Re\_challenge 1

Goal: print “You did it!”

Steps:

1. Open IDA: has graph of all the assembly
2. Looking at imports - it has printf, fgets, puts, and more, so it is probably in C
3. Make CFD
4. Analyze the assembly/Run
   1. Cmp dword ptr [eax], 3 -> check if argc == 3
   2. Running the program: it takes 2 arguments -- confirmed
   3. Fgets -> opening a looping through a file.
   4. Opens the file “strings”
   5. Loops through until it goes through the whole file
   6. Two functions: f1 -> adds 5 to argument, f2 -> adds 3 to argument
   7. When looping, it checks if the loop counter == 17 (because 12 + 5 = 17)
      1. If true, check that line and add one to some counter
      2. If false, check if the loop counter == 16(because 13 + 3 = 16)
         1. If true check that line and add 1 to some counter
      3. Adds one to the loop counter every time
   8. It first checks arg2 then arg1 on the next loop
5. Open the strings file and find lines 16 and 17 with the first line as line 0
6. Running the code -> have arg1 = line 17 and arg2 = line 16
   1. It printed my goal

Answer:

1. ZF = 1 to 0x0804859B
2. Jmp to 0x0804867C
3. Inside loop
   1. Loops here for a while
      1. ZF = 0 to 0x080485CF, ZF = 0 to 0x08048623, ZF = 0 to 0x08048675
   2. When loop counter == 16
      1. ZF = 0 to 0x080485CF, ZF = 0 to 0x08048623
      2. ZF = 1 continues, ZF = 1 continues to 0x08048675
   3. When loop counter == 17
      1. ZF = 0 to 0x080485CF
      2. ZF = 1 continues, ZF = 1 to 0x08048675
4. Loop exits
5. ZF = 1 continues
6. ZF = 1 continues
7. puts(“You did it”)

> ./re\_challenge deregister\_tm\_clones \_\_JCR\_LIST\_\_

CFD:

