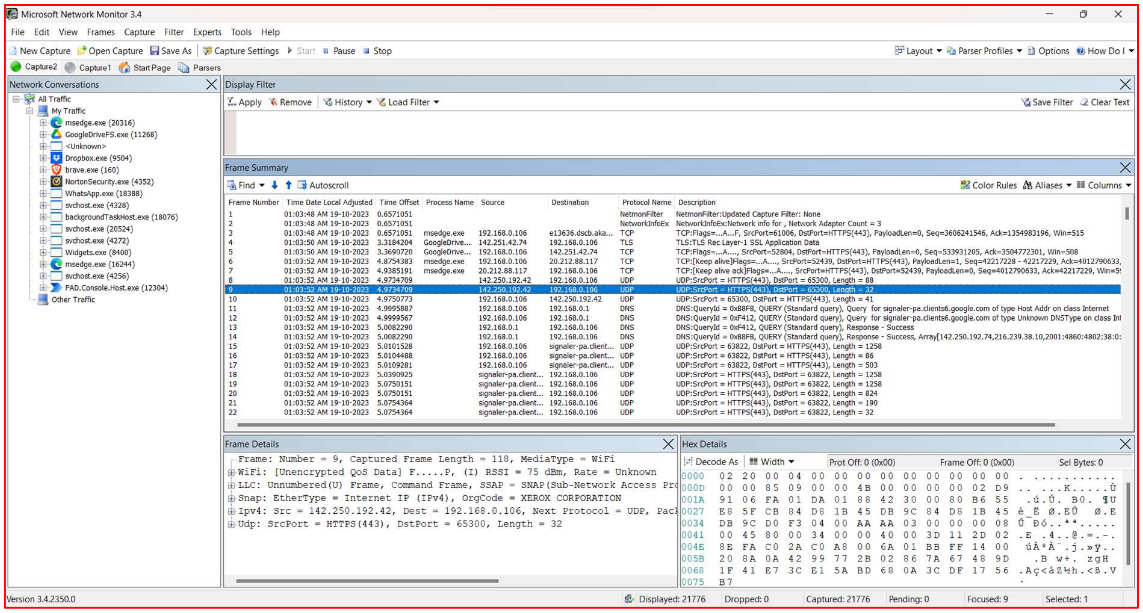
Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
1	01:03:48 AM 19-10-2023	0.6571051				NetmonFilter	NetmonFilter:Updated Capture Filter: None
2	01:03:48 AM 19-10-2023	0.6571051				NetworkInfoEx	NetworkInfoEx:Network info for , Network Adapter Count = 3
3	01:03:48 AM 19-10-2023	0.6571051	msedge.exe	192.168.0.106	23.212.242.34	TCP	TCP:Flags=...A...F, SrcPort=61006, DstPort=HTTPS(443), PayloadLen=0, Seq=3606241546, Ack=1354983196, Win=515
4	01:03:50 AM 19-10-2023	3.3184204	GoogleDrive...	142.251.42.74	192.168.0.106	TLS	TLS:TLS Rec Layer-1 SSL Application Data
5	01:03:50 AM 19-10-2023	3.3690720	GoogleDrive...	192.168.0.106	142.251.42.74	TCP	TCP:Flags=...A...., SrcPort=52804, DstPort=HTTPS(443), PayloadLen=0, Seq=533931205, Ack=3504772301, Win=508
6	01:03:52 AM 19-10-2023	4.8754383	msedge.exe	192.168.0.106	20.212.88.117	TCP	TCP:[Keep alive]Flags=...A...., SrcPort=52439, DstPort=HTTPS(443), PayloadLen=1, Seq=42217228 - 42217229, Ack=4012790633,
7	01:03:52 AM 19-10-2023	4.9385191	msedge.exe	20.212.88.117	192.168.0.106	TCP	TCP:[Keep alive ack]Flags=...A...., SrcPort=HTTPS(443), DstPort=52439, PayloadLen=0, Seq=4012790633, Ack=42217229, Win=5
8	01:03:52 AM 19-10-2023	4.9734709		142.250.192.42	192.168.0.106	UDP	UDP:SrcPort = HTTPS(443), DstPort = 65300, Length = 88
9	01:03:52 AM 19-10-2023	4.9734709		142.250.192.42	192.168.0.106	UDP	UDP:SrcPort = HTTPS(443), DstPort = 65300, Length = 32
10	01:03:52 AM 19-10-2023	4.9750773		192.168.0.106	142.250.192.42	UDP	UDP:SrcPort = 65300, DstPort = HTTPS(443), Length = 41
11	01:03:52 AM 19-10-2023	4.9995887		192.168.0.106	192.168.0.1	DNS	DNS:QueryId = 0xB8FB, QUERY (Standard query), Query for signaler-pa.clients6.google.com of type Host Addr on class Internet
12	01:03:52 AM 19-10-2023	4.9999567		192.168.0.106	192.168.0.1	DNS	DNS:QueryId = 0xF412, QUERY (Standard query), Query for signaler-pa.clients6.google.com of type Unknown DNSType on class Int
13	01:03:52 AM 19-10-2023	5.0082290		192.168.0.1	192.168.0.106	DNS	DNS:QueryId = 0xF412, QUERY (Standard query), Response - Success
14	01:03:52 AM 19-10-2023	5.0082290		192.168.0.1	192.168.0.106	DNS	DNS:QueryId = 0xB8FB, QUERY (Standard query), Response - Success, Array[142.250.192.74,216.239.38.10,2001:4860:4802:38:0:
15	01:03:52 AM 19-10-2023	5.0101528		192.168.0.106	signaler-pa.client...	UDP	UDP:SrcPort = 63822, DstPort = HTTPS(443), Length = 1258
16	01:03:52 AM 19-10-2023	5.0104488		192.168.0.106	signaler-pa.client...	UDP	UDP:SrcPort = 63822, DstPort = HTTPS(443), Length = 86
17	01:03:52 AM 19-10-2023	5.0109281		192.168.0.106	signaler-pa.client...	UDP	UDP:SrcPort = 63822, DstPort = HTTPS(443), Length = 503
18	01:03:52 AM 19-10-2023	5.0390925		signaler-pa.client...	192.168.0.106	UDP	UDP:SrcPort = HTTPS(443), DstPort = 63822, Length = 1258
19	01:03:52 AM 19-10-2023	5.0750151		signaler-pa.client...	192.168.0.106	UDP	UDP:SrcPort = HTTPS(443), DstPort = 63822, Length = 1258
20	01:03:52 AM 19-10-2023	5.0750151		signaler-pa.client...	192.168.0.106	UDP	UDP:SrcPort = HTTPS(443), DstPort = 63822, Length = 824
21	01:03:52 AM 19-10-2023	5.0754364		signaler-pa.client...	192.168.0.106	UDP	UDP:SrcPort = HTTPS(443), DstPort = 63822, Length = 190
22	01:03:52 AM 19-10-2023	5.0754364		signaler-pa.client...	192.168.0.106	UDP	UDP:SrcPort = HTTPS(443), DstPort = 63822, Length = 32

Prot Off: Frame Off: Sel Bytes:

0000

Version 3.4.2350.0 Displayed: 83 Dropped: 0 Captured: 83 Pending: 0 Focused: Selected:

If you click on any one networks you will find all the frame details and hex details


Microsoft Network Monitor 3.4
File Edit View Frames Capture Filter Experts Tools Help
New Capture Open Capture Save As Capture Settings Start Pause Stop
Layout Parser Profiles Options How Do I
Capture2 Capture1 Start Page Parsers
Network Conversations
Display Filter
Apply Remove History Load Filter
Save Filter Clear Text
Frame Summary
Find Autoscroll
Color Rules Aliases Columns
Frame Details
Hex Details
Decode As Width

- All Traffic
  - My Traffic
    - msedge.exe (20316)
    - GoogleDriveFS.exe (11268)
    - <Unknown>
    - Dropbox.exe (9504)
    - brave.exe (160)
    - NortonSecurity.exe (4352)
    - WhatsApp.exe (18388)
    - svchost.exe (4328)
    - backgroundTaskHost.exe (18076)
    - svchost.exe (20524)
    - svchost.exe (4272)
    - Widgets.exe (8400)
    - msedge.exe (16244)
    - svchost.exe (4256)
    - PAD.Console.Host.exe (12304)
  - Other Traffic

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
1	01:03:48 AM 19-10-2023	0.6571051				NetmonFilter	NetmonFilter:Updated Capture Filter: None
2	01:03:48 AM 19-10-2023	0.6571051				NetworkInfoEx	NetworkInfoEx:Network info for , Network Adapter Count = 3
3	01:03:48 AM 19-10-2023	0.6571051	msedge.exe	192.168.0.106	e13636.dscb.aka...	TCP	TCP:Flags=...A...F, SrcPort=61006, DstPort=HTTPS(443), PayloadLen=0, Seq=3606241546, Ack=1354983196, Win=515
4	01:03:50 AM 19-10-2023	3.3184204	GoogleDrive...	142.251.42.74	192.168.0.106	TLS	TLS:TLS Rec Layer-1 SSL Application Data
5	01:03:50 AM 19-10-2023	3.3690720	GoogleDrive...	192.168.0.106	142.251.42.74	TCP	TCP:Flags=...A...., SrcPort=52804, DstPort=HTTPS(443), PayloadLen=0, Seq=533931205, Ack=3504772301, Win=508
6	01:03:52 AM 19-10-2023	4.8754383	msedge.exe	192.168.0.106	20.212.88.117	TCP	TCP:[Keep alive]Flags=...A...., SrcPort=52439, DstPort=HTTPS(443), PayloadLen=1, Seq=42217228 - 42217229, Ack=4012790633,
7	01:03:52 AM 19-10-2023	4.9385191	msedge.exe	20.212.88.117	192.168.0.106	TCP	TCP:[Keep alive ack]Flags=...A...., SrcPort=HTTPS(443), DstPort=52439, PayloadLen=0, Seq=4012790633, Ack=42217229, Win=5
8	01:03:52 AM 19-10-2023	4.9734709		142.250.192.42	192.168.0.106	UDP	UDP:SrcPort = HTTPS(443), DstPort = 65300, Length = 88
9	01:03:52 AM 19-10-2023	4.9734709		142.250.192.42	192.168.0.106	UDP	UDP:SrcPort = HTTPS(443), DstPort = 65300, Length = 32
10	01:03:52 AM 19-10-2023	4.9750773		192.168.0.106	142.250.192.42	UDP	UDP:SrcPort = 65300, DstPort = HTTPS(443), Length = 41
11	01:03:52 AM 19-10-2023	4.9995887		192.168.0.106	192.168.0.1	DNS	DNS:QueryId = 0xB8FB, QUERY (Standard query), Query for signaler-pa.clients6.google.com of type Host Addr on class Internet
12	01:03:52 AM 19-10-2023	4.9999567		192.168.0.106	192.168.0.1	DNS	DNS:QueryId = 0xF412, QUERY (Standard query), Query for signaler-pa.clients6.google.com of type Unknown DNSType on class Int
13	01:03:52 AM 19-10-2023	5.0082290		192.168.0.1	192.168.0.106	DNS	DNS:QueryId = 0xF412, QUERY (Standard query), Response - Success
14	01:03:52 AM 19-10-2023	5.0082290		192.168.0.1	192.168.0.106	DNS	DNS:QueryId = 0xB8FB, QUERY (Standard query), Response - Success, Array[142.250.192.74,216.239.38.10,2001:4860:4802:38:0:
15	01:03:52 AM 19-10-2023	5.0101528		192.168.0.106	signaler-pa.client...	UDP	UDP:SrcPort = 63822, DstPort = HTTPS(443), Length = 1258
16	01:03:52 AM 19-10-2023	5.0104488		192.168.0.106	signaler-pa.client...	UDP	UDP:SrcPort = 63822, DstPort = HTTPS(443), Length = 86
17	01:03:52 AM 19-10-2023	5.0109281		192.168.0.106	signaler-pa.client...	UDP	UDP:SrcPort = 63822, DstPort = HTTPS(443), Length = 503
18	01:03:52 AM 19-10-2023	5.0390925		signaler-pa.client...	192.168.0.106	UDP	UDP:SrcPort = HTTPS(443), DstPort = 63822, Length = 1258
19	01:03:52 AM 19-10-2023	5.0750151		signaler-pa.client...	192.168.0.106	UDP	UDP:SrcPort = HTTPS(443), DstPort = 63822, Length = 1258
20	01:03:52 AM 19-10-2023	5.0750151		signaler-pa.client...	192.168.0.106	UDP	UDP:SrcPort = HTTPS(443), DstPort = 63822, Length = 824
21	01:03:52 AM 19-10-2023	5.0754364		signaler-pa.client...	192.168.0.106	UDP	UDP:SrcPort = HTTPS(443), DstPort = 63822, Length = 190
22	01:03:52 AM 19-10-2023	5.0754364		signaler-pa.client...	192.168.0.106	UDP	UDP:SrcPort = HTTPS(443), DstPort = 63822, Length = 32

```
Frame: Number = 9, Captured Frame Length = 118, MediaType = WiFi
⊞WiFi: [Unencrypted QoS Data] F.....P, (I) RSSI = 75 dBm, Rate = Unknown
⊞LLC: Unnumbered(U) Frame, Command Frame, SSAP = SNAP(Sub-Network Access Pro
⊞Snap: EtherType = Internet IP (IPv4), OrgCode = XEROX CORPORATION
⊞Ipv4: Src = 142.250.192.42, Dest = 192.168.0.106, Next Protocol = UDP, Pack
⊞Udp: SrcPort = HTTPS(443), DstPort = 65300, Length = 32
```

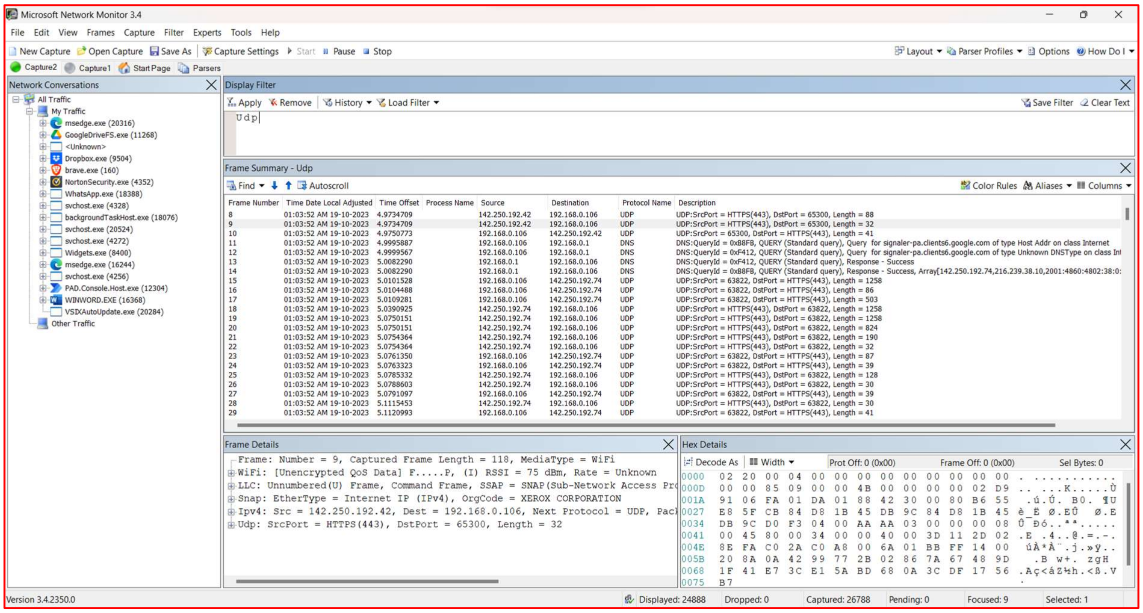
Prot Off: 0 (0x00) Frame Off: 0 (0x00) Sel Bytes: 0

```
0000  02 20 00 04 00 00 00 00 00 00 00 00 00  . ...........
000D  00 00 85 09 00 00 4B 00 00 00 00 02 D9  .. ...K.....Ù
001A  91 06 FA 01 DA 01 88 42 30 00 80 B6 55   .ú.Ú. B0. ¶U
0027  E8 5F CB 84 D8 1B 45 DB 9C 84 D8 1B 45  è_Ë Ø.EÛ  Ø.E
0034  DB 9C D0 F3 04 00 AA AA 03 00 00 00 08  Û Ðó..ªª.....
0041  00 45 80 00 34 00 00 40 00 3D 11 2D 02  .E .4..@.=.-.
004E  8E FA C0 2A C0 A8 00 6A 01 BB FF 14 00   úÀ*À¨.j.»ÿ..
005B  20 8A 0A 42 99 77 2B 02 86 7A 67 48 9D    .B w+. zgH
0068  1F 41 E7 3C E1 5A BD 68 0A 3C DF 17 56  .Aç<áZ½h.<ß.V
0075  B7                                      .
```

Version 3.4.2350.0 Displayed: 21776 Dropped: 0 Captured: 21776 Pending: 0 Focused: 9 Selected: 1

To use filters inside display filter search for udp and click on apply, it will show all the udp networks

(follow the same steps to search for TCP, IPv4, IPv6, IGMP, HTTP, SSDP, DNS, ARP, etc)


Microsoft Network Monitor 3.4
File Edit View Frames Capture Filter Experts Tools Help
New Capture Open Capture Save As Capture Settings Start Pause Stop
Layout Parser Profiles Options How Do I
Capture2 Capture1 Start Page Parsers
Network Conversations
All Traffic
My Traffic
msedge.exe (20316)
GoogleDriveFS.exe (11268)
<Unknown>
Dropbox.exe (9504)
brave.exe (160)
NortonSecurity.exe (4352)
WhatsApp.exe (18388)
svchost.exe (4328)
backgroundTaskHost.exe (18076)
svchost.exe (20524)
svchost.exe (4272)
Widgets.exe (8400)
msedge.exe (16244)
svchost.exe (4256)
PAD.Console.Host.exe (12304)
WINWORD.EXE (16368)
VSIXAutoUpdate.exe (20284)
Other Traffic
Display Filter
Apply Remove History Load Filter
Save Filter Clear Text
Frame Summary - Udp
Find Autoscroll
Color Rules Aliases Columns
Frame Details
Hex Details
Decode As Width

Udp

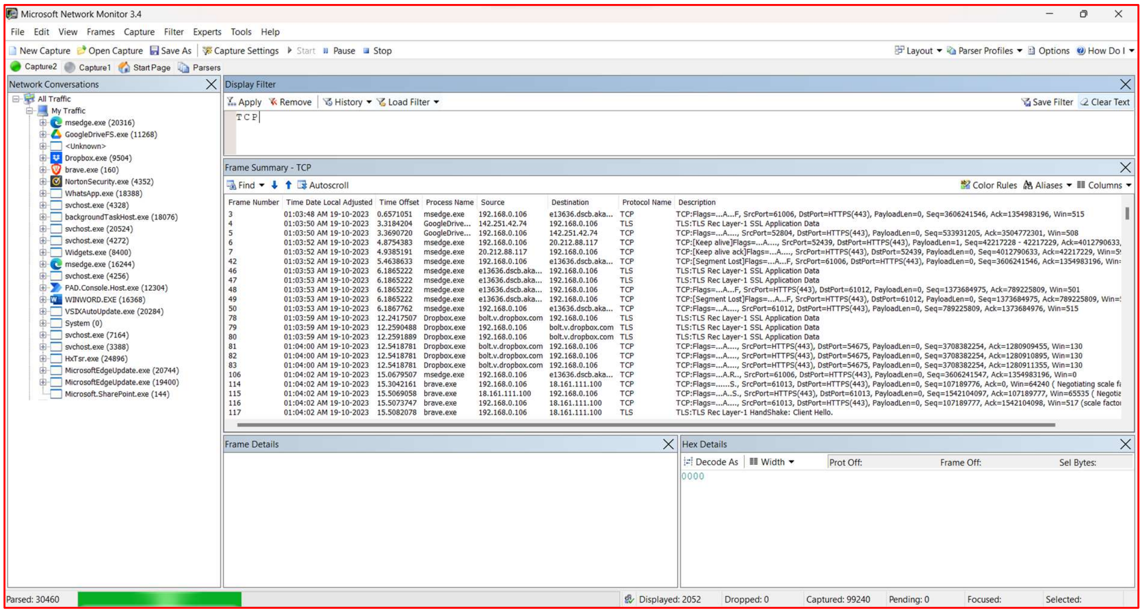
Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
8	01:03:52 AM 19-10-2023	4.9734709		142.250.192.42	192.168.0.106	UDP	UDP:SrcPort = HTTPS(443), DstPort = 65300, Length = 88
9	01:03:52 AM 19-10-2023	4.9734709		142.250.192.42	192.168.0.106	UDP	UDP:SrcPort = HTTPS(443), DstPort = 65300, Length = 32
10	01:03:52 AM 19-10-2023	4.9750773		192.168.0.106	142.250.192.42	UDP	UDP:SrcPort = 65300, DstPort = HTTPS(443), Length = 41
11	01:03:52 AM 19-10-2023	4.9995887		192.168.0.106	192.168.0.1	DNS	DNS:QueryId = 0x88FB, QUERY (Standard query), Query for signaler-pa.clients6.google.com of type Host Addr on class Internet
12	01:03:52 AM 19-10-2023	4.9999567		192.168.0.106	192.168.0.1	DNS	DNS:QueryId = 0xF412, QUERY (Standard query), Query for signaler-pa.clients6.google.com of type Unknown DNSType on class Int
13	01:03:52 AM 19-10-2023	5.0082290		192.168.0.1	192.168.0.106	DNS	DNS:QueryId = 0xF412, QUERY (Standard query), Response - Success
14	01:03:52 AM 19-10-2023	5.0082290		192.168.0.1	192.168.0.106	DNS	DNS:QueryId = 0x88FB, QUERY (Standard query), Response - Success, Array[142.250.192.74,216.239.38.10,2001:4860:4802:38:0:
15	01:03:52 AM 19-10-2023	5.0101528		192.168.0.106	142.250.192.74	UDP	UDP:SrcPort = 63822, DstPort = HTTPS(443), Length = 1258
16	01:03:52 AM 19-10-2023	5.0104488		192.168.0.106	142.250.192.74	UDP	UDP:SrcPort = 63822, DstPort = HTTPS(443), Length = 86
17	01:03:52 AM 19-10-2023	5.0109281		192.168.0.106	142.250.192.74	UDP	UDP:SrcPort = 63822, DstPort = HTTPS(443), Length = 503
18	01:03:52 AM 19-10-2023	5.0390925		142.250.192.74	192.168.0.106	UDP	UDP:SrcPort = HTTPS(443), DstPort = 63822, Length = 1258
19	01:03:52 AM 19-10-2023	5.0750151		142.250.192.74	192.168.0.106	UDP	UDP:SrcPort = HTTPS(443), DstPort = 63822, Length = 1258
20	01:03:52 AM 19-10-2023	5.0750151		142.250.192.74	192.168.0.106	UDP	UDP:SrcPort = HTTPS(443), DstPort = 63822, Length = 824
21	01:03:52 AM 19-10-2023	5.0754364		142.250.192.74	192.168.0.106	UDP	UDP:SrcPort = HTTPS(443), DstPort = 63822, Length = 190
22	01:03:52 AM 19-10-2023	5.0754364		142.250.192.74	192.168.0.106	UDP	UDP:SrcPort = HTTPS(443), DstPort = 63822, Length = 32
23	01:03:52 AM 19-10-2023	5.0761350		192.168.0.106	142.250.192.74	UDP	UDP:SrcPort = 63822, DstPort = HTTPS(443), Length = 87
24	01:03:52 AM 19-10-2023	5.0763323		192.168.0.106	142.250.192.74	UDP	UDP:SrcPort = 63822, DstPort = HTTPS(443), Length = 39
25	01:03:52 AM 19-10-2023	5.0785332		142.250.192.74	192.168.0.106	UDP	UDP:SrcPort = HTTPS(443), DstPort = 63822, Length = 128
26	01:03:52 AM 19-10-2023	5.0788603		142.250.192.74	192.168.0.106	UDP	UDP:SrcPort = HTTPS(443), DstPort = 63822, Length = 30
27	01:03:52 AM 19-10-2023	5.0791097		192.168.0.106	142.250.192.74	UDP	UDP:SrcPort = 63822, DstPort = HTTPS(443), Length = 39
28	01:03:52 AM 19-10-2023	5.1115453		142.250.192.74	192.168.0.106	UDP	UDP:SrcPort = HTTPS(443), DstPort = 63822, Length = 30
29	01:03:52 AM 19-10-2023	5.1120993		192.168.0.106	142.250.192.74	UDP	UDP:SrcPort = 63822, DstPort = HTTPS(443), Length = 41

```
Frame: Number = 9, Captured Frame Length = 118, MediaType = WiFi
WiFi: [Unencrypted QoS Data] F.....P, (I) RSSI = 75 dBm, Rate = Unknown
LLC: Unnumbered(U) Frame, Command Frame, SSAP = SNAP(Sub-Network Access Prc
Snap: EtherType = Internet IP (IPv4), OrgCode = XEROX CORPORATION
Ipv4: Src = 142.250.192.42, Dest = 192.168.0.106, Next Protocol = UDP, Pack
Udp: SrcPort = HTTPS(443), DstPort = 65300, Length = 32
```

Prot Off: 0 (0x00) Frame Off: 0 (0x00) Sel Bytes: 0

```
0000  02 20 00 04 00 00 00 00 00 00 00 00 00  . ...........
000D  00 00 85 09 00 00 4B 00 00 00 00 02 D9  ..  ...K.....Ù
001A  91 06 FA 01 DA 01 88 42 30 00 80 B6 55   .ú.Ú. B0. ¶U
0027  E8 5F CB 84 D8 1B 45 DB 9C 84 D8 1B 45  è_Ë Ø.EÛ  Ø.E
0034  DB 9C D0 F3 04 00 AA AA 03 00 00 00 08  Û Ðó..ªª.....
0041  00 45 80 00 34 00 00 40 00 3D 11 2D 02  .E .4..@.=.-.
004E  8E FA C0 2A C0 A8 00 6A 01 BB FF 14 00   úÀ*À¨.j.»ÿ..
005B  20 8A 0A 42 99 77 2B 02 86 7A 67 48 9D    .B w+. zgH
0068  1F 41 E7 3C E1 5A BD 68 0A 3C DF 17 56  .Aç<áZ½h.<ß.V
0075  B7                                      .
```

Version 3.4.2350.0 Displayed: 24888 Dropped: 0 Captured: 26788 Pending: 0 Focused: 9 Selected: 1


Microsoft Network Monitor 3.4
File Edit View Frames Capture Filter Experts Tools Help
New Capture Open Capture Save As Capture Settings Start Pause Stop
Layout Parser Profiles Options How Do I
Capture2 Capture1 Start Page Parsers
Network Conversations
All Traffic
My Traffic
msedge.exe (20316)
GoogleDriveFS.exe (11268)
<Unknown>
Dropbox.exe (9504)
brave.exe (160)
NortonSecurity.exe (4352)
WhatsApp.exe (18388)
svchost.exe (4328)
backgroundTaskHost.exe (18076)
svchost.exe (20524)
svchost.exe (4272)
Widgets.exe (8400)
msedge.exe (16244)
svchost.exe (4256)
PAD.Console.Host.exe (12304)
WINWORD.EXE (16368)
VSIXAutoUpdate.exe (20284)
System (0)
svchost.exe (7164)
svchost.exe (3388)
HxTsr.exe (24896)
MicrosoftEdgeUpdate.exe (20744)
MicrosoftEdgeUpdate.exe (19400)
Microsoft.SharePoint.exe (144)
Display Filter
Apply Remove History Load Filter
Save Filter Clear Text
Frame Summary - TCP
Find Autoscroll
Color Rules Aliases Columns
Frame Details
Hex Details
Decode As Width

TCP

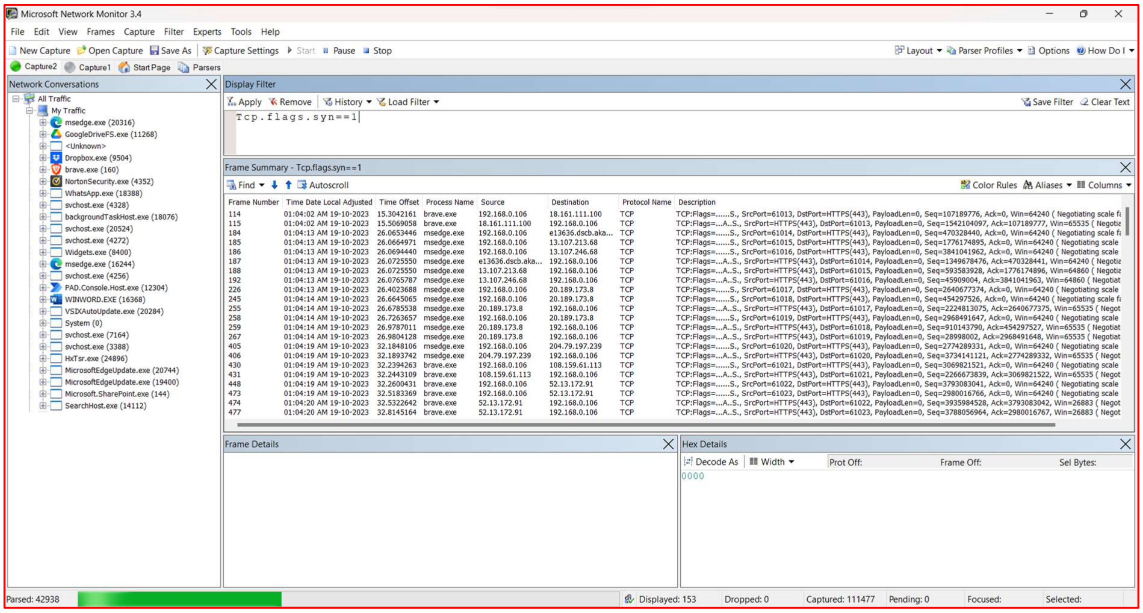
Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
3	01:03:48 AM 19-10-2023	0.6571051	msedge.exe	192.168.0.106	e13636.dscb.aka...	TCP	TCP:Flags=...A...F, SrcPort=61006, DstPort=HTTPS(443), PayloadLen=0, Seq=3606241546, Ack=1354983196, Win=515
4	01:03:50 AM 19-10-2023	3.3184204	GoogleDrive...	142.251.42.74	192.168.0.106	TLS	TLS:TLS Rec Layer-1 SSL Application Data
5	01:03:50 AM 19-10-2023	3.3690720	GoogleDrive...	192.168.0.106	142.251.42.74	TCP	TCP:Flags=...A...., SrcPort=52804, DstPort=HTTPS(443), PayloadLen=0, Seq=533931205, Ack=3504772301, Win=508
6	01:03:52 AM 19-10-2023	4.8754383	msedge.exe	192.168.0.106	20.212.88.117	TCP	TCP:[Keep alive]Flags=...A...., SrcPort=52439, DstPort=HTTPS(443), PayloadLen=1, Seq=42217228 - 42217229, Ack=4012790633,
7	01:03:52 AM 19-10-2023	4.9385191	msedge.exe	20.212.88.117	192.168.0.106	TCP	TCP:[Keep alive ack]Flags=...A...., SrcPort=HTTPS(443), DstPort=52439, PayloadLen=0, Seq=4012790633, Ack=42217229, Win=5
42	01:03:52 AM 19-10-2023	5.4638633	msedge.exe	192.168.0.106	e13636.dscb.aka...	TCP	TCP:[Segment Lost]Flags=...A...F, SrcPort=61006, DstPort=HTTPS(443), PayloadLen=0, Seq=3606241546, Ack=1354983196, Win=
46	01:03:53 AM 19-10-2023	6.1865222	msedge.exe	e13636.dscb.aka...	192.168.0.106	TLS	TLS:TLS Rec Layer-1 SSL Application Data
47	01:03:53 AM 19-10-2023	6.1865222	msedge.exe	e13636.dscb.aka...	192.168.0.106	TLS	TLS:TLS Rec Layer-1 SSL Application Data
48	01:03:53 AM 19-10-2023	6.1865222	msedge.exe	e13636.dscb.aka...	192.168.0.106	TCP	TCP:Flags=...A...F, SrcPort=HTTPS(443), DstPort=61012, PayloadLen=0, Seq=1373684975, Ack=789225809, Win=501
49	01:03:53 AM 19-10-2023	6.1865222	msedge.exe	e13636.dscb.aka...	192.168.0.106	TCP	TCP:[Segment Lost]Flags=...A...F, SrcPort=HTTPS(443), DstPort=61012, PayloadLen=0, Seq=1373684975, Ack=789225809, Win=
50	01:03:53 AM 19-10-2023	6.1867762	msedge.exe	192.168.0.106	e13636.dscb.aka...	TCP	TCP:Flags=...A...., SrcPort=61012, DstPort=HTTPS(443), PayloadLen=0, Seq=789225809, Ack=1373684976, Win=515
78	01:03:59 AM 19-10-2023	12.2417507	Dropbox.exe	bolt.v.dropbox.com	192.168.0.106	TLS	TLS:TLS Rec Layer-1 SSL Application Data
79	01:03:59 AM 19-10-2023	12.2590488	Dropbox.exe	192.168.0.106	bolt.v.dropbox.com	TLS	TLS:TLS Rec Layer-1 SSL Application Data
80	01:03:59 AM 19-10-2023	12.2591889	Dropbox.exe	192.168.0.106	bolt.v.dropbox.com	TLS	TLS:TLS Rec Layer-1 SSL Application Data
81	01:04:00 AM 19-10-2023	12.5418781	Dropbox.exe	bolt.v.dropbox.com	192.168.0.106	TCP	TCP:Flags=...A...., SrcPort=HTTPS(443), DstPort=54675, PayloadLen=0, Seq=3708382254, Ack=1280909455, Win=130
82	01:04:00 AM 19-10-2023	12.5418781	Dropbox.exe	bolt.v.dropbox.com	192.168.0.106	TCP	TCP:Flags=...A...., SrcPort=HTTPS(443), DstPort=54675, PayloadLen=0, Seq=3708382254, Ack=1280910895, Win=130
83	01:04:00 AM 19-10-2023	12.5418781	Dropbox.exe	bolt.v.dropbox.com	192.168.0.106	TCP	TCP:Flags=...A...., SrcPort=HTTPS(443), DstPort=54675, PayloadLen=0, Seq=3708382254, Ack=1280911355, Win=130
106	01:04:02 AM 19-10-2023	15.0679507	msedge.exe	192.168.0.106	e13636.dscb.aka...	TCP	TCP:Flags=...A.R.., SrcPort=61006, DstPort=HTTPS(443), PayloadLen=0, Seq=3606241547, Ack=1354983196, Win=0
114	01:04:02 AM 19-10-2023	15.3042161	brave.exe	192.168.0.106	18.161.111.100	TCP	TCP:Flags=......S., SrcPort=61013, DstPort=HTTPS(443), PayloadLen=0, Seq=107189776, Ack=0, Win=64240 (Negotiating scale fa
115	01:04:02 AM 19-10-2023	15.5069058	brave.exe	18.161.111.100	192.168.0.106	TCP	TCP:Flags=...A..S., SrcPort=HTTPS(443), DstPort=61013, PayloadLen=0, Seq=1542104097, Ack=107189777, Win=65535 (Negotia
116	01:04:02 AM 19-10-2023	15.5073747	brave.exe	192.168.0.106	18.161.111.100	TCP	TCP:Flags=...A...., SrcPort=61013, DstPort=HTTPS(443), PayloadLen=0, Seq=107189777, Ack=1542104098, Win=517 (scale facto
117	01:04:02 AM 19-10-2023	15.5082078	brave.exe	192.168.0.106	18.161.111.100	TLS	TLS:TLS Rec Layer-1 HandShake: Client Hello.

Prot Off: Frame Off: Sel Bytes:

0000

Parsed: 30460 Displayed: 2052 Dropped: 0 Captured: 99240 Pending: 0 Focused: Selected:

Search for Tcp.flags.syn==1



All Traffic
My Traffic
msedge.exe (20316)
GoogleDriveFS.exe (11268)
<Unknown>
Dropbox.exe (9504)
brave.exe (160)
NortonSecurity.exe (4352)
WhatsApp.exe (18388)
svchost.exe (4328)
backgroundTaskHost.exe (18076)
svchost.exe (20524)
svchost.exe (4272)
Widgets.exe (8400)
msedge.exe (16244)
svchost.exe (4256)
PAD.Console.Host.exe (12304)
WINWORD.EXE (16368)
VSIXAutoUpdate.exe (20284)
System (0)
svchost.exe (7164)
svchost.exe (3388)
HxTsr.exe (24896)
MicrosoftEdgeUpdate.exe (20744)
MicrosoftEdgeUpdate.exe (19400)
Microsoft.SharePoint.exe (144)
SearchHost.exe (14112)

```
Tcp.flags.syn==1
```

Frame Summary - Tcp.flags.syn==1

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
114	01:04:02 AM 19-10-2023	15.3042161	brave.exe	192.168.0.106	18.161.111.100	TCP	TCP:Flags=......S., SrcPort=61013, DstPort=HTTPS(443), PayloadLen=0, Seq=107189776, Ack=0, Win=64240 (Negotiating scale fa
115	01:04:02 AM 19-10-2023	15.5069058	brave.exe	18.161.111.100	192.168.0.106	TCP	TCP:Flags=...A..S., SrcPort=HTTPS(443), DstPort=61013, PayloadLen=0, Seq=1542104097, Ack=107189777, Win=65535 (Negotia
184	01:04:13 AM 19-10-2023	26.0653446	msedge.exe	192.168.0.106	e13636.dscb.aka...	TCP	TCP:Flags=......S., SrcPort=61014, DstPort=HTTPS(443), PayloadLen=0, Seq=470328440, Ack=0, Win=64240 (Negotiating scale fa
185	01:04:13 AM 19-10-2023	26.0664971	msedge.exe	192.168.0.106	13.107.213.68	TCP	TCP:Flags=......S., SrcPort=61015, DstPort=HTTPS(443), PayloadLen=0, Seq=1776174895, Ack=0, Win=64240 (Negotiating scale
186	01:04:13 AM 19-10-2023	26.0694440	msedge.exe	192.168.0.106	13.107.246.68	TCP	TCP:Flags=......S., SrcPort=61016, DstPort=HTTPS(443), PayloadLen=0, Seq=3841041962, Ack=0, Win=64240 (Negotiating scale
187	01:04:13 AM 19-10-2023	26.0725550	msedge.exe	e13636.dscb.aka...	192.168.0.106	TCP	TCP:Flags=...A..S., SrcPort=HTTPS(443), DstPort=61014, PayloadLen=0, Seq=1349678476, Ack=470328441, Win=64240 (Negotia
188	01:04:13 AM 19-10-2023	26.0725550	msedge.exe	13.107.213.68	192.168.0.106	TCP	TCP:Flags=...A..S., SrcPort=HTTPS(443), DstPort=61015, PayloadLen=0, Seq=593583928, Ack=1776174896, Win=64860 (Negotia
192	01:04:13 AM 19-10-2023	26.0765787	msedge.exe	13.107.246.68	192.168.0.106	TCP	TCP:Flags=...A..S., SrcPort=HTTPS(443), DstPort=61016, PayloadLen=0, Seq=45909004, Ack=3841041963, Win=64860 (Negotiat
226	01:04:13 AM 19-10-2023	26.4023688	msedge.exe	192.168.0.106	20.189.173.8	TCP	TCP:Flags=......S., SrcPort=61017, DstPort=HTTPS(443), PayloadLen=0, Seq=2640677374, Ack=0, Win=64240 (Negotiating scale
245	01:04:14 AM 19-10-2023	26.6645065	msedge.exe	192.168.0.106	20.189.173.8	TCP	TCP:Flags=......S., SrcPort=61018, DstPort=HTTPS(443), PayloadLen=0, Seq=454297526, Ack=0, Win=64240 (Negotiating scale fa
255	01:04:14 AM 19-10-2023	26.6785538	msedge.exe	20.189.173.8	192.168.0.106	TCP	TCP:Flags=...A..S., SrcPort=HTTPS(443), DstPort=61017, PayloadLen=0, Seq=2224813075, Ack=2640677375, Win=65535 (Negot
258	01:04:14 AM 19-10-2023	26.7263657	msedge.exe	192.168.0.106	20.189.173.8	TCP	TCP:Flags=......S., SrcPort=61019, DstPort=HTTPS(443), PayloadLen=0, Seq=2968491647, Ack=0, Win=64240 (Negotiating scale
259	01:04:14 AM 19-10-2023	26.9787011	msedge.exe	20.189.173.8	192.168.0.106	TCP	TCP:Flags=...A..S., SrcPort=HTTPS(443), DstPort=61018, PayloadLen=0, Seq=910143790, Ack=454297527, Win=65535 (Negotiat
267	01:04:14 AM 19-10-2023	26.9804128	msedge.exe	20.189.173.8	192.168.0.106	TCP	TCP:Flags=...A..S., SrcPort=HTTPS(443), DstPort=61019, PayloadLen=0, Seq=28998002, Ack=2968491648, Win=65535 (Negotiat
405	01:04:19 AM 19-10-2023	32.1848106	msedge.exe	192.168.0.106	204.79.197.239	TCP	TCP:Flags=......S., SrcPort=61020, DstPort=HTTPS(443), PayloadLen=0, Seq=2774289331, Ack=0, Win=64240 (Negotiating scale
406	01:04:19 AM 19-10-2023	32.1893742	msedge.exe	204.79.197.239	192.168.0.106	TCP	TCP:Flags=...A..S., SrcPort=HTTPS(443), DstPort=61020, PayloadLen=0, Seq=3734141121, Ack=2774289332, Win=65535 (Negot
430	01:04:19 AM 19-10-2023	32.2394263	brave.exe	192.168.0.106	108.159.61.113	TCP	TCP:Flags=......S., SrcPort=61021, DstPort=HTTPS(443), PayloadLen=0, Seq=3069821521, Ack=0, Win=64240 (Negotiating scale
431	01:04:19 AM 19-10-2023	32.2443109	brave.exe	108.159.61.113	192.168.0.106	TCP	TCP:Flags=...A..S., SrcPort=HTTPS(443), DstPort=61021, PayloadLen=0, Seq=2266673839, Ack=3069821522, Win=65535 (Negot
448	01:04:19 AM 19-10-2023	32.2600431	brave.exe	192.168.0.106	52.13.172.91	TCP	TCP:Flags=......S., SrcPort=61022, DstPort=HTTPS(443), PayloadLen=0, Seq=3793083041, Ack=0, Win=64240 (Negotiating scale
473	01:04:19 AM 19-10-2023	32.5183369	brave.exe	192.168.0.106	52.13.172.91	TCP	TCP:Flags=......S., SrcPort=61023, DstPort=HTTPS(443), PayloadLen=0, Seq=2980016766, Ack=0, Win=64240 (Negotiating scale
474	01:04:20 AM 19-10-2023	32.5322642	brave.exe	52.13.172.91	192.168.0.106	TCP	TCP:Flags=...A..S., SrcPort=HTTPS(443), DstPort=61022, PayloadLen=0, Seq=3935984528, Ack=3793083042, Win=26883 (Negot
477	01:04:20 AM 19-10-2023	32.8145164	brave.exe	52.13.172.91	192.168.0.106	TCP	TCP:Flags=...A..S., SrcPort=HTTPS(443), DstPort=61023, PayloadLen=0, Seq=3788056964, Ack=2980016767, Win=26883 (Negot

0000

Parsed: 42938 Displayed: 153 Dropped: 0 Captured: 111477 Pending: 0 Focused: Selected:

4.Autoruns

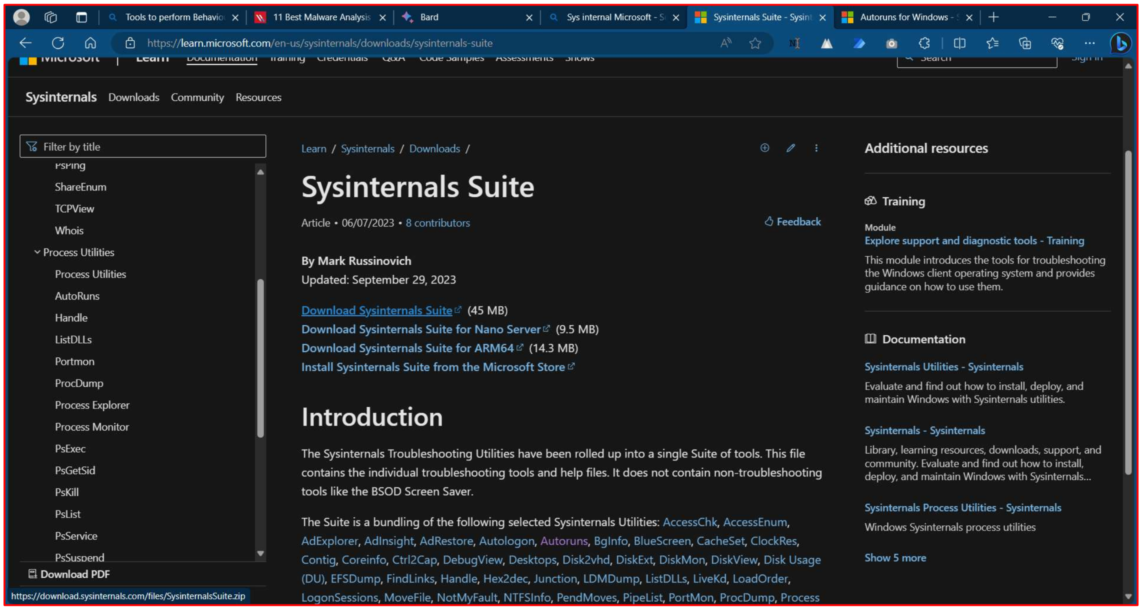
Description:-

Autoruns is another Microsoft tool that will display any installed software on a device that is set to launch when a machine is powered on. Malware can hide but ultimately it has to run and in order to survive a reboot a piece of malware must create a persistence mechanism.

There are a few techniques that can be employed to achieve this objective such as creating a scheduled task or creating specific run keys within the registry. After running a piece of malware in a VM running Autoruns will detect and highlight any new persistent software and the technique it has implemented making it ideal for malware analysis.

Steps:-

Download Sysinternals Suite from Sysinternals Microsoft official website.



Learn / Sysinternals / Downloads /

Sysinternals Suite

Article • 06/07/2023 • 8 contributors

By Mark Russinovich
Updated: September 29, 2023

Download Sysinternals Suite (45 MB)
Download Sysinternals Suite for Nano Server (9.5 MB)
Download Sysinternals Suite for ARM64 (14.3 MB)
Install Sysinternals Suite from the Microsoft Store

Introduction

The Sysinternals Troubleshooting Utilities have been rolled up into a single Suite of tools. This file contains the individual troubleshooting tools and help files. It does not contain non-troubleshooting tools like the BSOD Screen Saver.

The Suite is a bundling of the following selected Sysinternals Utilities: AccessChk, AccessEnum, AdExplorer, AdInsight, AdRestore, Autologon, Autoruns, BgInfo, BlueScreen, CacheSet, ClockRes, Contig, Coreinfo, Ctrl2Cap, DebugView, Desktops, Disk2vhd, DiskExt, DiskMon, DiskView, Disk Usage (DU), EFSDump, FindLinks, Handle, Hex2dec, Junction, LDMDump, ListDLLs, LiveKd, LoadOrder, LogonSessions, MoveFile, NotMyFault, NTFSInfo, PendMoves, PipeList, PortMon, ProcDump, Process

Additional resources

Training

Module
Explore support and diagnostic tools - Training
This module introduces the tools for troubleshooting the Windows client operating system and provides guidance on how to use them.

Documentation

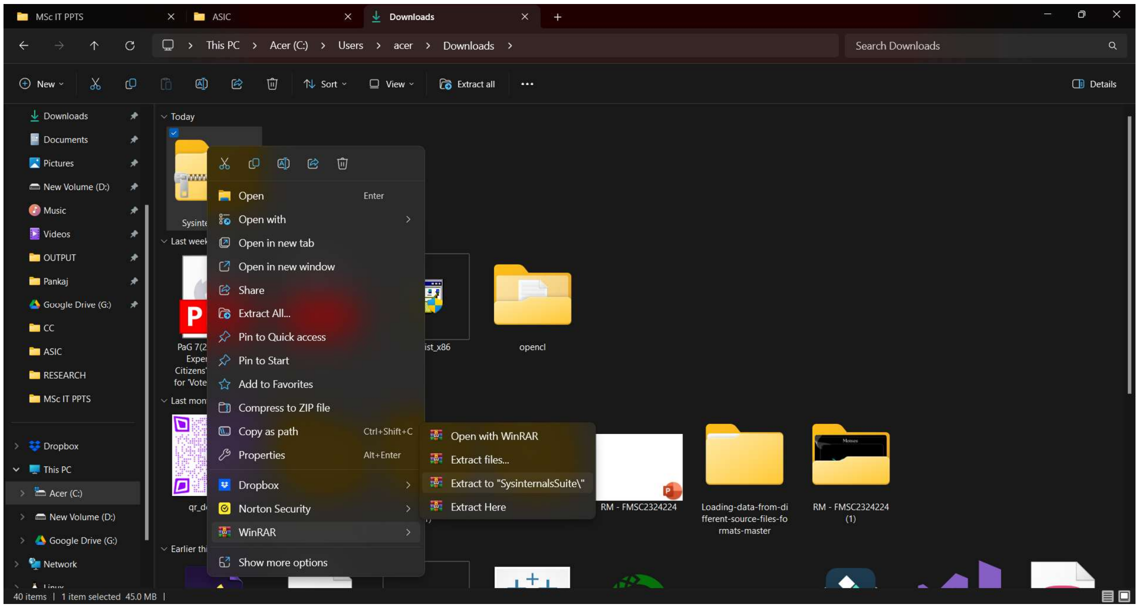
Sysinternals Utilities - Sysinternals
Evaluate and find out how to install, deploy, and maintain Windows with Sysinternals utilities.

Sysinternals - Sysinternals
Library, learning resources, downloads, support, and community. Evaluate and find out how to install, deploy, and maintain Windows with Sysinternals...

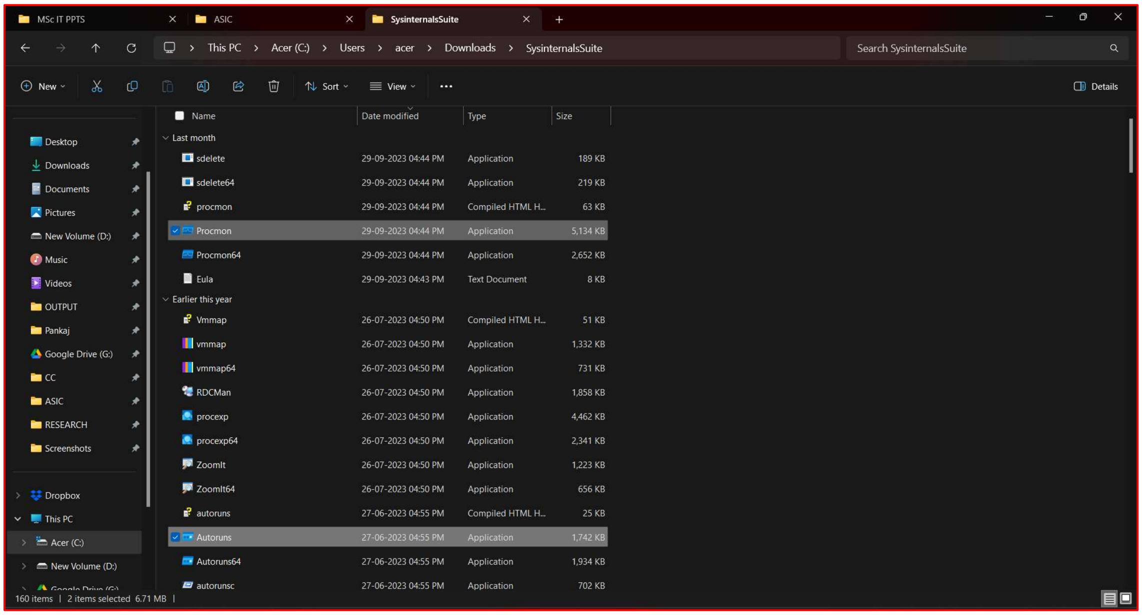
Sysinternals Process Utilities - Sysinternals
Windows Sysinternals process utilities

Show 5 more

Extract the downloaded file.



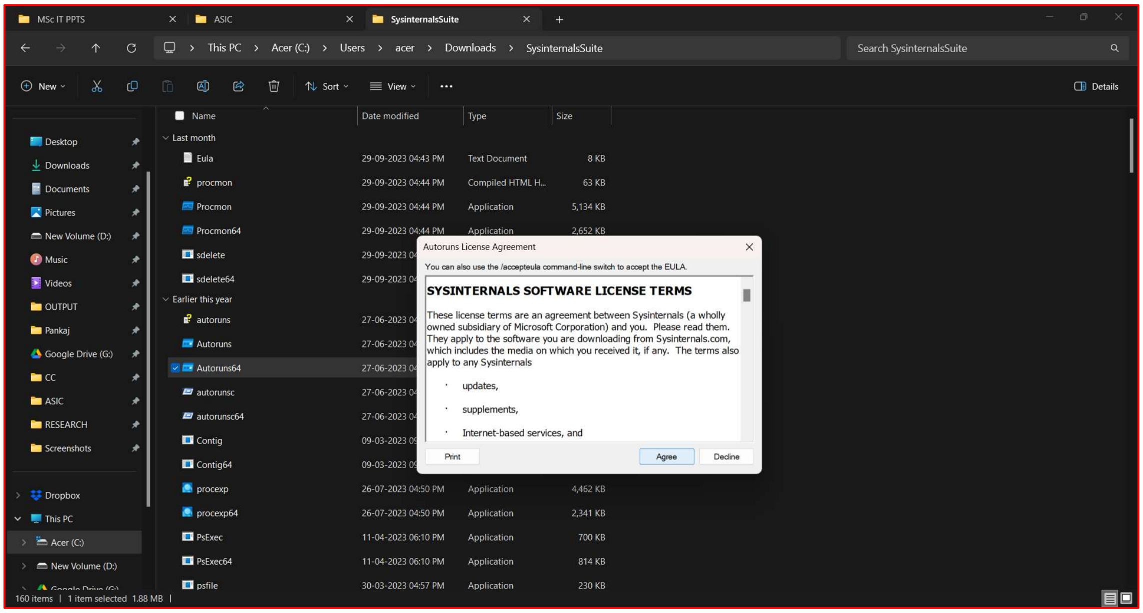
After opening the extracted file you can find the Autoruns application inside the folder and many other applications like procmon which is used in these practical earlier.


This PC > Acer (C:) > Users > acer > Downloads > SysinternalsSuite

Name	Date modified	Type	Size
Last month			
sdelete	29-09-2023 04:44 PM	Application	189 KB
sdelete64	29-09-2023 04:44 PM	Application	219 KB
procmon	29-09-2023 04:44 PM	Compiled HTML H...	63 KB
☑ Procmon	29-09-2023 04:44 PM	Application	5,134 KB
Procmon64	29-09-2023 04:44 PM	Application	2,652 KB
Eula	29-09-2023 04:43 PM	Text Document	8 KB
Earlier this year			
Vmmap	26-07-2023 04:50 PM	Compiled HTML H...	51 KB
vmmap	26-07-2023 04:50 PM	Application	1,332 KB
vmmap64	26-07-2023 04:50 PM	Application	731 KB
RDCMan	26-07-2023 04:50 PM	Application	1,858 KB
procexp	26-07-2023 04:50 PM	Application	4,462 KB
procexp64	26-07-2023 04:50 PM	Application	2,341 KB
ZoomIt	26-07-2023 04:50 PM	Application	1,223 KB
ZoomIt64	26-07-2023 04:50 PM	Application	656 KB
autoruns	27-06-2023 04:55 PM	Compiled HTML H...	25 KB
☑ Autoruns	27-06-2023 04:55 PM	Application	1,742 KB
Autoruns64	27-06-2023 04:55 PM	Application	1,934 KB
autorunsc	27-06-2023 04:55 PM	Application	702 KB

160 items | 2 items selected 6.71 MB |

Click on Autoruns64 > pop up will appear click agree.



Name	Date modified	Type	Size
Last month			
Eula	29-09-2023 04:43 PM	Text Document	8 KB
procmon	29-09-2023 04:44 PM	Compiled HTML H...	63 KB
Procmon	29-09-2023 04:44 PM	Application	5,134 KB
Procmon64	29-09-2023 04:44 PM	Application	2,652 KB
sdelete	29-09-2023 0		
sdelete64	29-09-2023 0		
Earlier this year			
autoruns	27-06-2023 0		
Autoruns	27-06-2023 0		
Autoruns64	27-06-2023 0		
autorunsc	27-06-2023 0		
autorunsc64	27-06-2023 0		
Contig	09-03-2023 0		
Contig64	09-03-2023 0		
procexp	26-07-2023 04:50 PM	Application	4,462 KB
procexp64	26-07-2023 04:50 PM	Application	2,341 KB
PsExec	11-04-2023 06:10 PM	Application	700 KB
PsExec64	11-04-2023 06:10 PM	Application	814 KB
psfile	30-03-2023 04:57 PM	Application	230 KB

160 items | 1 item selected 1.88 MB |

Autoruns License Agreement

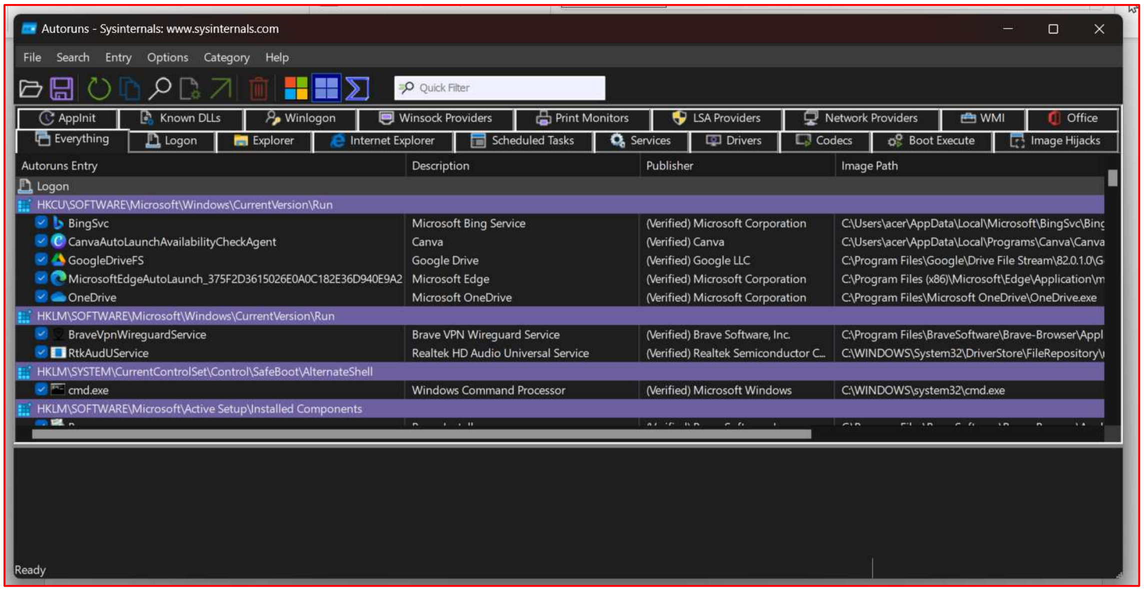
You can also use the /accepteula command-line switch to accept the EULA.

SYSINTERNALS SOFTWARE LICENSE TERMS

These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Sysinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals

- updates,
- supplements,
- Internet-based services, and

Autoruns window will appear



Autoruns Entry	Description	Publisher	Image Path
Logon			
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
☑ BingSvc	Microsoft Bing Service	(Verified) Microsoft Corporation	C:\Users\acer\AppData\Local\Microsoft\BingSvc\Bing
☑ CanvaAutoLaunchAvailabilityCheckAgent	Canva	(Verified) Canva	C:\Users\acer\AppData\Local\Programs\Canva\Canva
☑ GoogleDriveFS	Google Drive	(Verified) Google LLC	C:\Program Files\Google\Drive File Stream\82.0.1.0\G
☑ MicrosoftEdgeAutoLaunch_375F2D3615026E0A0C182E36D940E9A2	Microsoft Edge	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\m
☑ OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	C:\Program Files\Microsoft OneDrive\OneDrive.exe
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
☑ BraveVpnWireguardService	Brave VPN Wireguard Service	(Verified) Brave Software, Inc.	C:\Program Files\BraveSoftware\Brave-Browser\Appl
☑ RtkAudUService	Realtek HD Audio Universal Service	(Verified) Realtek Semiconductor C...	C:\WINDOWS\System32\DriverStore\FileRepository\
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell			
☑ cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	C:\WINDOWS\system32\cmd.exe
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components			