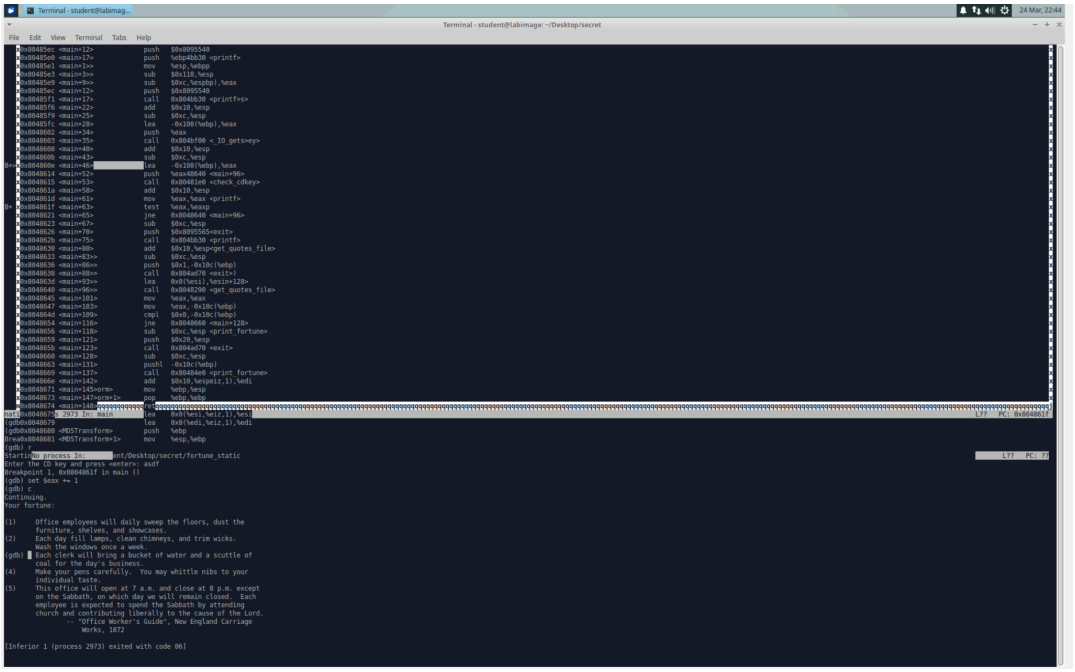
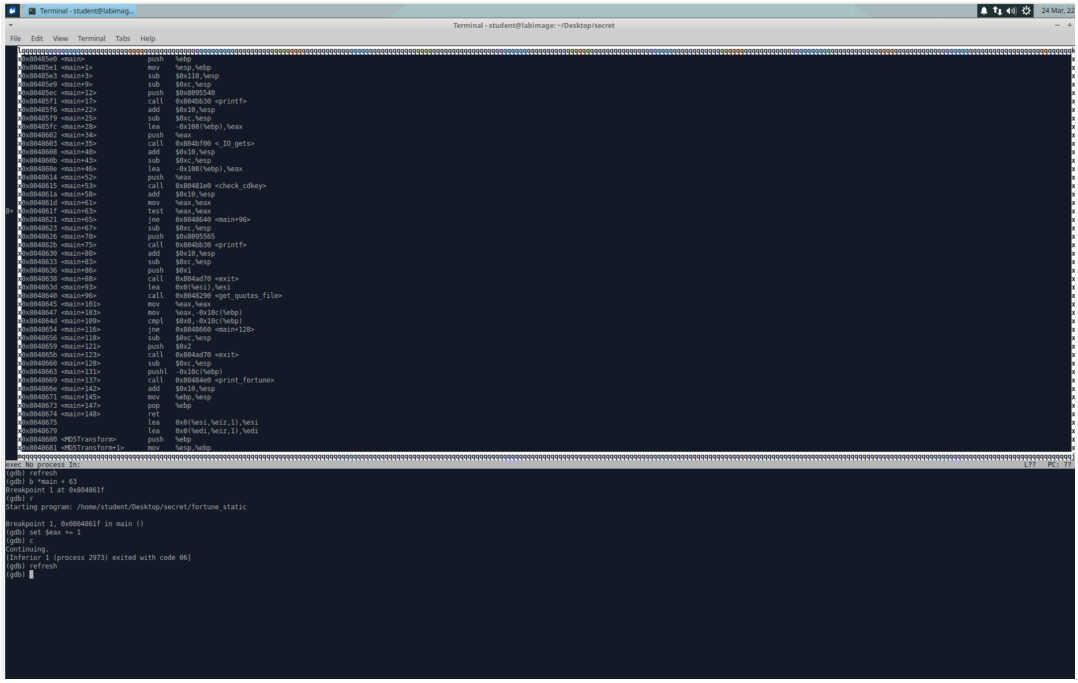
Extracting Secrets

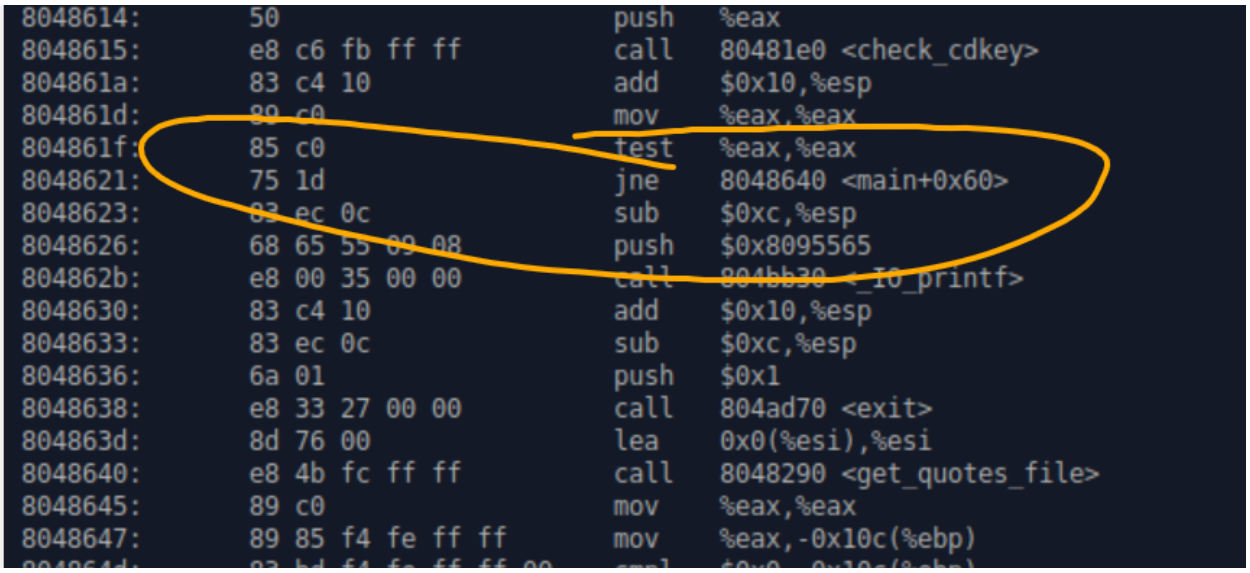
The first way I was able to extract secrets in this lab was through manual use of the gdb utility. To bypass the security check, I simply set $eax to 1 right before it was checked to determine if a password was valid or not. In the screenshot below, I set eax to 1, then continue. When I continue, I get a valid fortune, despite typing in ‘asdf’ as the password.



After typing refresh, the GUI updates, but it clears the stdout in the console. The screenshot shows my actual inputs/breakpoints better, but doesn’t show stdout.



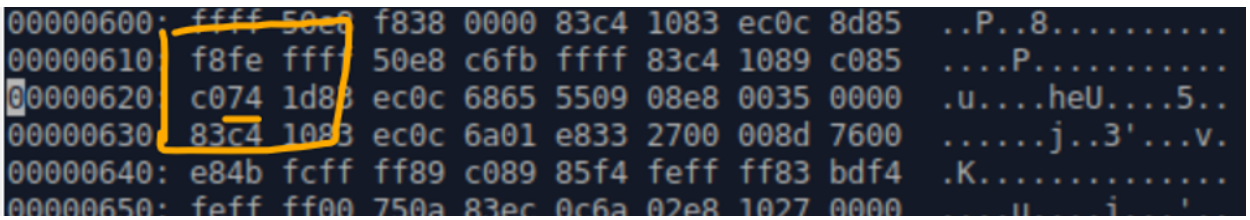
After the manual bypass, I wanted to create a new executable which would always provide a fortune. To do this, I inverted the JNE instruction into being a JE instruction. As is visible in the screenshot below, the JNE instruction is encoded with 75 1d. If we change the first byte to be 74, then this instruction becomes a JE. This allows us to use any password except valid ones. I don't know which passwords are valid, and I don't care, so this effectively cracks the program.



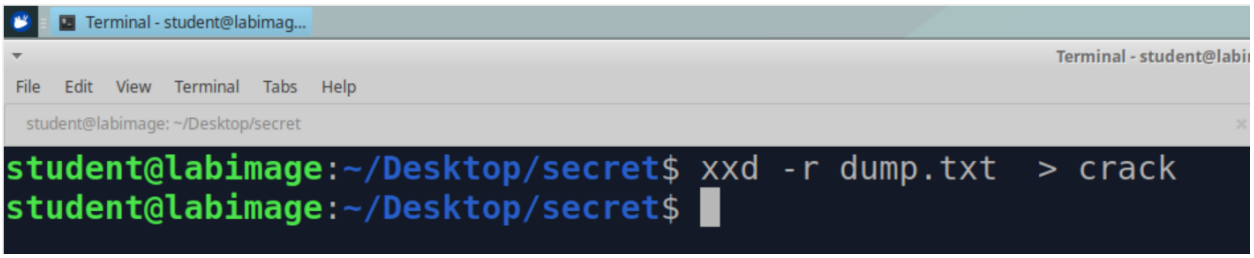
X86 encoding reference tells us what the encoding of JE is

		74							JZ	rel8		
									JE	rel8		
		75							JNZ	rel8		
									JNE	rel8		

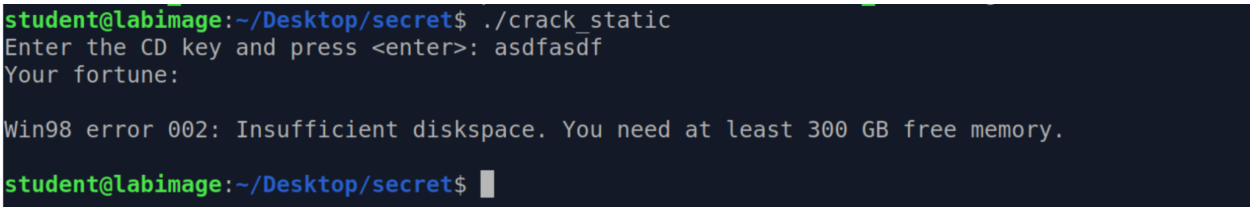
Using this knowledge, we can convert the program into a hex dump with xxd, identify the correct 0x75 by using the pattern of surrounding bytes, edit the 0x75 into a 0x74, then reverse dump with xxd -r. The below screenshot shows me after changing the 75 into a 74. Note the pattern of bytes before/after and how they correspond with the before/after bytes of the objdump above. After modifying this byte, I 'recompiled'.



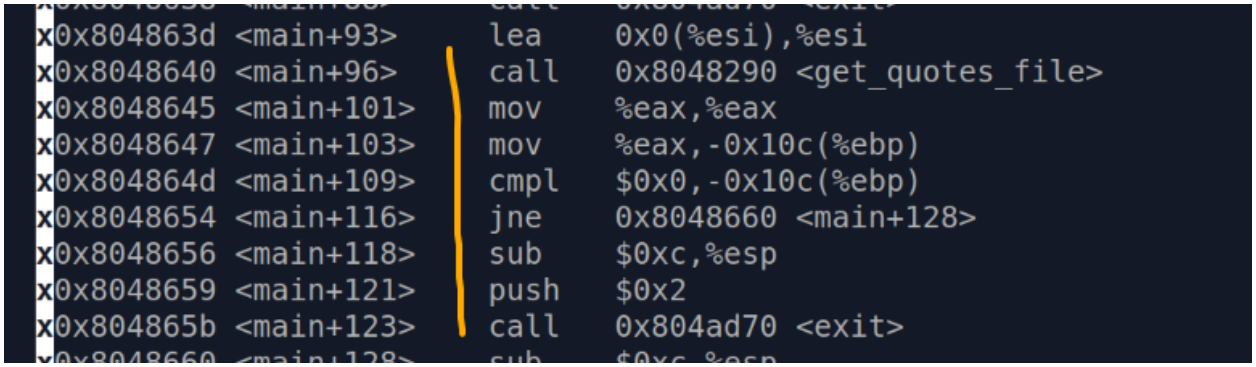
(the below screenshot was taken after completing the lab so the name is different, but the process was the same)



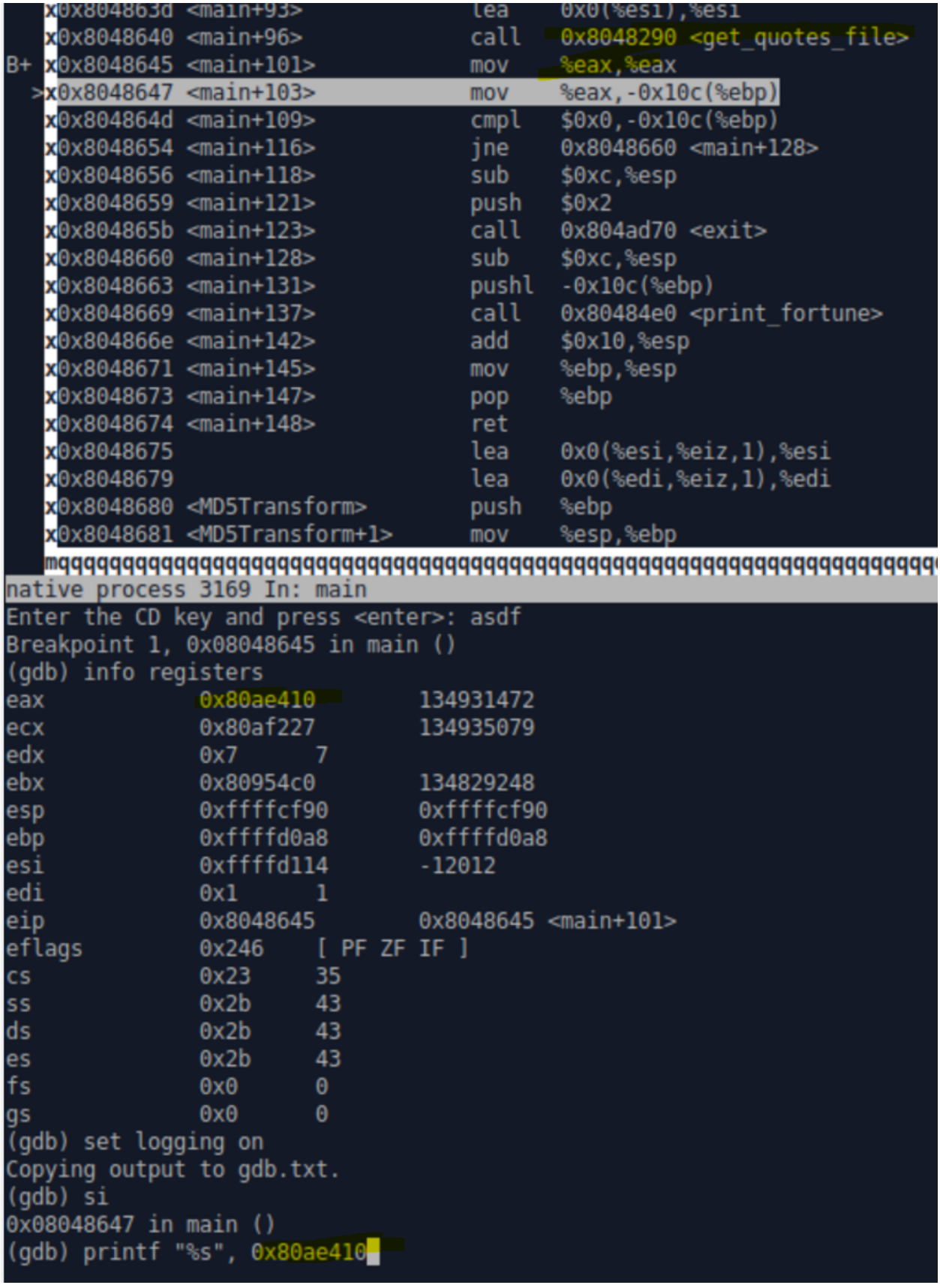
After cracking :

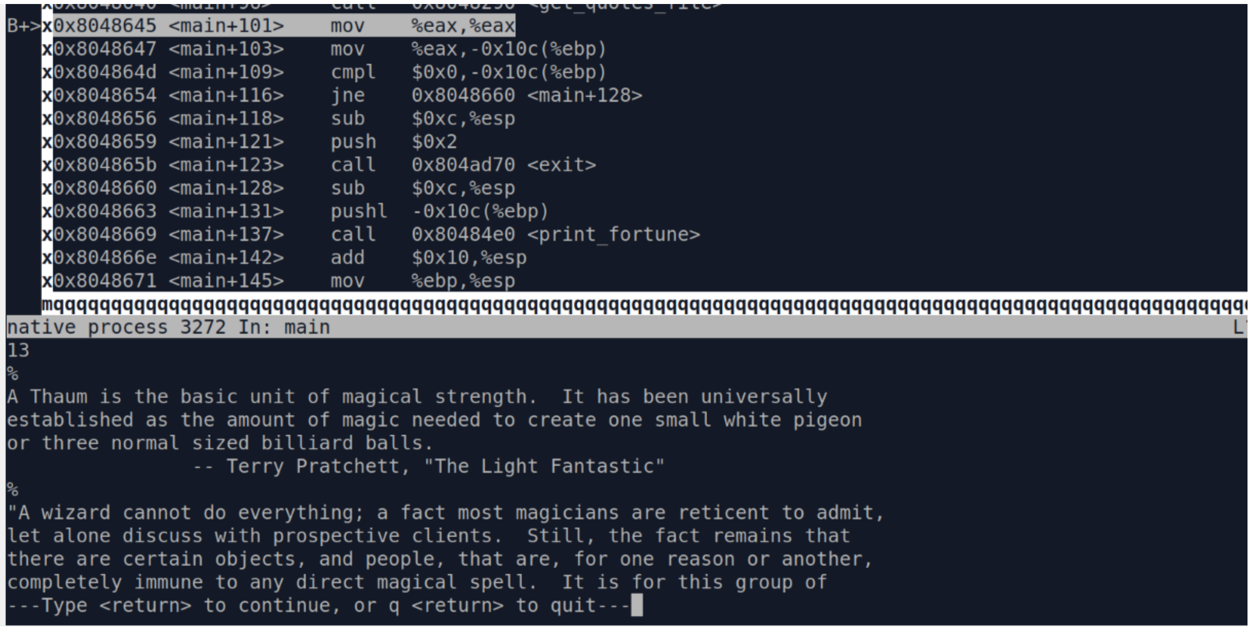


With the program cracked, I now had to find a way to extract all the fortunes in one go. After examining the main function, I noticed there was a function “get_quotes_file” which returned a value which was seemingly being null checked. It looked to me like this program was receiving a pointer, then if it was null the program would exit.

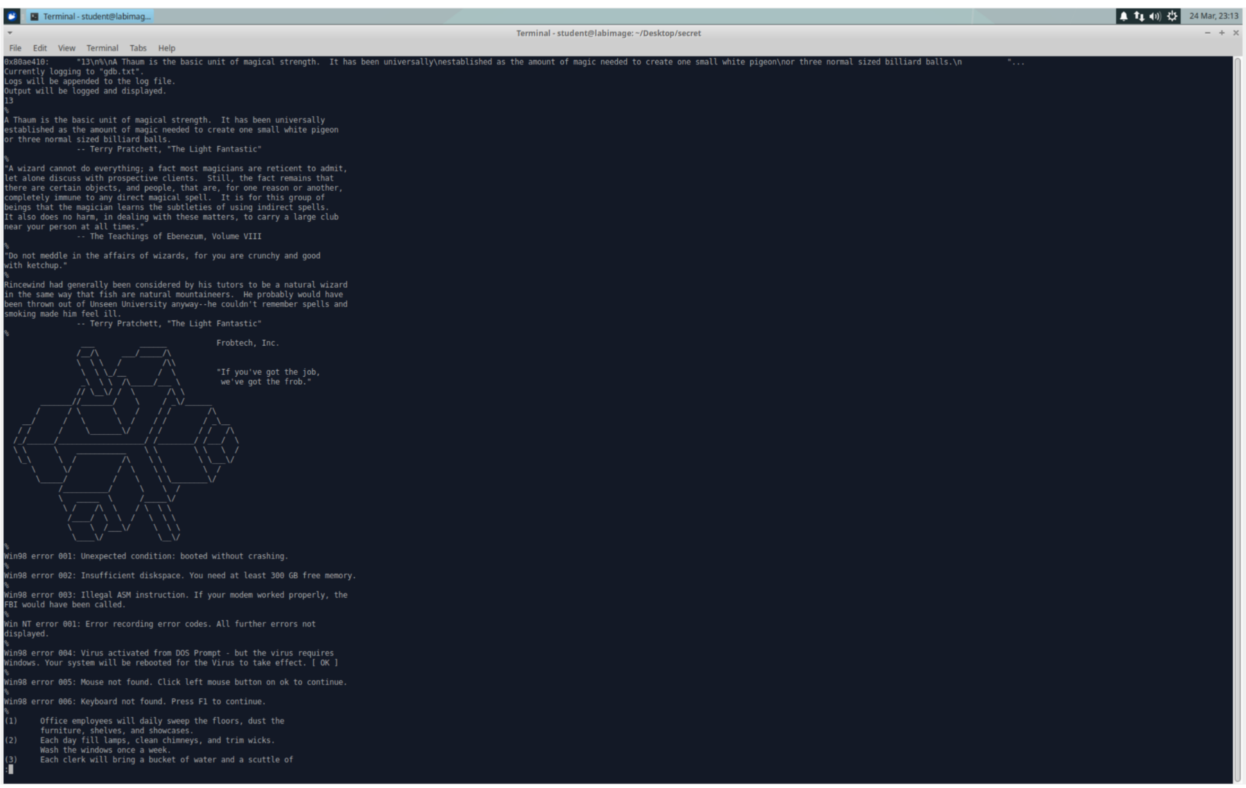


If the name alone didn’t give it away, this series of assembly tells me with high confidence that this function returns a pointer to the text. After swapping settings around so gdb would print the entire string rather than just a synopsis, I was able to get all the fortunes in a file.


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
0x804865b <main+123> call 0x804ad70 <exit>
0x8048660 <main+128> sub $0xc,%esp
0x8048663 <main+131> pushl -0x10c(%ebp)
0x8048669 <main+137> call 0x80484e0 <print_fortune>
0x804866e <main+142> add $0x10,%esp
0x8048671 <main+145> mov %ebp,%esp
0x8048673 <main+147> pop %ebp
0x8048674 <main+148> ret
0x8048675 lea 0x0(%esi,%eiz,1),%esi
0x8048679 lea 0x0(%edi,%eiz,1),%edi
0x8048680 <MD5Transform> push %ebp
0x8048681 <MD5Transform+1> mov %esp,%ebp
native process 3169 In: main
Enter the CD key and press <enter>: asdf
Breakpoint 1, 0x08048645 in main ()
(gdb) info registers
eax 0x80ae410 134931472
ecx 0x80af227 134935079
edx 0x7 7
ebx 0x80954c0 134829248
esp 0xffffcf90 0xffffcf90
ebp 0xffffd0a8 0xffffd0a8
esi 0xffffd114 -12012
edi 0x1 1
eip 0x8048645 0x8048645 <main+101>
eflags 0x246 [PF ZF IF]
cs 0x23 35
ss 0x2b 43
ds 0x2b 43
es 0x2b 43
fs 0x0 0
gs 0x0 0
(gdb) set logging on
Copying output to gdb.txt.
(gdb) si
0x08048647 in main ()
(gdb) printf "%s", 0x80ae410



After checking the gdb log file, we get this



The full list of fortunes is displayed on the next pages for your reading pleasure

13
%
A Thaum is the basic unit of magical strength. It has been universally established as the amount of magic needed to create one small white pigeon or three normal sized billiard balls.

-- Terry Pratchett, "The Light Fantastic"

%
"A wizard cannot do everything; a fact most magicians are reticent to admit, let alone discuss with prospective clients. Still, the fact remains that there are certain objects, and people, that are, for one reason or another, completely immune to any direct magical spell. It is for this group of beings that the magician learns the subtleties of using indirect spells. It also does no harm, in dealing with these matters, to carry a large club near your person at all times."

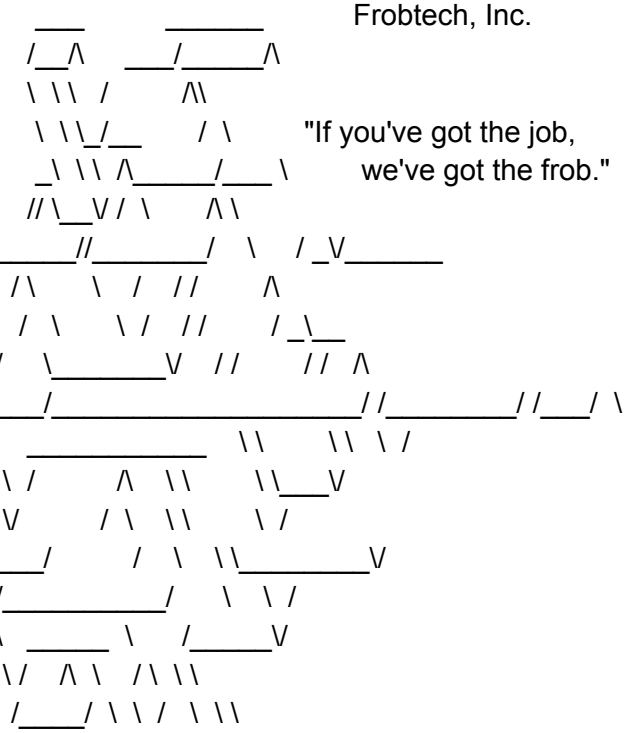
-- The Teachings of Ebenezum, Volume VIII

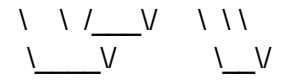
%
"Do not meddle in the affairs of wizards, for you are crunchy and good with ketchup."

%
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"

%





%
Win98 error 001: Unexpected condition: booted without crashing.
%
Win98 error 002: Insufficient diskspace. You need at least 300 GB free memory.
%
Win98 error 003: Illegal ASM instruction. If your modem worked properly, the FBI would have been called.
%
Win NT error 001: Error recording error codes. All further errors not displayed.
%
Win98 error 004: Virus activated from DOS Prompt - but the virus requires Windows. Your system will be rebooted for the Virus to take effect. [OK]
%
Win98 error 005: Mouse not found. Click left mouse button on ok to continue.
%
Win98 error 006: Keyboard not found. Press F1 to continue.
%

(1) Office employees will daily sweep the floors, dust the furniture, shelves, and showcases.

(2) Each day fill lamps, clean chimneys, and trim wicks. Wash the windows once a week.

(3) Each clerk will bring a bucket of water and a scuttle of coal for the day's business.

(4) Make your pens carefully. You may whittle nibs to your individual taste.

(5) This office will open at 7 a.m. and close at 8 p.m. except on the Sabbath, on which day we will remain closed. Each employee is expected to spend the Sabbath by attending church and contributing liberally to the cause of the Lord.

-- "Office Worker's Guide", New England Carriage Works, 1872