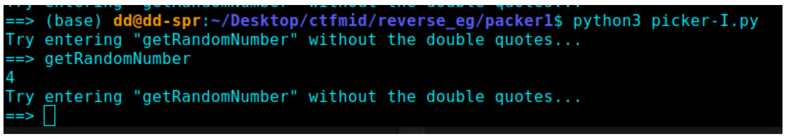
☰

Understanding the Program

Step 1: Understanding the Program

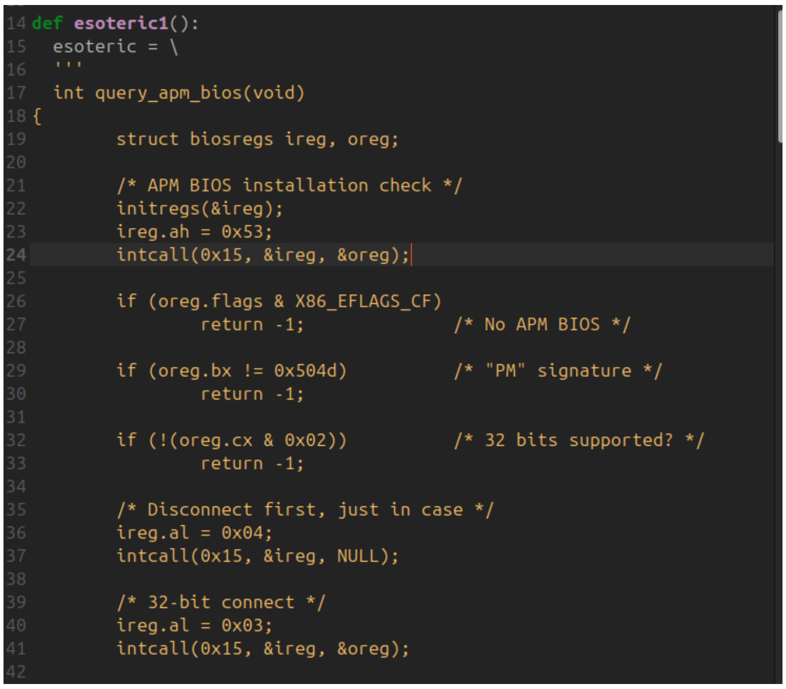
The program takes the name of a function as input and executes the function corresponding to the name you provided.



```
==> (base) dd@dd-spr:~/Desktop/ctfmid/reverse_eg/packer1$ python3 picker-I.py
Try entering "getRandomNumber" without the double quotes...
==> getRandomNumber
4
Try entering "getRandomNumber" without the double quotes...
==> 
```

Step 2: Key Observation

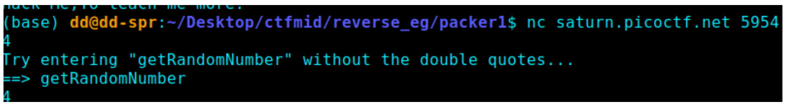
There are some extra, confusing, or unnecessary parts in the program (referred to as "crazy stuff"), but they don't matter for solving the challenge.



```
def esoteric1():
  esoteric = \
  '''
  int query_apm_bios(void)
{
        struct biosregs ireg, oreg;

        /* APM BIOS installation check */
        initregs(&ireg);
        ireg.ah = 0x53;
        intcall(0x15, &ireg, &oreg);

        if (oreg.flags & X86_EFLAGS_CF)
                return -1;              /* No APM BIOS */

        if (oreg.bx != 0x504d)          /* "PM" signature */
                return -1;

        if (!(oreg.cx & 0x02))          /* 32 bits supported? */
                return -1;

        /* Disconnect first, just in case */
        ireg.al = 0x04;
        intcall(0x15, &ireg, NULL);

        /* 32-bit connect */
        ireg.al = 0x03;
        intcall(0x15, &ireg, &oreg);
```

Step 3: Solution

Type **win** as the function name when prompted. The program will execute the **win** function, which contains the logic to give you the flag.



```
(base) dd@dd-spr:~/Desktop/ctfmid/reverse_eg/packer1$ nc saturn.picoctf.net 5954
4
Try entering "getRandomNumber" without the double quotes...
==> getRandomNumber
4
```