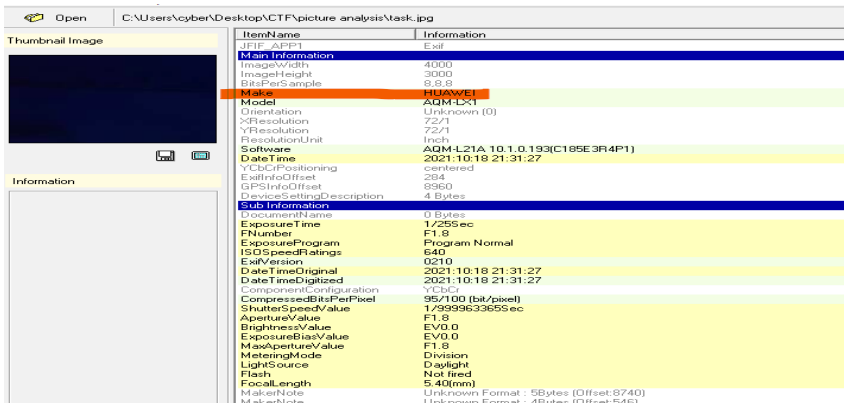
Picture Analysis Writeup
cybereagle2001
HackMaze V0.2

I – Picture Analysis 1:

Every file in the world and specially pictures have what we call it metadata.
Metadata which is a set of data that describes and gives information about other data. Can give us a lot of information about files and documents but also about the device and location used to create that file. In this Series players will analyse this Metadata and extract information about the file and the device , location of the person that took the picture.

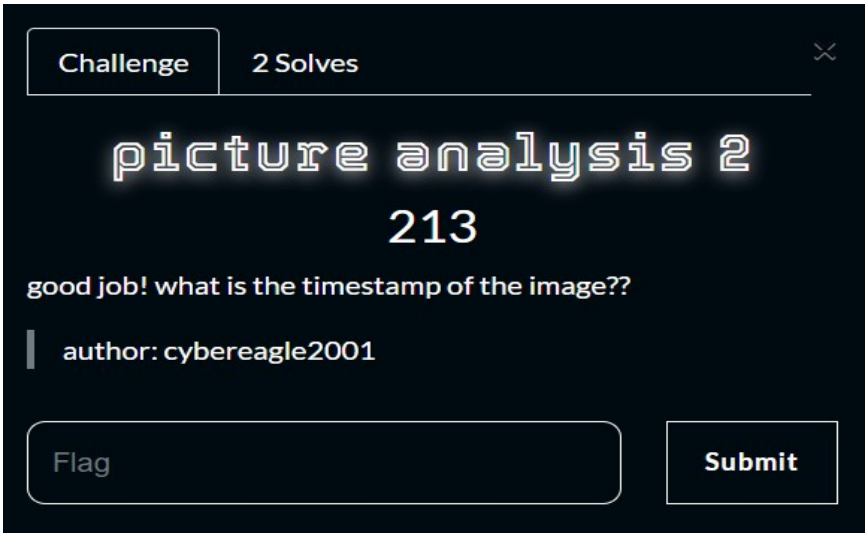
To do so we can use the exiftool pre-installed on kali linx, parrot OS and Sift OS but it will not give us a lot of detailed data. I used a tool called ExifRead.exe that will analyse the picture and extract more specific information.

After importing the task.jpg we can get this result :

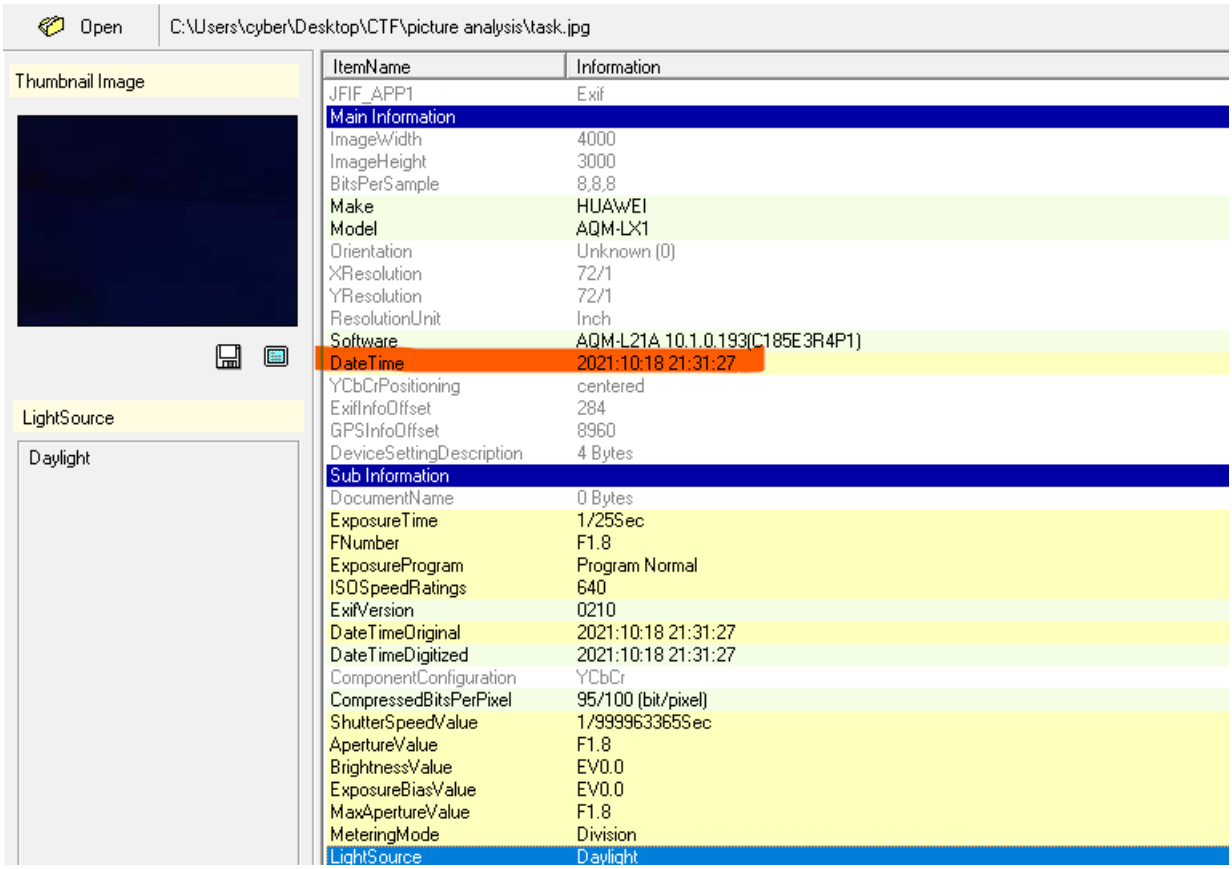


We can see that “Make : HUAWEI” this is the brand of our device.
The flag is : `ESFST{HUAWEI}`

II – Picture Analysis 2:



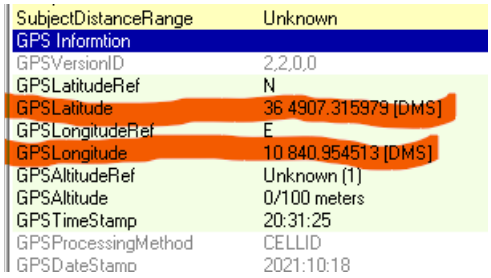
In the metdata we can find information about the time where the picture was created or taken that's what we call it a timestamp :



Our flag is : ESFST{2021:10:18 21:31:27}

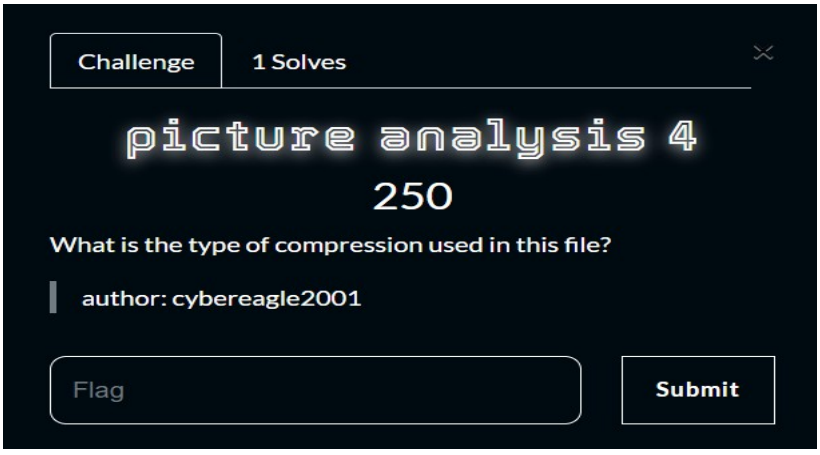
III – Picture Analysis 3 :

Let's try and locate our hacker lab. Actually the metadata of an image allowed FBI to arrest a drug dealer on the darkweb through the GPS location identified in a picture he took.

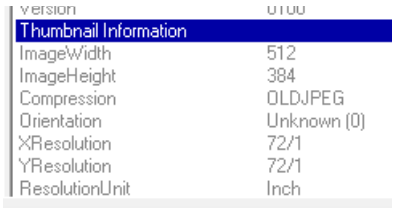


This is more than easy our flag is : ESFST{364907.315979,10840.954513}

IV – Picture Analysis 4 :



using the same tool we can get out flag :

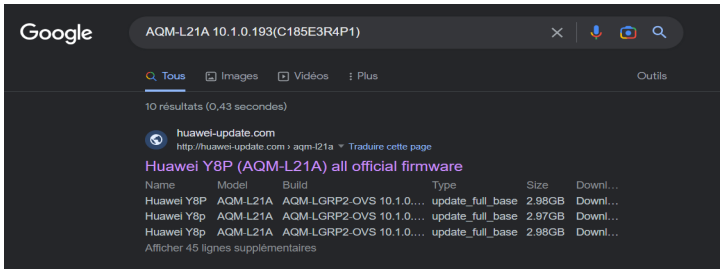


ESFST{OLDJPEG}

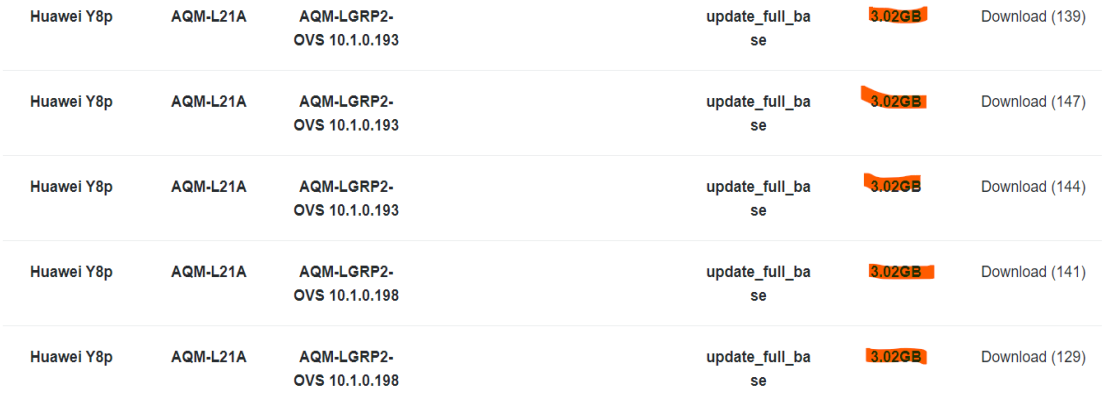
V – Picture Analysis 5:

Well forensics is not that easy we need to think beyond the data that we can collect from tools. How can we know how much storage an OS use on the device that the hacker used to create the picture.

We know that the hackers device is HUAWEI and the is AQM-LX1 the software version is AQM-L21A 10.1.0.193(C185E3R4P1) let's see what we can get from the internet ??



this is the website used to update the software of HUAWEI or to recover your phone if you have issues with the software we can see her all the data about all the versions of our Phone Model software :



Huawei Y8p	AQM-L21A	AQM-LGRP2-OVS 10.1.0.193	update_full_base	3.02GB	Download (139)
Huawei Y8p	AQM-L21A	AQM-LGRP2-OVS 10.1.0.193	update_full_base	3.02GB	Download (147)
Huawei Y8p	AQM-L21A	AQM-LGRP2-OVS 10.1.0.193	update_full_base	3.02GB	Download (144)
Huawei Y8p	AQM-L21A	AQM-LGRP2-OVS 10.1.0.198	update_full_base	3.02GB	Download (141)
Huawei Y8p	AQM-L21A	AQM-LGRP2-OVS 10.1.0.198	update_full_base	3.02GB	Download (129)

 All the versions of the software used in our hacker Phone Model use the same storage which is 3.02GB.

Our flag is : ESFST{3.02GB}