

## File types

### Forensics

## Description

This file was found among some files marked confidential but my pdf reader cannot read it, maybe yours can.

You can download the file from [here](#).

Hints:

- 1) Remember that some file types can contain and nest other files.

**Solution:**

- 1) The hint makes me think that the flag is nested in the file we just downloaded.

```

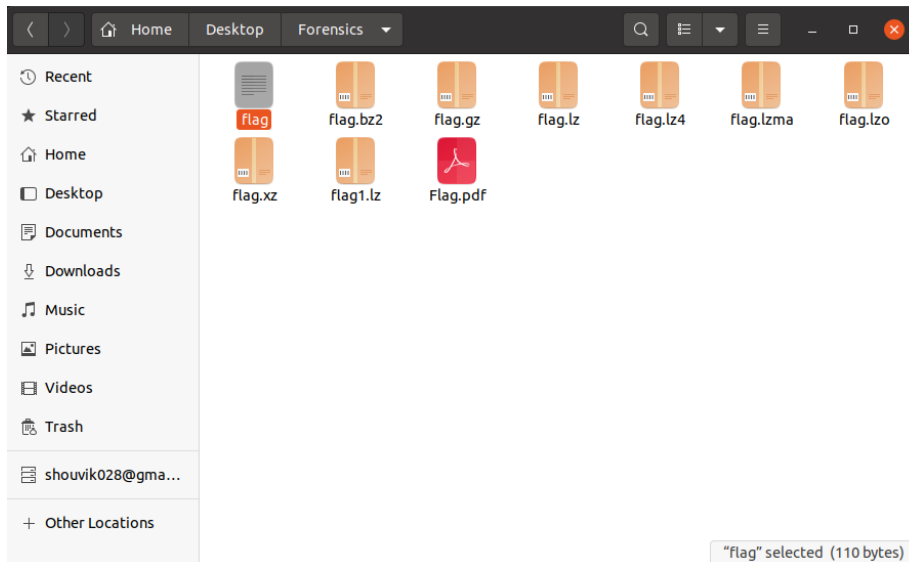
x86_64-v8-linux-ANVIS-SE - Desktop/Forensics
# x86_64-v8-linux-ANVIS-SE - Desktop/Forensics sudo apt install clip
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  clip
0 upgraded, 1 newly installed, 0 to remove and 235 not upgraded.
Need to get 73.3 kB of archives.
After this operation, 167 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 clip amd64 1:11-7 [73.3 kB]
Fetched 73.3 kB in 1s (60.1 kB/s)
Selecting previously unselected package clip.
(Reading database ... 191386 files and directories currently installed.)
Preparing to unpack .../clip:1:11-7_amd64.deb ...
Unpacking clip (1:11-7) ...
Setting up clip (1:11-7) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for install-info (6.7.0-3.dfsg.3) ...
# x86_64-v8-linux-ANVIS-SE - Desktop/Forensics lftp flag:z
lftp: Input file flag:z already has 'z' suffix.
x86_64-v8-linux-ANVIS-SE - Desktop/Forensics file flag
Flag: LZMA compressed data, non-streamed, slice 256
# x86_64-v8-linux-ANVIS-SE - Desktop/Forensics file flag:z
Flag: LZMA compressed data - version 1.040, LZMA1-1, os: Unix
# x86_64-v8-linux-ANVIS-SE - Desktop/Forensics file flag
Flag: LZMA compressed data - version 1.040, LZMA1-1, os: Unix
# x86_64-v8-linux-ANVIS-SE - Desktop/Forensics lftp
Command 'lftp' not found, but can be installed with:

sudo apt install lftp

x86_64-v8-linux-ANVIS-SE - Desktop/Forensics sudo apt install lftp
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  lftp
0 upgraded, 1 newly installed, 0 to remove and 235 not upgraded.
Need to get 82.8 kB of archives.
After this operation, 166 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 lftp amd64 1:04-1 [82.8 kB]
Fetched 82.8 kB in 1s (59.7 kB/s)
Selecting previously unselected package lftp.
(Reading database ... 191317 files and directories currently installed.)
Preparing to unpack .../lftp:1:04-1_amd64.deb ...
Unpacking lftp (1:04-1) ...
Setting up lftp (1:04-1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for lftp (1:04-1) ...
lftp: unknown suffix 'z' ignored
# x86_64-v8-linux-ANVIS-SE - Desktop/Forensics lftp flag:z
lftp: Input file flag:z already has 'z' suffix.
x86_64-v8-linux-ANVIS-SE - Desktop/Forensics file flag
Flag: LZMA compressed data, version 1
# x86_64-v8-linux-ANVIS-SE - Desktop/Forensics lftp

```

- 2) The given pdf is actually a shell script so change the extension to .sh
- 3) We will see that the files extracted after each step are to be renamed in order to open the contents inside.
- 4) We do this until we get a plain text file containing what looks to be hex characters.



5) We convert it to ascii to get the flag.

HOME / CONVERSION / NUMBER CONVERSION / HEX CODE TO ASCII TEXT

### Hex to ASCII Text String Converter

Enter hex bytes with any prefix / postfix / delimiter and press the *Convert* button  
(e.g. 45 78 61 6d 70 6c 65 21):

From:  To:

Paste hex numbers or drop file

```
7069636f4354467b66316c656e406d335f6d406e3170756c407431306
e5f
6630725f3062326375723137795f39353063346665657d0a
```

Character encoding:

```
picoCTF{f1len@m3_m@n1pul@t10n_f0r_0b2cur17y_950c4fee}
```

Flag: picoCTF{f1len@m3\_m@n1pul@t10n\_f0r\_0b2cur17y\_950c4fee}