Matt Christensen (mrc621)

November 5, 2021

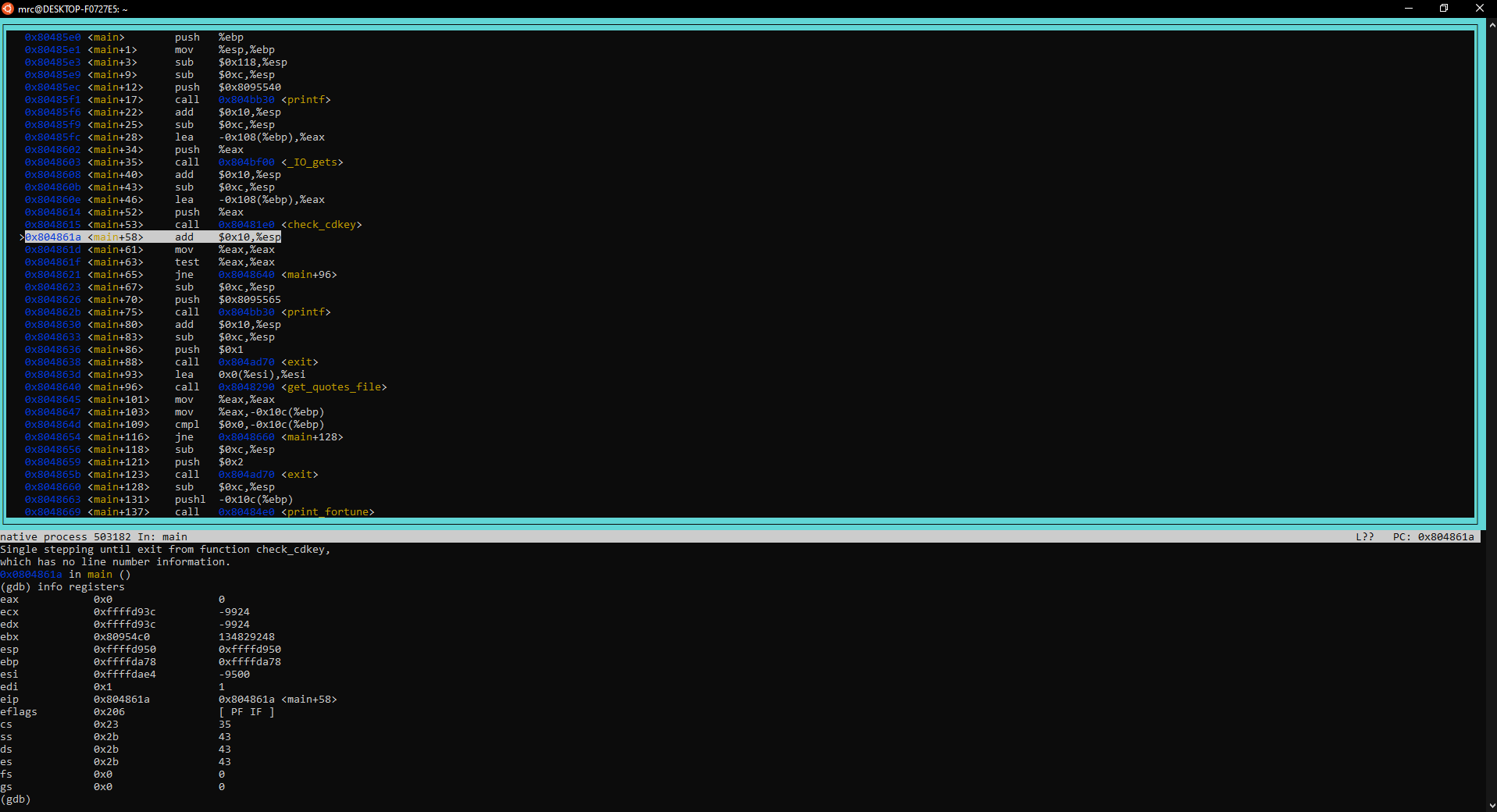
CS 465 (001) – Clift, Frederic M

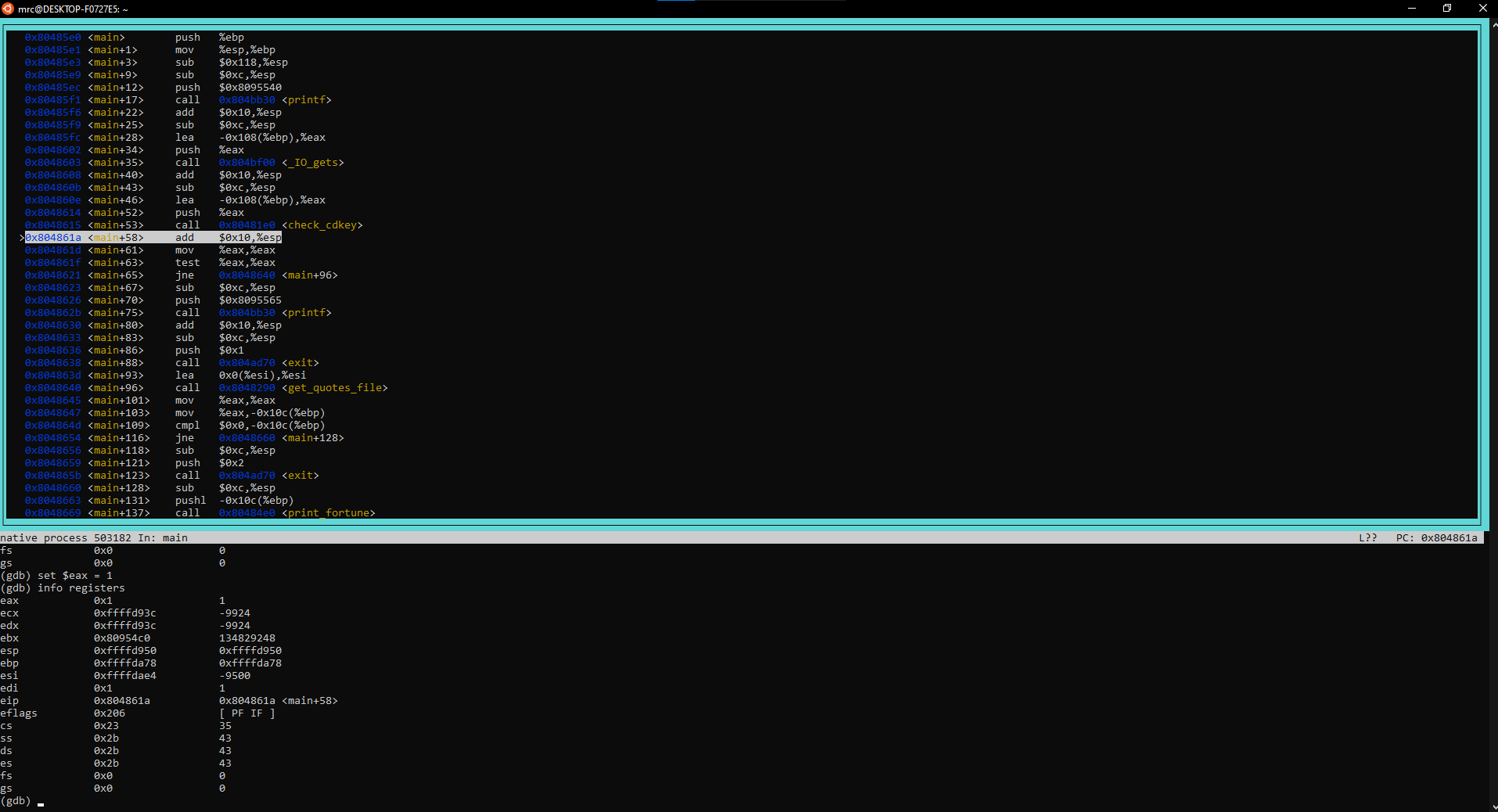
Project #8 – Extracting Secrets

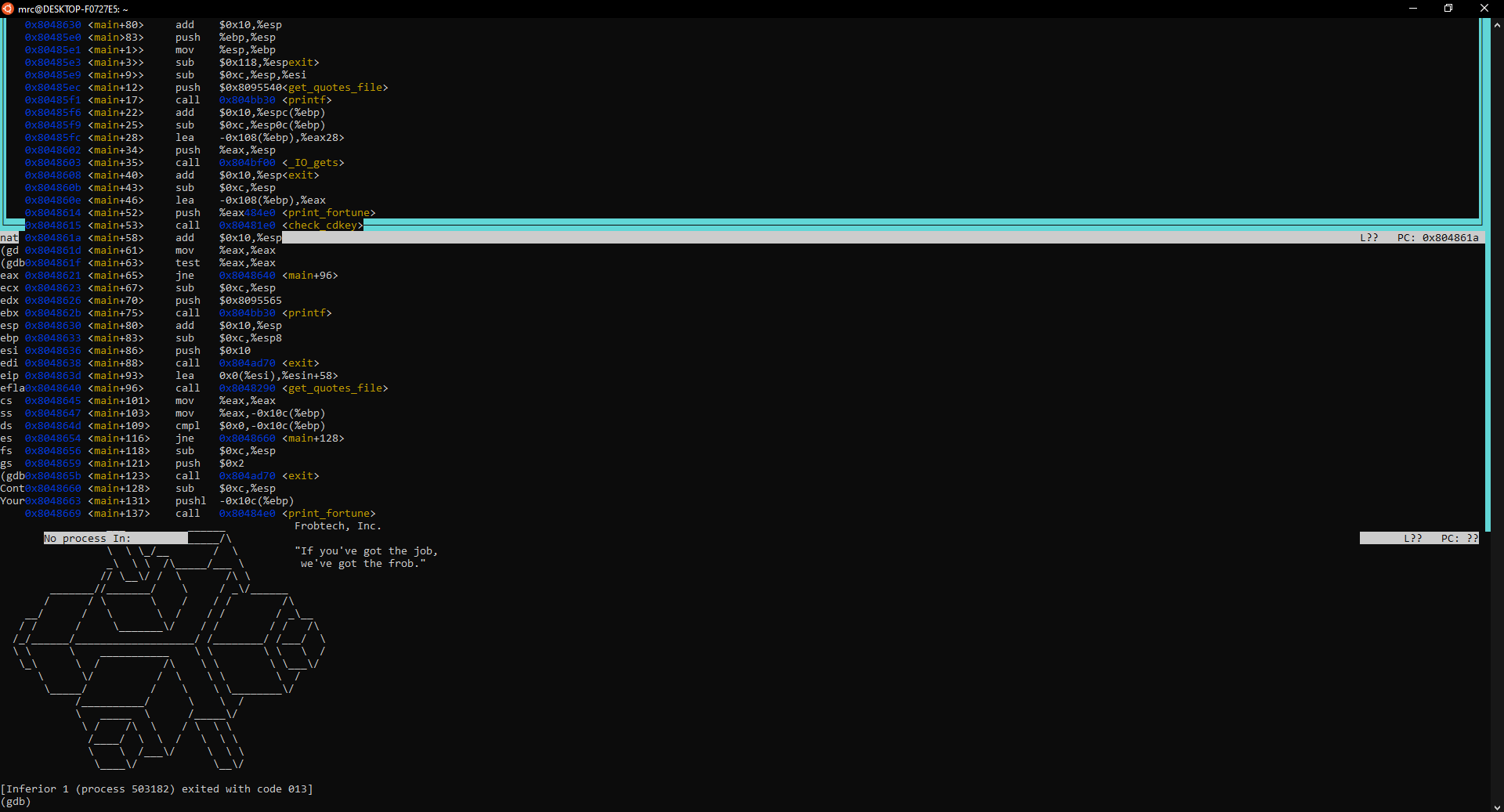
The first step of my process was the look at the program in a RE tool called Ghidra. I saw that the printing of the secret was dependent on the return value of *check\_cdkey()*.



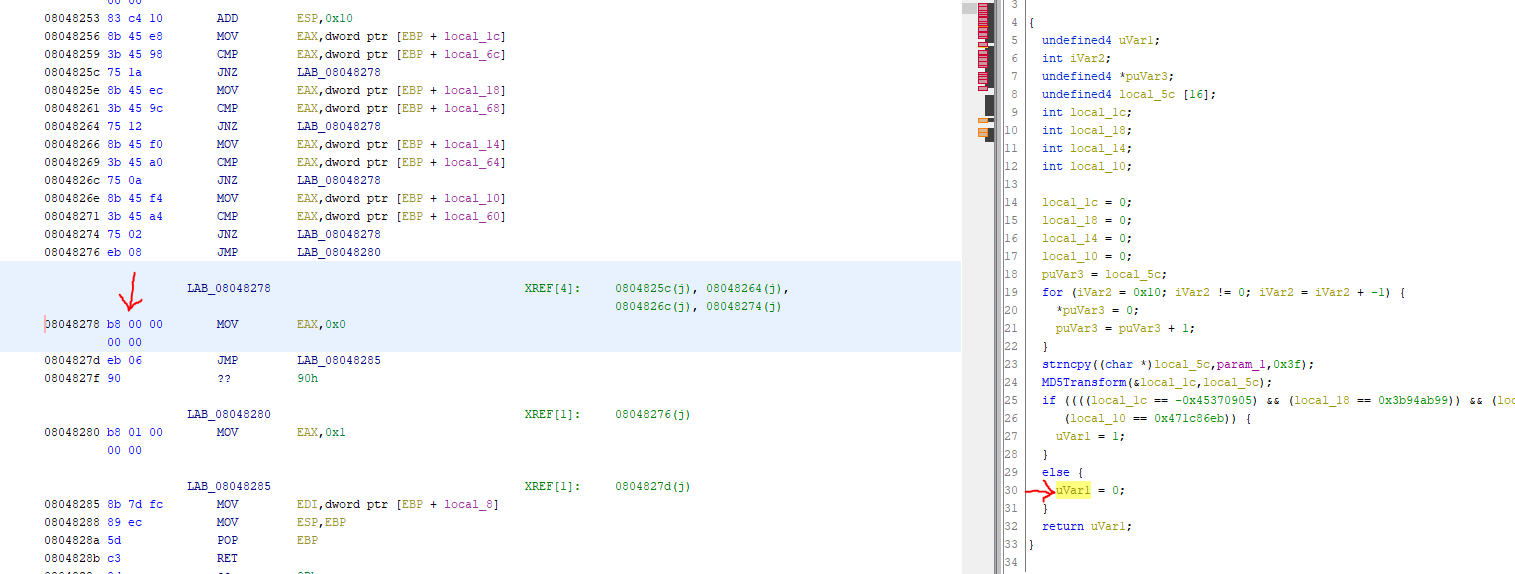
To test this, I ran to program in GDB and broke after the function returned. I then simply set the EAX register to 1 (using the ‘*set $eax = 1*’ command) and the program printed out a fortune (**requirement 1**).

****

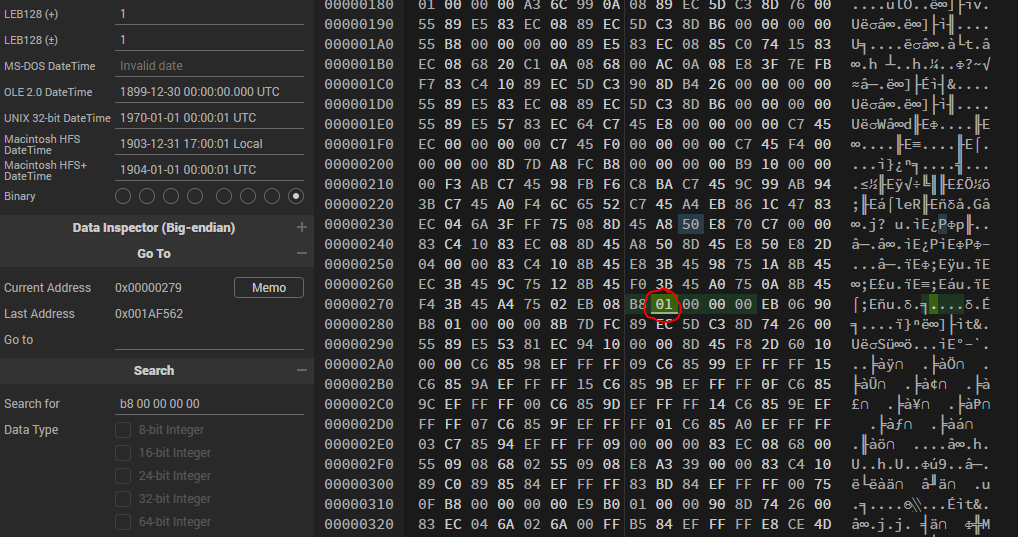
****

****

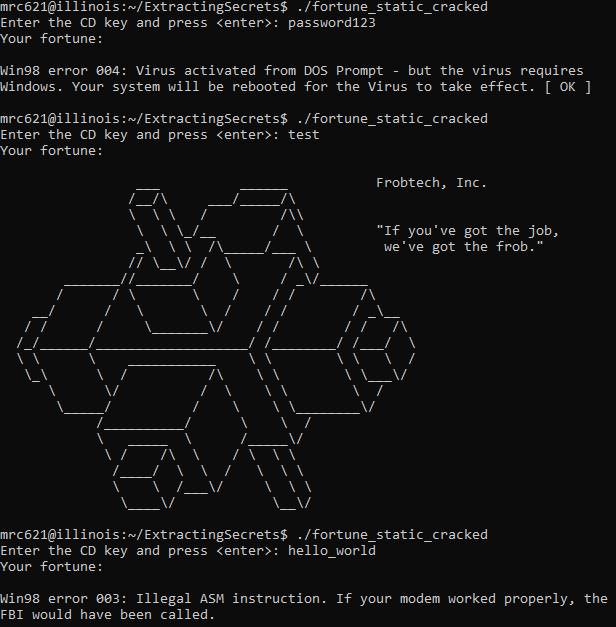
In order edit the program to bypass the cdkey mechanism, I simply found (in Ghidra) that the *check\_cdkey* function returned a one if the password was verified and a zero if the password was invalid.



So I simply found the instruction responsible for setting the return value to zero (*b8 00 00 00 00* – which moves zero into the EAX register), opened the *fortune\_static* binary in a hex editor, found the instruction, and changed it to move a one into the EAX register (with the instruction – *B8 01 00 00 00*).



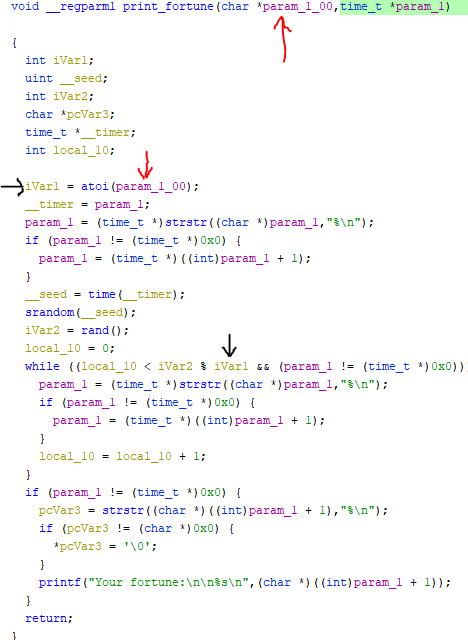
This new binary, when ran, would accept all passwords given and will always print a fortune (**requirement 2**).



Finally, we needed to extract all the possible secrets. I chose to run the cracked version in GDB and then break right after the call to *get\_quotes\_file*. I examined the registers and found the address 0x80ae410 in EAX. When examining that address, I got the number thirteen followed by what I assumed to be the first string:



This matches with what we see in Ghirdra, as it appears to number of strings is first used as a way of indexing and moding the random seed:



I proceeded to dump the memory info a file (using [logging](https://stackoverflow.com/questions/16095948/gdb-dump-memory-in-specific-region-save-formatted-output-into-a-file) and the “*x /3600 0x80ae410*” command) to find all the secret fortunes: (**requirement 3**)

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"

\_\_\_ \_\_\_\_\_\_ Frobtech, Inc.

/\_\_/\ \_\_\_/\_\_\_\_\_/\

\ \ \ / /\\

\ \ \\_/\_\_ / \ "If you've got the job,

\_\ \ \ /\\_\_\_\_\_/\_\_\_ \ we've got the frob."

// \\_\_\/ / \ /\ \

\_\_\_\_\_\_\_//\_\_\_\_\_\_\_/ \ / \_\/\_\_\_\_\_\_

/ / \ \ / / / /\

\_\_/ / \ \ / / / / \_\\_\_

/ / / \\_\_\_\_\_\_\_\/ / / / / /\

/\_/\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ /\_\_\_\_\_\_\_\_/ /\_\_\_/ \

\ \ \ \_\_\_\_\_\_\_\_\_\_\_ \ \ \ \ \ /

\\_\ \ / /\ \ \ \ \\_\_\_\/

\ \/ / \ \ \ \ /

\\_\_\_\_\_/ / \ \ \\_\_\_\_\_\_\_\_\/

/\_\_\_\_\_\_\_\_\_\_/ \ \ /

\ \_\_\_\_\_ \ /\_\_\_\_\_\/

\ / /\ \ / \ \ \

/\_\_\_\_/ \ \ / \ \ \

\ \ /\_\_\_\/ \ \ \

\\_\_\_\_\/ \\_\_\/

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