meta(forensics)

Created by	Ⓜ Manikandan N
Created time	@December 25, 2025 2:47 PM
Last edited by	Ⓜ Manikandan N
Last updated time	@December 25, 2025 2:48 PM
Category	blue team room what i learned and completed

🧪 Blue Team Labs – Image Forensics (Meta)

🔍 Post-Challenge Report (Learning, Struggles & Commands Used)

📌 Challenge Overview

The challenge involved analyzing **JPEG and PNG images** uploaded by a criminal claiming *"I'm roaming free. You will never catch me."*

The task was to use **digital forensics and OSINT techniques** to identify details such as camera model, timestamp, hidden comments, and finally infer **where the criminal could be**.

🛠️ Commands & Tools Used (VERY IMPORTANT)

🔷 1️⃣ Extracting the ZIP File

```
unzip cf7becafbbb525b3c1df03785a2b9ee6b96e41c.zip
```

Purpose:

- Extract images for analysis
- Always analyze **extracted files**, not ZIP contents

🔷 2️⃣ Navigating to the Correct Directory

```
cd Downloads
ls
```

Purpose:

- Ensure the image exists in the working directory
- Avoid file path errors

🔷 3️⃣ Opening the Image (Visual Inspection)

```
xdg-open uploaded_1.JPG
```

Purpose:

- Manually inspect image
- Look for visible clues (vehicles, environment, lighting, surroundings)

🔷 4️⃣ Extracting Metadata (Core DF Step)

```
exiftool uploaded_1.JPG
```

Findings:

- **Camera Model:** Canon EOS 550D
- **DateTimeOriginal:** 2021:11:02 13:20:23
- **Embedded Comment:** “relying on altered metadata to catch me?”

Purpose:

- Extract forensic metadata not visible in normal file properties

---

🔷 5️⃣ Checking GPS Metadata (Later Identified as Fake)

```
exiftool -gpsposition uploaded_1.JPG
```

and numeric format:

```
exiftool -n -gpslatitude -gpslongitude uploaded_1.JPG
```

Observation:

- GPS coordinates pointed to **Indian Ocean**
- This conflicted with real-world logic

Conclusion:

- GPS metadata was **intentionally altered**

🔷 6️⃣ Extracting Readable Strings

```
strings uploaded_1.JPG | less
```

Purpose:

- Search for hidden readable text
- Useful for comments, URLs, or flags

Observation:

- Produced large noisy output
- No city/location text found

Lesson:

- `strings` is **supporting**, not decisive, in image DF

🔷 7️⃣ Reverse Image Search (DECISIVE STEP)

Tool used:

- **Yandex Reverse Image Search**

Purpose:

- Identify real-world location using visual similarity
- Overcome misleading metadata

Result:

- Matching images identified as **Kathmandu, Nepal**
- Same tempo, street, and evening environment

✅ Final Answer Submitted

```
Kathmandu
```

✔️ Marked **Correct** by BTLO

🧠 What I Learned (Key Takeaways)

🔑 1. Exiftool Is a Forensic Tool, Not Just Properties

- Reveals camera, timestamps, comments, GPS
- Essential for image-based DF investigations

🔑 2. Metadata Can Be Manipulated

- GPS data is not always trustworthy
- Hidden comment explicitly hinted metadata tampering

> Never trust metadata blindly

🔑 3. Strings Has Limited Use in Image Forensics

- Useful for detecting comments or URLs
- Not useful for geographic identification in this case

🔑 4. OSINT Is Critical When Metadata Fails

- Reverse image search can outperform technical tools
- **Yandex** is especially effective for street scenes

🔑 5. Question Wording Matters

The question was:

> “Where could the criminal be?”

This allowed:

- Analytical reasoning
- Context-based inference
- Not literal metadata interpretation

⚠️ Struggles Faced (And Lessons)

❌ Initially Trusted GPS Metadata

- Converted coordinates
- Ended in Indian Ocean

✔️ Learned to question evidence validity

❌ Expected Tools to Give Direct Answers

- `strings` did not reveal city

✔️ Learned that **analysis > automation**

🧠 Golden Rule (Write This Down)

> When metadata lies, OSINT decides.

or

> Tools support the analyst — they don’t replace thinking.

🎯 Interview-Ready Explanation

> “In this image forensics challenge, EXIF metadata such as GPS was intentionally altered. After identifying this through a hidden comment, I used reverse image search and visual correlation to determine that the suspect could be in Kathmandu.”

📌 Reusable Checklist for Future Image DF Rooms

- ✅ unzip & extract files
- ✅ `exiftool` for camera, time, comments
- ⚠️ Verify GPS logic
- ❌ Don’t overuse `strings`
- 👀 Perform visual inspection
- 🌐 Use reverse image search (Yandex preferred)
- 🧠 Correlate evidence before concluding