# Practical Malware Analysis Lab 1-3

## Questions

1. Upload the Lab01-03.exe file to https://www.VirusTotal.com/. Does it match any existing antivirus definitions?
2. Are there any indications that this file is packed or obfuscated? If so, what are these indications? If the file is packed, unpack it if possible.
3. Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?
4. What host- or network-based indicators could be used to identify this malware on infected machines?

## Question 1

Result for Lab01-03.exe
MD5: 9c5c27494c28ed0b14853b346b113145

This EXE definitely seems malicious. The file was detected by 50/70 engines.

## Question 2

I believe this file is packed. The virtual size is much higher than it should be for a non packed file. Also VirusTotal says it was packed with FSG v1.00 (Eng) -> dulek/xt.

## Question 3

No not at all this program is packed

## Question 4

N/A

I don't know how to unpack files manually yet. When I get there in the book I will come back and analyse this file.