Pwnme

✍️ Author : Luhko

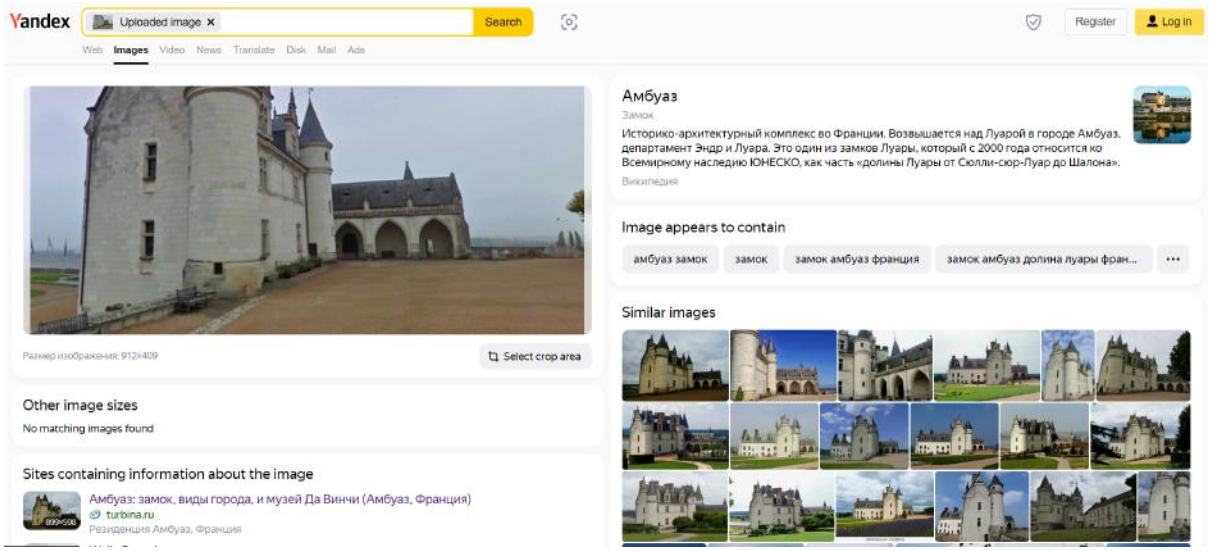
Geoint

Les vacances au chateau

We were given a castle image and we need to find its name. No data are inside the exif:

```
$ exiftool FirstPart.png
ExifTool Version Number         : 11.88
File Name                       : FirstPart.png
Directory                       : .
File Size                       : 688 kB
File Modification Date/Time     : 2022:07:01 22:44:37+02:00
File Access Date/Time           : 2022:07:01 23:26:07+02:00
File Inode Change Date/Time     : 2022:07:01 23:28:22+02:00
File Permissions                : rwxrwxrwx
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 912
Image Height                    : 409
Bit Depth                       : 8
Gamma                           : 2.2
Pixels Per Unit X               : 4724
Pixels Per Unit Y               : 4724
Pixel Units                     : meters
Image Size                      : 912x409
Megapixels                      : 0.373
```

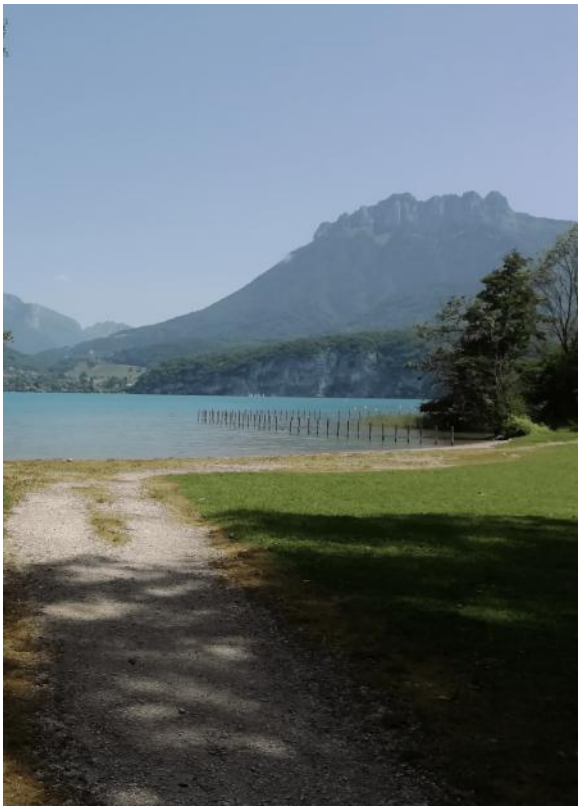
After submitting it to Yandex, we can find that the castle is named **Chateau d’Ambroise**:



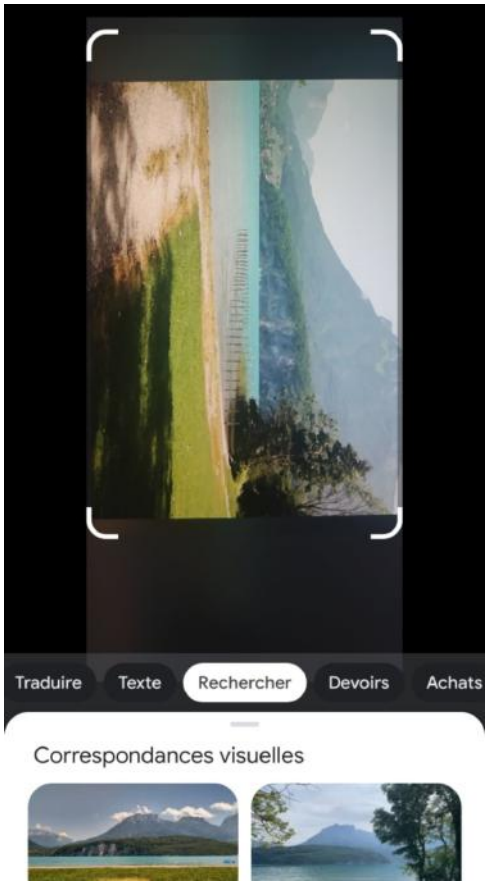
The flag is `PWNME{ambroise}`

Au bord de l’eau

We were given a second image where we need to find the name of the road:

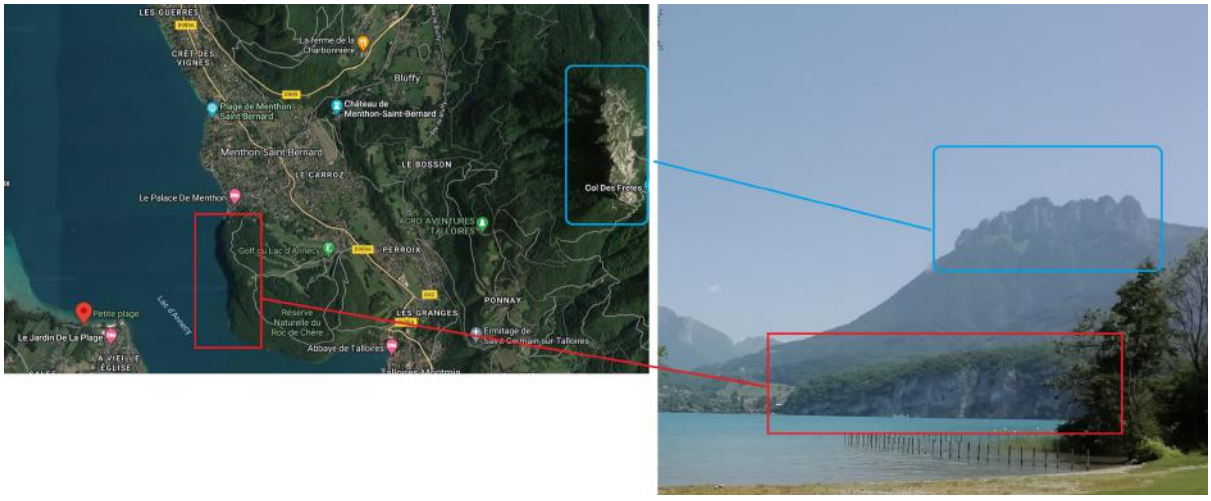


After submitting it to Google Lens, we can find a city named **Saint-Jorioz**.



The city is near a lake, and after some researches, we can see the mountain on the given picture.

Now that we have the town, we need to find the exact road. Looking at the angle of the photography, we can say easily determine a zone where the photo has been taken:



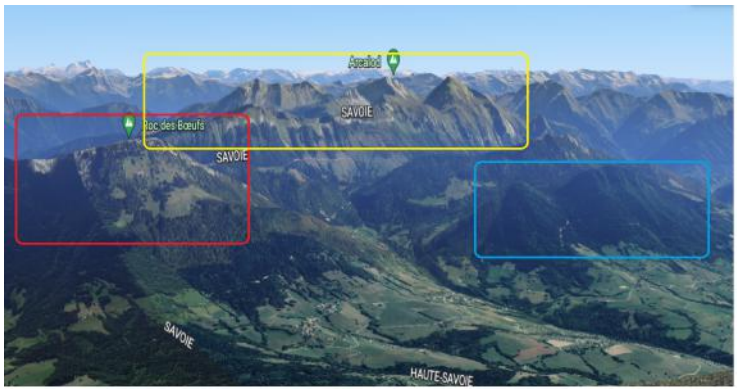
If we look on google maps, we can find “Le jardin de la plage”, with this picture:

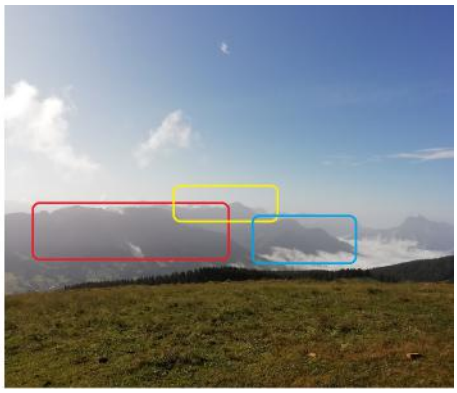
The road is **Digue à panade**.

Flag : `PWNME{digue_à_panade}`

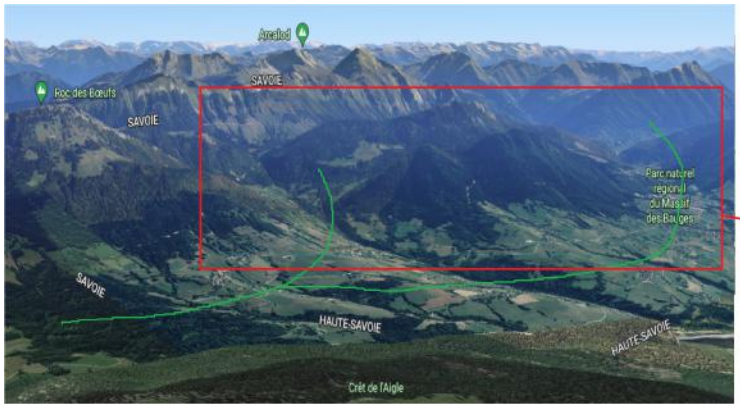
La tête dans les nuages :

We were given another image which has been taken on a mountain. We only know that the location is near the last one. I tried to identify the mountain pattern thanks to Google Earth (it wasn't easy!):





I also tried find the valley pattern, represented by the green line bellow:



Thanks to those informations, I found out a mountain named **Semnoz** which was the flag!

Flag : `PWNME{Semnoz}`

Forensics

It’s not just a cat story

We were given a file named `Acquisition.e01`

```
# file Acquisition.e01
Acquisition.e01: EWF/Expert Witness/EnCase image file format
```

After some reasearches on the web, we can find some tools that can be used for EWF files:

```
$ ewfinfo Acquisition.e01
ewfinfo 20140807

Acquiry information
        Case number:            2600
        Description:            We found this usb key during our search of the hacke
r's house
        Examiner name:          Monsieur Nouille
        Evidence number:        5200
        Acquisition date:       Tue Jun  7 14:11:48 2022
        System date:            Tue Jun  7 14:11:48 2022
        Password:               N/A

EWF information
        File format:            EnCase 1
        Sectors per chunk:      64
        Compression method:     deflate
        Compression level:      no compression
```

```
Media information
        Media type:             removable disk
        Is physical:            no
        Bytes per sector:       512
        Number of sectors:      81920
        Media size:             40 MiB (41943040 bytes)

Digest hash information
        MD5:                    f3e2d3ad77b3f580aca312b994319e04
```

Then we can try to mount it and gather some informations :

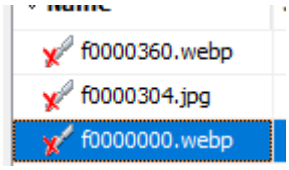
```
$ mkdir tmpmnt
$ ewfmount Acquisition.e01 tmpmnt
$ ls -l tmpmnt/
total 0
-r--r--r-- 1 root root 41943040 Jul  2 14:03 ewf1
$ file tmpmnt/ewf1
tmpmnt/ewf1: DOS/MBR boot sector

$ strings tmpmnt/ewf1
3,4@
b0VIM 8.2
...
/media/usb-drive/Pain.txt
U3210
#"!
Why
Why are we still here? Just suffer ?

$ binwalk tmpmnt/ewf1
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
2269184       0x22A000        JPEG image data, JFIF standard 1.01
2269214       0x22A01E        TIFF image data, little-endian offset of first image dir
ectory: 8
```

We can see that there might be an image. After extracting it, we get a cat image, which is not giving us the flag:

So I tried to open the original file, `Acquisition.e01`, with Autopsy. We can find 3 carved files:



After extracting those files, we have this image with the flag: