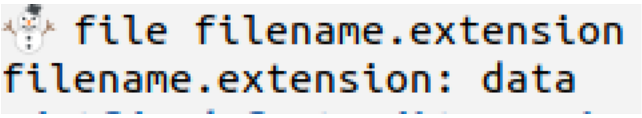
Codefest CTF 2018

Problem: It’s Magic (200, Forensics)
Repair given corrupted file to get the flag. download file here.

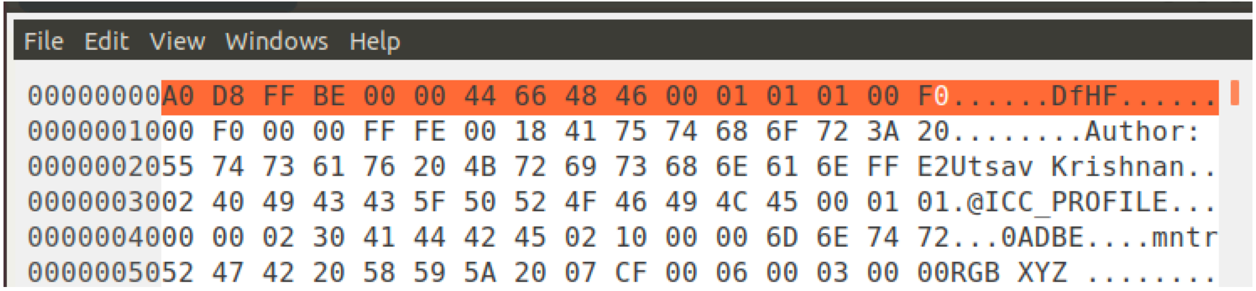
Output Format
CodefestCTF{flag}

Solution:
After downloading the file provided, I examine it using the **file** command:



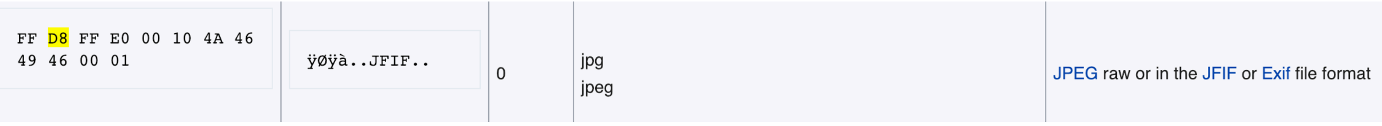
```
file filename.extension
filename.extension: data
```

I then run the **strings** command on the file and find nothing useful. Assuming the file is corrupted per the problem specification, I then examine it using **ghex** to find further hints regarding the file signature:



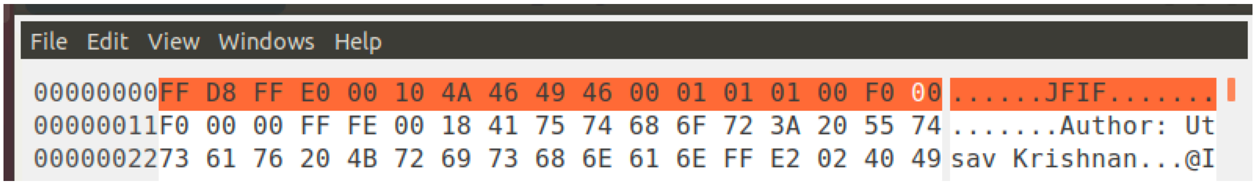
```
00000000A0 D8 FF BE 00 00 44 66 48 46 00 01 01 01 00 F0......DfHF......
0000001000 F0 00 00 FF FE 00 18 41 75 74 68 6F 72 3A 20........Author:
0000002055 74 73 61 76 20 4B 72 69 73 68 6E 61 6E FF E2Utsav Krishnan..
0000003002 40 49 43 43 5F 50 52 4F 46 49 4C 45 00 01 01.@ICC_PROFILE...
0000004000 00 02 30 41 44 42 45 02 10 00 00 6D 6E 74 72...0ADBE....mntr
0000005052 47 42 20 58 59 5A 20 07 CF 00 06 00 03 00 00RGB XYZ ........
```

Looking at the first 8 bytes (if it is the start of the file), it seems that the file closely resembles a JFIF file upon searching for common file signatures online. Searching by A0 didn’t yield anything useful, so a search by D8 yielded the following:



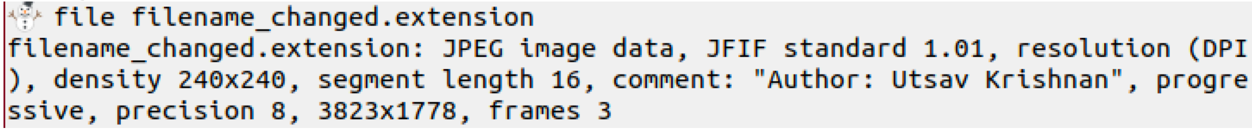
FF D8 FF E0 00 10 4A 46 49 46 00 01	ÿØÿà..JFIF..	0	jpg jpeg	JPEG raw or in the JFIF or Exif file format

A copy of the file is made, and I then change the bytes in the copy using **ghex**, where the changed bytes are highlighted:
A0 D8 FF BE 00 00 44 66 48 46
->
FF D8 FF E0 00 10 4A 46 49 46



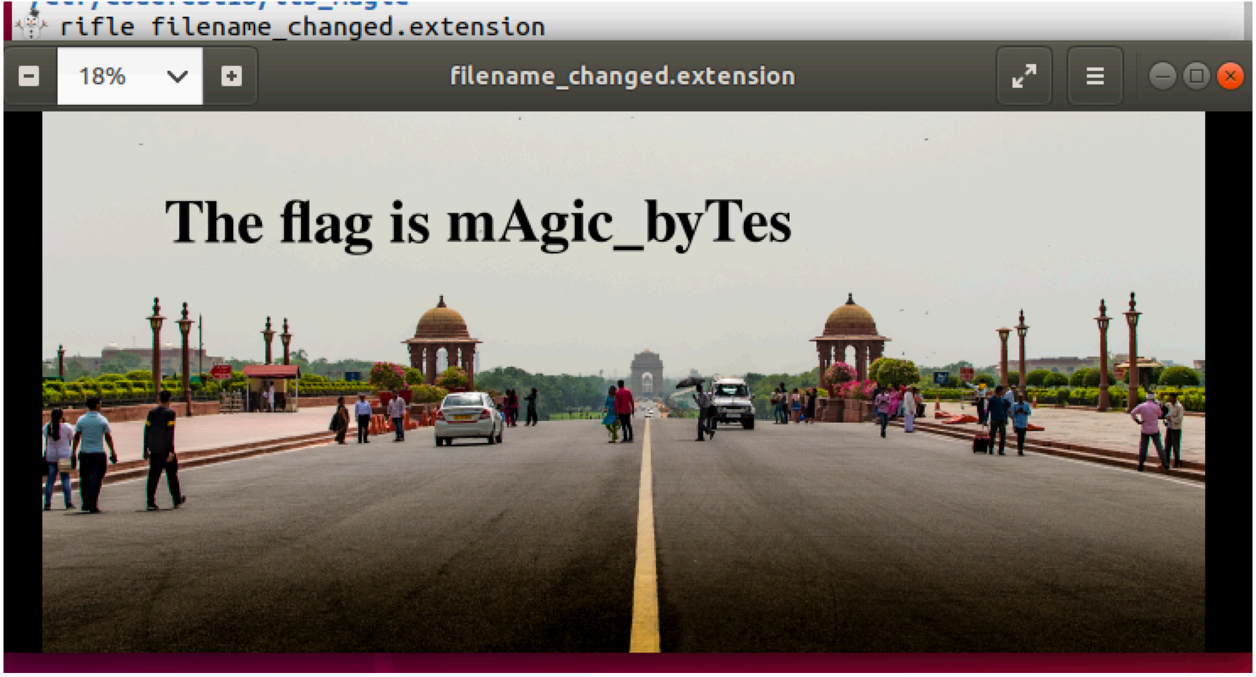
```
00000000FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 F0 00 ......JFIF.......
00000011F0 00 00 FF FE 00 18 41 75 74 68 6F 72 3A 20 55 74 .......Author: Ut
0000002273 61 76 20 4B 72 69 73 68 6E 61 6E FF E2 02 40 49 sav Krishnan...@I
```

The file is saved as **filename_changed.extension** and I examine it again using the **file** command:



```
file filename_changed.extension
filename_changed.extension: JPEG image data, JFIF standard 1.01, resolution (DPI
), density 240x240, segment length 16, comment: "Author: Utsav Krishnan", progre
ssive, precision 8, 3823x1778, frames 3
```

Opening the file using the **rifle** tool, the flag is obtained:



```
rifle filename_changed.extension
```

Flag:
CodefestCTF{mAgic_byTes}