1. Write a small Java program (any Java program) and compile it using Oracle’s javac compiler, then “disassemble” the class file using one of the tools covered in class. If you need an example, you can look at ReversingJava.java, linked above. Document the bytecode of the program that you wrote and explain each instruction. (Note: be sure to specify the version of javac used)

jdk-1.7.0\_79

1. Compare disassembly output when compiling with just ‘javac’ and with ‘javac -g:none’. Explain the differences.

|  |
| --- |
| JAVAC |
|  |
| javac -g:none |
|  |

b. Confirm your results by diff’ing the output of javap -c -verbose for both .class files. If you don’t have a go-to diff’ing tool, try installing meld on your remnux VM (sudo apt install meld). You can run meld by typing ‘meld <file1> <file2>’ to get a visual diff.

2.Use the class file from Question 1 to complete the following tasks.  
Download ProGuard  
 On Windows: download ProGuard (http://sourceforge.net/projects/proguard/files/proguard/).  
 On Remnux: install via ‘sudo apt install proguard’  
Obfuscate Java Application

a. Create a jar archive, named “ReversingProguard.jar” for the compiled class file from Question 1. Show the size and the content of the “ReversingProguard.jar” archive.  
 b. Run the “ReversingProguard.jar” file and show the command and output.  
 c. Use http://proguard.sourceforge.net/ as reference and obfuscate “ReversingProguard.jar”.  
 i) Using a command or the gui, capture the steps you used to obfuscate the jar file  
 ii) Show the content of the \*.pro file used during obfuscation  
 d. Show the size and the content of the obfuscated “ReversingProguard.jar” archive.  
 e. Run the obfuscated “ReversingProguard.jar” and show the command and output.  
 f. Unpack the obfuscated program and open the compiled class file in JD-GUI, show the decompiled code.