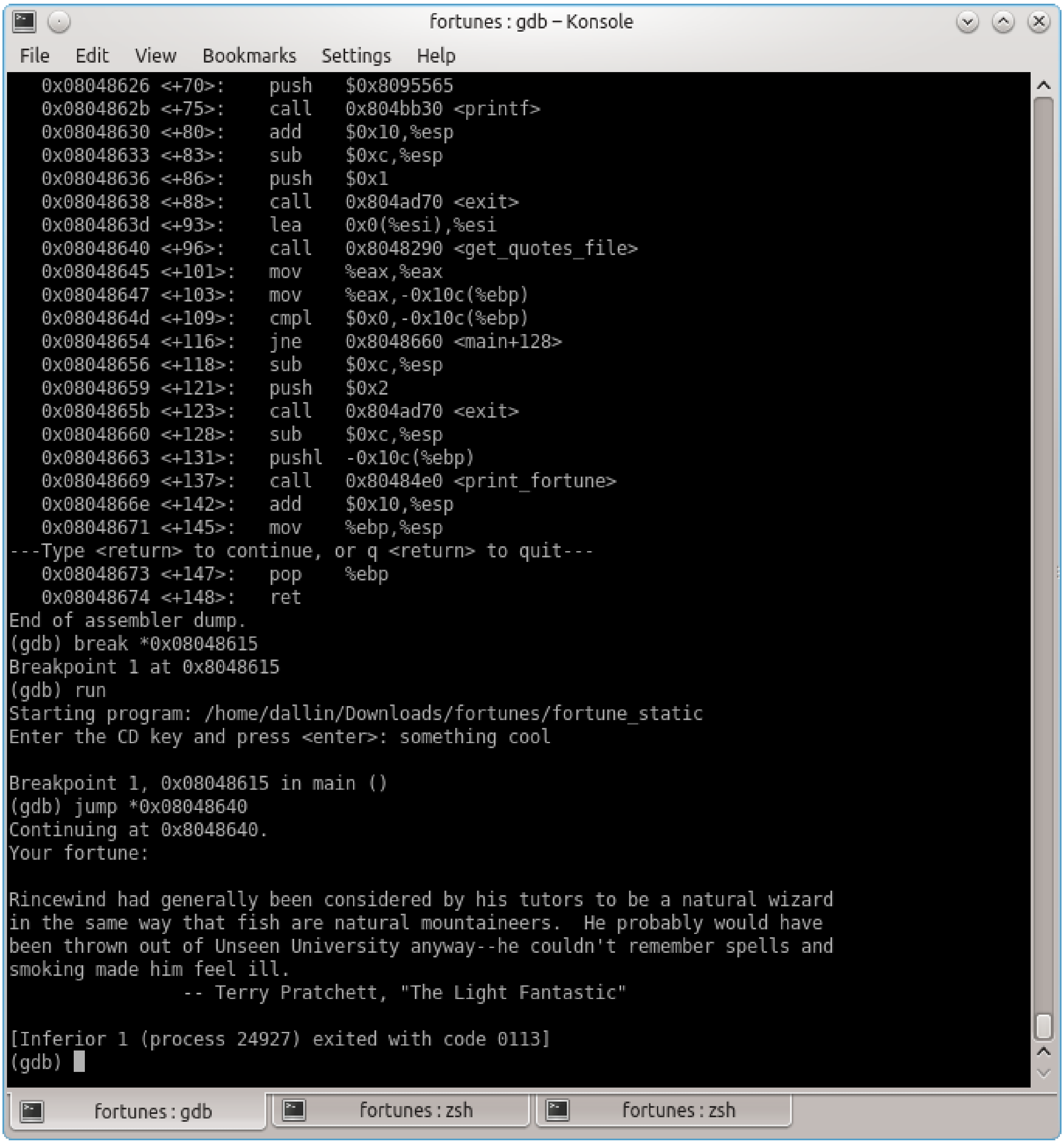
Dallin Christensen
CS 465

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.



```
   0x08048626 <+70>:    push   $0x8095565
   0x0804862b <+75>:    call   0x804bb30 <printf>
   0x08048630 <+80>:    add    $0x10,%esp
   0x08048633 <+83>:    sub    $0xc,%esp
   0x08048636 <+86>:    push   $0x1
   0x08048638 <+88>:    call   0x804ad70 <exit>
   0x0804863d <+93>:    lea    0x0(%esi),%esi
   0x08048640 <+96>:    call   0x8048290 <get_quotes_file>
   0x08048645 <+101>:   mov    %eax,%eax
   0x08048647 <+103>:   mov    %eax,-0x10c(%ebp)
   0x0804864d <+109>:   cmpl   $0x0,-0x10c(%ebp)
   0x08048654 <+116>:   jne    0x8048660 <main+128>
   0x08048656 <+118>:   sub    $0xc,%esp
   0x08048659 <+121>:   push   $0x2
   0x0804865b <+123>:   call   0x804ad70 <exit>
   0x08048660 <+128>:   sub    $0xc,%esp
   0x08048663 <+131>:   pushl  -0x10c(%ebp)
   0x08048669 <+137>:   call   0x80484e0 <print_fortune>
   0x0804866e <+142>:   add    $0x10,%esp
   0x08048671 <+145>:   mov    %ebp,%esp
---Type <return> to continue, or q <return> to quit---
   0x08048673 <+147>:   pop    %ebp
   0x08048674 <+148>:   ret
End of assembler dump.
(gdb) break *0x08048615
Breakpoint 1 at 0x8048615
(gdb) run
Starting program: /home/dallin/Downloads/fortunes/fortune_static
Enter the CD key and press <enter>: something cool

Breakpoint 1, 0x08048615 in main ()
(gdb) jump *0x08048640
Continuing at 0x8048640.
Your fortune:

Rincewind had generally been considered by his tutors to be a natural wizard
in the same way that fish are natural mountaineers.  He probably would have
been thrown out of Unseen University anyway--he couldn't remember spells and
smoking made him feel ill.
                -- Terry Pratchett, "The Light Fantastic"

[Inferior 1 (process 24927) exited with code 0113]
(gdb) █
```

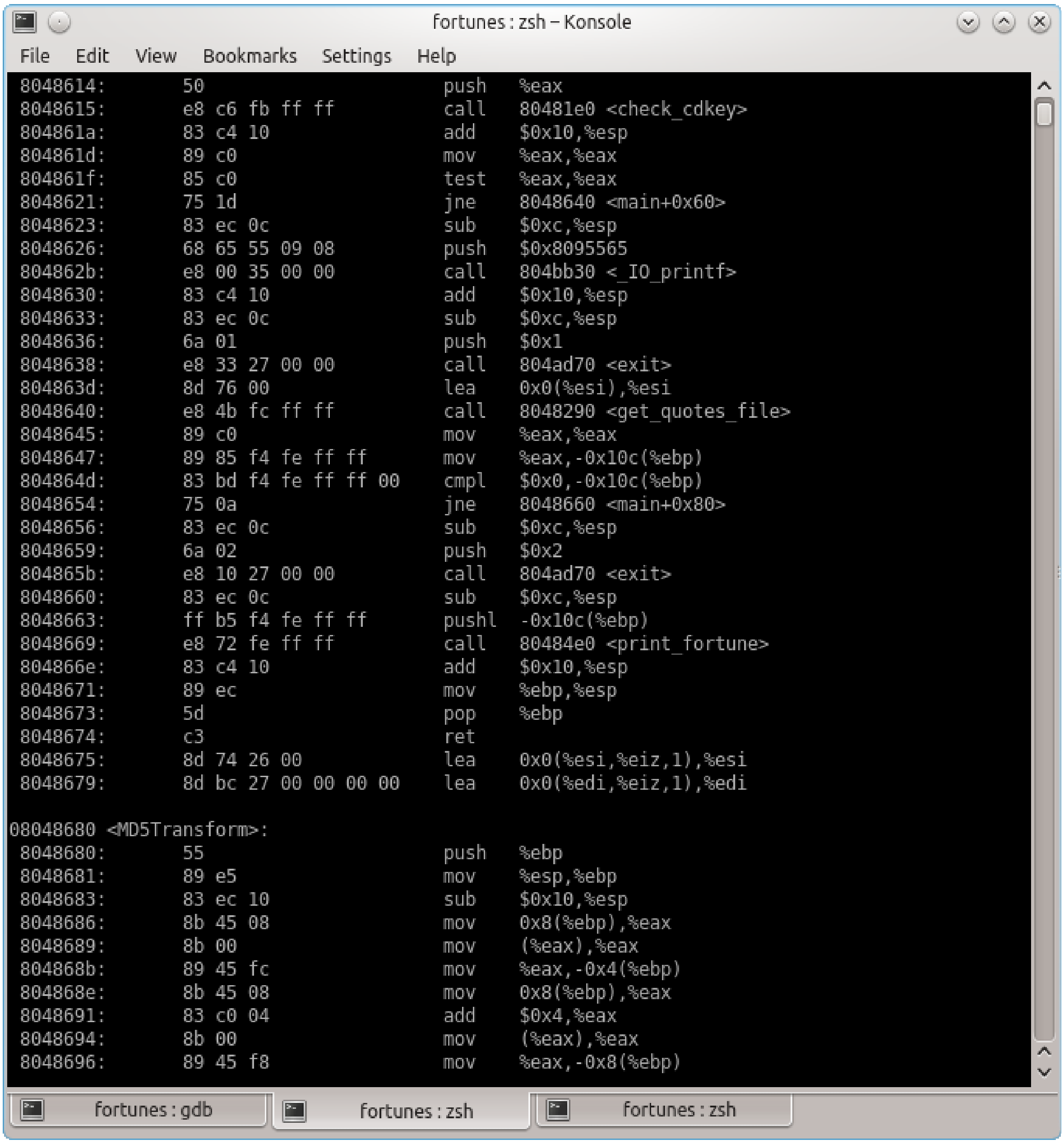
Screenshot 1: GDB disassembly and bypass

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?

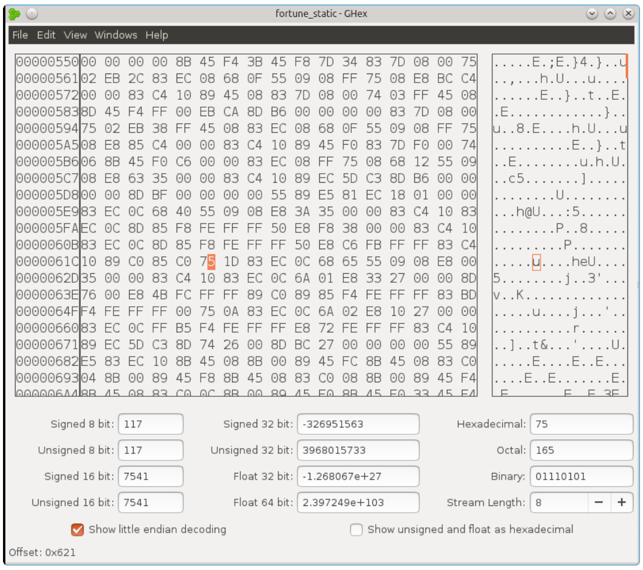
I did an objdump to see the assembly code with it's associated hex values. I then used Ghex to modify the values. I searched for the “jne” that would determine whether or not the code went to get_quotes_file and changed the value from 75 (jne) to 74 (je).



```
 8048614:       50                      push   %eax
 8048615:       e8 c6 fb ff ff          call   80481e0 <check_cdkey>
 804861a:       83 c4 10                add    $0x10,%esp
 804861d:       89 c0                   mov    %eax,%eax
 804861f:       85 c0                   test   %eax,%eax
 8048621:       75 1d                   jne    8048640 <main+0x60>
 8048623:       83 ec 0c                sub    $0xc,%esp
 8048626:       68 65 55 09 08          push   $0x8095565
 804862b:       e8 00 35 00 00          call   804bb30 <_IO_printf>
 8048630:       83 c4 10                add    $0x10,%esp
 8048633:       83 ec 0c                sub    $0xc,%esp
 8048636:       6a 01                   push   $0x1
 8048638:       e8 33 27 00 00          call   804ad70 <exit>
 804863d:       8d 76 00                lea    0x0(%esi),%esi
 8048640:       e8 4b fc ff ff          call   8048290 <get_quotes_file>
 8048645:       89 c0                   mov    %eax,%eax
 8048647:       89 85 f4 fe ff ff       mov    %eax,-0x10c(%ebp)
 804864d:       83 bd f4 fe ff ff 00    cmpl   $0x0,-0x10c(%ebp)
 8048654:       75 0a                   jne    8048660 <main+0x80>
 8048656:       83 ec 0c                sub    $0xc,%esp
 8048659:       6a 02                   push   $0x2
 804865b:       e8 10 27 00 00          call   804ad70 <exit>
 8048660:       83 ec 0c                sub    $0xc,%esp
 8048663:       ff b5 f4 fe ff ff       pushl  -0x10c(%ebp)
 8048669:       e8 72 fe ff ff          call   80484e0 <print_fortune>
 804866e:       83 c4 10                add    $0x10,%esp
 8048671:       89 ec                   mov    %ebp,%esp
 8048673:       5d                      pop    %ebp
 8048674:       c3                      ret
 8048675:       8d 74 26 00             lea    0x0(%esi,%eiz,1),%esi
 8048679:       8d bc 27 00 00 00 00    lea    0x0(%edi,%eiz,1),%edi

08048680 <MD5Transform>:
 8048680:       55                      push   %ebp
 8048681:       89 e5                   mov    %esp,%ebp
 8048683:       83 ec 10                sub    $0x10,%esp
 8048686:       8b 45 08                mov    0x8(%ebp),%eax
 8048689:       8b 00                   mov    (%eax),%eax
 804868b:       89 45 fc                mov    %eax,-0x4(%ebp)
 804868e:       8b 45 08                mov    0x8(%ebp),%eax
 8048691:       83 c0 04                add    $0x4,%eax
 8048694:       8b 00                   mov    (%eax),%eax
 8048696:       89 45 f8                mov    %eax,-0x8(%ebp)
```

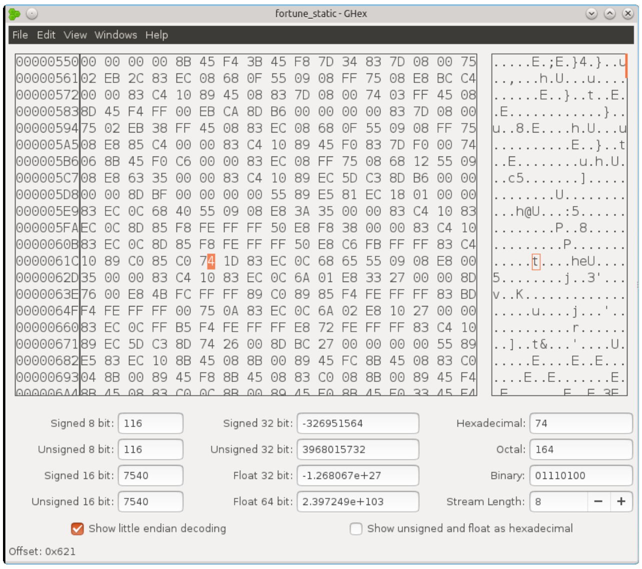
Screenshot 2: objdump (hex and assembly)



```
00000550 00 00 00 00 8B 45 F4 3B 45 F8 7D 34 83 7D 08 00 75  .....E.;E.}4.}..u
00000561 02 EB 2C 83 EC 08 68 0F 55 09 08 FF 75 08 E8 BC C4  ..,...h.U...u....
00000572 00 00 83 C4 10 89 45 08 83 7D 08 00 74 03 FF 45 08  ......E..}..t..E.
00000583 8D 45 F4 FF 00 EB CA 8D B6 00 00 00 00 83 7D 08 00  .E............}..
00000594 75 02 EB 38 FF 45 08 83 EC 08 68 0F 55 09 08 FF 75  u..8.E....h.U...u
000005A5 08 E8 85 C4 00 00 83 C4 10 89 45 F0 83 7D F0 00 74  ..........E..}..t
000005B6 06 8B 45 F0 C6 00 00 83 EC 08 FF 75 08 68 12 55 09  ..E........u.h.U.
000005C7 08 E8 63 35 00 00 83 C4 10 89 EC 5D C3 8D B6 00 00  ..c5.......].....
000005D8 00 00 8D BF 00 00 00 00 55 89 E5 81 EC 18 01 00 00  ........U........
000005E9 83 EC 0C 68 40 55 09 08 E8 3A 35 00 00 83 C4 10 83  ...h@U...:5......
000005FA EC 0C 8D 85 F8 FE FF FF 50 E8 F8 38 00 00 83 C4 10  ........P..8.....
0000060B 83 EC 0C 8D 85 F8 FE FF FF 50 E8 C6 FB FF FF 83 C4  .........P.......
0000061C 10 89 C0 85 C0 75 1D 83 EC 0C 68 65 55 09 08 E8 00  .....u....heU....
0000062D 35 00 00 83 C4 10 83 EC 0C 6A 01 E8 33 27 00 00 8D  5........j..3'...
0000063E 76 00 E8 4B FC FF FF 89 C0 89 85 F4 FE FF FF 83 BD  v..K.............
0000064F F4 FE FF FF 00 75 0A 83 EC 0C 6A 02 E8 10 27 00 00  .....u....j...'..
00000660 83 EC 0C FF B5 F4 FE FF FF E8 72 FE FF FF 83 C4 10  ..........r......
00000671 89 EC 5D C3 8D 74 26 00 8D BC 27 00 00 00 00 55 89  ..]..t&...'....U.
00000682 E5 83 EC 10 8B 45 08 8B 00 89 45 FC 8B 45 08 83 C0  .....E....E..E...
00000693 04 8B 00 89 45 F8 8B 45 08 83 C0 08 8B 00 89 45 F4  ....E..E.......E.
000006A4 8B 45 08 83 C0 0C 8B 00 89 45 F0 8B 45 F0 33 45 F4  .E.......E..E.3E.
```

Signed 8 bit: 117
Unsigned 8 bit: 117
Signed 16 bit: 7541
Unsigned 16 bit: 7541
Signed 32 bit: -326951563
Unsigned 32 bit: 3968015733
Float 32 bit: -1.268067e+27
Float 64 bit: 2.397249e+103
Hexadecimal: 75
Octal: 165
Binary: 01110101
Stream Length: 8 − +
☑ Show little endian decoding
☐ Show unsigned and float as hexadecimal
Offset: 0x621

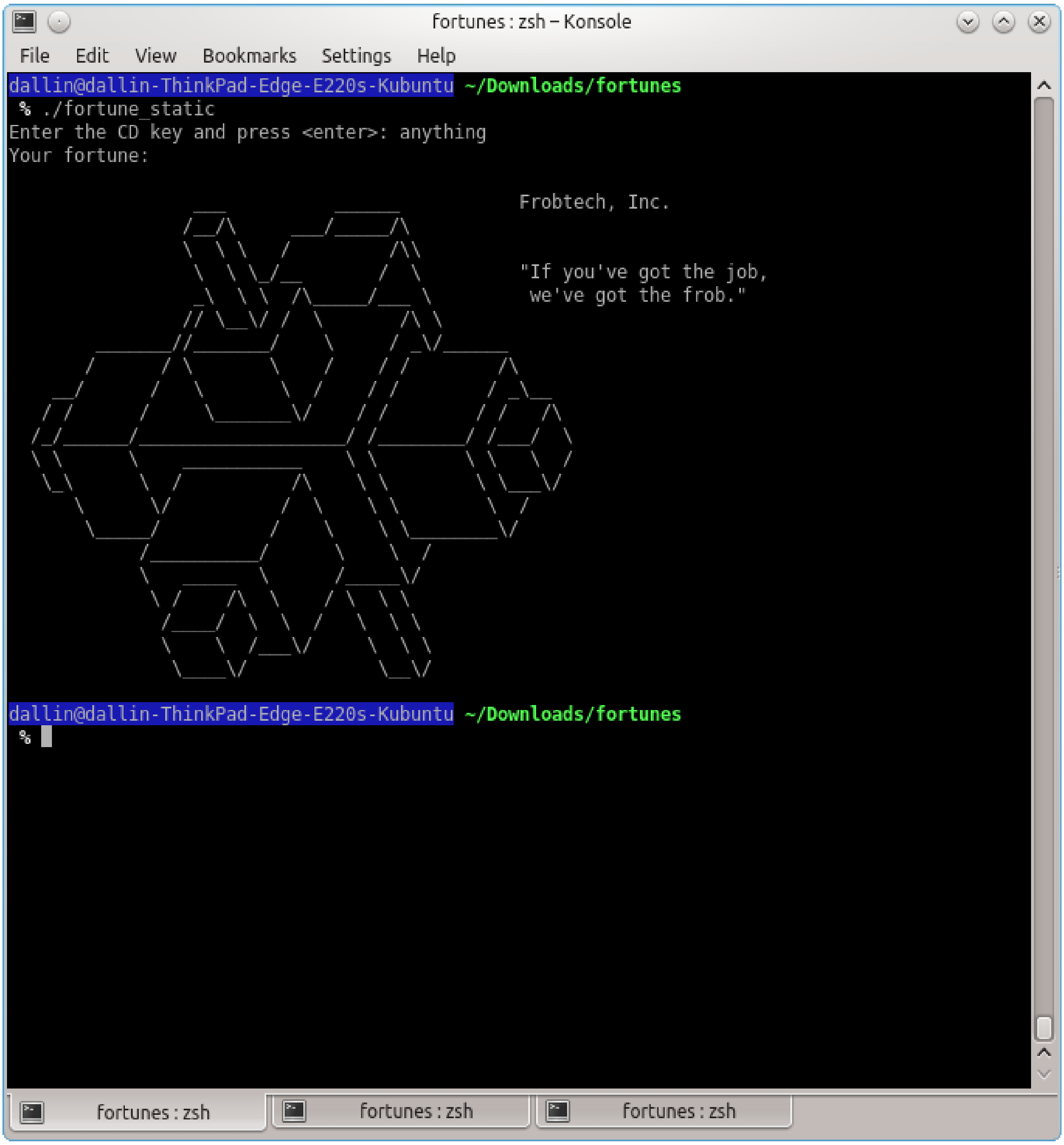
Screenshot 3: Hex (before)



```
00000550 00 00 00 00 8B 45 F4 3B 45 F8 7D 34 83 7D 08 00 75  .....E.;E.}4.}..u
00000561 02 EB 2C 83 EC 08 68 0F 55 09 08 FF 75 08 E8 BC C4  ..,...h.U...u....
00000572 00 00 83 C4 10 89 45 08 83 7D 08 00 74 03 FF 45 08  ......E..}..t..E.
00000583 8D 45 F4 FF 00 EB CA 8D B6 00 00 00 00 83 7D 08 00  .E............}..
00000594 75 02 EB 38 FF 45 08 83 EC 08 68 0F 55 09 08 FF 75  u..8.E....h.U...u
000005A5 08 E8 85 C4 00 00 83 C4 10 89 45 F0 83 7D F0 00 74  ..........E..}..t
000005B6 06 8B 45 F0 C6 00 00 83 EC 08 FF 75 08 68 12 55 09  ..E........u.h.U.
000005C7 08 E8 63 35 00 00 83 C4 10 89 EC 5D C3 8D B6 00 00  ..c5.......].....
000005D8 00 00 8D BF 00 00 00 00 55 89 E5 81 EC 18 01 00 00  ........U........
000005E9 83 EC 0C 68 40 55 09 08 E8 3A 35 00 00 83 C4 10 83  ...h@U...:5......
000005FA EC 0C 8D 85 F8 FE FF FF 50 E8 F8 38 00 00 83 C4 10  ........P..8.....
0000060B 83 EC 0C 8D 85 F8 FE FF FF 50 E8 C6 FB FF FF 83 C4  .........P.......
0000061C 10 89 C0 85 C0 74 1D 83 EC 0C 68 65 55 09 08 E8 00  .....t....heU....
0000062D 35 00 00 83 C4 10 83 EC 0C 6A 01 E8 33 27 00 00 8D  5........j..3'...
0000063E 76 00 E8 4B FC FF FF 89 C0 89 85 F4 FE FF FF 83 BD  v..K.............
0000064F F4 FE FF FF 00 75 0A 83 EC 0C 6A 02 E8 10 27 00 00  .....u....j...'..
00000660 83 EC 0C FF B5 F4 FE FF FF E8 72 FE FF FF 83 C4 10  ..........r......
00000671 89 EC 5D C3 8D 74 26 00 8D BC 27 00 00 00 00 55 89  ..]..t&...'....U.
00000682 E5 83 EC 10 8B 45 08 8B 00 89 45 FC 8B 45 08 83 C0  .....E....E..E...
00000693 04 8B 00 89 45 F8 8B 45 08 83 C0 08 8B 00 89 45 F4  ....E..E.......E.
000006A4 8B 45 08 83 C0 0C 8B 00 89 45 F0 8B 45 F0 33 45 F4  .E.......E..E.3E.
```

Signed 8 bit: 116
Unsigned 8 bit: 116
Signed 16 bit: 7540
Unsigned 16 bit: 7540
Signed 32 bit: -326951564
Unsigned 32 bit: 3968015732
Float 32 bit: -1.268067e+27
Float 64 bit: 2.397249e+103
Hexadecimal: 74
Octal: 164
Binary: 01110100
Stream Length: 8 − +
☑ Show little endian decoding
☐ Show unsigned and float as hexadecimal
Offset: 0x621

Screenshot 4: Hex (after)



```
dallin@dallin-ThinkPad-Edge-E220s-Kubuntu ~/Downloads/fortunes
 % ./fortune_static
Enter the CD key and press <enter>: anything
Your fortune:

                 ___          ______           Frobtech, Inc.
                /__/\     ___/_____/\
                \  \ \   /         /\\
                 \  \ \_/__       /  \         "If you've got the job,
                 _\  \ \  /\_____/___ \         we've got the frob."
                // \__\/ /  \       /\ \
        _______//_______/    \     / _\/______
       /      / \       \    /    / /        /\
    __/      /   \       \  /    / /        / _\__
   / /      /     \_______\/    / /        / /   /\
  /_/______/___________________/ /________/ /___/  \
  \ \      \    ___________    \ \        \ \   \  /
   \_\      \  /          /\    \ \        \ \___\/
      \      \/          /  \    \ \        \  /
       \_____/          /    \    \ \________\/
            /__________/      \    \  /
            \   _____  \      /_____\/
             \ /    /\  \    / \  \ \
              /____/  \  \  /   \  \ \
              \    \  /___\/     \  \ \
               \____\/            \__\/

dallin@dallin-ThinkPad-Edge-E220s-Kubuntu ~/Downloads/fortunes
 %
```

Screenshot 5: Modified binary allowing any password