Forensic Analysis Notes:

Case Information

Case: analyze sunset.jpg file

Analyst: Julius Niyonzima

Professor: Dr. Chris Lamb

Email: [jnbfg@umkc.edu](mailto:jnbfg@umkc.edu)

|  |  |  |  |
| --- | --- | --- | --- |
| Id | File name | Hash(None) | Notes |
| 1 | Sunset.jpg | Verified using file command | Suspected steganography |

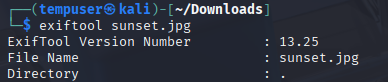
Tools and Environment

Kali Linux v2025.2

A screen shot of a computer code

AI-generated content may be incorrect.

Exiftool v13.25



Strings v2.44

A screen shot of a computer

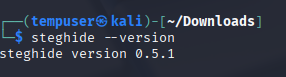
AI-generated content may be incorrect.

Binwalk v2.4.3

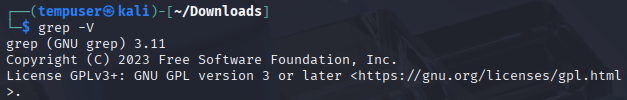
A computer screen with text

AI-generated content may be incorrect.

Steghid v0.5.1



Grep v3.11



File v5.46

A screen shot of a computer

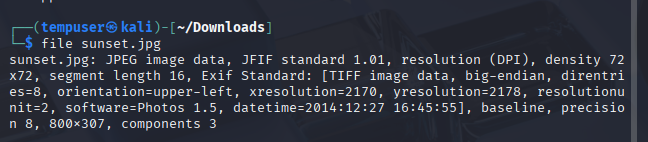
AI-generated content may be incorrect.

Analysis Steps :

Step1: Verified file type using the file command

Command: File sunset.jpg

Result: the file was confirmed to be a JPEG image

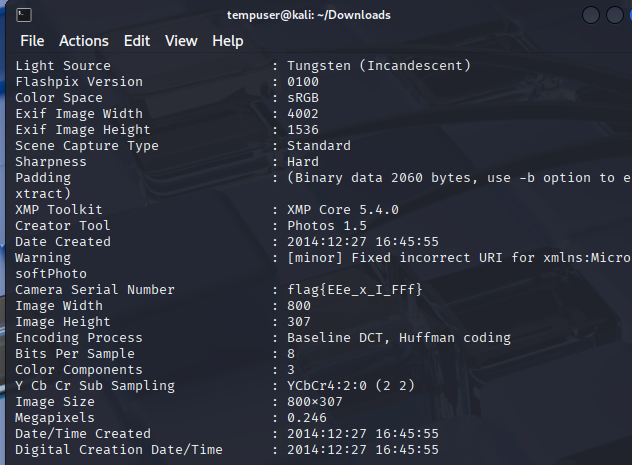


Status: Worked

Step2 : Check the metadata with exfitool

Command : exiftool sunset.jpg

Result: The file was confirmed to be taken with a standard camera, with standard camera info. Flag information was detected



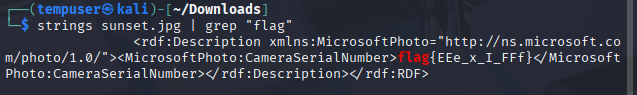
Status: Worked

Step3: Searched for readable string using strings with grep

Command : strings sunset.jpeg | grep “flag”

Result: Extracted all readable ASCII strings from binary-formatted JPEG.

The flag was found to be embedded in the XMP metadata



Status: Flag confirmed

Step4: Tested for embedded file using binwalk

Command : binwalk -e sunset.jpg

Result: failed to extract embedded data from the file

A screenshot of a computer

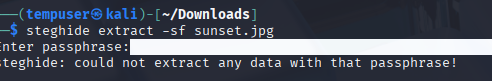
AI-generated content may be incorrect.

Status: Did not work

Step 4: Attempted Steganography extraction

Command: steghide extract -sf sunset.jpg

Result: No phrase was provided. I was not able to extract anything from the file

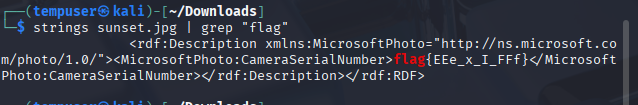


Status: Did not work

Findings:

After running various commands, I used the strings command with grep, and the flag was revealed.

Flag {EE\_xt\_FFr}



No other additional details were uncovered during the analysis

Conclusion.

The flag was successfully located with the help of the strings and grep commands. It is recommended to use hashing and steganography for file integrity and obfuscation.