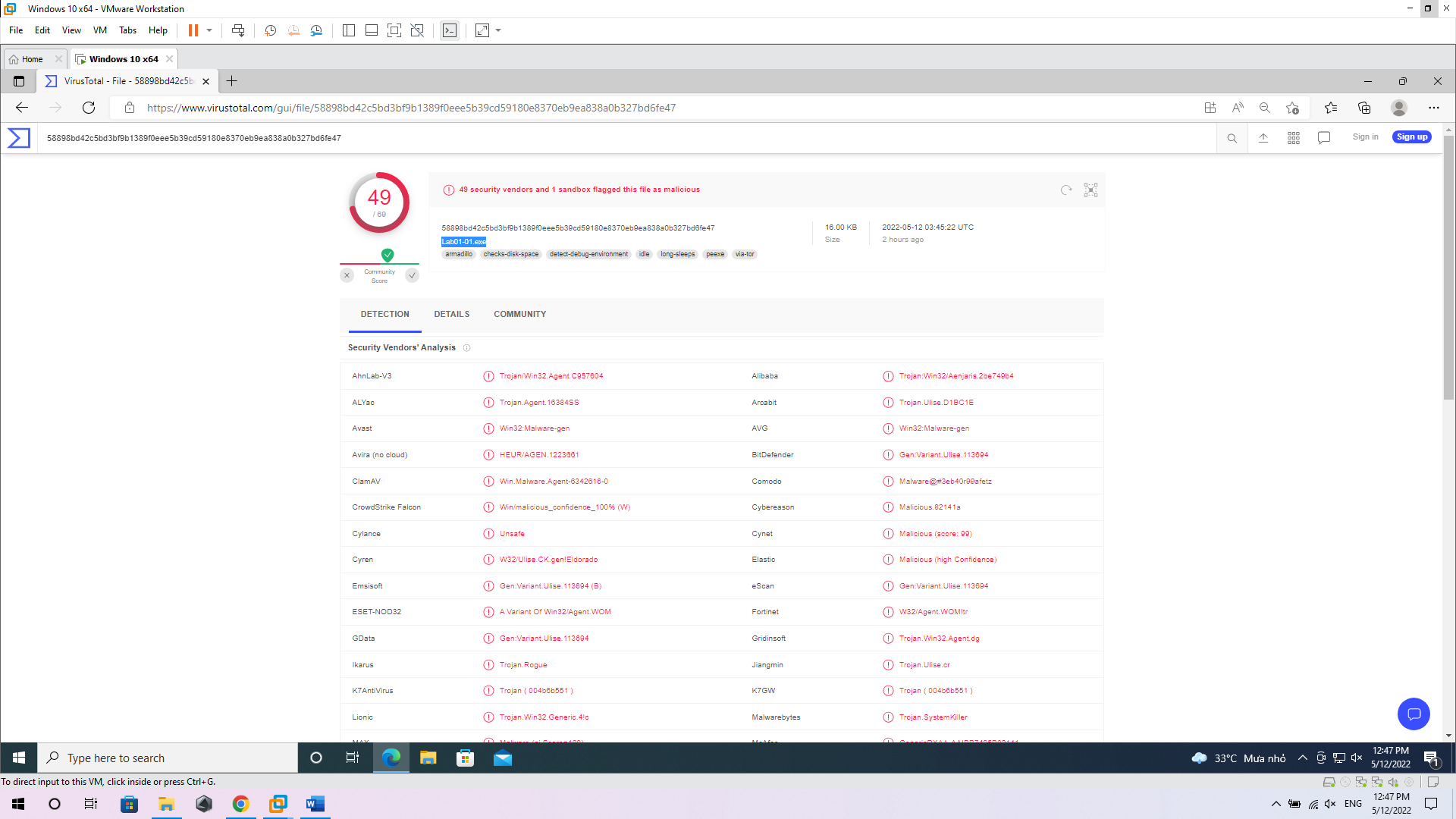
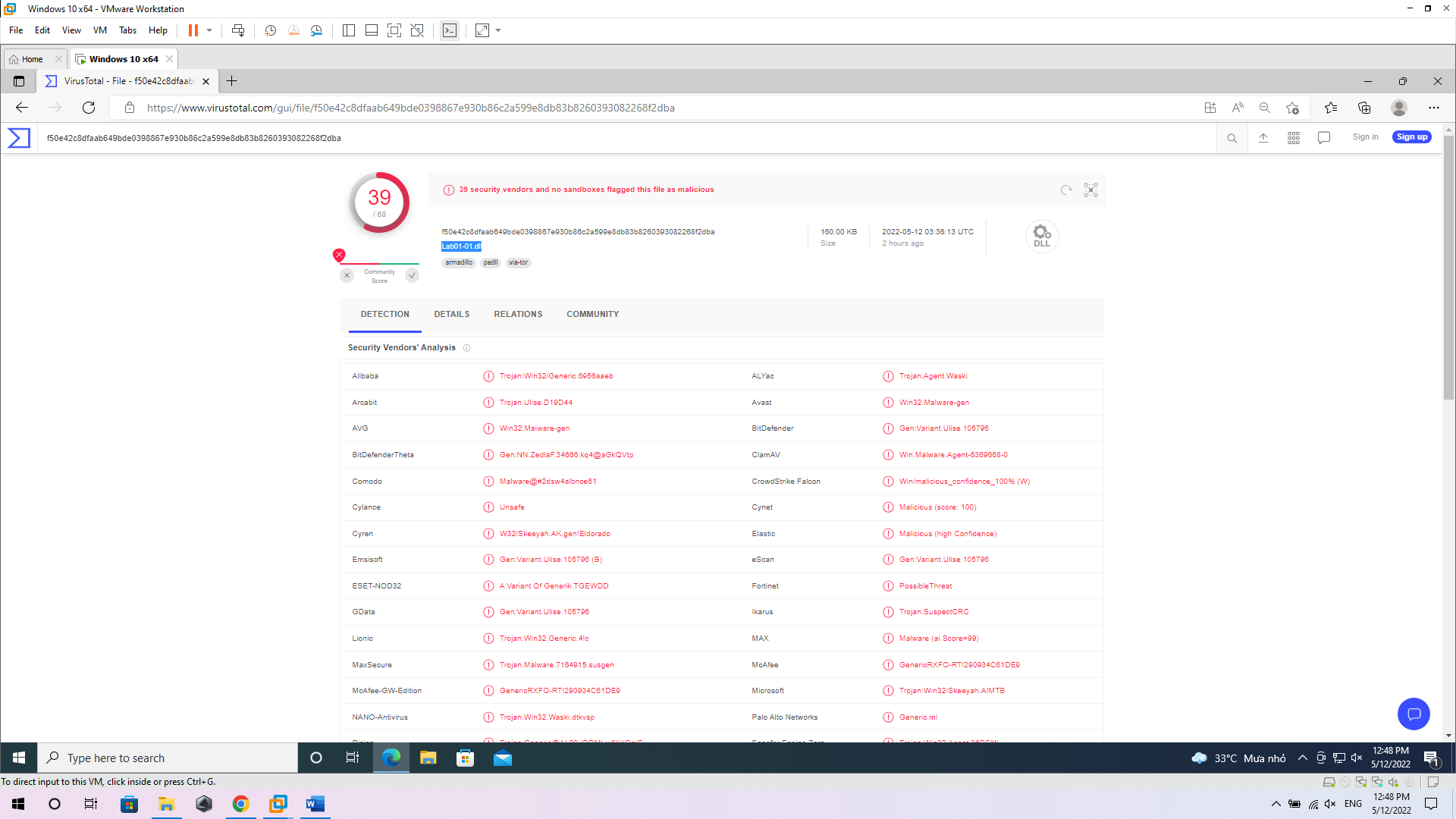
Lab 1-1

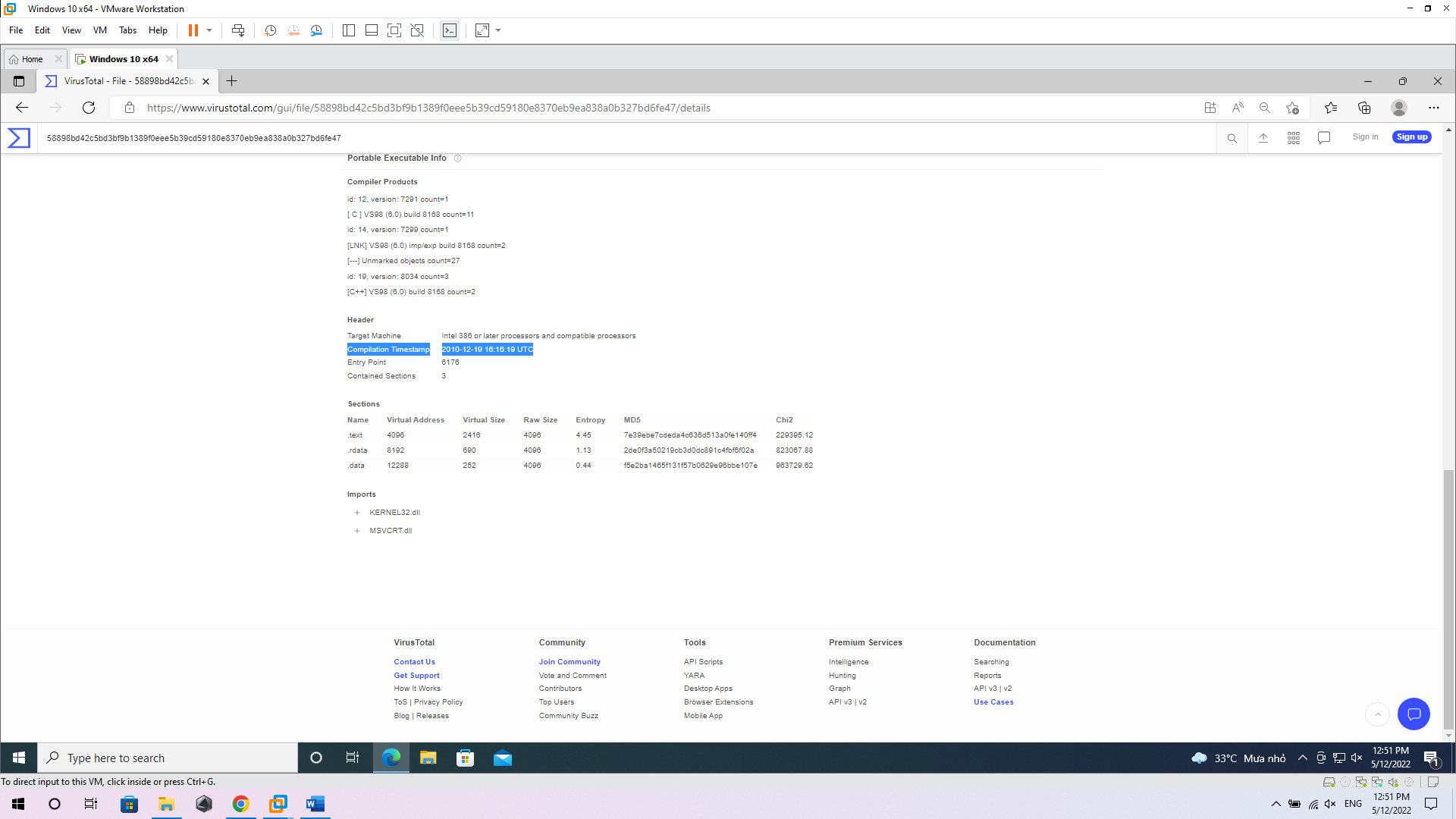
1. Upload:



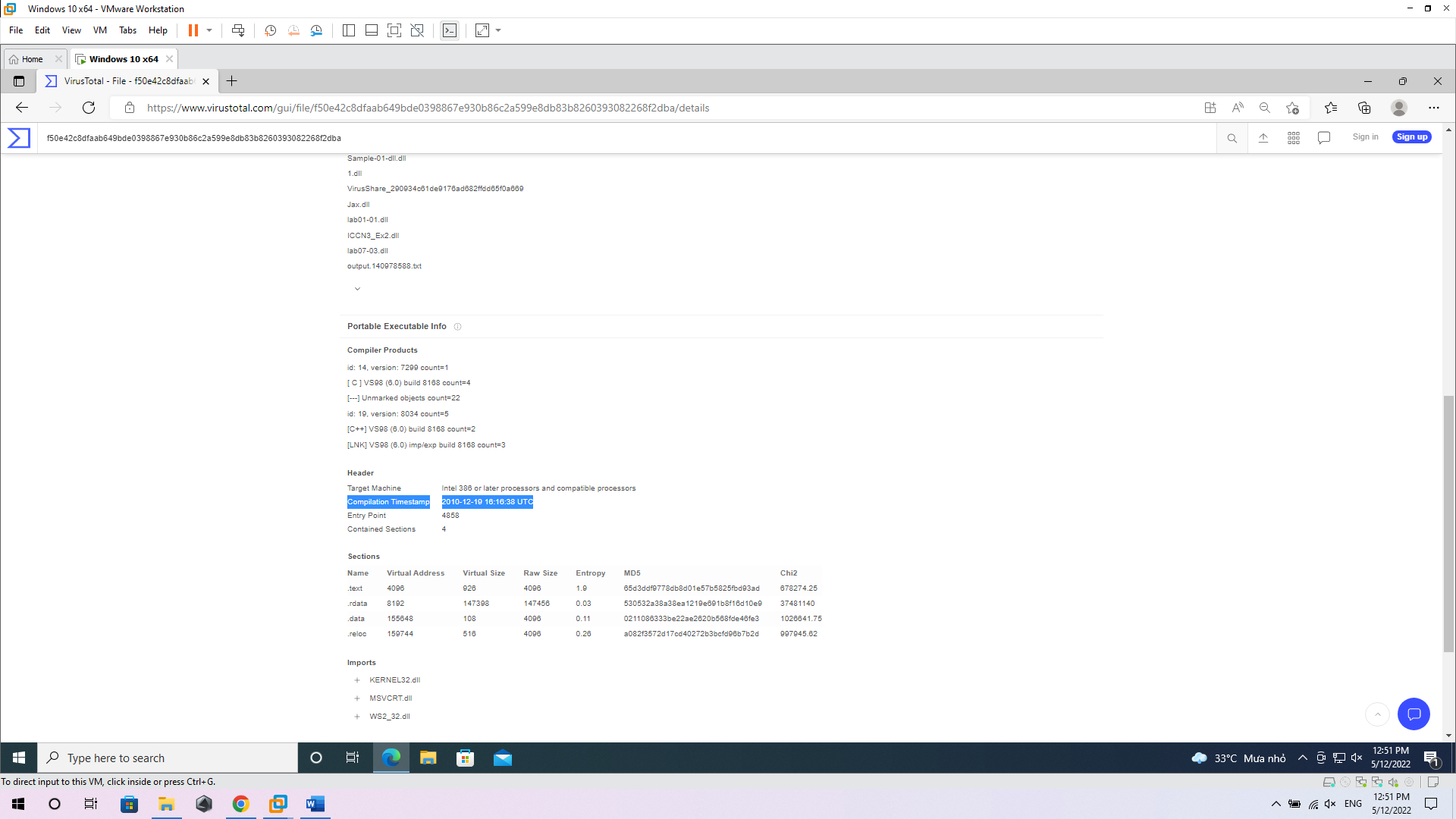


1. When were these files compiled?

Lab01-01.exe



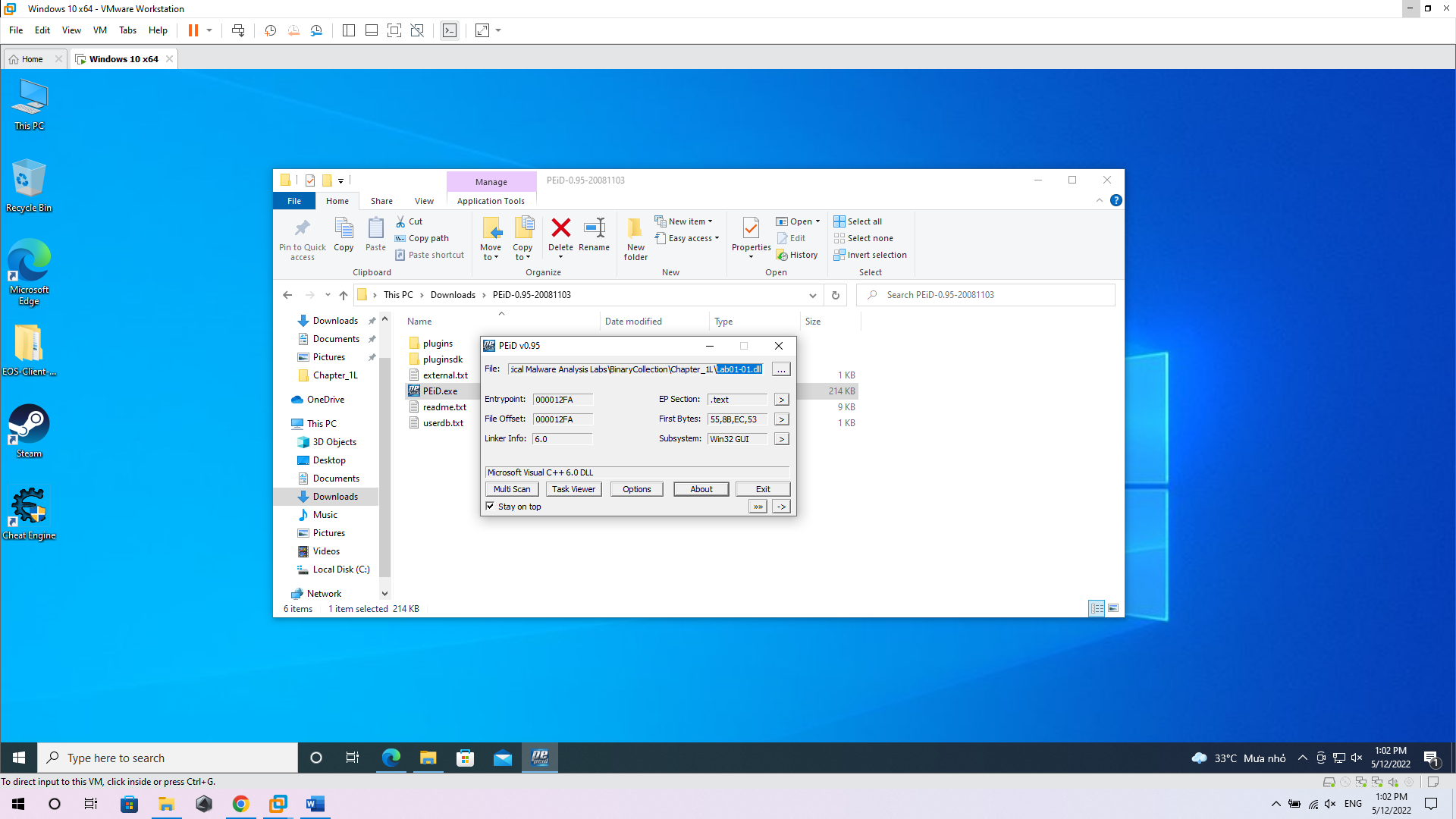
Lab01-01.dll

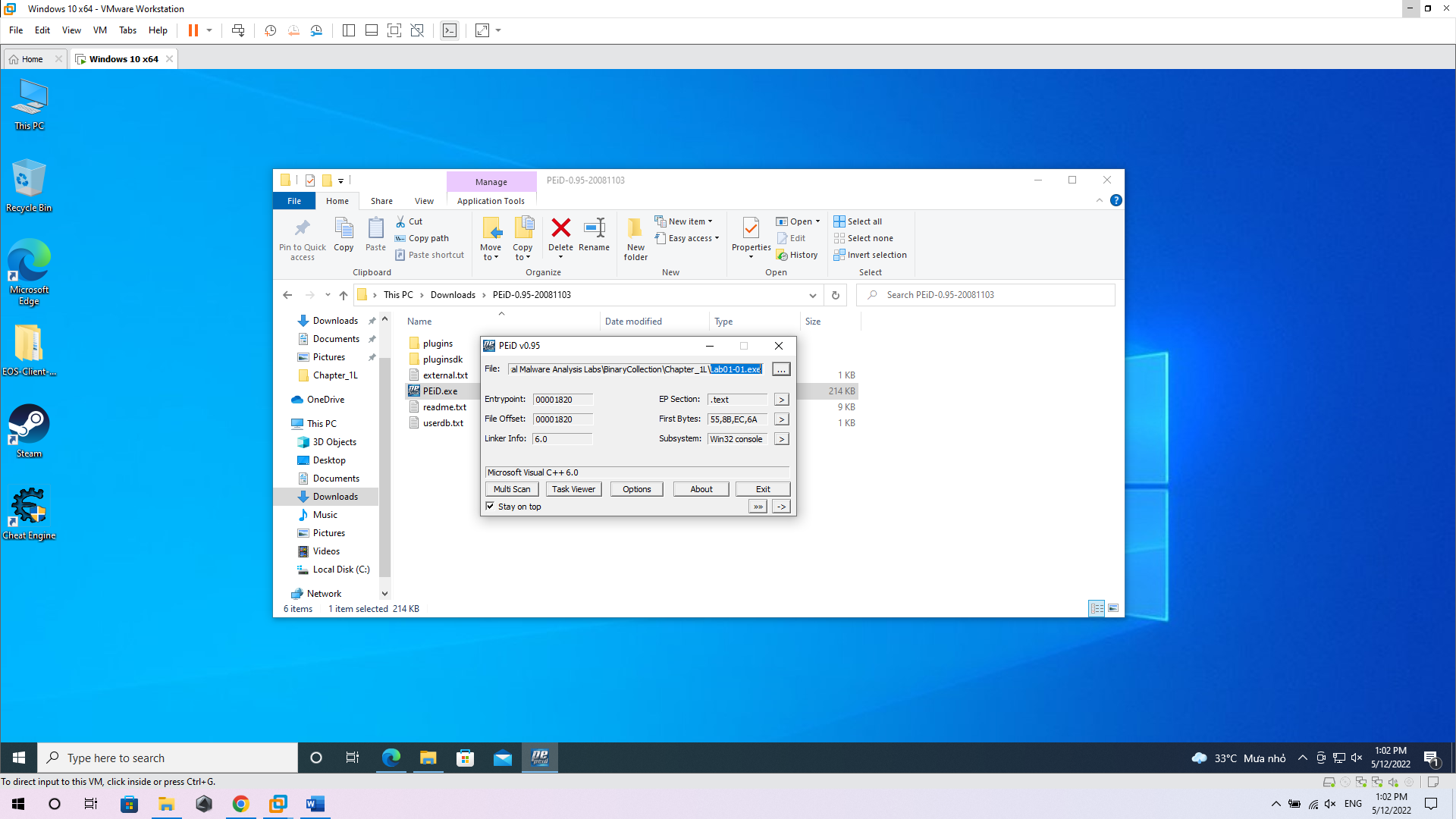


Lab01–01.exe → 2010–12–19 16:16:19

Lab01–01.dll → 2010–12–19 16:16:38

1. Are there any indications that either of these files is packed or obfuscated?





PEiD can be used to find the packed or obfuscated file although we were able to find all the necessary details and the strings. So we conclude that both of these files were not been packed or obfuscated.

1. Do any imports hint at what this malware does? If so, which imports are they?

**Lab01-01.exe:**

-FindFirstFileA and FindNextFileA give us an indication that this Malware might be looking for files.

-CreateFileA suggests that this Malware might create files.

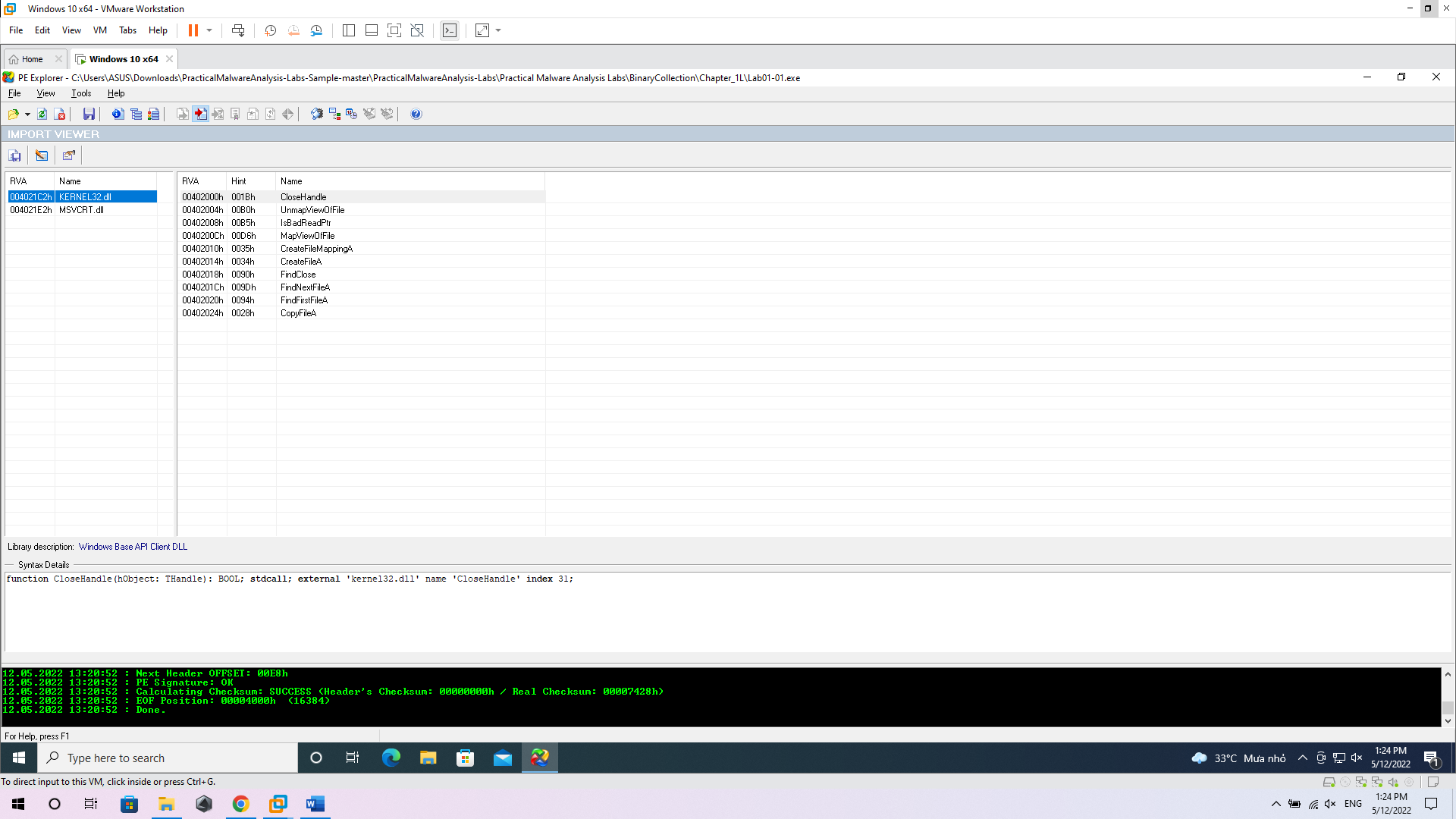
-CopyFileA suggests that this Malware might copy files.

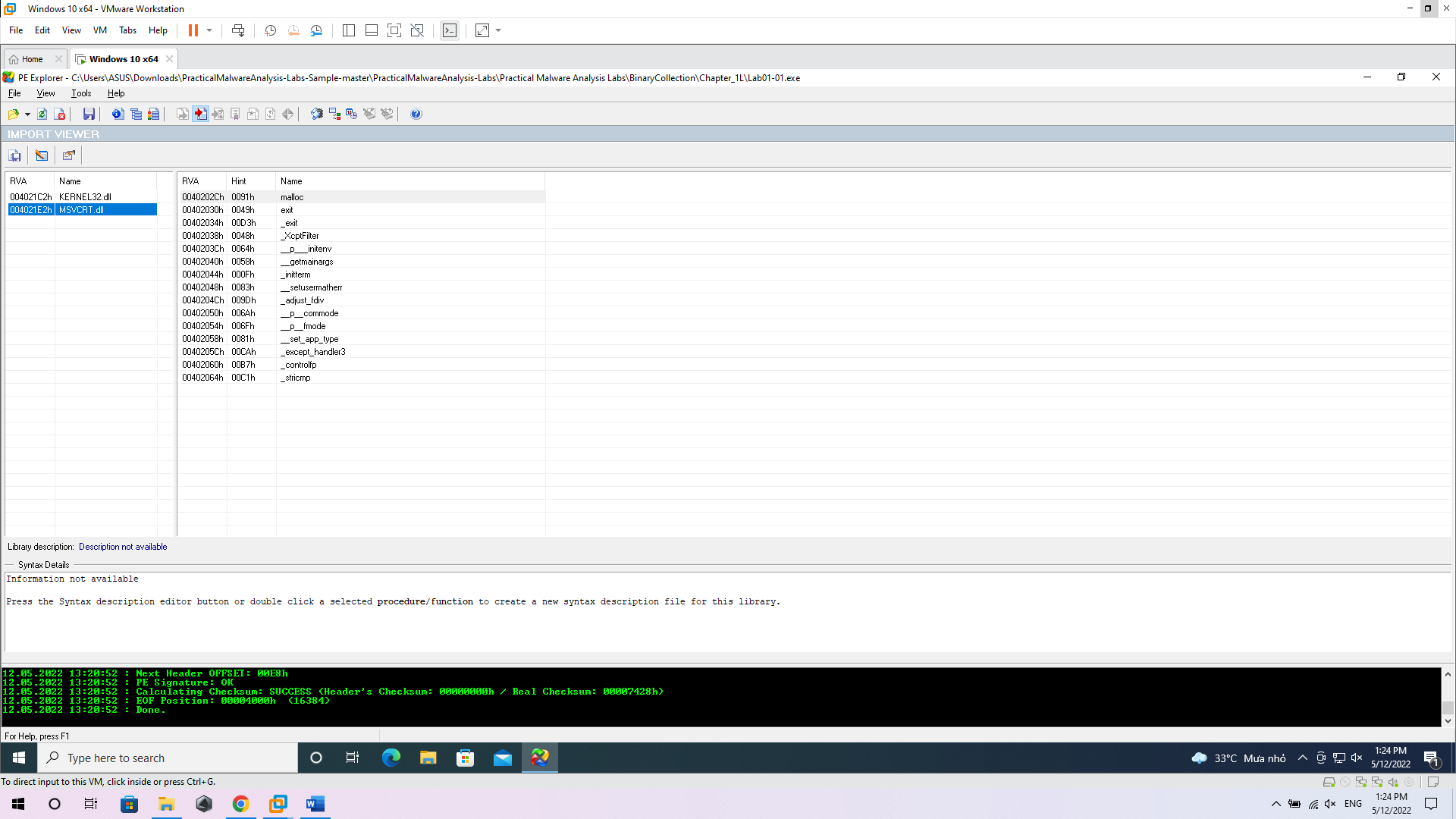
**Lab01-01.dll:**

-CreateProcessA gives the information that this Malware will probably create a Process.

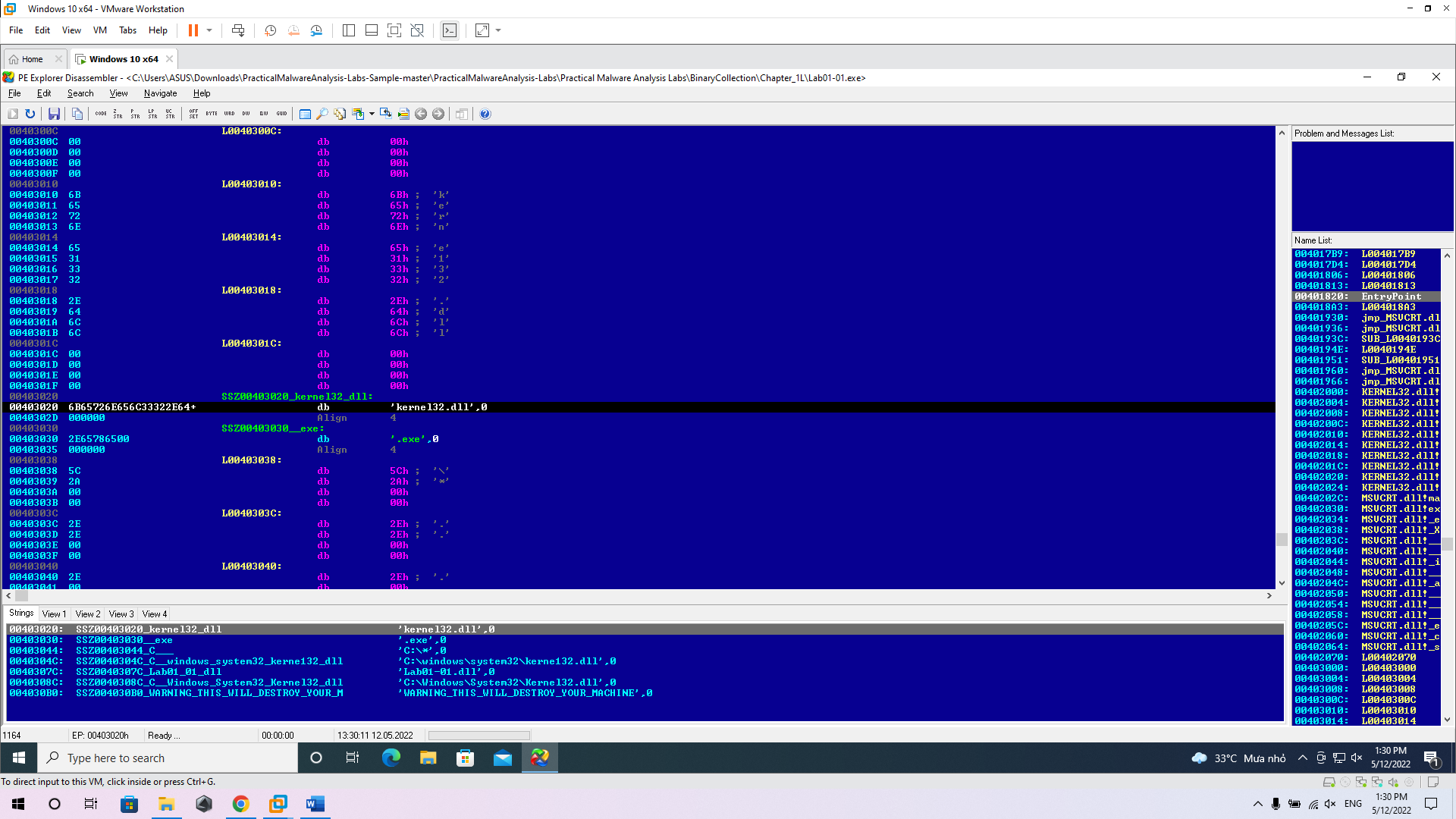
-The Malware imports functions from WS2\_32.dll such as socket, connect, send, recv, and closesocket which suggests that this Malware might communicate with a server.

-Also, the Sleep import might indicate that the Malware might wait sometime before executing any malicious activity.





1. Are there any other files or host-based indicators that you could look for on infected systems?



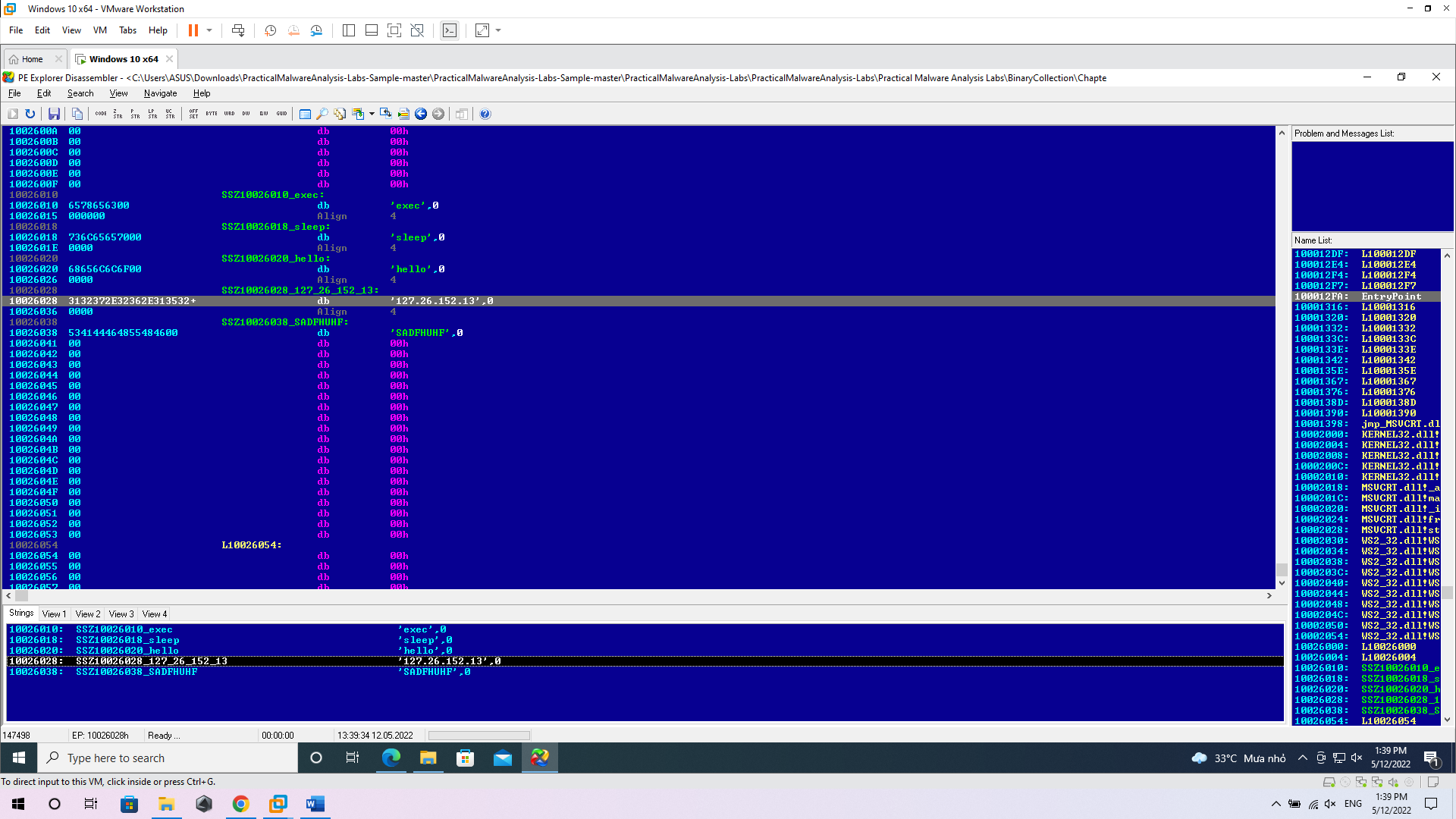
**Lab01-01.exe:**

This file has the string C:\windows\system32\kerne123.dll. This is probably an attempt to disguise the DLL as the legit kernel32.dll.

**Lab01-01.dll:**

There are no indicators.

1. What network-based indicators could be used to find this malware on infected machines?



**Lab01-01.exe:**

There are no indicators.

**Lab01-01.dll:**

There’s a string containing an IP Address: 127.26.152.13

1. What would you guess is the purpose of these files?

**Lab01-01.exe:**

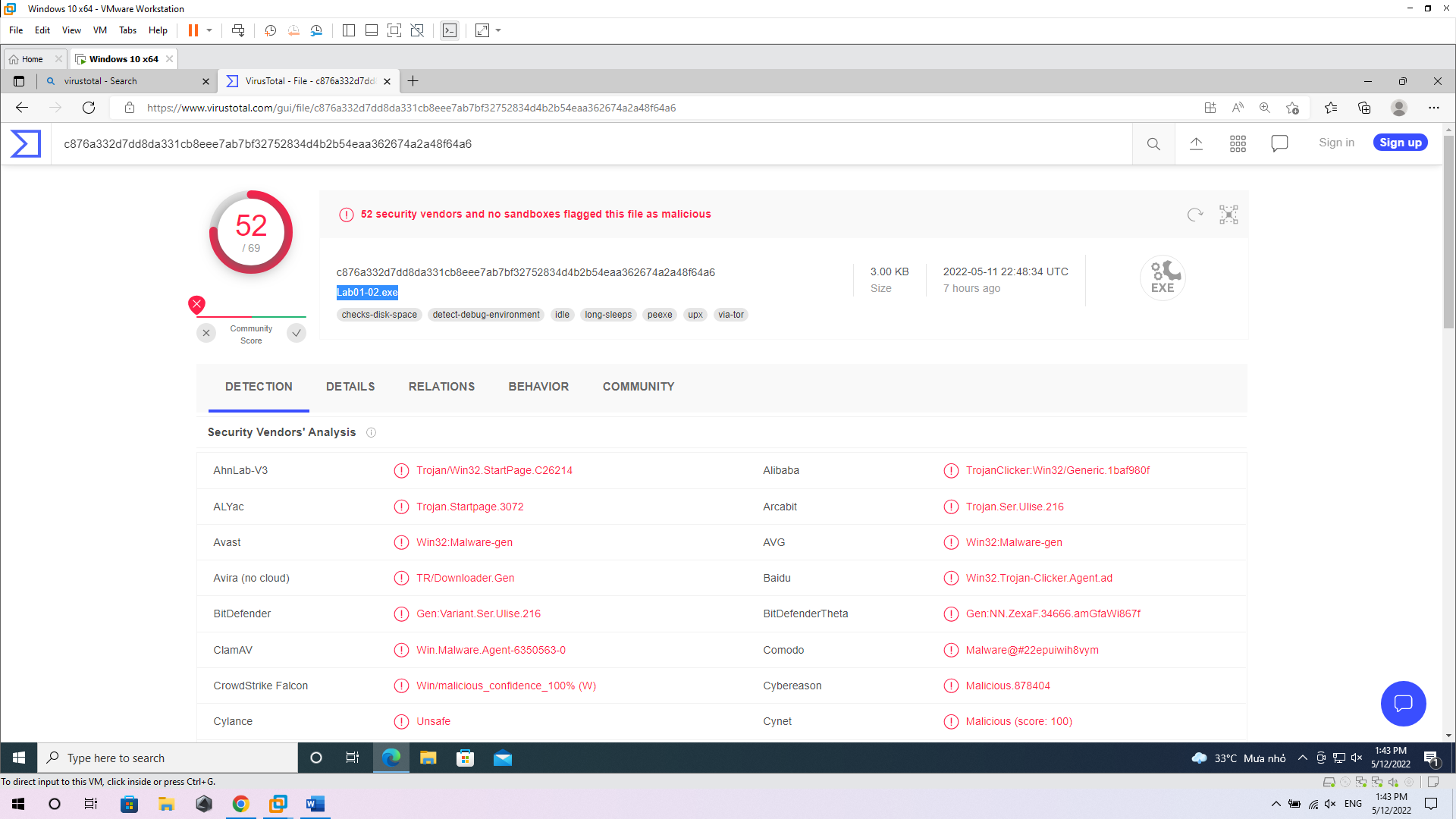
The purpose is to run the DLL.

**Lab01-01.dll:**

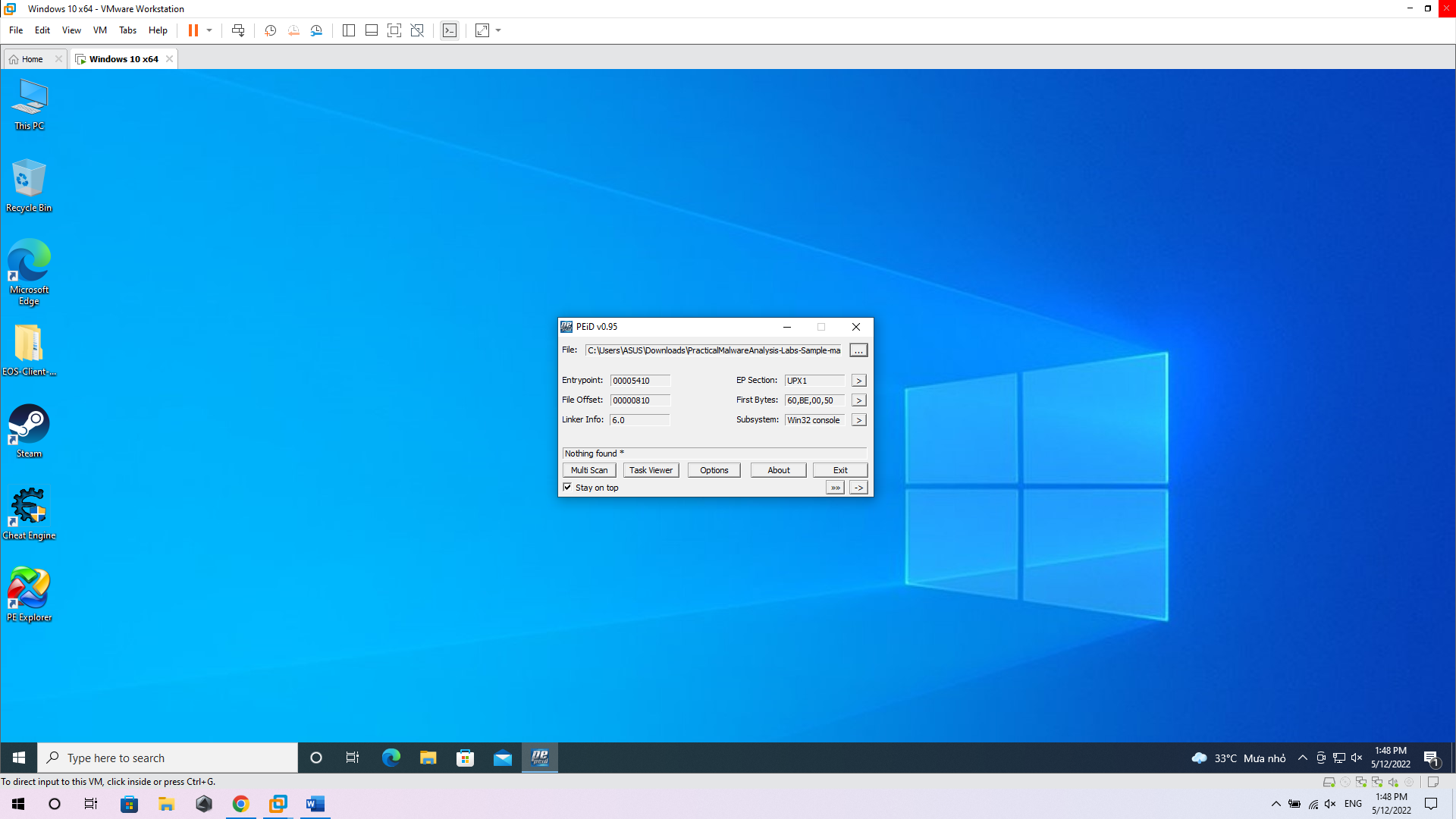
Probably a backdoor.

Lab 1-2

1. Upload



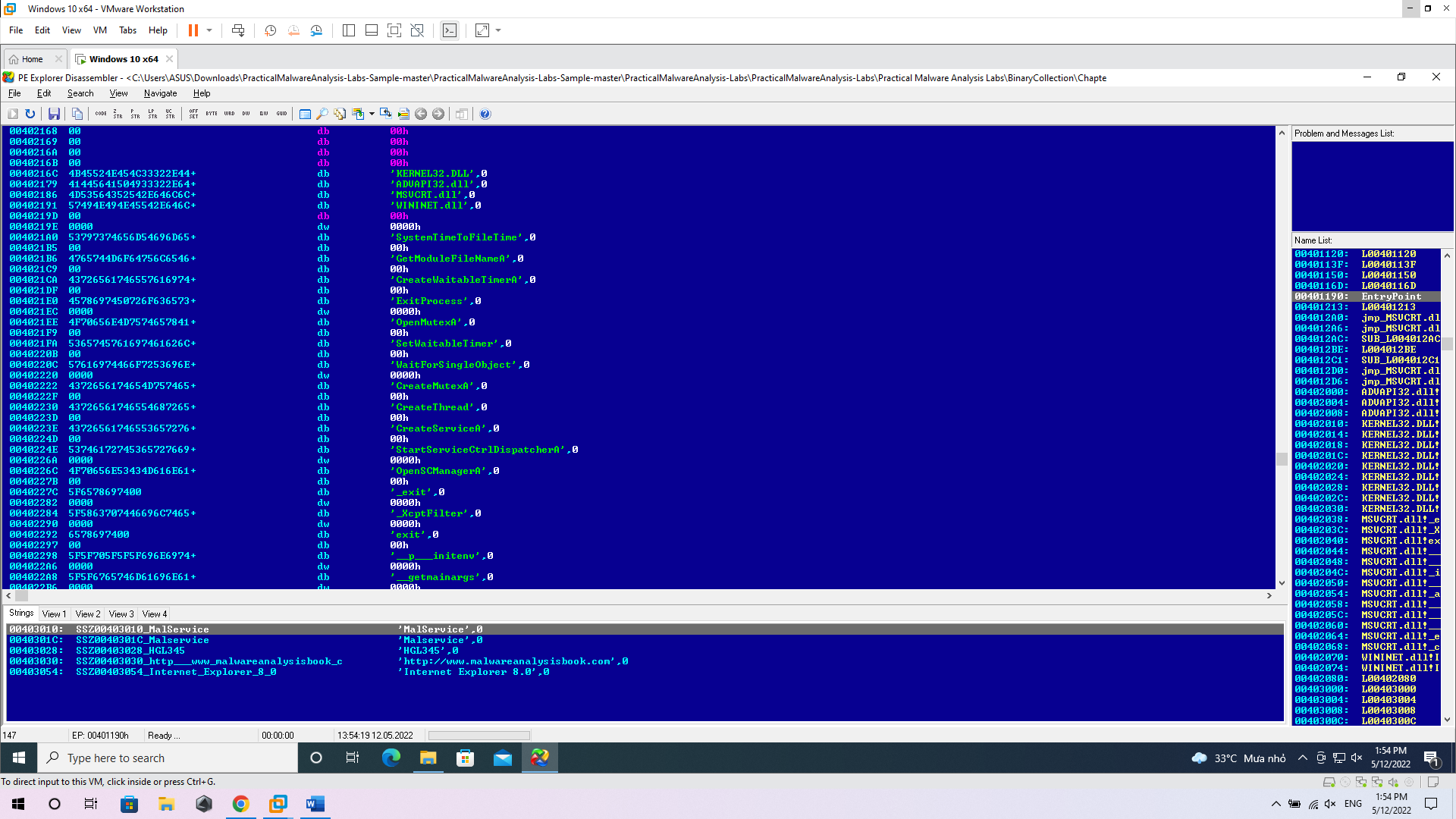
1. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.



We can unpack it running UPX: upx –o Lab01-02\_unpacked.exe –d Lab01-02.exe

1. Do any imports hint at this program’s functionality? If so, which imports are they and what do they tell you?

The imports of the Unpacked version hint that this Malware has the ability to perform external connections (InternetOpenA and InternetOpenUrlA), also the malware creates a Service (CreateServiceA).



1. What host- or network-based indicators could be used to identify this malware on infected machines?

We can look for the service named MalService via services.msc also we can check for the dnslookups for <http://malwareanalysisbook.com/> via a specific Internet Explorer string which will be passed via the browser user-agent FIELD. Moreover we can create a firewall rule to block such traffic.