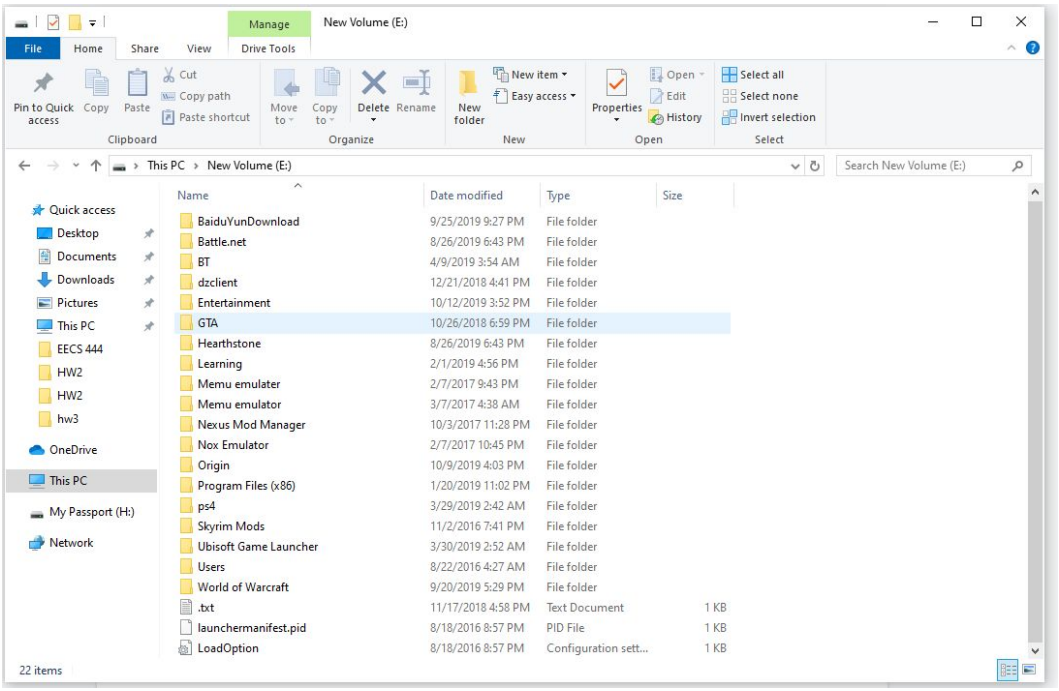
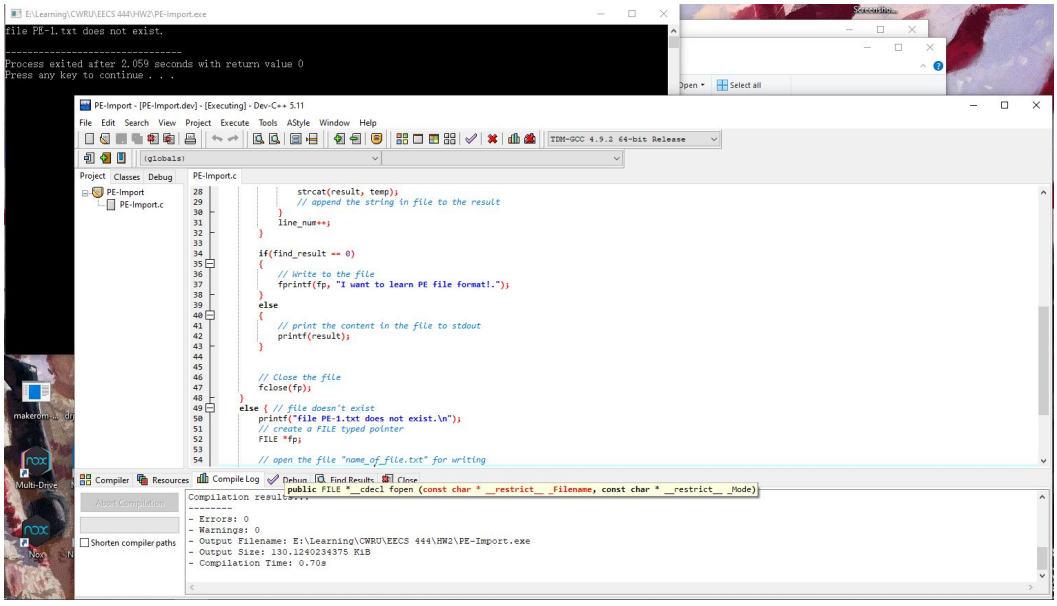
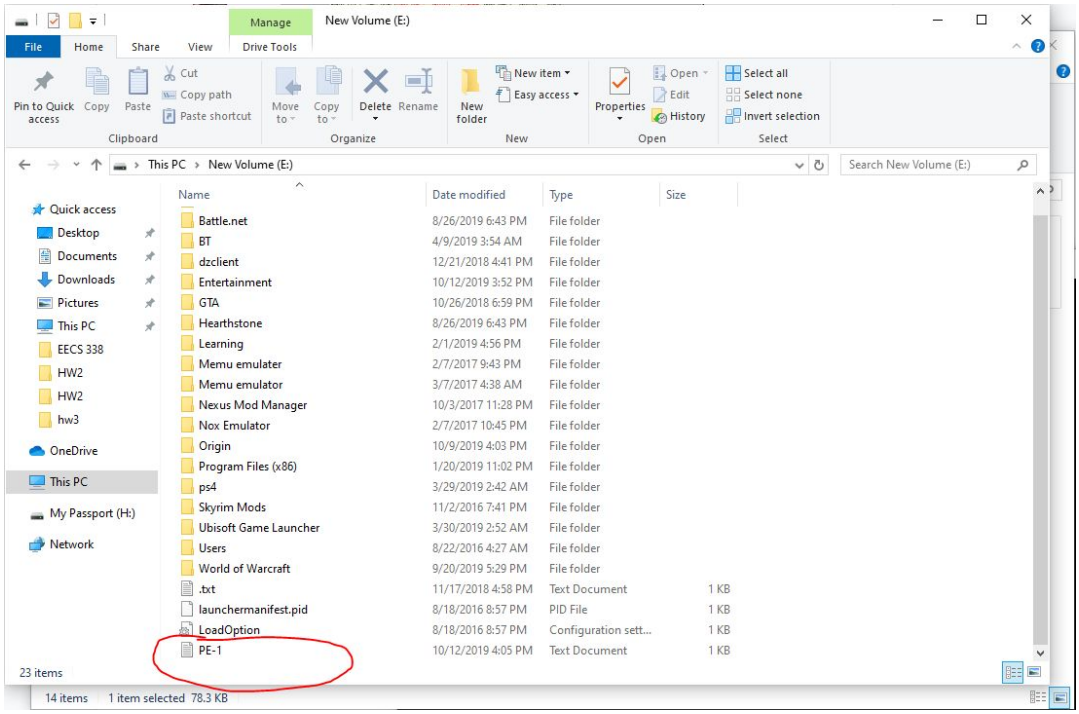
Because I do not have permission to write in the root directory, instead of creating the “PE-1.txt” in the root directory, my program creates a text file in another directory.

Step 1.1: Before we compile and execute the “PE-Import.c”, there is no “PE-1.txt” in this directory.

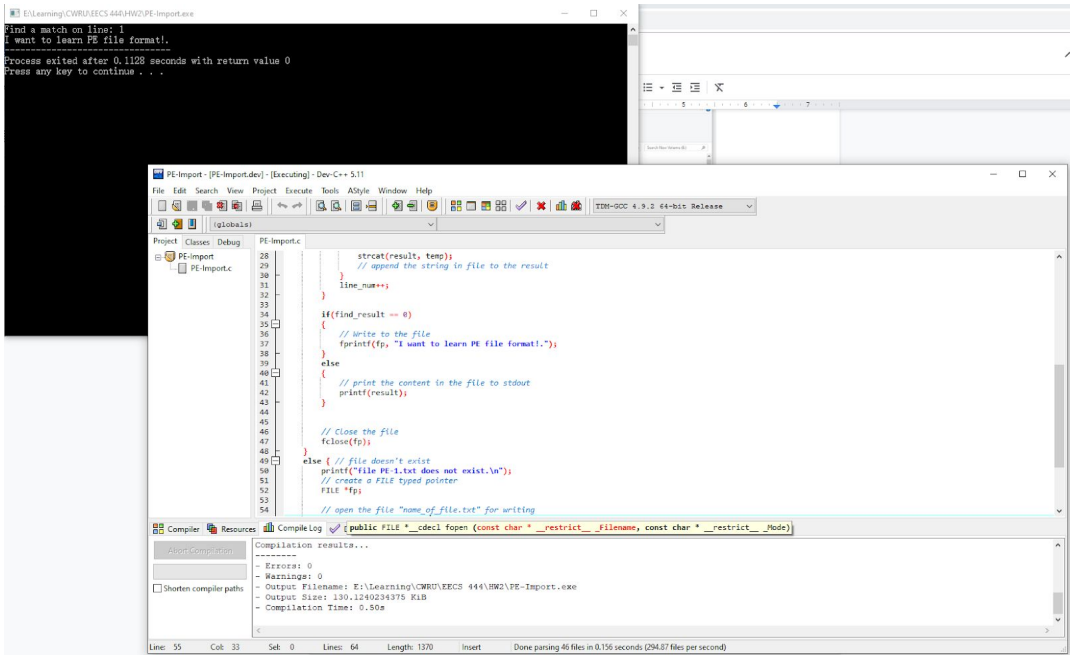


Step 1.2: The program prints out “file PE-1.txt does not exist” to Stdout and creates a “PE-1.txt” in this directory.

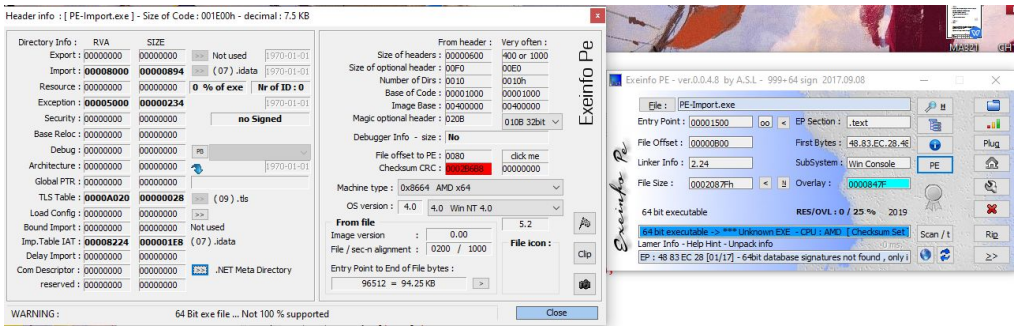




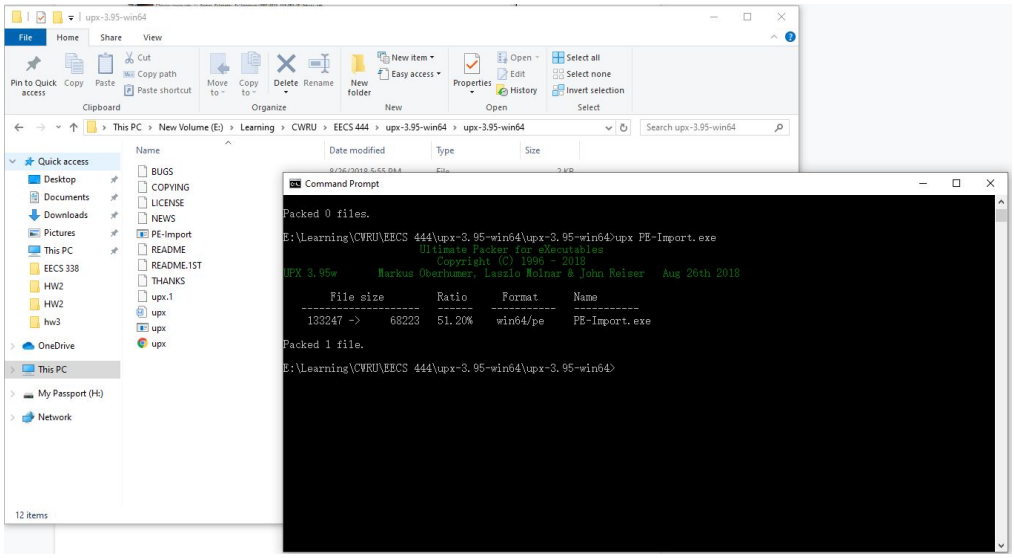
Step 1.3: The program will print out the content “I want to learn PE file format” to Stdout if the “PE-1.txt” is already exist in this directory.



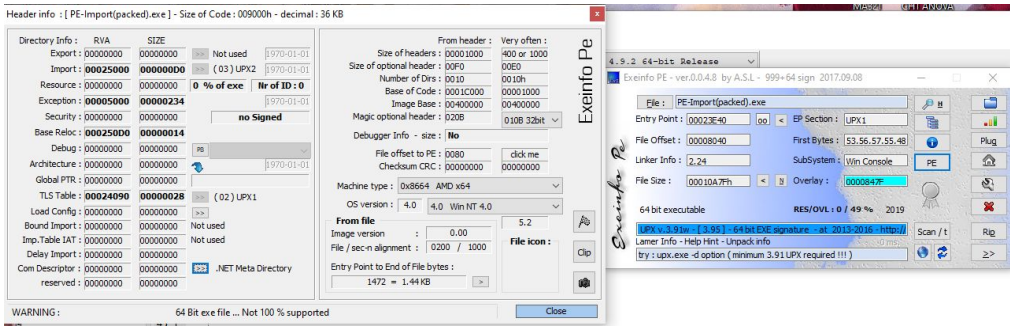
Step 2.1: Use Exeinfo PE to check the content in the Import Table for program “PE-Import.exe”.



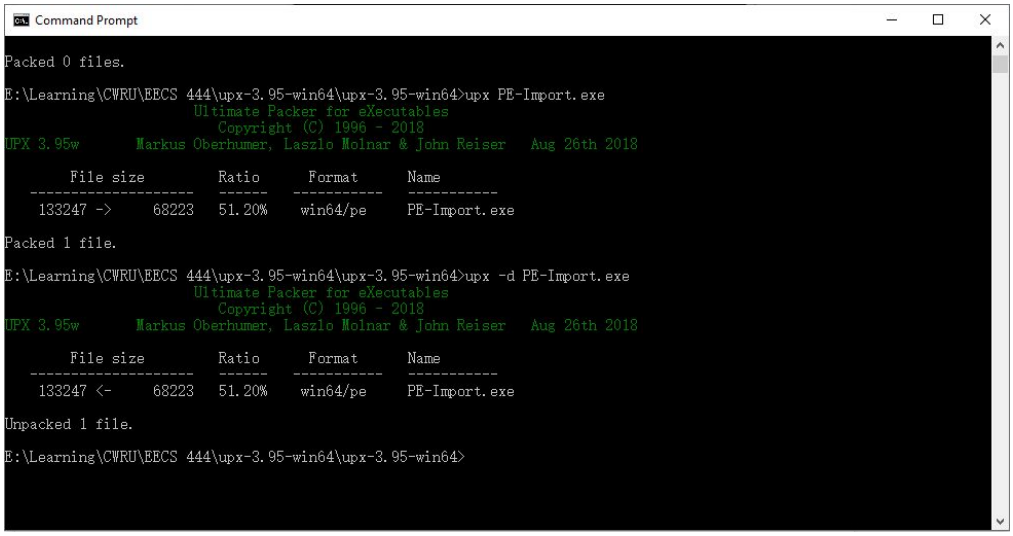
Step 3.1: Use UPX to pack the PE-Import.exe.



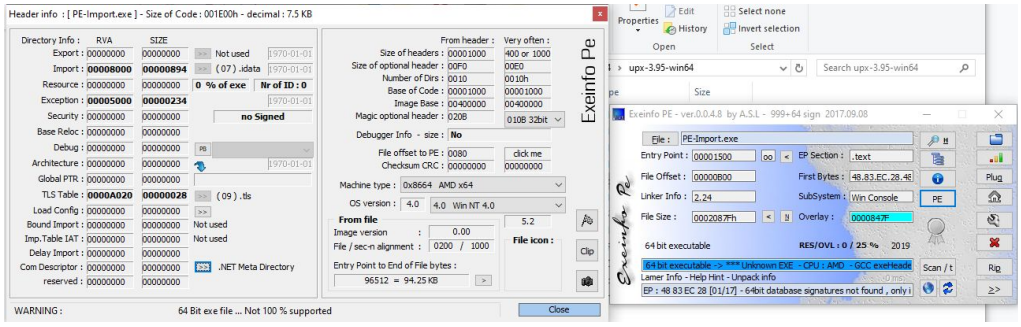
Step 3.2: Use Exeinfo PE to check the content in the Import Table for packed “PE-Import.exe”.



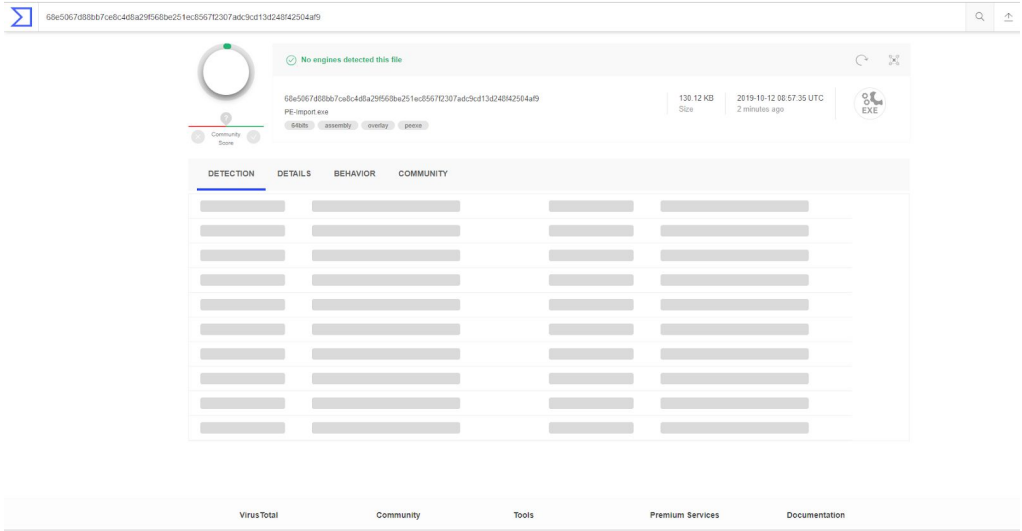
Step 3.3: Use UPX to unpack the PE-Import.exe.



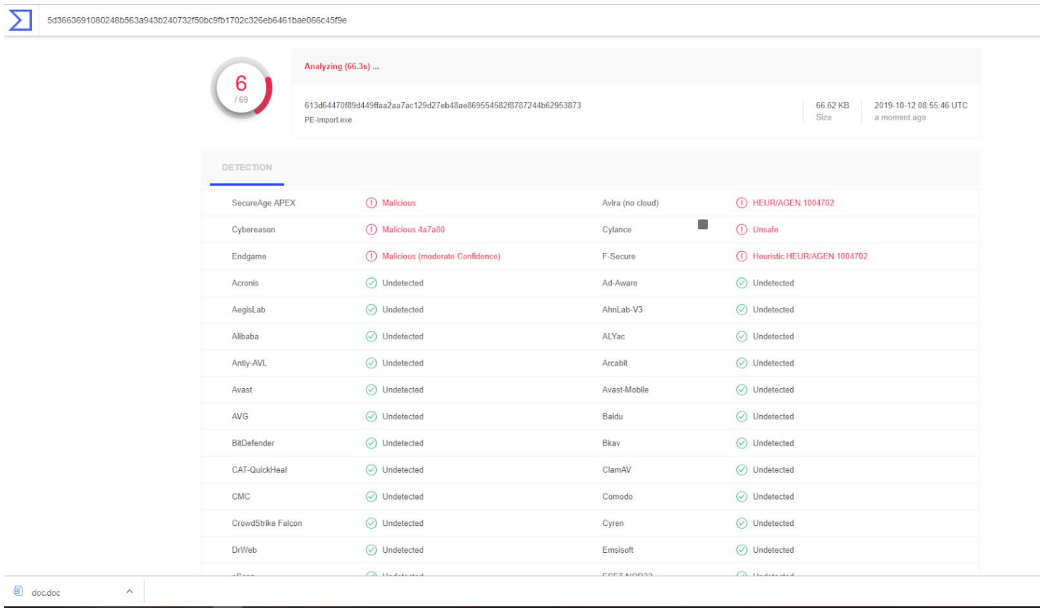
Step 3.4: Use Exeinfo PE to check the content in the Import Table for unpacked "PE-Import.exe".



Step 4.1: The result of anti-malware scanner for "PE-Import" before using any technique.



Step 4.2: The result of anti-malware scanner for "PE-Import" by using packing.


5d3663691080248b563a943b240732f50bc9fb1702c326eb6461bae066c45f9e
6
/ 69
Analyzing (66.3s) ...
613d64470f89d449ffaa2aa7ac129d27eb48ae8695545828787244b62953873
PE-Import.exe
66.62 KB
Size
2019-10-12 08:55:46 UTC
a moment ago
DETECTION
SecureAge APEX
Malicious
Avira (no cloud)
HEUR/AGEN.1004702
Cybereason
Malicious.4a7a80
Cylance
Unsafe
Endgame
Malicious (moderate Confidence)
F-Secure
Heuristic.HEUR/AGEN.1004702
Acronis
Undetected
Ad-Aware
Undetected
AegisLab
Undetected
AhnLab-V3
Undetected
Alibaba
Undetected
ALYac
Undetected
Antiy-AVL
Undetected
Arcabit
Undetected
Avast
Undetected
Avast-Mobile
Undetected
AVG
Undetected
Baidu
Undetected
BitDefender
Undetected
Bkav
Undetected
CAT-QuickHeal
Undetected
ClamAV
Undetected
CMC
Undetected
Comodo
Undetected
CrowdStrike Falcon
Undetected
Cyren
Undetected
DrWeb
Undetected
Emsisoft
Undetected
doc.doc