1. Title page

- **Analyst**: Julius Niyonzima
- **Date**:09/09/2025
- **Case Name**: find the flag in the sunset.jpg files
- **Contact Information:** email: jnbfg@umkc.edu

2. Table of Content : page Number

1. **Case Summary:**

On September 9th, 2025, Julius downloaded a JPG file named **sunset.jpg:2025FS-COMP_SCI-436-0001** to locate a hidden flag in the format flag{secret_text}. He downloaded it to find detailed information contained in the hidden flag.

2. **Tools & Environment**

```
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
VERSION_ID="2025.3"
VERSION="2025.3"
VERSION_CODENAME=kali-rolling
ID=kali
ID_LIKE=debian
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
ANSI_COLOR="1;31"
```

Used Kali Linux 2025.5,

```
└─$ exiftool -ver
13.25
```

exiftool 13.25 , strings 2.45,grep, less

3. **EVIDENCE :**sunset.jpg: 2025FS-COMP_SCI-436-0001

On September 02 I obtained the sunset.jpg image from canvas as shown below. I downloaded it on kali

I ran 'exiftool sunset.jpg' to obtain the image metadata

```
└─$ exiftool sunset.jpg
ExifTool Version Number         : 13.25
File Name                       : sunset.jpg
Directory                       : .
File Size                       : 104 kB
File Modification Date/Time     : 2025:09:02 22:47:00-04:00
File Access Date/Time           : 2025:09:02 22:54:02-04:00
File Inode Change Date/Time     : 2025:09:02 22:47:00-04:00
File Permissions                : -rw-rw-r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Current IPTC Digest             : dbad0204d16a63027791298bc460859a
Coded Character Set             : UTF8
Application Record Version      : 2
Digital Creation Time           : 16:45:55
Digital Creation Date           : 2014:12:27
Time Created                    : 16:45:55
IPTC Digest                     : dbad0204d16a63027791298bc460859a
Exif Byte Order                 : Big-endian (Motorola, MM)
Orientation                     : Horizontal (normal)
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Software                        : Photos 1.5
Modify Date                     : 2014:12:27 16:45:55
Exif Version                    : 0221
Date/Time Original              : 2014:12:27 16:45:55
Create Date                     : 2014:12:27 16:45:55
Components Configuration        : Y, Cb, Cr, -
Light Source                    : Tungsten (Incandescent)
Flashpix Version                : 0100
Color Space                     : sRGB
Exif Image Width                : 4002
Exif Image Height               : 1536
Scene Capture Type              : Standard
Sharpness                       : Hard
Padding                         : (Binary data 2060 bytes, use -b option to e
xtract)
XMP Toolkit                     : XMP Core 5.4.0
Creator Tool                    : Photos 1.5
Date Created                    : 2014:12:27 16:45:55
Warning                         : [minor] Fixed incorrect URI for xmlns:Micro
softPhoto
Camera Serial Number            : flag{EEe_x_I_FFf}
```

I ran exiftool tool on the image to gather details related to the image

4. **Procedures**
    1. I ran the "exiftool sunset.jpg' to gather the camera metadata
    2. I ran ` strings sunset.jpg | less ` no result was displayed

```
└─$ string sunset.jpg |less

┌──(tempuser㉿kali)-[~/Downloads]
└─$ strings sunset.jpg |less
```

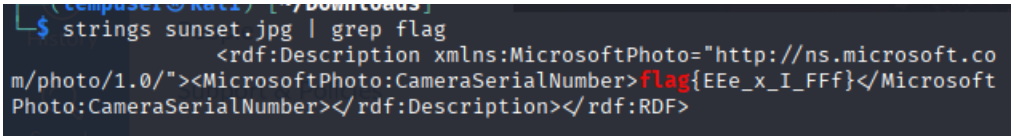
.

    3. I ran 'strings sunset.jpg | grep flag', information related to the flag was displayed.

```
└─$ strings sunset.jpg | grep flag
                <rdf:Description xmlns:MicrosoftPhoto="http://ns.microsoft.co
m/photo/1.0/"><MicrosoftPhoto:CameraSerialNumber>flag{EEe_x_I_FFf}</Microsoft
Photo:CameraSerialNumber></rdf:Description></rdf:RDF>
```

5. Findings / Observations

The flag was found in the jpg image embedded in the camera metadata



6. Result

The flag was found in the jpg image file -> flag{EEe_x_I-FFf}

7. Conclusions:

Used Steghide, which required a password but none was provided. ExifTool provided camera metadata, which was not detailed enough to directly point me to the flag. strings with grep was helpful in filtering out the flag from the image metadata