Is it really just a picture?

Problem: Sometimes a file is used to hide other files. Is there anything in this image?
Hint: Try comparing it to the original
Given: Spurs.jpg

Notes: You can easily search for the original image with google's search by image feature. This is not necessary to solve this problem, but is useful.

Steps:

1) Download the above picture Spurs.jpg from the CTF site.

2) Go to https://images.google.com/, click the small camera icon to "Search by image". Upload the picture and then search the original image.
If compared to the original it is easy to see that the given image is larger than the original image. 294.9kB for the given and 281.6kB for the original. Something has been added to this file.

3) There are several forensics tools that can be used to search for hidden files. For example, use a HEX editor (such as Bless) to open the picture. Because it is a JPG file, you can see the file starts with FFD8. The JPG file should end with FFD9. So, search FFD9 in the file. you will find FFD9 somewhere in the middle of the file, but not at the end. Below is what we can see in Bless. Obviously, after FFD9, we see "%PDF-1.4" that is the starting characters in a PDF file. We can conclude that a PDF file is appended to the end of a JPG file. This is a very common way to piggyback a file to another file.

```
00044bf8 15 A3 F6 2C 74 74 27 AF 02 BD DB 83 90 88 12 78 C7 47 ...,tt'........x.G
00044c0a 47 47 73 23 FF D9 25 50 44 46 2D 31 2E 34 0A 25 C3 A4 GGs#..%PDF-1.4.%..
00044c1c C3 BC C3 B6 C3 9F 0A 32 20 30 20 6F 62 6A 0A 3C 3C 2F .......2 0 obj.<</
```

4) Now, we need a tool to extract the PDF file. Foremost File Carver will work.
Note: “Foremost is a console program to recover files based on their headers, footers, and internal data structures. This process is commonly referred to as data carving. Foremost can work on image files, such as those generated by dd, Safeback, Encase, etc, or directly on a drive. The headers and footers can be specified by a configuration file or you can use command line switches to specify built-in file types. These built-in types look at the data structures of a given file format allowing for a more reliable and faster recovery.”
http://foremost.sourceforge.net/

From the command line inside of the directory of the picture, enter foremost -v -i Spurs.jpg

```
[qijun@glap forensics]$ foremost -v -i Spurs.jpg
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Tue Mar 21 09:04:07 2017
Invocation: foremost -v -i Spurs.jpg
Output directory: /home/qijun/teaching/ctf/txctf-writeups/forensics/output
Configuration file: /etc/foremost.conf
Processing: Spurs.jpg
|------------------------------------------------------------------
File: Spurs.jpg
Start: Tue Mar 21 09:04:07 2017
Length: 287 KB (294866 bytes)

Num      Name (bs=512)         Size      File Offset     Comment

0:      00000550.pdf          12 KB          281616
*|
Finish: Tue Mar 21 09:04:07 2017

1 FILES EXTRACTED

pdf:= 1
------------------------------------------------------------------

Foremost finished at Tue Mar 21 09:04:07 2017
[qijun@glap forensics]$
```

5) The hidden pdf will be placed in a directory labeled ‘output’ by default. Inside will be pdf. Open the pdf file and we see something lyrics but not a flag.

now this is a story all about how
my life got Flipped-turned upside down
and I'd Like to take a minute
just sit right there
i'll tell you how i became the prince of a town called bel-air

6) Notice that some lines have capital letters.