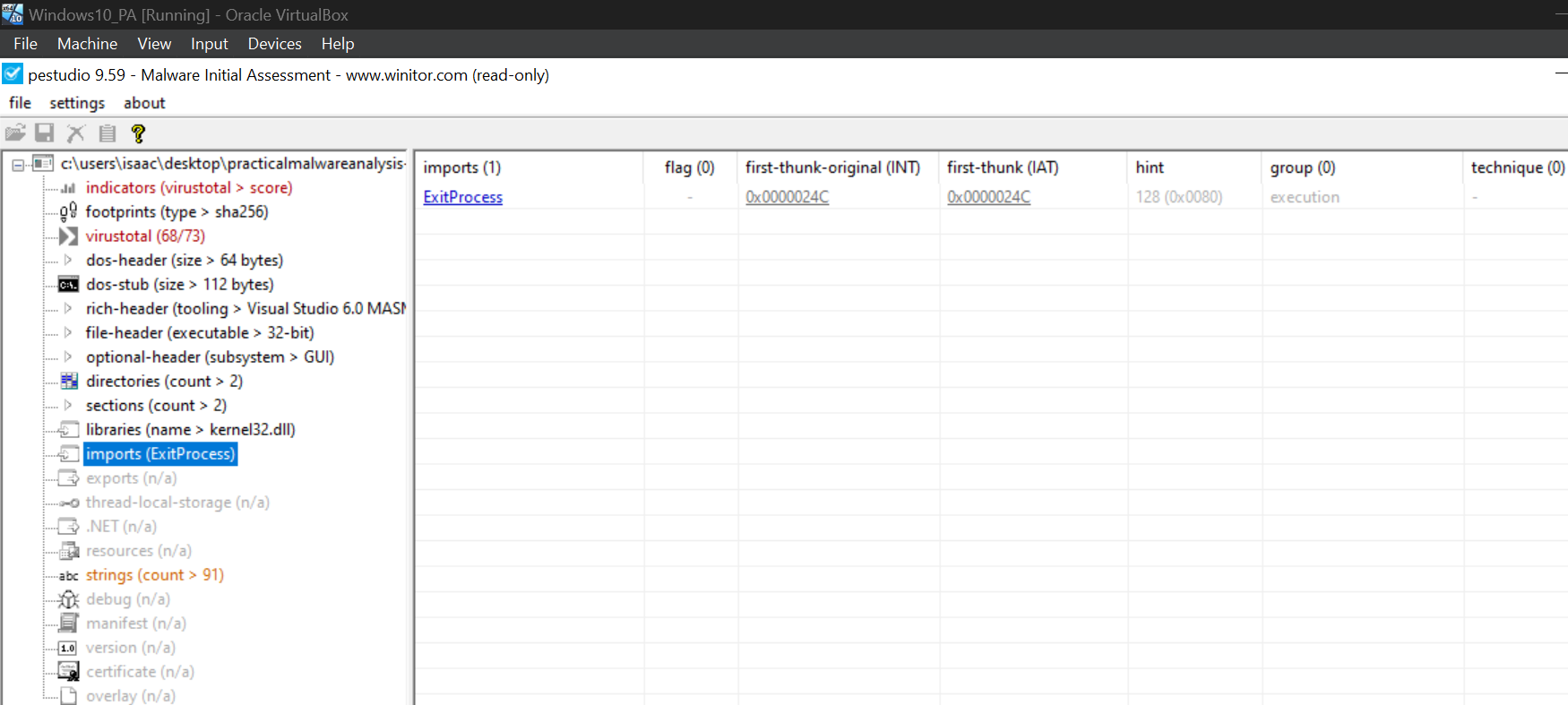
**150182 - Kipruto Isaac**

**Chapter 3. Basic Dynamic Analysis**

**Lab 3-1**

This lab uses the file Lab03-01.exe. Analyse this using basic dynamic analysis tools.

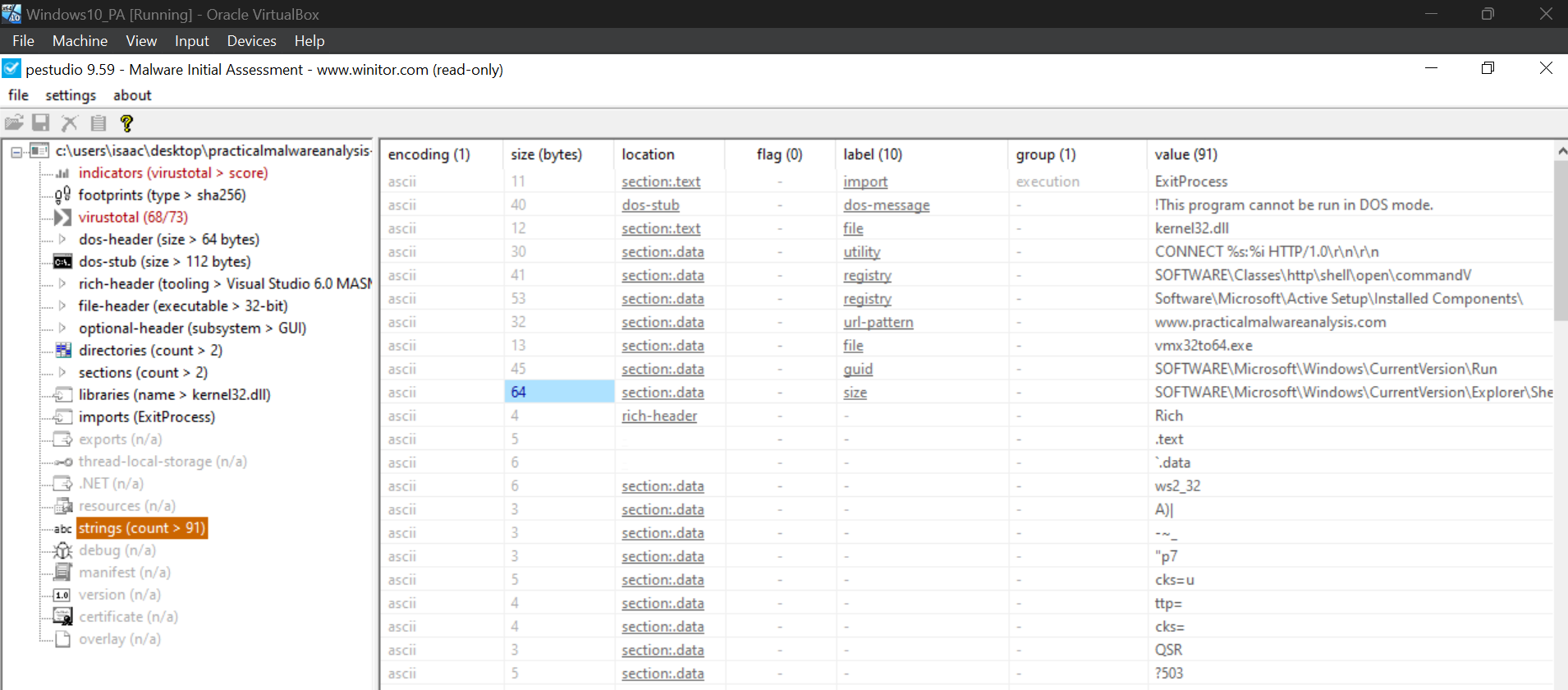
**Question** 1

What are this malware’s imports and strings? 



PE Studio to gain a lot of insight into the file, and determine both its imports and strings.

Based on the low number of imports we can assume this file is packed.

****

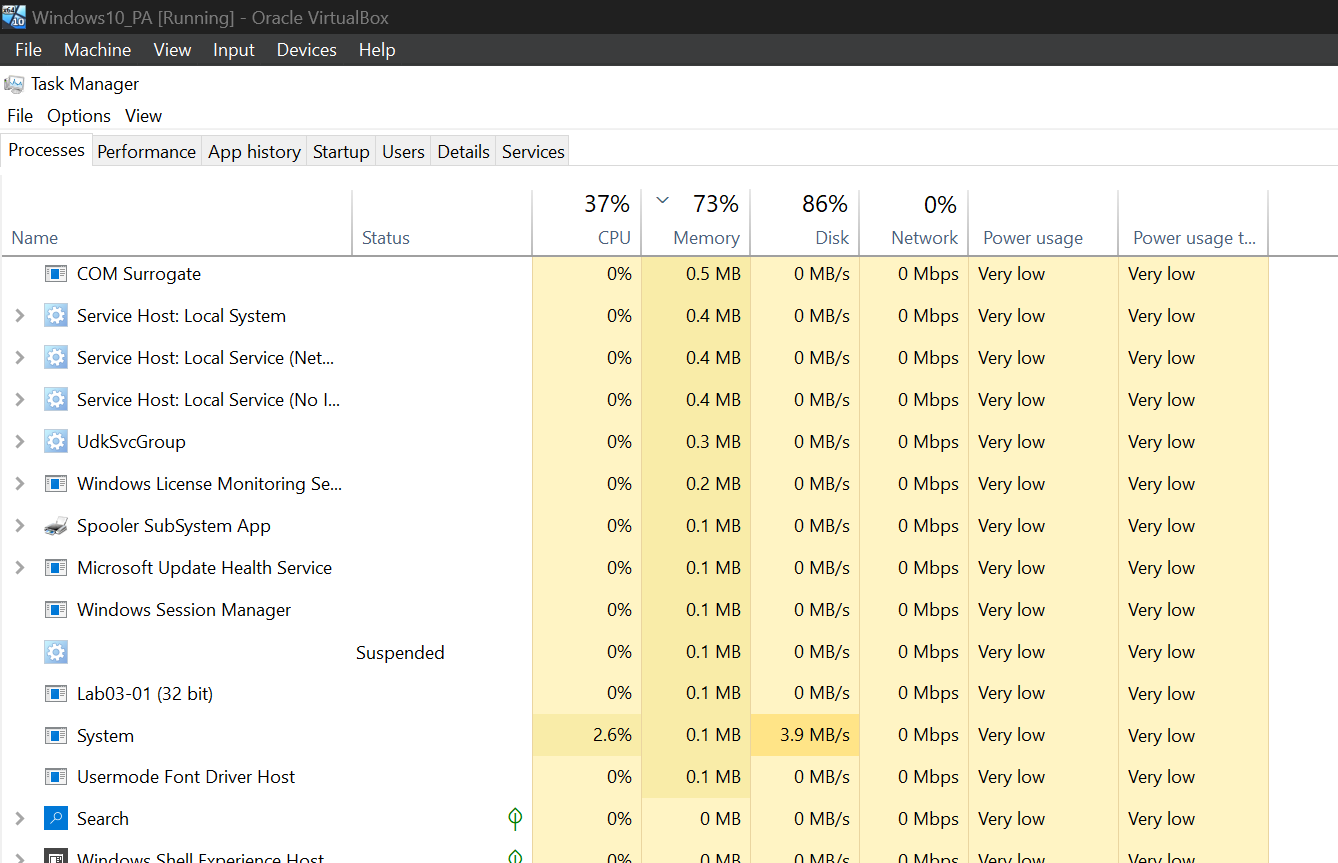
**Question 2**

What are the malware’s host-based indicators?

**Attempting to run this file within a Windows 7 and Windows 10 VM causes it to crash and fail.**

**Question 3**

Are there any useful network-based signatures for this malware? If so, what are they?



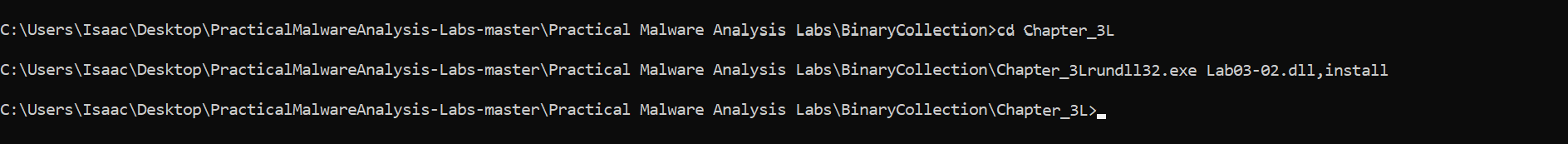


**Lab 3-2**

This lab uses the file Lab03-02.dll. Analyse this using basic dynamic analysis tools.

**Question 1**

How can you get this malware to install itself?



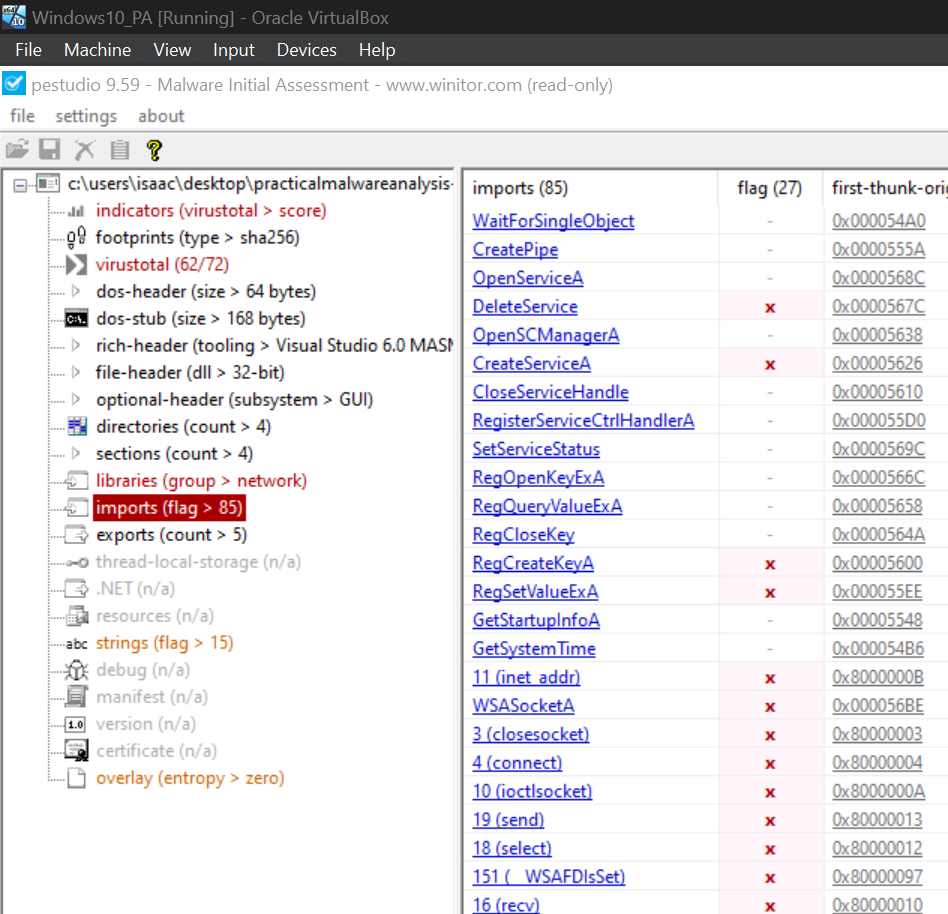
**Question 2**

How would you get this malware to run after installation?

**SC start IPRIP**

**net start IPRIP**

**Question 3**

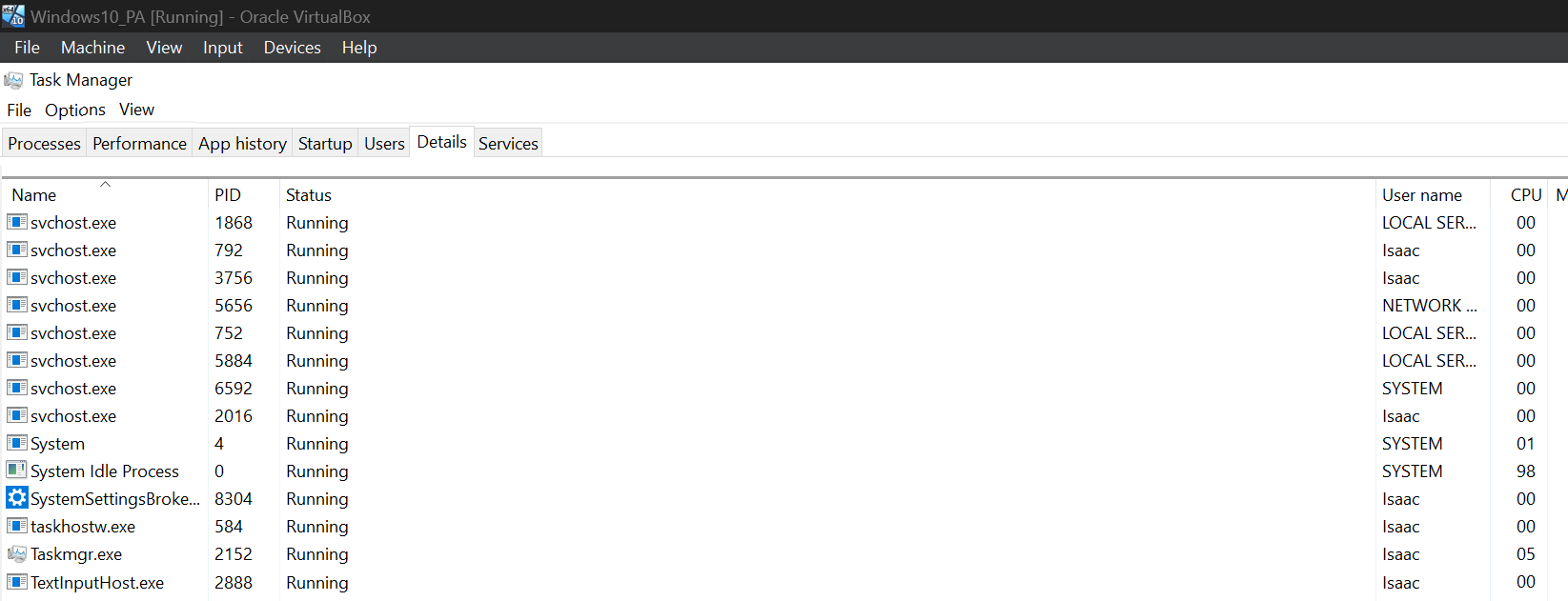
How can you find the process under which this malware is running? 

**Question 4**

Which filters could you set to use Promon to glean information?

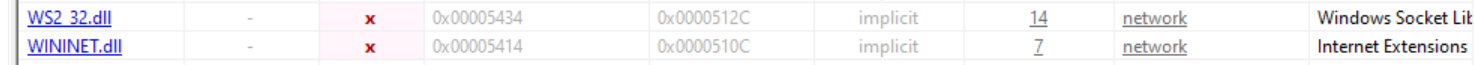
**Because there’s likely to be multiple svchost processes, we can filter by the Process ID to glean information only on the svchost process responsible for running this malware.**

**Question 5**

What are the malware’s host-based indicators? 

**Question 6**

Are there any useful network-based signatures for this malware?



**Lab 3-3**

This lab uses the file Lab03-03.exe. Analyse this using basic dynamic analysis tools.

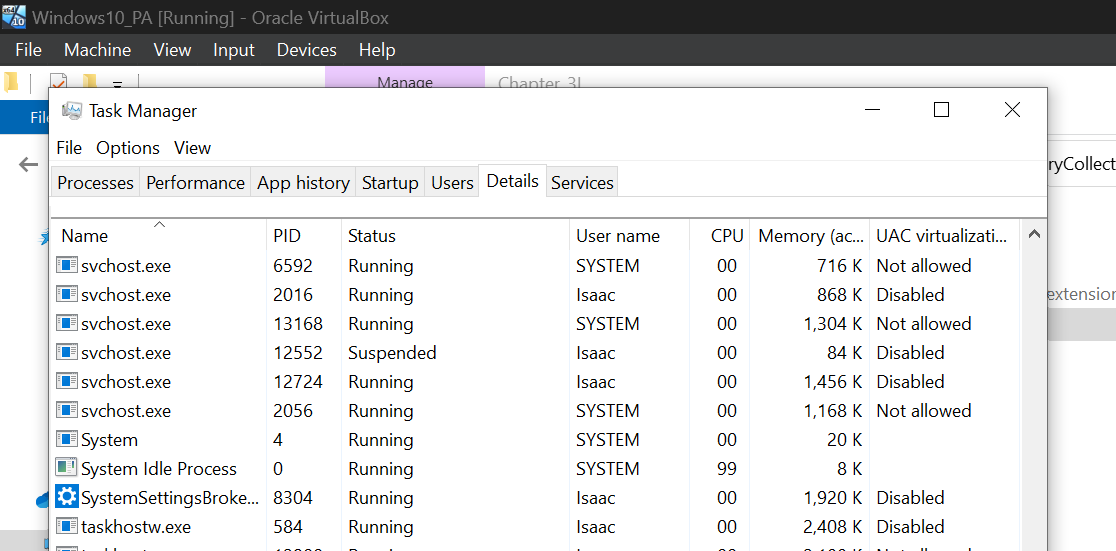
**Question 1**

What do you notice when monitoring this malware with Process Explorer?

**We notice that when the malware is run. The actual process is shown which then creates the child process and then removes itself leaving an orphan process.**

**Question 2**

Can you identify any live memory modifications?



**Question 3**

What are the malware’s host-based indicators?

**The host-based indicators for this malware is the file “practicalmalwareanalysis.log” presence on the system.**

**Question 4**

What is the purpose of this program?

**The purpose of this program is to log all of the keystrokes from the keyboard and then save them into the log file.**

**Lab 3-4**

This lab uses the file Lab03-04.exe. Analyse this using basic dynamic analysis tools.

**Question 1**

What happens when you run this file?

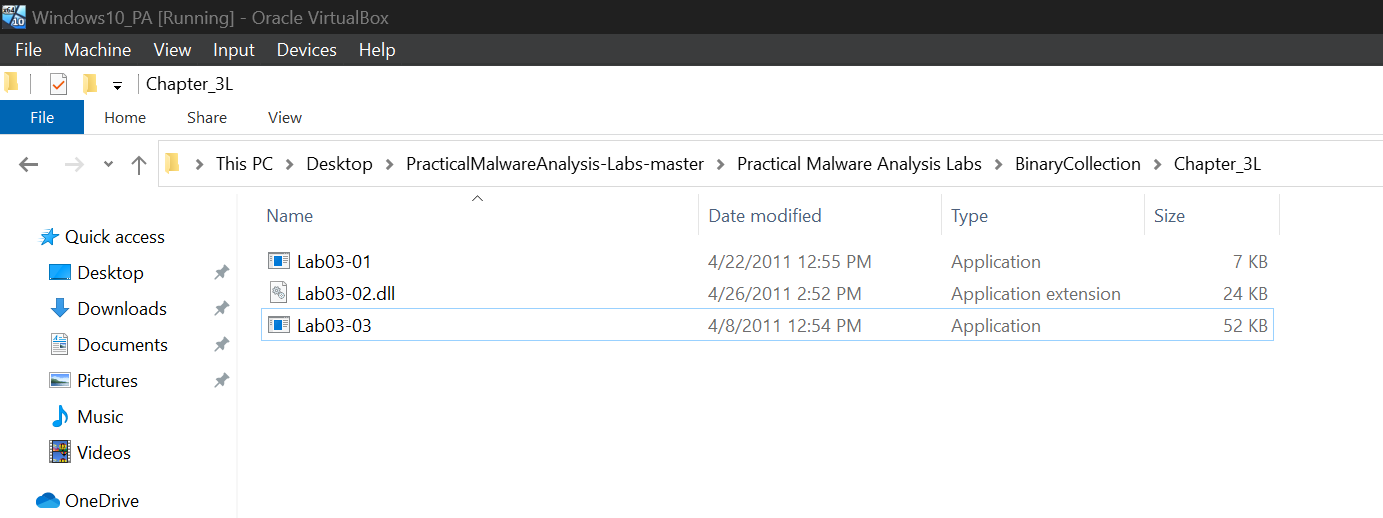
A black screen with white text

Description automatically generated

When we run the file. Process is created which opens up the CMD and then deleted the original executable after making it execute and hide itself somewhere else.

**Question 2**

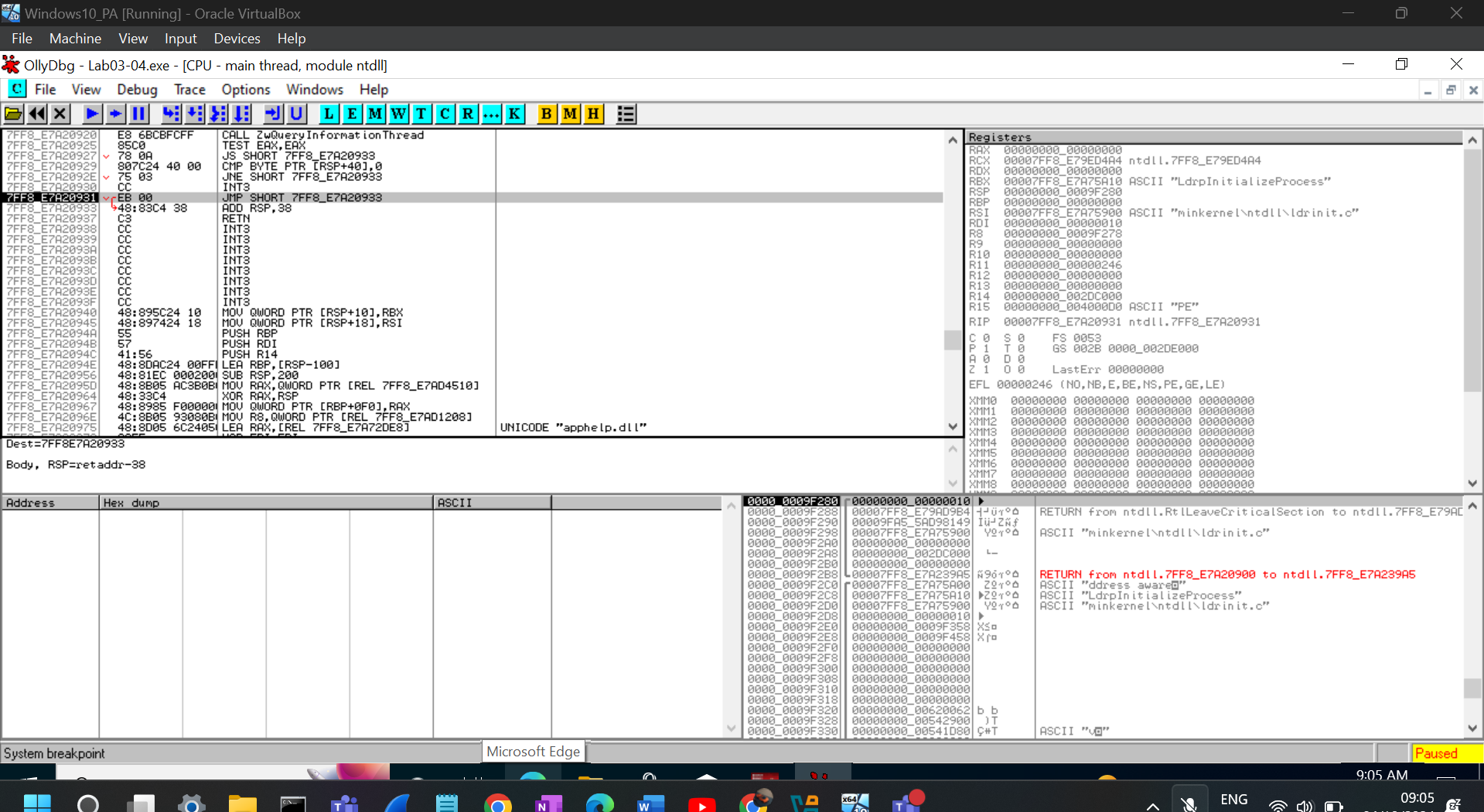
What is causing the roadblock in dynamic analysis?

The executable is evasive and trying to evade itself by checking whether the system is VM or not. AV-Detection etc. Obviously this will make it difficult to observer the file via dynamic analysis. 

**Question 3**

Are there other ways to run this program?

**The other ways can be to open this executable using IDA pro where we can analyze it in a more efficient way.**

****