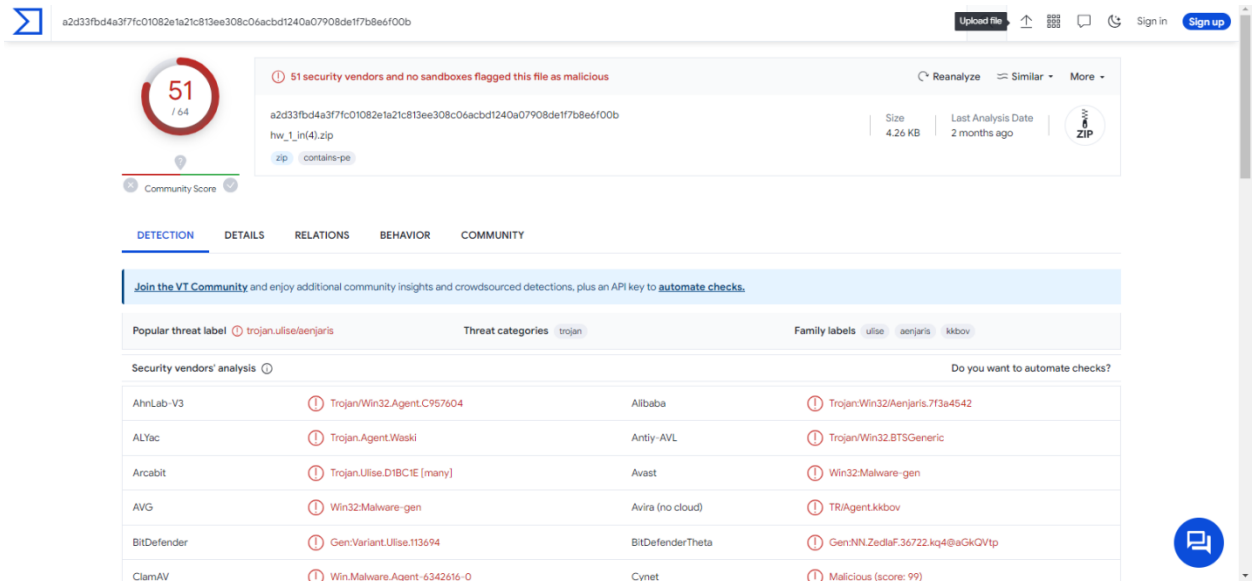
Alanna Richerson

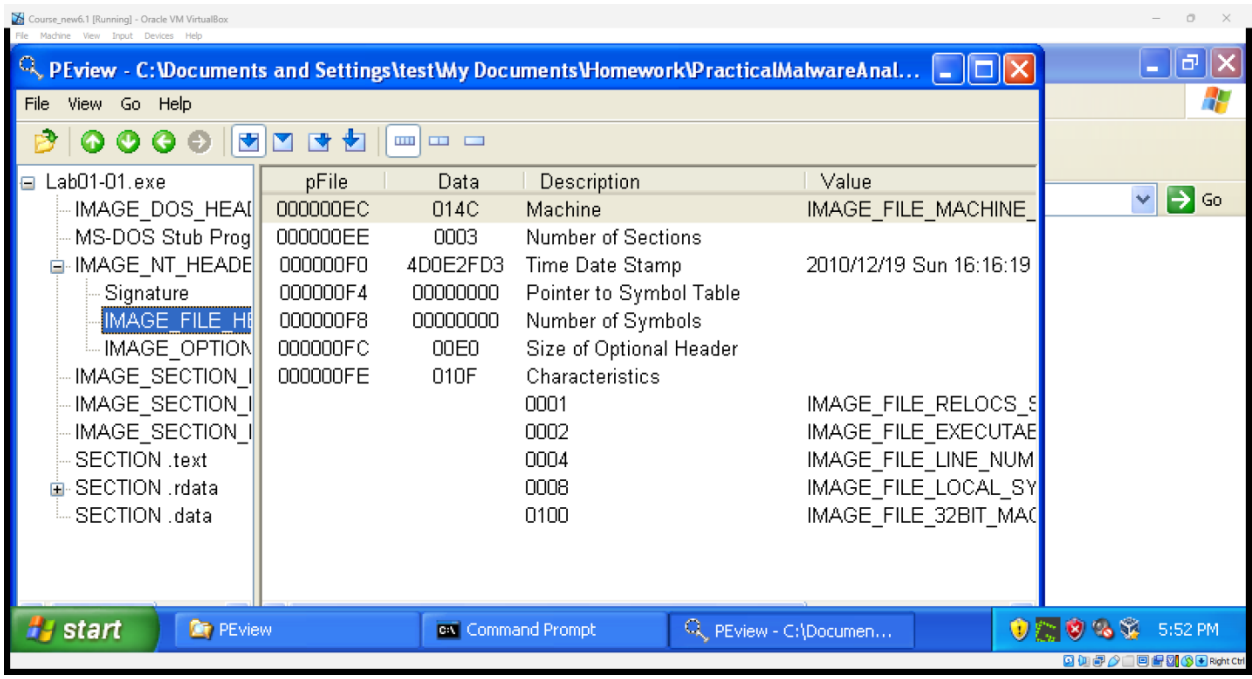
01168621

Download the zip file from Canvas that contains hw_1_in.exe and hw_1_in.dll (or Lab01-02.exe in "Chapter_1L" if you are having trouble of downloading the file). Unzip them to a location on your VM. Please address the following queries (attach screenshots to support your answers):

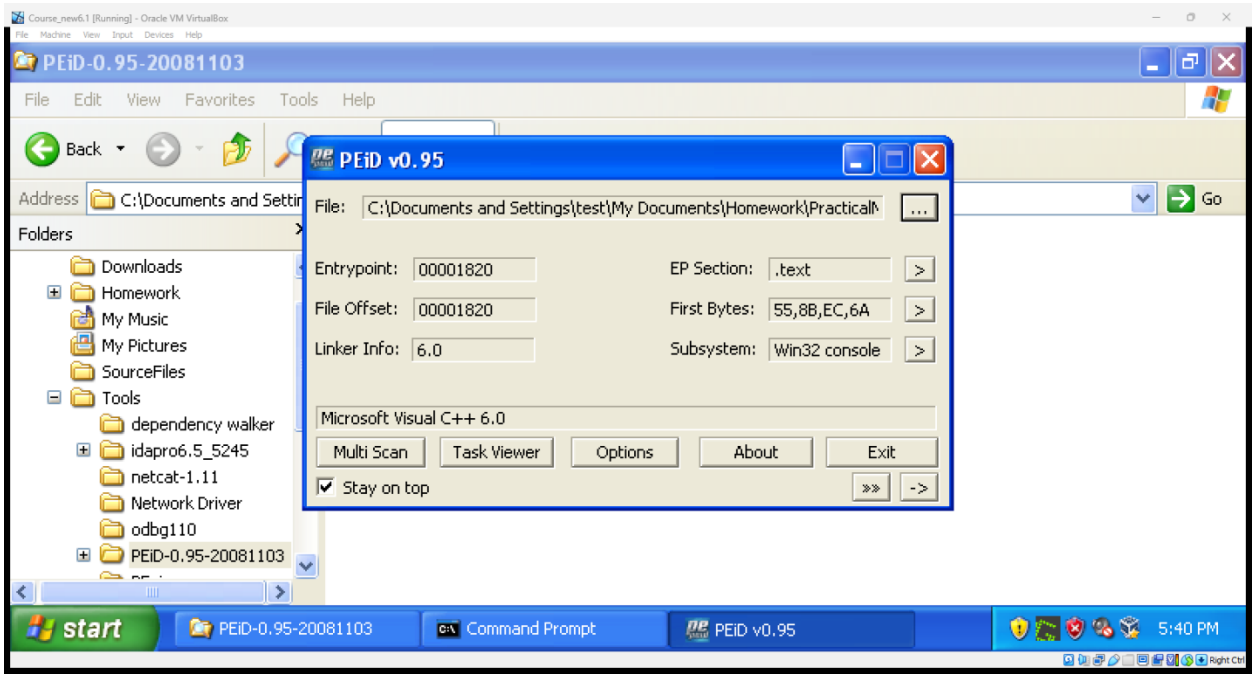
1. Upload the files to VirusTotal and evaluate the generated reports. Does the consensus suggest that they are malicious? If so, can you pinpoint the type of malware indicated?

1. 

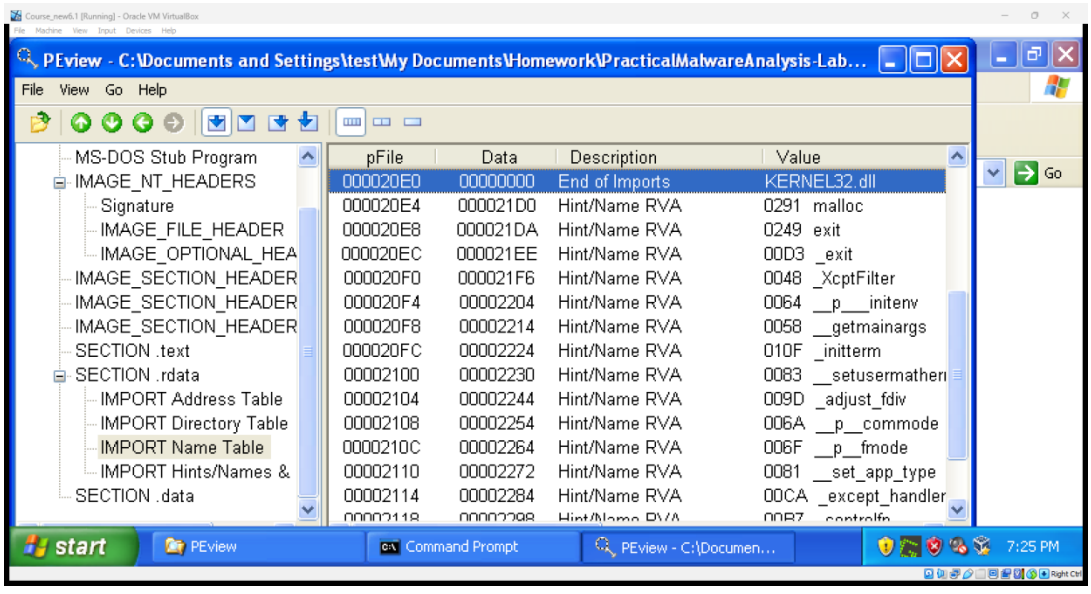
2. Identify the compilation dates of the files.

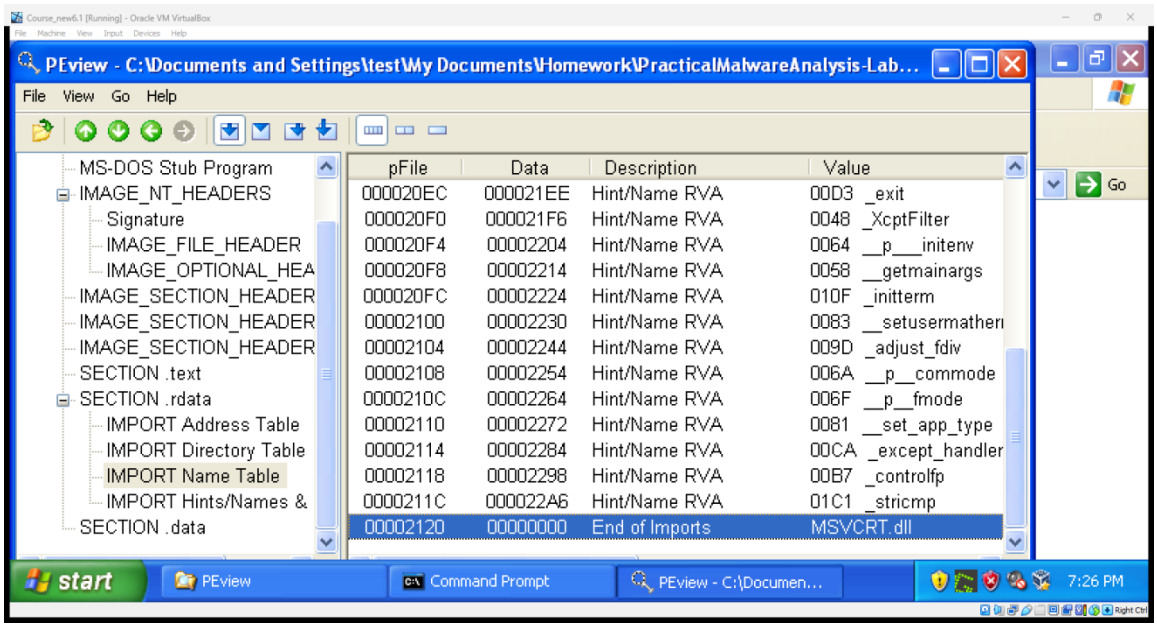
1. 

3. Examine whether the program is packed. Could you describe the method you utilized to find this out? Support your answer with screenshots.

1. 

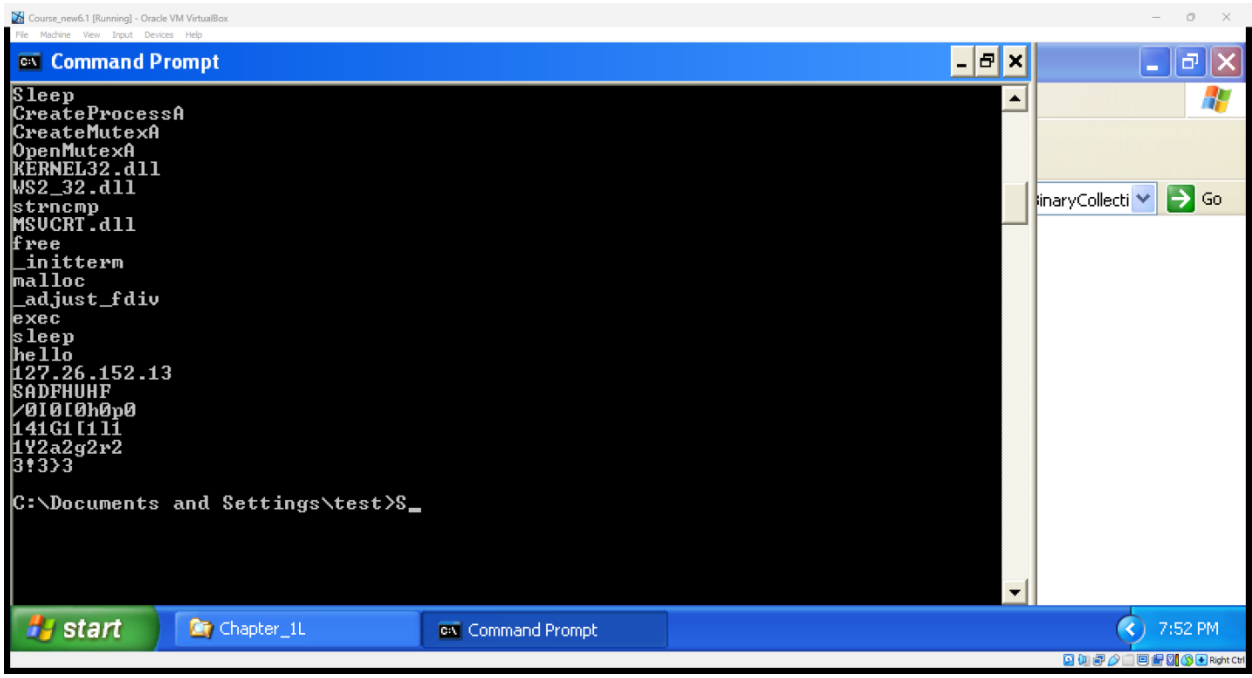
4. List down the imports. Are there any that raise suspicion? Can you deduce the malware's functionalities from the imports?

1. 

2. 

3. This malware allows for a network-enabled back door

5. Are there any signs of network-based indicators? If an IP address is evident, what is it, and what insights can be gained from it?

1. 

6. Based on your analysis, can you speculate on the malware's objective?

    1. The malware's speculated objective is to create a backdoor. The exec string will probably be transmitted to the IP address for initializing the backdoor via CreateProcess, employing sleep to avoid detection.

Remember to attach screenshots wherever possible to substantiate your findings.