Warning - Reminder

The files you are working with are live malware payloads, download and use them only within a virtual environment. In some cases, you might be asked to disable or enable your outbound network connection.

Part 1 [80 pts]

Use the python library pefile (https://github.com/erocarrera/pefile) to scan through a directory of files and create a report of all of those files. The report should attempt to answer as many questions as possible that you had to answer in lab 1. For questions you can't answer definitively, provide a sliding scale (very unlikely, unlikely, unknown, likely, very likely).

Part 2 [70 pts]

Extend your PE tool you've developed to do anything you want. Ideas:

- Modify contents of the PE file (still retain functionality of the program)- can you mask important information or make legitimate files appear to be malware?,
- Perform additional data analysis, aggregate information about the entire set of programs,
- Generate and compare graphs of the internal structure of PE files
- Create an html page/report that contains relevant information about imports/exports

Group Details / Submission[50 pts]

- You may (should?) work in groups of up to three.
- You must use version control (github?) [all or nothing]
- Your repository must:
  - include me in your project (borowczak@gmail.com) and/or be a publicly accessible project

  10 pts must have a readme.md file that describes the purpose and usage of your tool, and should including some sample usages and outputs

  10 pts must include a requirements.txt file containing a listing of the libraries I would need to run your code

  30 pts must include the outputs of your tool being run on the malware directory, as well as the program file directory of the malware VM.