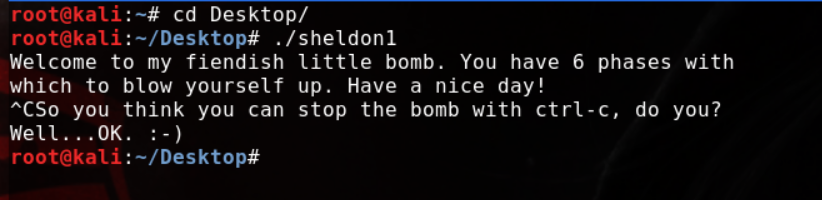
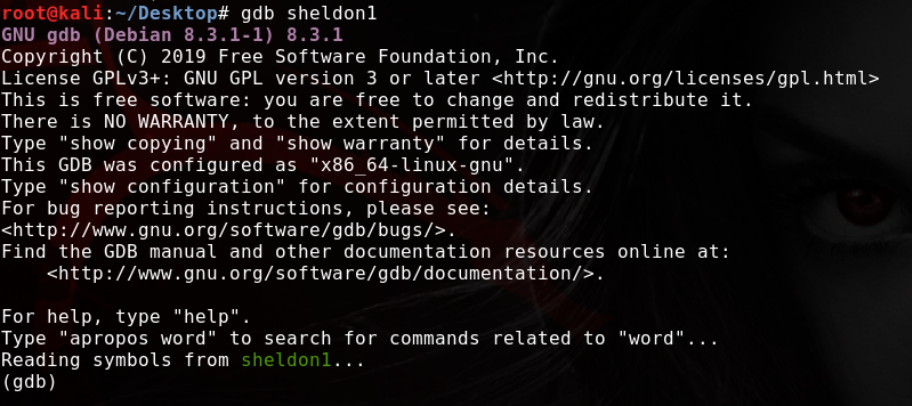
**Bigbangtheory\_Solutions (Phase01)**

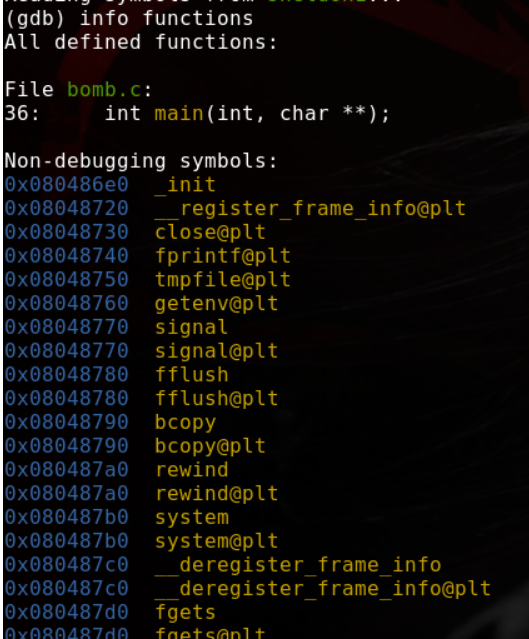
Give execute permission to the file sheldon1 and then run it using ./sheldon1



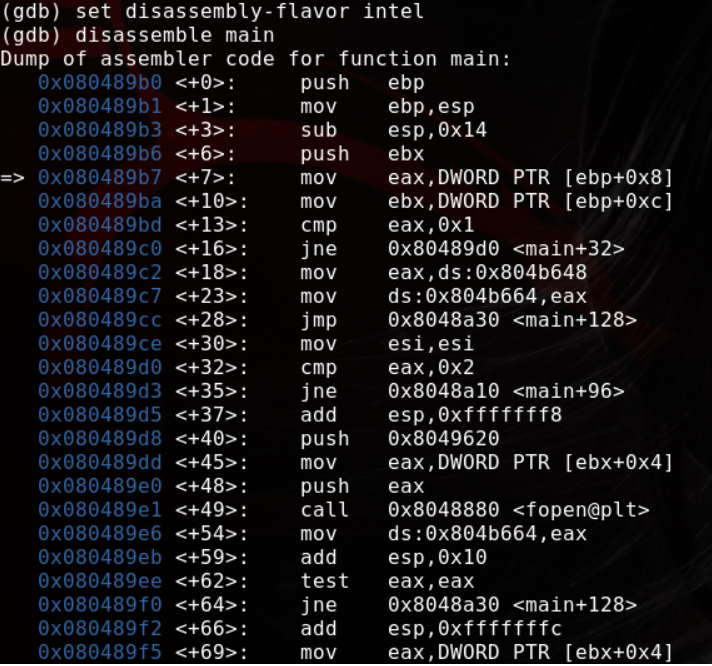
Use gdb with sheldon1.



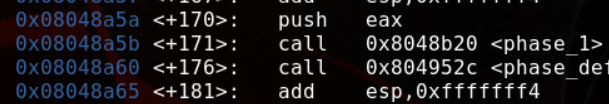
Use gdb's info functions command to get all available functions in sheldon1, and identify the "main" function (can use start as well).



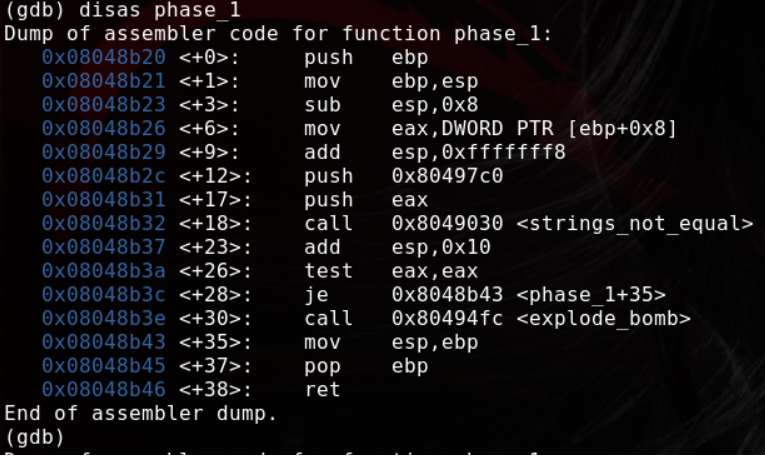
Then set the disassemble flavour as intel and then disassemble the main function



Find a special function called phase\_1



Disassemble the paese\_1 function using disas phase\_1 command



Here, you can find an instruction named test and there the program will check the values of eax and eax. In top of that, about like 4 lines before, there is a static push to the stack.  
Print out the string value of this using x/s and get the passphrase for phase\_1.

