PROJECT

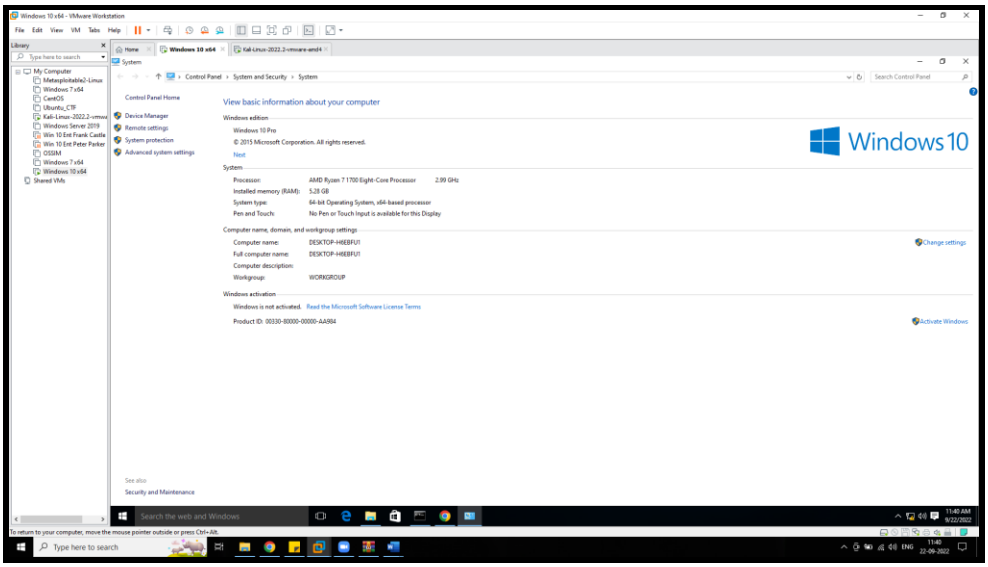
Mayank Rahalkar

Table of Contents

Table of Contents 2
Part 1 – Creation of Analysis Station 3
Part 2 – Basic Static Analysis of unknown binary files 3
Part 3 – Basic Dynamic Analysis of unknown binary files 12

Part 1 – Creation of Analysis Station

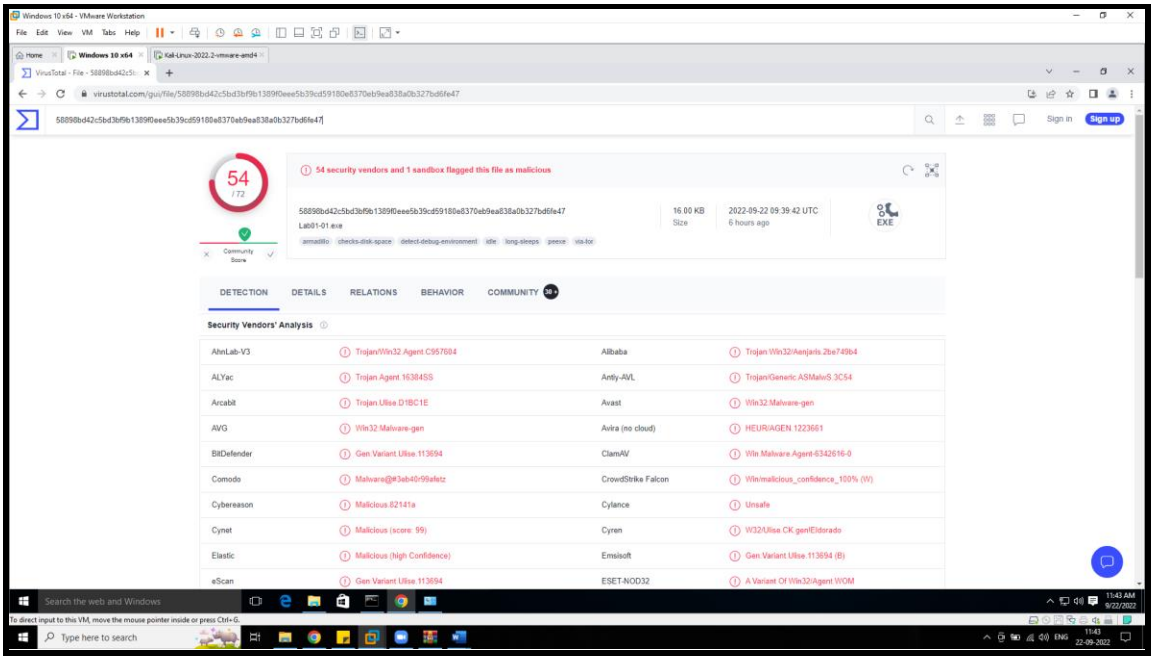
I deployed a Windows 10 VM in VMWare Workstation Pro. The specifications and configurations of the VM are shown in the screenshot below.



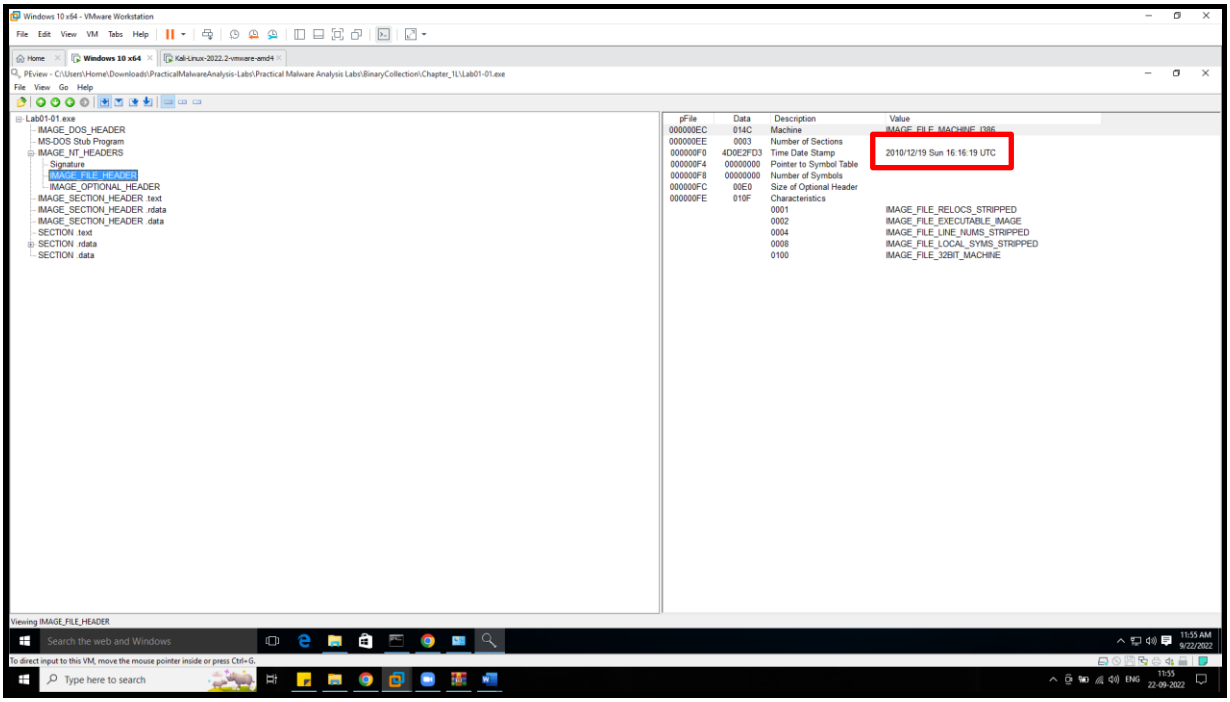
Part 2 – Basic Static Analysis of unknown binary files

1)

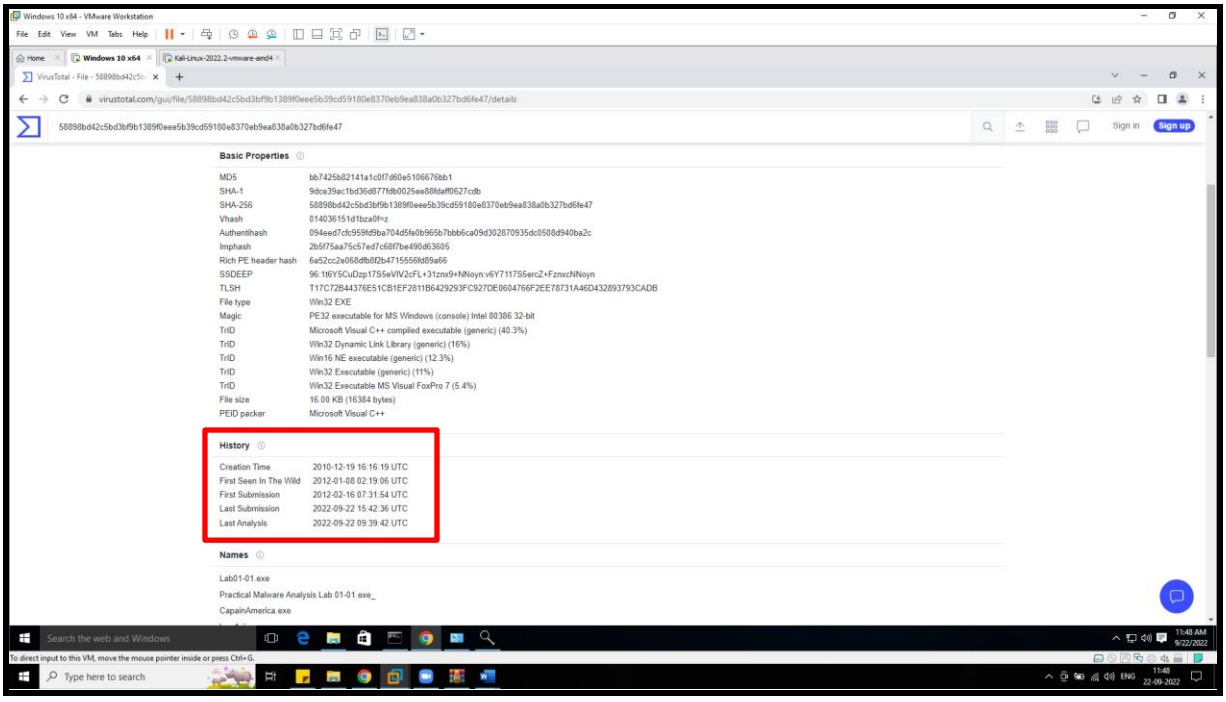
The below screenshot shows the report of Virus Total for Lab01-01.exe. It shows that malware signature has been identified by multiple sites.



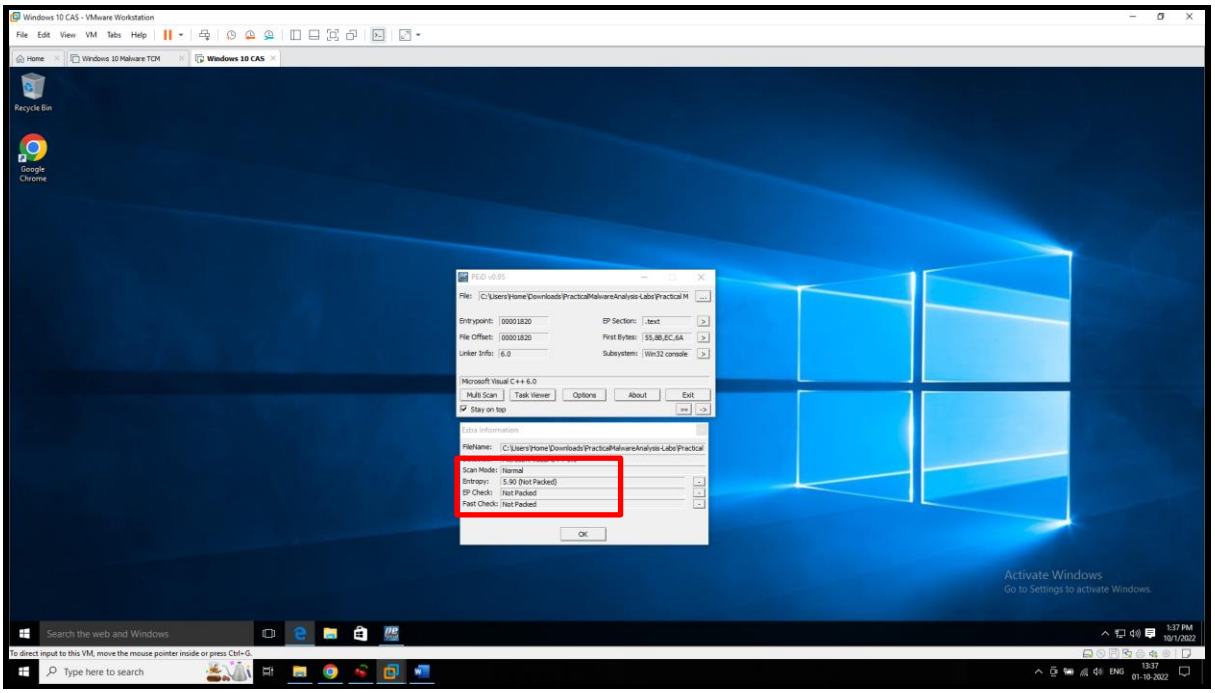
The below screenshot shows the compilation time of the malware Lab01-01.exe. The tool used is PE-View



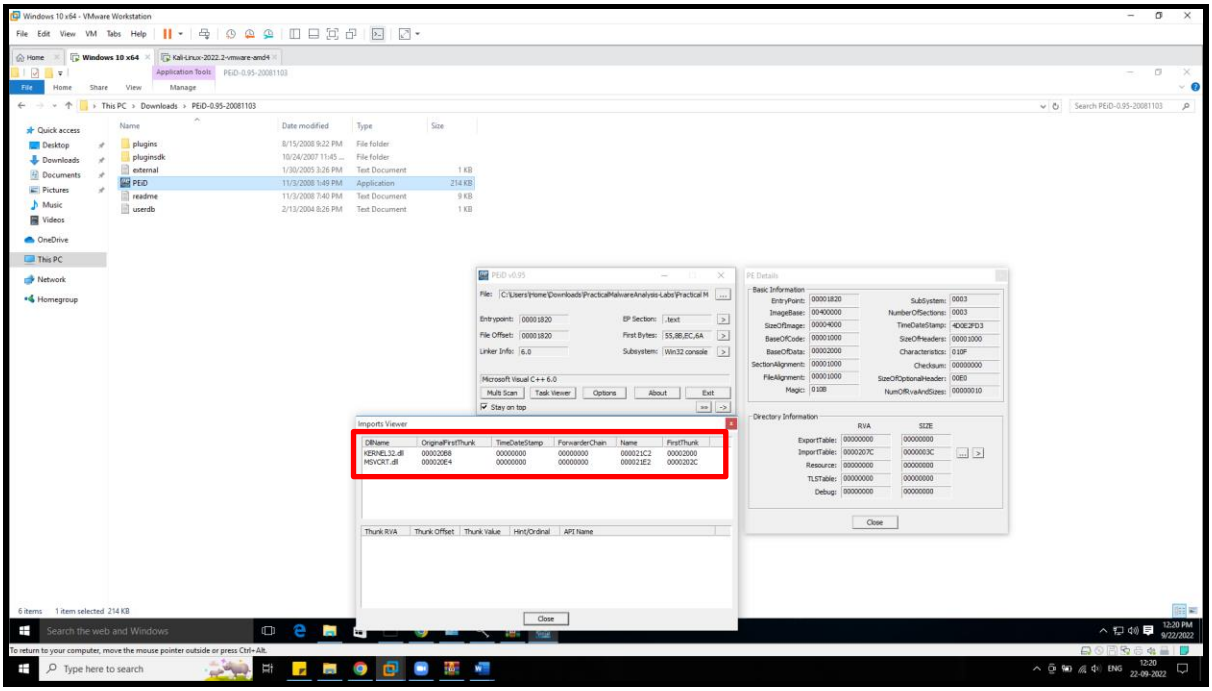
The below screenshot shows the compilation time of the malware Lab01-01.exe in Virus Total



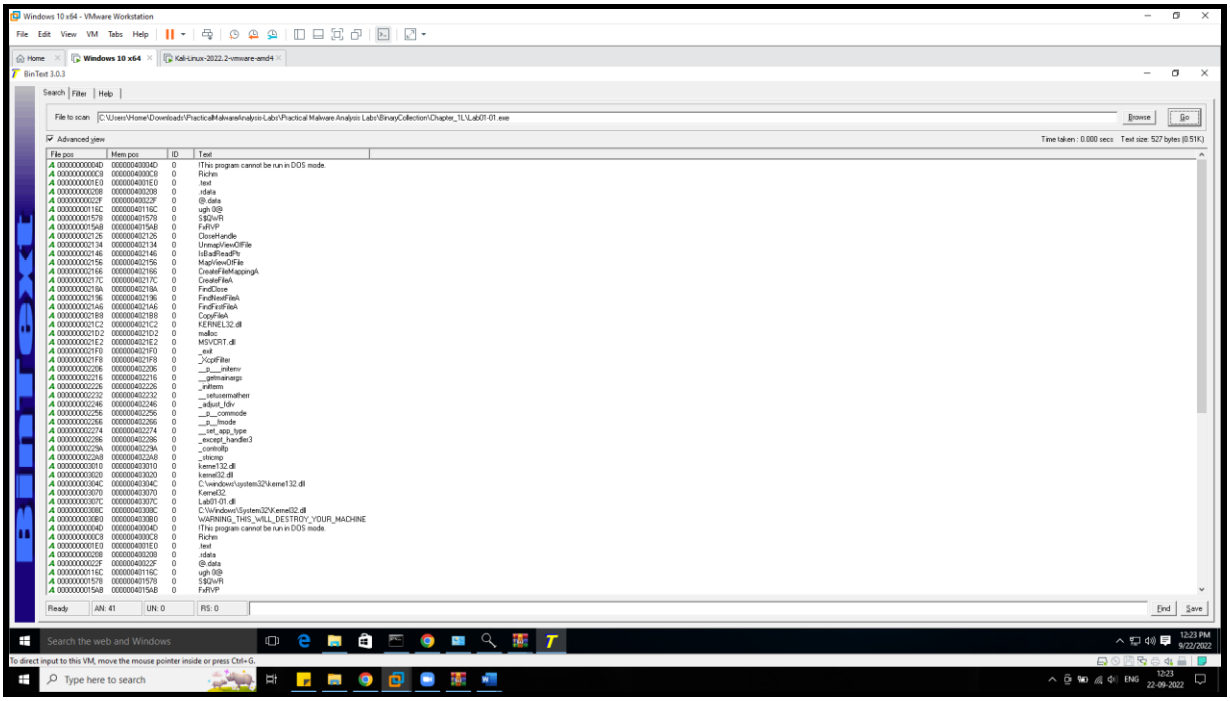
The below two screenshot shows that the binary is not packed.



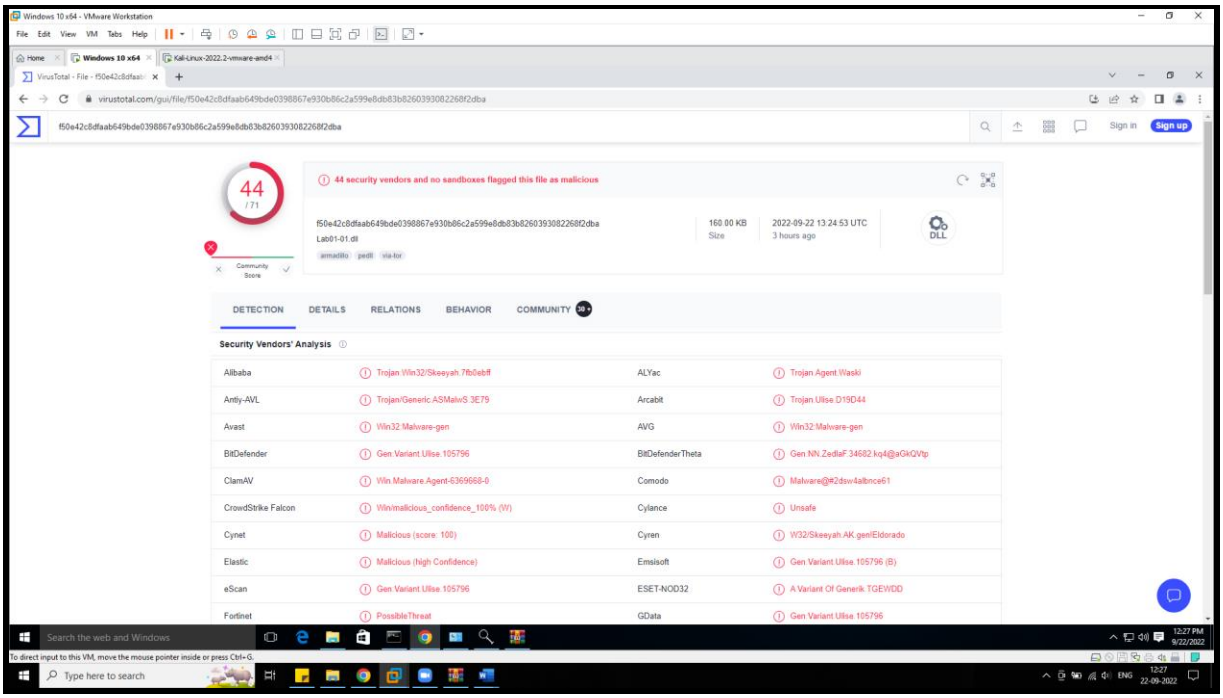
By analyzing the binary in PEiD, we can see that there are two imports: KERNEL32.dll and MSVCRT.dll.



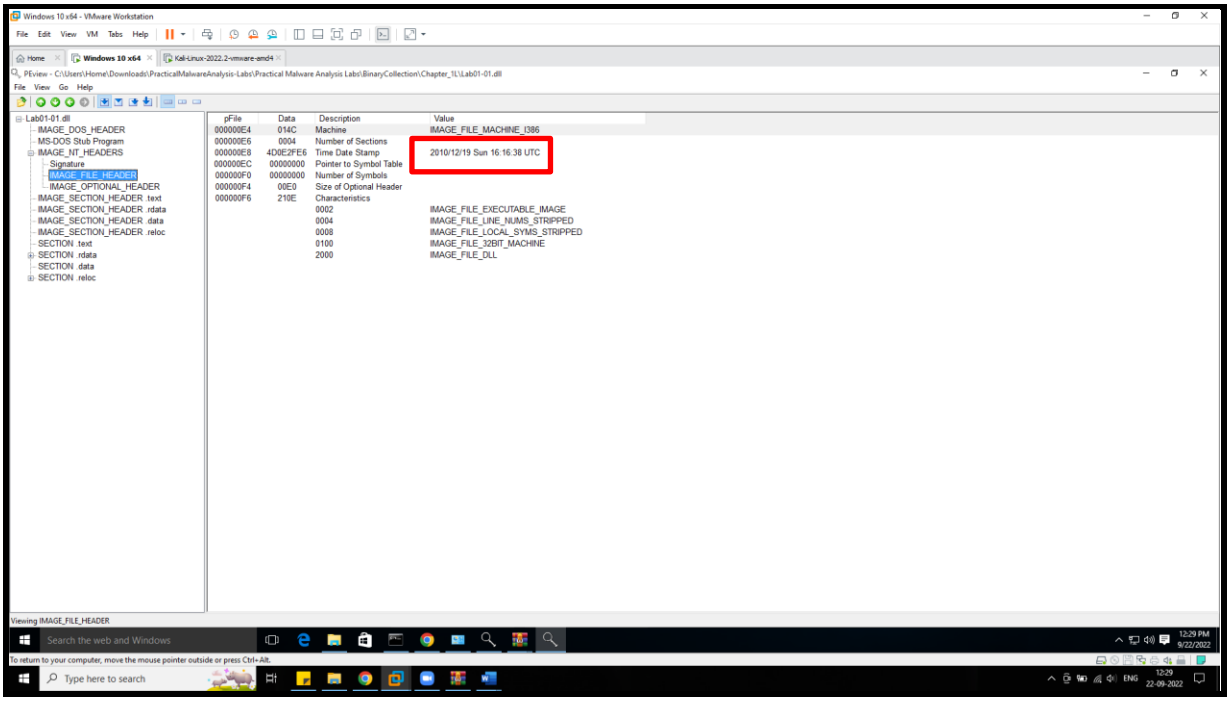
I used BinText to find host or network-based indicators. There were no network-based indicators. The only host-based indicator I could find was the calling of the DLLs



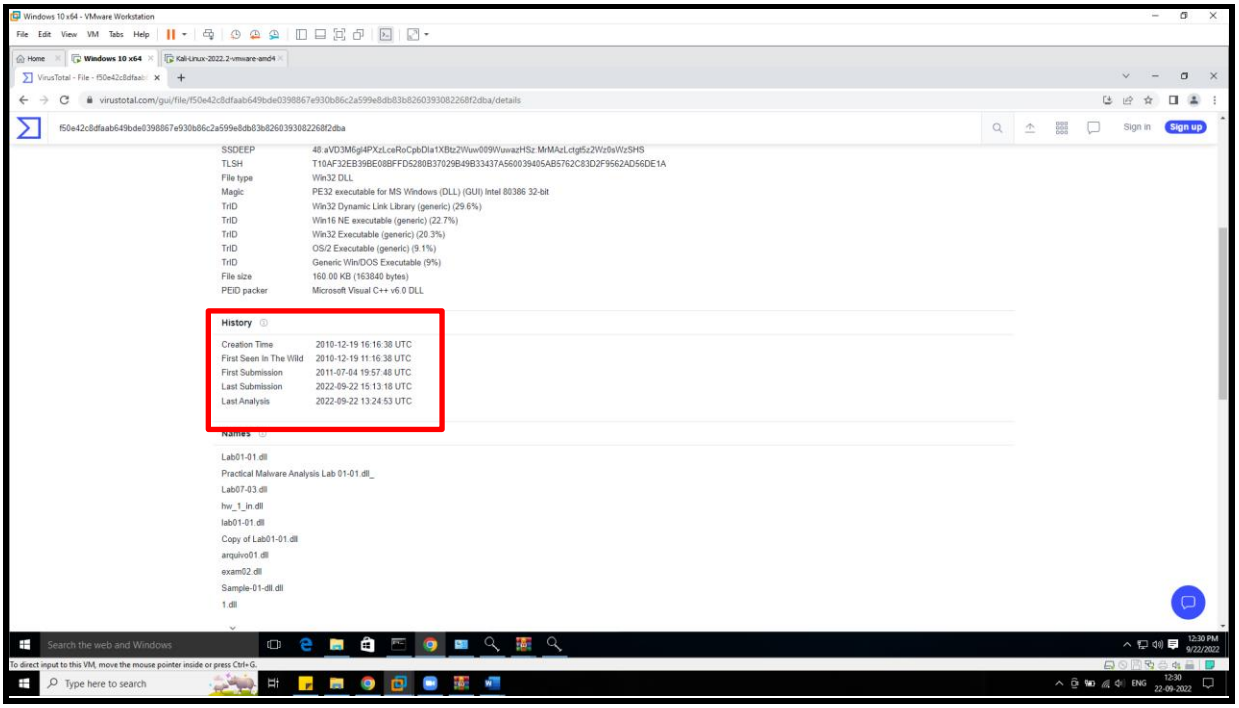
The below screenshot shows the report of Virus Total for Lab01-01.dll. It shows that malware signature has been identified by multiple sites.



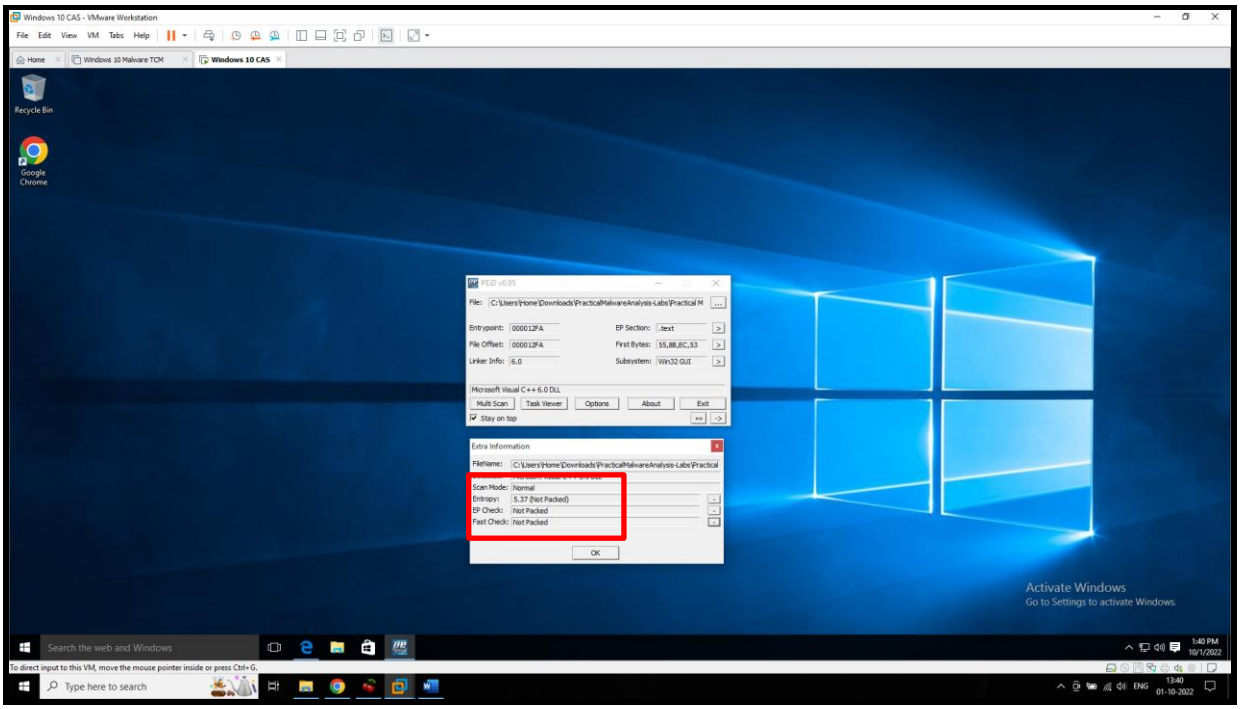
The below screenshot shows the compilation time of the malware Lab01-01.dll. The tool used is PE-View



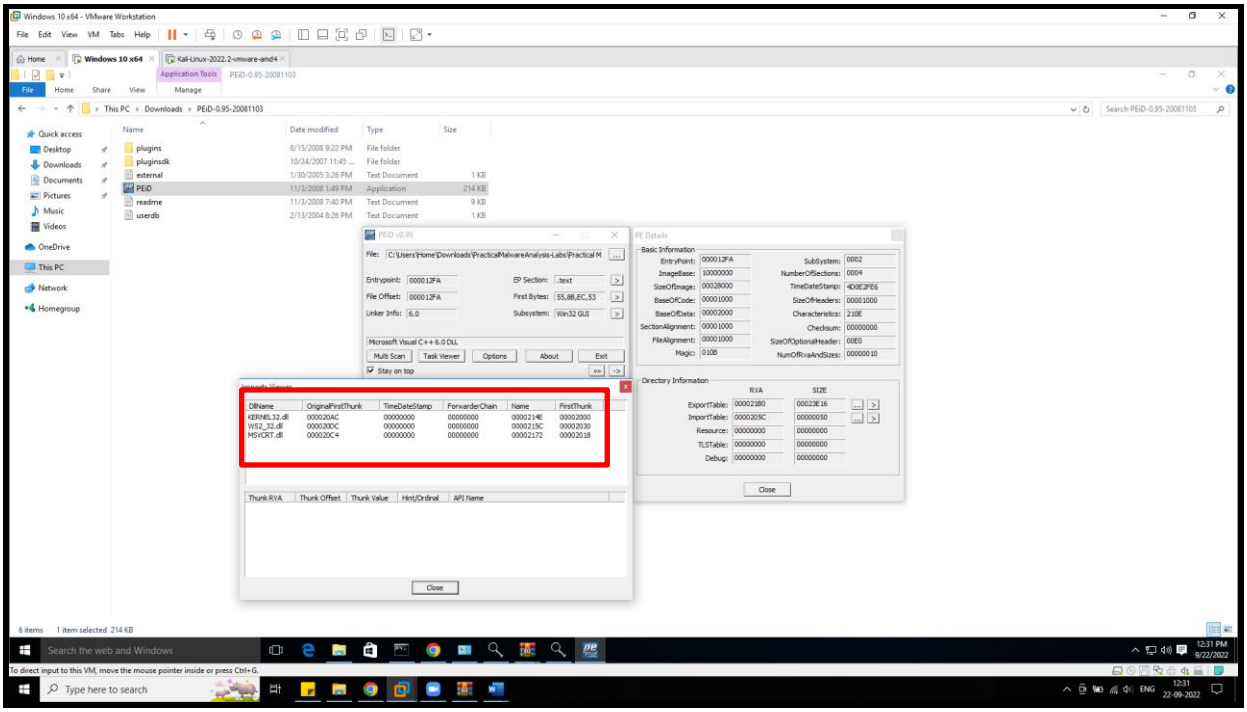
The below screenshot shows the compilation time of the malware Lab01-01.dll in Virus Total



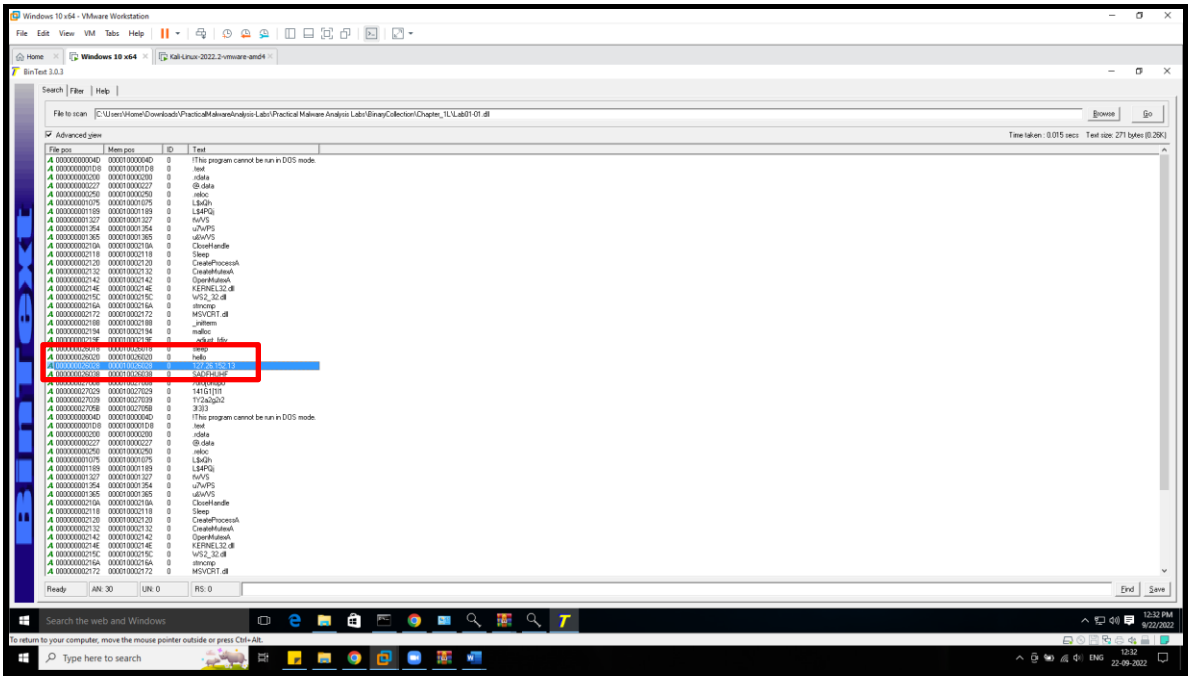
The below two screenshot shows that the binary is not packed.



By analyzing the binary in PEiD, we can see that there are three imports: KERNEL32.dll, MSVCRT.dll and WS2_32.dll.

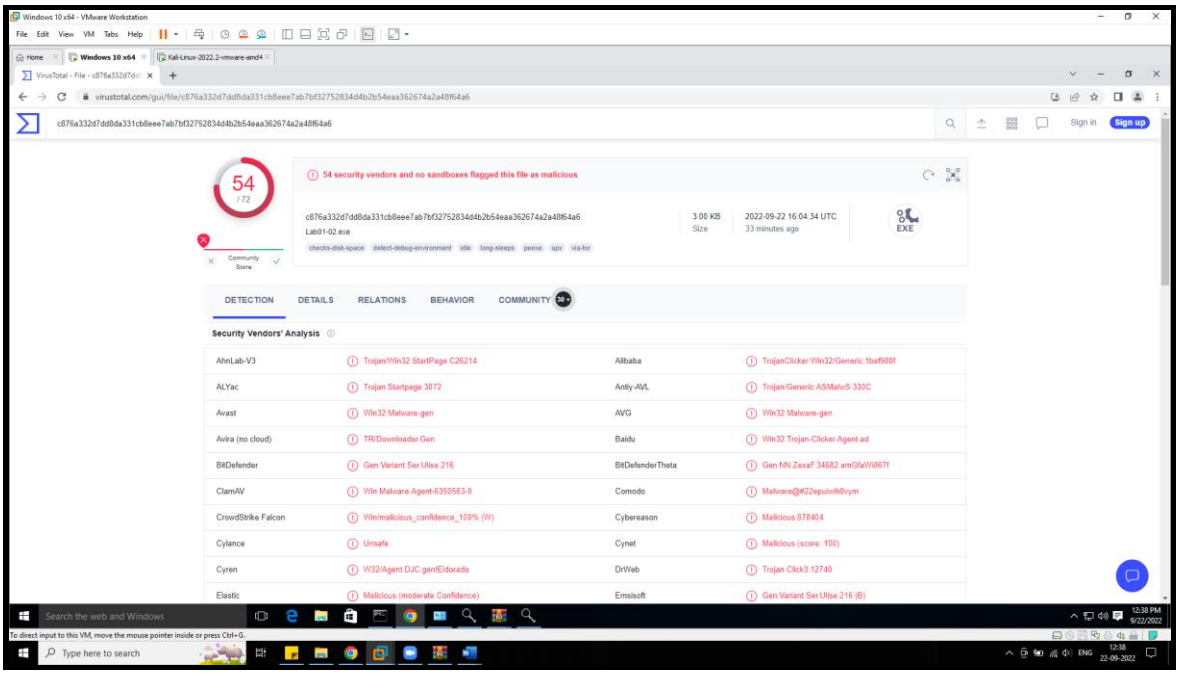


I used BinText to find host or network-based indicators. There were no network-based indicators. The only host-based indicator I could find was the calling of the DLLs

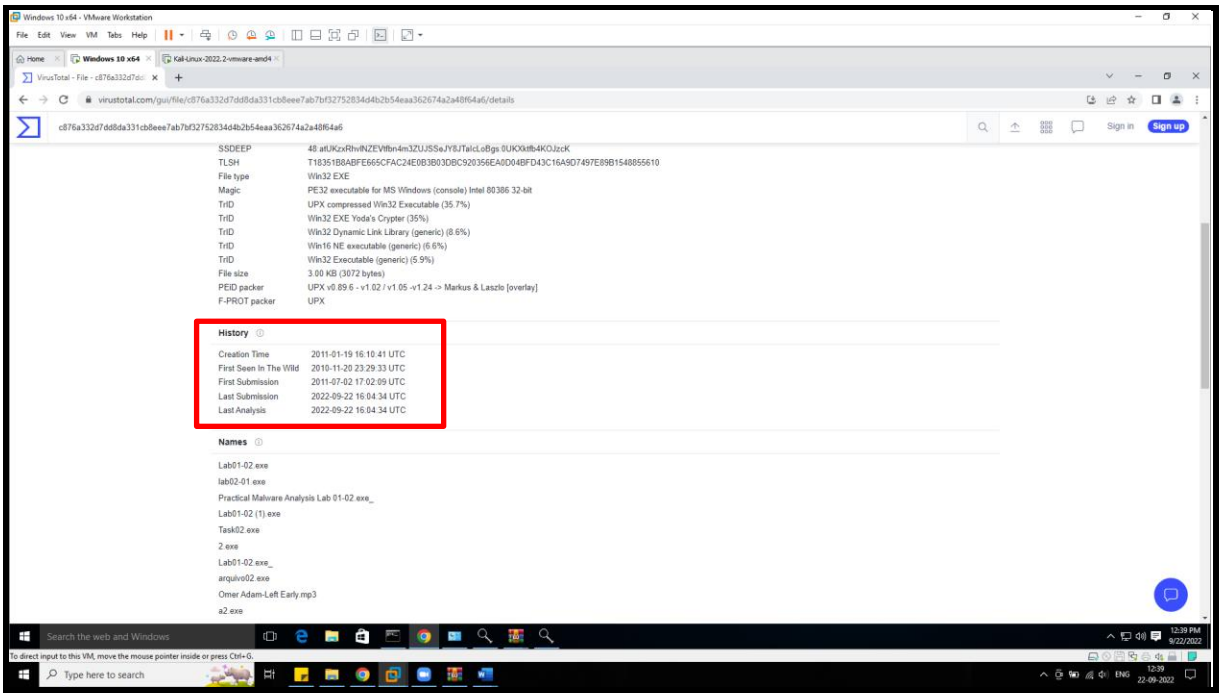


2)

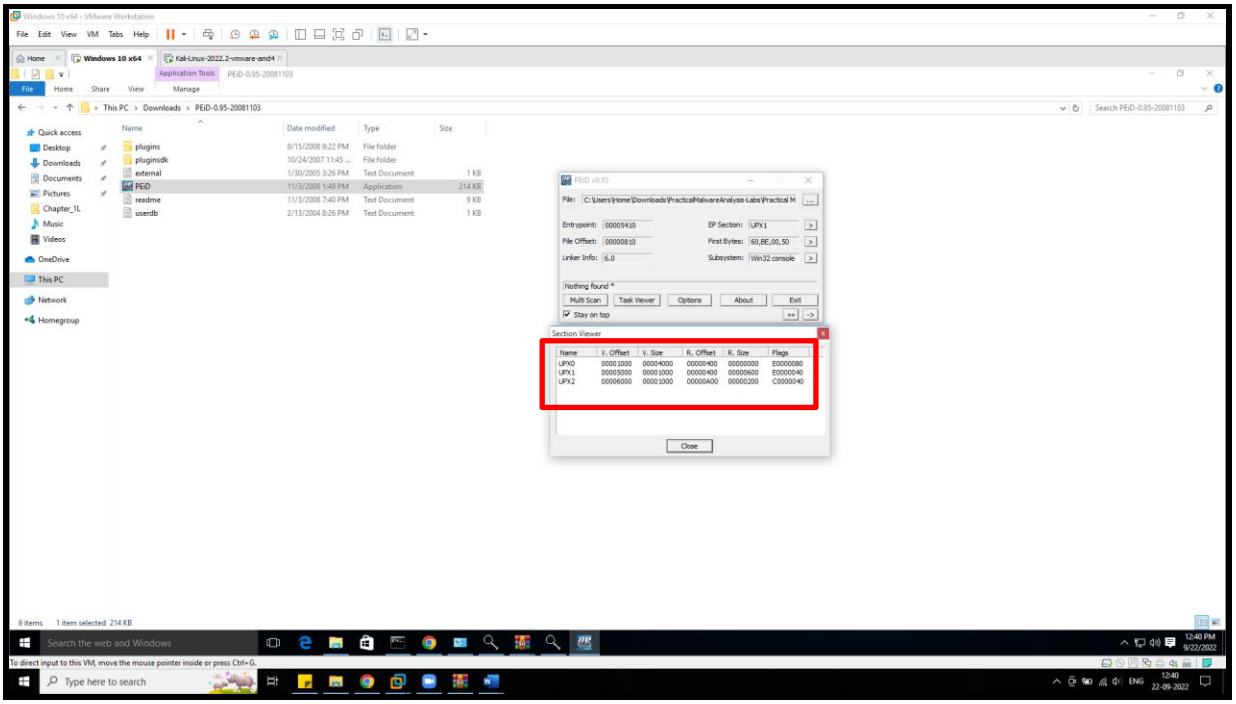
The below screenshot shows the report of Virus Total for Lab01-02.exe. It shows that malware signature has been identified by multiple sites.

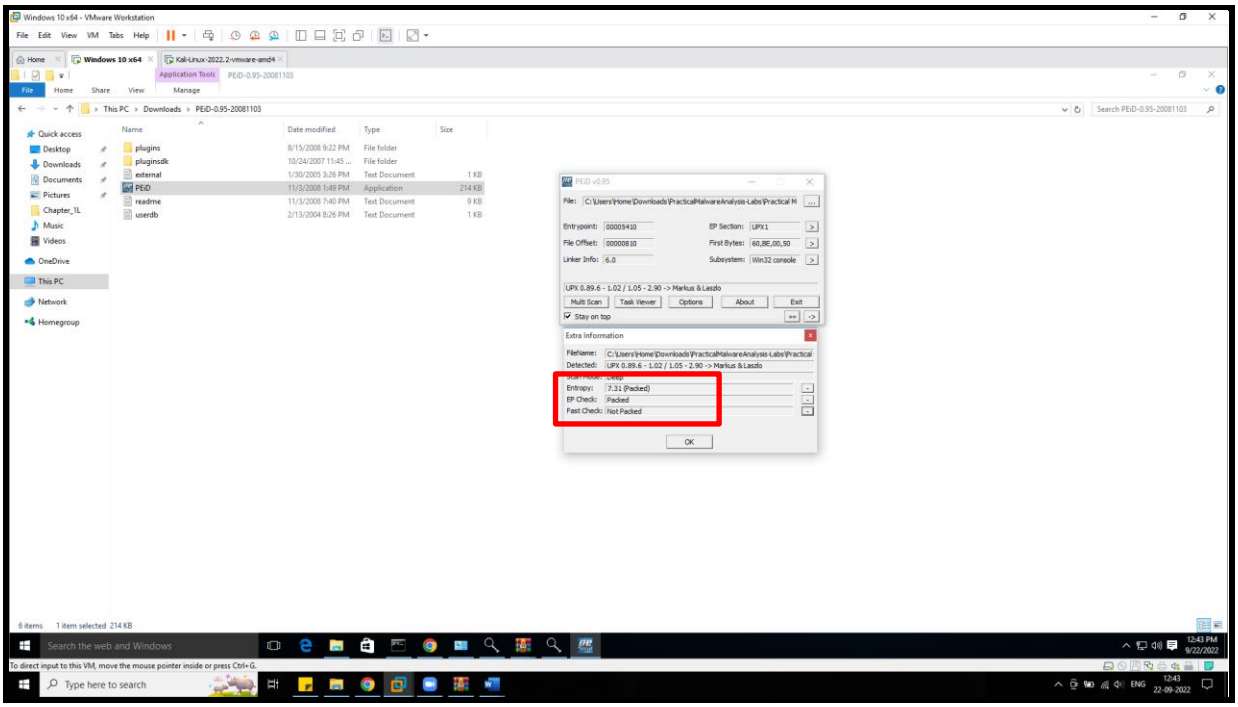


The below screenshot shows the compilation time of the malware Lab01-02.exe in Virus Total

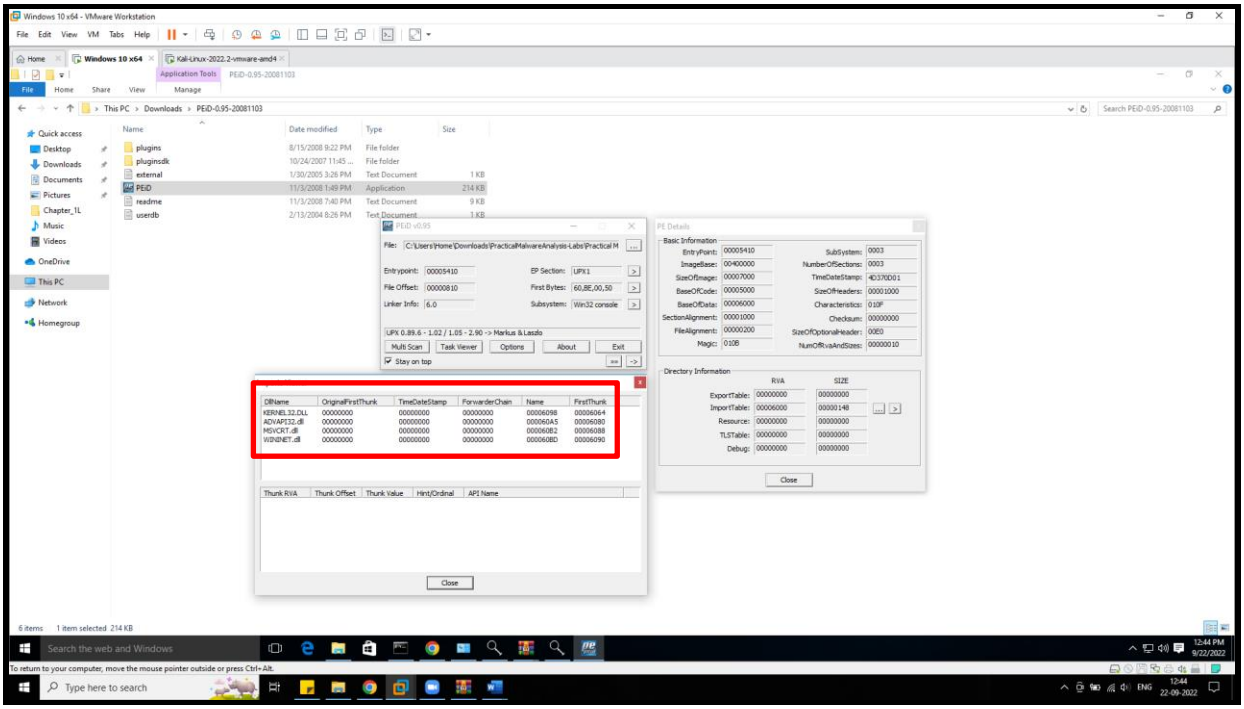


The below two screenshot shows that the binary is packed. The indicators that show this are the UPX0, UPX1, UPX2. These are the software used to pack the binaries.

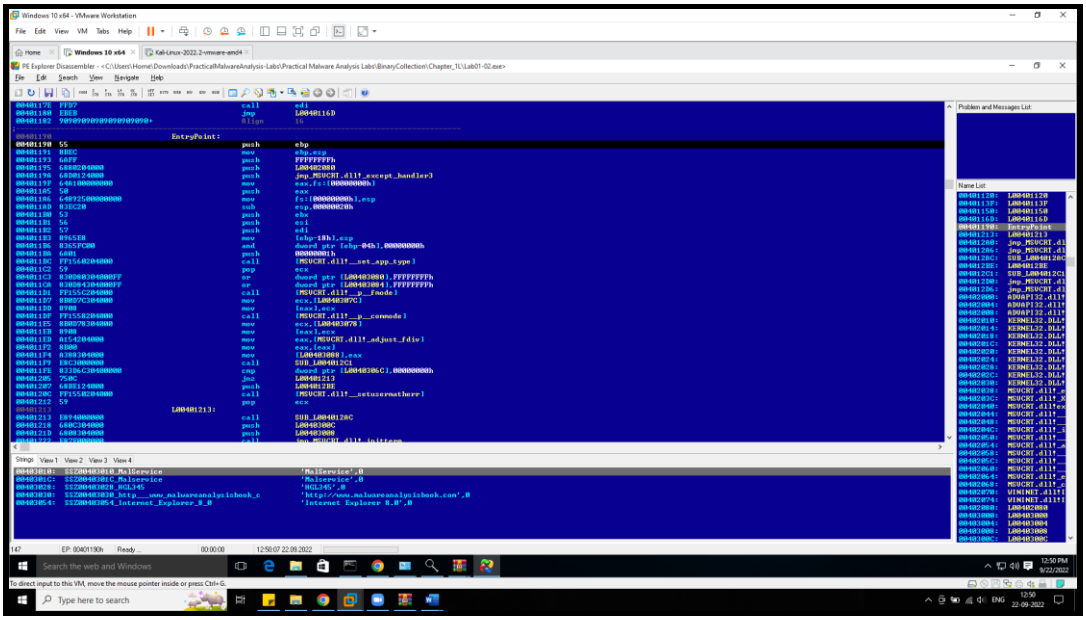




By analyzing the binary in PEiD, we can see that there are four imports: KERNEL32.dll, MSVCRT.dll, ADVAPI32.dll and WININET.dll.

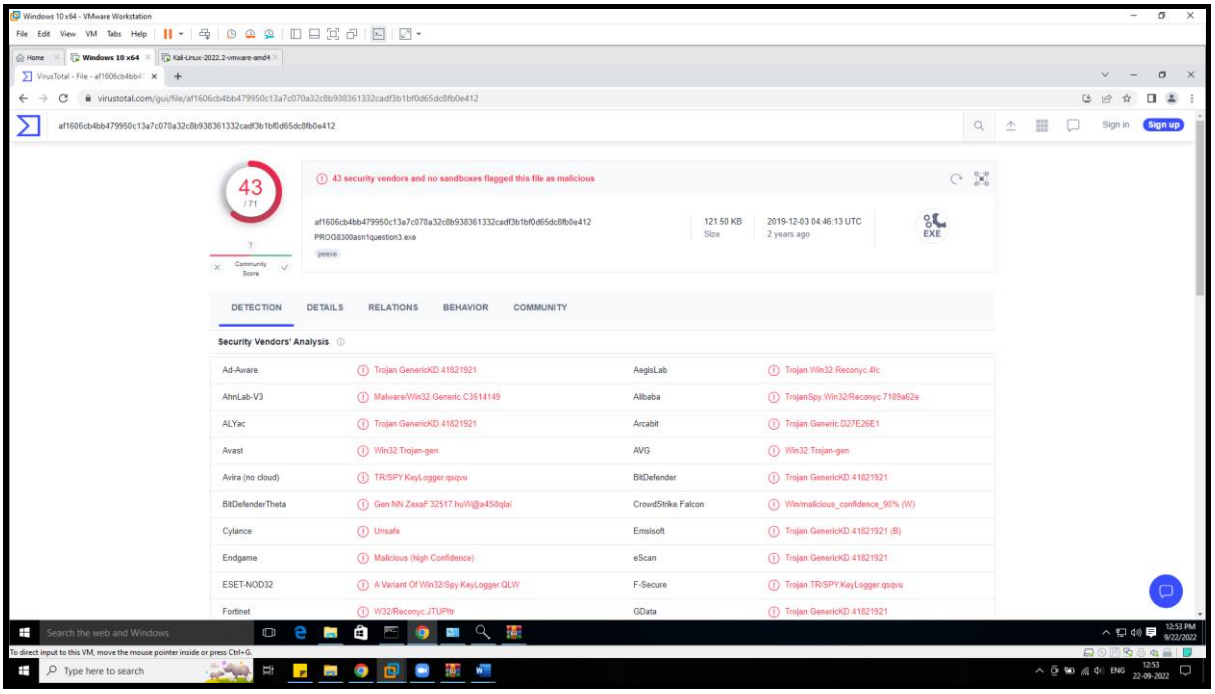


By analyzing the binary in PE Explorer, we can see that there is a host or network-based indicator present which is http://www.malwareanalysisbook.exe.

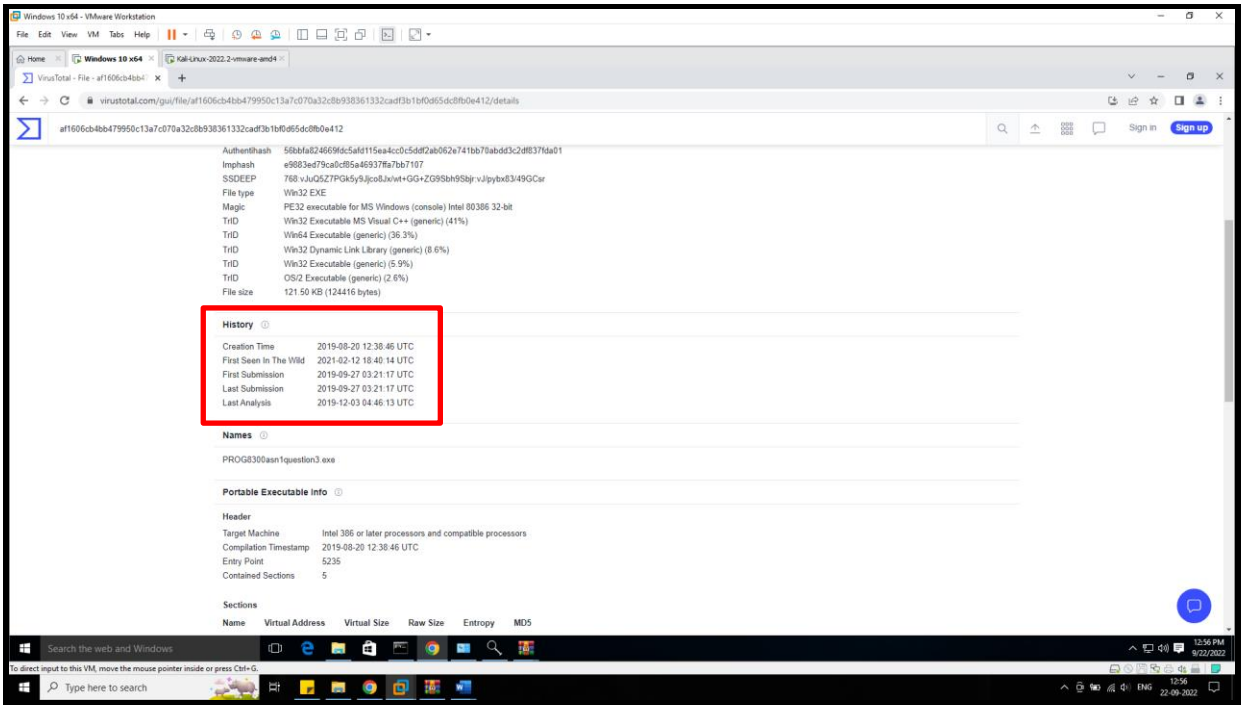


Part 3 – Basic Dynamic Analysis of unknown binary files

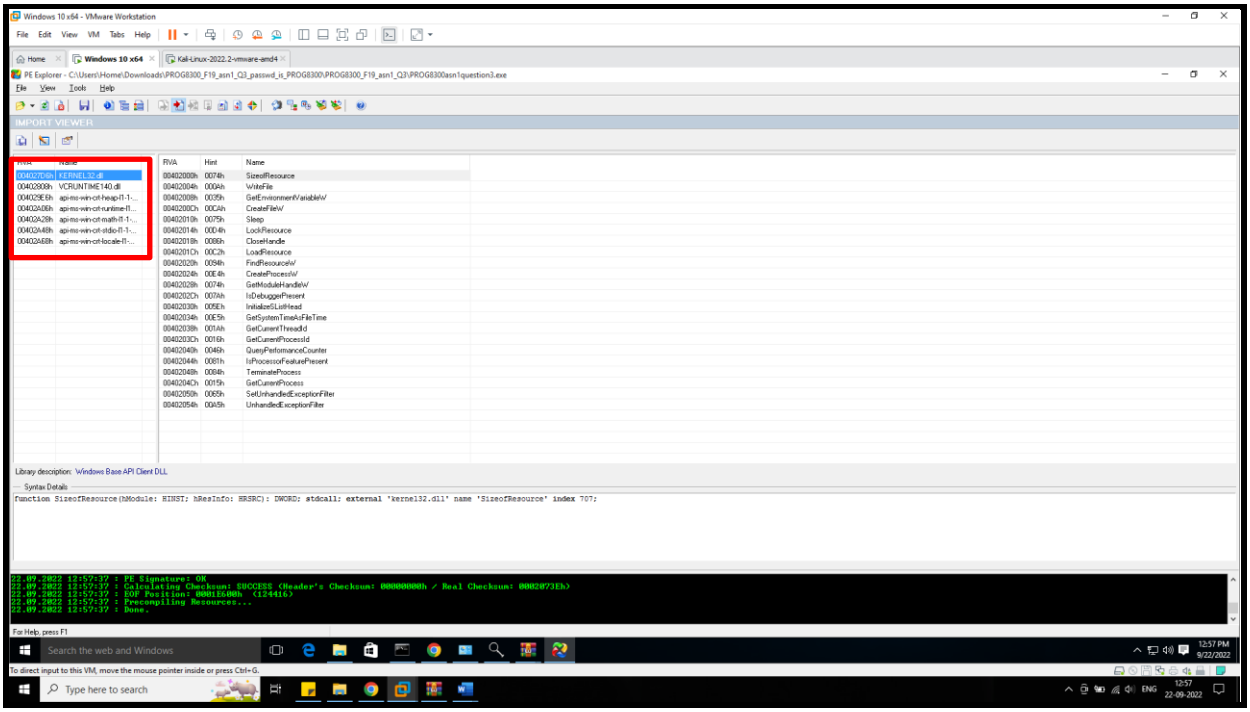
The below screenshot shows the report of Virus Total for PROG8300asn1question3.exe. It shows that malware signature has been identified by multiple sites.



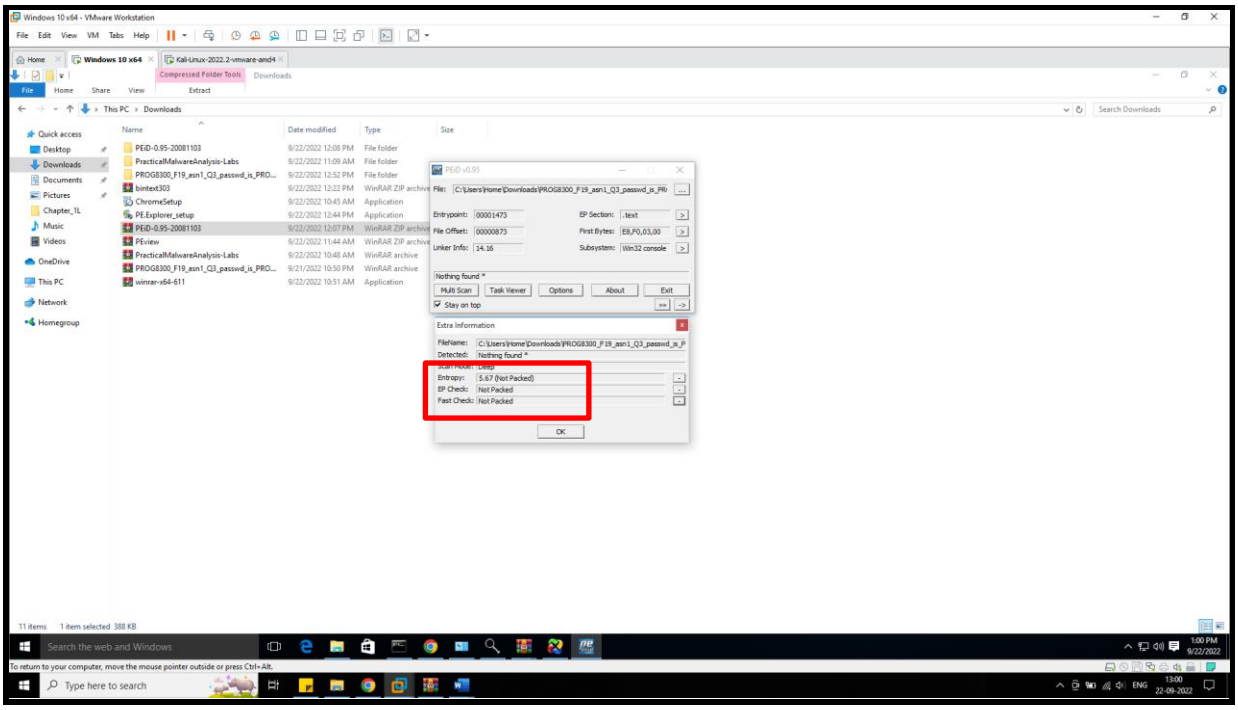
The below screenshot shows the compilation time of the malware PROG8300asn1question3.exe in Virus Total

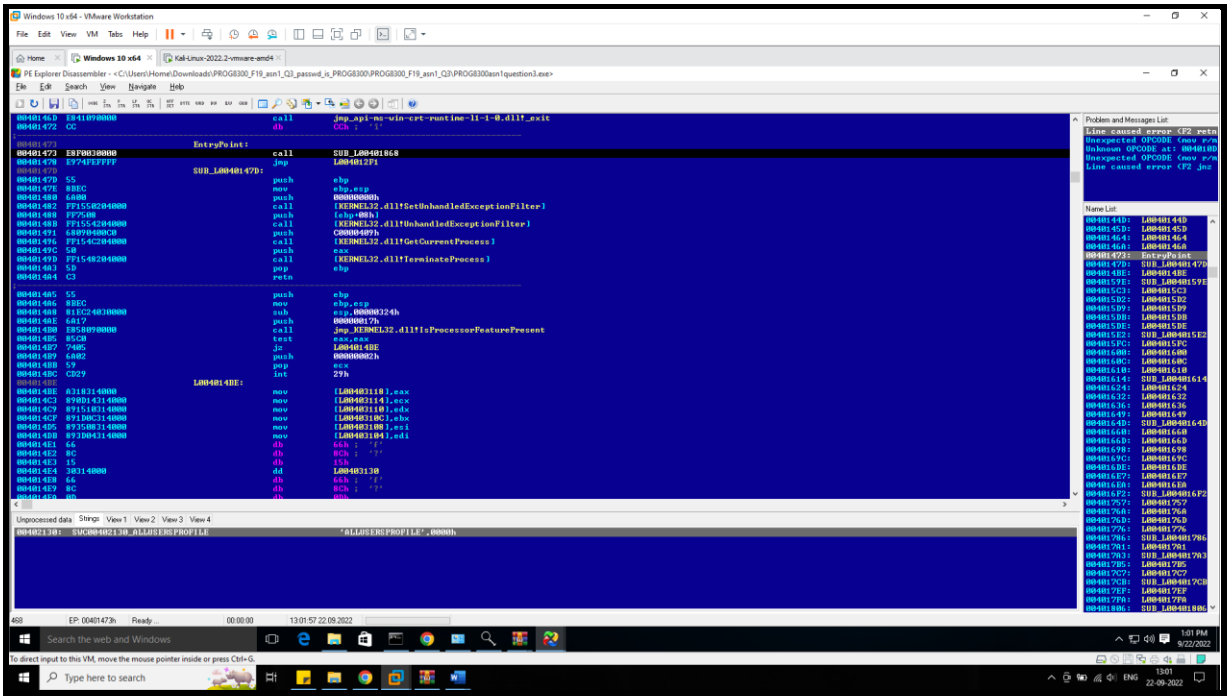


By analyzing the binary in PEiD, we can see that there are seven imports.

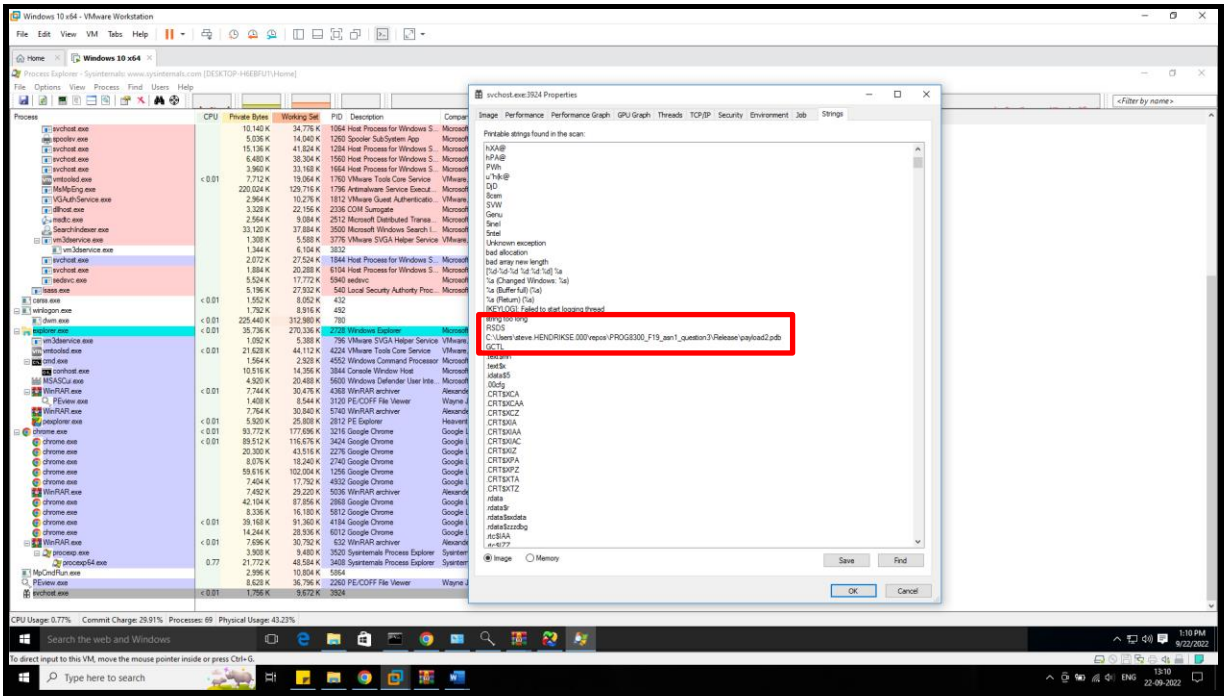


The below screenshot shows that the binary is not packed.

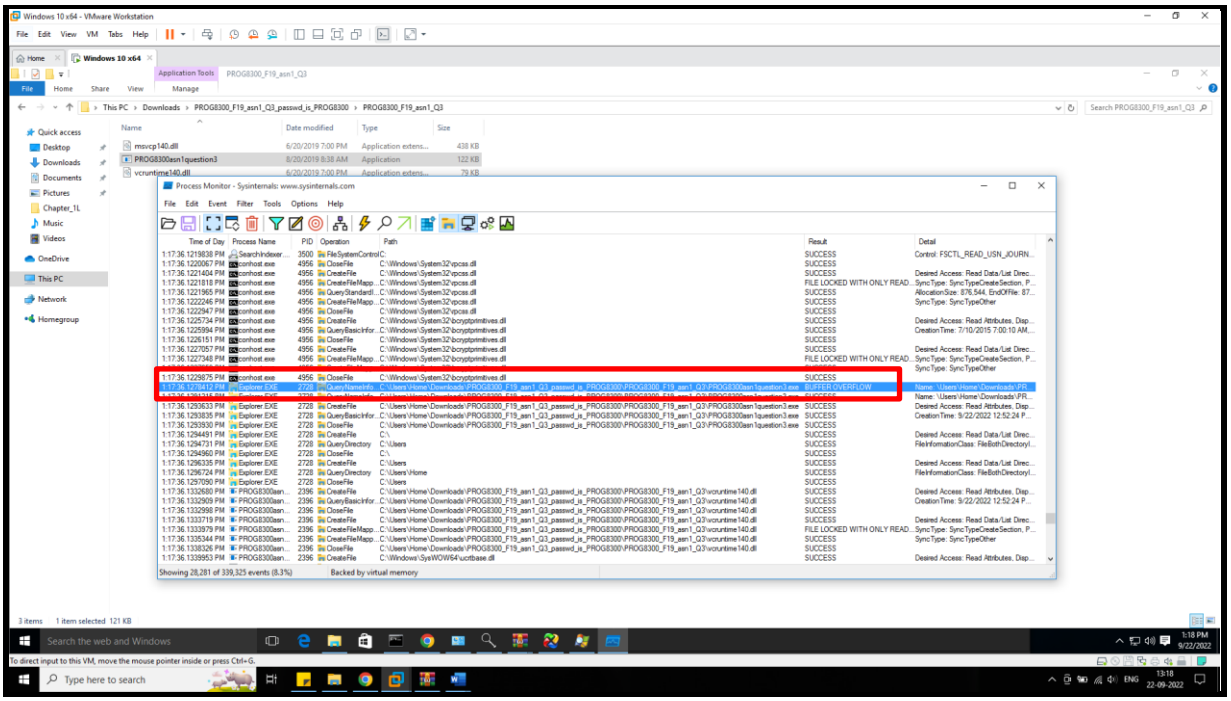


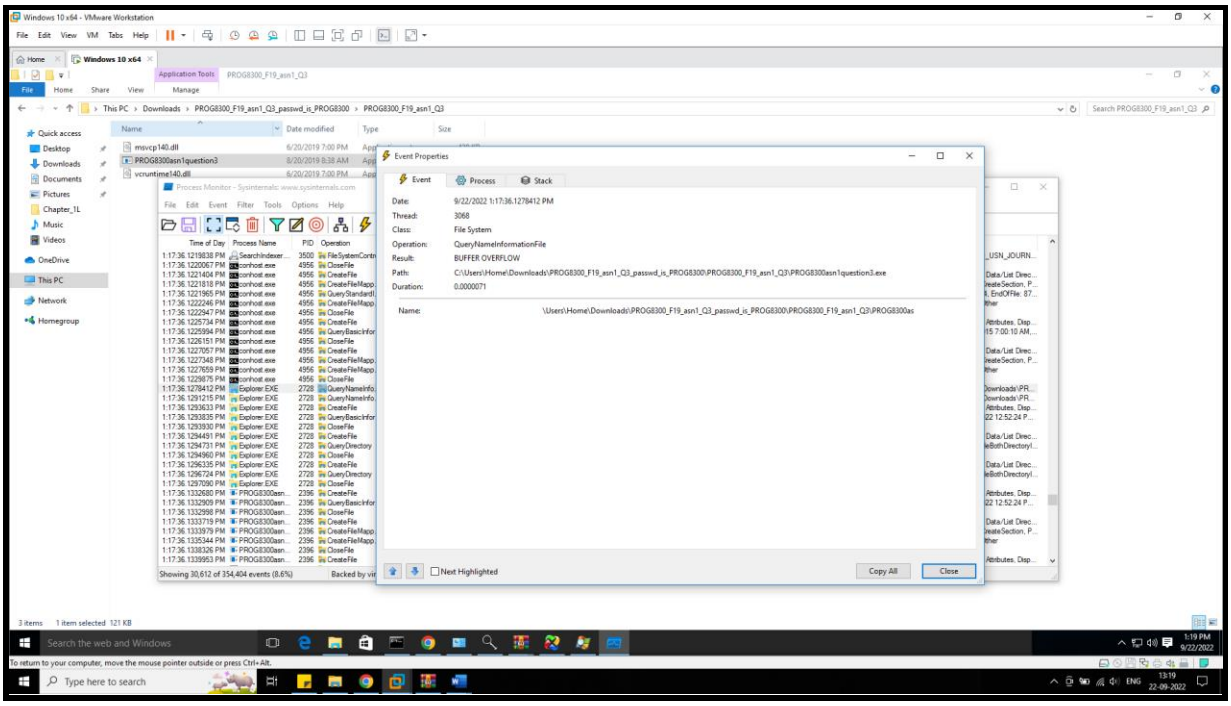


Using the Process Explorer after running the binary, we can see that I have got a host-based indicator. The binary executes a file payload2.pdb. This is found from the svchost.exe.



Another host-based indicator we can see is that upon running the binary, we have a condition of buffer overflow. Below two screenshots demonstrate that.





I setup INETSIM in Remnux VM. Inetsim acts as a fake internet. I added the IP of Windows machine as the DNS of the remnux machine. Upon running the binary, we can see that the malware tries to reach the internet. This is demonstrated by the Wireshark output. We can see the IP address of the windows machine.