Sri Lanka Institute of Information Technology
Introduction to Cyber Security - IE2022
Lab Sheet 10
Year 2, Semester 1

Malware Introductory

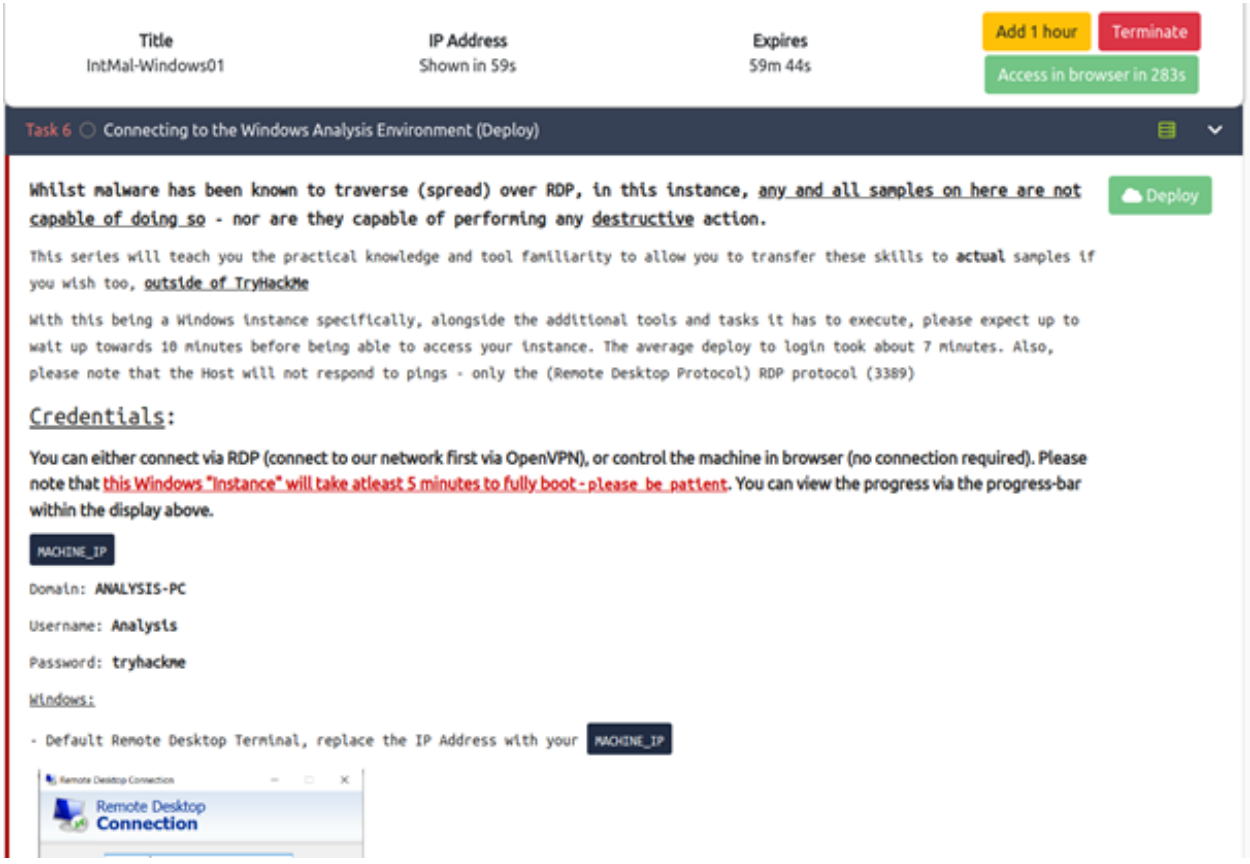
Lab Access Link : [Malware Analysis]

Task 01 - Task 05 : Theory Part of Malware Analysis you have to answer questions in Task 02 and Task 03.

Practical (Practical Session Start in Task 06)

Task 06 : Connecting to the Windows Analysis Environment

- Start Machine and wait for the Machine IP address



Sri Lanka Institute of Information Technology
Introduction to Cyber Security - IE2022
Lab Sheet 10
Year 2, Semester 1

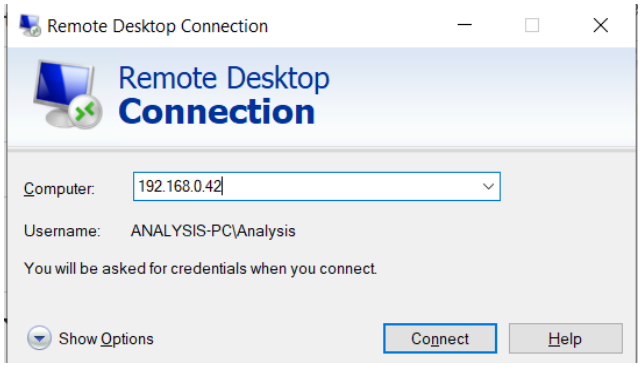
- Get the remmina and RDP

Username: Analysis

Password: Tryhackme123!

Windows:

- Default Remote Desktop Terminal, replace the IP Address with your MACHINE_IP

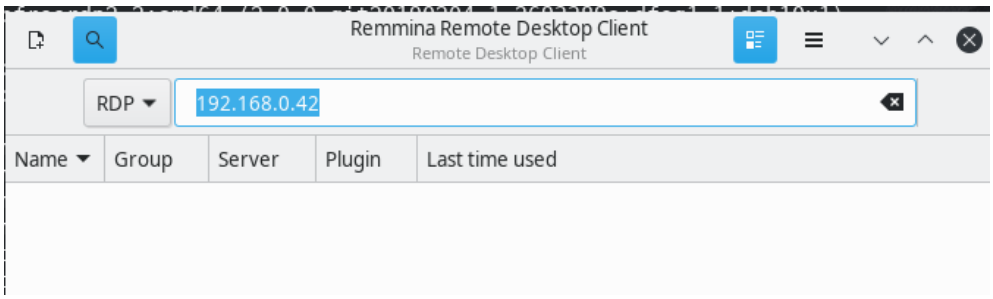


Linux:

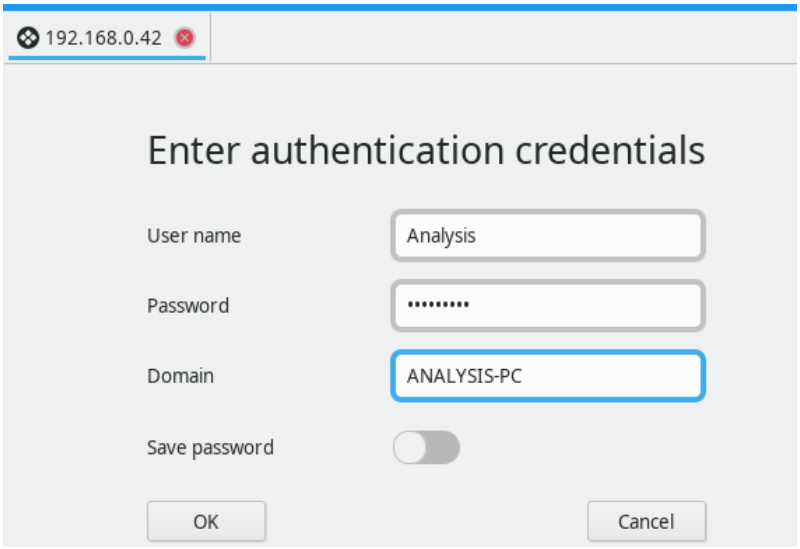
Any compatible RDP client such as Remmina:

sudo apt-get install remmina

Again, replacing the IP address with your MACHINE_IP



Sri Lanka Institute of Information Technology
Introduction to Cyber Security - IE2022
Lab Sheet 10
Year 2, Semester 1



Task 07 : Obtaining MD5 Checksums of Provided Files

- Navigate to the "Tasks" Folder on the Desktop, and then enter the "Task 7" Directory, where there will be three files:

- aws.exe

- NetLog.exe

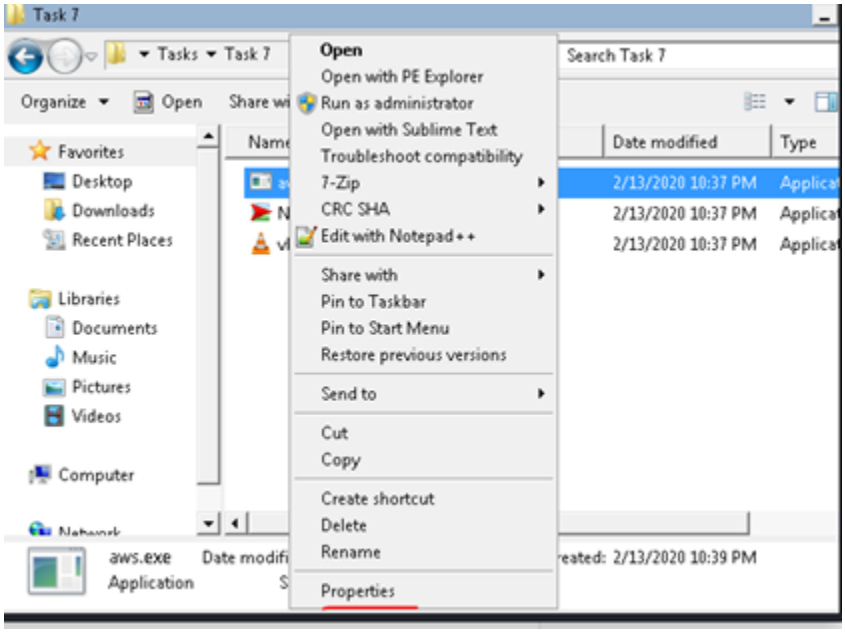
- vlc.exe

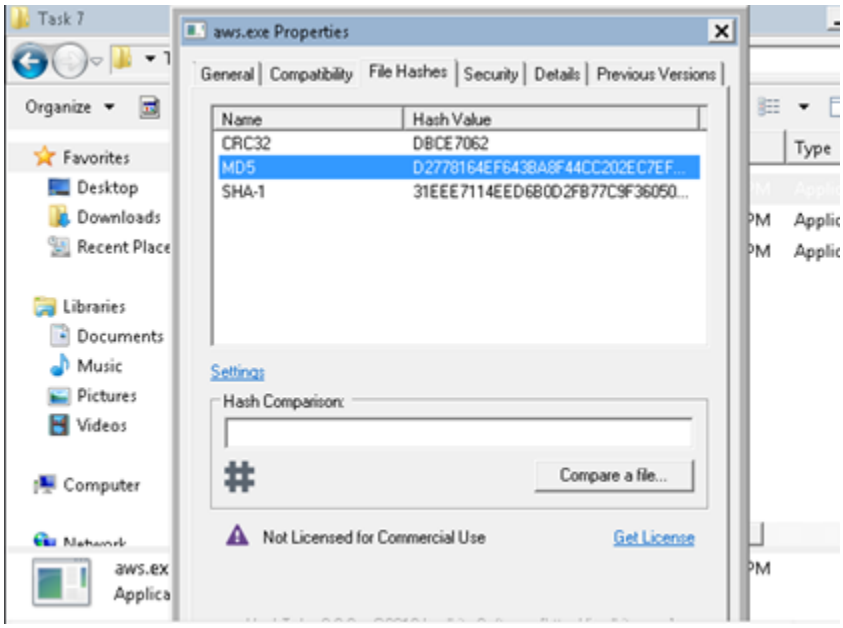
These are common names of executables, but anyone can name an executable as whatever they like! Just because it says "vlc" doesn't mean it is indeed the VLC application! This is where identifying their MD5 Checksum is useful, as no matter the name - their MD5 reveals its true identity.

You have to install the "HashTab" application, which calculates a file's MD5 sum - amongst others, directly within Windows Explorer as if you were inspecting its properties.

- Go to the "aws.exe" and right click go to the Properties > File Hashes

Sri Lanka Institute of Information Technology
Introduction to Cyber Security - IE2022
Lab Sheet 10
Year 2, Semester 1



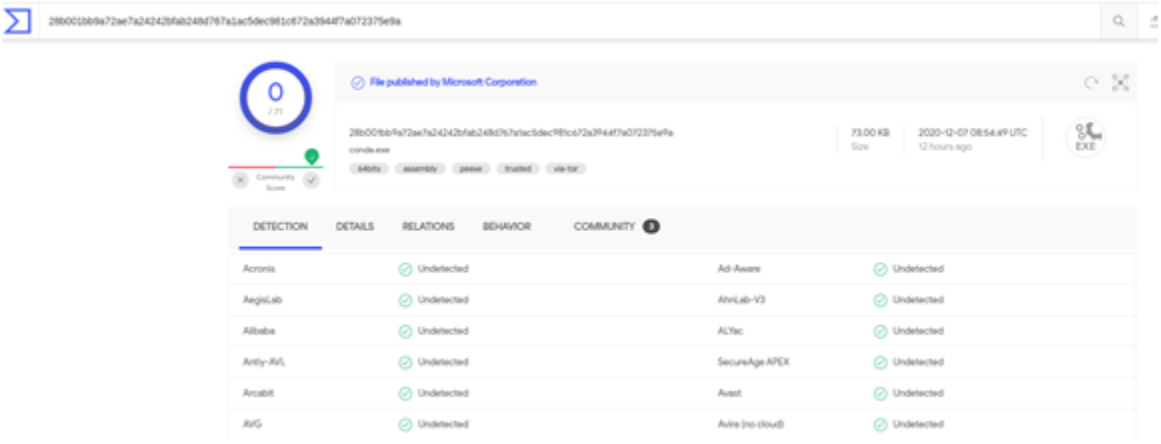


- Same steps used for other two files in "Task 7" to Identify the MD5 Checksums.

Sri Lanka Institute of Information Technology
Introduction to Cyber Security - IE2022
Lab Sheet 10
Year 2, Semester 1

Task 08 : Now lets see if the MD5 Checksums have been analysed before

- Outside of the Remote Windows Environment i.e. Kali or your Windows PC, look up those MD5 "Checksums" on VirusTotal to solve this task.
- Put three hashes that u found in Task 07 to VirusTotal and see if they are harmful or harmless



Task 09 : Identifying if the Executables are obfuscated / packed

There are a few provided tools on this Windows instance that are capable of identifying the compiler / packer of a file. However, PeID has a huge database and is a great tool for this.

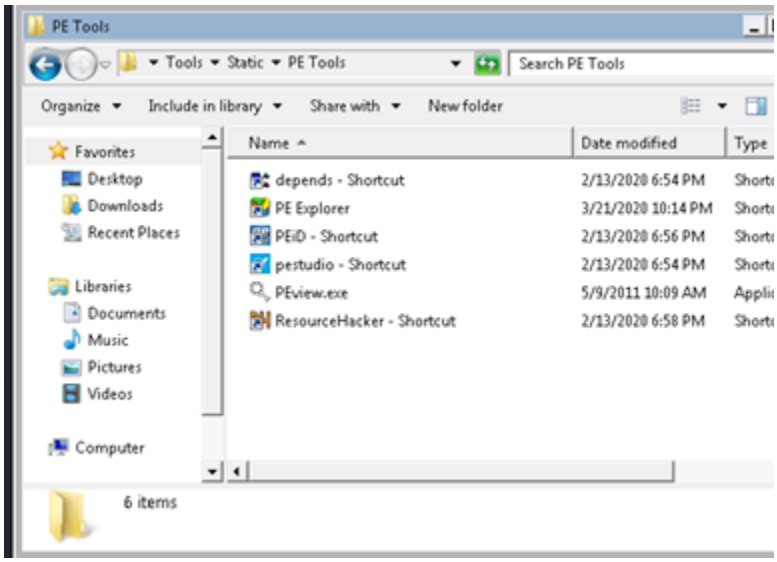
Moreover, just because a file doesn't have the ".exe" extension, doesn't mean it isn't an actual executable! For instance, it can have the ".jpg" extension and still be an executable piece of code. This is a tad-bit out of scope for this room specifically, but essentially, files have identifying attributes within its hex - known as file headers.

E.g. The hex value for an executable is always "4D 5A". So if a file with a ".jpg" file has the hex header of "4D 5A", then it is obviously not a jpg file. You can read more into file headers / trailers here, which are great resources for data carving in file forensics / recovery.

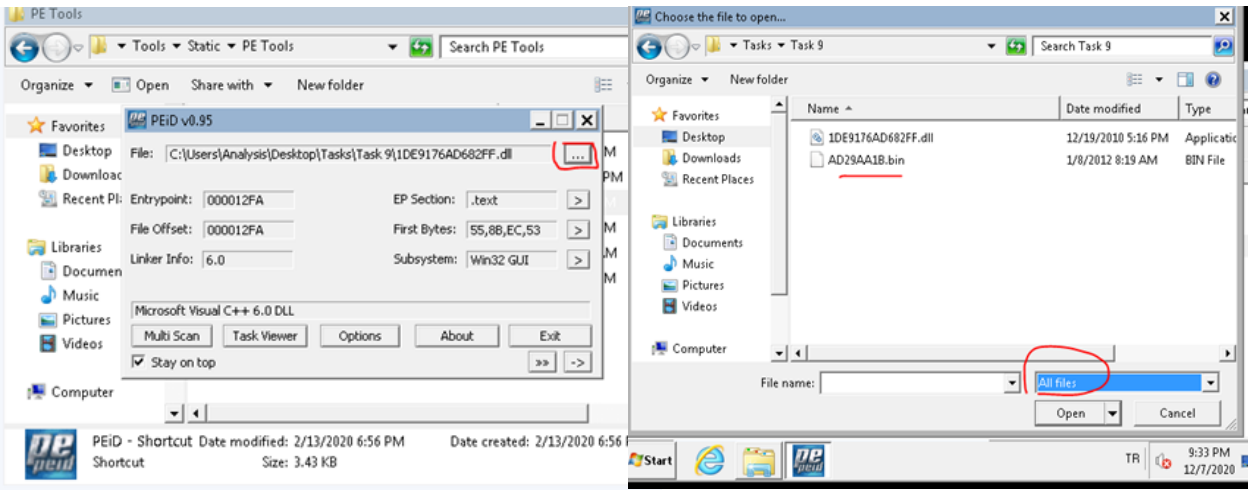
Sri Lanka Institute of Information Technology
Introduction to Cyber Security - IE2022
Lab Sheet 10
Year 2, Semester 1

Provided Tools: PeID

C:\Users\Analysis\Desktop\Tools\Static\PE Tools\PeID



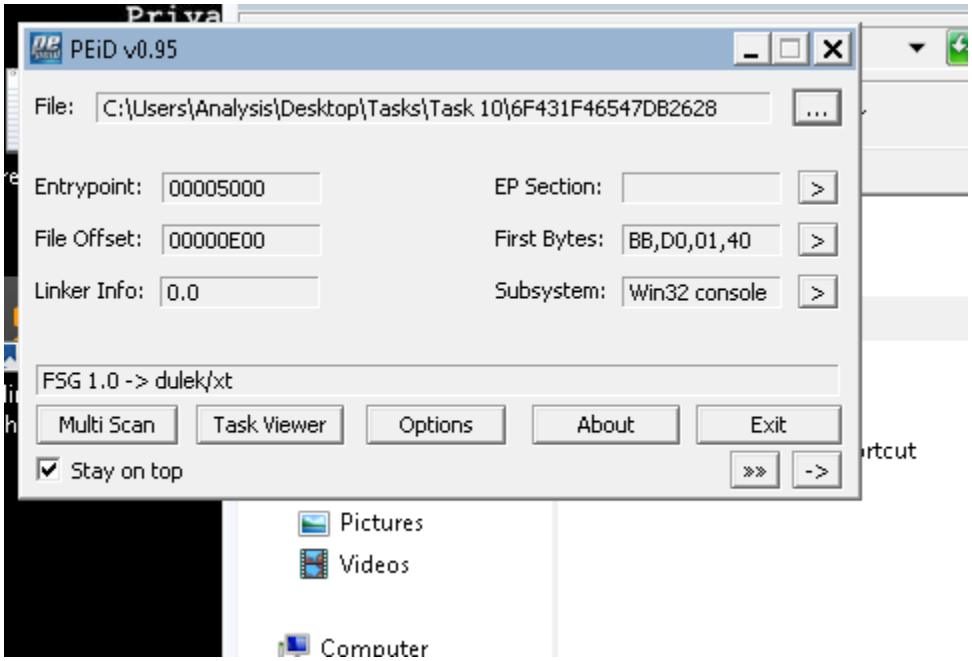
- Now using "PeID", identify the compiler / packer of the following two files in the Directory "Tasks/Task 9" to answer the questions In Task 9.



Sri Lanka Institute of Information Technology
Introduction to Cyber Security - IE2022
Lab Sheet 10
Year 2, Semester 1

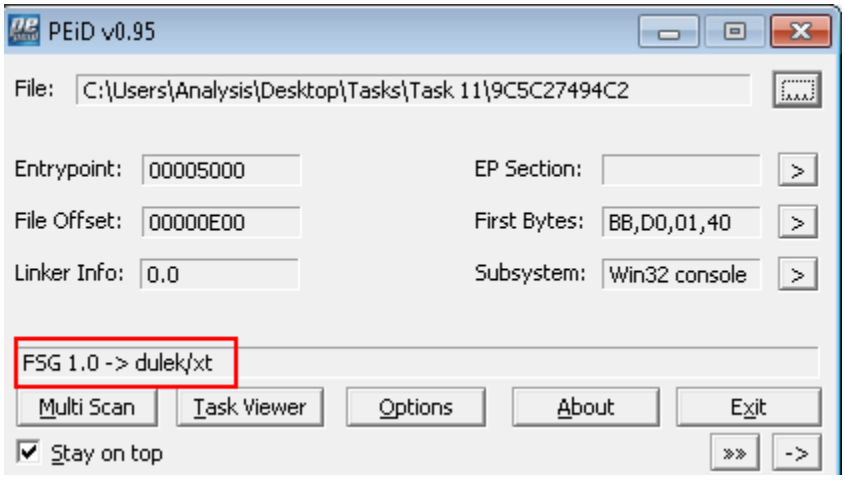
Task 10 : What is Obfuscation / Packing?

- Your task is to identify whether or not the file "6F431F46547DB2628" located in the Directory of "Tasks\Task 10" is packed using the tool "PeID" akin to the task.



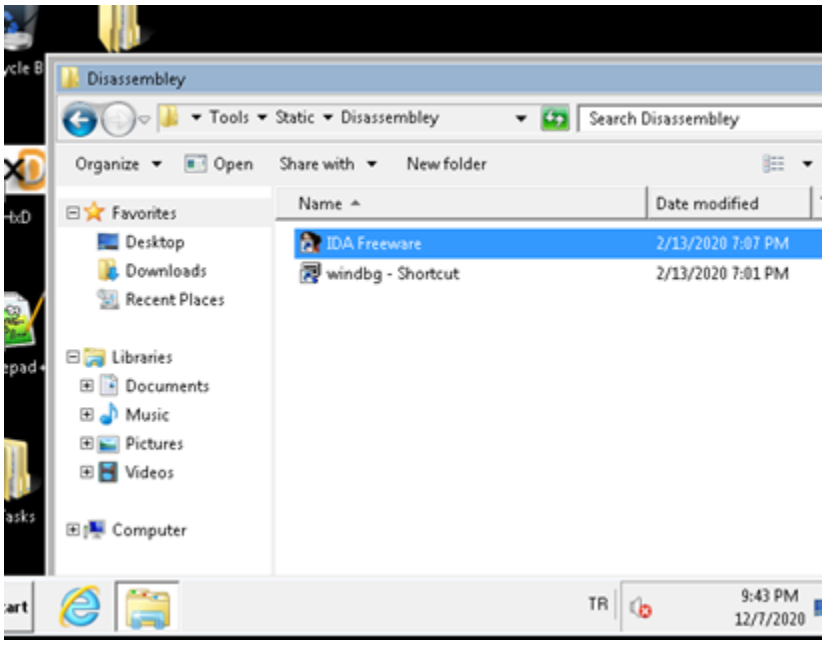
Task 11 : Visualising the Differences Between Packed & Non-Packed Code

- You can try this yourself by navigating to the directory "Tasks/Task 11" and dragging and dropping that file into PeID. What does it tell us?

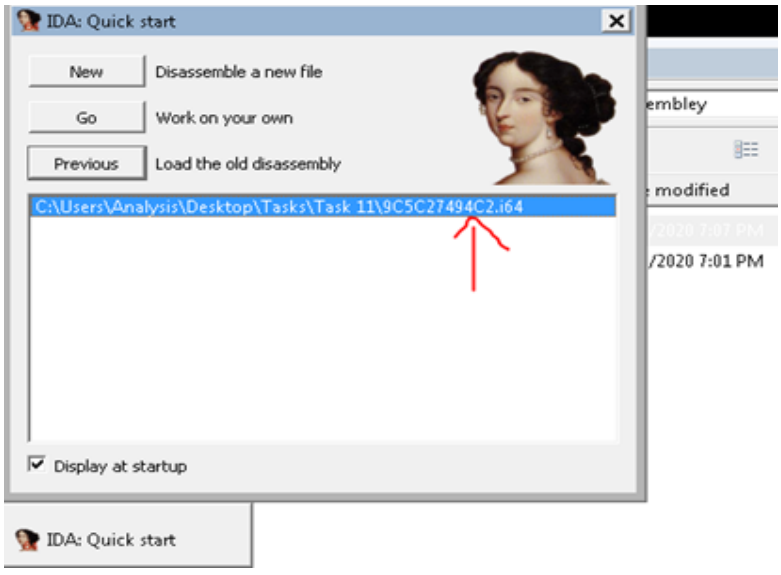


In this instance, PeID is able to detect what packer has been used to obfuscate the code. Whilst PeID is capable of detecting the possibility of packers being used, it is not able to automatically de-obfuscate them. This is a process we will have to do manually - at a later stage.

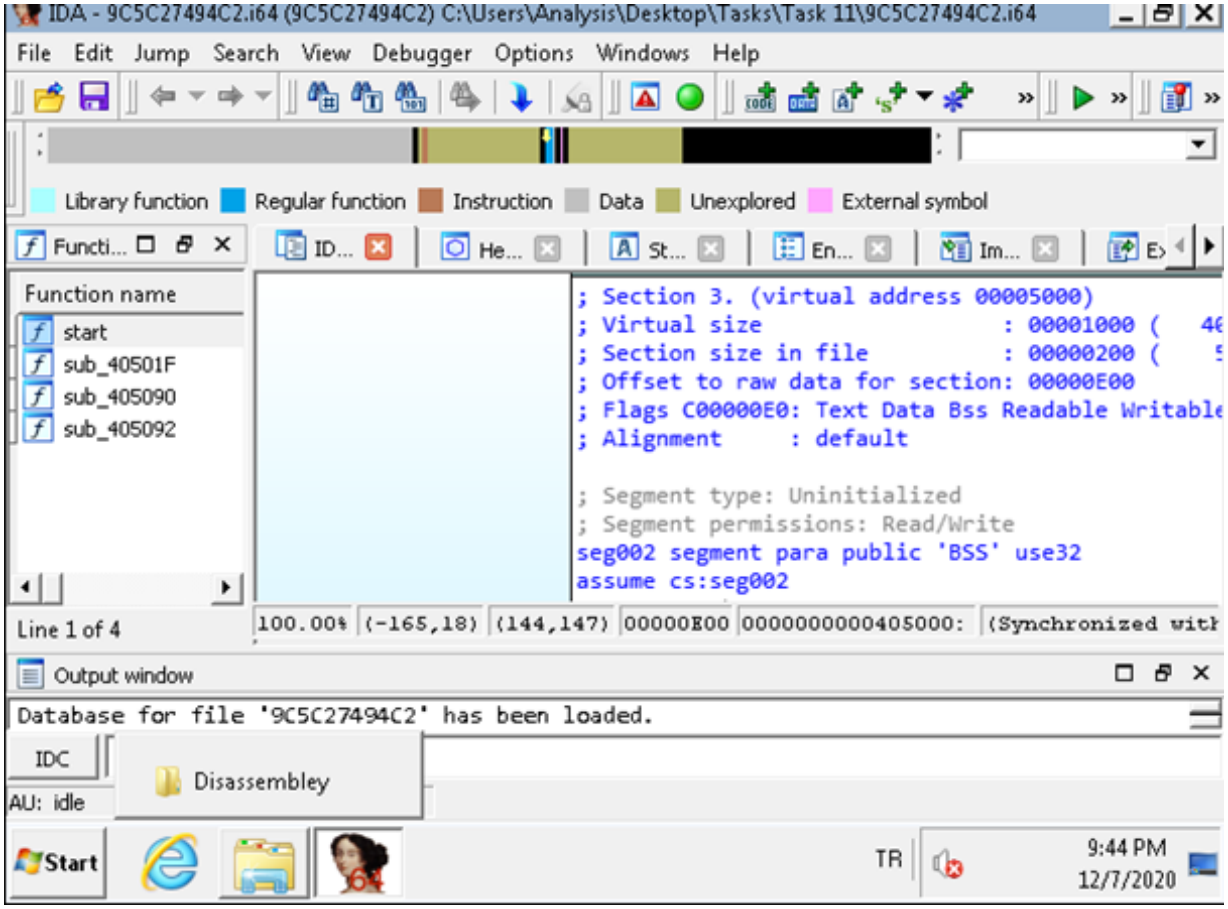
- After confirming that this file is indeed packed, let's open it up with a tool called IDA Freeware. This is located in the "Tools/Static/Disassembly" directory (or you can search for it through Windows Toolbar). Notice how there is a very minimal amount of information provided to us? For example, the "Imports" tab is practically empty.



- When opening the file, a few dialogue boxes may appear - it's just IDA Freeware processing the file, it'll take a couple of seconds.



Sri Lanka Institute of Information Technology
Introduction to Cyber Security - IE2022
Lab Sheet 10
Year 2, Semester 1



Task 12 : Introduction to Strings

- Open a Command prompt on the Windows Machine and navigate to the directory "Tools\Sysinternalssuite"

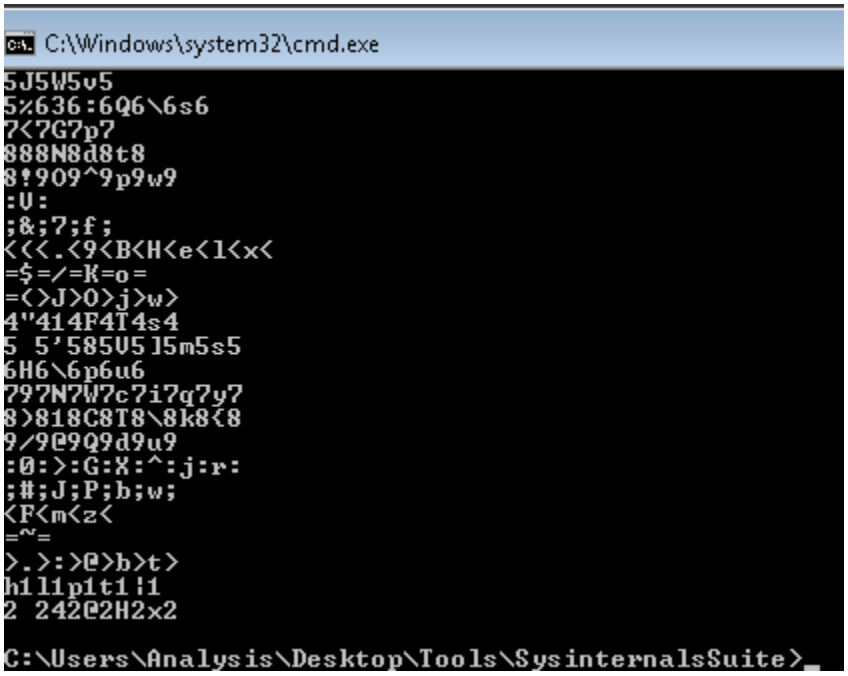
```
cd C:\Users\Analysis\Desktop\Tools\SysinternalsSuite
```

Keep this terminal open.

- We're going to use Microsoft's Sysinternals "Strings" program to output the retained strings within the specified file in "Task 12". We can do this by:

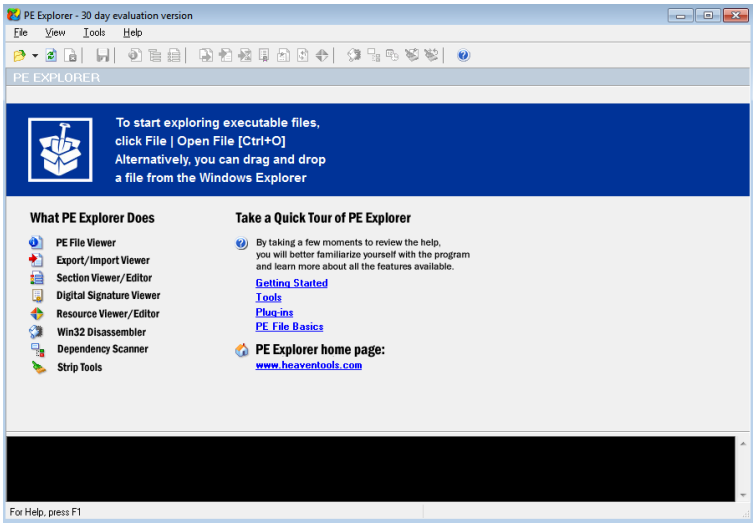
```
strings "C:\Users\Analysis\Desktop\Tasks\Task 12\67844C01"
```

You will receive a whole load of text,

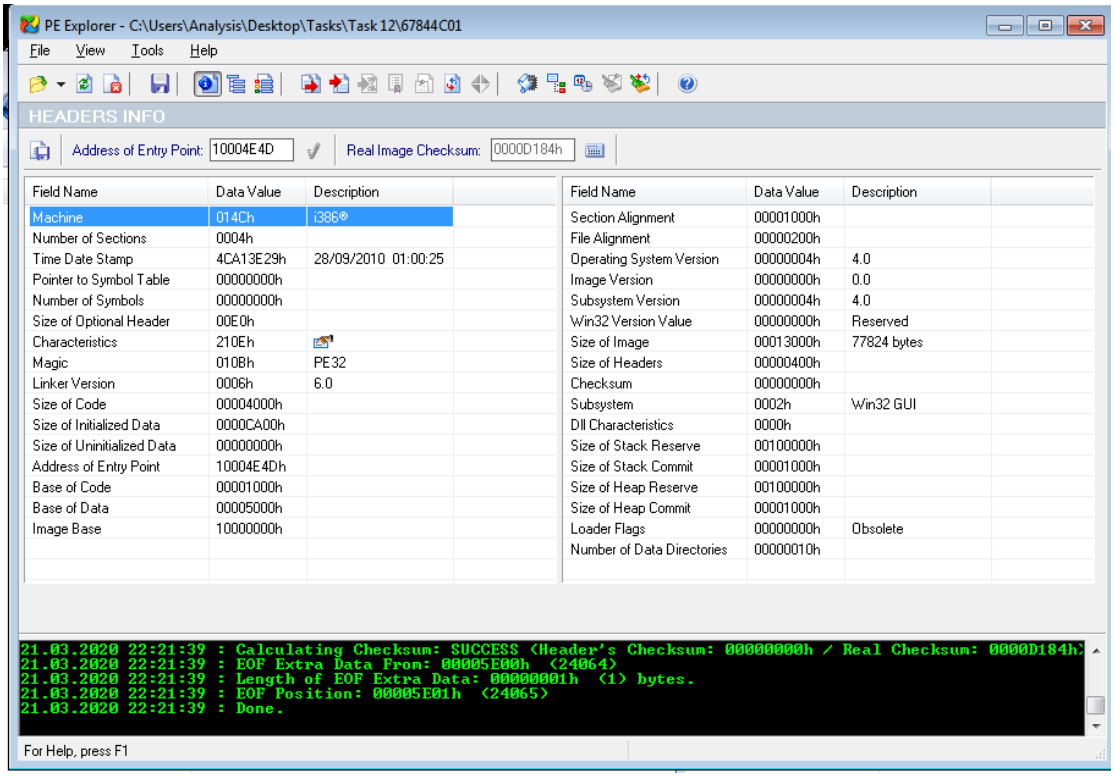


You'll find that programs often contain large amounts of strings and using the "strings" tool from sysinternals may only display 10% of these.

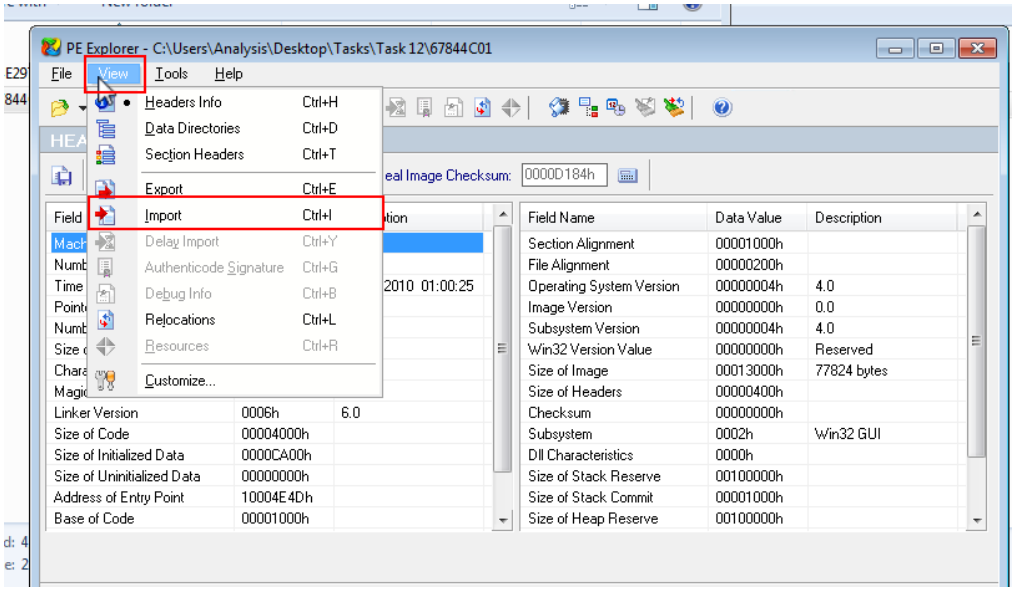
- Launch the application within "Tools/Static/PE Tools/PE Explorer" and drag and drop the same file "67844C01" from the previous question into the application.



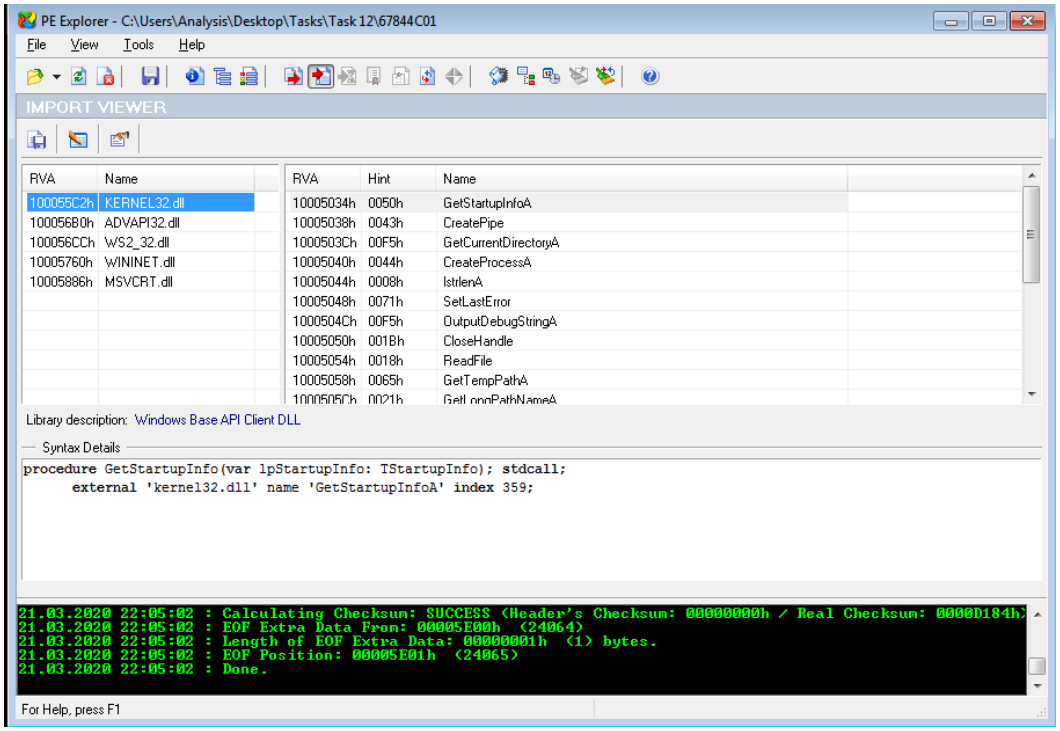
- Where you will be presented with the following, indicating that it has successfully imported:



- After import. Navigate to "View -> Imports"

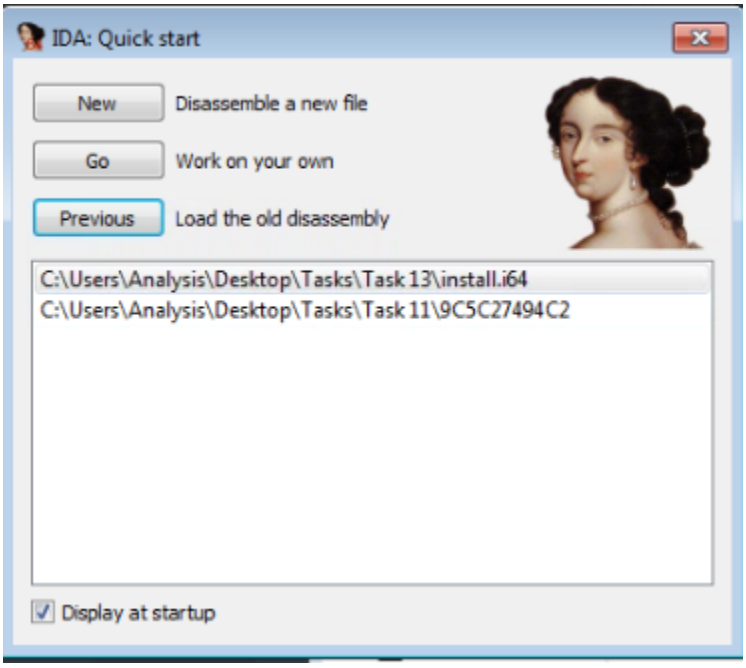


Sri Lanka Institute of Information Technology
Introduction to Cyber Security - IE2022
Lab Sheet 10
Year 2, Semester 1

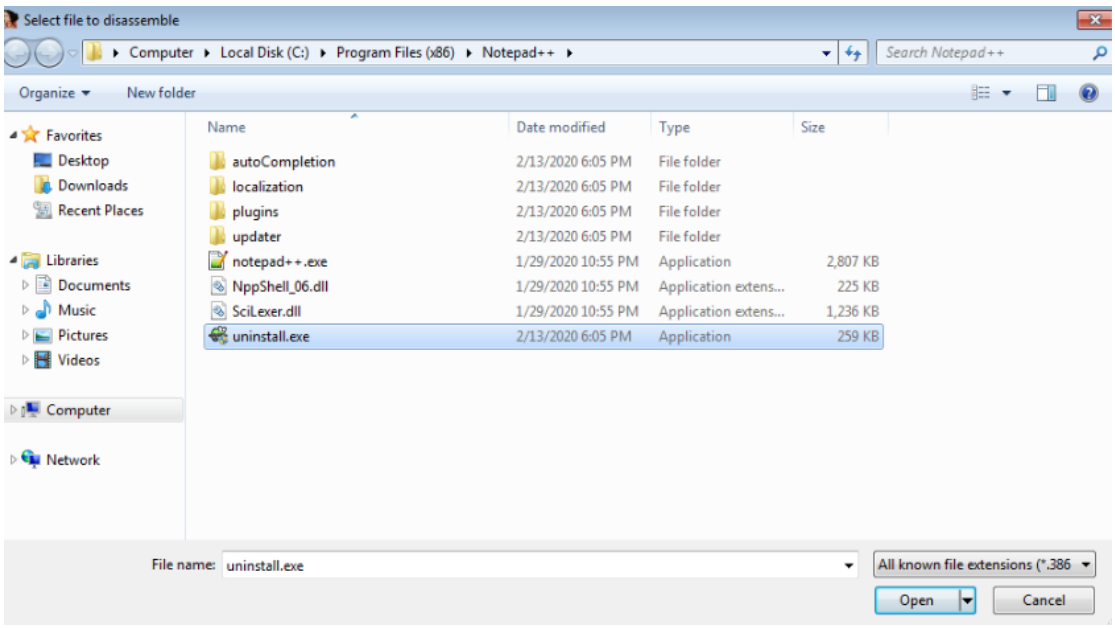


Task 13 : Introduction to Imports

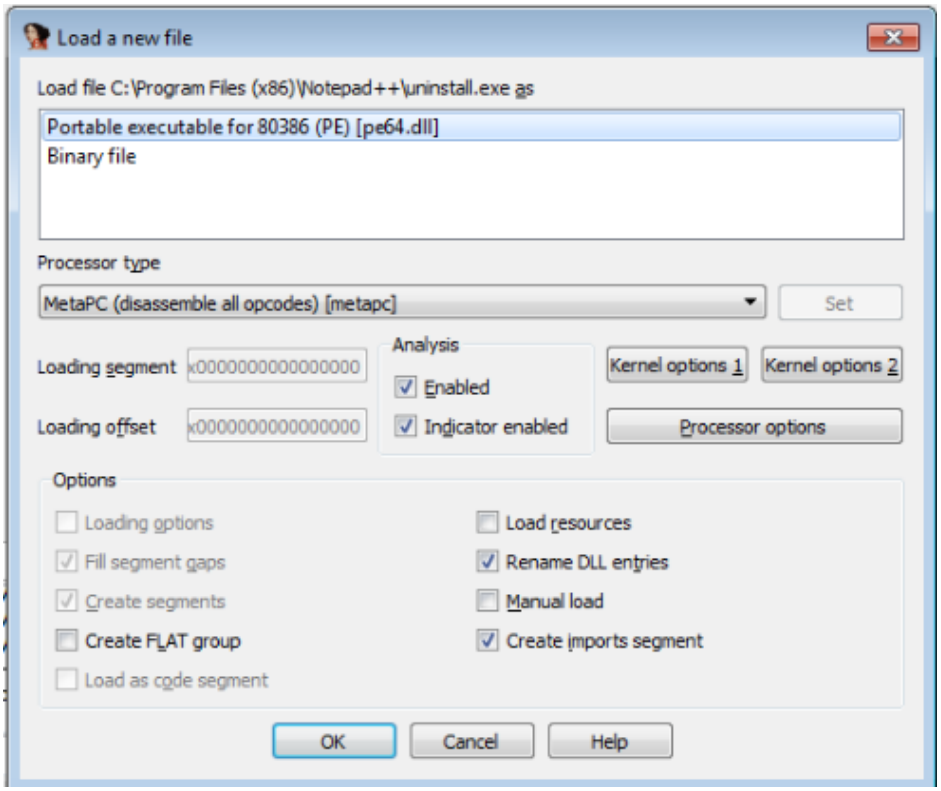
- Lets launch "IDA Freeware" and select the file to import, in this case we'll be using "uninstall.exe"



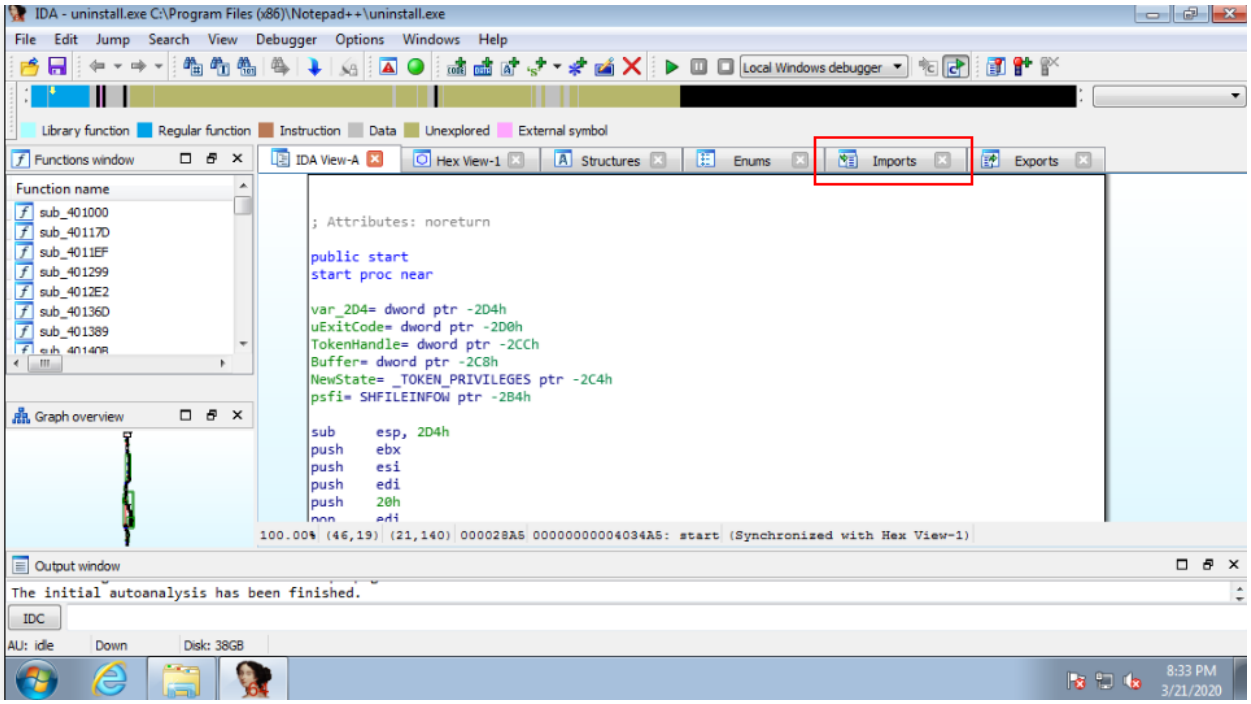
And navigate to the file.



- Since we know it is an executable file, we select "Portable executable for 80386 (PE) [pe64.dll]"



- After pressing "OK" the application will load. Allow a few minutes for the executable to be decompiled.



There are various tabs, similar to what we saw in "PE Explorer" i.e. "Imports" and "Exports".

- Navigate to the directory "Tasks/Task 13" and open "install.exe" with IDA Freeware, just like we did in the example above. Again, this may take a few seconds to a couple of minutes to compute depending upon the size of the application.

Task 14 : Practical Summary

We are not going to walk you through this one, but you have done all the necessary steps above to achieve this.

If you struggle, revisit the techniques you used above.

The file specified for analysis is "ComplexCalculator.exe" in the Directory "Tasks/Task 14". I'll leave it up to you to figure out what tool(s) out of what we've used above is best and you have to answer questions in Task 14.