**CFSS Internship Practicals Solutions.**

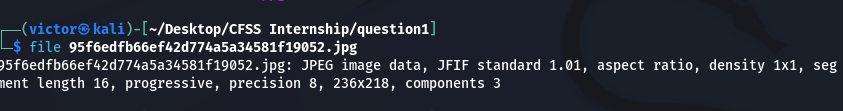
1. https://ctflearn.com/challenge/96

Think the flag is somewhere in there. Would you help me find it? <https://mega.nz/#!OHohCbTa!wbg60PARf4u6E6juuvK9-aDRe_bgEL937VO01EImM7c>

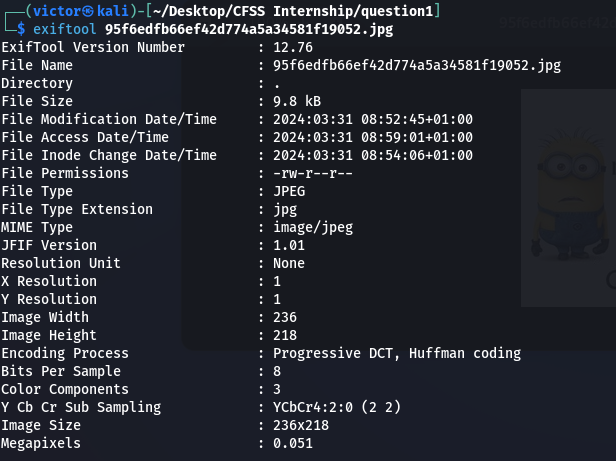
Solution

I downloaded the file and using the terminal ran the ‘file’ command to determine the file type of a file and the extension.





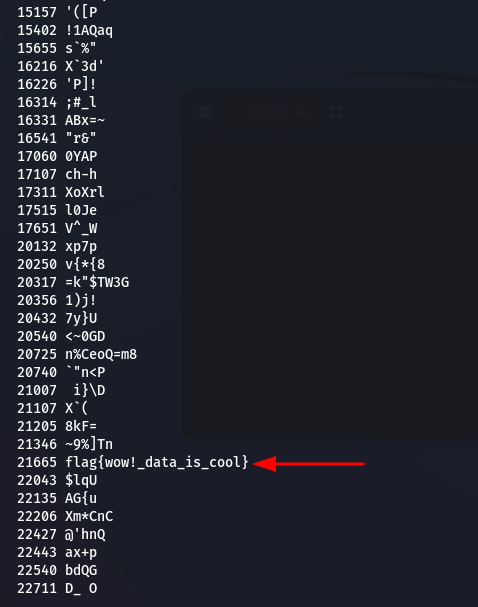
Since we’re looking for flags, I used the ‘exiftool’ display all available metadata for the image file.



Further in my investigation, I utilized the xxd command to generate hexadecimal dumps of the JPEG file and to convert binary data for detailed analysis, enhancing my ability to reconstruct and analyze digital evidence efficiently. This step proved instrumental in uncovering crucial insights and contributing to the successful progression of the investigation.



This produced readable and non-readable text. So I used the strings command with the -ao option to extract ASCII and Unicode strings from the JPEG file, enabling the identification of human-readable text embedded within the binary data. 



I copied the flag and pasted it in the CTF and submitted it.

