[LinkedIn]

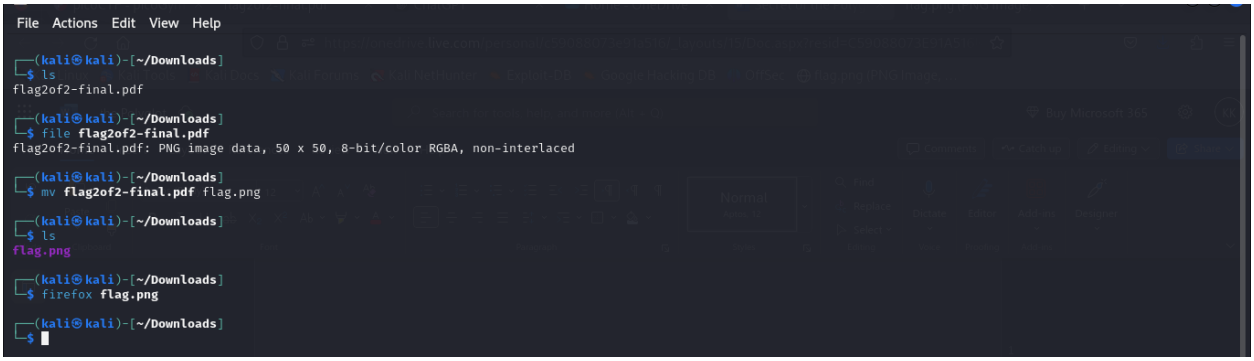
Description

The Network Operations Center (NOC) of your local institution picked up a suspicious file, they're getting conflicting information on what type of file it is. They've brought you in as an external expert to examine the file. Can you extract all the information from this strange file? Download the suspicious file here.

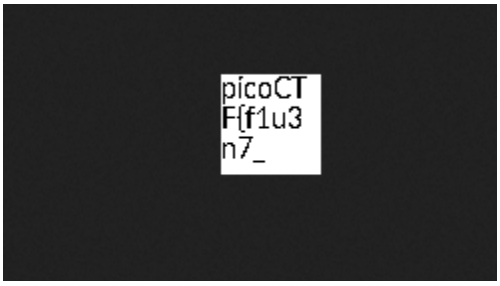
Hint: *This problem can be solved by just opening the file in different ways*

Solution

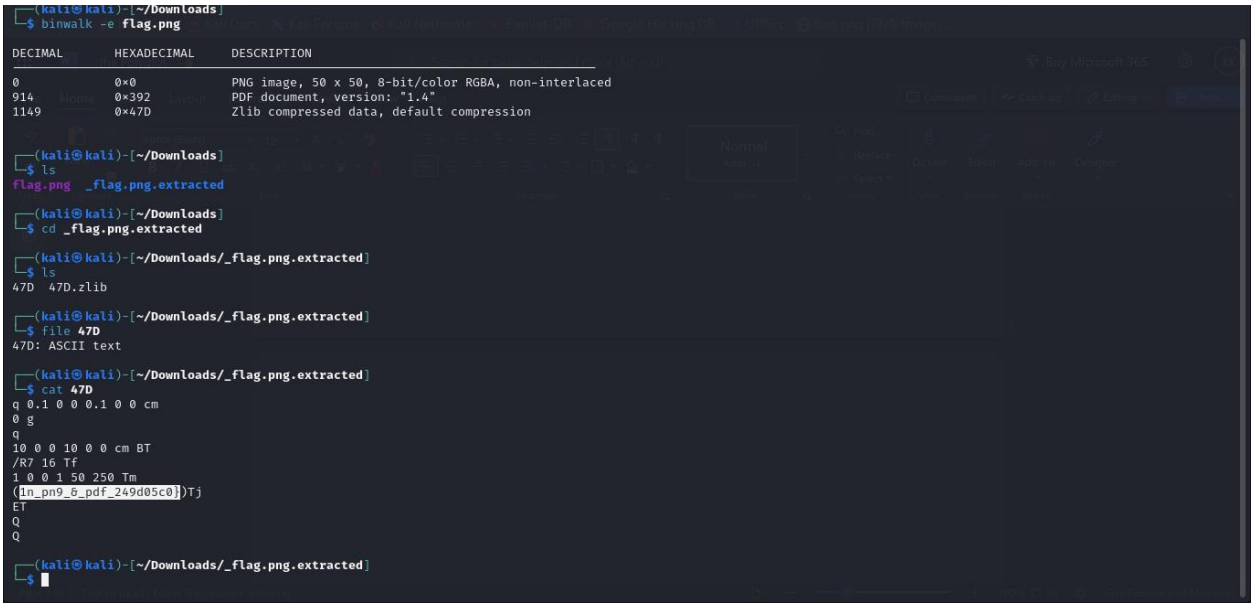
I started by downloading the suspicious file, which had a .pdf extension. Upon closer inspection using the **file** command, I found that it wasn't actually a PDF but a PNG image. I renamed the file to flag.png to reflect its true format and opened it in Firefox.



Inside the image, I found part of the flag: picoCTF{f1u3n7_



Next, I used binwalk to analyze the file further. The tool revealed that the PNG image contained embedded data, including a Zlib compressed block. I extracted the files, which placed a file named 47D.zlib in a folder called _flag.png.extracted. Inside the 47D file, I found ASCII text that appeared to be a continuation of the flag.



After combining this with the partial flag from the image, I recovered the full flag:

picoCTF{f1u3n7_1n_pn9_&_pdf_249d05c0}