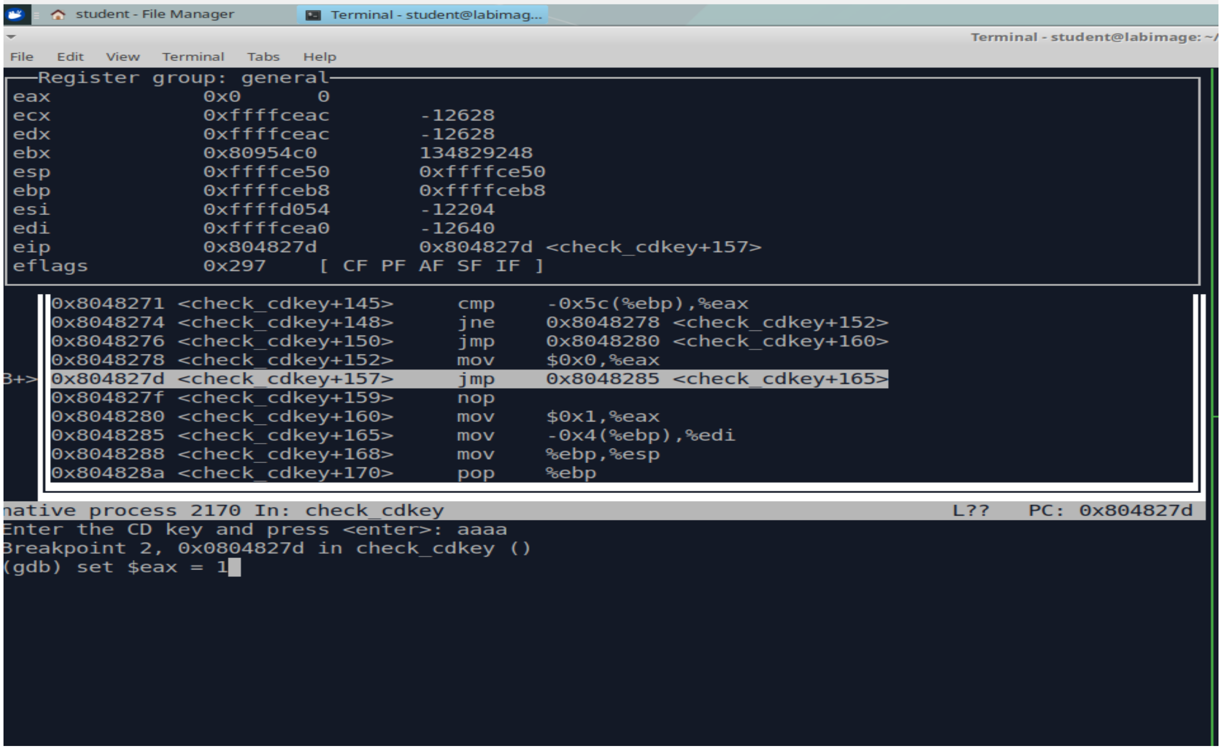
Thomas Hart
CS 465
Project 8 – Extracting Secrets

1) Place where I changed the register:



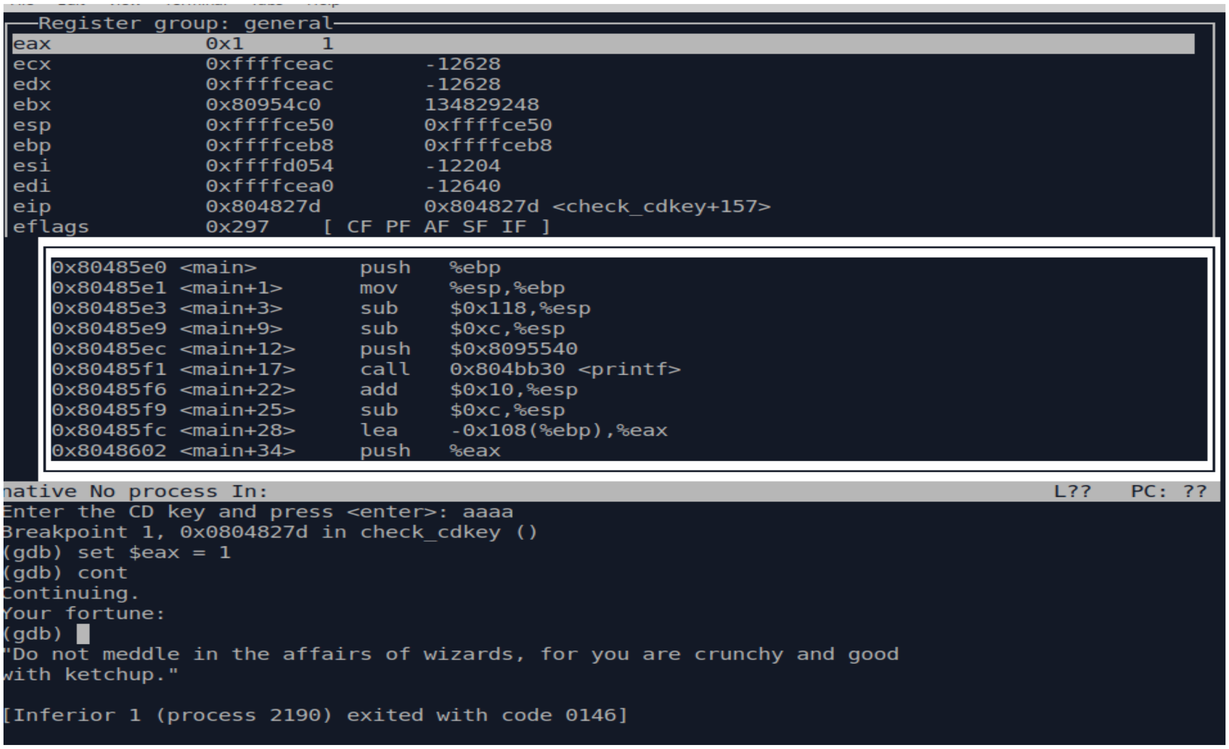
student - File Manager
Terminal - student@labimag...
Terminal - student@labimage: ~/
File
Edit
View
Terminal
Tabs
Help

```
──Register group: general─
 eax            0x0      0
 ecx            0xffffceac       -12628
 edx            0xffffceac       -12628
 ebx            0x80954c0        134829248
 esp            0xffffce50       0xffffce50
 ebp            0xffffceb8       0xffffceb8
 esi            0xffffd054       -12204
 edi            0xffffcea0       -12640
 eip            0x804827d        0x804827d <check_cdkey+157>
 eflags         0x297     [ CF PF AF SF IF ]

    0x8048271 <check_cdkey+145>      cmp    -0x5c(%ebp),%eax
    0x8048274 <check_cdkey+148>      jne    0x8048278 <check_cdkey+152>
    0x8048276 <check_cdkey+150>      jmp    0x8048280 <check_cdkey+160>
    0x8048278 <check_cdkey+152>      mov    $0x0,%eax
B+> 0x804827d <check_cdkey+157>      jmp    0x8048285 <check_cdkey+165>
    0x804827f <check_cdkey+159>      nop
    0x8048280 <check_cdkey+160>      mov    $0x1,%eax
    0x8048285 <check_cdkey+165>      mov    -0x4(%ebp),%edi
    0x8048288 <check_cdkey+168>      mov    %ebp,%esp
    0x804828a <check_cdkey+170>      pop    %ebp

native process 2170 In: check_cdkey                          L??   PC: 0x804827d
Enter the CD key and press <enter>: aaaa
Breakpoint 2, 0x0804827d in check_cdkey ()
(gdb) set $eax = 1
```

Fortune printing out in the debugger after changing the eax register:



```
──Register group: general─
 eax            0x1      1
 ecx            0xffffceac       -12628
 edx            0xffffceac       -12628
 ebx            0x80954c0        134829248
 esp            0xffffce50       0xffffce50
 ebp            0xffffceb8       0xffffceb8
 esi            0xffffd054       -12204
 edi            0xffffcea0       -12640
 eip            0x804827d        0x804827d <check_cdkey+157>
 eflags         0x297     [ CF PF AF SF IF ]

    0x80485e0 <main>         push   %ebp
    0x80485e1 <main+1>       mov    %esp,%ebp
    0x80485e3 <main+3>       sub    $0x118,%esp
    0x80485e9 <main+9>       sub    $0xc,%esp
    0x80485ec <main+12>      push   $0x8095540
    0x80485f1 <main+17>      call   0x804bb30 <printf>
    0x80485f6 <main+22>      add    $0x10,%esp
    0x80485f9 <main+25>      sub    $0xc,%esp
    0x80485fc <main+28>      lea    -0x108(%ebp),%eax
    0x8048602 <main+34>      push   %eax

native No process In:                                        L??   PC: ??
Enter the CD key and press <enter>: aaaa
Breakpoint 1, 0x0804827d in check_cdkey ()
(gdb) set $eax = 1
(gdb) cont
Continuing.
Your fortune:
(gdb) 
"Do not meddle in the affairs of wizards, for you are crunchy and good
with ketchup."

[Inferior 1 (process 2190) exited with code 0146]
```

I tried a lot of different things but changing the eax register in “check_cdkey” finally made a random fortune print out. I found this by setting random breakpoints in the functions that sounded like they would deal with granting access through the cd key (addresses and functions found in objdump) and changing registers to see if it eventually granted access later in the program.

2) In order to edit the program, I used the objdump to find the bytes associated with “check_cdkey”. I noticed the line highlighted in the first screenshot caused the program to skip over the instruction that would have set eax to 1 if the cdkey had been correct. The objdump showed a short jump instruction that jumped 6 bytes forward, so I needed it to only jump 1 byte forward to land in the nop instruction, which would then continue to the next instruction that set eax to 1. I used “xxd” on the fortune_static to dump the hex. I used vim and “/” to find the exact bytes that matched the objdump jmp instruction. I just changed the 06 byte to a 01 byte. I then made a new executable with that new hex using “xxd -r”. Sure enough, I could run the new executable and get a random fortune each time regardless of the key I entered.

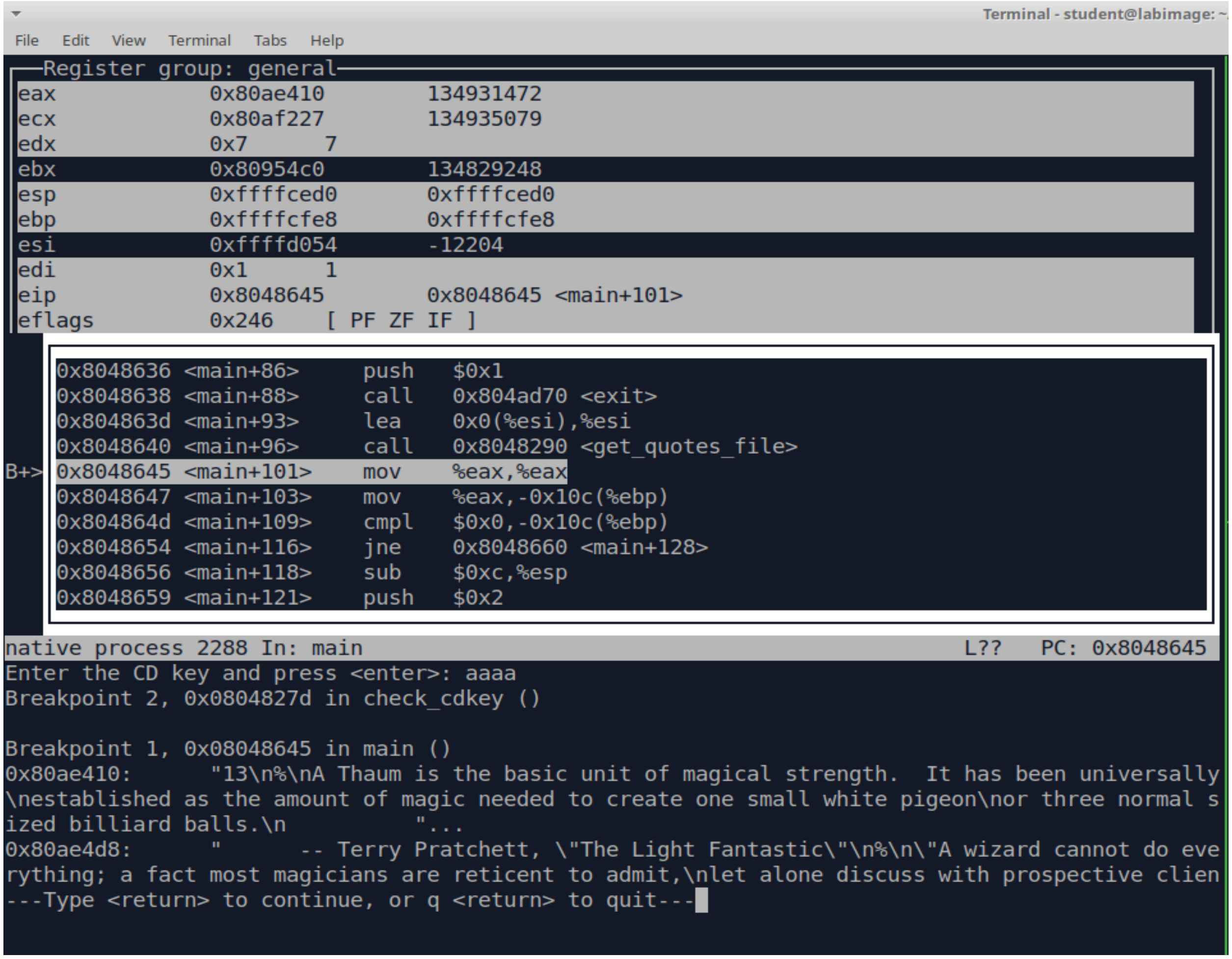
3) To get all the fortunes, I put a breakpoint in <main> right after <get_quotes_file> returned. The eax register had the return value, which was the address where all the fortunes were stored. I used a print command in the debugger to print a long list of strings starting at that address and fortunately, it was the fortunes.

Fortunes:

```
0x80ae410:      "13\n%\nA Thaum is the basic unit of magical strength.  It has been
universally\nestablished as the amount of magic needed to create one small white
pigeon\nor three normal sized billiard balls.\n          "...
0x80ae4d8:      "      -- Terry Pratchett, \"The Light Fantastic\"\n%\n\"A wizard
cannot do everything; a fact most magicians are reticent to admit,\nlet alone discuss
with prospective clients.  Still, the fact remains that"...
0x80ae5a0:      " \nthere are certain objects, and people, that are, for one reason or
another, \ncompletely immune to any direct magical spell.  It is for this group
of\nbeings that the magician learns the subtleties of"...
0x80ae668:      " using indirect spells.\nIt also does no harm, in dealing with these
matters, to carry a large club\nnear your person at all times.\"\n", ' ' <repeats 16
times>, "-- The Teachings of Ebenezum, Volume VIII\n%\n\"Do not m"...
0x80ae730:      "eddle in the affairs of wizards, for you are crunchy and good\nwith
ketchup.\"\n%\nRincewind had generally been considered by his tutors to be a natural
wizard\nin the same way that fish are natural mounta"...
0x80ae7f8:      "ineers.  He probably would have\nbeen thrown out of Unseen University
anyway--he couldn't remember spells and\nsmoking made him feel ill.\n", ' ' <repeats
16 times>, "-- Terry Pratchett, \"The Light Fantastic\"\n%\n    "...
0x80ae8c0:      ' ' <repeats 13 times>, "___             ______", ' ' <repeats 11 times>,
"Frobtech, Inc.\n", ' ' <repeats 16 times>, "/__/\\     ___/_____/\\          \n", ' '
<repeats 16 times>, "\\  \\ \\   /         /\\\\\n", ' ' <repeats 17 times>, "\\  \\
\\_/__      /  \\         \"If you'"...
0x80ae988:      "ve got the job,\n", ' ' <repeats 17 times>, "_\\  \\ \\  /\\_____/___
\\         we've got the frob.\"\n", ' ' <repeats 16 times>, "// \\__\\/ /  \\
/\\ \\\n        _______//_______/    \\     / _\\/______\n      /      / \\       \\
"...
0x80aea50:      "  /    / /       /\\\n    __/      /   \\        \\  /    / /
/ _\\__\n   / /      /     \\_______\\/    / /          / /   /\\\n  /_/______/", '_'
<repeats 19 times>, "/ /________/ /___/  \\\n  \\ \\        \\    _______"...
0x80aeb18:      "____      \\ \\         \\ \\    \\  /\n   \\_\\       \\  /           /\\
\\ \\        \\ \\___\\/\n      \\        \\/          /  \\      \\ \\        \\  /\n
\\_____/          /    \\    \\ \\_________\\/\n", ' ' <repeats 12 times>,
"/________"...
```

```
0x80aebe0:      "__/      \\    \\  /\n", ' ' <repeats 12 times>, "\\   _____  \\
/_____\\/\n", ' ' <repeats 13 times>, "\\ /    /\\  \\    / \\  \\ \\\n", ' ' <repeats
14 times>, "/____/  \\  \\  /   \\  \\ \\\n", ' ' <repeats 14 times>, "\\    \\
/___\\/    \\  \\ \\\n", ' ' <repeats 15 times>, "\\____\\/   "...
0x80aeca8:      "         \\__\\/\n%\nWin98 error 001: Unexpected condition: booted
without crashing.\n%\nWin98 error 002: Insufficient diskspace. You need at least 300
GB free memory.\n%\nWin98 error 003: Illegal ASM instruc"...
0x80aed70:      "tion. If your modem worked properly, the\nFBI would have been
called.\n%\nWin NT error 001: Error recording error codes. All further errors
not\ndisplayed.\n%\nWin98 error 004: Virus activated from DOS Prom"...
0x80aee38:      "pt - but the virus requires\nWindows. Your system will be rebooted
for the Virus to take effect. [ OK ]\n%\nWin98 error 005: Mouse not found. Click left
mouse button on ok to continue.\n%\nWin98 error 006:"...
0x80aef00:      " Keyboard not found. Press F1 to continue.\n%\n(1)     Office
employees will daily sweep the floors, dust the\n        furniture, shelves, and
showcases.\n(2)     Each day fill lamps, clean chimneys, and "...
0x80aefc8:      "trim wicks.\n        Wash the windows once a week.\n(3)     Each
clerk will bring a bucket of water and a scuttle of\n        coal for the day's
business.\n(4)     Make your pens carefully.  You may whitt"...
0x80af090:      "le nibs to your\n        individual taste.\n(5)     This office will
open at 7 a.m. and close at 8 p.m. except\n        on the Sabbath, on which day we
will remain closed.  Each\n        employee is expec"...
0x80af158:      "ted to spend the Sabbath by attending\n        church and
contributing liberally to the cause of the Lord.\n", ' ' <repeats 16 times>, "--
\"Office Worker's Guide\", New England Carriage\n", ' ' <repeats 20 times>, "Works,
18"...
```

Screenshots of printing all the fortunes:

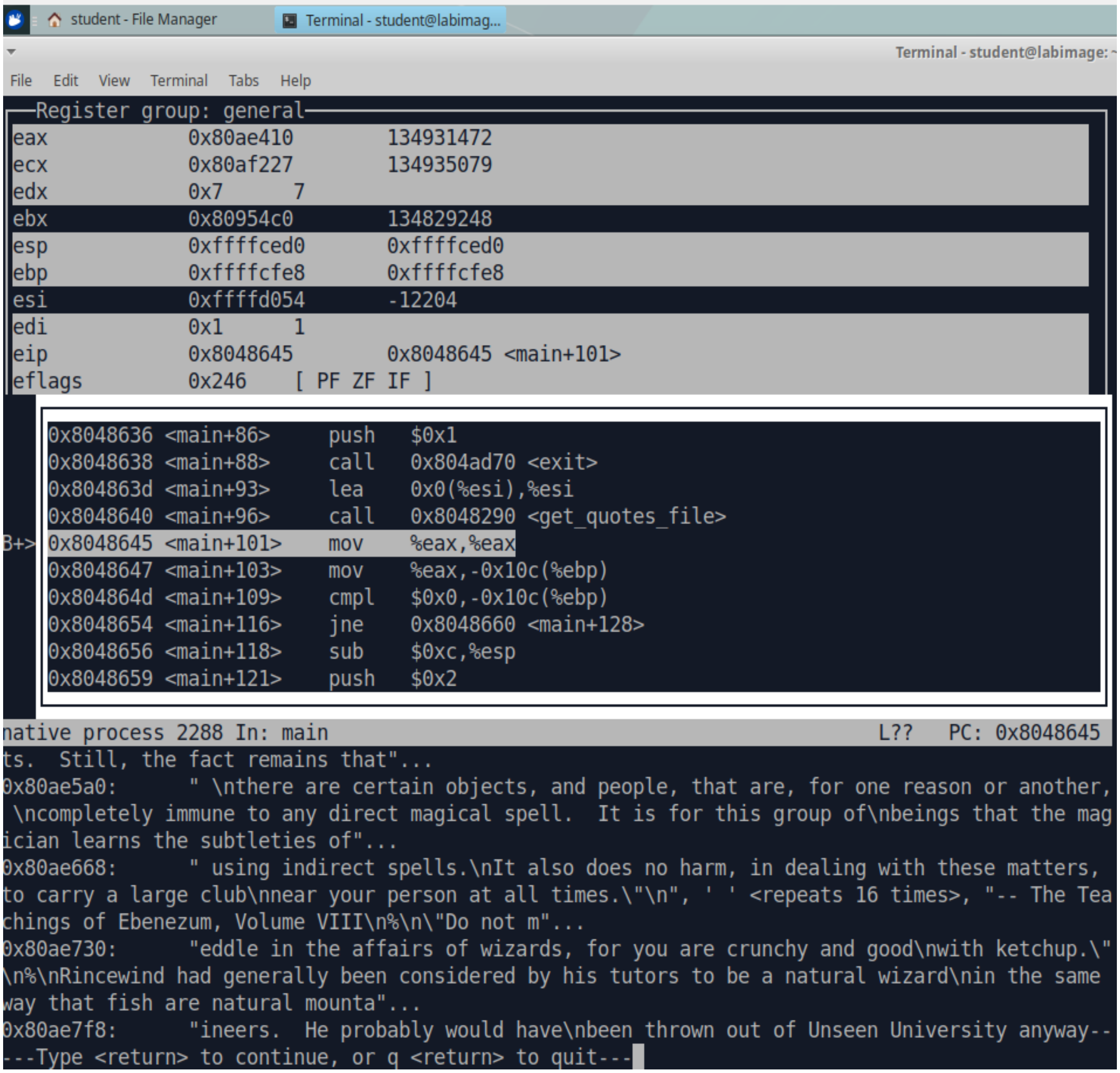

Terminal - student@labimage: ~
File Edit View Terminal Tabs Help

```
┌─Register group: general─
│eax            0x80ae410        134931472
│ecx            0x80af227        134935079
│edx            0x7      7
│ebx            0x80954c0        134829248
│esp            0xffffced0       0xffffced0
│ebp            0xffffcfe8       0xffffcfe8
│esi            0xffffd054       -12204
│edi            0x1      1
│eip            0x8048645        0x8048645 <main+101>
│eflags         0x246    [ PF ZF IF ]

   0x8048636 <main+86>      push   $0x1
   0x8048638 <main+88>      call   0x804ad70 <exit>
   0x804863d <main+93>      lea    0x0(%esi),%esi
   0x8048640 <main+96>      call   0x8048290 <get_quotes_file>
B+>0x8048645 <main+101>     mov    %eax,%eax
   0x8048647 <main+103>     mov    %eax,-0x10c(%ebp)
   0x804864d <main+109>     cmpl   $0x0,-0x10c(%ebp)
   0x8048654 <main+116>     jne    0x8048660 <main+128>
   0x8048656 <main+118>     sub    $0xc,%esp
   0x8048659 <main+121>     push   $0x2

native process 2288 In: main                              L??   PC: 0x8048645
Enter the CD key and press <enter>: aaaa
Breakpoint 2, 0x0804827d in check_cdkey ()

Breakpoint 1, 0x08048645 in main ()
0x80ae410:      "13\n%\nA Thaum is the basic unit of magical strength.  It has been universally
\nestablished as the amount of magic needed to create one small white pigeon\nor three normal s
ized billiard balls.\n          "...
0x80ae4d8:      "       -- Terry Pratchett, \"The Light Fantastic\"\n%\n\"A wizard cannot do eve
rything; a fact most magicians are reticent to admit,\nlet alone discuss with prospective clien
---Type <return> to continue, or q <return> to quit---
```



```
┌─Register group: general─────────────────────────────────────────────────────┐
│eax            0x80ae410        134931472
│ecx            0x80af227        134935079
│edx            0x7      7
│ebx            0x80954c0        134829248
│esp            0xffffced0       0xffffced0
│ebp            0xffffcfe8       0xffffcfe8
│esi            0xffffd054       -12204
│edi            0x1      1
│eip            0x8048645        0x8048645 <main+101>
│eflags         0x246    [ PF ZF IF ]

   0x8048636 <main+86>     push   $0x1
   0x8048638 <main+88>     call   0x804ad70 <exit>
   0x804863d <main+93>     lea    0x0(%esi),%esi
   0x8048640 <main+96>     call   0x8048290 <get_quotes_file>
B+>0x8048645 <main+101>    mov    %eax,%eax
   0x8048647 <main+103>    mov    %eax,-0x10c(%ebp)
   0x804864d <main+109>    cmpl   $0x0,-0x10c(%ebp)
   0x8048654 <main+116>    jne    0x8048660 <main+128>
   0x8048656 <main+118>    sub    $0xc,%esp
   0x8048659 <main+121>    push   $0x2

native process 2288 In: main                                  L??   PC: 0x8048645
ts.  Still, the fact remains that"...
0x80ae5a0:      " \nthere are certain objects, and people, that are, for one reason or another,
 \ncompletely immune to any direct magical spell.  It is for this group of\nbeings that the mag
ician learns the subtleties of"...
0x80ae668:      " using indirect spells.\nIt also does no harm, in dealing with these matters,
to carry a large club\nnear your person at all times.\"\n", ' ' <repeats 16 times>, "-- The Tea
chings of Ebenezum, Volume VIII\n%\n\"Do not m"...
0x80ae730:      "eddle in the affairs of wizards, for you are crunchy and good\nwith ketchup.\"
\n%\nRincewind had generally been considered by his tutors to be a natural wizard\nin the same
way that fish are natural mounta"...
0x80ae7f8:      "ineers.  He probably would have\nbeen thrown out of Unseen University anyway--
---Type <return> to continue, or q <return> to quit---
```