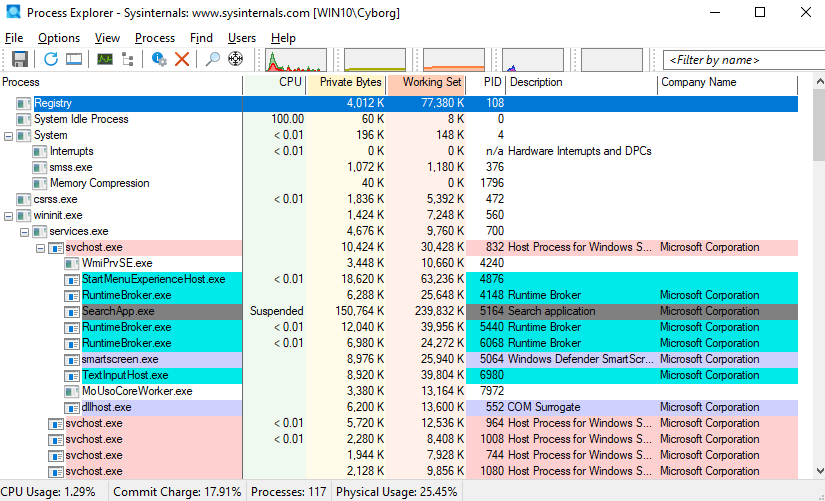
**LAB – 2**

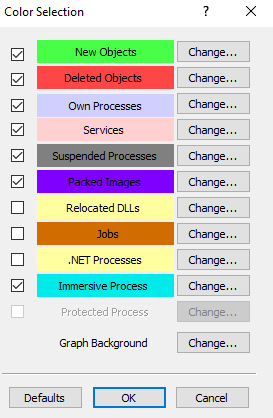
**AIM: - To explore the system processes and understand them using process explorer.**

Software Required: - Process Explorer

Theory:-

The Windows Sysinternals tools were created by Mark Russinovich and Bryce Cogswell. They were initially conceived and developed to help administrators and developers in their activity, but over the years’ multiple capabilities have been added and tools have been created to aid malware analysts in finding malicious behavior. The Sysinternals suite contains more than 70 tools, in this malware series we’ll be taking a look at three in particular: Process Explorer, Procmon and Autoruns.

**Process explorer** is a tool that let us access a lot of information about processes running on a machine, and offer some nice functionalities out of the box which we can leverage to analyze and determine if something is malicious.



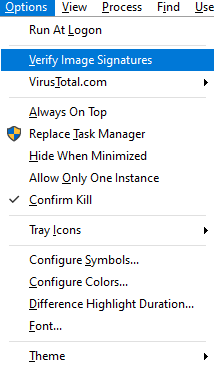
1. **Understanding All Those Colors -**

Each process will get assigned a certain color based on its type and state. We can use these colors to determine for example: “services” or “packed images”.

The default configuration has the following color scheme.

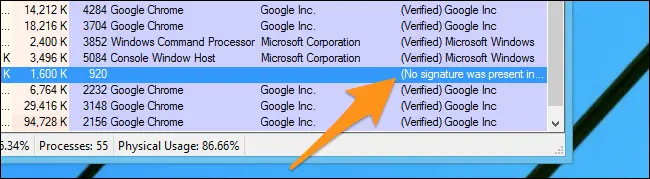
For example, if we see a process with the “Services” or “Packed Images” color and its doesn’t contain any description or company name, then this could very well be indicative of something suspicious.

1. **Verifying Application Identity –**

One really useful option that we’re surprised isn’t enabled by default is found at

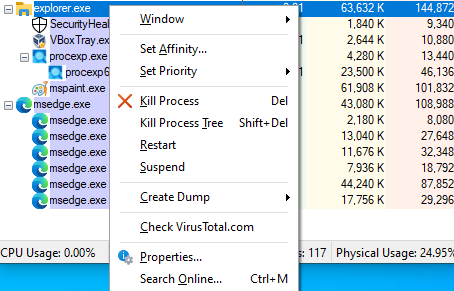
**Options -> Verify Image Signatures**.

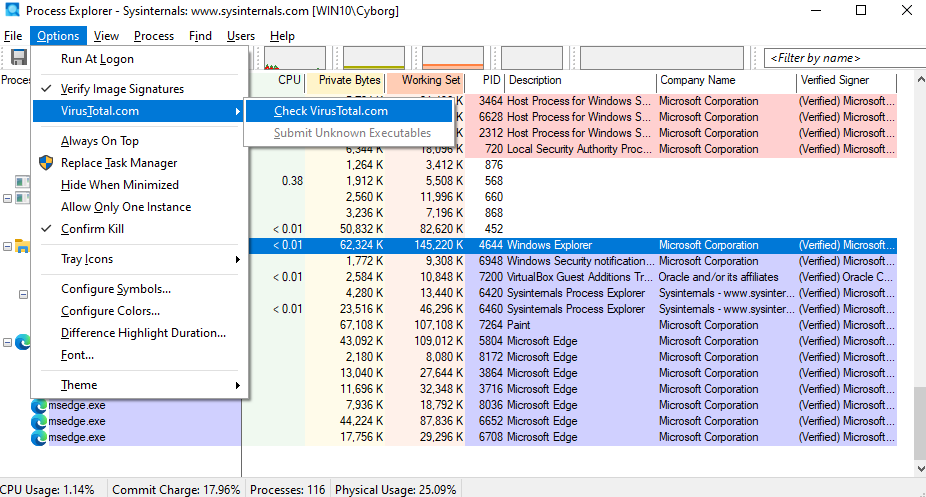
This option will check the digital signature for each executable file in the list, which is an invaluable troubleshooting tool when you are looking at some suspicious application that is running in the list.



1. **Taking Action on a Process -**

You can quickly take action on any process by right-clicking on it and choosing from one of the options, or by using the shortcut keys if you prefer. Those options include:



1. **Virus Total –**

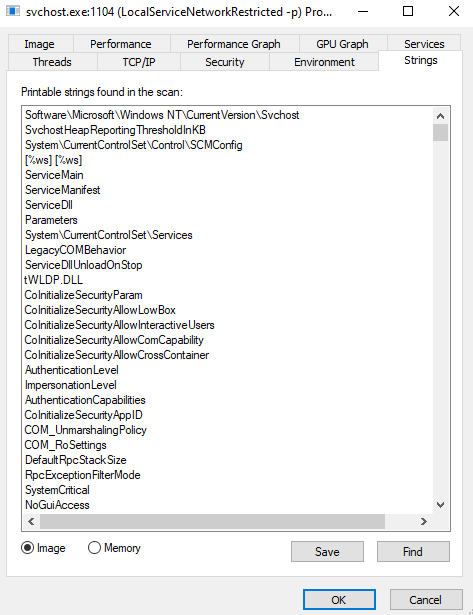
Process explorer also integrates by default with Virus Total so it can send the hashes of the executables and DLL’s to check if they’re already flagged by AV engines.

If the machine we’re analyzing has access to the internet I highly suggest to turn on this feature, as it can be of great help during analysis.

This feature can also be enabled via the “Options” menu.

1. **Strings –**

Analyzing the strings of an executable has always been a powerful technique during static analysis, as they contain most of the times interesting indicators.



1. **Handles, DLLs & Threads –**

Click on **View > select Show Lower Pane > Handles, DLLs , Threads**

