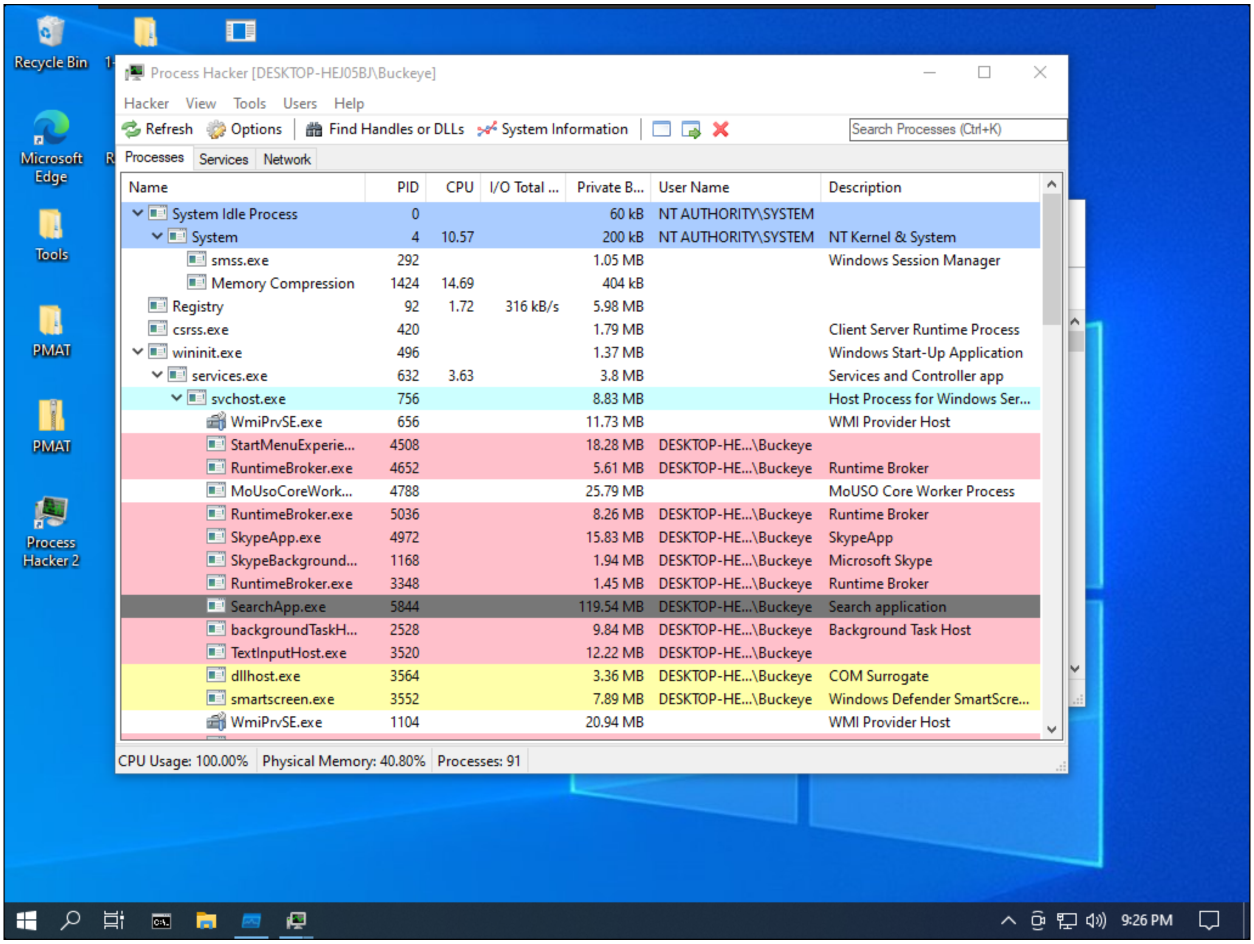
Assignment

Name: Hassan Ahmed
Class: BS DFCS
Section: A
ID: Fa 19/BS DFCS/026
Instructor: Sir Taseer Suleeman

Generate a Procmon-based report. Also write about the details of windows based processes such as explorer.exe, procmon.exe, ntoskrnl.exe.

Process Hacker

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.

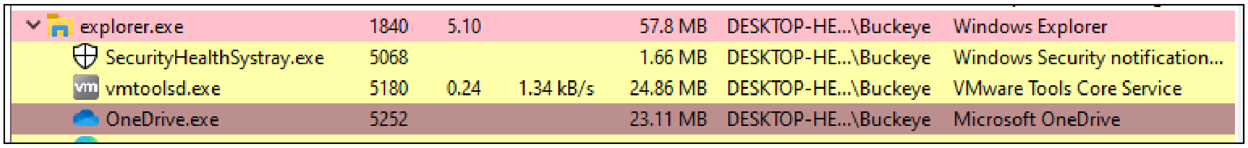

Recycle Bin
Microsoft Edge
Tools
PMAT
PMAT
Process Hacker 2
Process Hacker [DESKTOP-HEJ05BJ\Buckeye]
Hacker View Tools Users Help
Refresh Options Find Handles or DLLs System Information
Search Processes (Ctrl+K)
Processes Services Network
9:26 PM

Name	PID	CPU	I/O Total ...	Private B...	User Name	Description
System Idle Process	0			60 kB	NT AUTHORITY\SYSTEM	
System	4	10.57		200 kB	NT AUTHORITY\SYSTEM	NT Kernel & System
smss.exe	292			1.05 MB		Windows Session Manager
Memory Compression	1424	14.69		404 kB		
Registry	92	1.72	316 kB/s	5.98 MB		
csrss.exe	420			1.79 MB		Client Server Runtime Process
wininit.exe	496			1.37 MB		Windows Start-Up Application
services.exe	632	3.63		3.8 MB		Services and Controller app
svchost.exe	756			8.83 MB		Host Process for Windows Ser...
WmiPrvSE.exe	656			11.73 MB		WMI Provider Host
StartMenuExperie...	4508			18.28 MB	DESKTOP-HE...\Buckeye	
RuntimeBroker.exe	4652			5.61 MB	DESKTOP-HE...\Buckeye	Runtime Broker
MoUsoCoreWork...	4788			25.79 MB		MoUSO Core Worker Process
RuntimeBroker.exe	5036			8.26 MB	DESKTOP-HE...\Buckeye	Runtime Broker
SkypeApp.exe	4972			15.83 MB	DESKTOP-HE...\Buckeye	SkypeApp
SkypeBackground...	1168			1.94 MB	DESKTOP-HE...\Buckeye	Microsoft Skype
RuntimeBroker.exe	3348			1.45 MB	DESKTOP-HE...\Buckeye	Runtime Broker
SearchApp.exe	5844			119.54 MB	DESKTOP-HE...\Buckeye	Search application
backgroundTaskH...	2528			9.84 MB	DESKTOP-HE...\Buckeye	Background Task Host
TextInputHost.exe	3520			12.22 MB	DESKTOP-HE...\Buckeye	
dllhost.exe	3564			3.36 MB	DESKTOP-HE...\Buckeye	COM Surrogate
smartscreen.exe	3552			7.89 MB	DESKTOP-HE...\Buckeye	Windows Defender SmartScre...
WmiPrvSE.exe	1104			20.94 MB		WMI Provider Host

CPU Usage: 100.00% | Physical Memory: 40.80% | Processes: 91

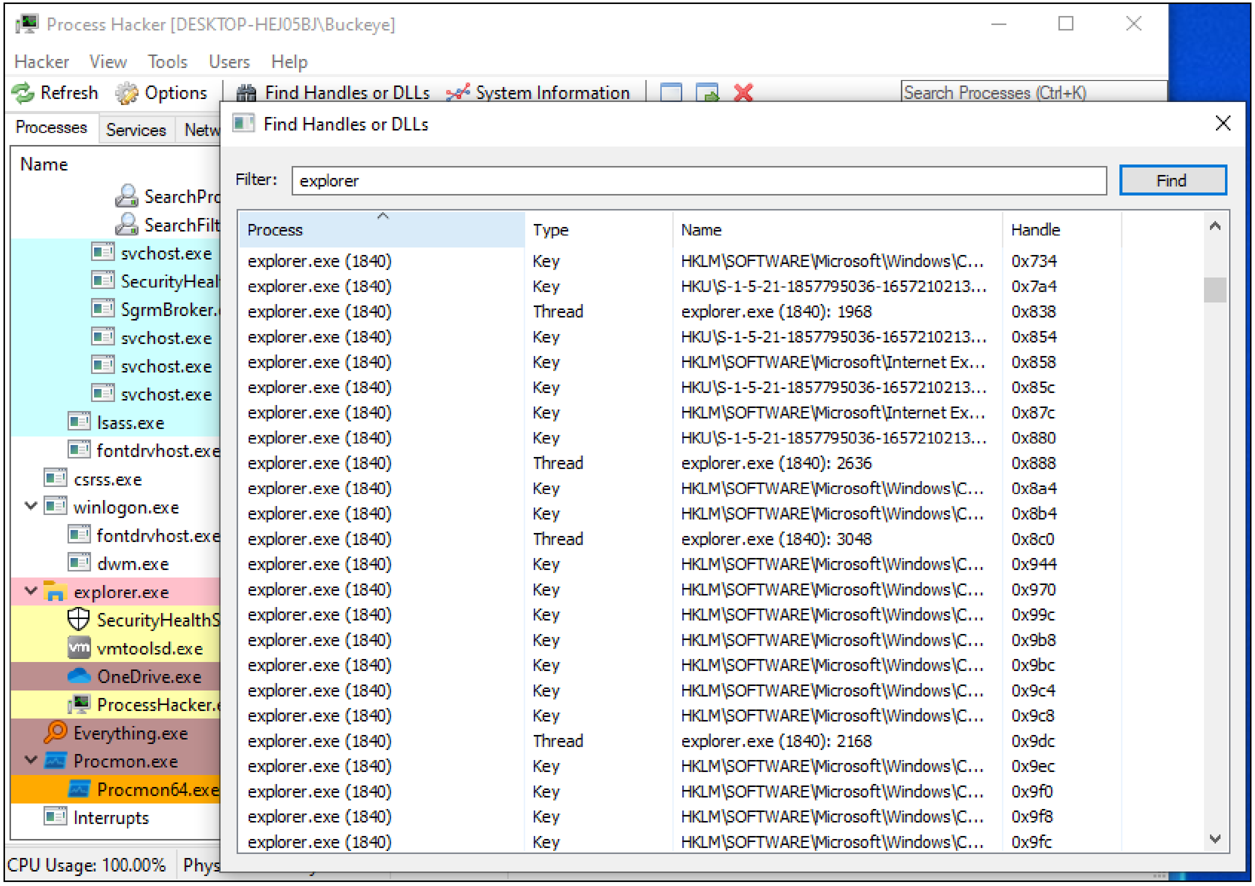
It runs a process "explorer.exe"

Windows Explorer (Explorer.exe) is the process responsible for starting and displaying most of the user interface (UI), including the desktop, taskbar, Action Center, Start menu, and File Explorer



explorer.exe	1840	5.10		57.8 MB	DESKTOP-HE...\Buckeye	Windows Explorer
SecurityHealthSystray.exe	5068			1.66 MB	DESKTOP-HE...\Buckeye	Windows Security notification...
vmtoolsd.exe	5180	0.24	1.34 kB/s	24.86 MB	DESKTOP-HE...\Buckeye	VMware Tools Core Service
OneDrive.exe	5252			23.11 MB	DESKTOP-HE...\Buckeye	Microsoft OneDrive

To view dll and threads, we will click on the top “Finds Handles or DLLs”

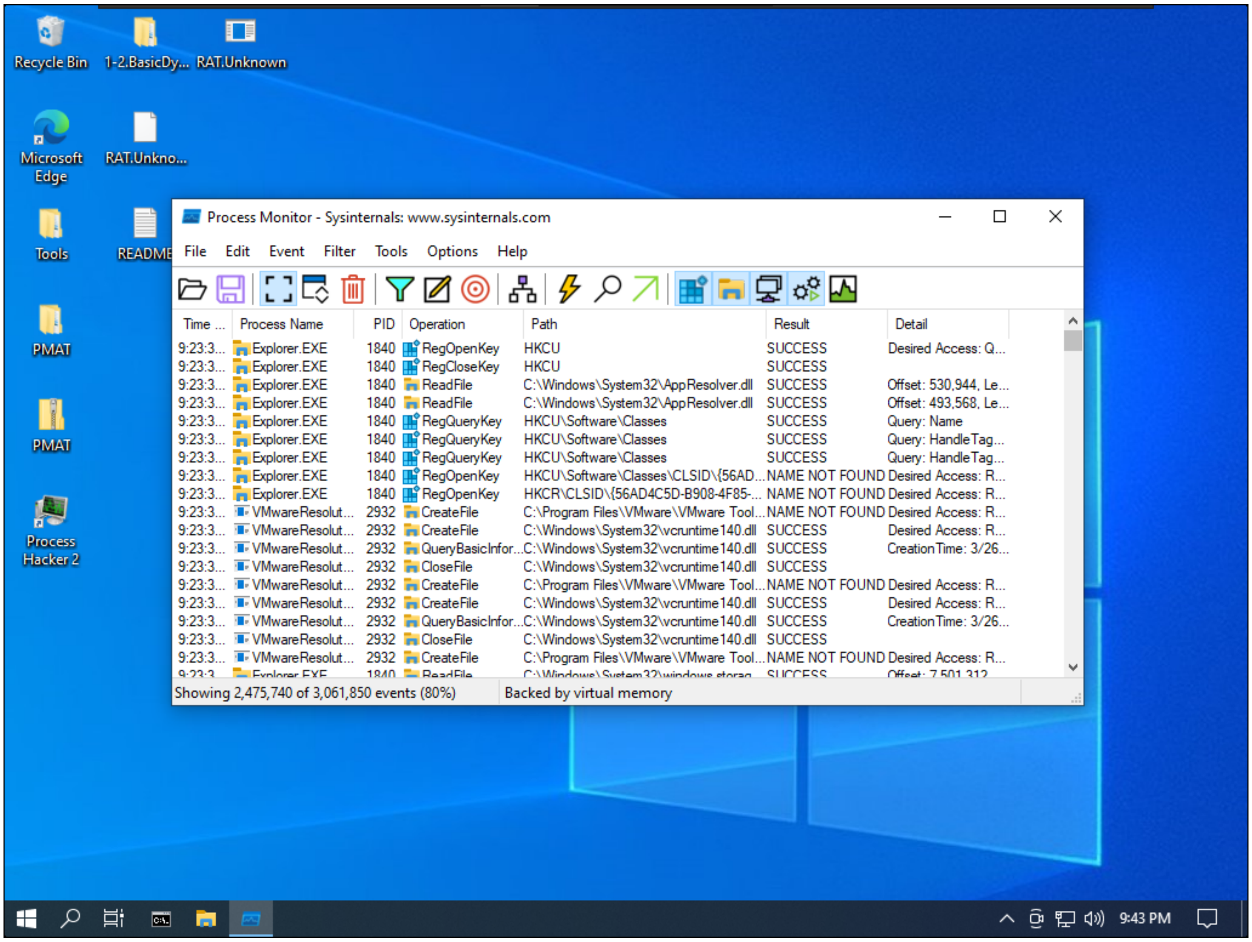


Filter: explorer

Process	Type	Name	Handle
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x734
explorer.exe (1840)	Key	HKU\S-1-5-21-1857795036-1657210213...	0x7a4
explorer.exe (1840)	Thread	explorer.exe (1840): 1968	0x838
explorer.exe (1840)	Key	HKU\S-1-5-21-1857795036-1657210213...	0x854
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Internet Ex...	0x858
explorer.exe (1840)	Key	HKU\S-1-5-21-1857795036-1657210213...	0x85c
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Internet Ex...	0x87c
explorer.exe (1840)	Key	HKU\S-1-5-21-1857795036-1657210213...	0x880
explorer.exe (1840)	Thread	explorer.exe (1840): 2636	0x888
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x8a4
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x8b4
explorer.exe (1840)	Thread	explorer.exe (1840): 3048	0x8c0
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x944
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x970
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x99c
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x9b8
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x9bc
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x9c4
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x9c8
explorer.exe (1840)	Thread	explorer.exe (1840): 2168	0x9dc
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x9ec
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x9f0
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x9f8
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x9fc

Procmon(Process Monitor)

Process Monitor is a tool from Windows Sysinternals, part of the Microsoft TechNet website. The tool monitors and displays in real-time all file system activity on a Microsoft Windows or Unix-like operating system.

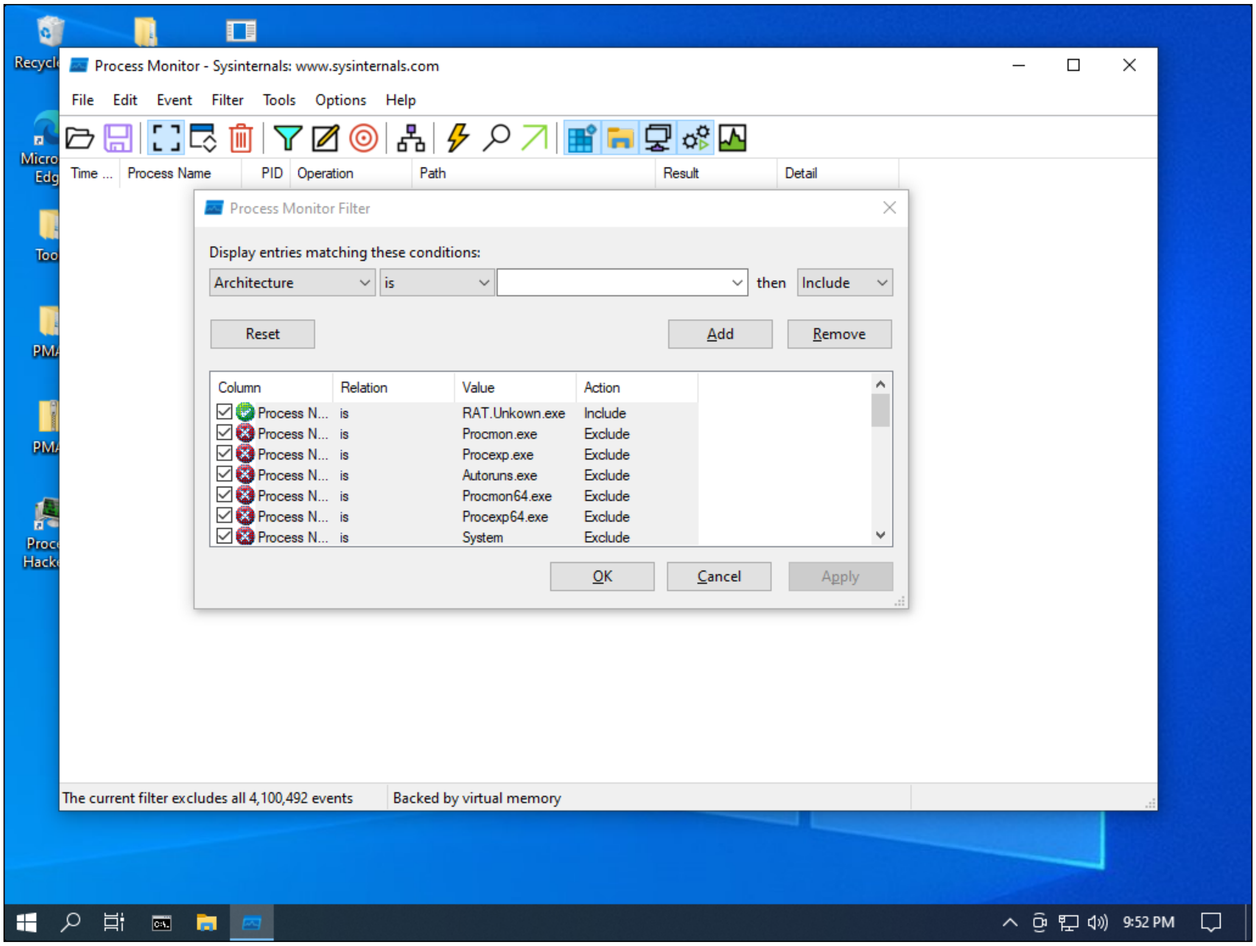


Process Monitor - Sysinternals: www.sysinternals.com

Time ...	Process Name	PID	Operation	Path	Result	Detail
9:23:3...	Explorer.EXE	1840	RegOpenKey	HKCU	SUCCESS	Desired Access: Q...
9:23:3...	Explorer.EXE	1840	RegCloseKey	HKCU	SUCCESS	
9:23:3...	Explorer.EXE	1840	ReadFile	C:\Windows\System32\AppResolver.dll	SUCCESS	Offset: 530,944, Le...
9:23:3...	Explorer.EXE	1840	ReadFile	C:\Windows\System32\AppResolver.dll	SUCCESS	Offset: 493,568, Le...
9:23:3...	Explorer.EXE	1840	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
9:23:3...	Explorer.EXE	1840	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
9:23:3...	Explorer.EXE	1840	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
9:23:3...	Explorer.EXE	1840	RegOpenKey	HKCU\Software\Classes\CLSID\{56AD...	NAME NOT FOUND	Desired Access: R...
9:23:3...	Explorer.EXE	1840	RegOpenKey	HKCR\CLSID\{56AD4C5D-B908-4F85-...	NAME NOT FOUND	Desired Access: R...
9:23:3...	VMwareResolut...	2932	CreateFile	C:\Program Files\VMware\VMware Tool...	NAME NOT FOUND	Desired Access: R...
9:23:3...	VMwareResolut...	2932	CreateFile	C:\Windows\System32\vcruntime140.dll	SUCCESS	Desired Access: R...
9:23:3...	VMwareResolut...	2932	QueryBasicInfor...	C:\Windows\System32\vcruntime140.dll	SUCCESS	CreationTime: 3/26...
9:23:3...	VMwareResolut...	2932	CloseFile	C:\Windows\System32\vcruntime140.dll	SUCCESS	
9:23:3...	VMwareResolut...	2932	CreateFile	C:\Program Files\VMware\VMware Tool...	NAME NOT FOUND	Desired Access: R...
9:23:3...	VMwareResolut...	2932	CreateFile	C:\Windows\System32\vcruntime140.dll	SUCCESS	Desired Access: R...
9:23:3...	VMwareResolut...	2932	QueryBasicInfor...	C:\Windows\System32\vcruntime140.dll	SUCCESS	CreationTime: 3/26...
9:23:3...	VMwareResolut...	2932	CloseFile	C:\Windows\System32\vcruntime140.dll	SUCCESS	
9:23:3...	VMwareResolut...	2932	CreateFile	C:\Program Files\VMware\VMware Tool...	NAME NOT FOUND	Desired Access: R...
9:23:3	Explorer.EXE	1840	ReadFile	C:\Windows\System32\windows.storag	SUCCESS	Offset: 7,501,312

Showing 2,475,740 of 3,061,850 events (80%) Backed by virtual memory

It show all process currently running on the system. If we want to check specific malware process then we have to make filer on it and run the process


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
Process Monitor Filter
Reset
Add
Remove
OK
Cancel
Apply
9:52 PM

Display entries matching these conditions:

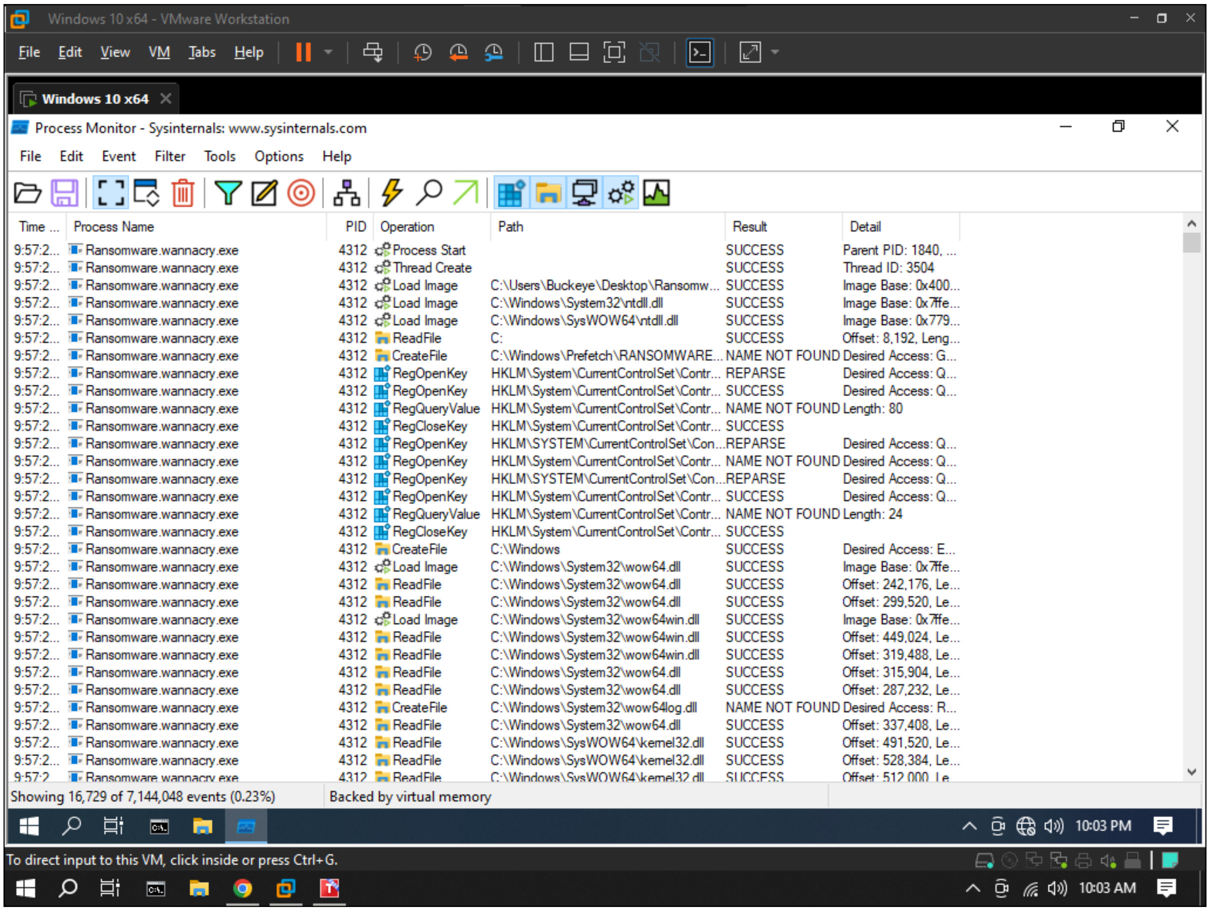
Architecture | is | | then Include

Column	Relation	Value	Action
☑ Process N...	is	RAT.Unkown.exe	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

The current filter excludes all 4,100,492 events

Backed by virtual memory

Now Running the one of known malware “Wannacry.exe”


Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
Windows 10 x64
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
10:03 PM
10:03 AM

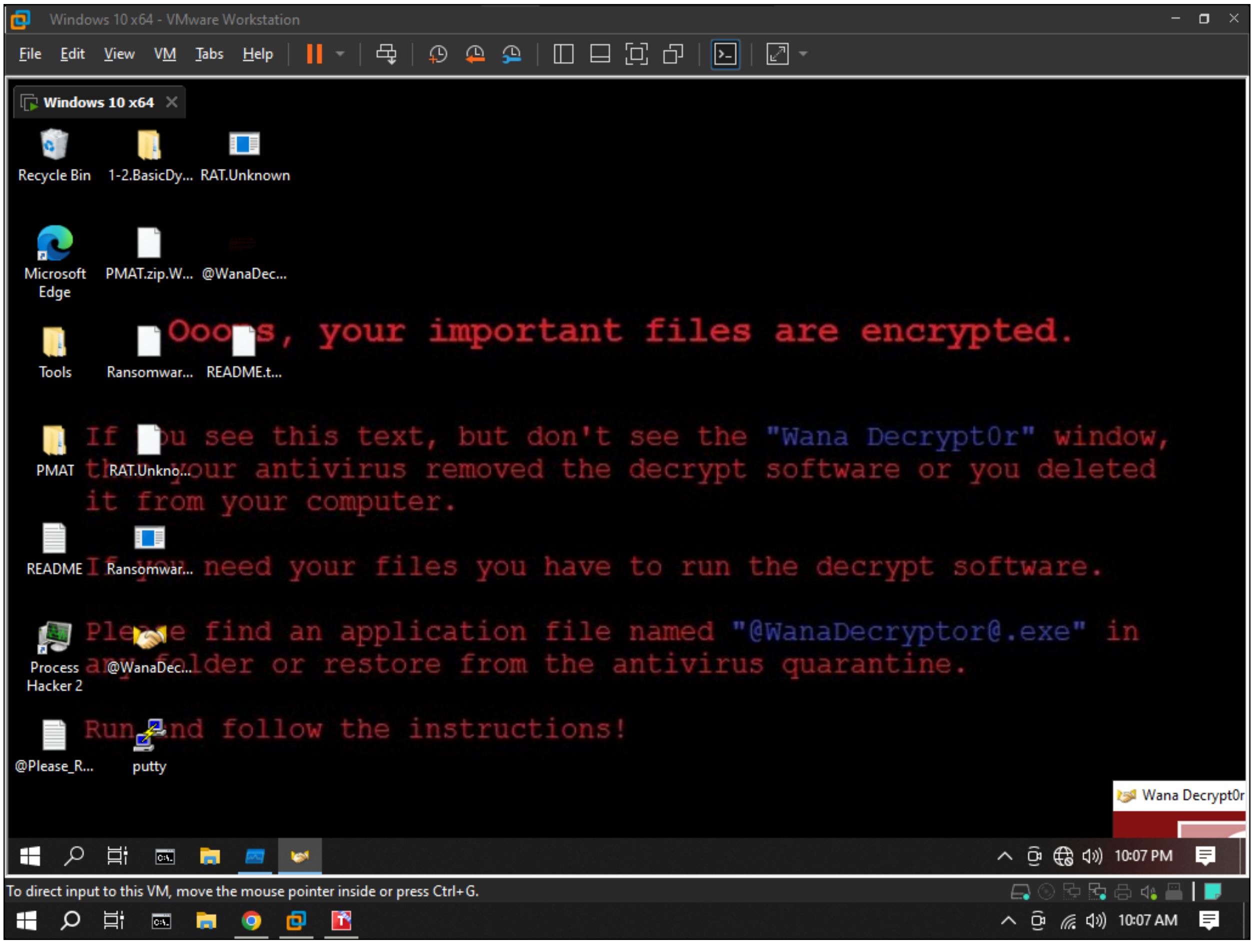
Time ...	Process Name	PID	Operation	Path	Result	Detail
9:57:2...	Ransomware.wannacry.exe	4312	Process Start		SUCCESS	Parent PID: 1840, ...
9:57:2...	Ransomware.wannacry.exe	4312	Thread Create		SUCCESS	Thread ID: 3504
9:57:2...	Ransomware.wannacry.exe	4312	Load Image	C:\Users\Buckeye\Desktop\Ransomw...	SUCCESS	Image Base: 0x400...
9:57:2...	Ransomware.wannacry.exe	4312	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffe...
9:57:2...	Ransomware.wannacry.exe	4312	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x779...
9:57:2...	Ransomware.wannacry.exe	4312	ReadFile	C:	SUCCESS	Offset: 8,192, Leng...
9:57:2...	Ransomware.wannacry.exe	4312	CreateFile	C:\Windows\Prefetch\RANSOMWARE...	NAME NOT FOUND	Desired Access: G...
9:57:2...	Ransomware.wannacry.exe	4312	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
9:57:2...	Ransomware.wannacry.exe	4312	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
9:57:2...	Ransomware.wannacry.exe	4312	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 80
9:57:2...	Ransomware.wannacry.exe	4312	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
9:57:2...	Ransomware.wannacry.exe	4312	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
9:57:2...	Ransomware.wannacry.exe	4312	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
9:57:2...	Ransomware.wannacry.exe	4312	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
9:57:2...	Ransomware.wannacry.exe	4312	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
9:57:2...	Ransomware.wannacry.exe	4312	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 24
9:57:2...	Ransomware.wannacry.exe	4312	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
9:57:2...	Ransomware.wannacry.exe	4312	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
9:57:2...	Ransomware.wannacry.exe	4312	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x7ffe...
9:57:2...	Ransomware.wannacry.exe	4312	ReadFile	C:\Windows\System32\wow64.dll	SUCCESS	Offset: 242,176, Le...
9:57:2...	Ransomware.wannacry.exe	4312	ReadFile	C:\Windows\System32\wow64.dll	SUCCESS	Offset: 299,520, Le...
9:57:2...	Ransomware.wannacry.exe	4312	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x7ffe...
9:57:2...	Ransomware.wannacry.exe	4312	ReadFile	C:\Windows\System32\wow64win.dll	SUCCESS	Offset: 449,024, Le...
9:57:2...	Ransomware.wannacry.exe	4312	ReadFile	C:\Windows\System32\wow64win.dll	SUCCESS	Offset: 319,488, Le...
9:57:2...	Ransomware.wannacry.exe	4312	ReadFile	C:\Windows\System32\wow64.dll	SUCCESS	Offset: 315,904, Le...
9:57:2...	Ransomware.wannacry.exe	4312	ReadFile	C:\Windows\System32\wow64.dll	SUCCESS	Offset: 287,232, Le...
9:57:2...	Ransomware.wannacry.exe	4312	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access: R...
9:57:2...	Ransomware.wannacry.exe	4312	ReadFile	C:\Windows\System32\wow64.dll	SUCCESS	Offset: 337,408, Le...
9:57:2...	Ransomware.wannacry.exe	4312	ReadFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Offset: 491,520, Le...
9:57:2...	Ransomware.wannacry.exe	4312	ReadFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Offset: 528,384, Le...
9:57:2	Ransomware.wannacry.exe	4312	ReadFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Offset: 512,000, Le

Showing 16,729 of 7,144,048 events (0.23%)   Backed by virtual memory

To direct input to this VM, click inside or press Ctrl+G.

So here are the process load by the WannaCry.exe

Because of not setting the network and domain used by this ransomware, it didn't proceed , as it need to request a domain first but it execute some host based process:



Windows 10 x64 - VMware Workstation

Ooo s, your important files are encrypted.

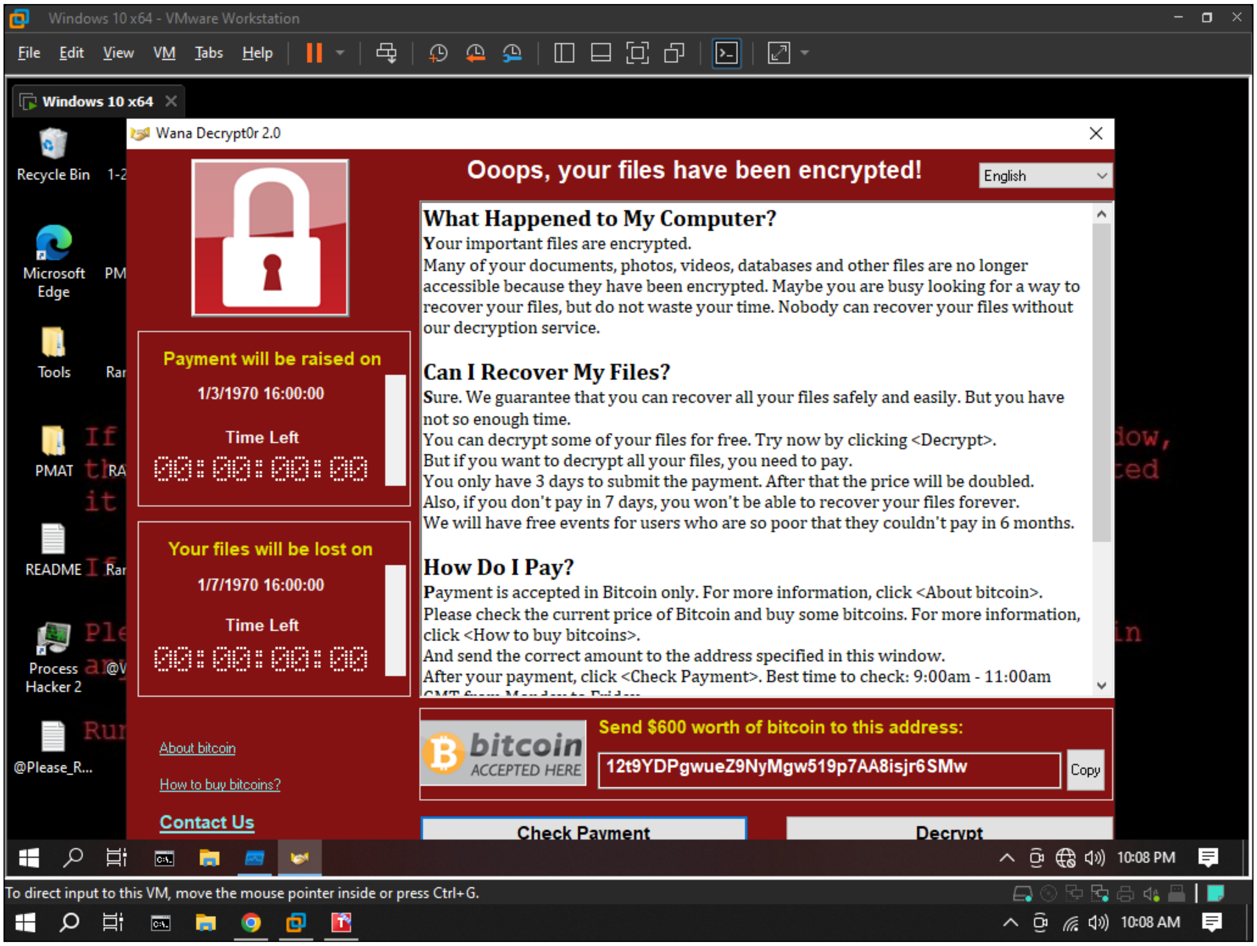
If u see this text, but don't see the "Wana Decrypt0r" window,
t our antivirus removed the decrypt software or you deleted
it from your computer.

I need your files you have to run the decrypt software.

Ple e find an application file named "@WanaDecryptor@.exe" in
a older or restore from the antivirus quarantine.

Run nd follow the instructions!

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Ooops, your files have been encrypted!

Payment will be raised on

1/3/1970 16:00:00

Time Left

00:00:00:00

Your files will be lost on

1/7/1970 16:00:00

Time Left

00:00:00:00

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $600 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

ntoskrnl.exe

ntoskrnl.exe (short for Windows NT operating system kernel executable), also known as the kernel image, contains the kernel and executive layers of the Microsoft Windows NT kernel, and is responsible for hardware abstraction, process handling, and memory management. In addition to the kernel and executive mentioned earlier, it contains the cache manager, security reference monitor, memory manager, scheduler (Dispatcher), and blue screen of death (the prose and portions of the code.