Practical Malware Analysis Lab 3-1

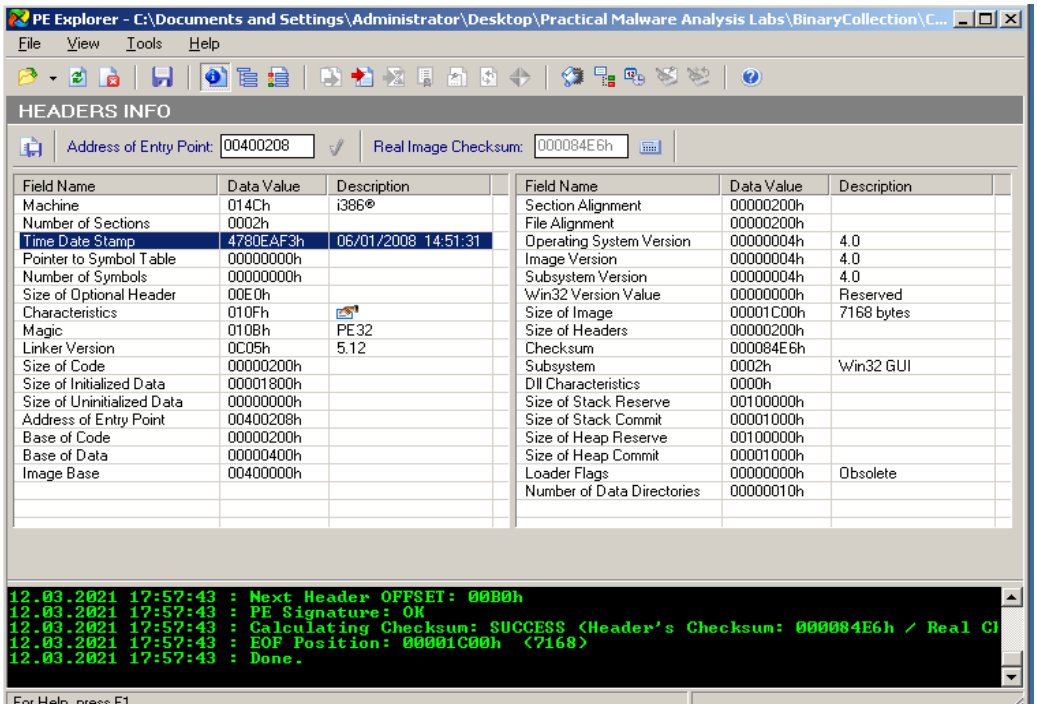
Questions

1. What are this malware's imports and strings?
2. What are the malware's host based indicators?
3. Are there any useful network-based signatures for this malware If so, what are they?

Question 1

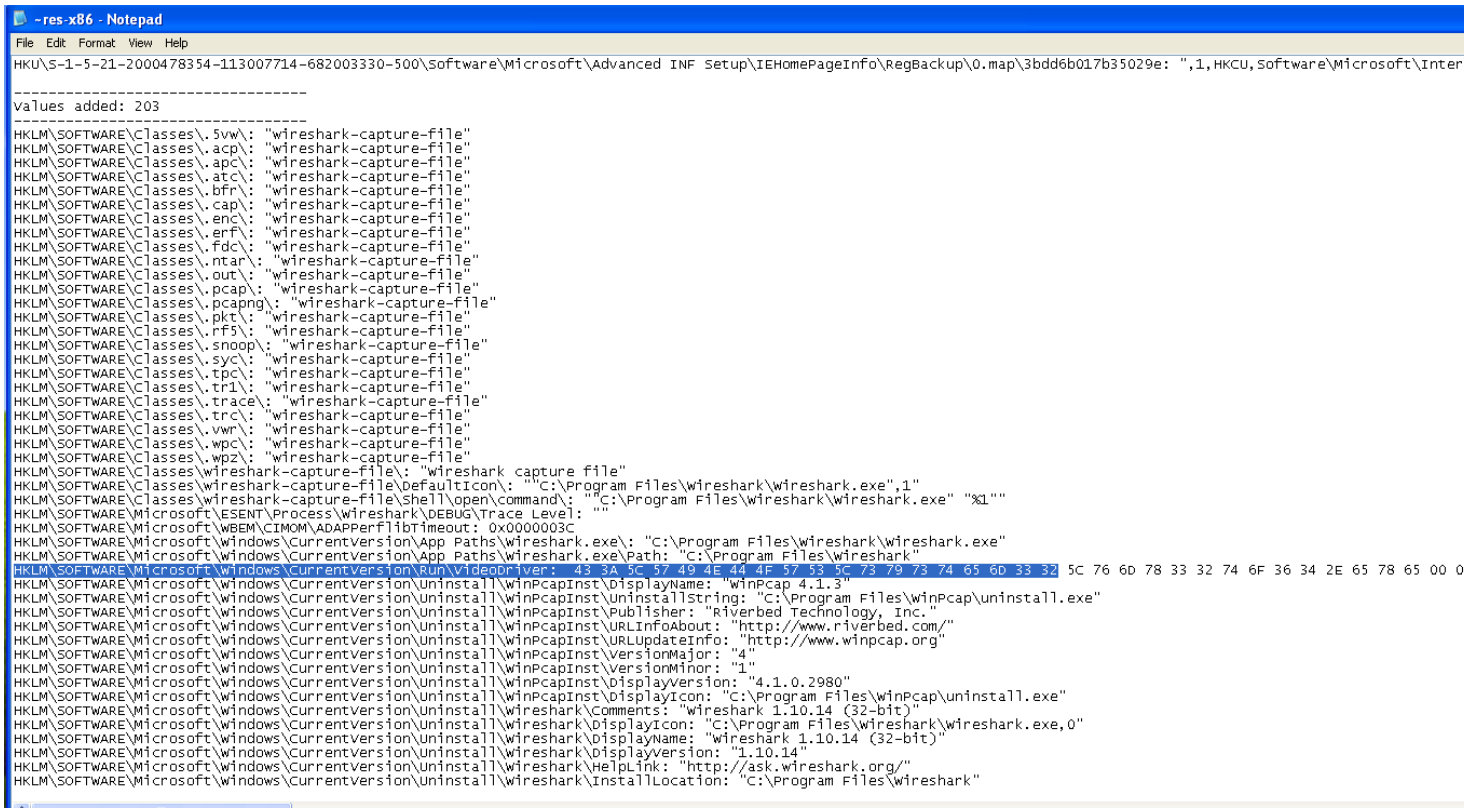
When putting the exe Lab03-01.exe into Dependencies it only showed one import kernel32.dll and the function ExitProcess. The strings gave us more information about what this malware does.

StubPath
SOFTWARE\Classes\http\shell\open\commandV
Software\Microsoft\Active Setup\Installed Components\
test
www.practicalmalwareanalysis.com
Admin
?503
200
advpack
CONNECT %s:%i HTTP/1.0
VideoDriver
WinVMX32-
Vmx32to64.exe
SOFTWARE\Classes\http\shell\open\commandV
Software\Microsoft\Active Setup\Installed Components\
SOFTWARE\Microsoft\Windows\CurrentVersion\Run

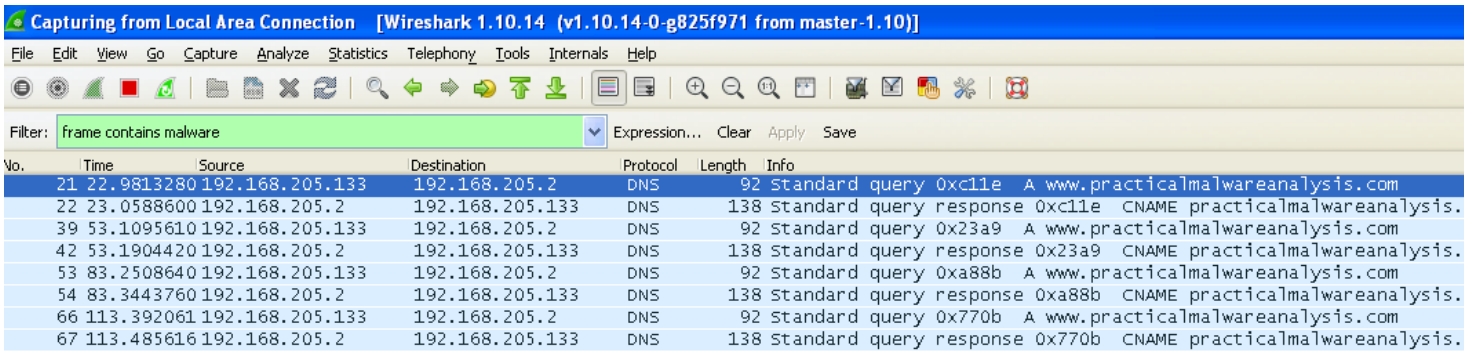


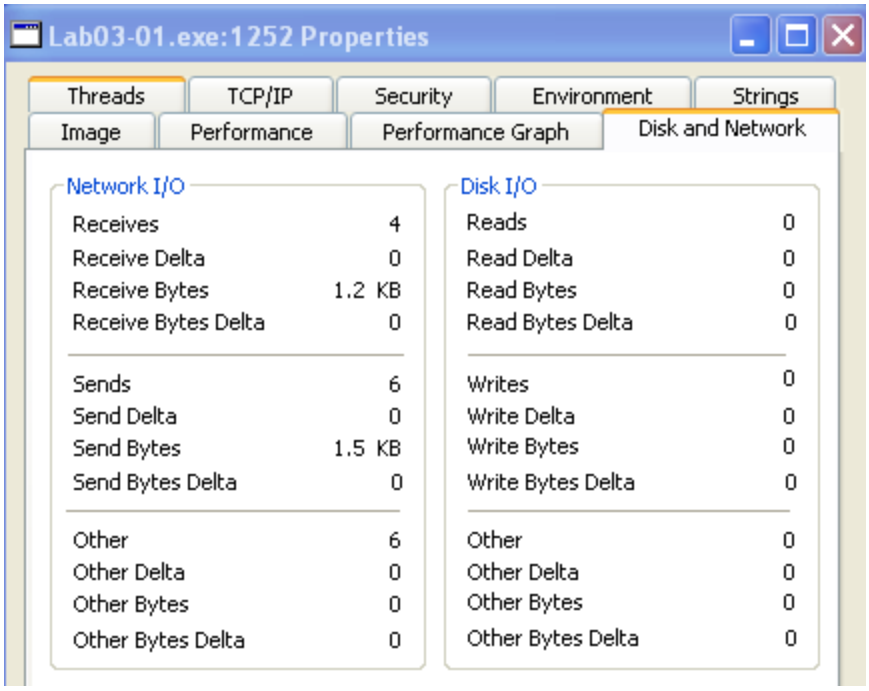
Dynamic Analysis

Regshot Results



Wireshark Results





Question 2

Some host based indicators include the exe Vmx32to64.exe, and the registry entry of VideoDriver.

Question 3

Traffic to the website www.practicalmalwareanalysis.com