



## 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

The screenshot shows the TryHackMe interface for Task 6. At the top, there is a table with columns: Title, IP Address, Expires, and buttons for 'Add 1 hour', 'Terminate', and 'Access in browser in 283s'. The title is 'IntMal-Windows01' and the IP address is 'Shown in 59s'. Below the table, the task title 'Task 6 Connecting to the Windows Analysis Environment (Deploy)' is displayed. The main content area contains a description of the task, a 'Deploy' button, and a section titled 'Credentials:' with the following information: Domain: ANALYSIS-PC, Username: Analysis, Password: tryhackme. Below the credentials, there is a 'MACHINE\_IP' placeholder and a note about the Remote Desktop Terminal. At the bottom, there is a 'Remote Desktop Connection' window showing the connection progress.

Title	IP Address	Expires	Buttons
IntMal-Windows01	Shown in 59s	Expires 59m 44s	<button>Add 1 hour</button> <button>Terminate</button> <button>Access in browser in 283s</button>

**Task 6** Connecting to the Windows Analysis Environment (Deploy)

Whilst malware has been known to traverse (spread) over RDP, in this instance, any and all samples on here are not capable of doing so - nor are they capable of performing any destructive action.

This series will teach you the practical knowledge and tool familiarity to allow you to transfer these skills to actual samples if you wish too, outside of TryHackMe

With this being a Windows instance specifically, alongside the additional tools and tasks it has to execute, please expect up to wait up towards 10 minutes before being able to access your instance. The average deploy to login took about 7 minutes. Also, please note that the Host will not respond to pings - only the (Remote Desktop Protocol) RDP protocol (3389)

Credentials:

You can either connect via RDP (connect to our network first via OpenVPN), or control the machine in browser (no connection required). Please note that this Windows "instance" will take atleast 5 minutes to fully boot - please be patient. You can view the progress via the progress-bar within the display above.

**MACHINE\_IP**

Domain: ANALYSIS-PC  
Username: Analysis  
Password: tryhackme

Windows:

- Default Remote Desktop Terminal, replace the IP Address with your **MACHINE\_IP**

Remote Desktop Connection

Remote Desktop Connection

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



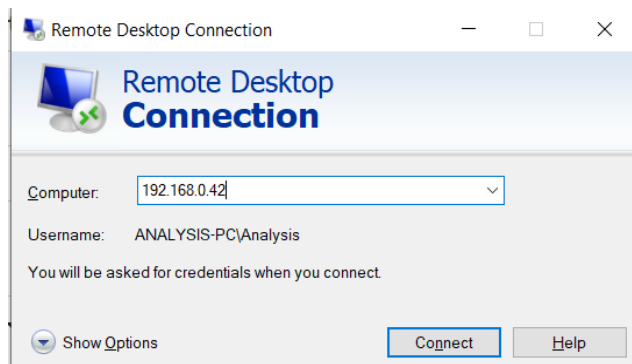
- Get the remmina and RDP

Username: Analysis

Password: Tryhackme123!

**Windows:**

- Default Remote Desktop Terminal, replace the IP Address with your MACHINE\_IP

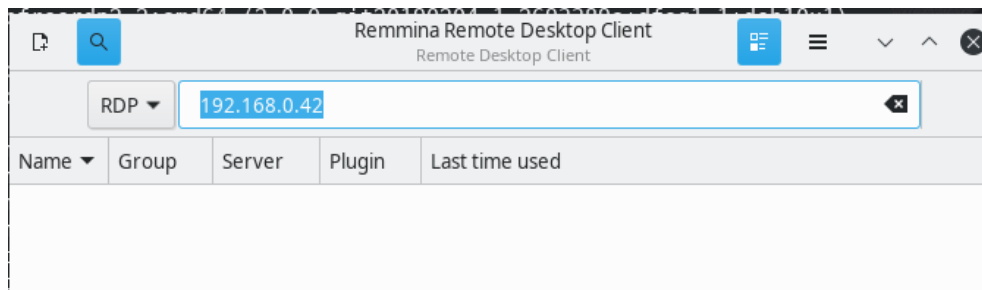


**Linux:**

Any compatible RDP client such as Remmina:

sudo apt-get install remmina

Again, replacing the IP address with your MACHINE\_IP



A screenshot of a Windows authentication dialog box. The title bar shows the IP address '192.168.0.42'. The main title is 'Enter authentication credentials'. It contains four fields: 'User name' with the text 'Analysis', 'Password' with masked characters '\*\*\*\*\*', 'Domain' with the text 'ANALYSIS-PC', and a 'Save password' toggle switch which is currently turned off. At the bottom, there are 'OK' and 'Cancel' buttons.

### 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

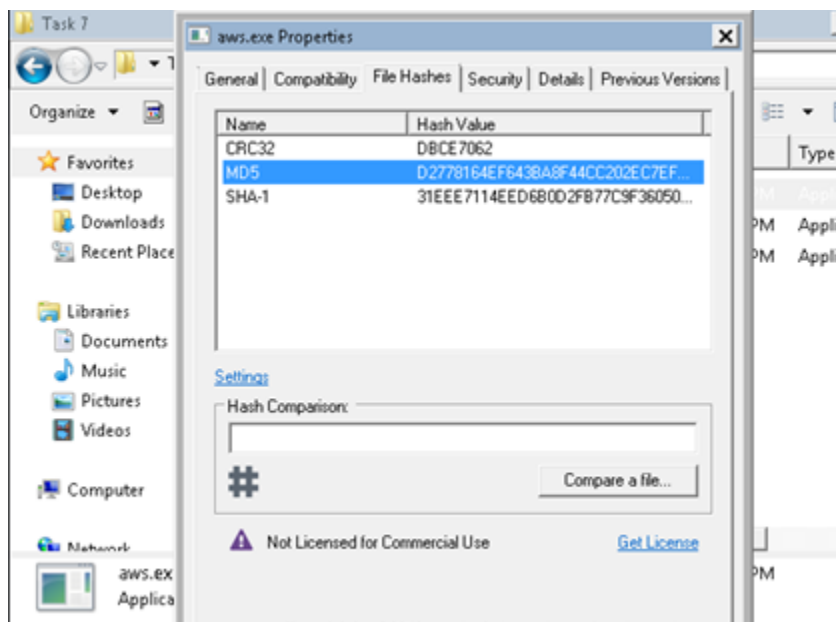
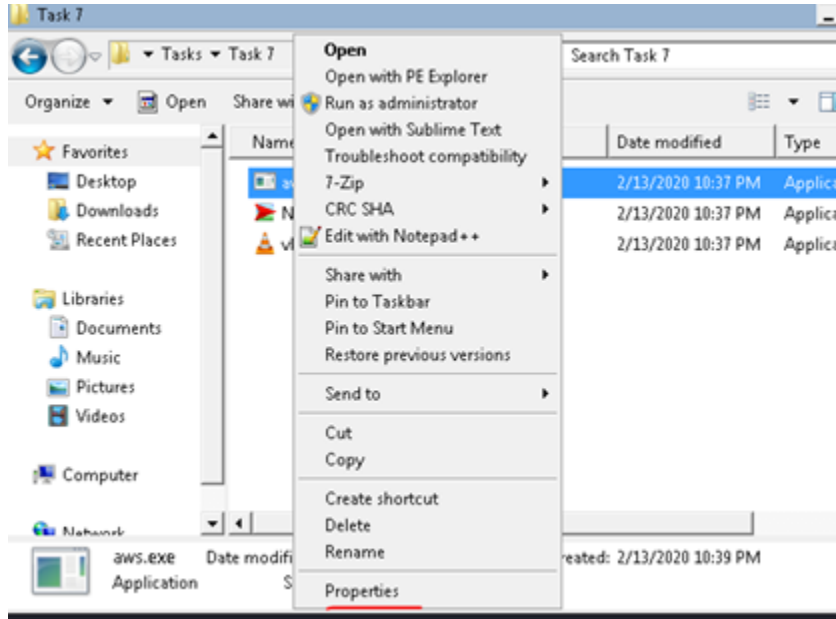
- vlc.exe

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**

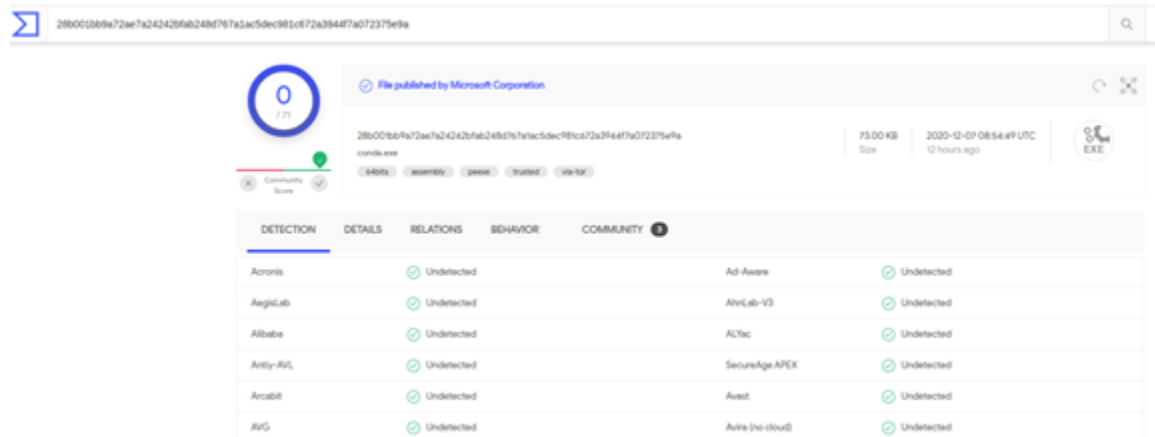


- Same steps used for other two files in "Task 7" to Identify the MD5 Checksums.



### 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](https://www.virustotal.com) to solve this task.
- Put three hashes that u found in Task 07 to [VirusTotal](https://www.virustotal.com) 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.

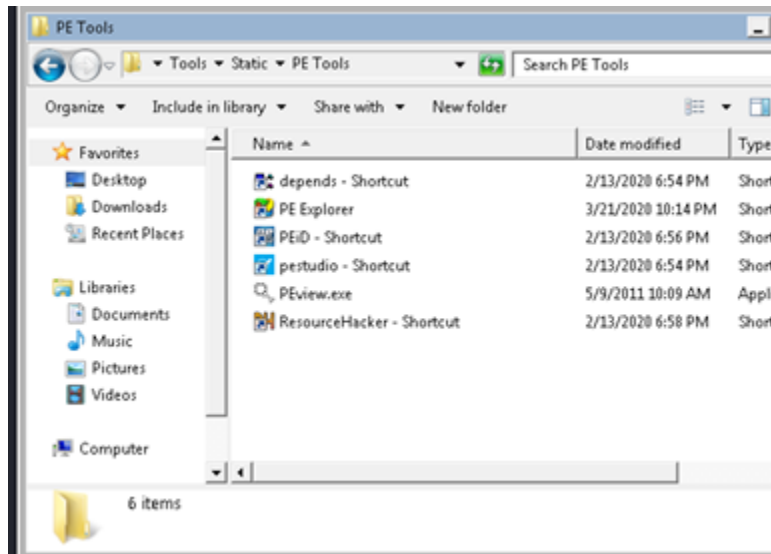
E.g. The hex value for an executable is always "4D 5A". So if a file with a ".jpg" file has the hex header of "4D 5A", then it is obviously not a jpg file. You can read more into file headers / trailers here, which are great resources for data carving in file forensics / recovery.

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

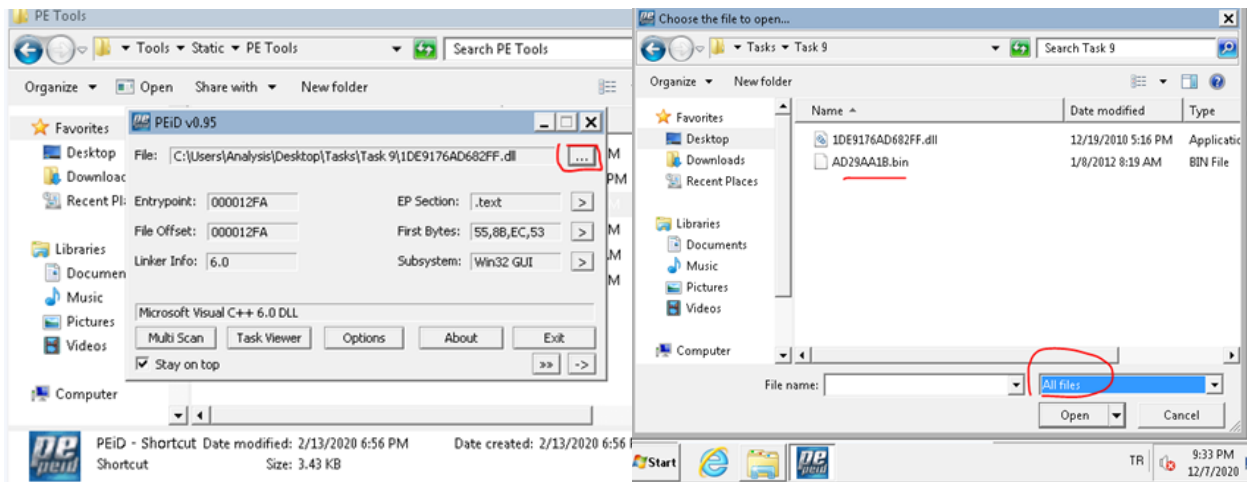


Provided Tools: **PeID**

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



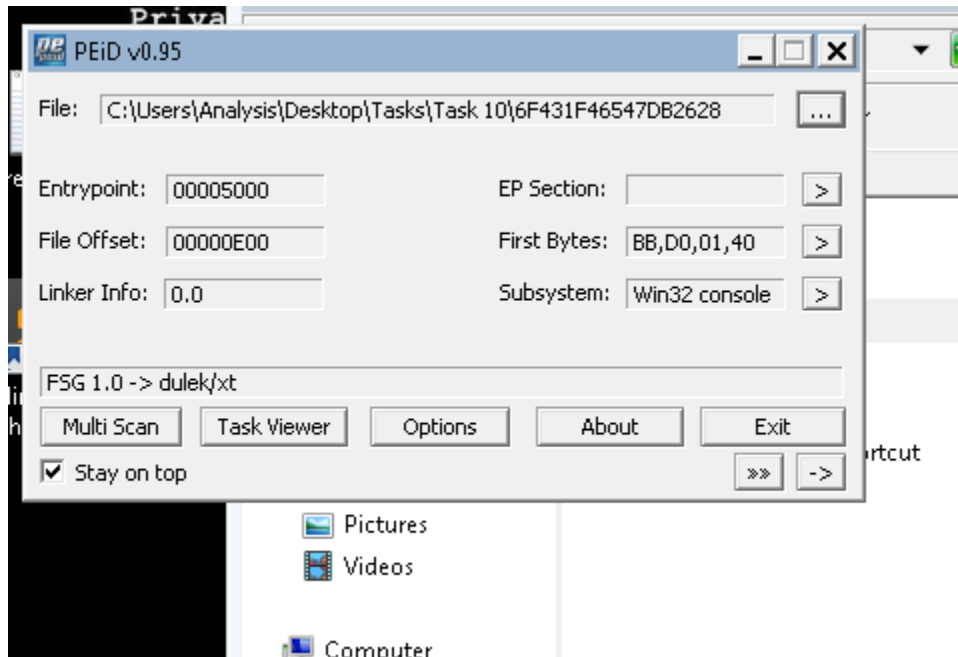
- Now using **"PeID"**, identify the compiler / packer of the following two files in the Directory **"Tasks/Task 9"** to answer the questions In Task 9.





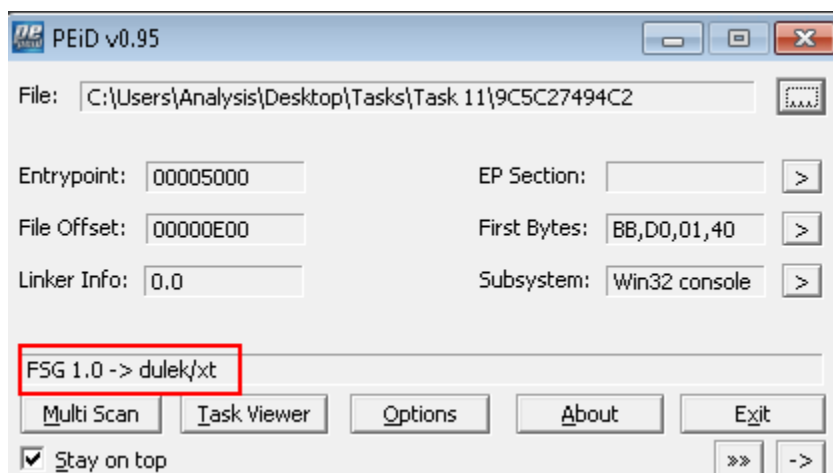
### Task 10 : What is Obfuscation / Packing?

- 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?

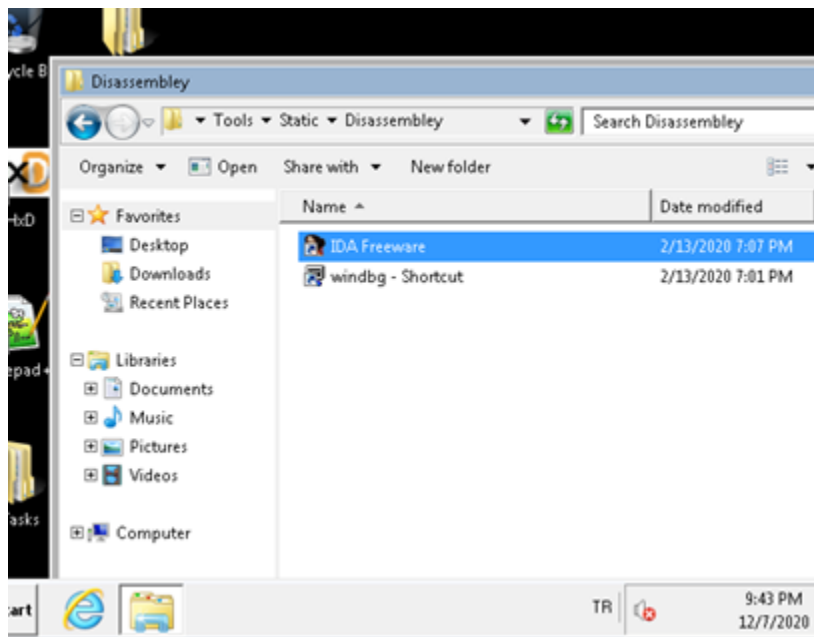


**Sri Lanka Institute of Information Technology**  
**Introduction to Cyber Security - IE2022**  
**Lab Sheet 10**  
**Year 2, Semester 1**

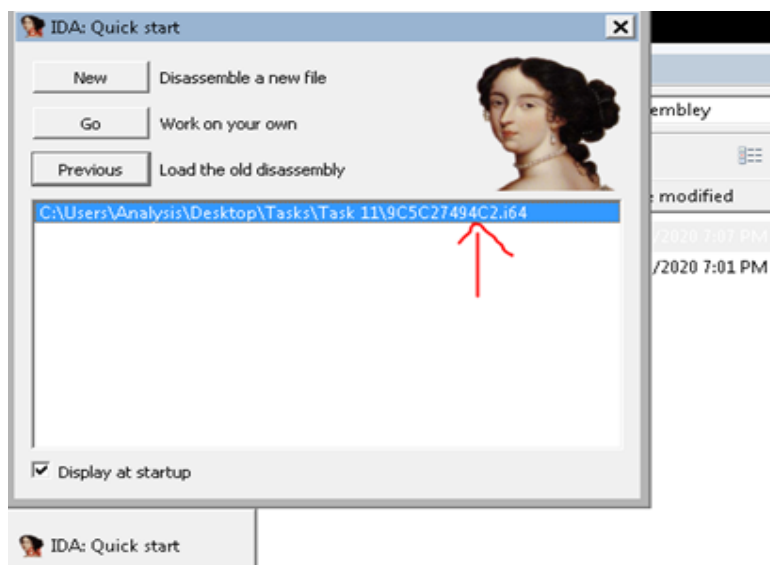


In this instance, PeID is able to detect what packer has been used to obfuscate the code. Whilst PeID is capable of detecting the possibility of packers being used, it is not able to automatically de-obfuscate them. This is a process we will have to do manually - at a later stage.

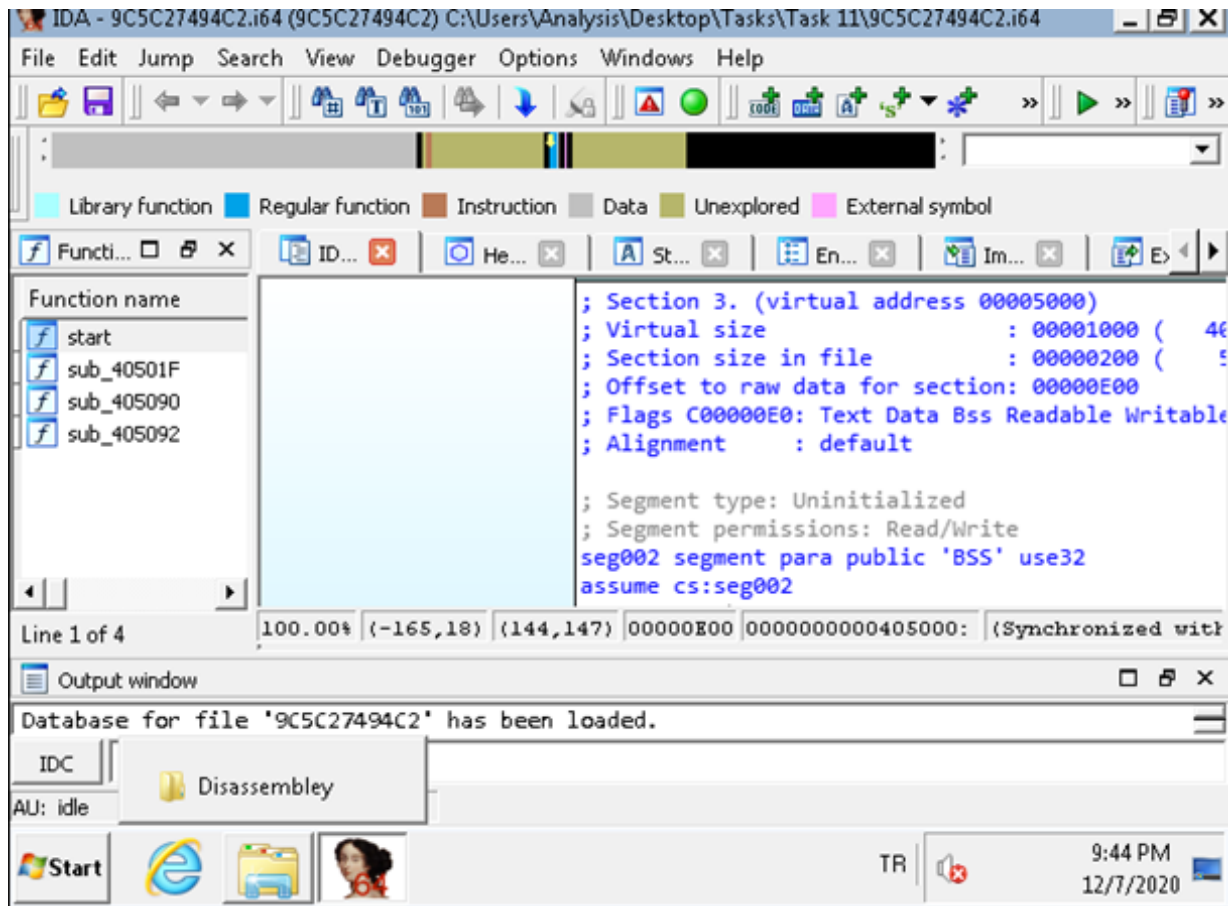
- After confirming that this file is indeed packed, let's open it up with a tool called **IDA Freeware**. This is located in the **"Tools/Static/Disassembly"** directory (or you can search for it through Windows Toolbar). Notice how there is a very minimal amount of information provided to us? For example,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







## 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"

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

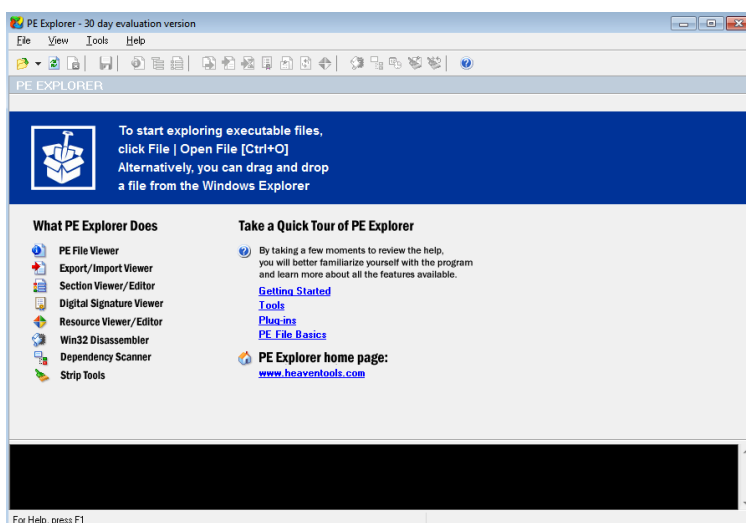


You will receive a whole load of text,

```
C:\Windows\system32\cmd.exe
5J5W5v5
5x636:6Q6\6s6
7<7G7p7
888N8d8t8
8!909^9p9w9
:U:
;&;7;f;
<<<.<9<B<H<e<1<x<
=$=/=K=o=
=<>J>O>j>w>
4"414F4I4s4
5 5'585U5 I5m5s5
6H6\6p6u6
797N7W7c7i7q7y7
8>818C8I8\8k8<8
9/9Q9Q9d9u9
:0:>:G:X:^:j:r:
;#;J;P;b;w;
<F<m<z<
=~=
>.>:>e>b>t>
h111p1t1!1
2 242Q2H2x2
C:\Users\Analysis\Desktop\Tools\SysinternalsSuite>
```

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

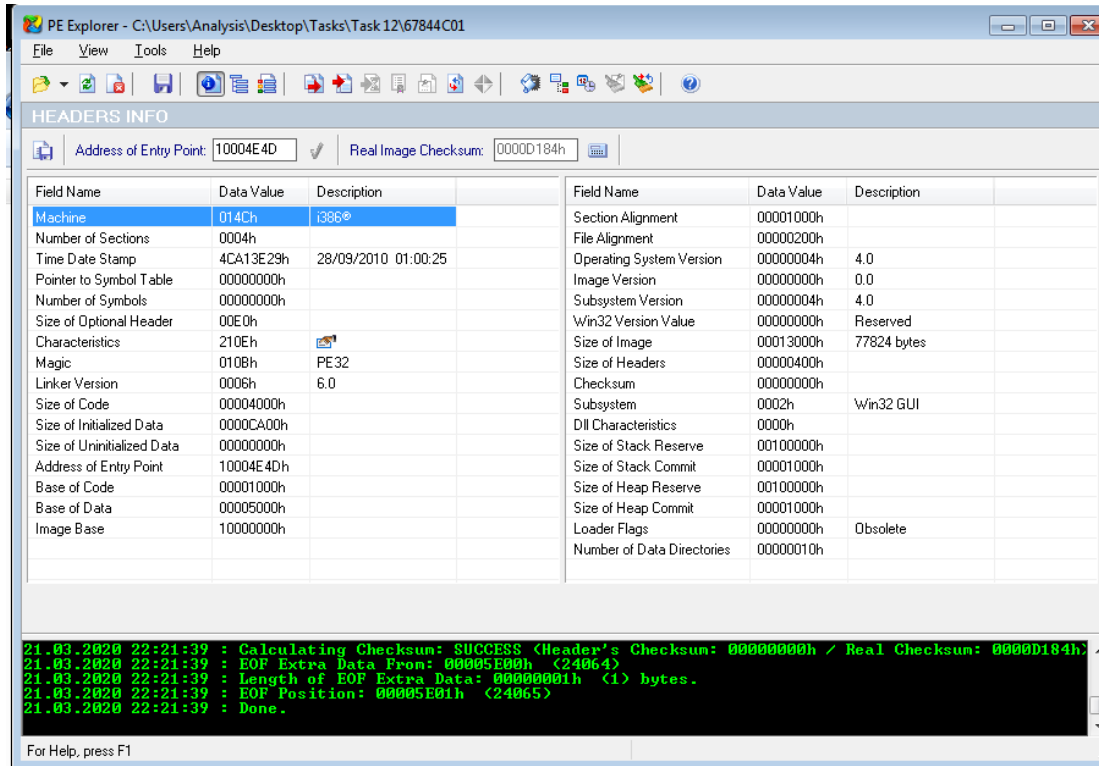
- Launch the application within "Tools/Static/PE Tools/PE Explorer" and drag and drop the same file "67844C01" from the previous question into the application.



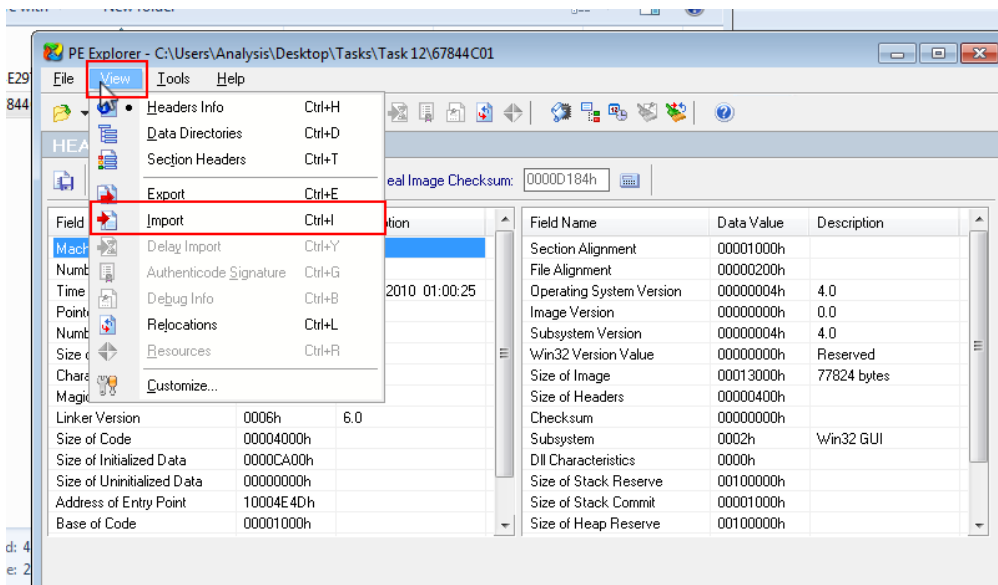
**Sri Lanka Institute of Information Technology**  
**Introduction to Cyber Security - IE2022**  
**Lab Sheet 10**  
**Year 2, Semester 1**



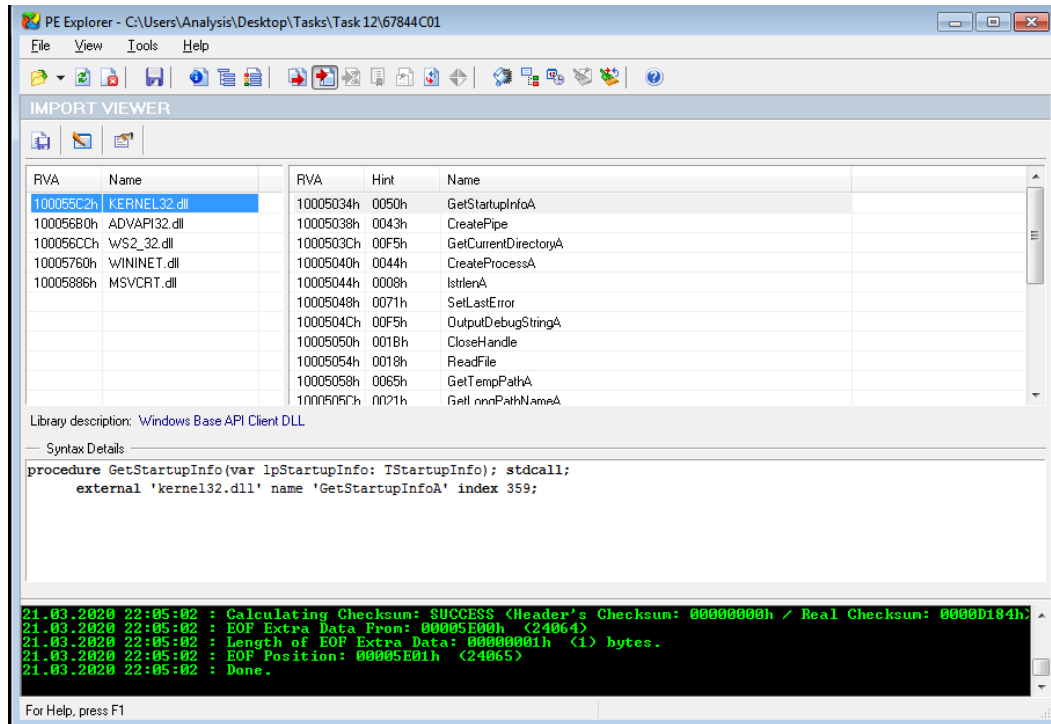
- Where you will be presented with the following, indicating that it has successfully imported:



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

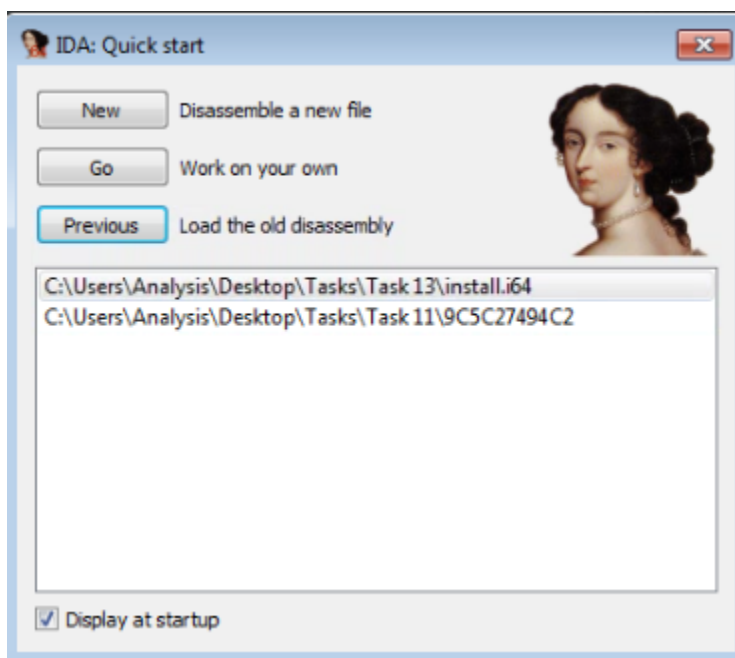


**Sri Lanka Institute of Information Technology**  
**Introduction to Cyber Security - IE2022**  
**Lab Sheet 10**  
**Year 2, Semester 1**



**Task 13 : Introduction to Imports**

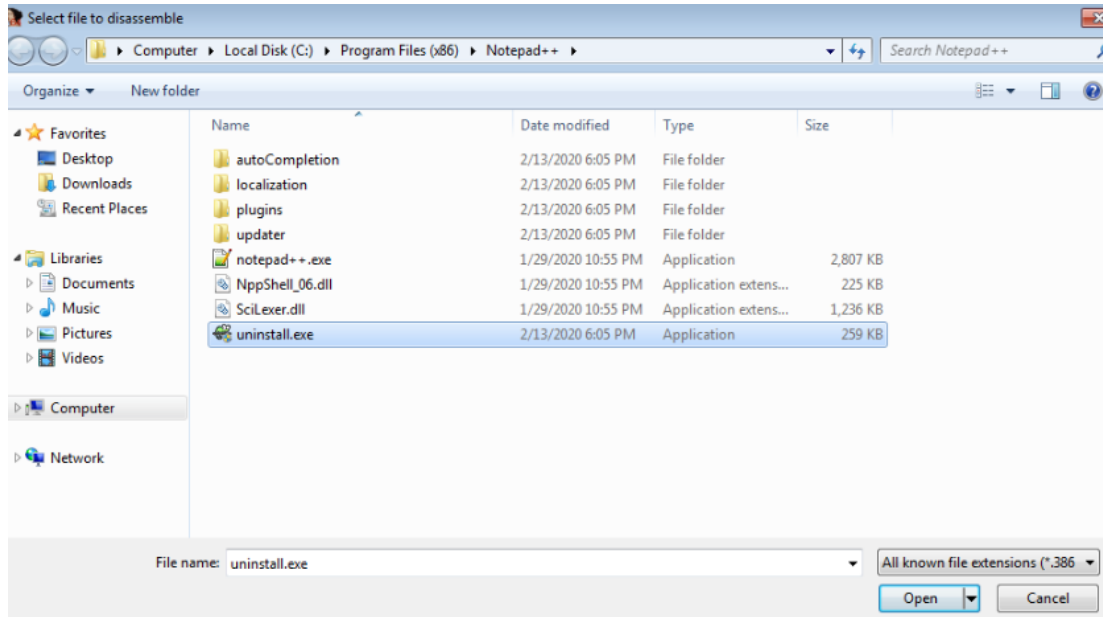
- Lets launch "IDA Freeware" and select the file to import, in this case we'll be using "uninstall.exe"



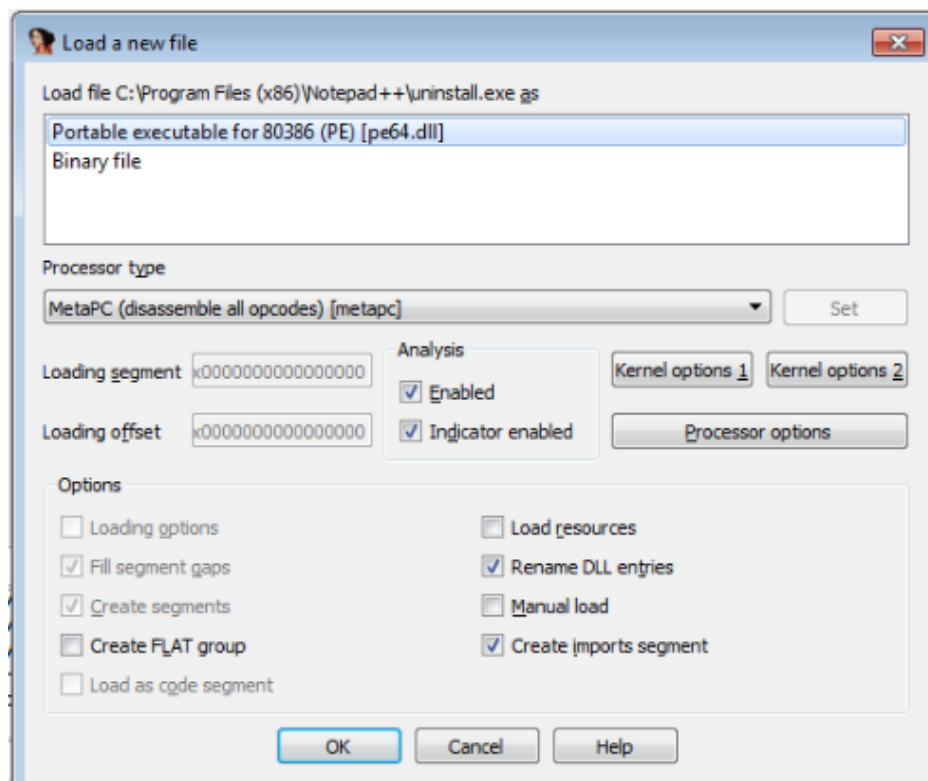
**Sri Lanka Institute of Information Technology**  
**Introduction to Cyber Security - IE2022**  
**Lab Sheet 10**  
**Year 2, Semester 1**



And navigate to the file.

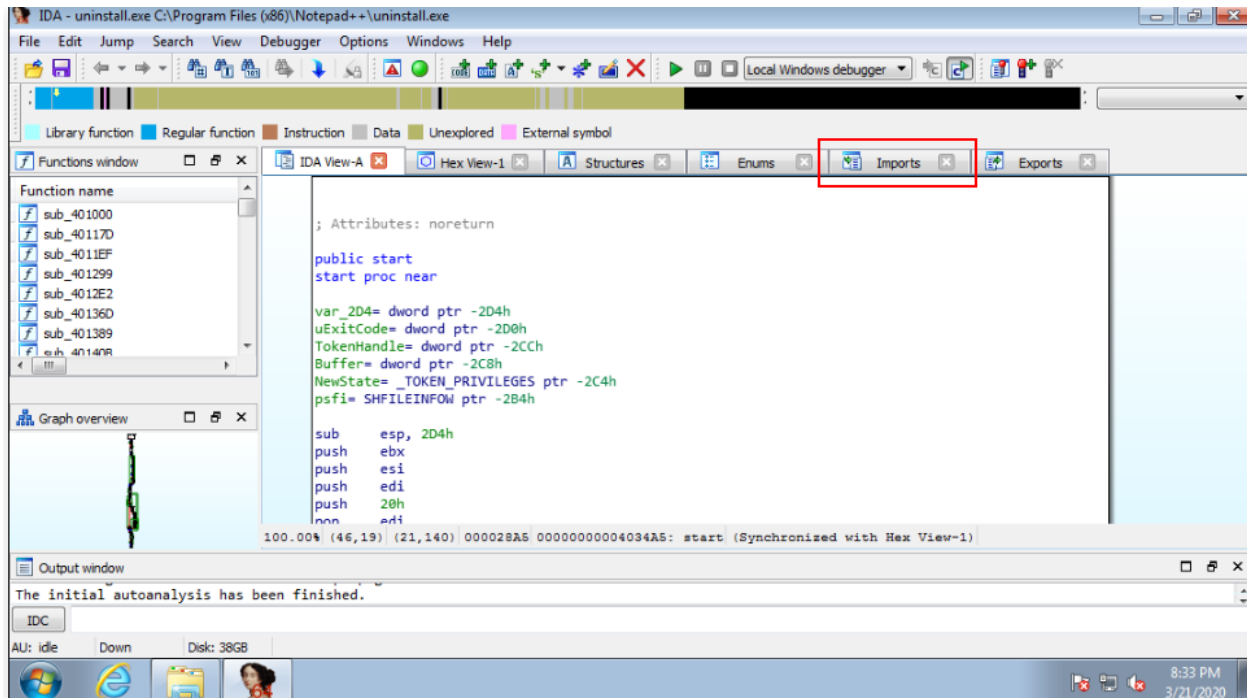


- Since we know it is an executable file, we select "Portable executable for 80386 (PE) [pe64.dll]"





- 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.