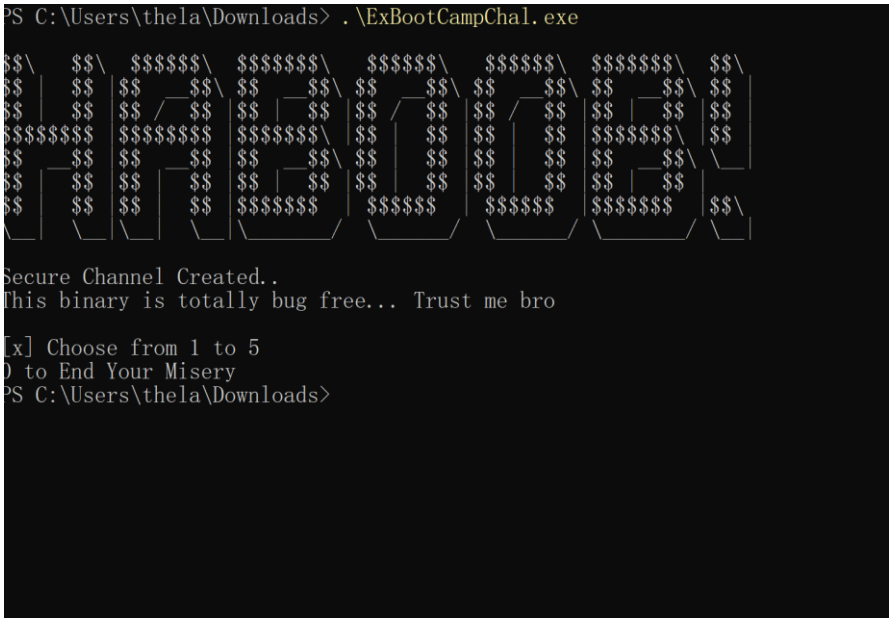
HABOOB HACKING REPORT

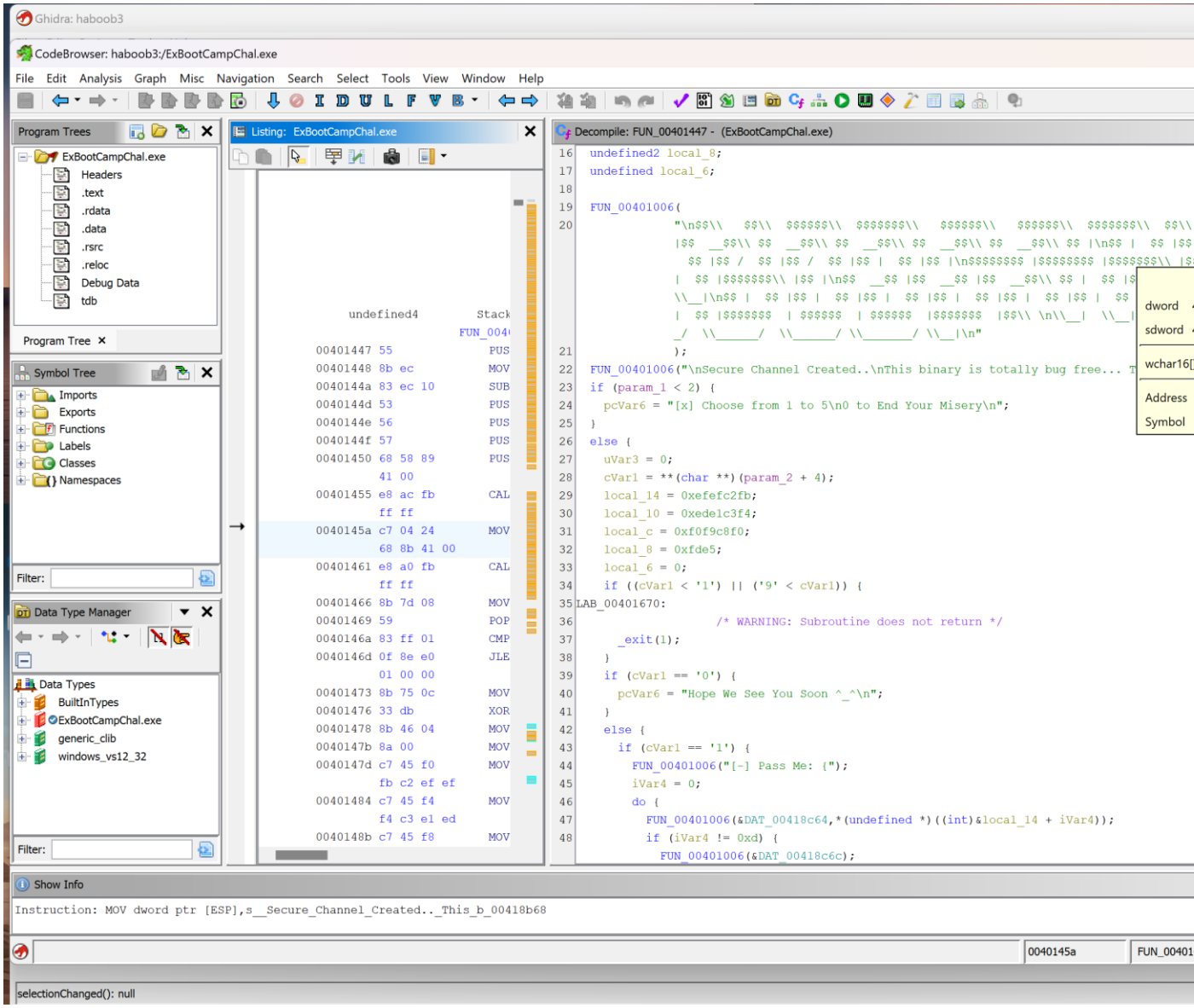
Click or tap here to enter text.

TABLE OF CONTENTS



INTRODUCTION

By running the software you will face the main function which has print statements that can be found by searching by string in GHDIRA


Ghidra: haboob3
CodeBrowser: haboob3:/ExBootCampChal.exe
File Edit Analysis Graph Misc Navigation Search Select Tools View Window Help
Program Trees
ExBootCampChal.exe
Headers
.text
.rdata
.data
.rsrc
.reloc
Debug Data
tdb
Program Tree
Symbol Tree
Imports
Exports
Functions
Labels
Classes
Namespaces
Filter:
Data Type Manager
Data Types
BuiltInTypes
ExBootCampChal.exe
generic_clib
windows_vs12_32
Filter:
Listing: ExBootCampChal.exe
undefined4 Stack
FUN_004
00401447 55 PUS
00401448 8b ec MOV
0040144a 83 ec 10 SUB
0040144d 53 PUS
0040144e 56 PUS
0040144f 57 PUS
00401450 68 58 89 PUS
41 00
00401455 e8 ac fb CAL
ff ff
0040145a c7 04 24 MOV
68 8b 41 00
00401461 e8 a0 fb CAL
ff ff
00401466 8b 7d 08 MOV
00401469 59 POP
0040146a 83 ff 01 CMP
0040146d 0f 8e e0 JLE
01 00 00
00401473 8b 75 0c MOV
00401476 33 db XOR
00401478 8b 46 04 MOV
0040147b 8a 00 MOV
0040147d c7 45 f0 MOV
fb c2 ef ef
00401484 c7 45 f4 MOV
f4 c3 e1 ed
0040148b c7 45 f8 MOV
Decompile: FUN_00401447 - (ExBootCampChal.exe)
undefined2 local_8;
undefined local_6;
FUN_00401006(
"\n$$\\ $$\\ $$$$$$\\ $$$$$$$\\ $$$$$$\\ $$$$$$\\ $$$$$$$\\ $$\\
|$$ __$$\\ $$ __$$\\ $$ __$$\\ $$ __$$\\ $$ __$$\\ $$ |\n$$ | $$ |$$
$$ |$$ / $$ |$$ / $$ |$$ | $$ |$$ |\n$$$$$$$$ |$$$$$$$$ |$$$$$$$\\ |$
| $$ |$$$$$$$\\ |$$ |\n$$ __$$ |$$ __$$ |$$ __$$\\ $$ | $$ |$
__|\n$$ | $$ |$$ | $$ |$$ | $$ |$$ | $$ |$$ | $$ |$$ | $$
| $$ |$$$$$$$ | $$$$$$ | $$$$$$ |$$$$$$$ |$$\\ \n__| __|
_/ _____/ _____/ _____/ __|\n"
);
FUN_00401006("\nSecure Channel Created..\nThis binary is totally bug free... T
if (param_1 < 2) {
pcVar6 = "[x] Choose from 1 to 5\n0 to End Your Misery\n";
}
else {
uVar3 = 0;
cVar1 = **(char **)(param_2 + 4);
local_14 = 0xefefc2fb;
local_10 = 0xede1c3f4;
local_c = 0xf0f9c8f0;
local_8 = 0xfde5;
local_6 = 0;
if ((cVar1 < '1') || ('9' < cVar1)) {
LAB_00401670:
/* WARNING: Subroutine does not return */
_exit(1);
}
if (cVar1 == '0') {
pcVar6 = "Hope We See You Soon ^_^\n";
}
else {
if (cVar1 == '1') {
FUN_00401006("[-] Pass Me: {");
iVar4 = 0;
do {
FUN_00401006(&DAT_00418c64,*(undefined *)((int)&local_14 + iVar4));
if (iVar4 != 0xd) {
FUN_00401006(&DAT_00418c6c);
dword
sdword
wchar16[
Address
Symbol
Show Info
Instruction: MOV dword ptr [ESP],s__Secure_Channel_Created.._This_b_00418b68
0040145a
FUN_00401
selectionChanged(): null

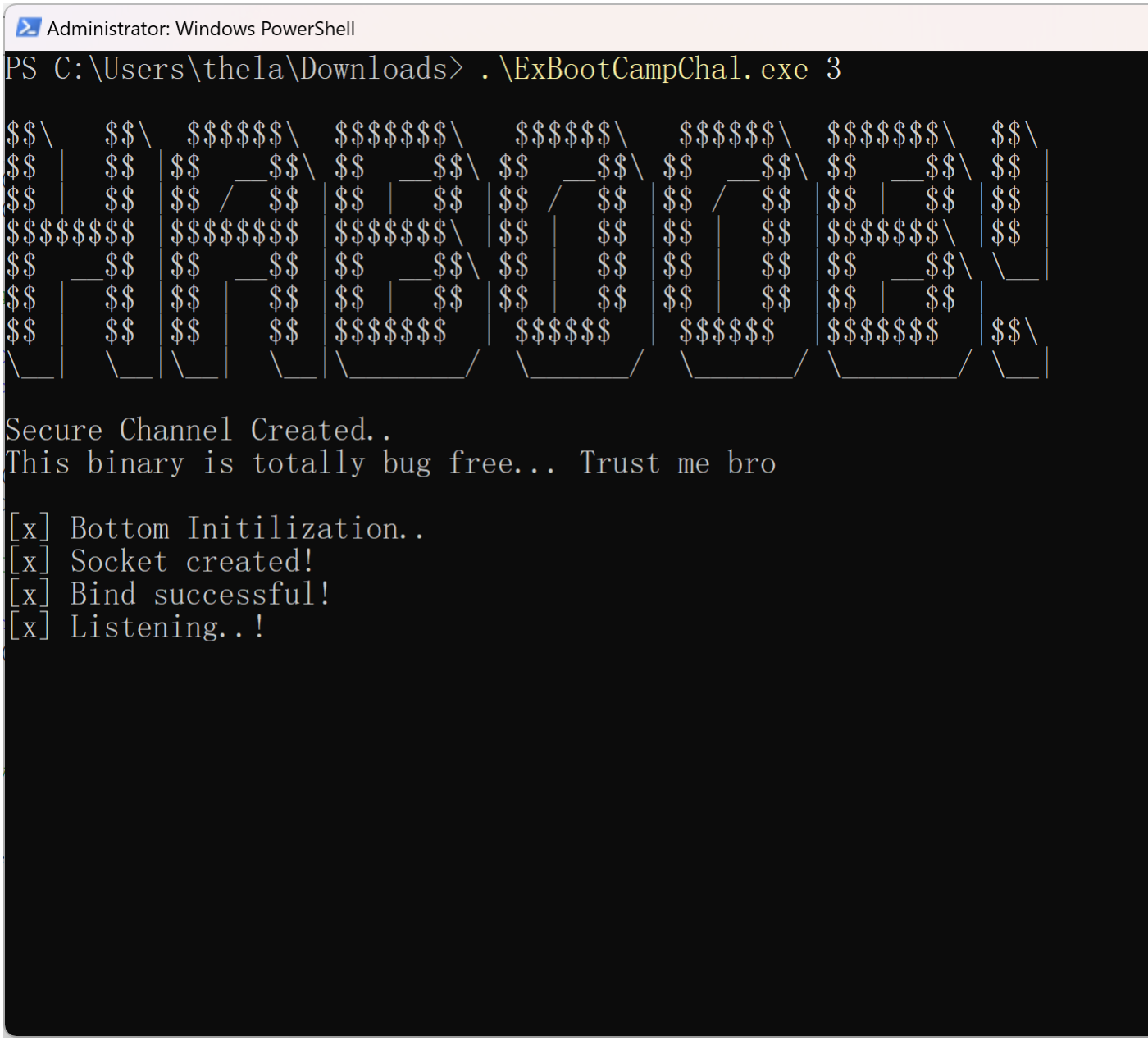
Decompile: FUN_00401447 - (ExBootCampChal.exe)

```
40      pcVar6 = "Hope We See You Soon ^_^\n";
41    }
42    else {
43      if (cVar1 == '1') {
44        FUN_00401006("[-] Pass Me: {");
45        iVar4 = 0;
46        do {
47          FUN_00401006(&DAT_00418c64,*(undefined *)((int)&local_14 + iVar4));
48          if (iVar4 != 0xd) {
49            FUN_00401006(&DAT_00418c6c);
50          }
51          iVar4 = iVar4 + 1;
52        } while (iVar4 < 0xe);
53        FUN_00401006(&DAT_00418c70);
54        if (param_1 != 3) {
55          return 0;
56        }
57        sVar2 = _strlen(*(char **)(param_2 + 8));
58        if (sVar2 == 0) {
59          return 0;
60        }
61        pcVar6 = *(char **)(param_2 + 8);
62        if (*pcVar6 != '{') {
63          return 0;
64        }
65        uVar5 = 0;
66        sVar2 = __mbslen((uchar *)&local_14);
67        if (sVar2 != 0) {
68          do {
69            *(byte *)((int)&local_14 + uVar5) = *(byte *)((int)&local_14 + uVar5) | 0x80;
70            uVar5 = uVar5 + 1;
71            sVar2 = __mbslen((uchar *)&local_14);
72          } while (uVar5 < sVar2);
73        }
74        sVar2 = __mbslen((uchar *)&local_14);
75        if (sVar2 != 0) {
76          do {
77            *(byte *)((int)&local_14 + uVar3) = *(byte *)((int)&local_14 + uVar3) & 0x7f;
78            uVar3 = uVar3 + 1;
              sVar2 = __mbslen((uchar *)&local_14);
```

Here we can see closely that by choosing different arguments different function will be triggered

```
    else {
      if (cVar1 == '3') {
        FUN_00401006("[x] Bottom Initilization..\n");
        FUN_004011ef();
        return 0;
      }
      if (cVar1 != '4') {
        if (cVar1 == '5') {
          FUN_00401006("[x] Starting Secret Data Exchange..\n");
          FUN_004016b3();
          return 0;
        }
        FUN_00401006("[-] Invalid Choice.\n");
        goto LAB_00401670;
      }
      FUN_00401006("[x] Sending Secret..\n");
      if (param_1 == 4) {
        _strtoul(*(char **)(param_2 + 0xc),(char **)0x0,0);
        FUN_00401344();
        return 0;
      }
    }
    pcVar6 = "[-] Invalid number of arguments.\n";
  }
}
FUN_00401006(pcVar6);
return 0;
```

Here the 3 argument looks interesting to me by clicking on 3 arguments you will trigger this function.



Bind? Socket? This is tcp connection key-words! Specifically listen! Nice lets check if we really established tcp connection or not?

By using process hacker click on network you will find this

ExBootCampChal.exe (2776)	BDR-PC	31337	TCP	Listen

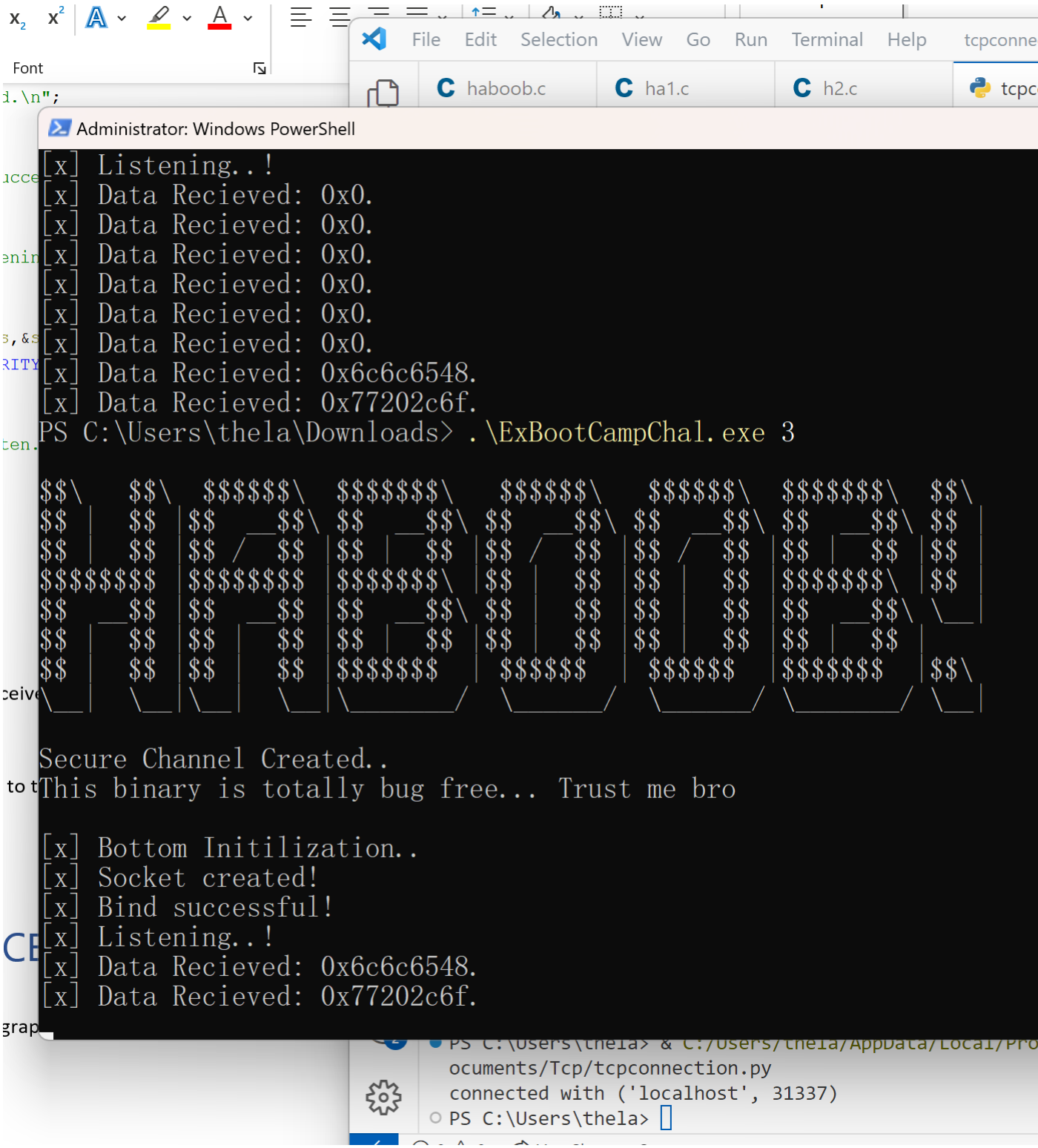
My educated guess came out true!! It is tcp listening connection at 31337 port locally !!!

By search by string in ghadria we find this

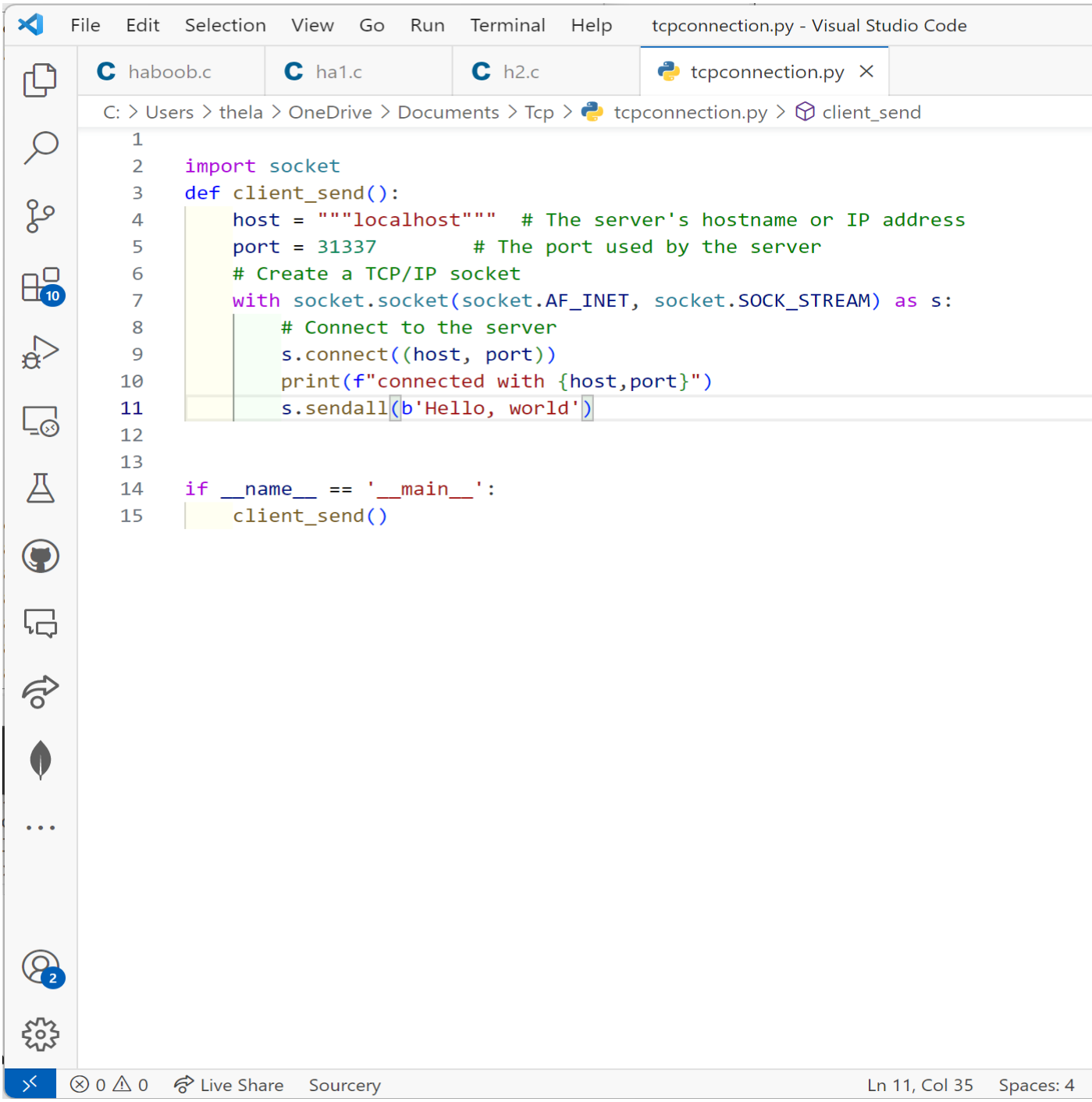
```
else {
  FUN_00401006("[x] Socket created!\n");
  sStack_1b8.sa_family = 2;
  sStack_1b8.sa_data._0_2_ = htons(0x7a69);
  phVar2 = gethostbyname("");
  inet_ntoa((in_addr)((_union_1226 *)*phVar2->h_addr_list)->S_un_b);
  sStack_1b8.sa_data._2_4_ = inet_addr("0.0.0.0");
  iVar1 = bind(s,&sStack_1b8,0x10);
  if (iVar1 == -1) {
    pcVar3 = "[x] Error, bind.\n";
  }
  else {
    FUN_00401006("[x] Bind successful!\n");
    iVar1 = listen(s,1);
    if (iVar1 != -1) {
      FUN_00401006("[x] Listening..!\n");
      iStack_1c4 = 0x10;
      do {
        SStack_1c0 = accept(s,&sStack_1a8,&iStack_1c4);
        CreateThread((LPSECURITY_ATTRIBUTES)0x0,0,FUN_004010a0,&SStack_1c0,0,&DStack_1bc);
      } while( true );
    }
    pcVar3 = "[x] Error, listen.\n";
  }
  FUN_00401006(pcVar3);
  closesocket(s);
  WSACleanup();
```

It is listening and this pass the received data to a function CreateThread which process it !

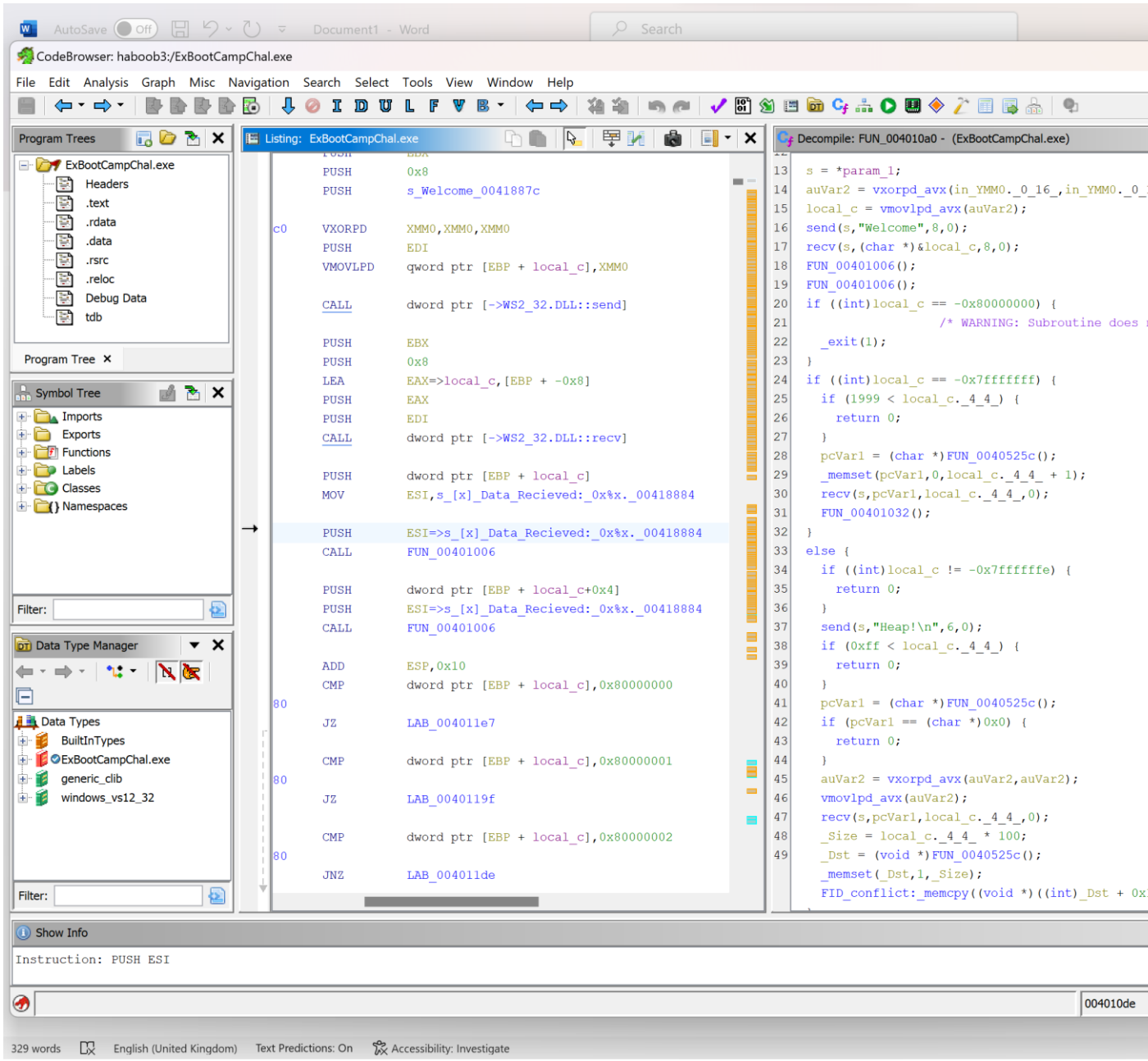
Now by using python let connect to the listener !



That's the python code



Wow its working!!!!!!!! Now lets search by string “Data Received” to really know what is going on

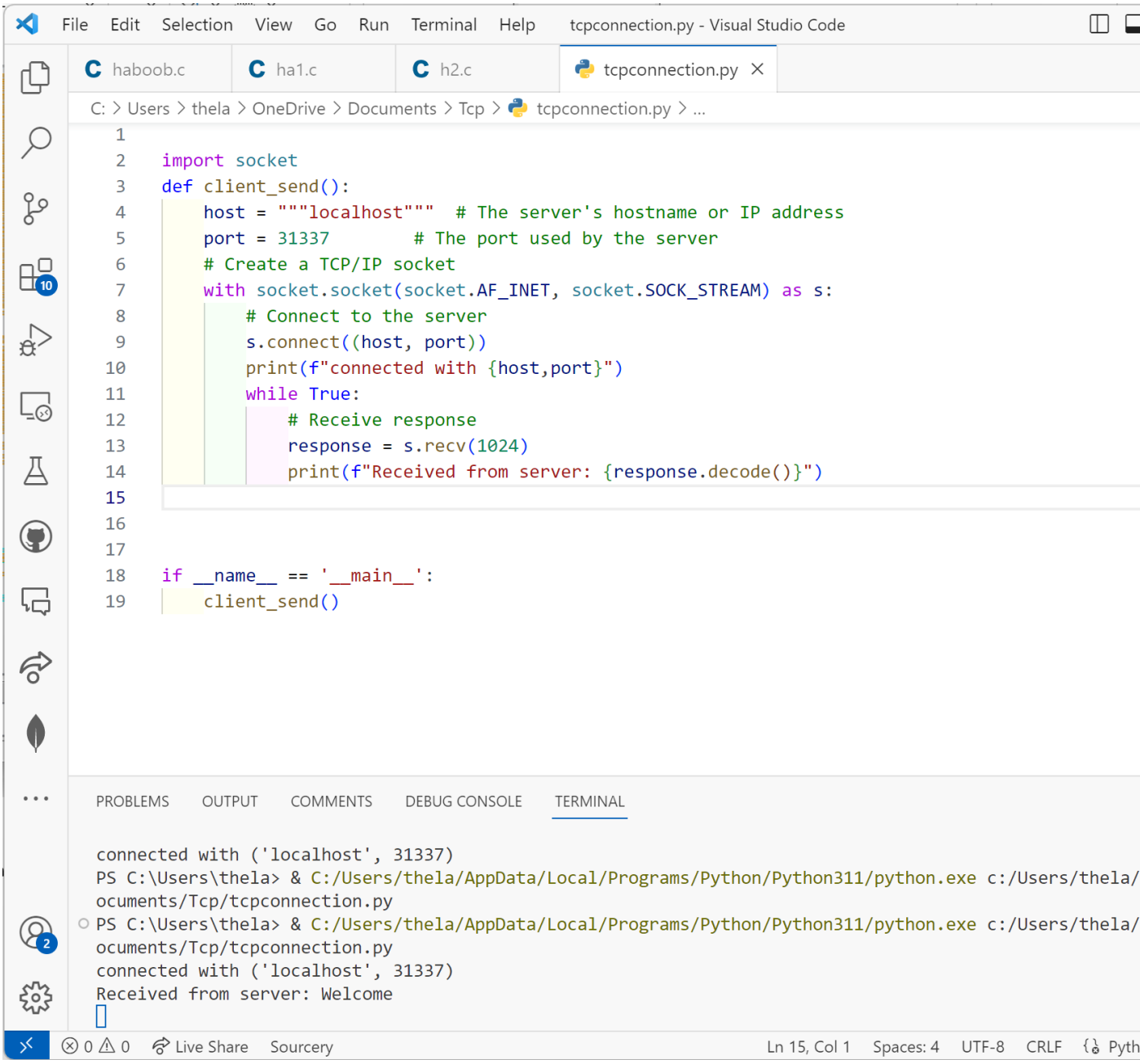


Each time we send a message it CALL FUN_00401006 and in the right side another function but decompiled.

Here FUN_00401006 decompiled

Send welcome? Lets try to receive and read the message

Using python



It is working !!!! which means FUN_00401a0 have socket that receive and send plus store to the memory

In FUN_00401006 it pass an argument to another function and print and address of that argument which explain the response “Data received xyz” xyz is where the data is located in the heap

Decompile: FUN_00401000 - (ExBootCampChal.exe)

```
1
2 undefined * FUN_00401000(void)
3
4 {
5   return &DAT_0041b308;
6 }
7
```

Now search about by string DAT_004lb308

PRODUCT/SERVICE/METHODOLOGY

Describe the methods and demographics you used to obtain your data. Why did you choose the research tactics you implemented? How will this strategy inform on the topic you're covering?

KEY FINDINGS

Key Findings #1

Research and argument

[To replace a photo with your own, just delete it and then, on the Insert tab, click Picture.]

Key Findings #2

Research and argument

Key Findings #3

Research and argument

Visual Data

Insert any data tables/charts/graphs/infographics etc.

CONCLUSION

Time to wrap it up. What is your conclusion? How would you synthesise all the information into something even the busiest CEO wants to read? What are the key takeaways? How does your product/service/methodology uniquely address the issues raised by your study?

Key Takeaways

- Takeaway #1
- Takeaway #2
- Takeaway #3