Lab3: Build a Dynamic Heuristic Analysis Tool for Detection of Unknown Malware (8 Points)

ransomware

Objectives and Targets

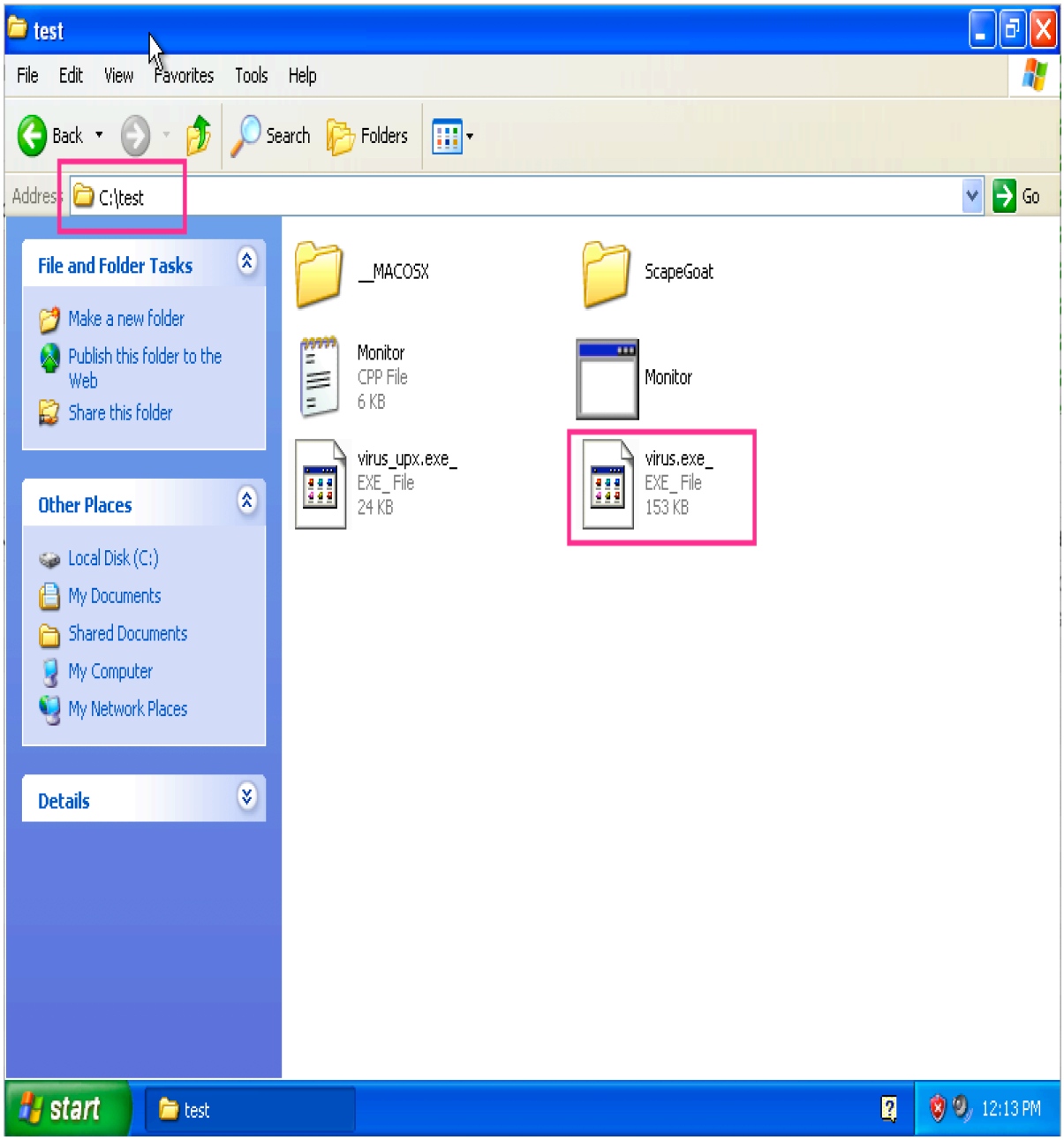
In today's society virus makers have a large set of obfuscation tools to avoid classic signature detection used by antivirus
software. Therefore there is a need to identify new and obfuscated viruses in a better way. One option is to look at the behavior of
a program by executing the program in a virtual environment to determine if it is malicious or benign. This approach is called dynamic
heuristic analysis.

In this lab, you are asked to develop a new heuristic dynamic analysis tool for detecting unknown ransomware.

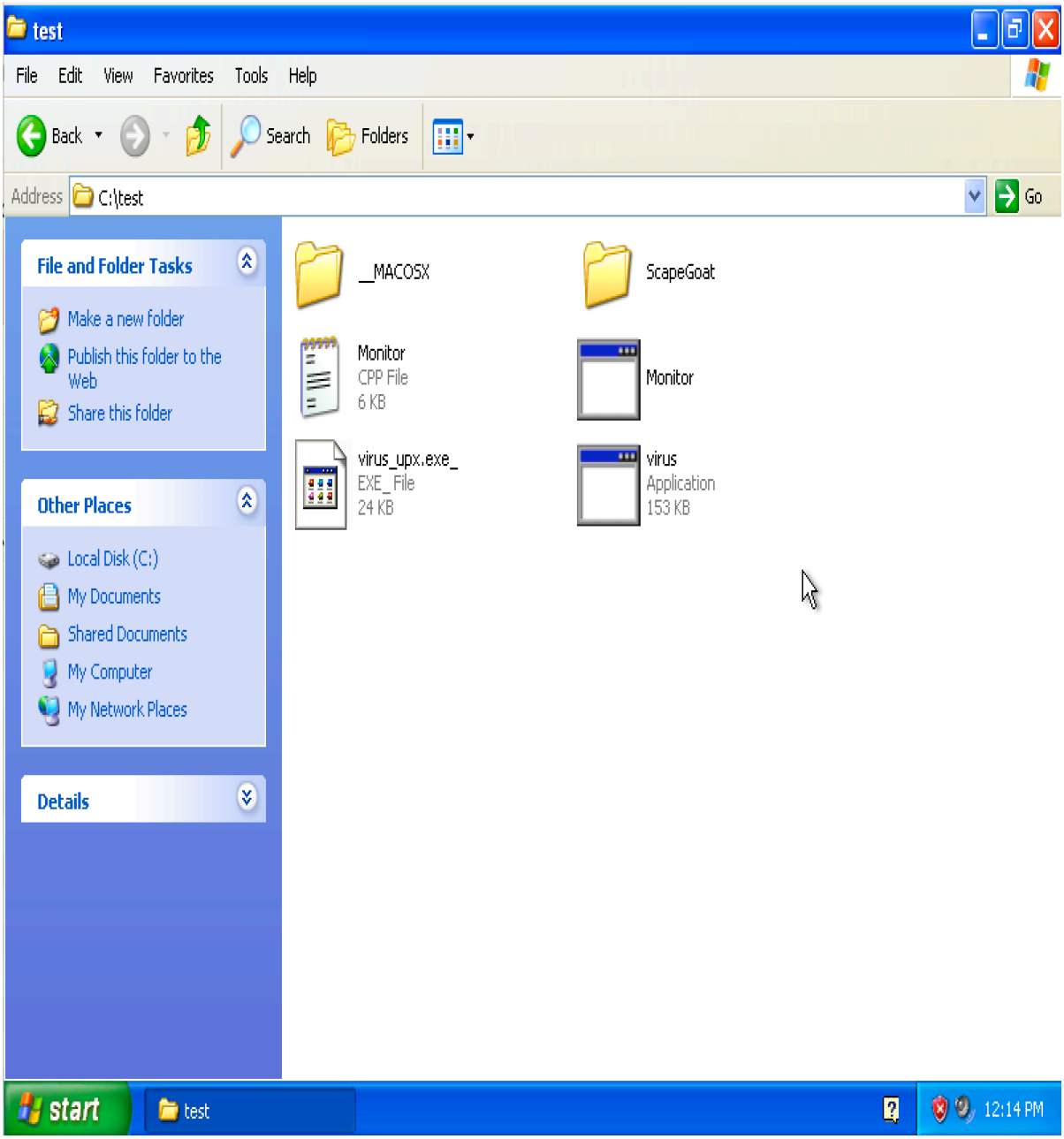
Target 1: Generate Log file (3 points):

Step 1: In a Windows XP environment (Link). Download ransomware sample and a monitor program (Link).

Step 2: Unzip the file with password `infected`, then create a new folder `test` under `C:\`, copy all files to that folder (`C:\test`)



Step 3: Rename `virus.exe_` to `virus.exe`



Step 4: Double click and run `Monitor.exe`
Step 5: Double click and run `virus.exe`
Step 6: Close `Monitor.exe`
Step 7: Open `log.txt` which contains the log data recorded by `Monitor.exe`. It should record all the activities that happened in this folder.

Target 2: Analysis Log file and implement heuristic rules (5 points):

Step 8: Please **create a runnable program** (recommend using Python). **This program should be able to read the log.txt file and detect if these logged**

activities are malicious or not based on the following rules:

1. **More than three word documents (docx) in `ScapeGoat` folder have been renamed**
2. **More than 3 files in `ScapeGoat` folder have been modified**
3. **The number of file self-deletes (a file been created and then deleted) activity is larger than or equal to 1**

A program is malicious ransomware if and only if it violates all three rules. And your program should then output

`malware detected --> HEUR:Trojan-Ransom.DocxEncrypt.Generic`

Deliverables:

- A zip file (**source_code.zip**) that contains the source code of your malware detection program.
- A detailed project report (**lab3_report.pdf**) in **PDF format** to describe what you have done, including screenshots and code snippets.
- **DO NOT** upload malware sample to D2L

Submission

- Check lab due date on the course website. Late submission will not be accepted.
- The assignment should be submitted to D2L directly.
- Your submission should include two separated files **(lab3_report.pdf)**
- No copy or cheating is tolerated. If your work is based on others', please give clear attribution. Otherwise, you **WILL FAIL** this course.