Ryan Cohen
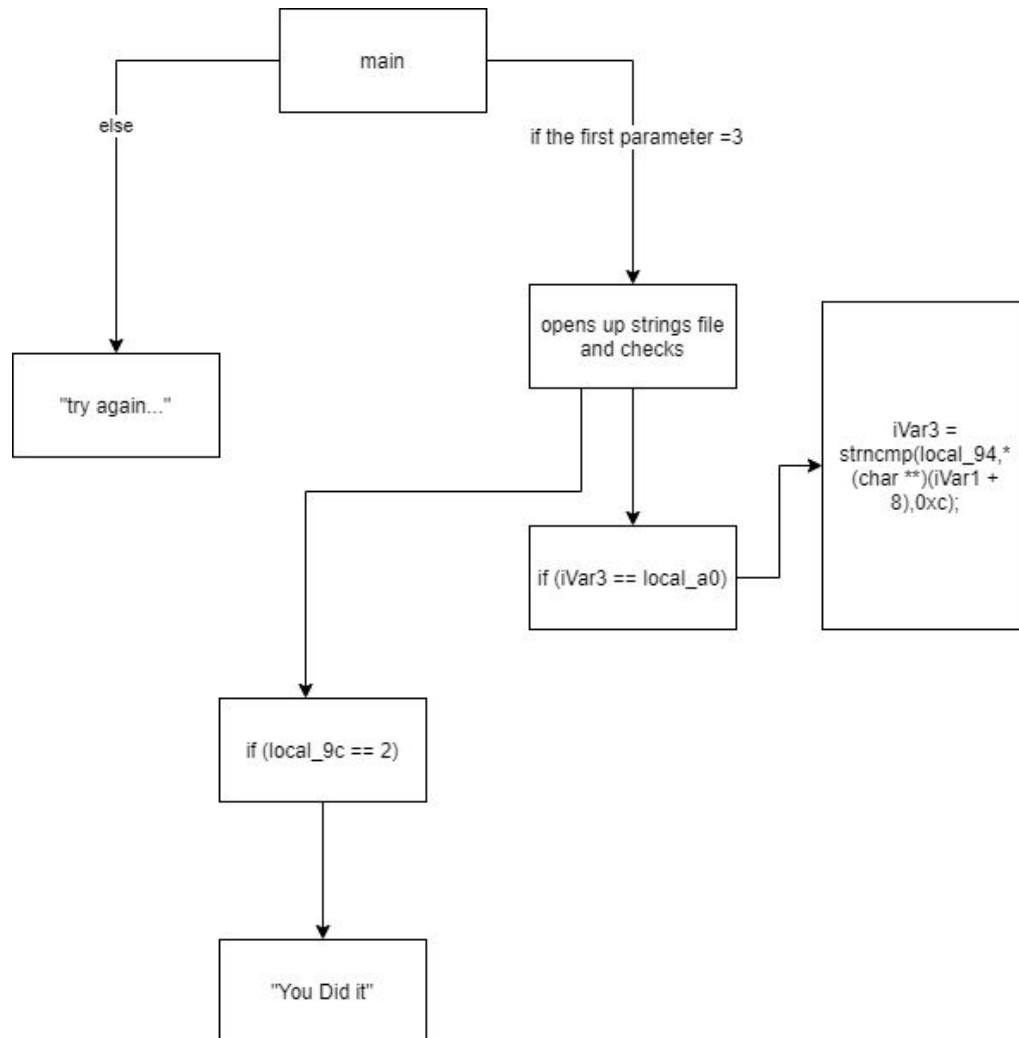
1. `

    a. Problem Goal: Print "You did it!"

    b. Thought Process: First thought was to run the program and see what happens. It gave me a "Try again….". I then put two parameters to try to see if anything changed, and it then said ""close, but no cigar". So I knew that I had to include two parameters for this question.

```
                        ┌──────────────┐
                        │     main     │
                        └──────────────┘
         else                              if the first parameter =3

                                          ┌──────────────────┐
                                          │ opens up strings file │      ┌──────────────────┐
    ┌──────────────┐                      │   and checks      │      │    iVar3 =        │
    │  "try again..." │                    └──────────────────┘      │ strncmp(local_94,* │
    └──────────────┘                                                 │  (char **)(iVar1 + │
                                          ┌──────────────────┐       │    8),0xc);        │
                                          │ if (iVar3 == local_a0) │  └──────────────────┘
                                          └──────────────────┘

         ┌──────────────┐
         │ if (local_9c == 2) │
         └──────────────┘

         ┌──────────────┐
         │  "You Did it"  │
         └──────────────┘
```

    c.

    d. After running through the program it prints two random strings. Upon further inspection in Ghidra those strings that it prints are what it compares it to. I tried now putting the variables that it printed out into the program as the arguments in the flipped order and I was able to achieve the answer.
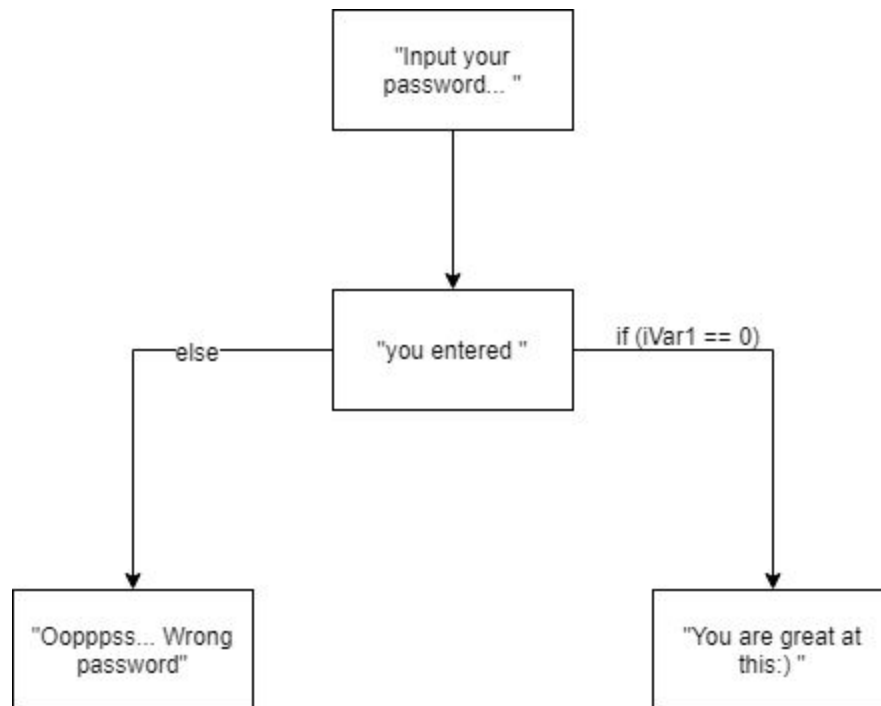
```
ryanc@ryanc-VirtualBox:~/Downloads/lab$ ./re_challenege1 deregister_tm_clones
__JCR_LIST__
__JCR_LIST__
deregister_tm_clones
You did it!
ryanc@ryanc-VirtualBox:~/Downloads/lab$
```

    e.

2. `

    a. Goal: Print "You are great this"

    b. Thought Process: I started with simply running the program. With running the program without any arguments I got prompted to enter a password. I entered something random and I got "you entered " and the "Oopppss...Wrong Password". I then decided to take a further look in Ghidra. Something popped to me instantly. There were a bunch of local variables with different addresses associated with them. All of them together as a char would equal "RkxBR2ZsyagababaZ0ZMQUdmbGF". I knew that group of characters would be important. I then went further down and saw **strtok**'s. With some googling I learned it essentially split stuff at wherever was put in the second argument. The first one took it down to yagababaZ0ZMQUdmbGF and then the second one took it down to yagababa making that the final password.

```
                    ┌──────────────┐
                    │ "Input your  │
                    │ password..." │
                    └──────┬───────┘
                           │
                           ▼
        ┌──────────────────────────────────┐
  else──│         "you entered "           │── if (iVar1 == 0)
        └──────────────────────────────────┘
        │                                  │
        ▼                                  ▼
┌──────────────┐                  ┌──────────────┐
│ "Oopppss...  │                  │ "You are     │
│  Wrong       │                  │  great at    │
│  password"   │                  │  this:) "    │
└──────────────┘                  └──────────────┘
```

    c.

    d. When entering yagababa I got the right password, printing the correct statement.
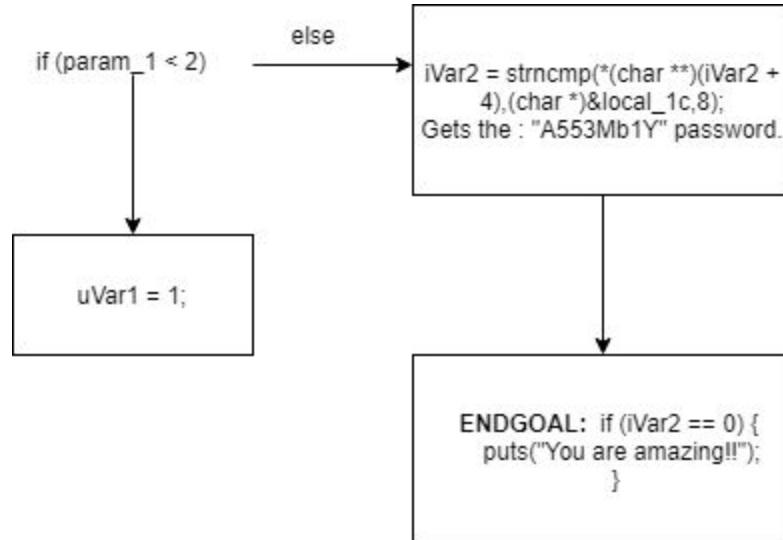
```
ryanc@ryanc-VirtualBox:~/Downloads/lab$ ./re_challenge2new
Input your password...
yagababa
you entered yagababa
You are great at this :)
ryanc@ryanc-VirtualBox:~/Downloads/lab$ 
```

    e.

3. `

    a. The goal was to print "you are amazing!!"

    b. When first running the program with no arguments I get "The answer: 1" and "Maybe it's this:5". Running the program with any number with arguments returns the same thing. I now knew it was time to open up Ghidra. Similar to the last

problem I saw two local variables with addresses. Hovering over them I saw that they were "A553 and "Mb1Y". I saw in the program itself that it checks for parameters and then does a strncmp with what we put in the parameter and then what the local variables were moving on for 8 characters. O put "A553Mb1Y" as my parameter and I got the goal message.

```
                              else
  if (param_1 < 2)    ───────────────▶   iVar2 = strncmp(*(char **)(iVar2 +
                                           4),(char *)&local_1c,8);
          │                             Gets the : "A553Mb1Y" password.
          │
          ▼
  ┌────────────────┐
  │  uVar1 = 1;    │                                │
  │                │                                │
  └────────────────┘                                ▼
                                         ┌──────────────────────────────┐
                                         │  ENDGOAL:  if (iVar2 == 0) {  │
                                         │   puts("You are amazing!!");  │
                                         │              }                │
                                         └──────────────────────────────┘
```

c.

d. The answer was "A553Mb1Y"

```
ryanc@ryanc-VirtualBox:~/Downloads/lab$ ./re_challenge3 A553Mb1Y
The answer: 1
Maybe it's this:5
You are amazing!!
```

e.