

COS20030

**Malware Analysis**

*Lab 4*

**Basic** **Dynamic Analysis**

# Purpose

In this lab, we are going to perform basic dynamic analysis on keylogger malware. Dynamic analysis can provide different insight into a program compared to static analysis. You can see the actual effect a program has on different resources of a system through dynamic analysis. Hence, dynamic analysis is a high-risk task and it has to be done in an isolated environment in order to keep your system safe from infection.

# Outcome

* Learn how to use the Process Monitor utility to gain an understanding of system events and look for suspicious behaviour
* Learn how to use the Process Explorer utility to find out information about running processes and also ro terminate a process
* Use Process Monitor and Process Explorer to perform basic dynamic analysis on a keylogger malware

# Basic dynamic analysis

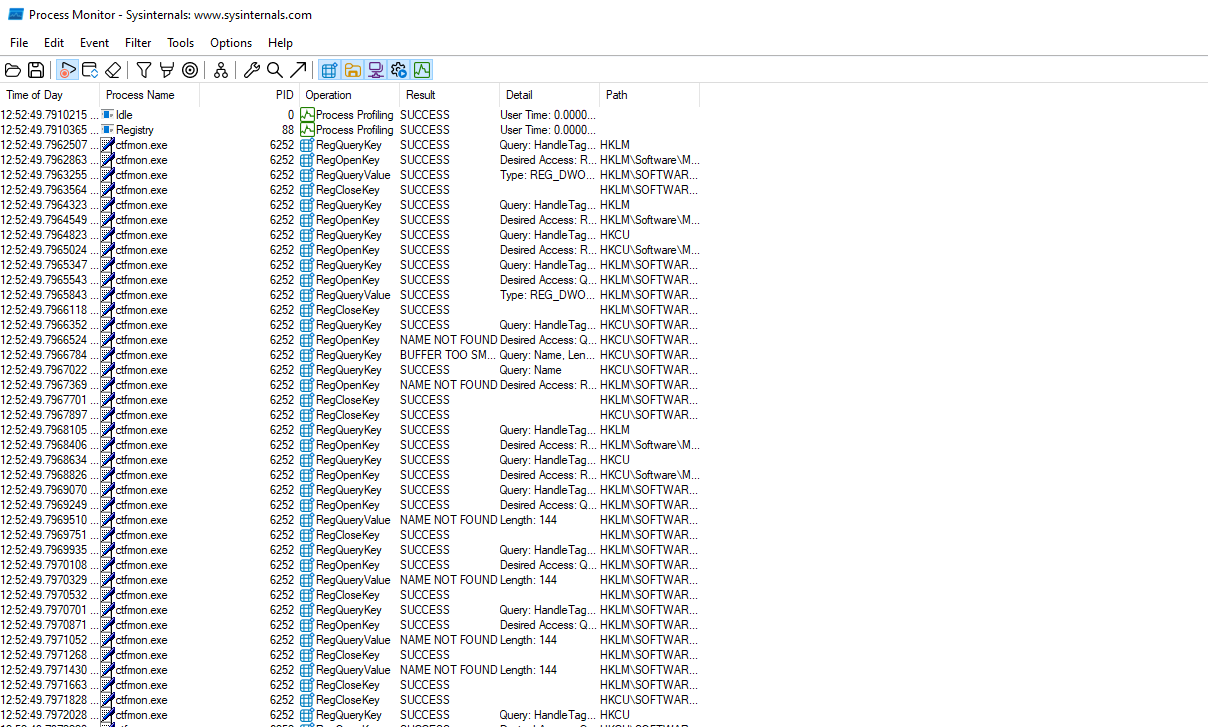
Basic dynamic analysis is more or less like a sandbox analysis with some differences that you will learn in this lab. The main idea of basic dynamic analysis is to execute the program(in this case, malware sample) and monitor events on the system, or examine details of the running process to understand the behaviour and the goal of the program. We are going to use the two most common and useful tools for basic dynamic analysis in this lab, Process Monitor and Process Explorer.

#### Process Monitor

*Purpose:* Learn how to use ProcMon.exe to investigate the behaviour of different processes running on a system.

Execute the ProcMon.exe via its desktop shortcut. “Agree” to the licence terms and click on “Yes” on the Windows User Account Control alert.

ProcMon is a utility that monitors and logs every event that is happening on your machine. Each row in the log shows details of one event. The tool can be used to observe activities related to the file system operations, process operations, registry operations and network operations. It also has a profiling capability which shows the amount of processor time and memory each process uses.( Refer to the following screenshot showing different parts of the ProcMon interface.)



Click on each button to enable/disable logging a type of activity (Highlighted means enabled)

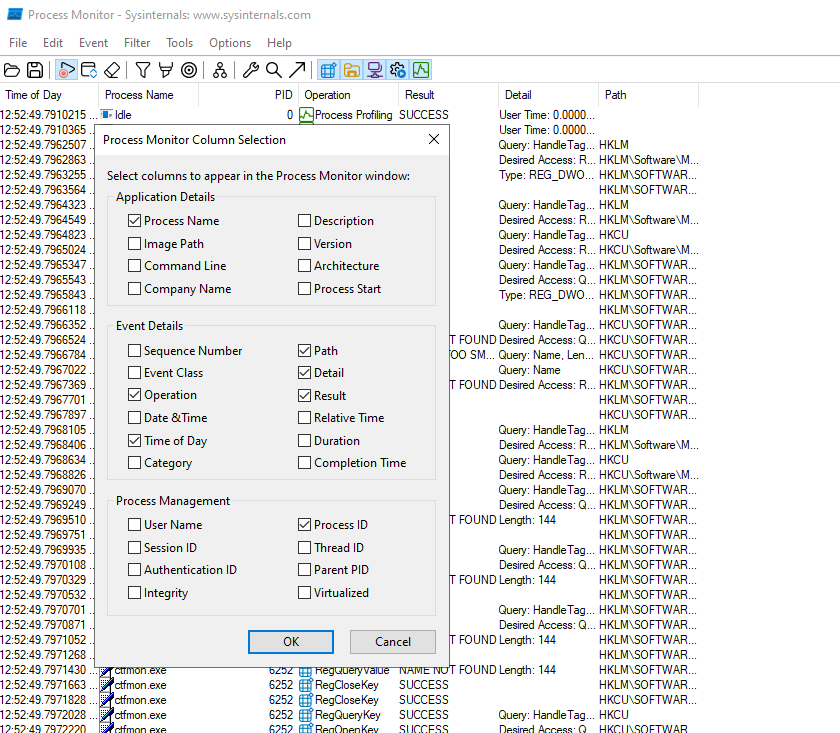
Filter button

Each row belongs to one event on the system

Each column shows one type of details related to the event

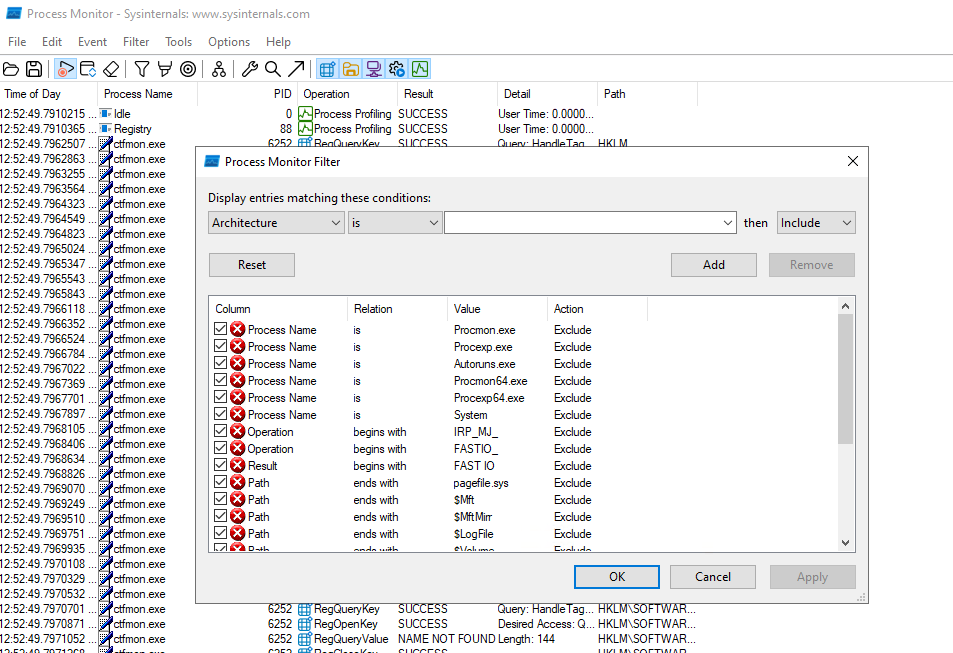
###### Customise log view

From Options -> Select Columns, you can add other columns to the main view. (See the screenshot below)



###### Create Filter

To create a filter, click on the “Filter” button (Refer to the screenshot of the main view). In the filter windows, you can create filters based on various criteria. You can also add multiple filters to the list or remove some of the previously existing filters.



List of the filters

Attribute

Comparison Operation

Attribute value

Include/Exclude

You can choose the “attribute field”, “Comparison operation”, “Attribute value”, and then choose “Include” or “Exclude”. The drop-down menu for “Attribute Field” has the exact list of the event detail type that you could add as a column to the main view. Remember that even if a column is not shown in the main window, you can create a filter based on it.

You can save the log with your filters in a file using the “Save” button for future analysis.

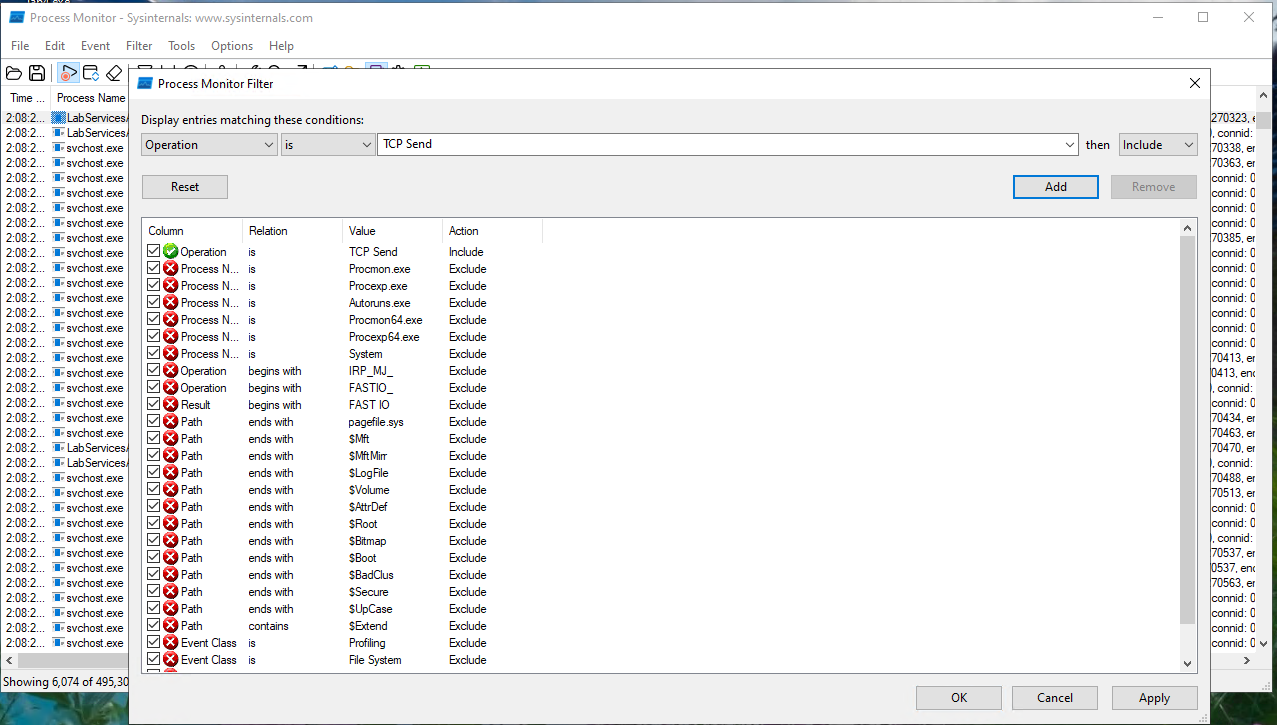
##### Exercise 1

Create filters to find IP addresses that the “LabServicesAgent.exe” process sends TCP packets to. This is a process related to the Azure Lab environment.

*Purpose:* The goal of this exercise is to learn how ProcMon can be used to find information about the network activities on a system.

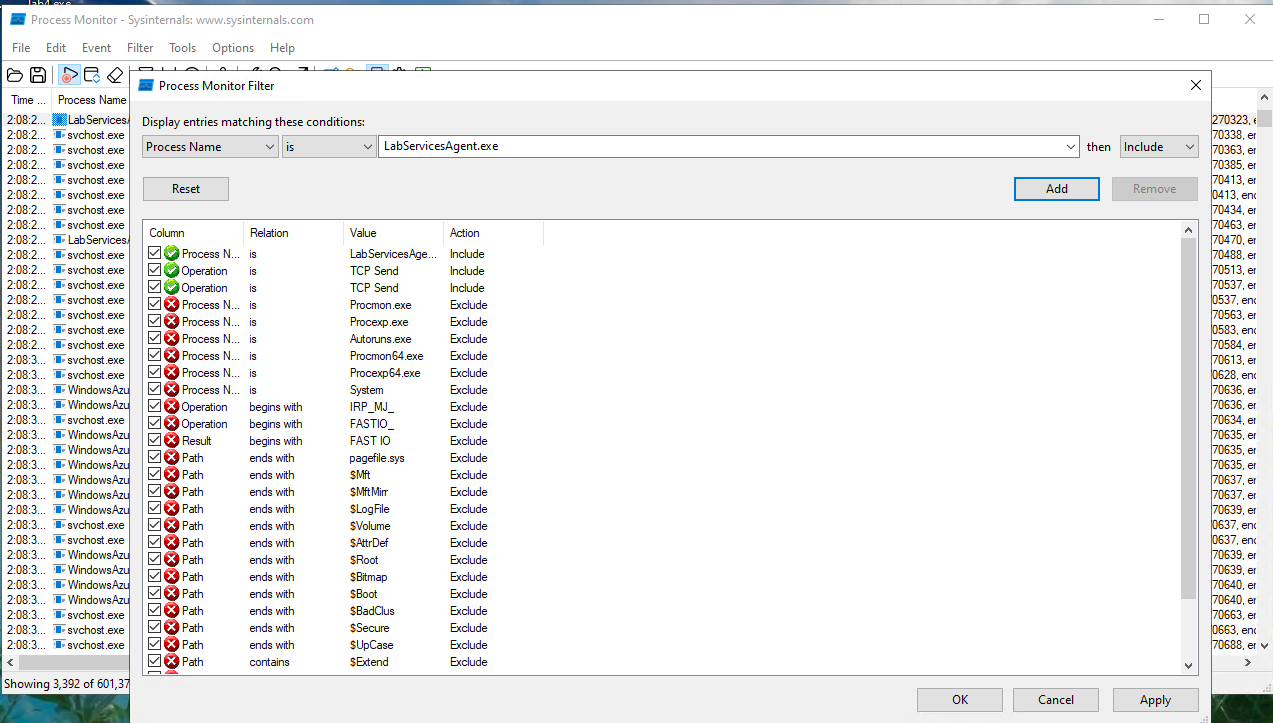
Follow the steps below to create a proper filter for our goal:

1. We need to make sure that the relevant types of events are shown in the list. Enable “Show Network Activity” using its corresponding button (Refer to the screenshot of the main view). Note that It might be enabled by default. Make sure you don’t disable it.
2. Disable showing of other types of events.
3. Click on the “Filter” button to create a filter to show all the events related to TCP Send. For the filter, choose “Operation” as the Attribute, set the Comparison Operation as “is” and the Attribute Value as “TCP Send”. Then include this filter in the list and click on “Add”, then on “Apply”, and finally on “OK”. (Refer to the screenshot below)



Now, you will see a list that shows all the events related to “TCP Send”. However, we only want to see the connections going out from the “LabServicesAgent” process

1. Add another filter on top of the TCP connection to show events that related to the TCP send events made by the LabServicesAgent process. (Refer to the screenshot below)



1. To summarise the details and find a clean list of IP addresses which this process connects to. Go to Tools -> Network Summary and find the IP addresses in the “Path” column.

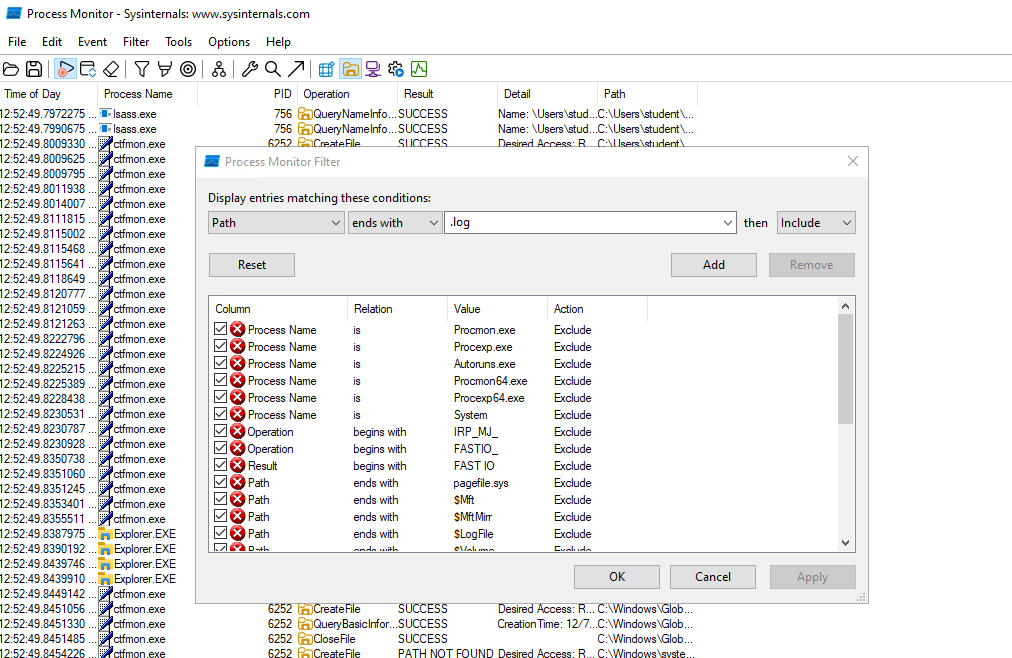
|  |  |
| --- | --- |
| Question | Answer |
| What IP addresses does this process connect to | 13.107.246.32:https  20.189.173.7:https  40.117.80.207:https |

##### Exercise 2

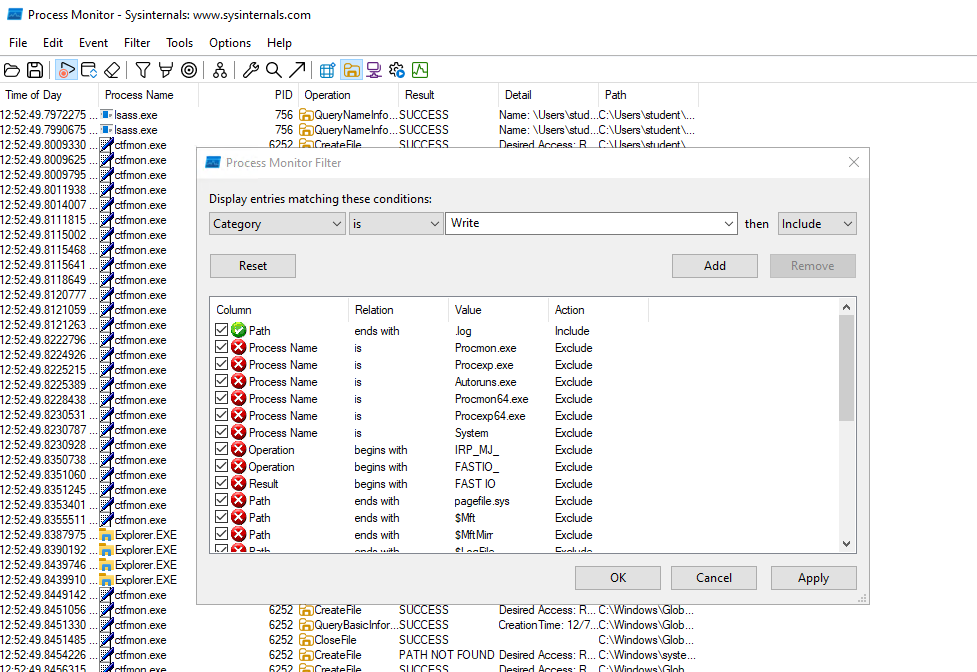
Create filters to find a list of log files with “.log” extension written on by various system processes.

*Purpose:* The goal of this exercise is to learn how ProcMon can be used to look at file system operations.

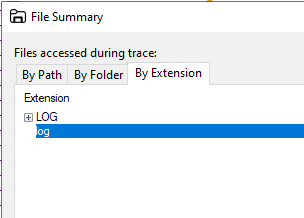
1. We need to make sure that the relevant types of events are shown in the list. Enable “Show File System Activity” using its corresponding button (Refer to the screenshot of the main view). Note that It might be enabled by default. Make sure you don’t disable it.
2. Disable showing of other types of events.
3. Click on the “Filter” button to create some filters to find what we are looking for.
4. Remove the filters you created for the previous exercise.
5. Create one filter to list all the events that have a “path” that end with “.log”. (Refer to the screenshot below)



1. Now to see writing operations to find the events related to writing on files with “.log” extension.



1. Now the list of events is quite large, however you can summarise it. To summarise the events go to Tools -> File Summary.
2. Go to the “By Extension” tab. Click on the + sign next to the log in the left hand side pane and expand the list.



Here you can see the list of all such log files. You can even click on the “Save” button to save the list of files with relevant details of the write operations.

|  |
| --- |
| List file path for all the log files found in this exercise |
| "Extension","File Time","Total Events","Opens","Closes","Reads","Writes","Read Bytes","Write Bytes","Get ACL","Set ACL","Other"  "log","3.4647891","500","0","0","0","497","0","702,473","0","0","3"  "C:\ProgramData\Microsoft\EdgeUpdate\Log\MicrosoftEdgeUpdate.log","3.0958833","69","0","0","0","69","0","106,986","0","0","0"  "C:\ProgramData\Microsoft\Network\Downloader\edb.log","0.0228705","8","0","0","0","8","0","32,768","0","0","0"  "C:\Users\student\AppData\Local\Microsoft\Edge\User Data\Default\Asset Store\assets.db\000016.log","0.0265214","4","0","0","0","4","0","8,580","0","0","0"  "C:\Users\student\AppData\Local\Temp\jusched.log","0.0001013","2","0","0","0","2","0","580","0","0","0"  "C:\WindowsAzure\Logs\TransparentInstaller.log","0.0003139","27","0","0","0","27","0","2,954","0","0","0"  "C:\WindowsAzure\Logs\WaAppAgent.log","0.0007446","51","0","0","0","51","0","5,799","0","0","0"  "C:\WindowsAzure\Logs\WaAppAgentSupplementary.log","0.0005015","30","0","0","0","30","0","11,520","0","0","0"  "C:\Windows\Logs\CBS\CBS.log","0.0038695","40","0","0","0","40","0","15,810","0","0","0"  "C:\Windows\Logs\MoSetup\UpdateAgent.log","0.0023597","178","0","0","0","178","0","48,766","0","0","0"  "C:\Windows\SoftwareDistribution\DataStore\Logs\edb.log","0.2914093","76","0","0","0","75","0","438,272","0","0","1"  "C:\Windows\SoftwareDistribution\DataStore\Logs\edb00061.log","0.0031229","1","0","0","0","0","0","0","0","0","1"  "C:\Windows\SoftwareDistribution\DataStore\Logs\edbtmp.log","0.0111907","2","0","0","0","1","0","4,096","0","0","1"  "C:\Windows\SoftwareDistribution\ReportingEvents.log","0.0059005","12","0","0","0","12","0","26,342","0","0","0" |

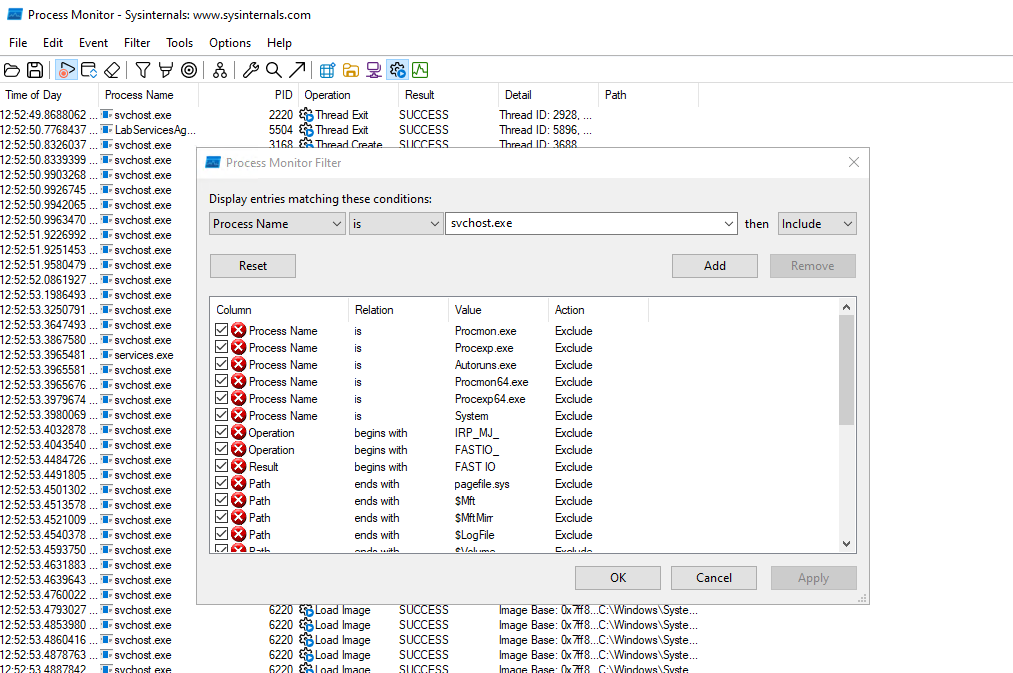
##### Exercise 3

Create filters to find a list of command line arguments from different instances of the “svchost.exe” process. Each instance of the Service Host Process(svchost.exe) is responsible for hosting one group of files, modules and processes that the operating system needs.

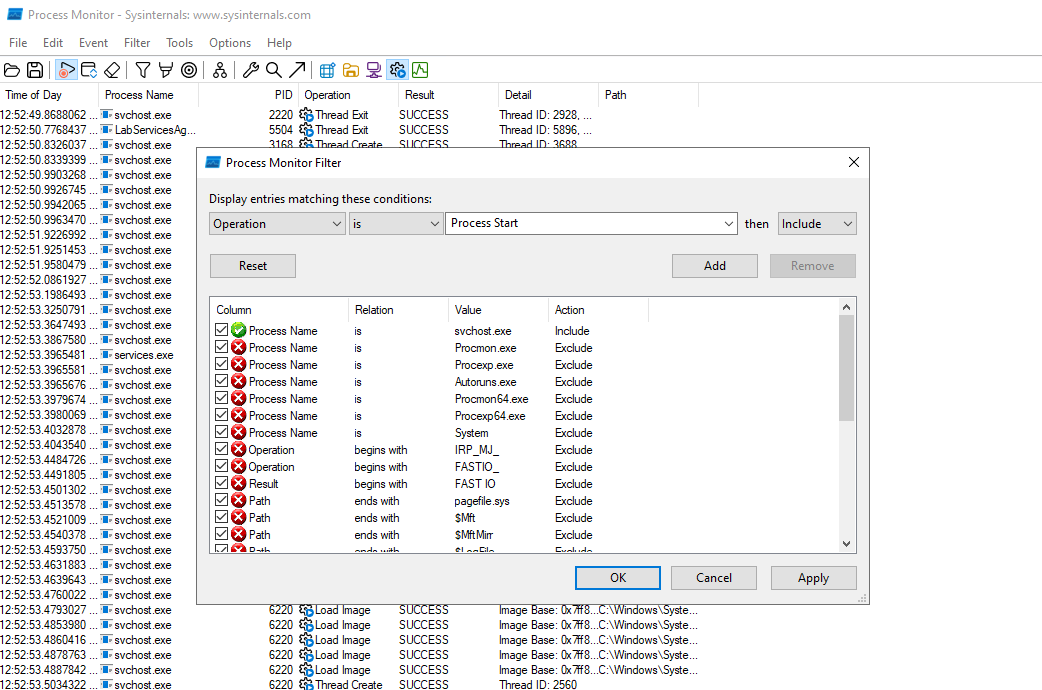
*Purpose:* The goal of this exercise is to learn how ProcMon can be used to look at Process and Thread Activity.

To do this, you need to follow these steps:

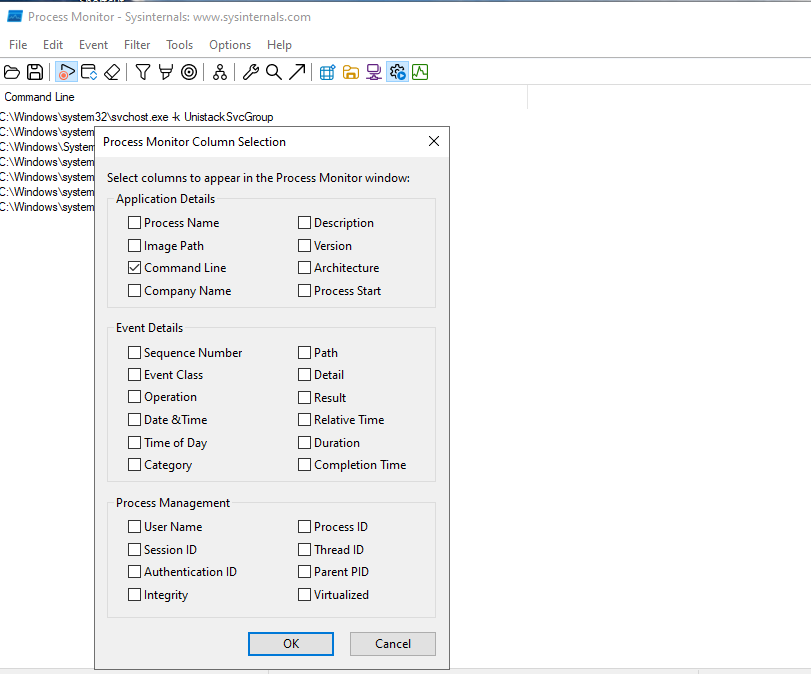
1. Only enable showing the “Process and Thread Activity” events.
2. Remove the filters you created for the previous exercise.
3. Create and add a filter to include events with the process name “svchost.exe”. (See the screenshot below)



1. Create and add a filter to include events related to “Process Starts” operations. (See the screenshot below)



1. Once the relevant events are listed, go to Options -> Select Columns and uncheck everything except “Command Line”. (See the screenshot below)



1. Now save the results in a .CSV file on your Desktop.

To further learn about using ProcMon, refer to the manual document named “procmon.chm” inside the SysinternalsSuite directory.

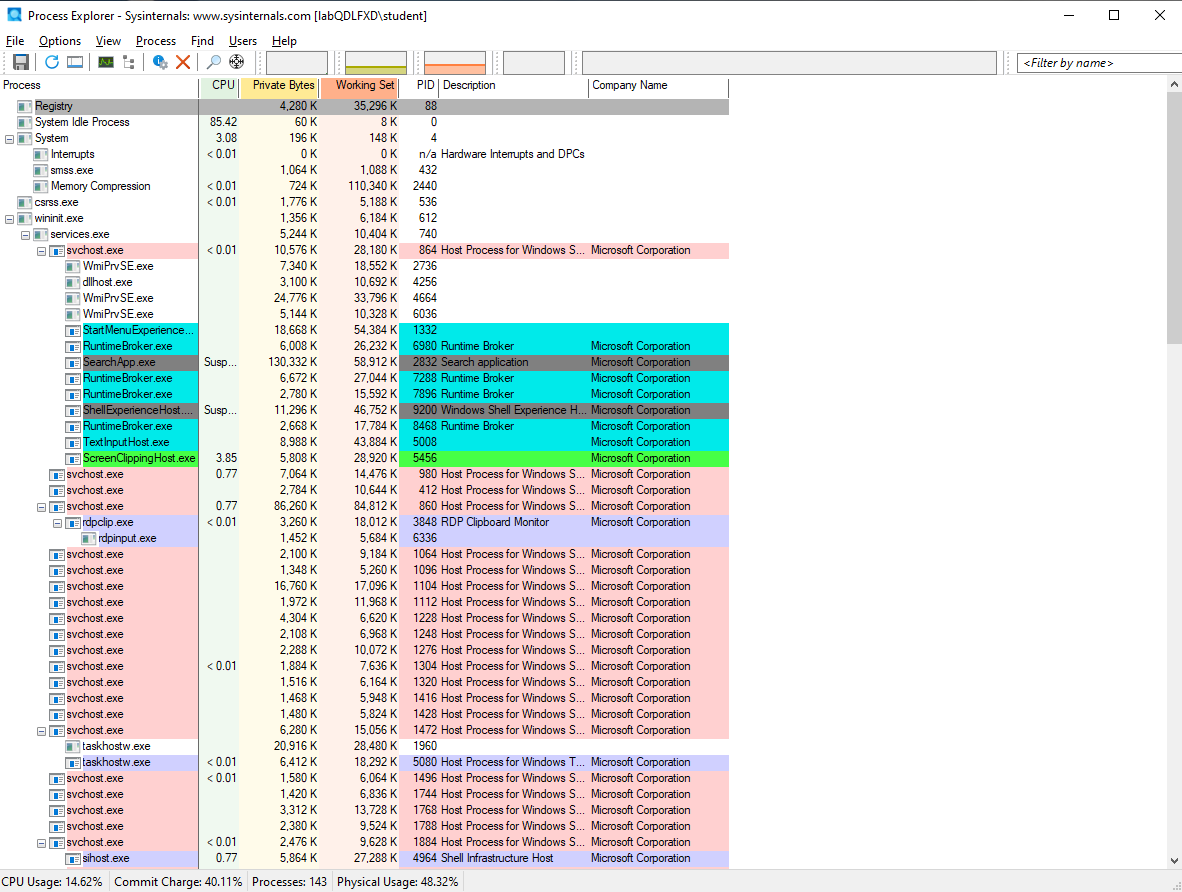
#### Process Explorer

*Purpose:* Learn how to use ProcExp.exe to investigate the details and characteristics of processes running on a system.

The next utility which is very useful when doing basic dynamic analysis is Process Explorer. This tool is also part of the Sysinternals Utility from Microsoft. Process Explorer (ProcExp.exe) shows important details about all the processes running on the machine. It is similar to Windows Task Manager but gives you a lot more capabilities. We use this tool to see details related to the malicious process when we do basic dynamic analysis.

Execute this tool via its desktop shortcut. Click on the “Agree” button to agree with the licence terms.

The main window shows all the processes. The parent-child relationship between processes is shown by the hierarchy representation, that means which process has created which process.



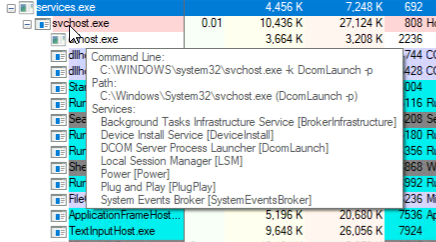
The colours used for highlighting also have specific meanings including but not limited to the security context of the process or if a process is new or suspended.

###### Customise colouring

To see the description of each colour or even customise the colours, you can go to Options -> Configure Color.

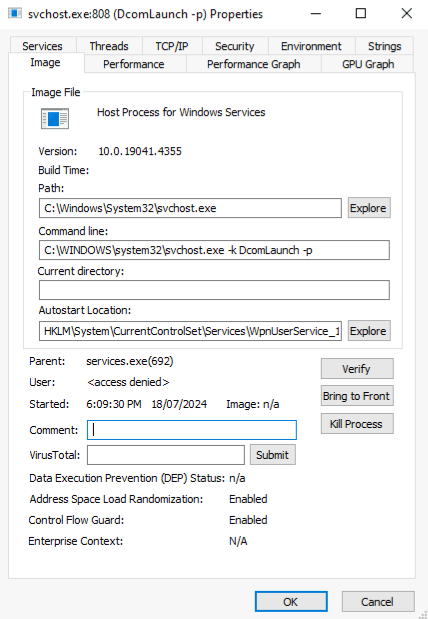
###### See process details

Hovering on the name of each process shows various details about the process. Screenshot below shows an example of hovering on a process.



By double-clicking on each process name, you can see the Properties of that process. The Properties show various types of details from basic details such as the path, command line, directory of the image file, and parent process to more advanced details such as details of the process threads and each thread's stack. It can also list all the strings found in the memory of the process and strings found in the process’s image file. (Refer to the example screenshot below for an instance of the svchost.exe process)

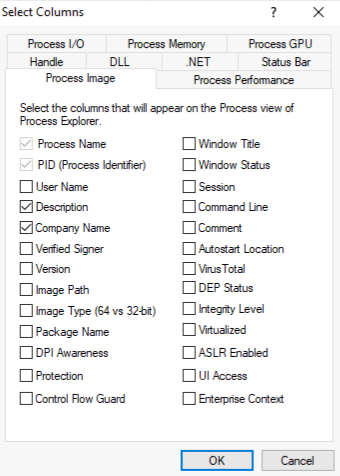
Clicking on each tab at the top of this window, shows corresponding details.



Try checking on several processes to understand what type of information you can get from this view.

###### Customise details shown for each process

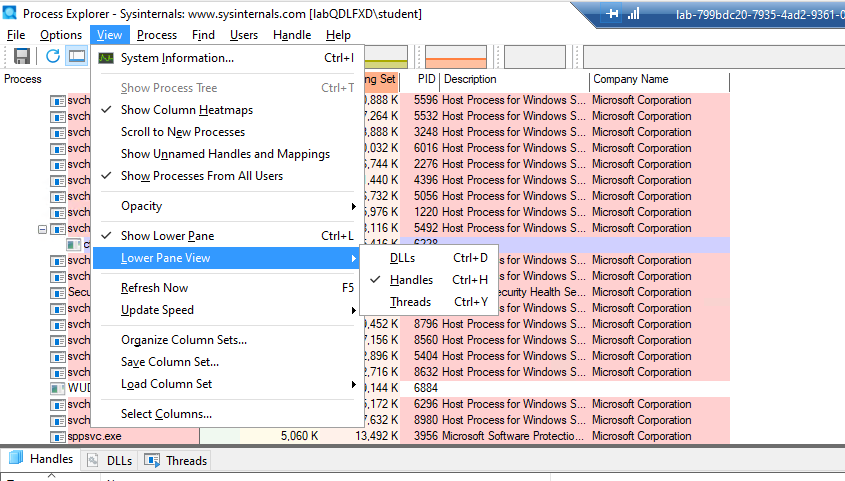
Process Explorer also gives you the ability to choose the columns shown in the main window by going to View -> Select Columns. You can see that there are different types of parameters categorised in groups shown as separate tabs. You can choose any column that is relevant to the goal you want to achieve.



###### Add lower pane to see extra details

You can also add another view to the main window to see the handles each process possesses, or the modules loaded inside the memory space of each process.

To do that, go to View and click to put a check mark next to “Show Lower Pane” to add this view to the main window. Then to choose the details you want to see in the lower pane, go to View -> Lower Pane View and choose which details to show in the lower pane.



To further learn about using ProcExp, refer to the manual document named “procexp.chm” inside the SysinternalsSuite directory.

##### Exercise 4: Keylogger - Basic dynamic analysis

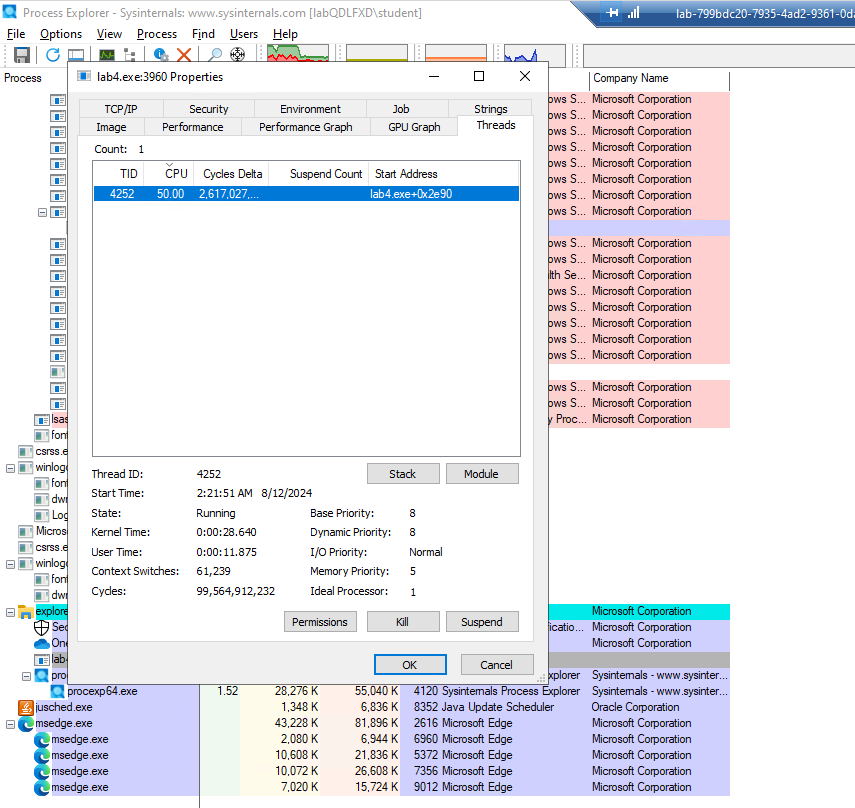
*Purpose:* Now that we learned how to use the two most useful tools to monitor the behaviour of the system and its processes. We want to examine behaviour of a Keylogger malware to practise basic dynamic analysis.

First of all, we need to execute the program in order to monitor and investigate its behaviour. Follow the steps below:

1. Extract lab4.zip with the password “infected”.
2. Copy the “lab4.exe\_” on your desktop and change the extension to “.exe”.
3. Double-click on the file to execute it.

This file is a copy of the keylogger malware we analysed in Lab3. From the previous lab, we know that the keylogger malware captures all the keystrokes and logs them in a log file.

1. Press a few keys from your keyboard and also the mouse buttons, for the keylogger to capture them. You should see the “log.txt” file created on the desktop. You can open the file and see the logged keystrokes to confirm that the keylogger is working correctly.
2. Execute Process Explorer (ProcExp.exe)
3. From the list of processes, confirm that the keylogger process is running.
4. Double-click on the process name and go to the Threads view. Check the Stack for the thread with a high CPU value and note the stack details below.(Refer to the screenshot below)



|  |
| --- |
| Copy the Stack details |
| USER32.dll!CallWindowProcW+0x813  win32u.dll!NtUserGetAsyncKeyState+0x14  USER32.dll!GetAsyncKeyState+0xbd  lab4.exe+0x12eb  lab4.exe+0x2e20  KERNEL32.DLL!BaseThreadInitThunk+0x14  ntdll.dll!RtlUserThreadStart+0x21 |

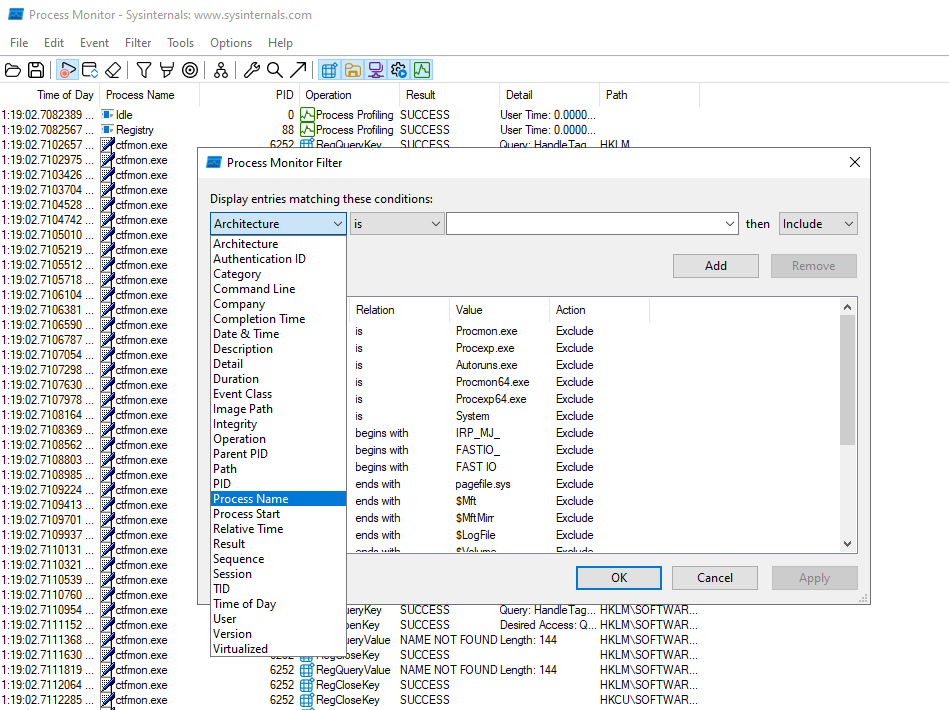
1. Go to the Strings Tab and use “Find” to look for “log.txt” strings in the Image and also in Memory.

You can also save all the strings in a text file to investigate later. However, we have already investigated the strings in this program in lab3.

1. Add Lower Pane with Handles view and write down the “File” handles the keylogger possesses.

|  |
| --- |
| File Handles |
| C:\Users\student\Desktop |

1. Execute Process Monitor(ProcMon.exe” to try and find more information about this process.
2. To start with, make sure you change the column views and the filters to the initial state.
3. Enable showing Registry, File system, Network and Process events by pressing all their buttons. Make sure all of them are in highlighted mode.
4. Before proceeding with creating relevant filters, make sure to remove the filters you created for the previous exercise.
5. We need to create a filter to only show the behaviour of the malware sample. The process name for a program is similar to its module’s file name. To do so, create and add a relevant filter for “Process Name”.



By creating the right filter, you should see a few events happening in the same sequence over and over. These events show the logging of the captured keystrokes in the log file. Write down the sequence of Operation values below.

|  |
| --- |
| Keylogger processes results in the following Operations |
| Create file, QueryStandardInformationFile, QueryStandardInformationFile, WriteFile, CloseFile |

1. Now your job is done with the analysis and you have to clean the machine. To terminate the keylogger process, right-click on the process name on ProcExp and choose Kill Process.
2. Delete the log file from Desktop.

*End of Lab*