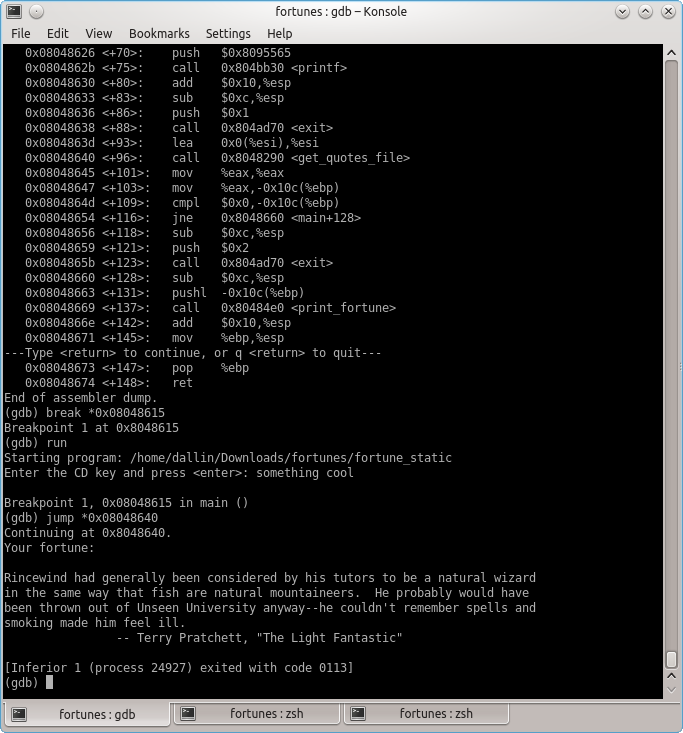
Dallin Christensen

CS 465

Project 11 (Extracting Secrets)

1) How did you use the debugger to bypass the password mechanism? What variables were modified? Please include a screenshot of the debugger in the report.

In GDB I set a break point at 0x08048615 (check\_cdkey). Instead of letting the check\_cdkey code execute, I jumped straight to 0x08048640 (get\_quotes\_file). I did not modify any variables in the debugger.

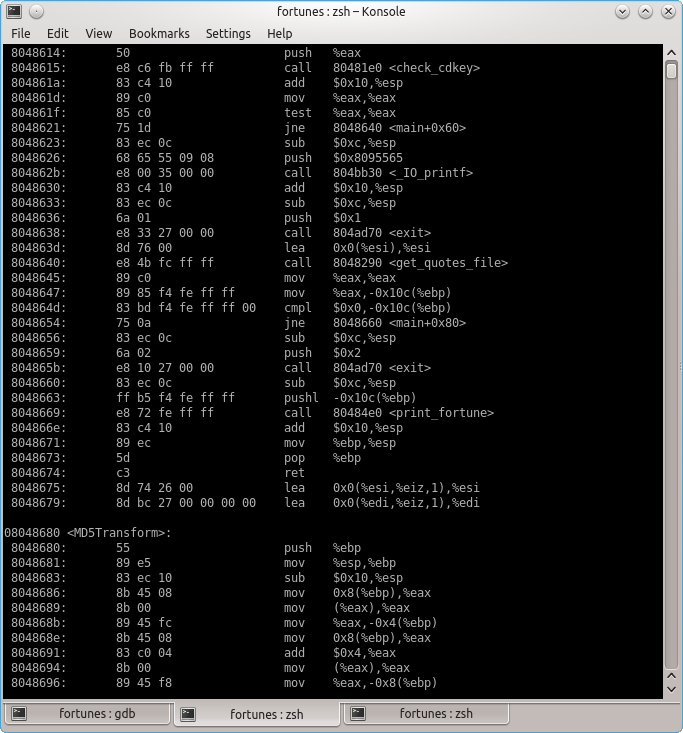
Screenshot 1: GDB disassembly and bypass

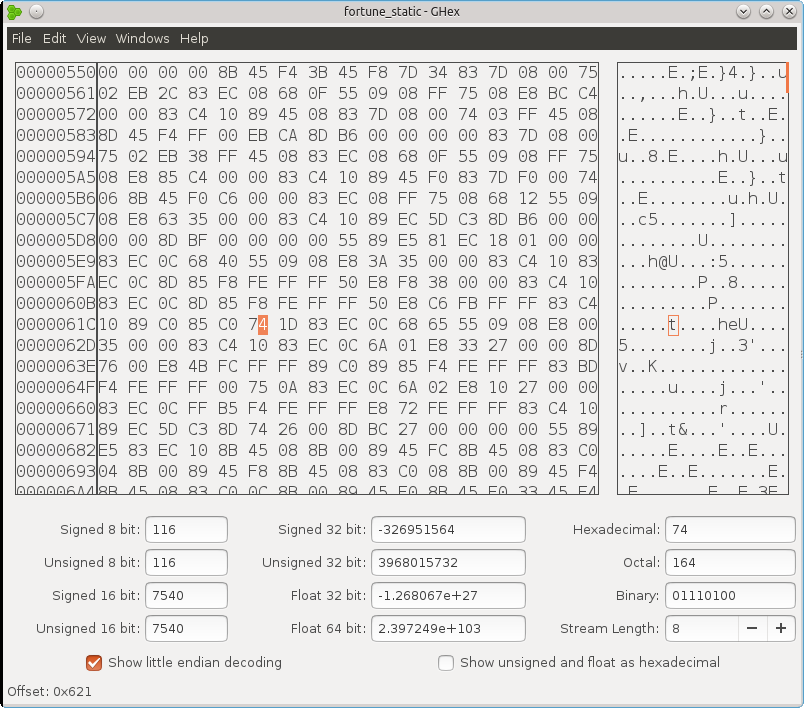
2) How did you edit the program to bypass the cdkey mechanism?

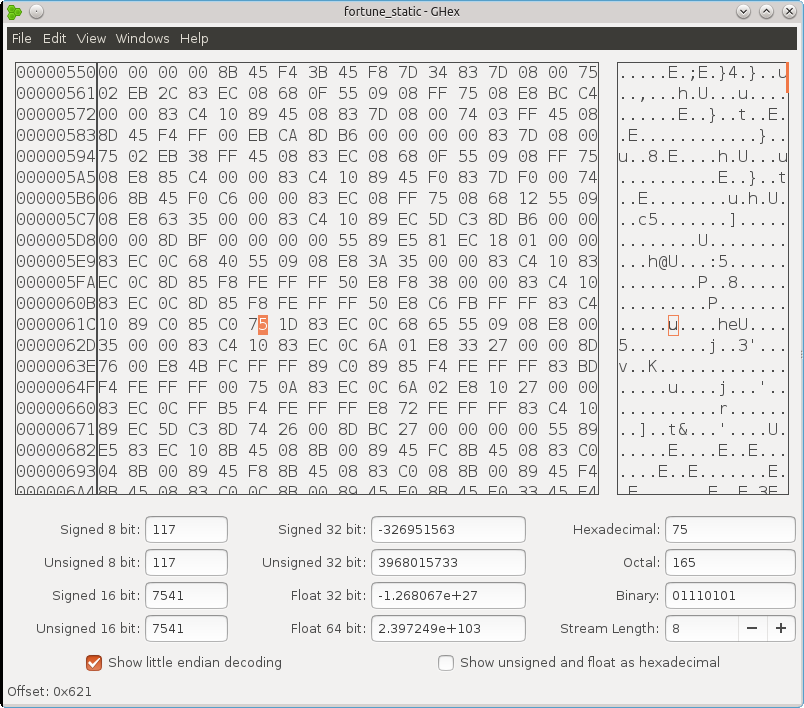
See above.

3) How did you obtain all the fortunes from the encrypted file?

I did an objdump to see the assembly code with it's associated hex values. I then used Ghex to modify the values. I searched for the “jne” that would determine whether or not the code went to get\_quotes\_file and changed the value from 75 (jne) to 74 (je).

Screenshot 2: objdump (hex and assembly)

Screenshot 4: Hex (after)

Screenshot 3: Hex (before)

Screenshot 5: Modified binary allowing any password