Challenge 1

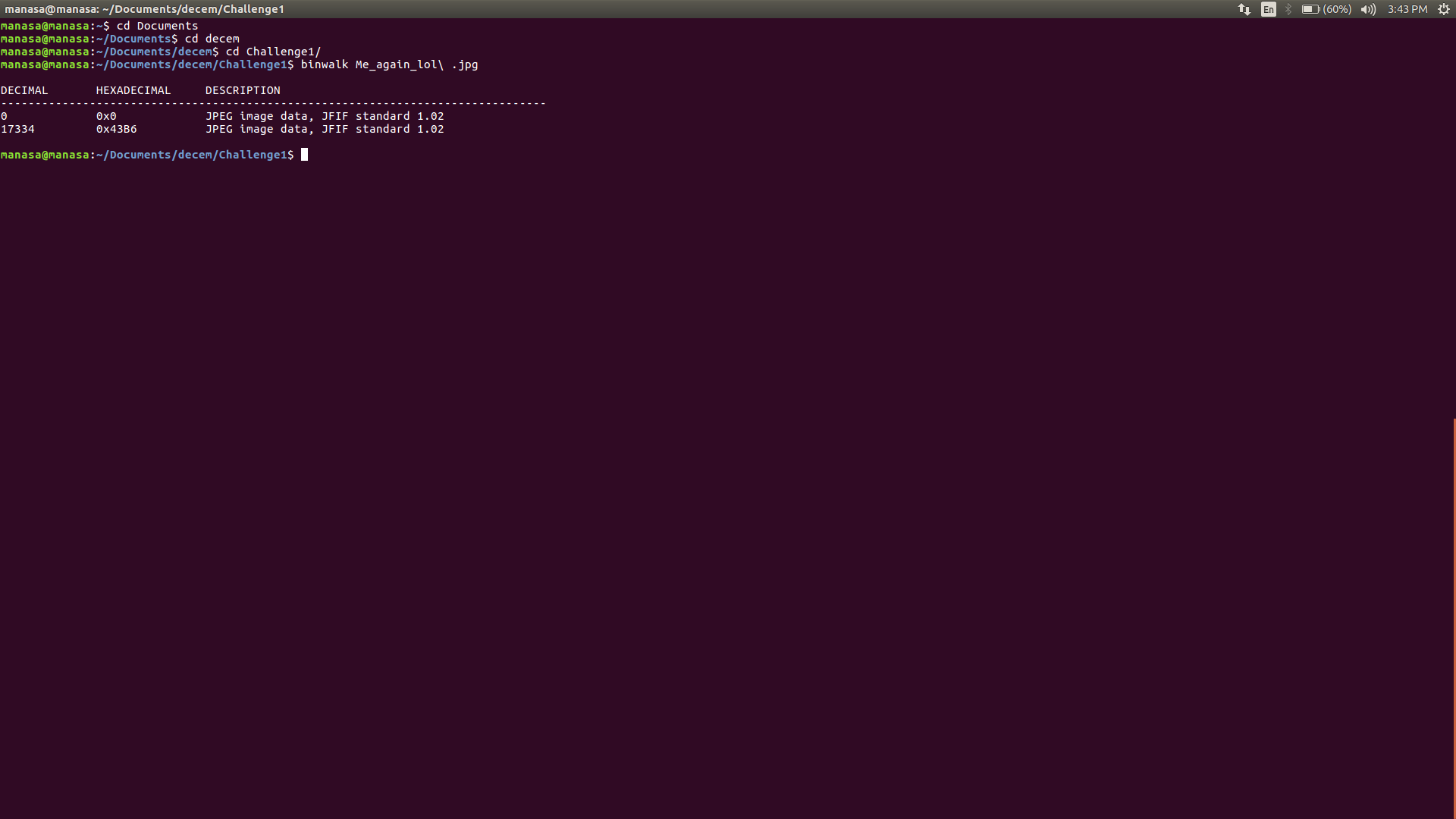
Download the challenge from Challenge file in this repo.



The image in the challenge can be examined by various forensic tools like binwalk, strings,exiftool,hexdump,xxd etc.

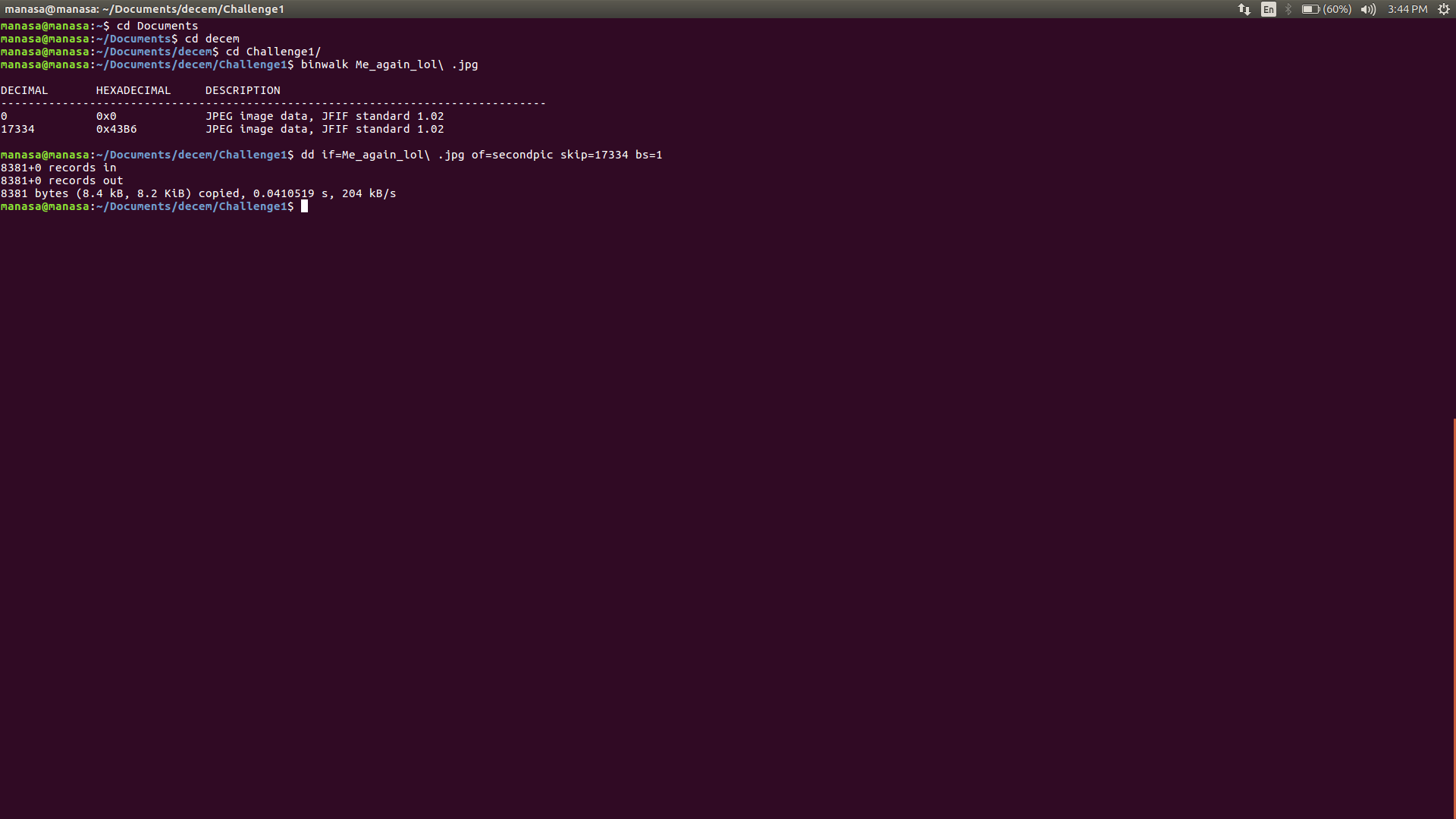
By using binwalk, it was clear that the image had two JPEG file in it.

>> binwalk Me\_again\_lol .jpg



By using dd tool, the second image can be extracted.

>> dd if=Me\_again\_lol.jpg of=secondpic skip=17334 bs=1

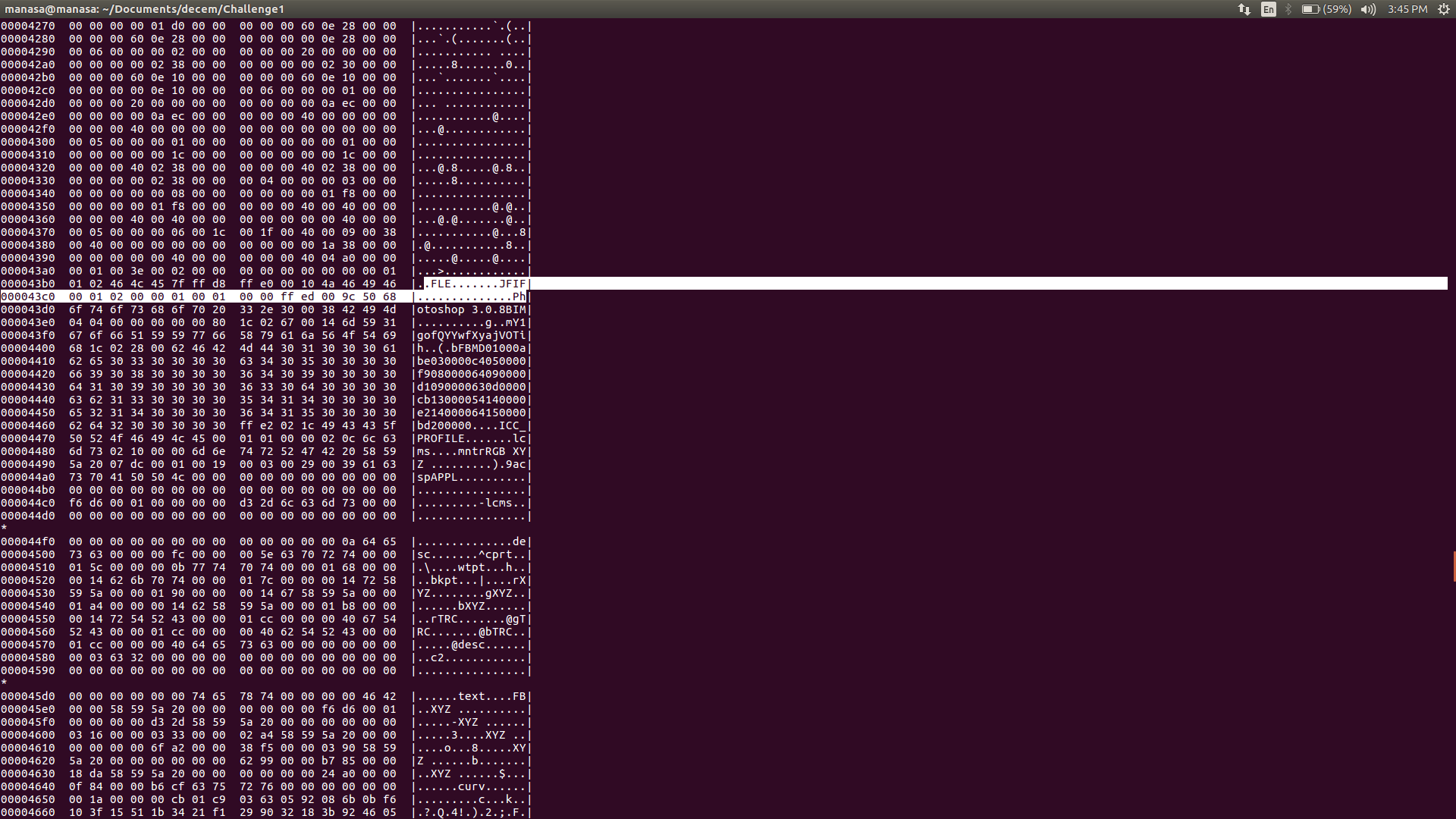


The second pic is :



After looking into the hexdump of both images, we observe a string "FLE" in the beginning of second images data.

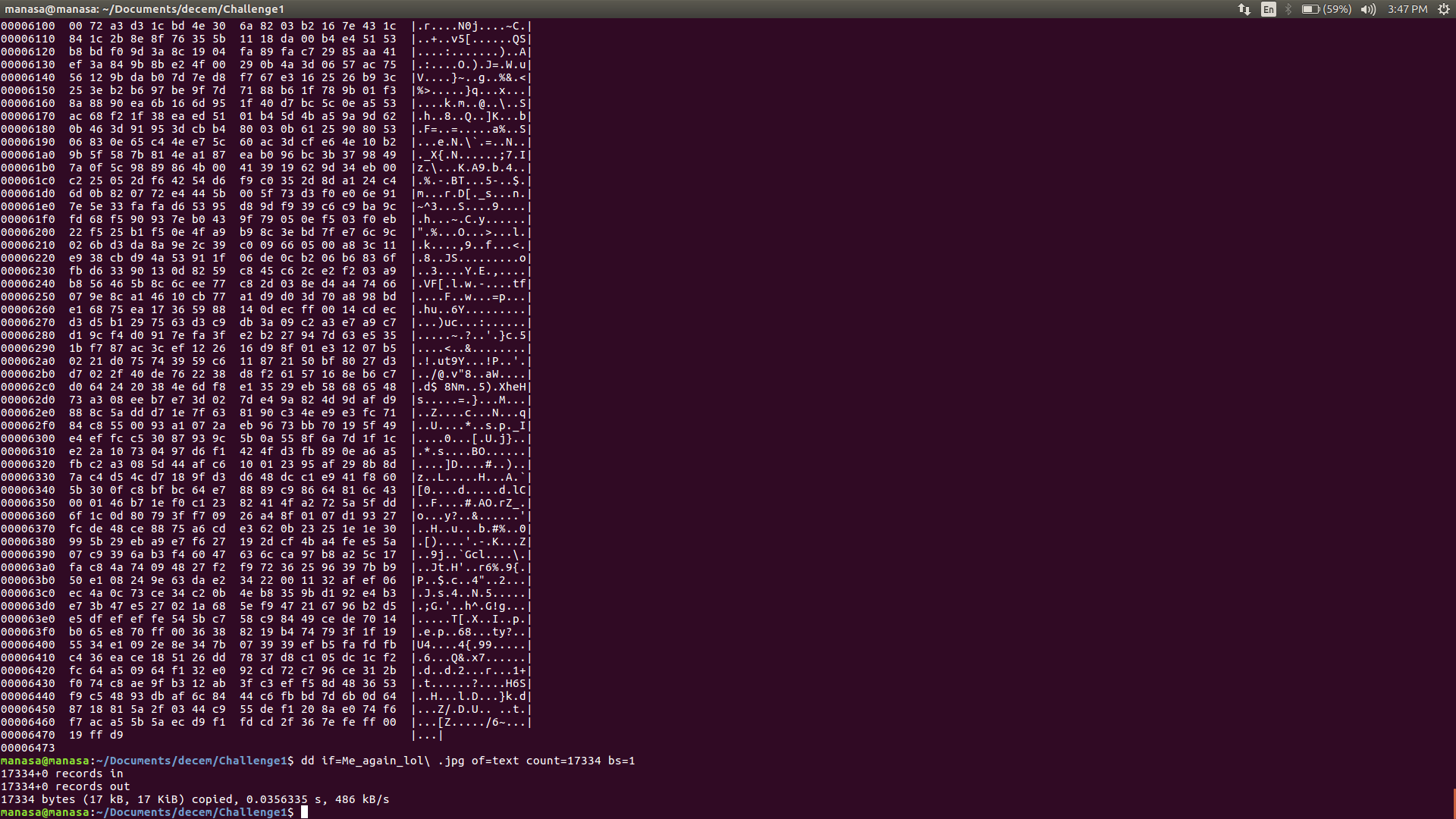
"FLE" is nothing but the reverse of ELF format, Executable and Linked Format.



We need to extract a file from that data and convert it into a ELF file and find the flag from it using reversing.

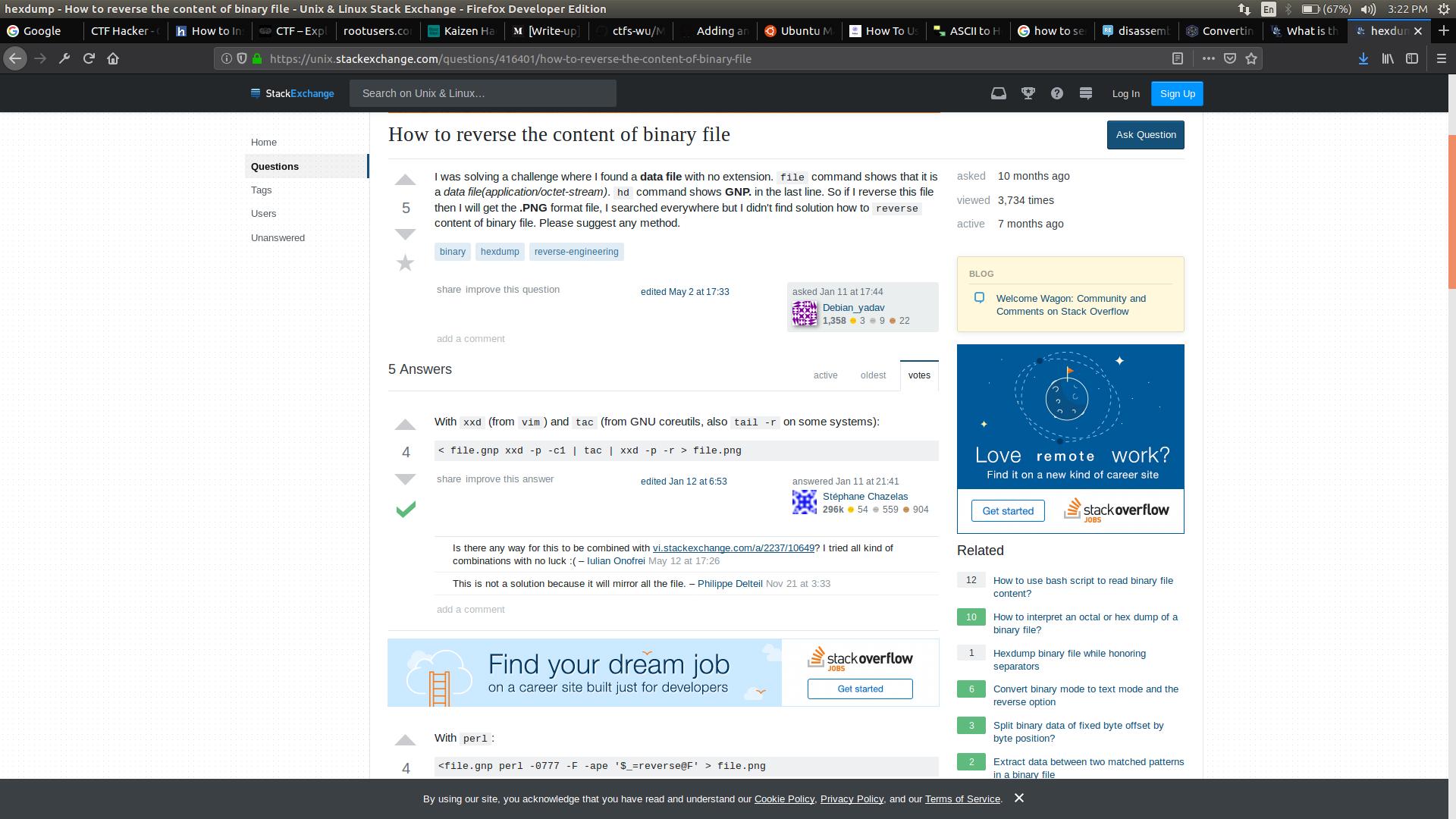
By using dd tool, a file `text` is extracted till the FLE string, so as to convert it into ELF format.

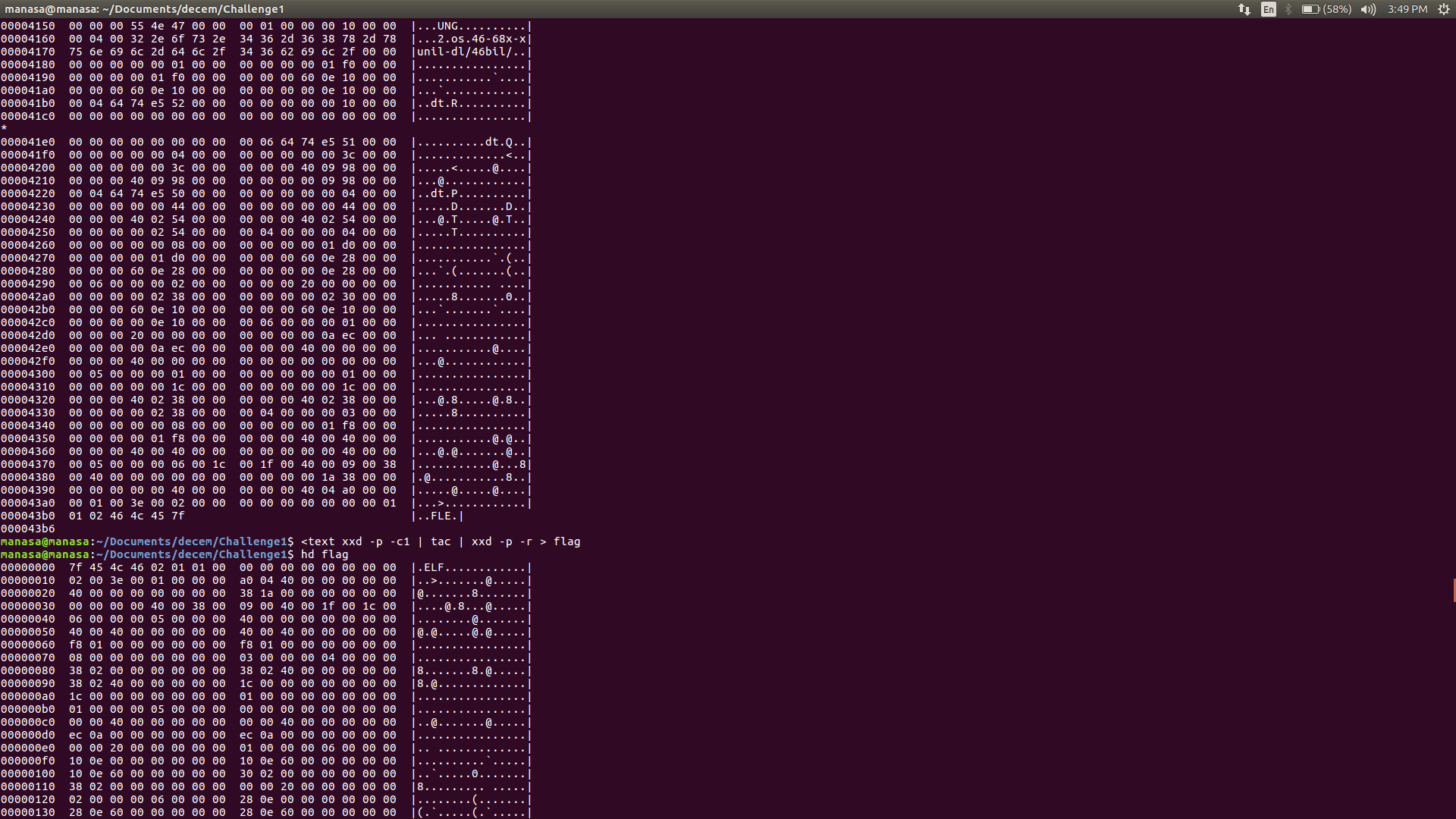
>> dd if=Me\_again\_lol .jpg of=text count=17734 bs=1



On viewing the hexdump and data of text, we notice "ELF" at the end of the file.

Reverse the content of the file. On searching xxd commandfor reversing the content.



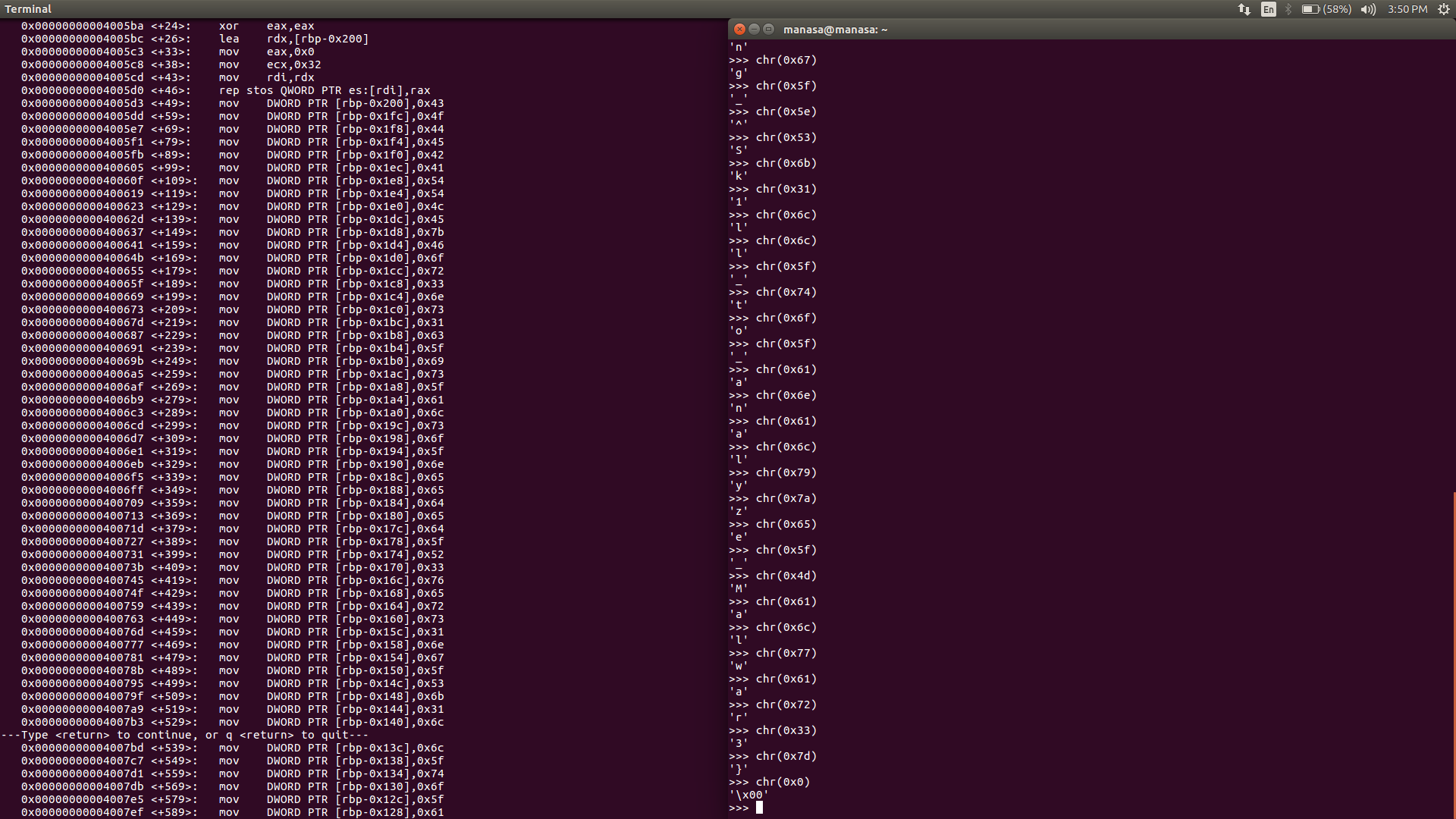


Now, the file `flag` is an Executable file. To find the flag, we will have to reverse it.

I used gdb, a debugger to find the flag.

>> gdb flag

>> disas main



On finding the ascii character for each instruction, the flag for the challenge is obtained.

Flag : CODEBATTLE{For3ns1c\_is\_also\_needed\_R3vers1ng\_Sk1ll\_to\_analyze\_Malwar3}