Practical – Static Analysis of Windows Malware
A virtual machine has been provided for this practical. This is a safe environment for doing malware analysis without harming the lab computer or university network.

**** Please note - all activity on lab computers is monitored and recorded by Information Services. Please don't try to remove malware from the virtual machine or run it on the lab computers. Thank you. ****

Introduction
In this practical we will analyse several example Windows malware files using freely available static analysis tools. Please refer to your lecture notes for more information on the appropriate tools. Hint – these tools are very powerful so we can't include everything in the notes. Feel free to use google to find more information on each one.

Finally, remember to write a report about what you have found.

Starting the Virtual Machine

Follow these instructions to start the virtual machine and open a folder containing the required programs and example malware for analysis:

1. Using Windows Explorer browse to S:\Labs2020-21\CSC3059\
2. Double Click on 'CSC3059 Dynamic' (this may take some time)
3. Click on VM icon at bottom of screen
4. Select MW_Windows in left-hand pane
5. Click Start
6. On the VM, log in to account Labuser with password 'malware'
7. On the VM, Using Windows Explorer on VM navigate to C:\Labs

Starting the Practical
The malware files needed for the practical are stored on the virtual machine at:
C:\Labs\BinaryCollection\Chapter_1L\

The following malware analysis tools are stored in folders of C:\Labs\

- Dependency Viewer
- PEView
- PEiD

The following tools are stored in C:\Apps
- Strings
- MD5
- SHA1, SHA256

Resource Hacker - accessible via the Start Menu

Part 1

Use the tools introduced in the lecture to answer the following questions about the files

Lab01-01.exe
Lab01-01.dll

1. When were each of the files compiled?

    Hint – use PEView to examine IMAGE_NT_HEADERS -> IMAGE_FILE_HEADER

2. Are there indications that these files have been packed or obfuscated?

    Hint – use PEiD to check if a packer was used.

3. Examine the imports of each file. Do the imported functions indicate anything about what these files do? Which imports do you think are indicative of the functionality of the files and why.

    Hint - use Dependency Walker to examine which functions are imported by the .exe or .dll. You can also use the MSDN website to look up more information about the function names and what they do https://msdn.microsoft.com. Alternatively, you might find it easier to just google "MSDN X" where X is the function name.

4. In Lab01-01.exe are there any indicators of files on the host computer that could also be infected i.e. are there any host based indicators?

    Hint – use PEVIEW to examine the strings in SECTION .data, or use strings. Is there anything suspicious about the .dll strings mentioned here?

5. Are there any network-based indicators that could be used to identify these files on infected machines?

    Hint – use PEVIEW/strings to check for strings related to network activity e.g. web or IP addresses.

Part 2

Examine the file Lab01-03.exe.

a. Are there any indications that this file was packed?

> Hint - check the difference between the Virtual Size and Size of Raw Data using PEView. What does this tell us?

b. What are the file imports?

Part 3

Examine the file Lab01-04.exe in order to answer the following questions:

a. Are there any indicators that this file is packed?
b. When was this file compiled, and what does this indicate?
c. What are the file imports? What do they tell about its functionality?
d. Are there any host-based indicators that could be used to identify this malware?
e. Are there any indicators of network activity?