

FORENSIC – Tux!


Soal

EASY

LIVE

Tux!


Jul 22nd 20 20 points 384 Solves Forensics Easy

kcbowhunter 

Community Rating: 4.66 / 5

The flag is hidden inside the Penguin! Solve this challenge before solving my 100 point Scope challenge which uses similar techniques as this one.

Tux.jpg



Flag


CTFlearn{...}


SUBMIT

First 10 Solvers

RANK	USERNAME	RANK	USERNAME
1	Fixed	6	ApToX
2	ebouteillon	7	evrest
3	lenoci	8	Ntoskrnl
4	xvenom	9	coox
5	yupwn	10	DaBaddest

Comment (Supports Markdown)

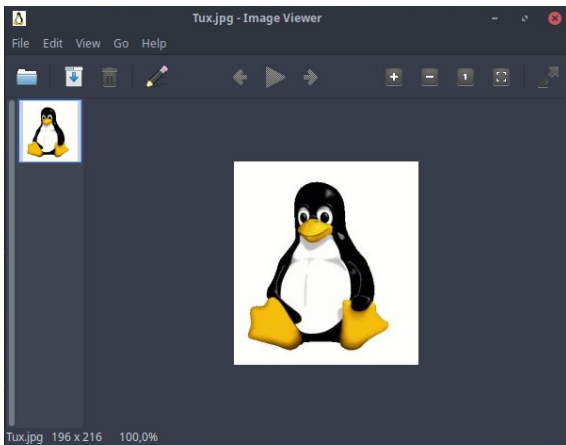


Protect this comment ☐ 

COMMENT

Penjelasan

Dari soal diberikan sebuah file gambar Tux.jpg



Pada soal terdapat clue bahwa “*The flag is hidden inside the Penguin*”

Langkahnya:

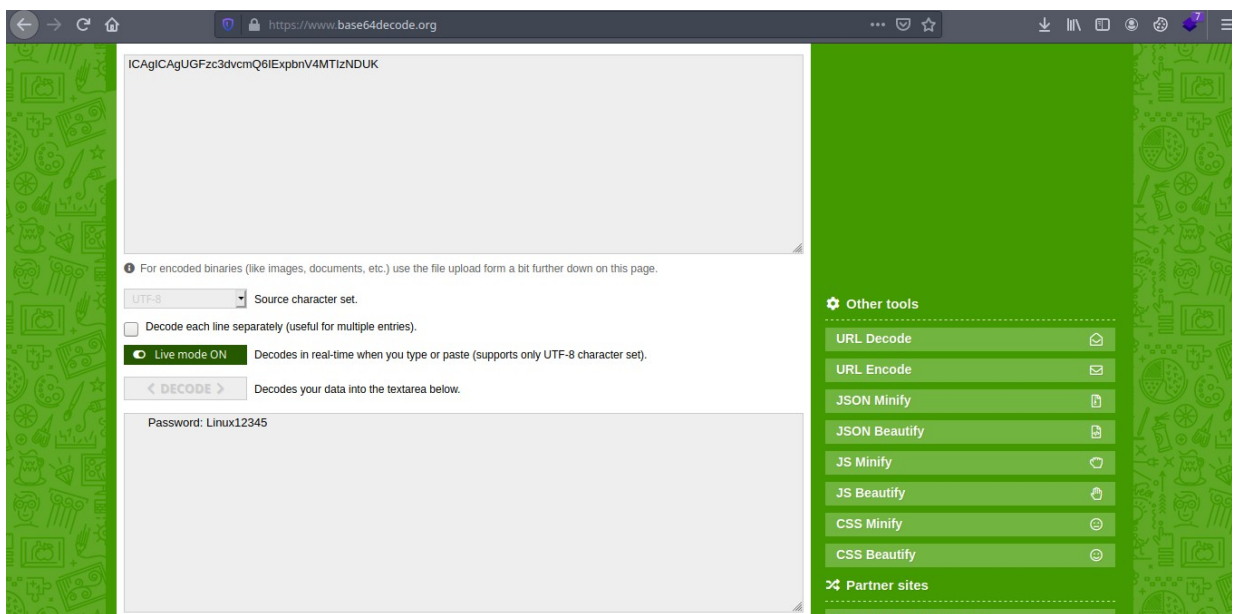
1. Gunakan exiftool terlebih dahulu untuk menganalisis file gambar tersebut

```
fariq@x441n ~/Downloads/ctf/CTFLEARN/forensic/Tux$ exiftool Tux.jpg
ExifTool Version Number      : 10.80
File Name                    : Tux.jpg
Directory                   : .
File Size                    : 5.6 kB
File Modification Date/Time  : 2020:09:27 11:38:08+07:00
File Access Date/Time       : 2020:09:27 11:38:31+07:00
File Inode Change Date/Time  : 2020:09:27 11:38:19+07:00
File Permissions             : rw-rw-r--
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
JFIF Version                : 1.01
Resolution Unit             : None
X Resolution                : 1
Y Resolution                : 1
Comment                     : ICAgICAgUGFzc3dvcnQ6IExpbnV4MTIzNDUK.
Image Width                 : 190
Image Height                : 216
Encoding Process            : Baseline DCT, Huffman coding
Bits Per Sample             : 8
Color Components            : 3
Y Cb Cr Sub Sampling       : YCbCr4:2:0 (2 2)
Image Size                  : 196x216
Megapixels                  : 0.042
fariq@x441n ~/Downloads/ctf/CTFLEARN/forensic/Tux$
```

Pada comment terdapat karakter aneh, yang di curigai sebuah encode base64,

*untuk exiftool bisa di download pada website <https://exiftool.org/>

2. Setelah itu kita coba decode karakter tersebut pada webiste <https://www.base64decode.org/>



Setelah di decode ternyata didapat sebuah password **Linux12345**

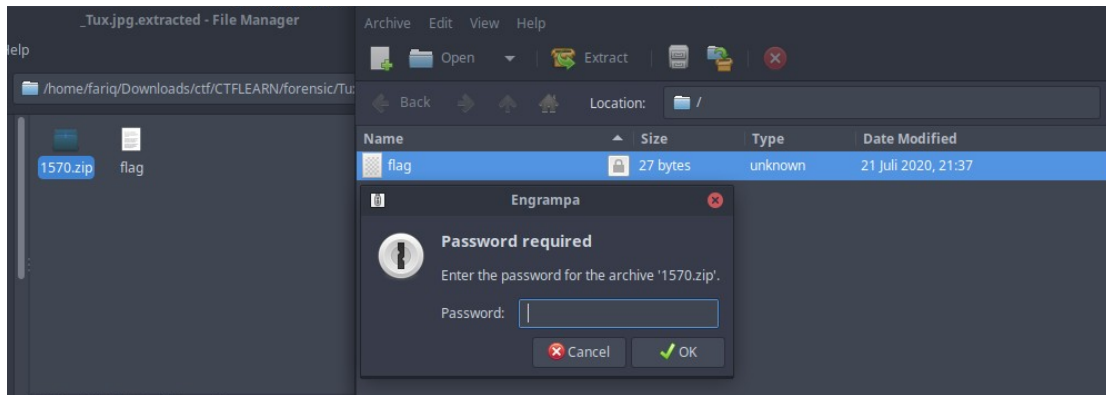
3. Karena clue menyatakan flag ada di dalam penguin, dengan kata lain file yang berisi flag disembunyikan di dalam file gambar penguin.

Kita pastikan kebenarannya dengan tools **binwalk** untuk mengekstrak file tersembunyi tersebut.

```
fariq@x441n ~/Downloads/ctf/CTFLEARN/forensic/Tux binwalk -e Tux.jpg
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01
5488	0x1570	Zip archive data, encrypted at least v1.0 to extract, compressed size: 39, uncompressed size: 27, name: flag
5679	0x162F	End of Zip archive

4. Ternyata ada 2 file tersembunyi didalam file gambar penguin tersebut



File flag saat dibuka ternyata tidak ada isinya, sedangkan file **1570.zip** saat diekstrak ada file **flag** lagi tetapi membutuhkan password untuk proses ekstraknya. Sebelumnya kita sudah mendapatkan password **Linux12345**

Flag ditemukan pada saat file flag sudah di ekstrak



Flag: CTFlearn{Linux_Is_Awesome}