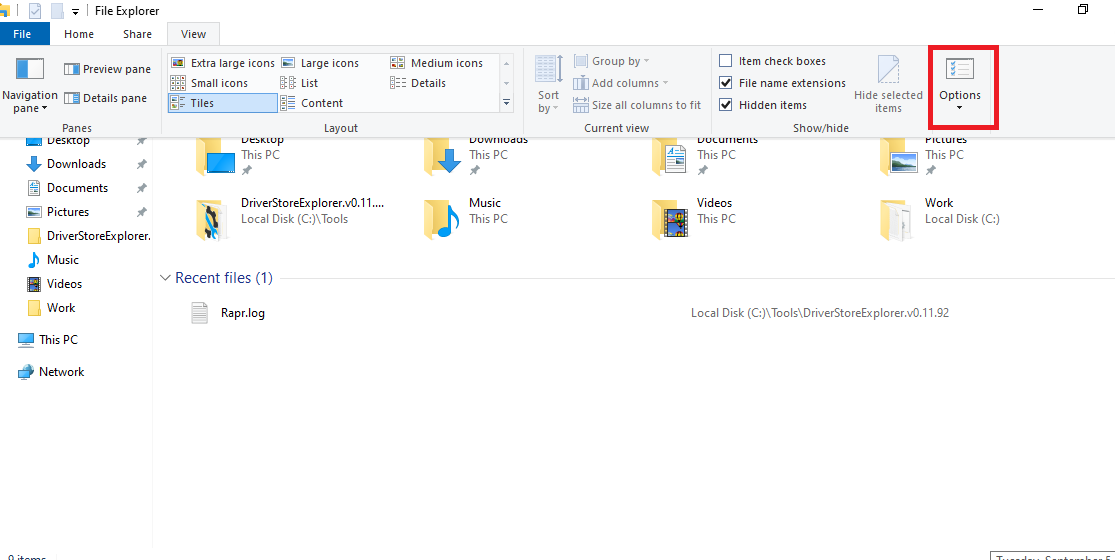
Hi Lukas.

I am going to explained my experience in Windows system management.

I want my experience to help you. If any question, please contact me.

1. Windows System Configure

Please set to show hidden file and file extensions



Why?

- hidden file

If file hidden property is set, this file is not showed in File Explorer.

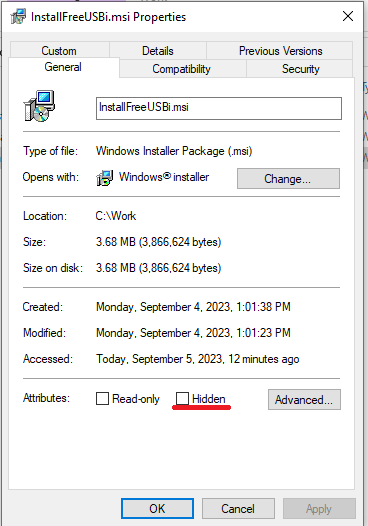
System hidden property is strong than general hidden property.

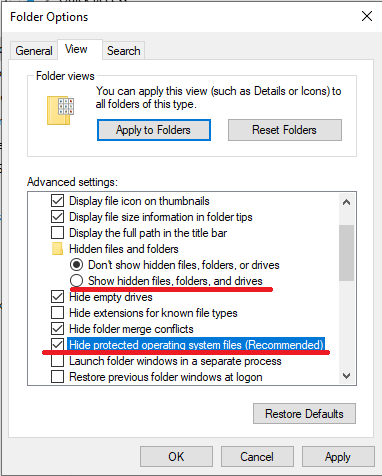
After initial installation Windows, showing hidden/system hidden file is disabled.

So, user can feel C drive is very clean, but malware abuse this point.

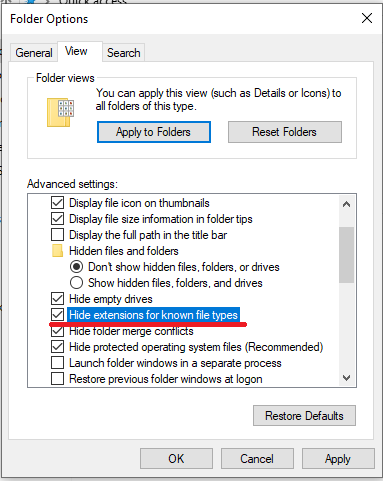
If user have seen malware file, user can have doubt for this file.

So, malware set self as a hidden file.





- file extension



There many funny malwares to scam users

Windows set hidden extensions for known file typed to unchecked initially.

Almost all Standalone virus or malware have exe extension.

Only if malware must be run, it can achieve his goal.

But if extension is exe, user can doubt it, so malware set his name "girl.jpg.exe" for example and malware's icon to image icon.

Since hidden extensions for known file typed is unchecked, File explorer display file name to "girl.jpg", it causes user's interesting.

Because of user's interesting, when user click this file to look image (in fact, this is not image. this is malware), malware run immediately. thus, malware is spread to system.

Advantage: user can see all files, so user can check files easily.

Disadvantage: Since many files is shown, there are users that dislike this configure. Only if user know well about system file, this configure has effect. But it is necessary to set "hide extensions for known file typed"

2. Monitoring CPU usage rate of Processes

- Why?

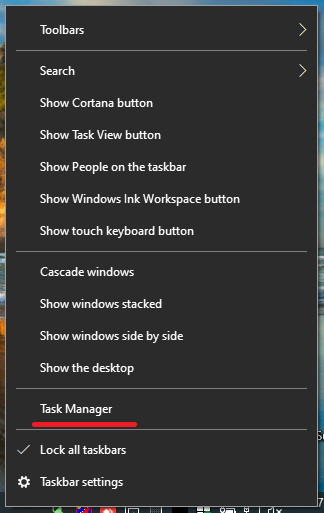
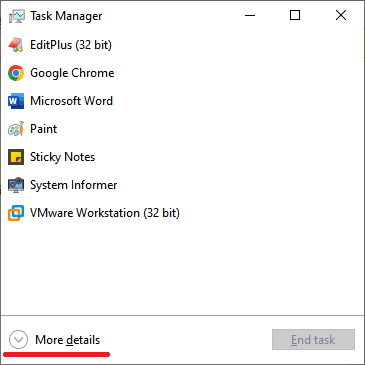
CPU is best important resource in Computer.

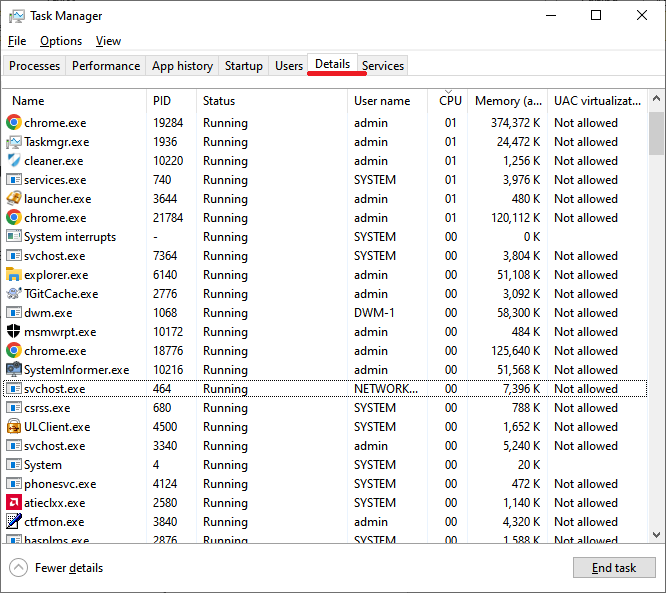
To perform any action, anyone must to use CPU.

If process's CPU usage rate is always higher than 15% , it is malware or strange action.

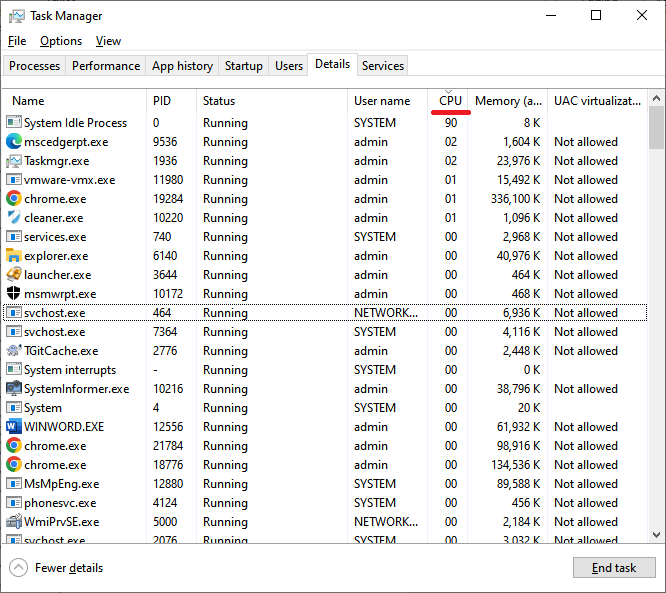
- Monitoring Method

You can monitor using Windows Task Manager’s detail. Windows task manager can be run by right clicking taskbar.



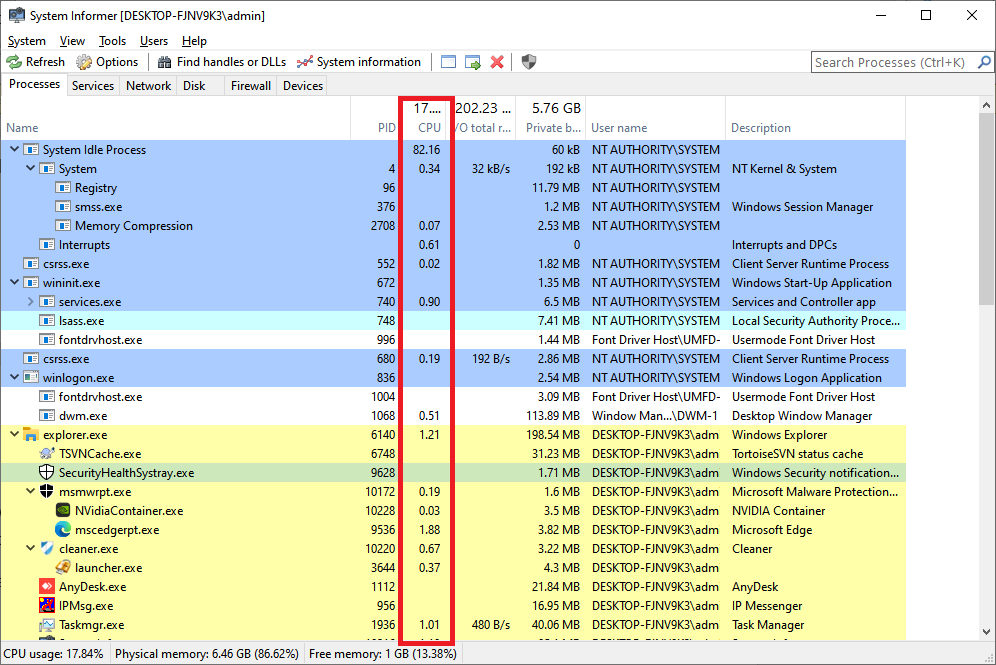
In Detail tab, you can look at the process list. If we align to the decreased CPU usage rate, you can look at the process which consumes CPU best.



In the above figure, System Idle Process has a 90% CPU usage rate. System Idle Process represents the CPU on idle.

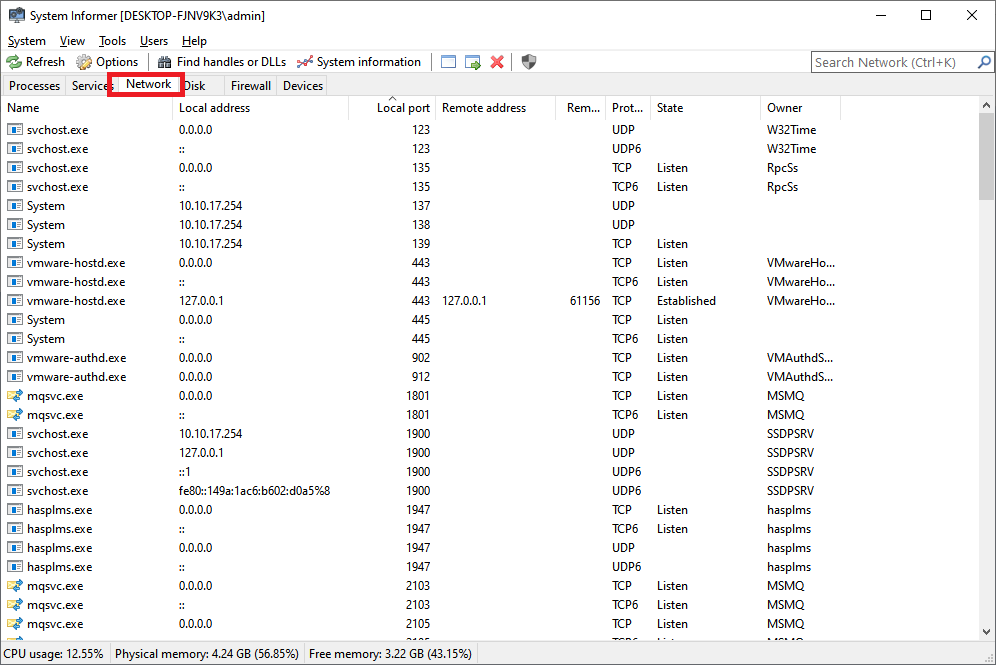
In figure, if mscedgerpt.exe always has 2% CPU usage rate, it means that mscedgerpt.exe is monitoring my computer in real-time, and if it is not my intention, this process is malware.

In order to monitor CPU usage rate of process, you can use Process Hacker



3. Monitoring Network status.

You can use Process Hacker to monitor Network status.



In this tab, you can see the network's real-time status.

Each column’s meaning is the following

Name: process name, which is connected to a network.

Local address: endpoint address on your computer. It is your ip, localhost, or 0.0.0.0

Local port: endpoint port on your computer.

Remote address: remote address which is connected with your computer

 remote port: remote port which is connected with your computer.

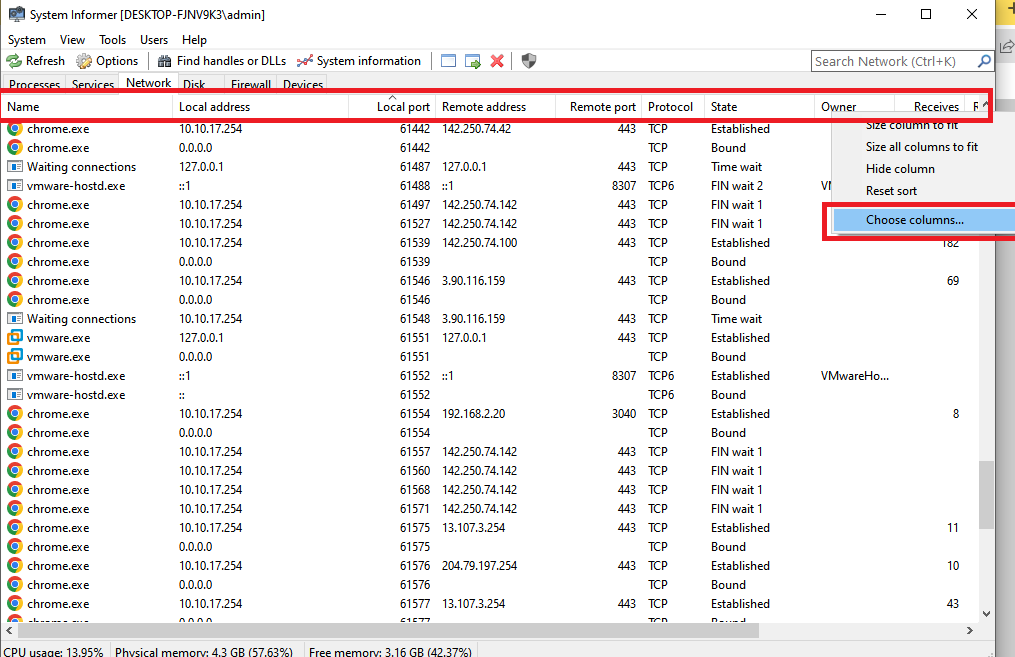
Protocol: connection protocol. TCP/TCP6 or UDP/UDP6

State: connection state.

You can add the columns for other information.

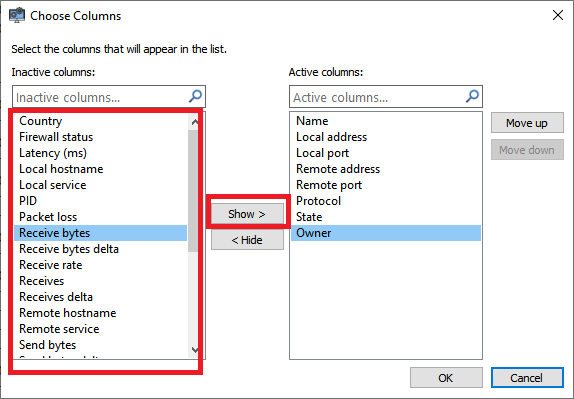
1) Right Click header.

2) Choose Columns

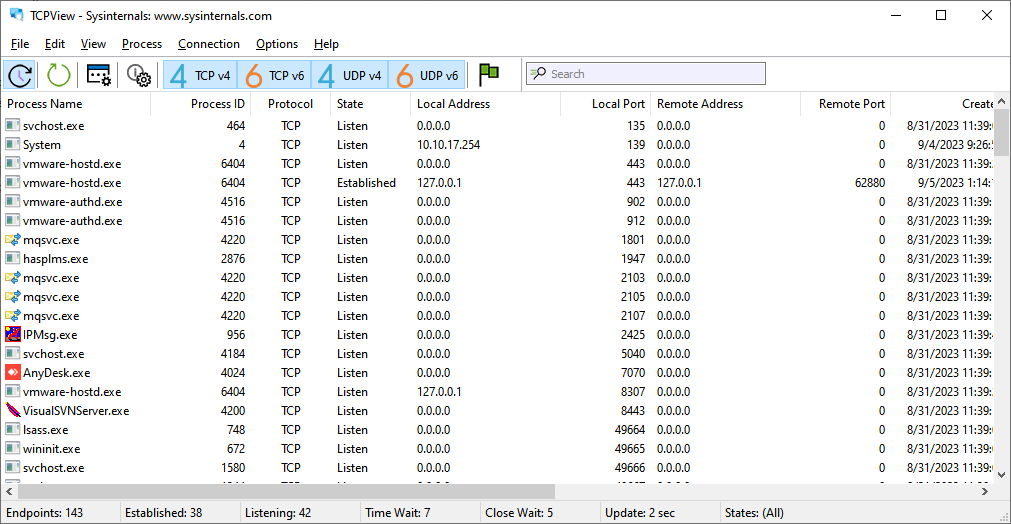


3) Select the column you need from the left list and click the Show button.

I think the column you need is Receives, Receive rate, Receive bytes, Send Bytes, Send Rate, Sends

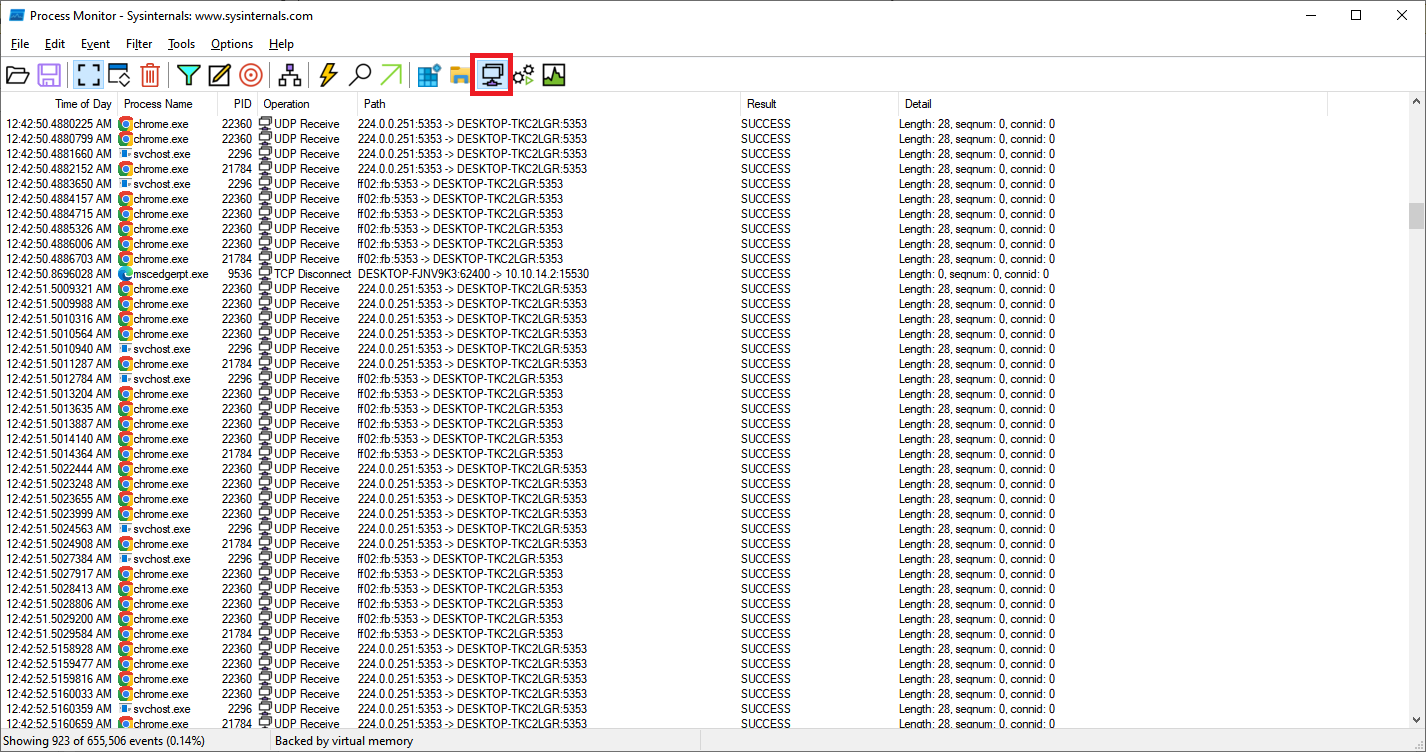


You can use the TCPView too.



The Tcpview's function is similar to Process Hacker's Network Tab, but it has more in detail.

And you can use Process Monitor’s Show Network Activity



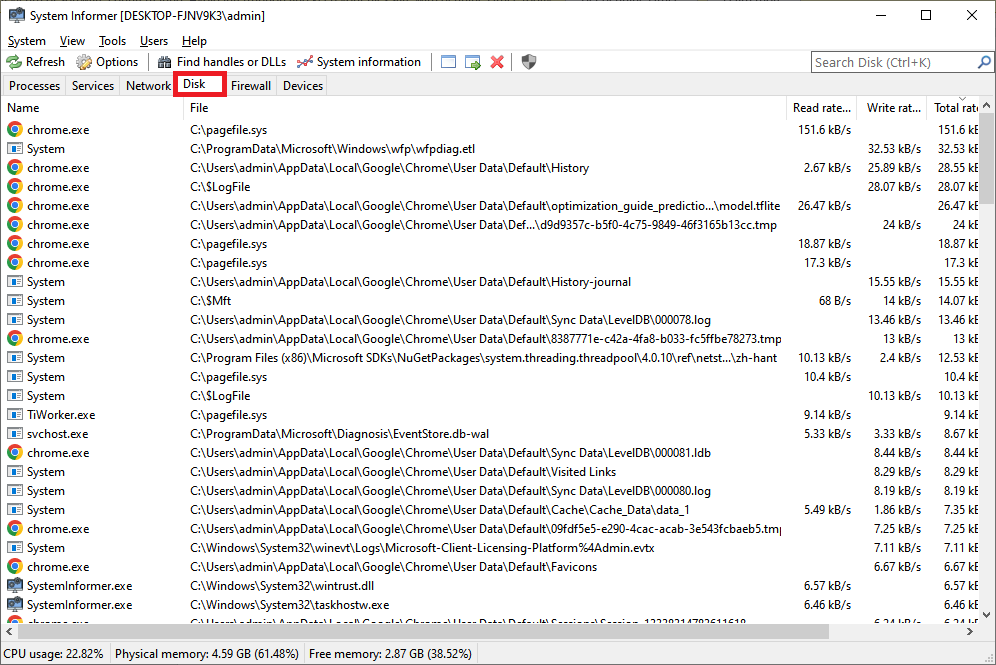
I think Process Monitor’s network monitoring function is better comfortable.

Please use tools you are comfortable with.

4. Monitoring file/directory operation.

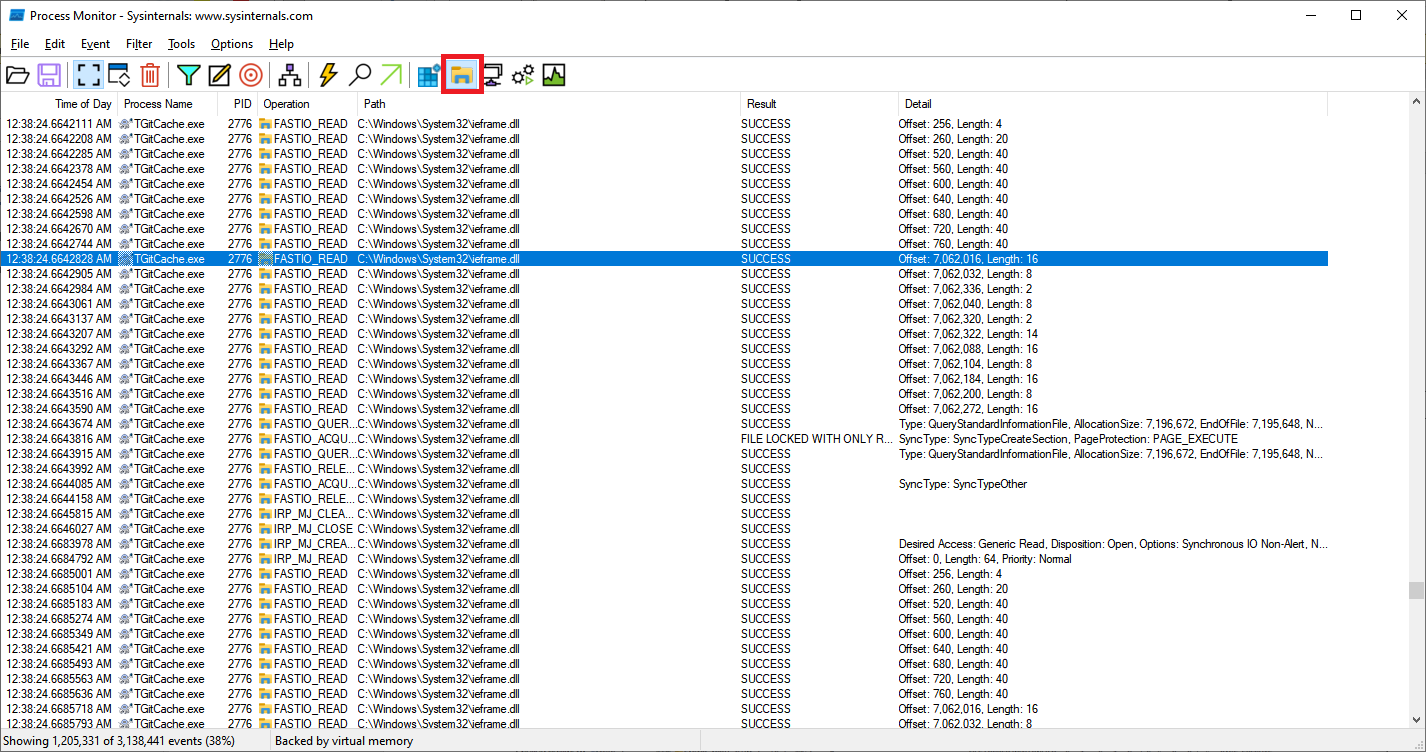
You can use the Process Hacker's Disk tab.

This tab shows file read/write operation of the process.

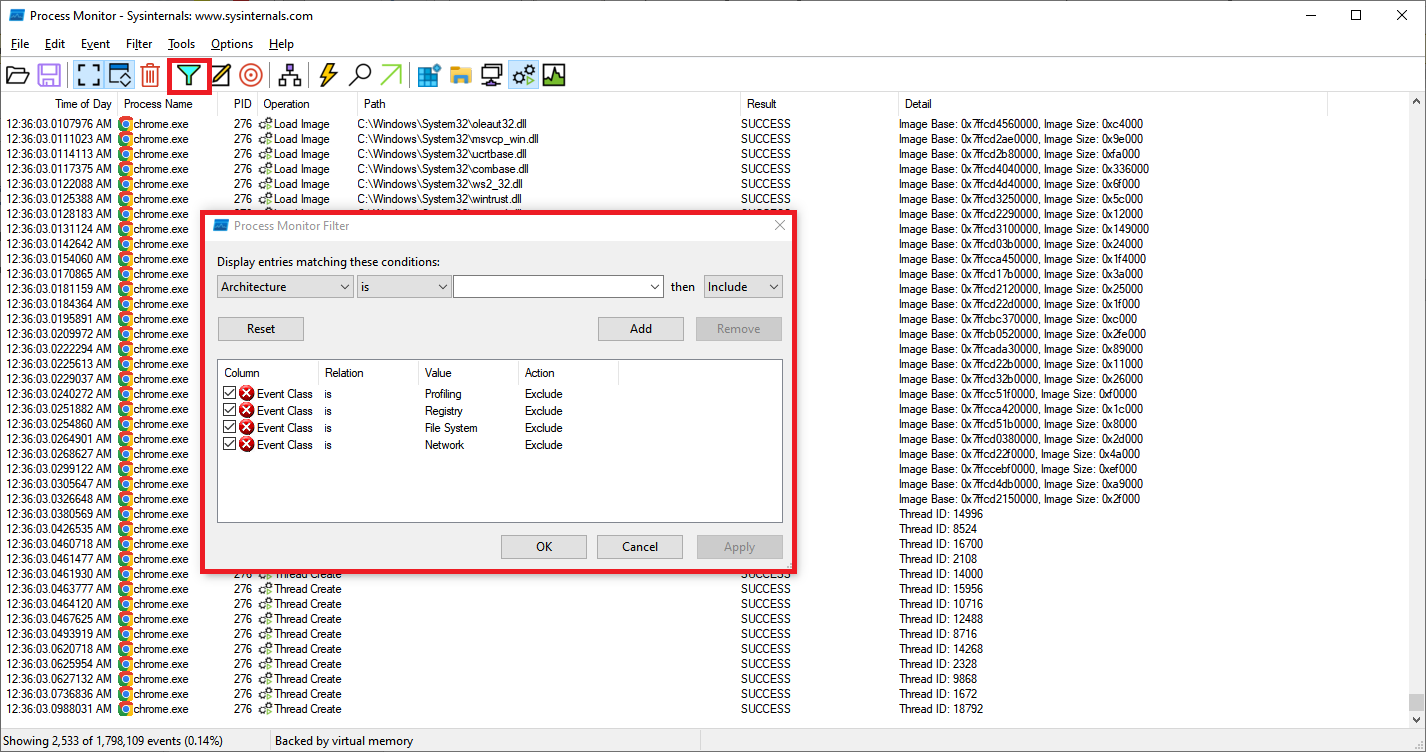


I think you can know each column's meaning.

You can also use Process Monitor’s Show File System Activity function for monitoring of file access.

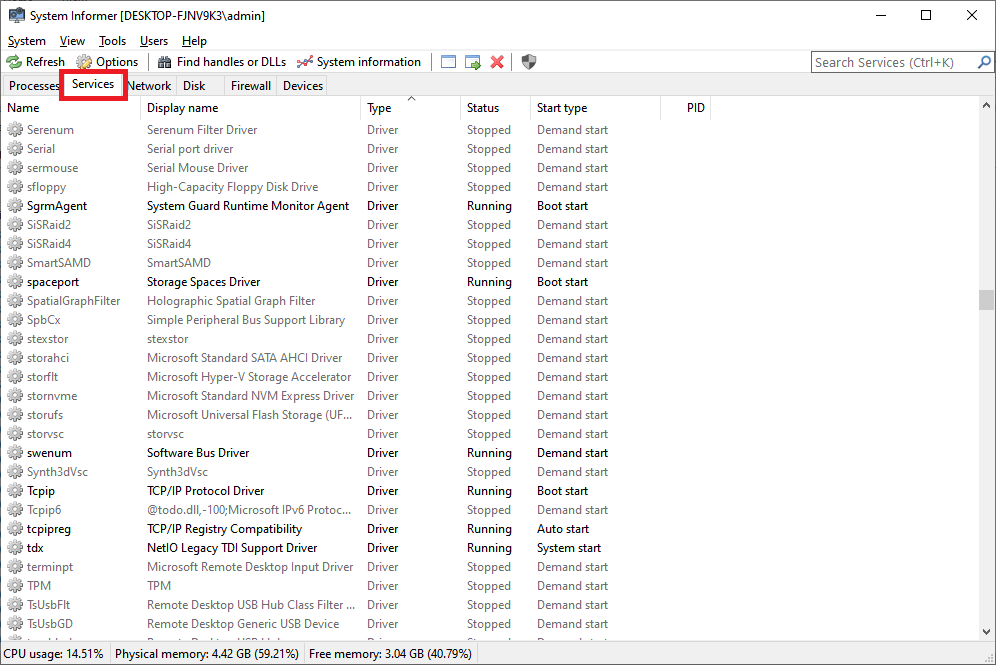


Process monitor is more specified, but because there are many logs, it can be difficult to identify logs. Please use the filter appropriately.



5. Windows Service Monitoring.

You can use Process Hacker for service monitoring.



Because there is a lot of malwares that works as Windows services, service monitoring is important.

But unfortunely, easy method to identify the malware in the service does not exist.

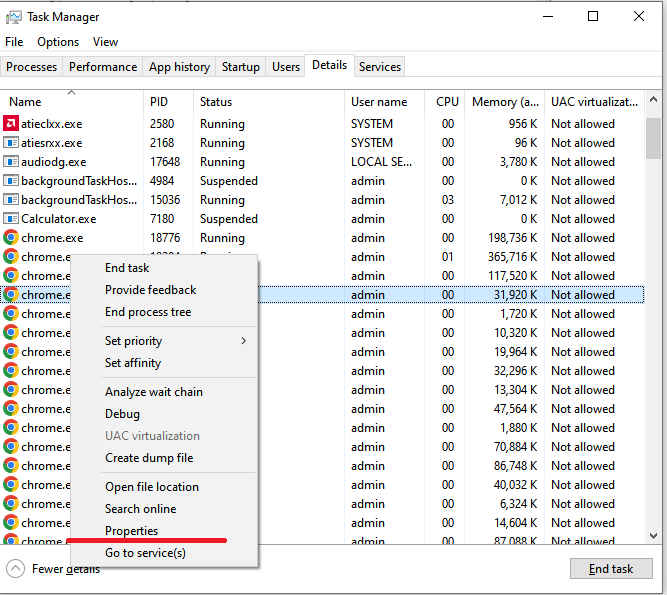
Wrong action on a service can cause a system halt.

If a Process hacker is running, when a service creates newly, a Process hacker creates a notification. It is a very comfortable function for real-time monitoring, but it doesn’t leave file log.

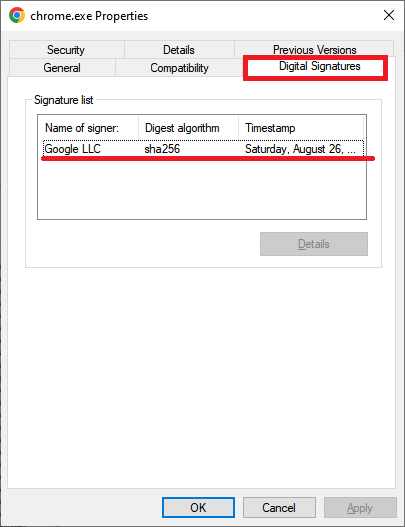
6. How to trust the process

1) Select targeted process from Process hacker or Task Manager

2) Mouse right click and select Properties



3) If a Digital Signatures tab exists, select Digital Signatures. If a tab does not exist, it can be trusted.



4) Confirm digital sign

Checking digital certification is an easy method to confirm the process. But if malware is injected into authorized processes, this method has no effect.

7. Conclusion

There are a lot of tools for monitoring. But a perfect tool that has all the functions you want does not exist.

Many tools support real-time monitoring, but don't support real-time log files​.

Process Monitor has many functions you want relatively.

Process Monitor provides exporting log files, but does not provide real-time file log.

I think you can achieve your aim by combining several tools.