

Malware Analysis

Assignment 2 – Basic Static Analysis

10 points

Kush Patel

LAB

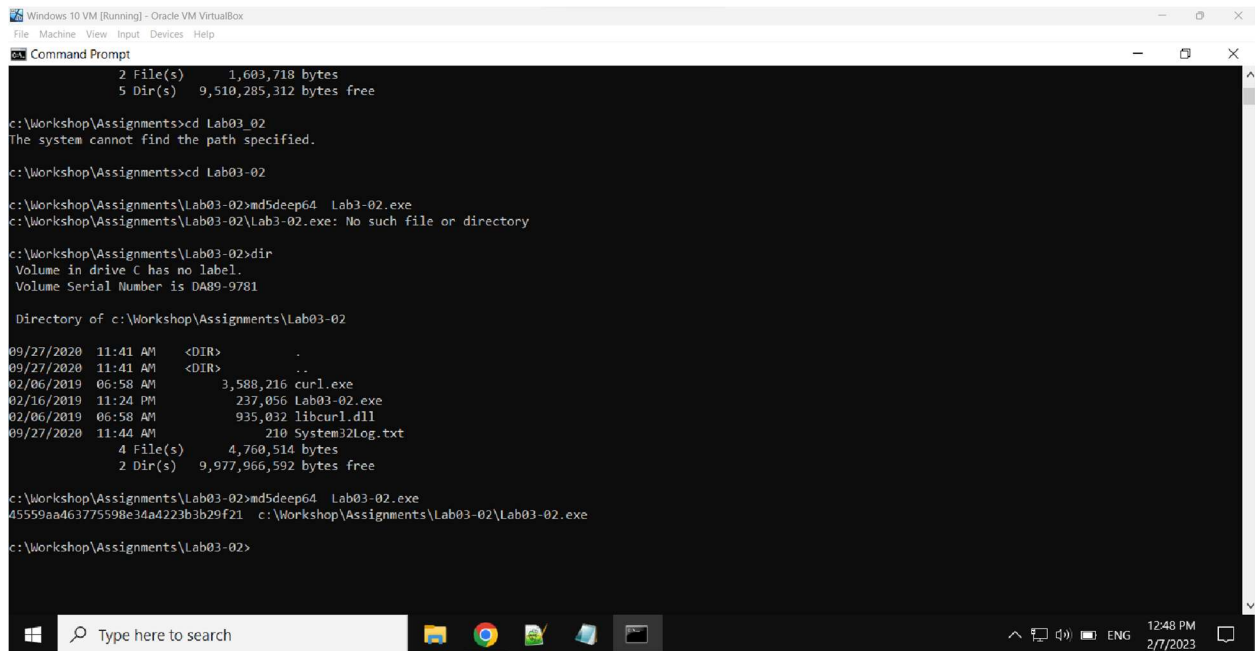
Please download Lab03-02.7z (password to unzip: malware) from Blackboard under this assignment to the Windows 10 VM.

- **Note:** Lab03-02.7z is a zipped file. Our Windows VM has a tool called 7-Zip to unzip the file. Right click the file and use 7-Zip to extract files.

Note: We have all needed tools on Windows VM. No need of downloading extra software.

1. Run all tools in Chapter 1 on Lab03-02.exe within Lab03-02.7z, and copy and paste the output of the output or screenshot from these tools below. (3 points in total)

Output from [md5deep](#) (0.5 point)



```
Windows 10 VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Command Prompt

2 File(s)      1,603,718 bytes
5 Dir(s)      9,510,285,312 bytes free

c:\Workshop\Assignments>cd Lab03_02
The system cannot find the path specified.

c:\Workshop\Assignments>cd Lab03-02
c:\Workshop\Assignments\Lab03-02>md5deep64 Lab03-02.exe
c:\Workshop\Assignments\Lab03-02\Lab03-02.exe: No such file or directory

c:\Workshop\Assignments\Lab03-02>dir
Volume in drive C has no label.
Volume Serial Number is DA89-9781

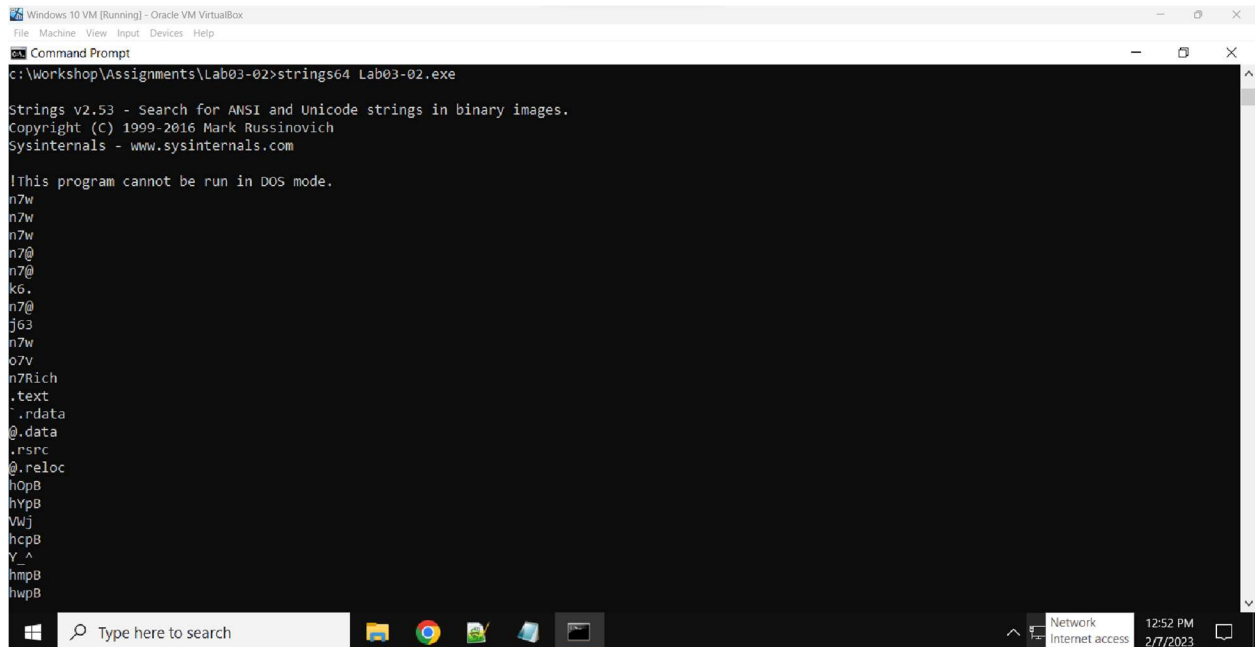
Directory of c:\Workshop\Assignments\Lab03-02

09/27/2020  11:41 AM  <DIR>          .
09/27/2020  11:41 AM  <DIR>          ..
02/06/2019  06:58 AM           3,588,216 curl.exe
02/16/2019  11:24 PM           237,056 Lab03-02.exe
02/06/2019  06:58 AM           935,032 libcurl.dll
09/27/2020  11:44 AM              210 System32Log.txt
4 File(s)      4,760,514 bytes
2 Dir(s)      9,977,966,592 bytes free

c:\Workshop\Assignments\Lab03-02>md5deep64 Lab03-02.exe
45559aa463775598e34a4223b3b29f21  c:\Workshop\Assignments\Lab03-02\Lab03-02.exe

c:\Workshop\Assignments\Lab03-02>
```

Output from [Strings](#) (0.5 point)

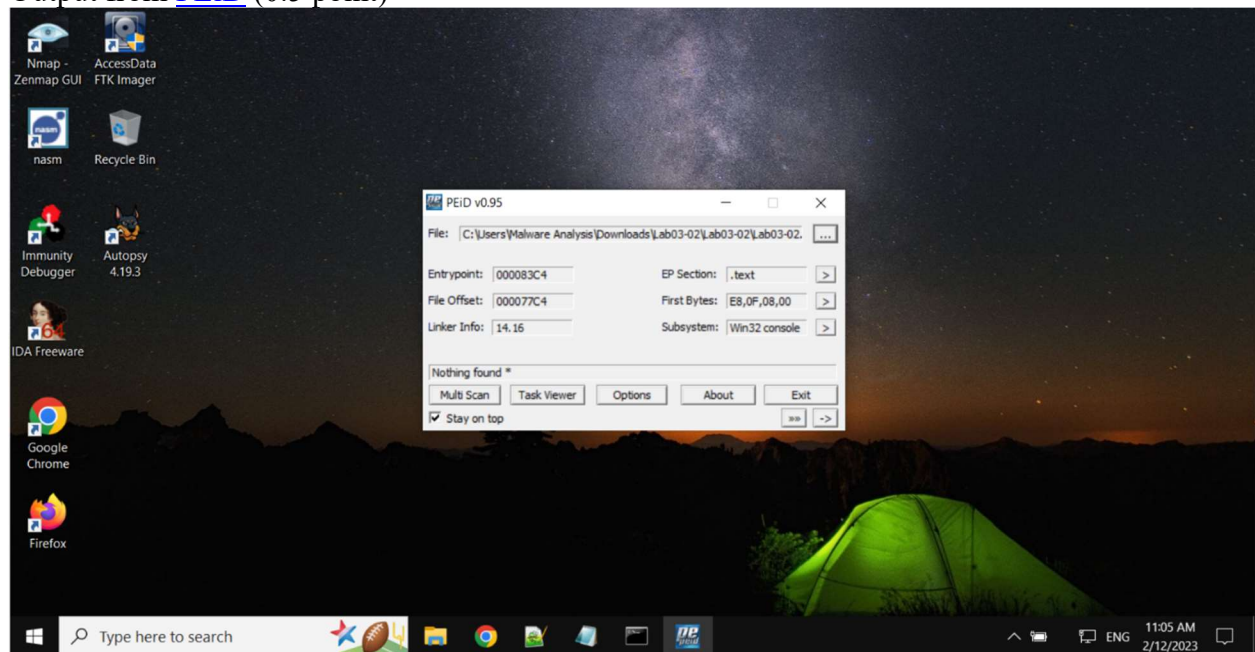


```
c:\Workshop\Assignments\Lab03-02>strings64 Lab03-02.exe

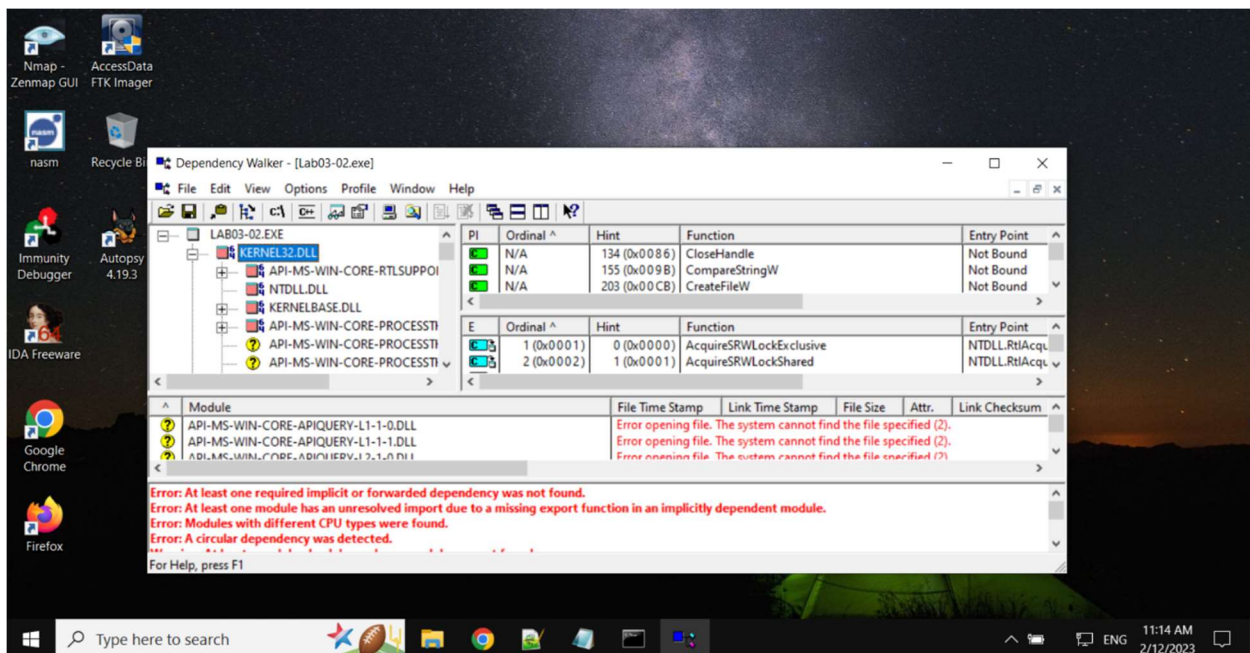
Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
n7w
n7w
n7w
n7@
n7@
k6.
n7@
j63
n7w
07v
n7Rich
.text
.rdata
@.data
.rsrc
@.reloc
hOpB
hYpB
VWj
hOpB
Y ^
hmpB
hwpB
```

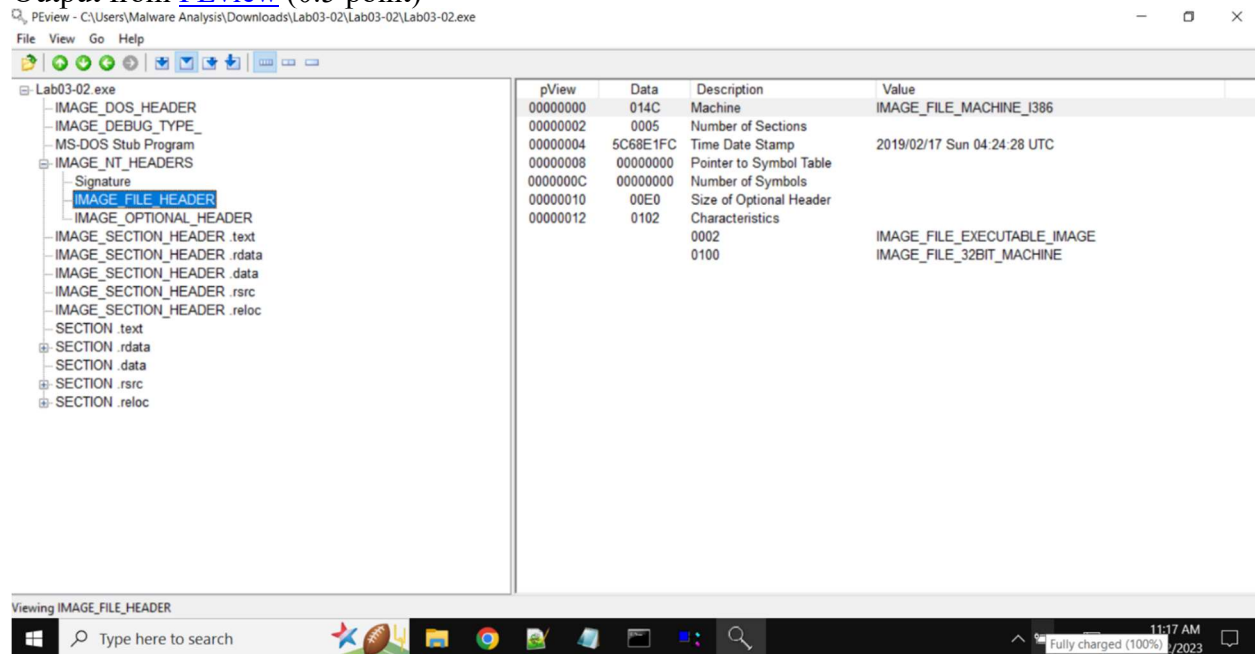
Output from [PEiD](#) (0.5 point)



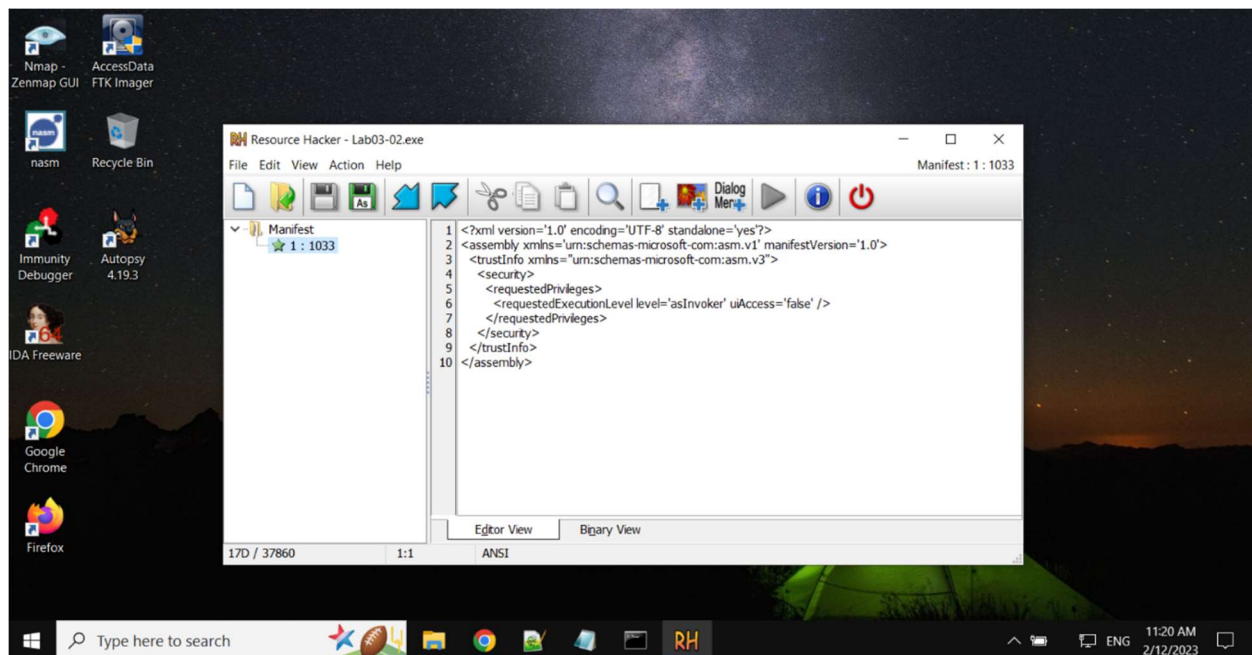
Output from [Dependency Walker 2.2](#) (0.5 point)



Output from [PEview](#) (0.5 point)



Output from [Resource Hacker](#) (0.5 point)



2. When is Lab03-02.exe compiled? (0.5 point)

Compiled on 2019/02/17 Sunday at 4:28 am.

3. Are there any indications that Lab03-02.exe is packed or obfuscated? If so, what are these indicators? (0.5 point)

No indications because there a lot of strings visible and would be very few if there were indications.

4. Do any imports hint at what this malware does? If so, which imports are they? (0.5 point)

The imports hint they can pretend to be another process. The imports are Kernel32.dll, libcurl.dll.

5. Are there any other files or host-based indicators that you could look for on infected systems? (0.5 point)

Files that look similar to .dll files are host-based indicators and I did not see any.

6. What network-based indicators could be used to find this malware on infected machines? (2 points)

IP addresses are network-based indicators and I didn't find any.

7. What would you guess is the purpose of Lab03-02.exe? (3 points)

The purpose of this lab is to introduce us to malware and see if we can recognize it.