

Challenge Name : Stegnanba

Category: Steganography

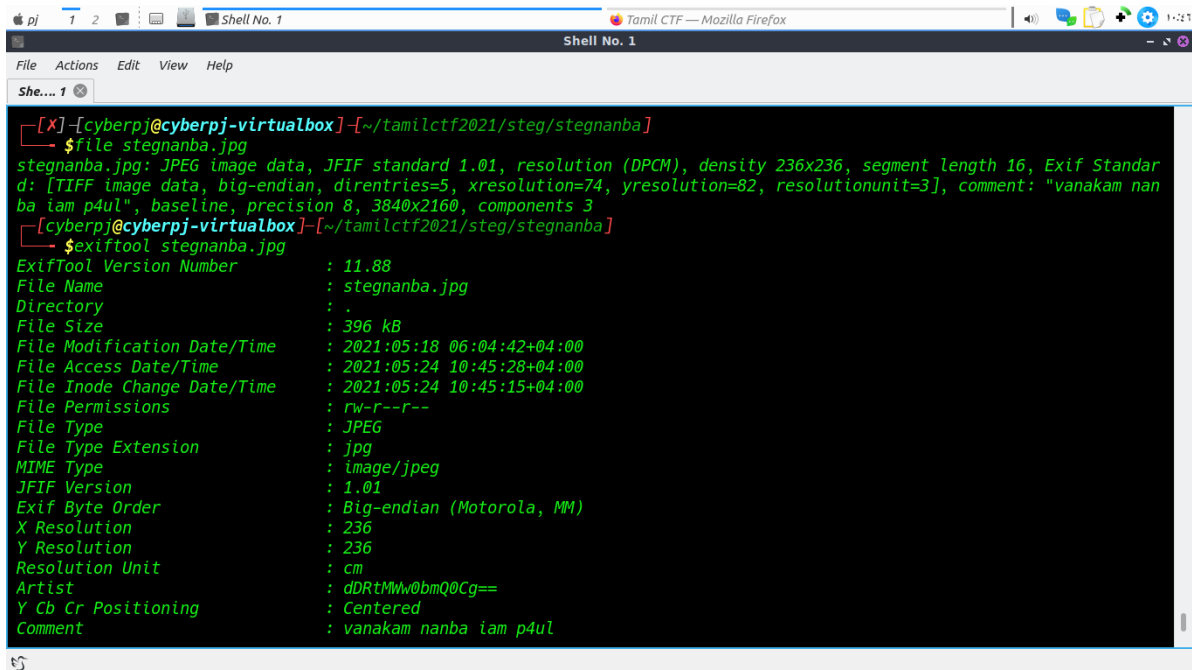
level : Easy

Author: Paul

solution :

1. The Given file is with the extension of ".jpg".
2. file says JPEG YES !
3. exif tool or string the image

```
(p4ul@none) - [~/ctf/tamil-ctf]
$ exiftool stegnanba.jpg
```



```
[X]-[cyberpj@cyberpj-virtualbox] - [~/tamilctf2021/steg/stegnanba]
$ file stegnanba.jpg
stegnanba.jpg: JPEG image data, JFIF standard 1.01, resolution (DPCM), density 236x236, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=5, xresolution=74, yresolution=82, resolutionunit=3], comment: "vanakam nanba iam p4ul", baseline, precision 8, 3840x2160, components 3
[cyberpj@cyberpj-virtualbox] - [~/tamilctf2021/steg/stegnanba]
$ exiftool stegnanba.jpg
ExifTool Version Number      : 11.88
File Name                    : stegnanba.jpg
Directory                   : .
File Size                    : 396 kB
File Modification Date/Time  : 2021:05:18 06:04:42+04:00
File Access Date/Time       : 2021:05:24 10:45:28+04:00
File Inode Change Date/Time  : 2021:05:24 10:45:15+04:00
File Permissions             : rw-r--r--
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
JFIF Version                : 1.01
Exif Byte Order             : Big-endian (Motorola, MM)
X Resolution                 : 236
Y Resolution                 : 236
Resolution Unit             : cm
Artist                      : dDRtMWw0bmQ0Cg==
Y Cb Cr Positioning         : Centered
Comment                     : vanakam nanba iam p4ul
```

- You can Get some comments and lots of information
- Artist data looks weird
- **nothing but base64 :**

- artist : dDRtMWw0bmQ0Cg==

```
(p4ul@none) - [~/ctf/tamil-ctf]
$ echo "dDRtMWw0bmQ0Cg==" | base64 -d
output: t4m1l4nd4
```

! ok it contain something called t4m1l4nd4

- The challenge name is stegnanba
- :) **Steghide** is the hero here , not ~~vanakam nanba~~!

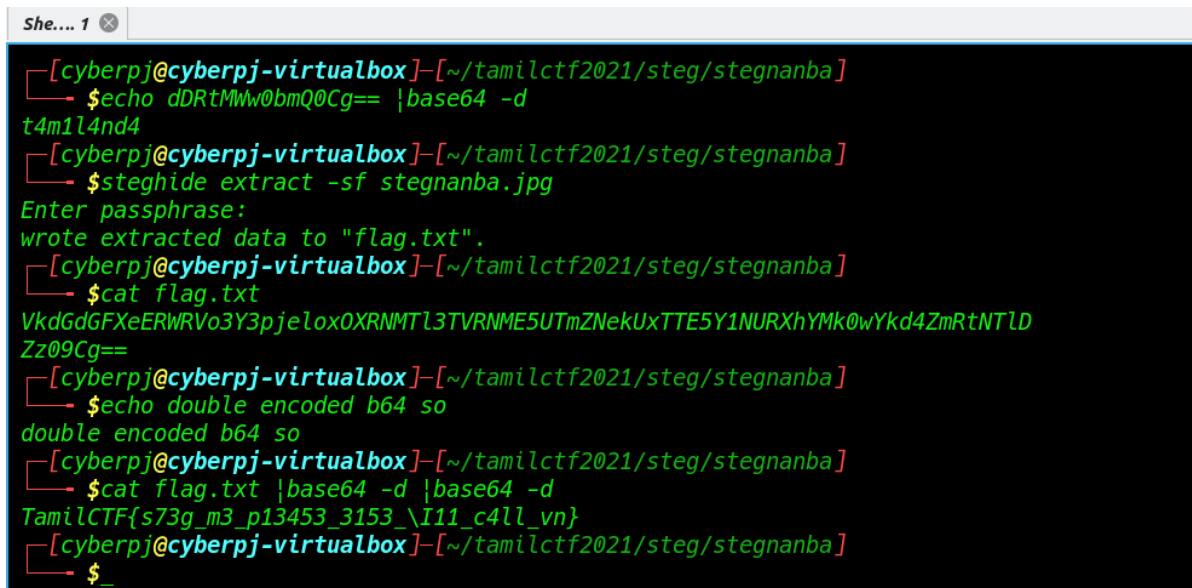
Steghide used to extract information or embed and lot can do with it

```
(p4ul@none) - [~/ctf/tamil-ctf]
└─$ steghide extract -sf stegnanba.jpg
press enter
Enter that password (enter the password : t4m1l4nd4)

wrote extracted data to flag.txt
```

1. flag.txt contain double encoded base64

```
(p4ul@none) - [~/ctf/tamil-ctf]
└─$ cat flag.txt |base64 -d |base64 -d
output: TamilCTF{s73g_m3_p13453_3153_\I11_c4ll_vn}
```



```
She... 1 x
[cyberpj@cyberpj-virtualbox] - [~/tamilctf2021/steg/stegnanba]
└─$ echo dDRtMww@bmQ0Cg== |base64 -d
t4m1l4nd4
[cyberpj@cyberpj-virtualbox] - [~/tamilctf2021/steg/stegnanba]
└─$ steghide extract -sf stegnanba.jpg
Enter passphrase:
wrote extracted data to "flag.txt".
[cyberpj@cyberpj-virtualbox] - [~/tamilctf2021/steg/stegnanba]
└─$ cat flag.txt
VkdGdGFxeERWRVo3Y3pjeloX0XRNMTl3TVRNME5UTmZNekUxTTE5Y1NURXhYMk0wYkd4ZmRtNTlD
Zz09Cg==
[cyberpj@cyberpj-virtualbox] - [~/tamilctf2021/steg/stegnanba]
└─$ echo double encoded b64 so
double encoded b64 so
[cyberpj@cyberpj-virtualbox] - [~/tamilctf2021/steg/stegnanba]
└─$ cat flag.txt |base64 -d |base64 -d
TamilCTF{s73g_m3_p13453_3153_\I11_c4ll_vn}
[cyberpj@cyberpj-virtualbox] - [~/tamilctf2021/steg/stegnanba]
└─$ _
```

THATS ALL NANBA

THANK YOU

BY TAMILCTF2021 TEAM