DIGITAL FORENSICS(IMAGE) - SMITH GRACE

IMAGE METADATA EXTRACTION

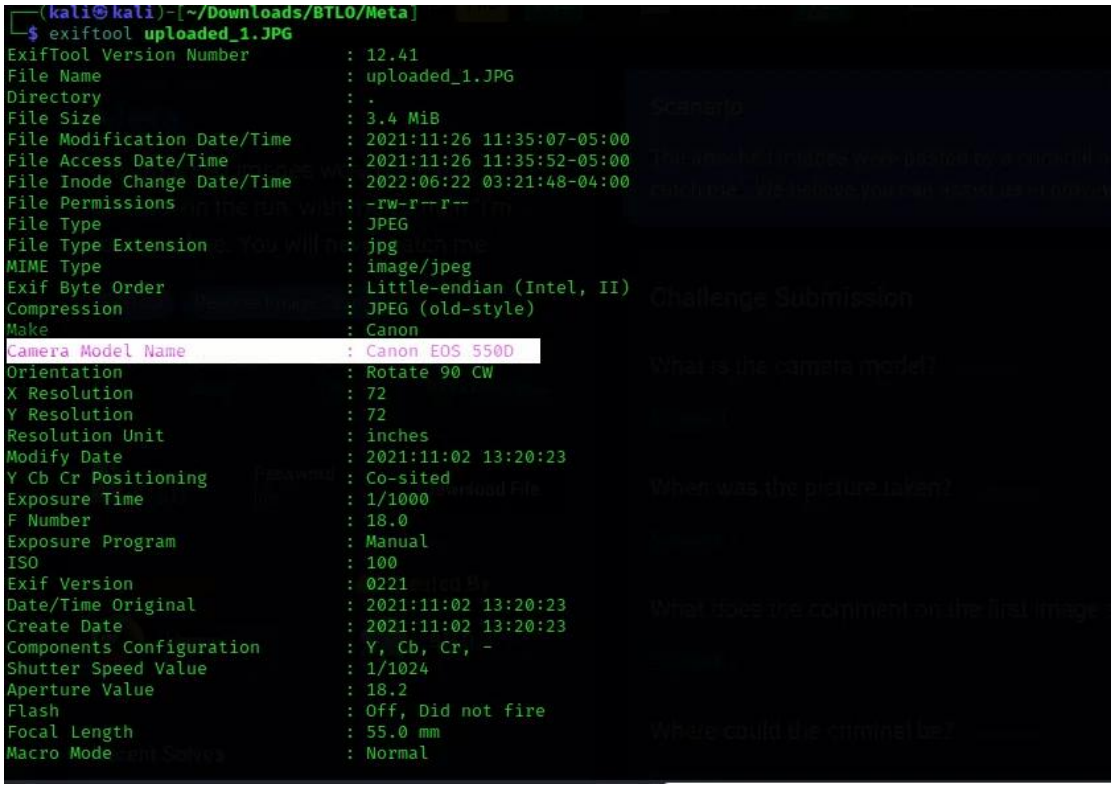
Scenario

The attached images were posted by a criminal on the run, with the caption “I’m roaming free. You will never catch me”. We believe you can assist us in proving him wrong. We download the given file and extract its contents and get into solving the challenges.

1. What is the camera model?

I used the exiftool for printing out this diagnostic information which showed me the metadata from an image.

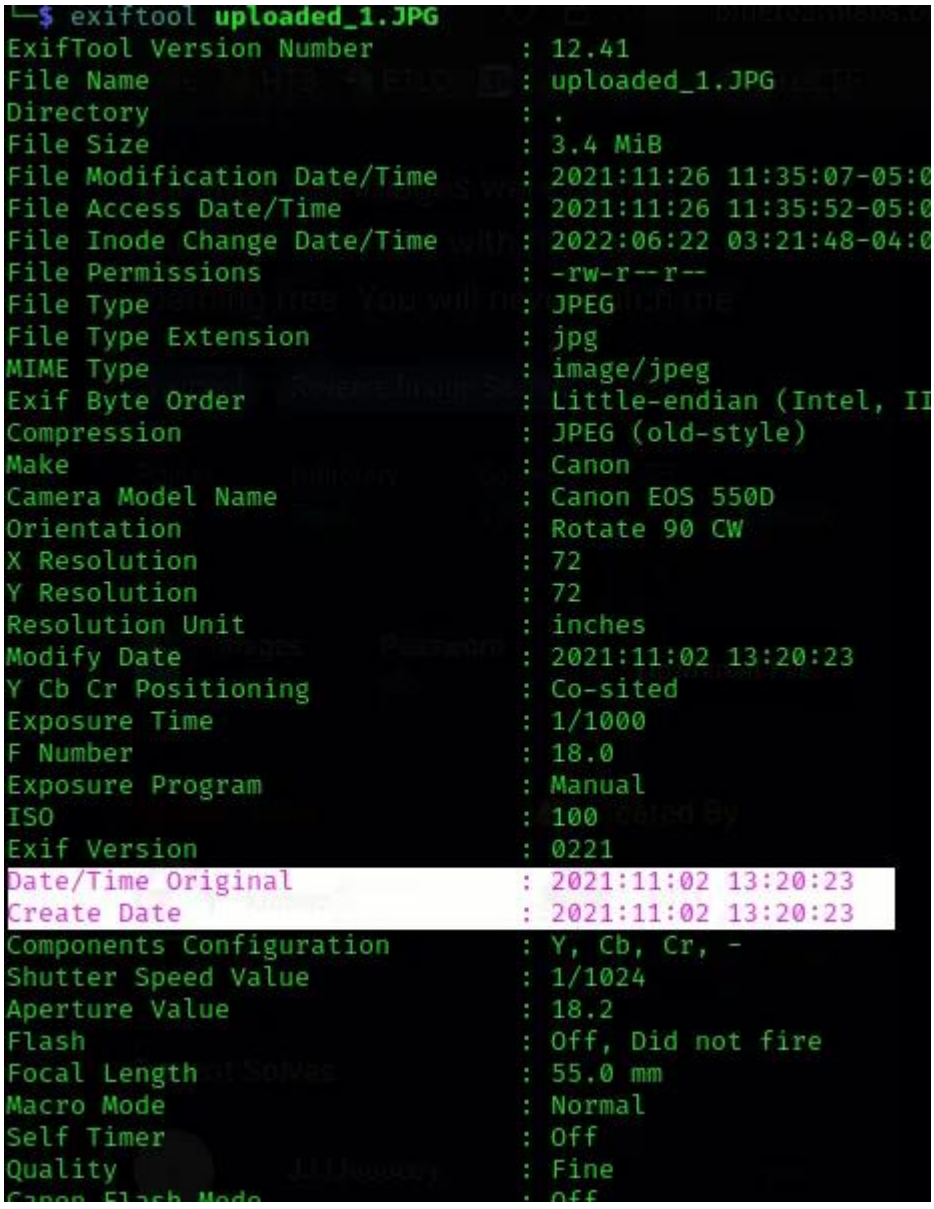
Answer : Canon EOS 550D



2. **When was the picture taken?**

Still on the metadata, I got the flag for this. I checked on the original date/time it was created.

Answer: *2021:11:02 13:20:23*



3. **What does the comment on the first image says?**

Still on the metadata of the first image scrolling down I got the comment section.

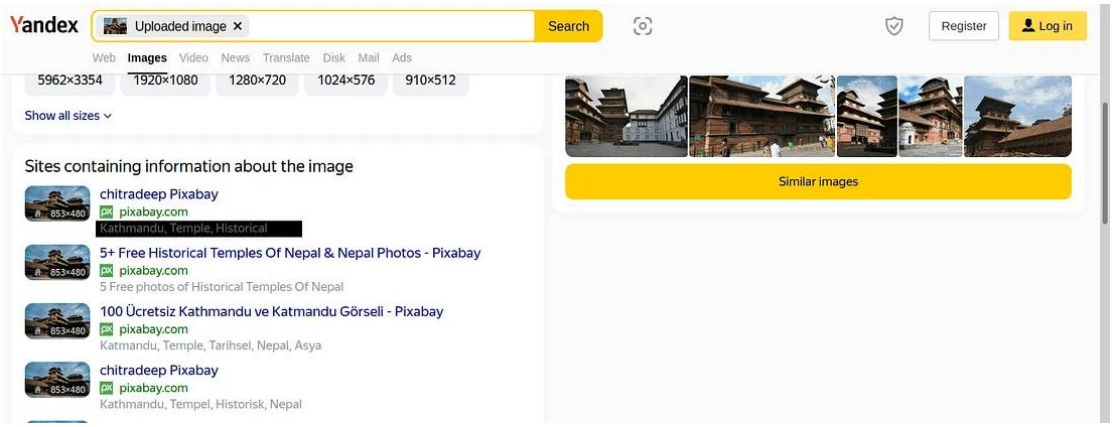
Answer: *relying on altered metadata to catch me?*

```
Focal Plane Resolution Unit     : inches
Custom Rendered                 : Normal
Exposure Mode                   : Manual
Scene Capture Type              : Standard
GPS Latitude Ref                : South
GPS Longitude Ref               : West
Thumbnail Offset                : 7902
Thumbnail Length                : 6101
Comment                         : relying on altered metadata to catch me?
Image Width                     : 5184
Image Height                    : 3456
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:2 (2 1)
Drive Mode                      : Single-frame Shooting
File Number                     : 102-3845
Lens                            : 55.0 - 250.0 mm
```

4. Where could the criminal be?

The finally challenge was doing a reverse image search on the images. I like using Yandex for my image search because it gives extensive and broad search as compared to other search engines. I used the first image but gave me various locations so I jumped onto the second image and it gave me the exact location of the criminal.

Answer: *Kathmandu*



Key Takeaways

1. Understanding the Power of Metadata

- I learned how metadata can contain personally identifiable information (PII).
- I realized how metadata supports attribution in investigations.

2. Awareness of Digital Privacy Risks

- Real-world images can leak sensitive data.
- OPSEC and privacy training are essential in both corporate and personal contexts.

3. Metadata as Forensic Evidence

- Metadata is non-visible but admissible evidence in investigations.
- Supports incident response timelines and insider threat assessments.

4. Hands-on Experience with a Real Forensics Tool

- Improved command-line proficiency.
- Developed automation skills for batch analysis.

5. Detection of Metadata Tampering

- I explored limitations and how attackers may cover tracks.
- Reinforced my need for layered analysis.

6. Use Cases Across Cybersecurity Domains

- Practical applications in threat hunting, phishing analysis, and ransomware investigation.
- Positioned metadata analysis as part of an IR or OSINT toolkit.