

Challenge Name: Guatemala

Dev: Aman Narnaware

Category: Steganography

Level: Easy

Flag format: vishwaCTF{}

Description:

My friend wanted to install antivirus for his computer,
but the creator of antivirus was caught!

Attached Files:



Writeup:

- 1) Download the attached file.
- 2) The description talks about some antivirus and its creator. [John McAfee](#).
- 3) The description says how he was caught. If we google about it, we can find out that his [EXIF](#) data of an image leaked his location.
- 4) We can use [exiftool](#) to search the image.
- 5) We can find a base64 string in the comment tag of the metadata.

```
(root@192)-[~/Desktop]
# exiftool Kazuma.gif
ExifTool Version Number      : 12.44
File Name                    : Kazuma.gif
Directory                   : .
File Size                   : 1112 kB
File Modification Date/Time  : 2023:02:03 06:48:48-05:00
File Access Date/Time       : 2023:02:03 07:16:32-05:00
File Inode Change Date/Time  : 2023:02:03 07:16:32-05:00
File Permissions             : -rw-r--rw-
File Type                   : GIF
File Type Extension         : gif
MIME Type                   : image/gif
GIF Version                 : 89a
Image Width                 : 498
Image Height                : 498
Has Color Map               : Yes
Color Resolution Depth      : 8
Bits Per Pixel              : 8
Background Color            : 0
Animation Iterations        : Infinite
Comment                     : dmlzaHdhQ1RGe3ByMDczYzdfdXJfM1gxRn0=
Frame Count                 : 17
Duration                    : 2.04 s
Image Size                  : 498x498
Megapixels                  : 0.248
```

- 6) Decode the following base64 string and you get the flag.

```
(root@192)-[~/Desktop]
# echo "dmlzaHdhQ1RGe3ByMDczYzdfdXJfM1gxRn0=" | base64 -d
vishwaCTF{pr073c7_ur_3X1F}
```

Flag:

vishwaCTF{pr073c7_ur_3X1F}