Paul Badu Yakubu

Penetration Testing

Prof. Anthony J Candeias

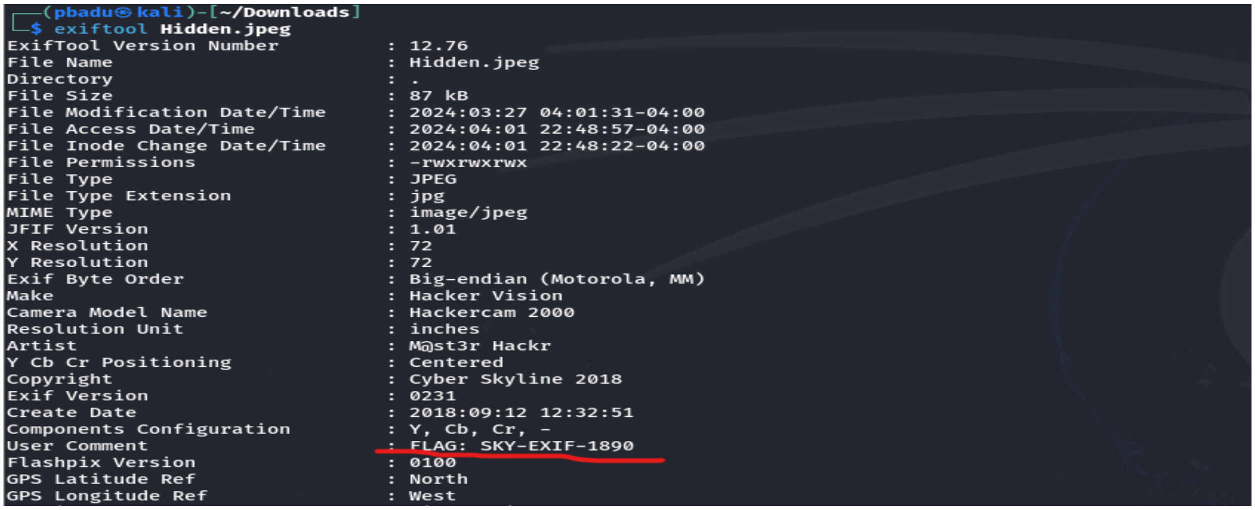
April 1, 2024

NCL Writeup: Practice Game

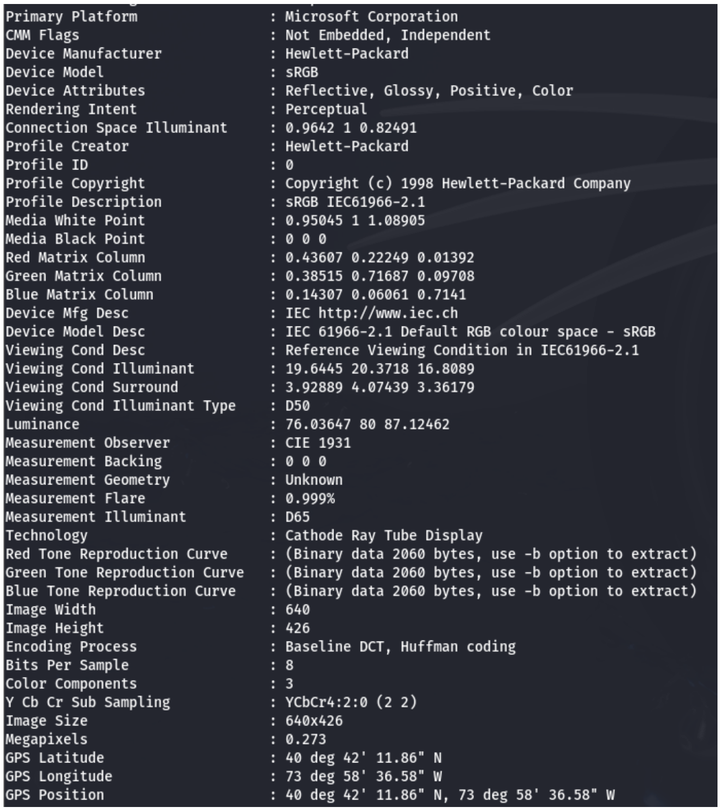
For the National Cyber League (NCL), the cryptography challenge involved attempting to find hidden flags in files and get metadata of given files. The one I attempted involved an image file(jpeg) with a hidden flag embedded in it.

To find the hidden flag, I used a kali Linux tool called exiftool. ExifTool is a powerful command-line utility for reading, writing, and editing meta information in various files. ExifTool supports many metadata formats, including EXIF, GPS, IPTC, XMP, and more. It can process a vast array of file types and is particularly popular for its ability to handle metadata in images and documents.The tool allows users to extract, modify, or remove metadata from files. This can be useful for various purposes, from digital forensics to organizing media collections. ExifTool is known for its flexibility, speed, and the extensive range of file formats it supports.

For the challenge, I simply ran the exiftool command followed by the filename, which returns a whole lot of information about the file, including the creation date, file type, GPS coordinates of where the file was created, and many more. Reading through the metadata of the file, I found the hidden flag in a field named “User comment” with the flag “ SKY-EXIF-1890” .



```
┌──(pbadu㉿kali)-[~/Downloads]
└─$ exiftool Hidden.jpeg
ExifTool Version Number         : 12.76
File Name                       : Hidden.jpeg
Directory                       : .
File Size                       : 87 kB
File Modification Date/Time     : 2024:03:27 04:01:31-04:00
File Access Date/Time           : 2024:04:01 22:48:57-04:00
File Inode Change Date/Time     : 2024:04:01 22:48:22-04:00
File Permissions                : -rwxrwxrwx
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
X Resolution                    : 72
Y Resolution                    : 72
Exif Byte Order                 : Big-endian (Motorola, MM)
Make                            : Hacker Vision
Camera Model Name               : Hackercam 2000
Resolution Unit                 : inches
Artist                          : M@st3r Hackr
Y Cb Cr Positioning             : Centered
Copyright                       : Cyber Skyline 2018
Exif Version                    : 0231
Create Date                     : 2018:09:12 12:32:51
Components Configuration        : Y, Cb, Cr, -
User Comment                    : FLAG: SKY-EXIF-1890
Flashpix Version                : 0100
GPS Latitude Ref                : North
GPS Longitude Ref               : West
```



```
Primary Platform                : Microsoft Corporation
CMM Flags                       : Not Embedded, Independent
Device Manufacturer             : Hewlett-Packard
Device Model                    : sRGB
Device Attributes               : Reflective, Glossy, Positive, Color
Rendering Intent                : Perceptual
Connection Space Illuminant     : 0.9642 1 0.82491
Profile Creator                 : Hewlett-Packard
Profile ID                      : 0
Profile Copyright               : Copyright (c) 1998 Hewlett-Packard Company
Profile Description             : sRGB IEC61966-2.1
Media White Point               : 0.95045 1 1.08905
Media Black Point               : 0 0 0
Red Matrix Column               : 0.43607 0.22249 0.01392
Green Matrix Column             : 0.38515 0.71687 0.09708
Blue Matrix Column              : 0.14307 0.06061 0.7141
Device Mfg Desc                 : IEC http://www.iec.ch
Device Model Desc               : IEC 61966-2.1 Default RGB colour space - sRGB
Viewing Cond Desc               : Reference Viewing Condition in IEC61966-2.1
Viewing Cond Illuminant         : 19.6445 20.3718 16.8089
Viewing Cond Surround           : 3.92889 4.07439 3.36179
Viewing Cond Illuminant Type    : D50
Luminance                       : 76.03647 80 87.12462
Measurement Observer            : CIE 1931
Measurement Backing             : 0 0 0
Measurement Geometry            : Unknown
Measurement Flare               : 0.999%
Measurement Illuminant          : D65
Technology                      : Cathode Ray Tube Display
Red Tone Reproduction Curve     : (Binary data 2060 bytes, use -b option to extract)
Green Tone Reproduction Curve   : (Binary data 2060 bytes, use -b option to extract)
Blue Tone Reproduction Curve    : (Binary data 2060 bytes, use -b option to extract)
Image Width                     : 640
Image Height                    : 426
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 640x426
Megapixels                      : 0.273
GPS Latitude                    : 40 deg 42' 11.86" N
GPS Longitude                   : 73 deg 58' 36.58" W
GPS Position                    : 40 deg 42' 11.86" N, 73 deg 58' 36.58" W
```