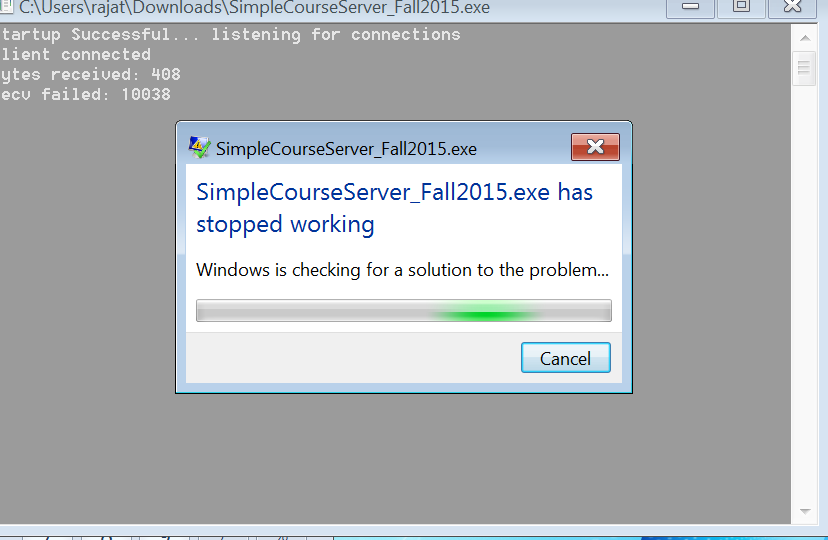
CND Assignment – 1

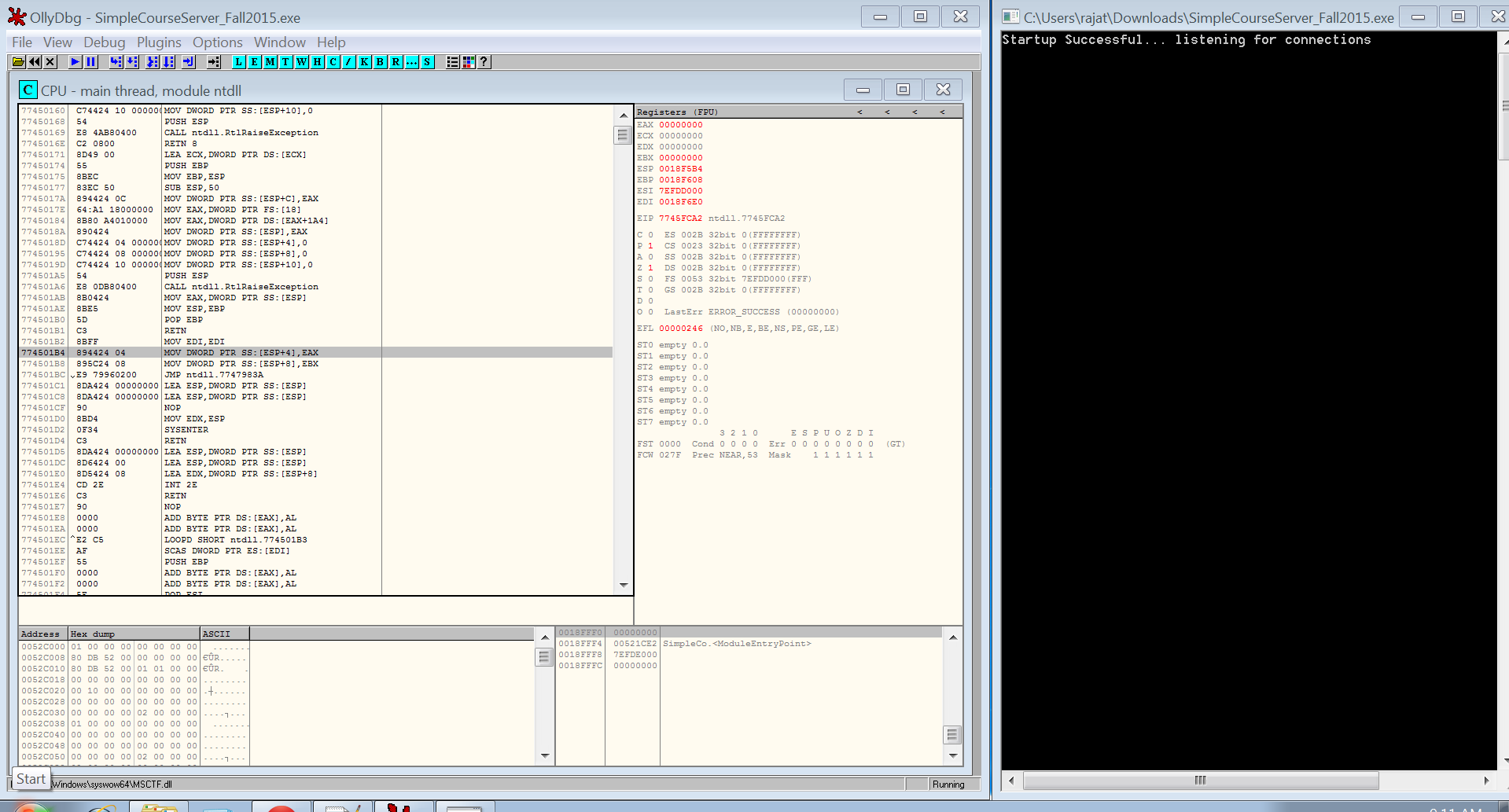
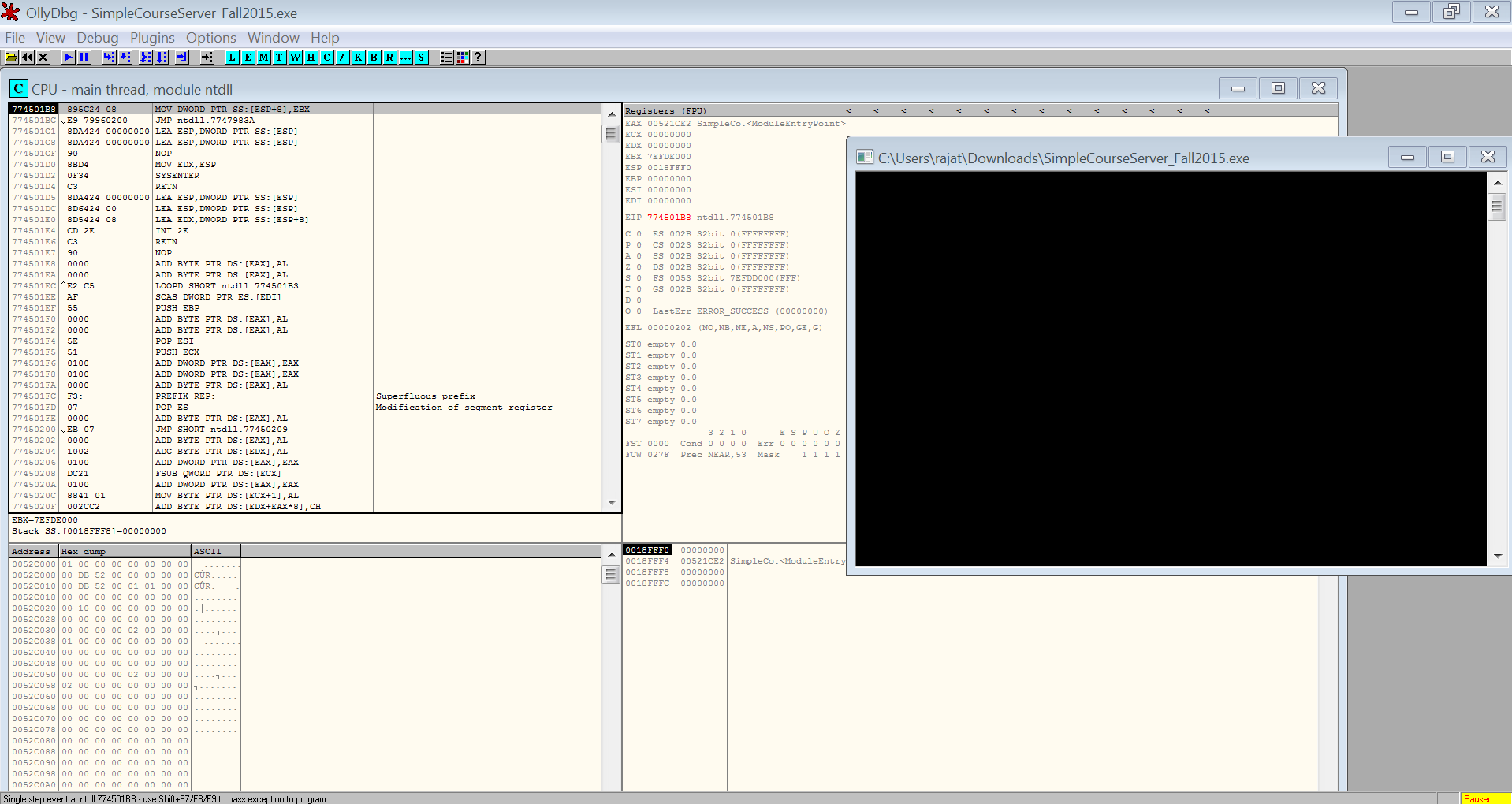
Name: Rajat Vij

Ans 1.1 I used ollydb to know the values of EIP and EBP of the program at different situations and used netcat to connect to simpleprogram.exe.

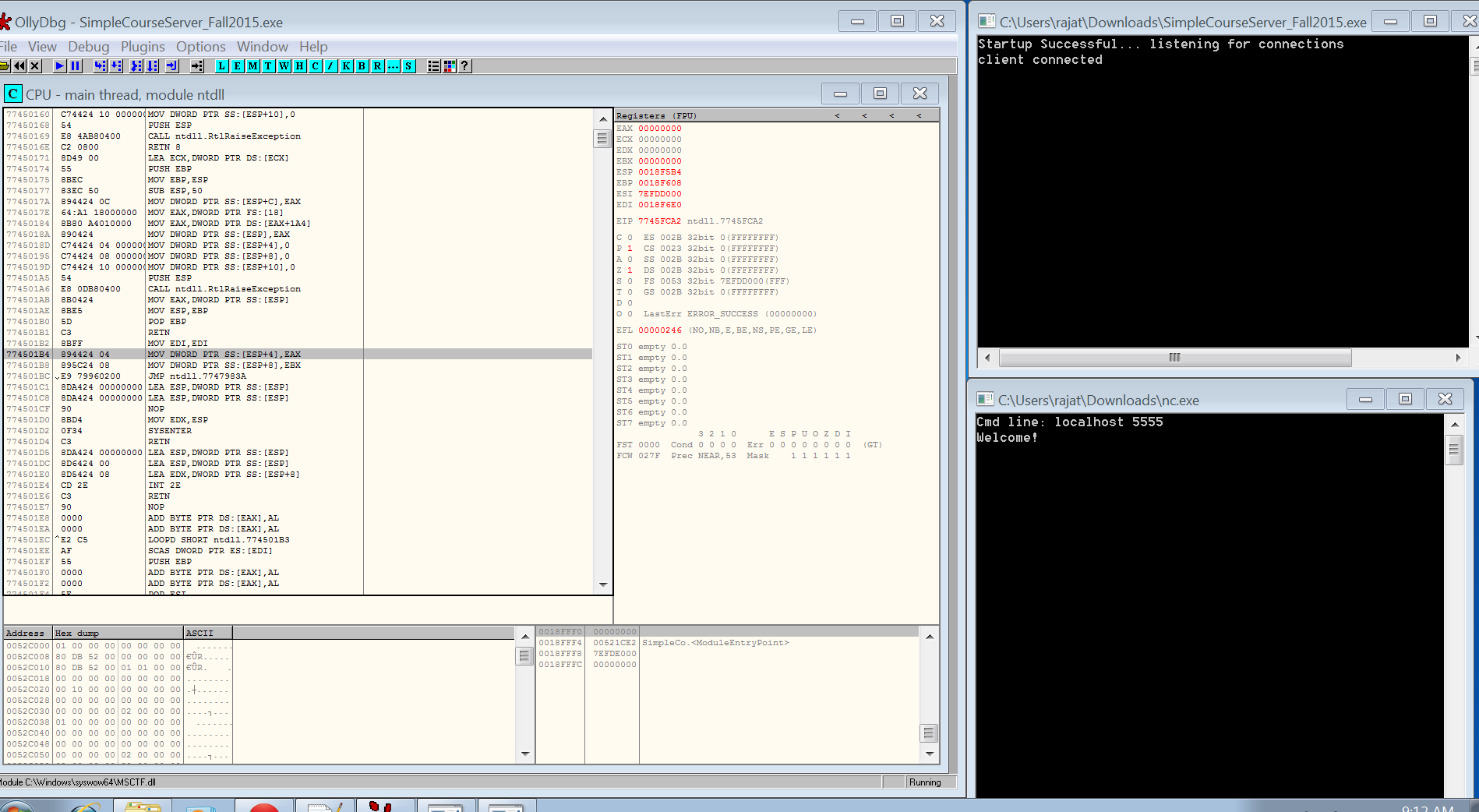
(Ans 1.2)First thing I discovered is that user can provide any number of input characters and the size of stack that input can have is limited. So program crashed when we input 407(via netcat) or more characters. i.e., program crashes when it receives more than 408 bytes(1 byte is for enter and 1 byte is for 1 character).



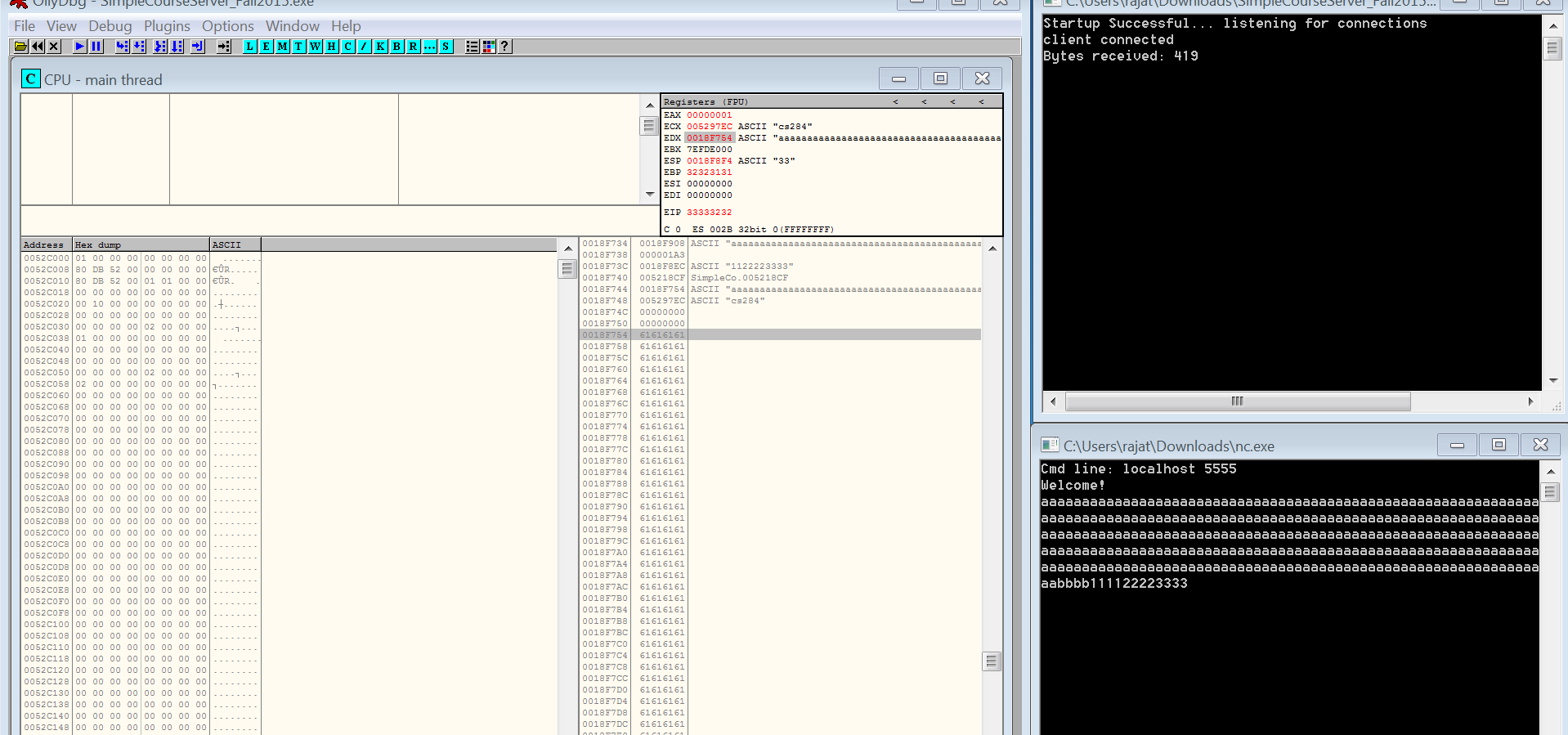
Then I ran the program via ollydb to know the address values of EBP and EIP.

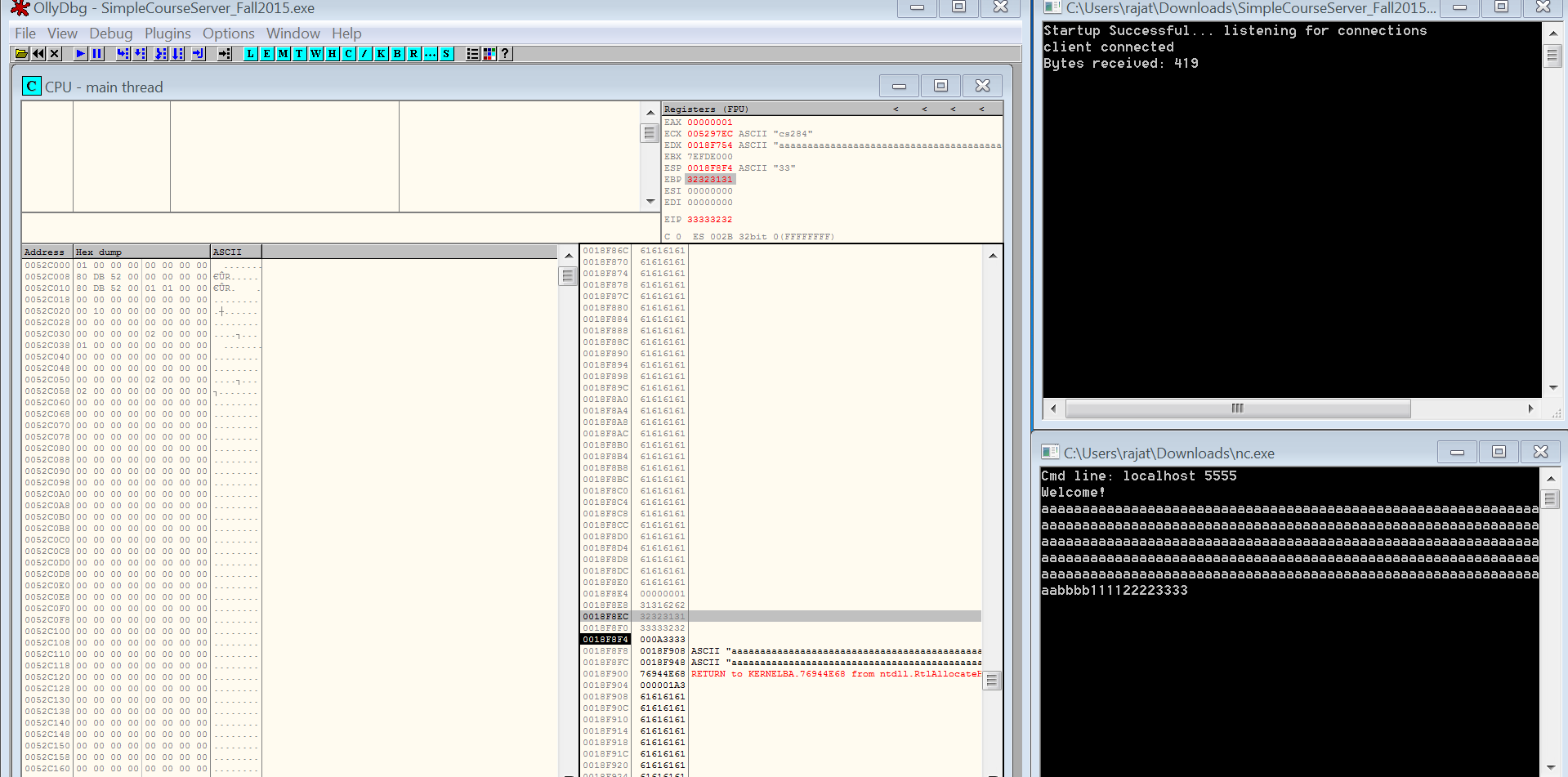


Then I ran nc.exe



(Ans 1.3 and 1.4)Then I checked the address value of Welcome message in ollydb. Then I entered similar 406 character and the different set of multiple 4 characters afterwards to check the value of EBP and EIP where the program is crashing and the start of stack.





Ans 1.2. Program is crashing when entering more than 407 characters and 408 bytes.

Used simple trial and error to find the number of characters required to crash the program.

Ans 1.3. Address where our input begins on stack - 0018f908 and 0018f754.

Ans 1.4. Address that becomes EIP which contains user input is 0018faa4.

Ans 1.5. Programmer and write a condition where an error message is displayed if input is more than the desired characters and tell the user to enter only desired number of characters.

Programmer can also trip the input to the desired number of characters.

Ans 2.1. Sleep is located at 0x762510ff in kernel32.dll

OS Name: Microsoft Windows 7 Professional

OS Version: 6.1.7601 Service Pack 1 Build 7601

System Locale: en-us;English (United States)

Input Locale: en-us;English (United States)

Ans 2.2. and 2.3. Please check the folder for Answer 2 – CND for various files displayed in the screenshot

