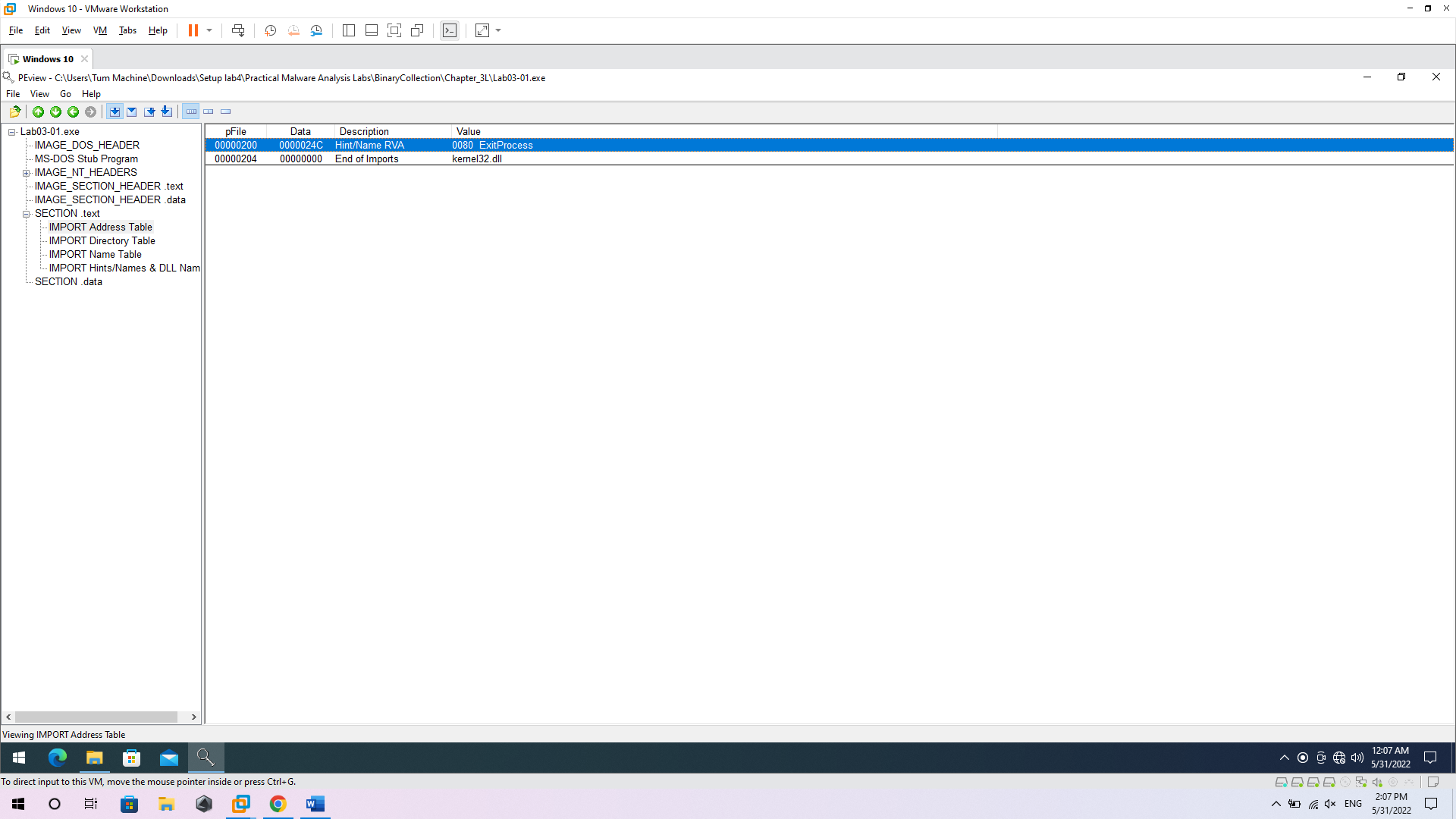
LAB 4

Nguyễn Thanh Hoài Lộc – SE151250

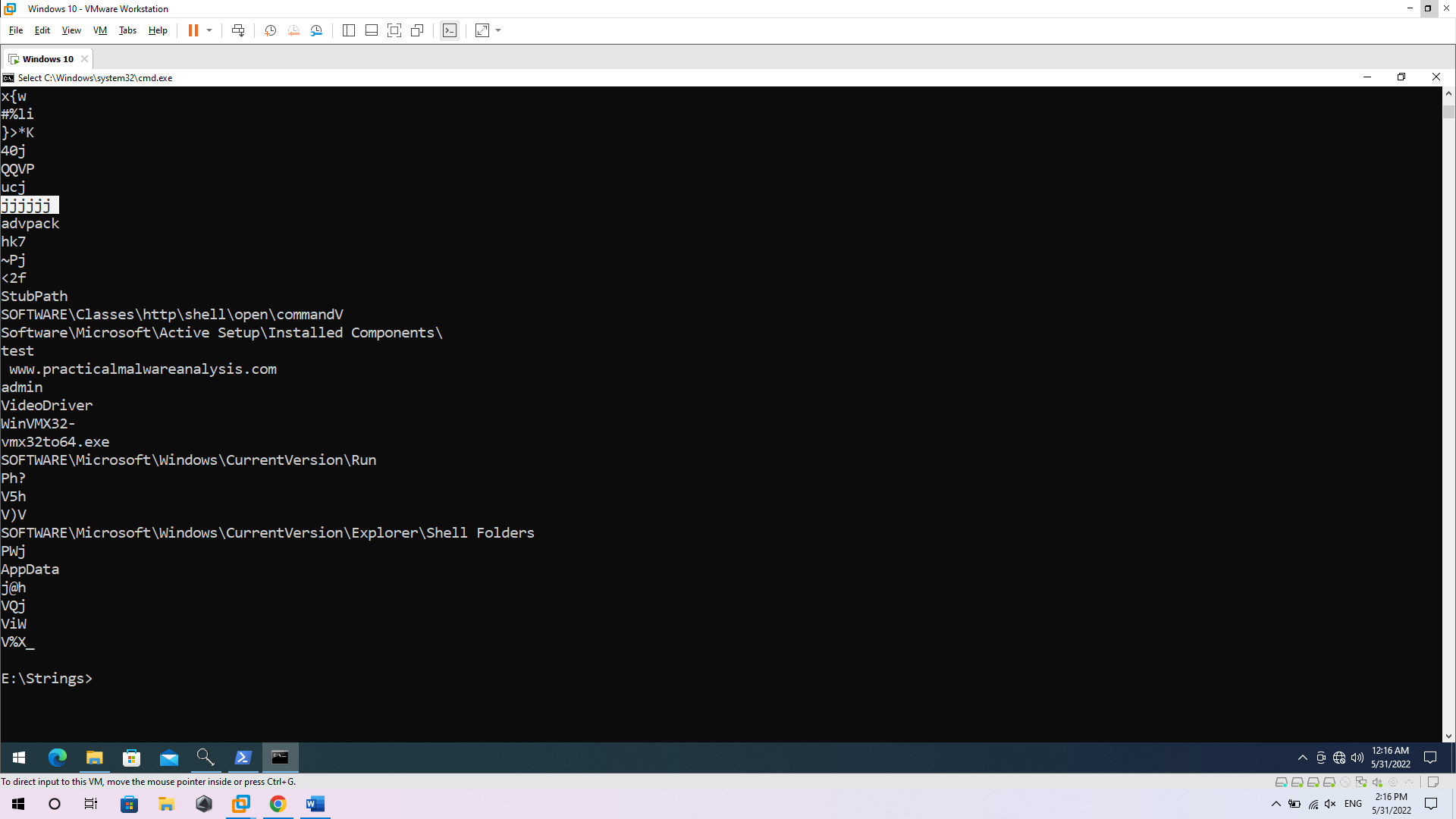
1. Using Peview

* Now if we try to look into this executable using PEview we can see that only one import is being made



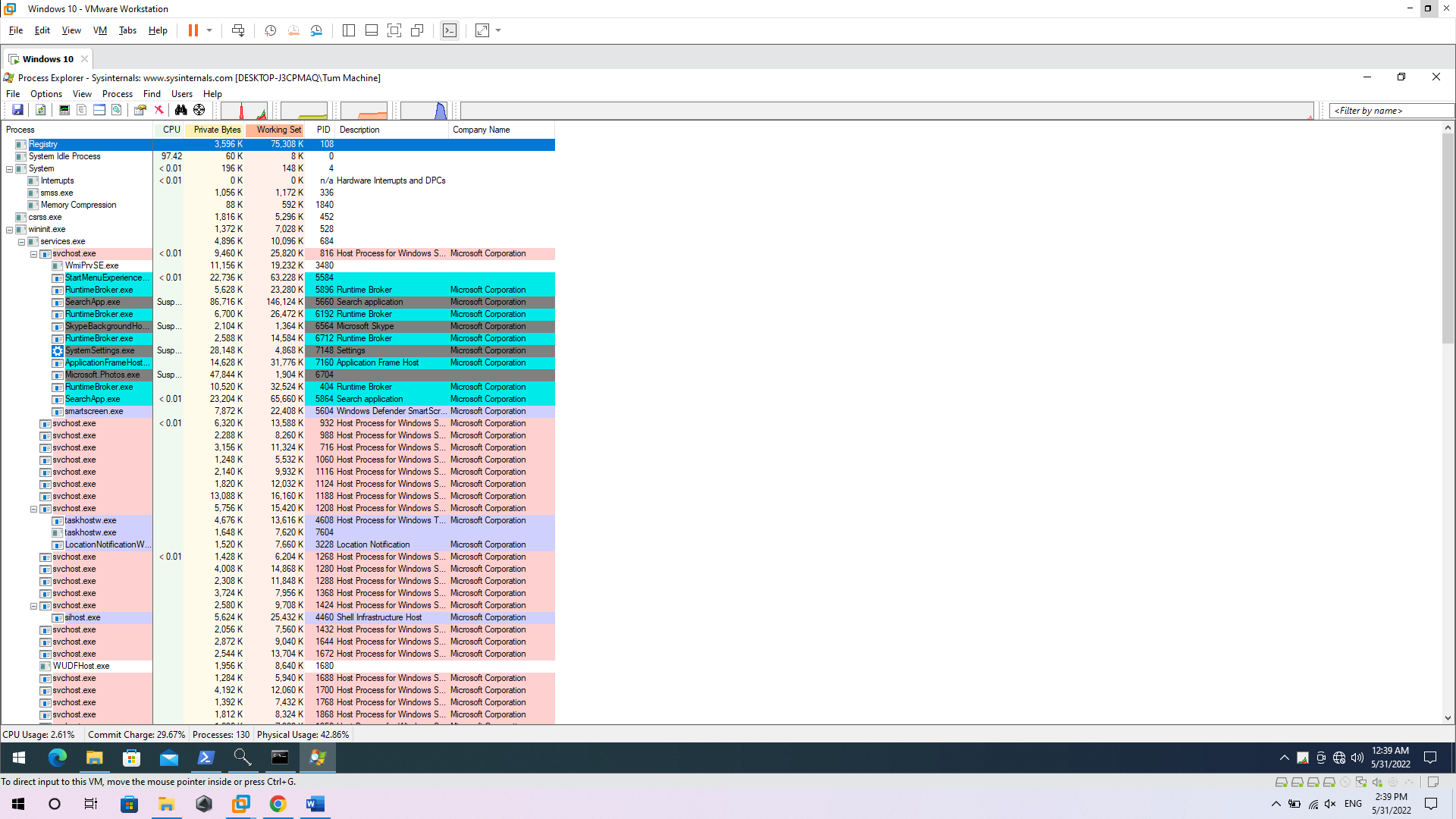
1. Using Strings

* E:\Strings>strings.exe "C:\Users\Tum Machine\Downloads\Setup lab4\Practical Malware Analysis Labs\BinaryCollection\Chapter\_3L\Lab03-01.exe"

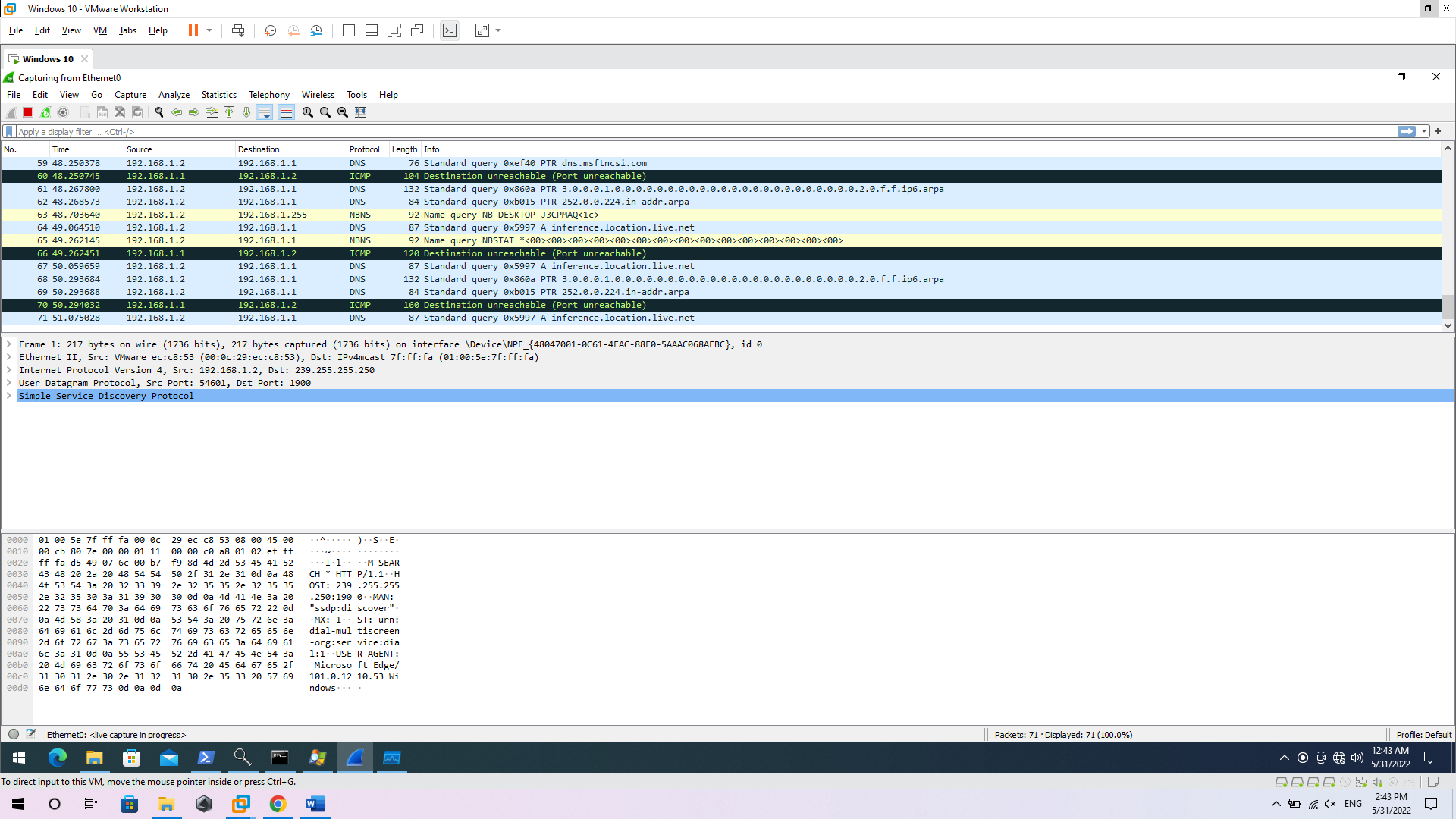


* The strings have revealed some more DLL information and some registry details.

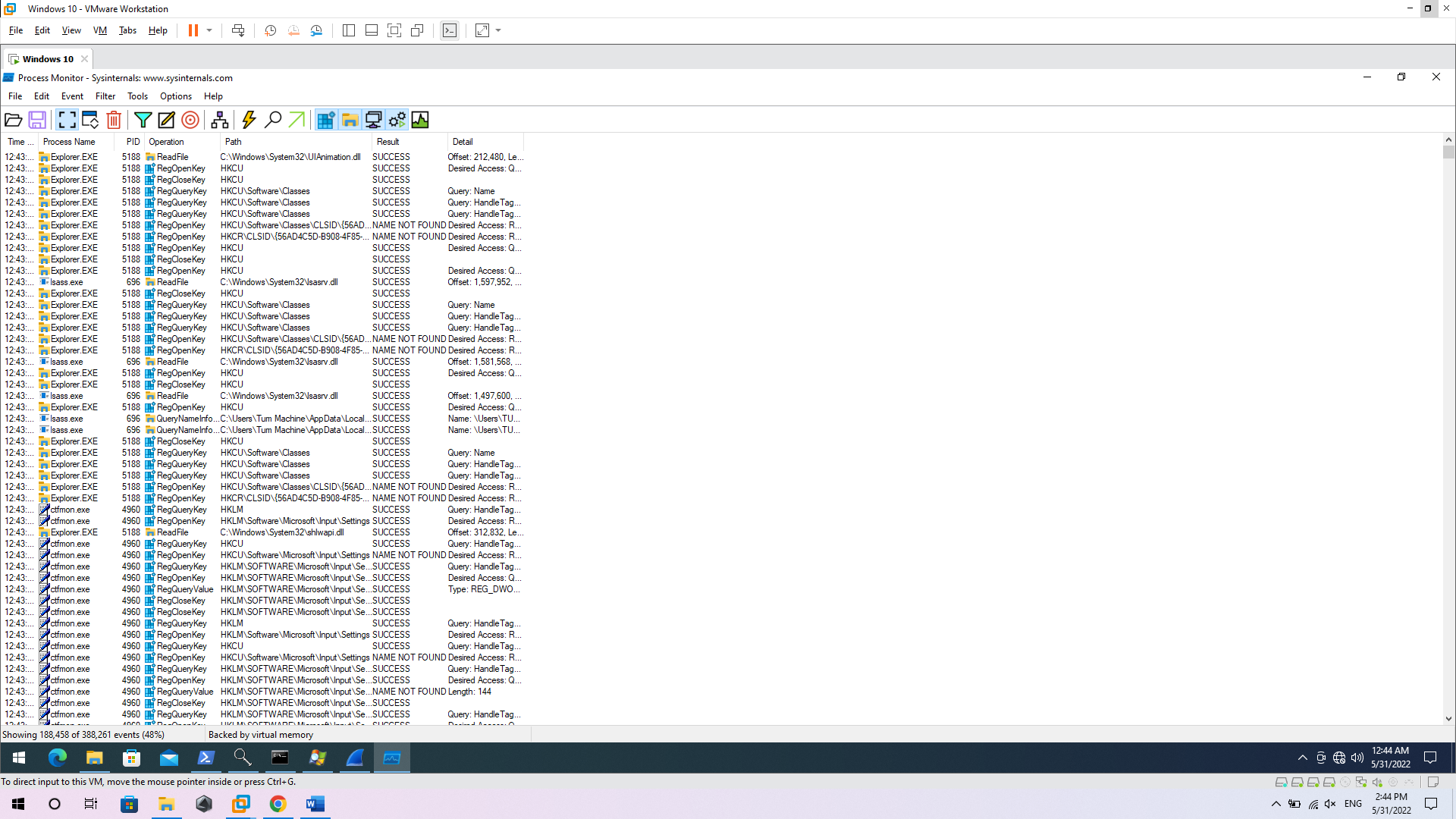
1. Run Process Explorer



1. Run Wireshark



1. Start Process Monitor



1. Run the Lab03-01.exe File and see in Wireshark of KaliLinux

