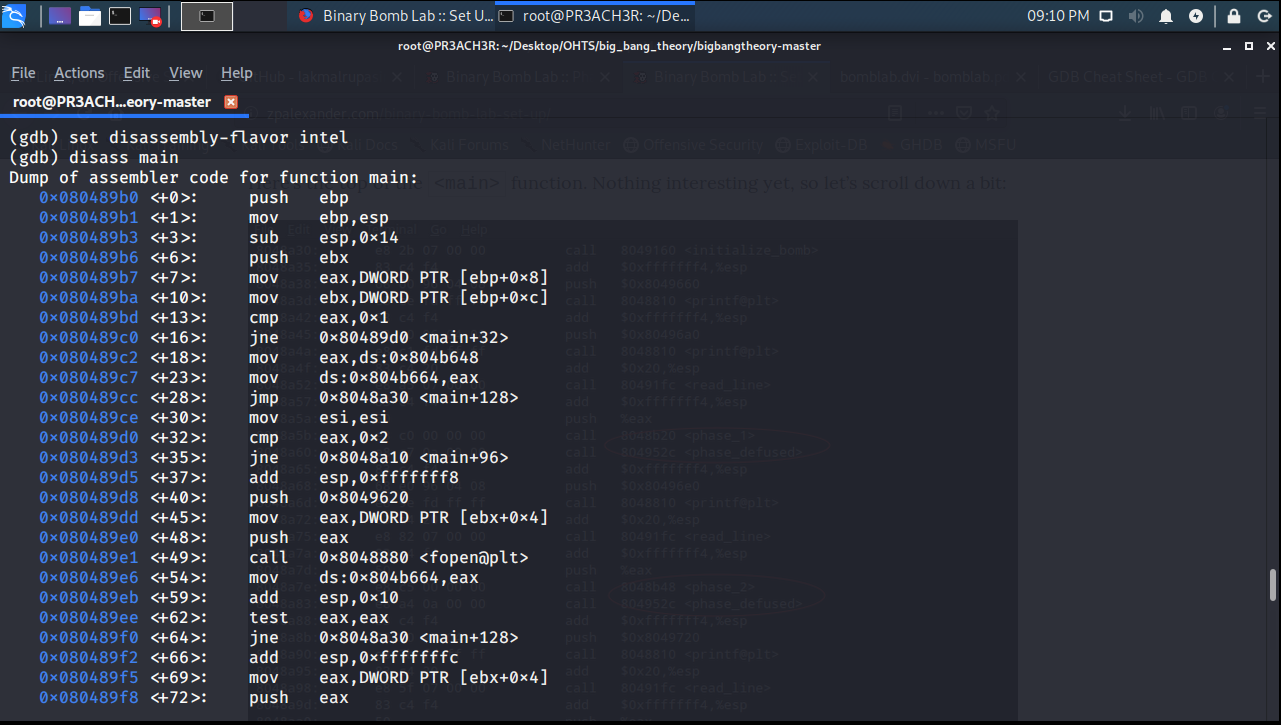
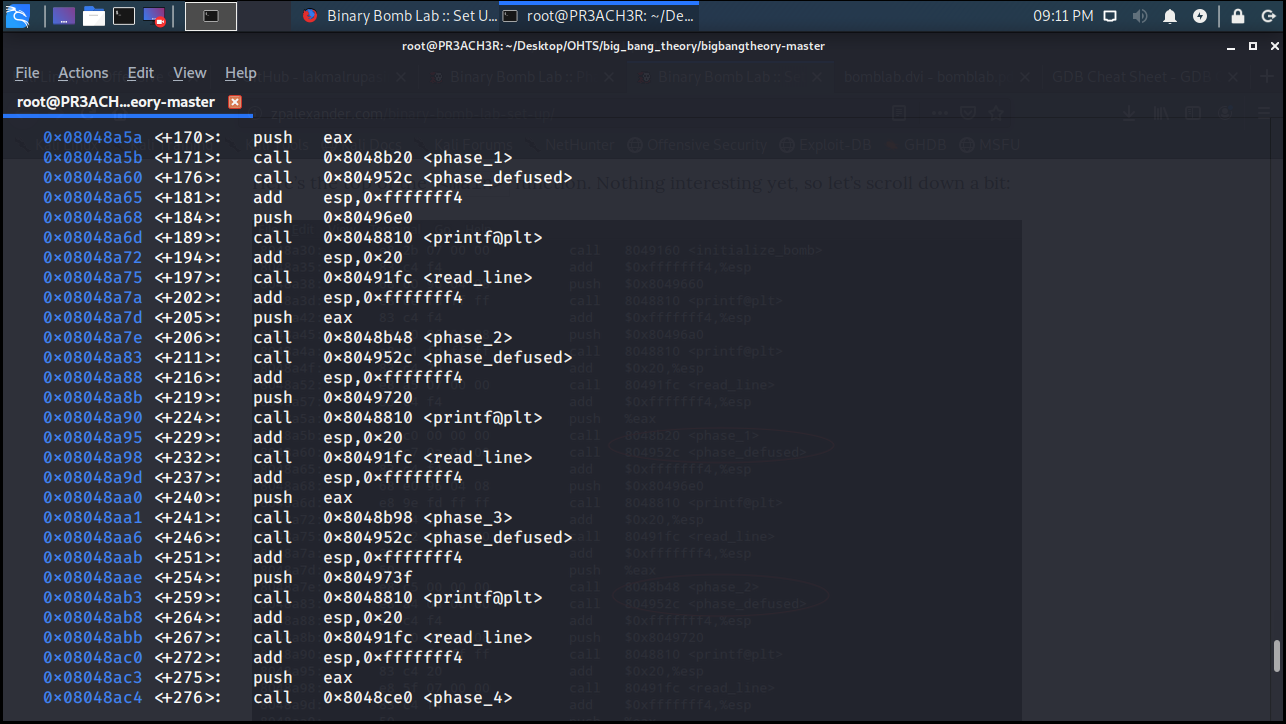
**IT17015622**

**K. Shanith Rathnayake**

**Report – Big Bang Theory**

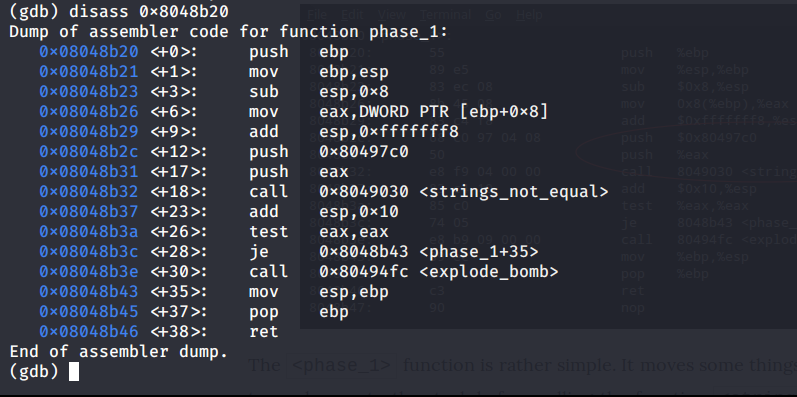
First, I used gdb to disassemble the main function of sheldon1.



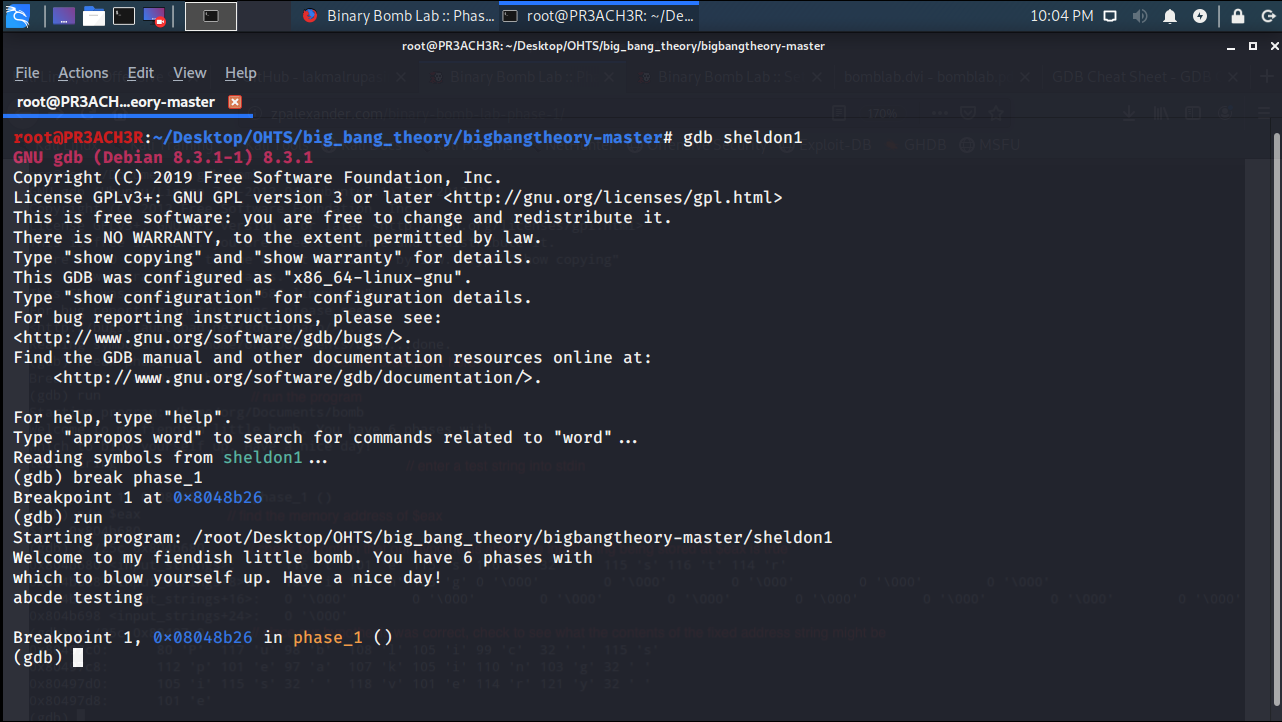


Here we can identify various functions being called for various phases in order to diffuse the bombs.

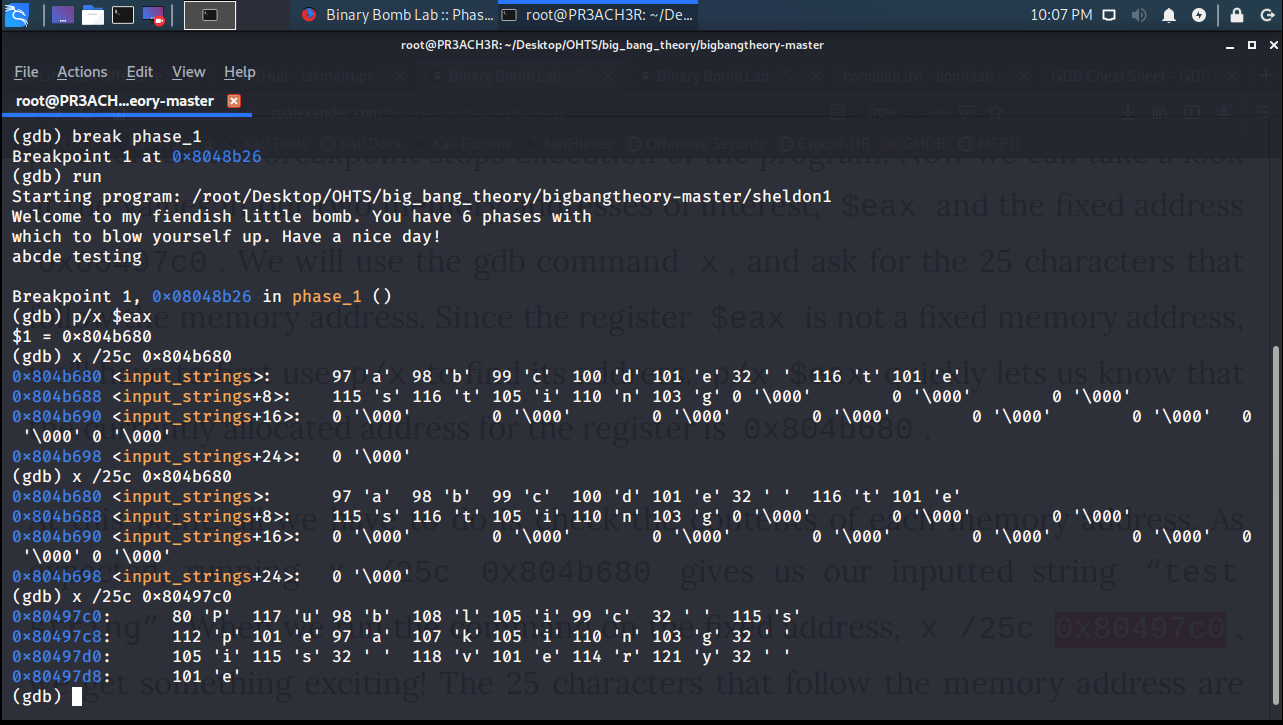
Next we must disassemble the phase 1 function to view it’s assembler code.



**Solving Phase 1 –**



Here, in order to prevent the bomb from exploding, we set a breakpoint at the phase 1 function and run the program.

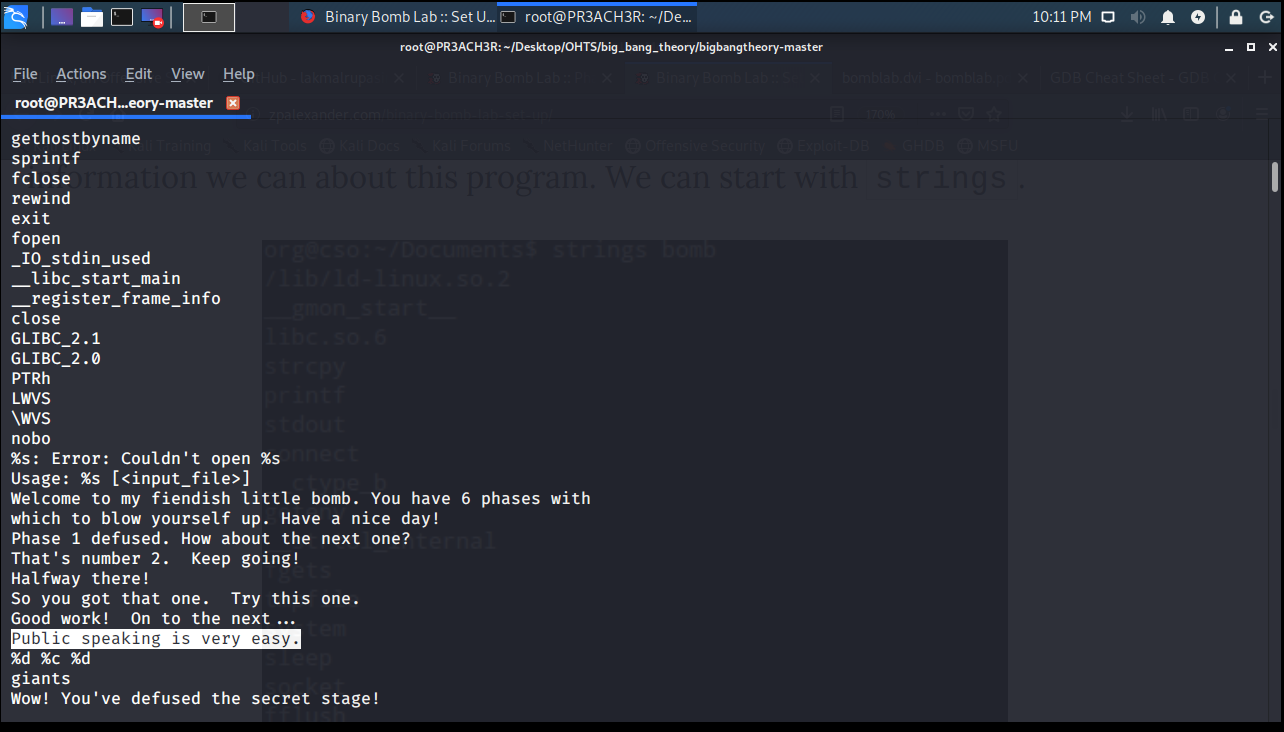


Next, we identify the memory location of $eax and print the first 25 characters of that location. Here we provide a random string “abcde testing”, and verify whether the input strings actually match.

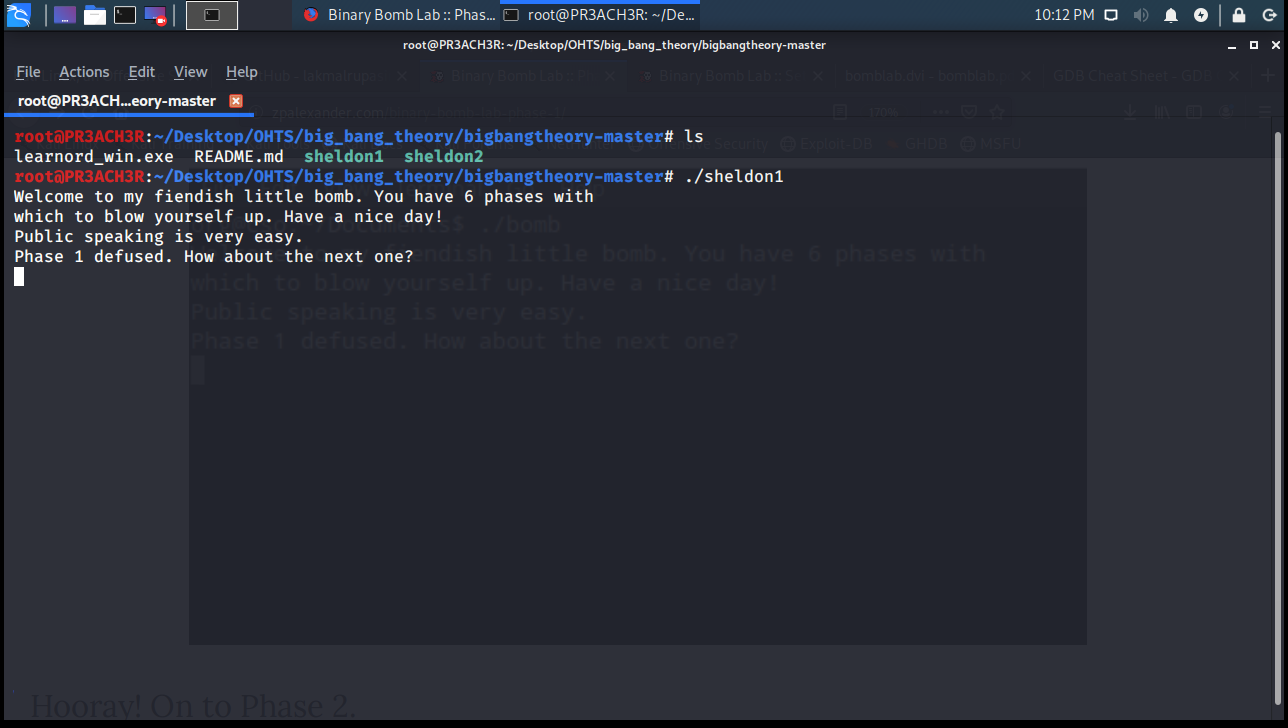
Next, we use the same command to identify which string of characters are present in the memory location identified in the main function of phase 1 which is used for the comparison (0x80497c0).

Using that, we identify that the password should contain the character string, “public speaking is very e”.

To identify the remaining set of characters, we use “strings sheldon1” command.



Here we can identify that the full phrase is, “Public speaking is very easy”.



Finally, by entering that pass-phrase, we can diffuse the first bomb.