Exiftool Demo

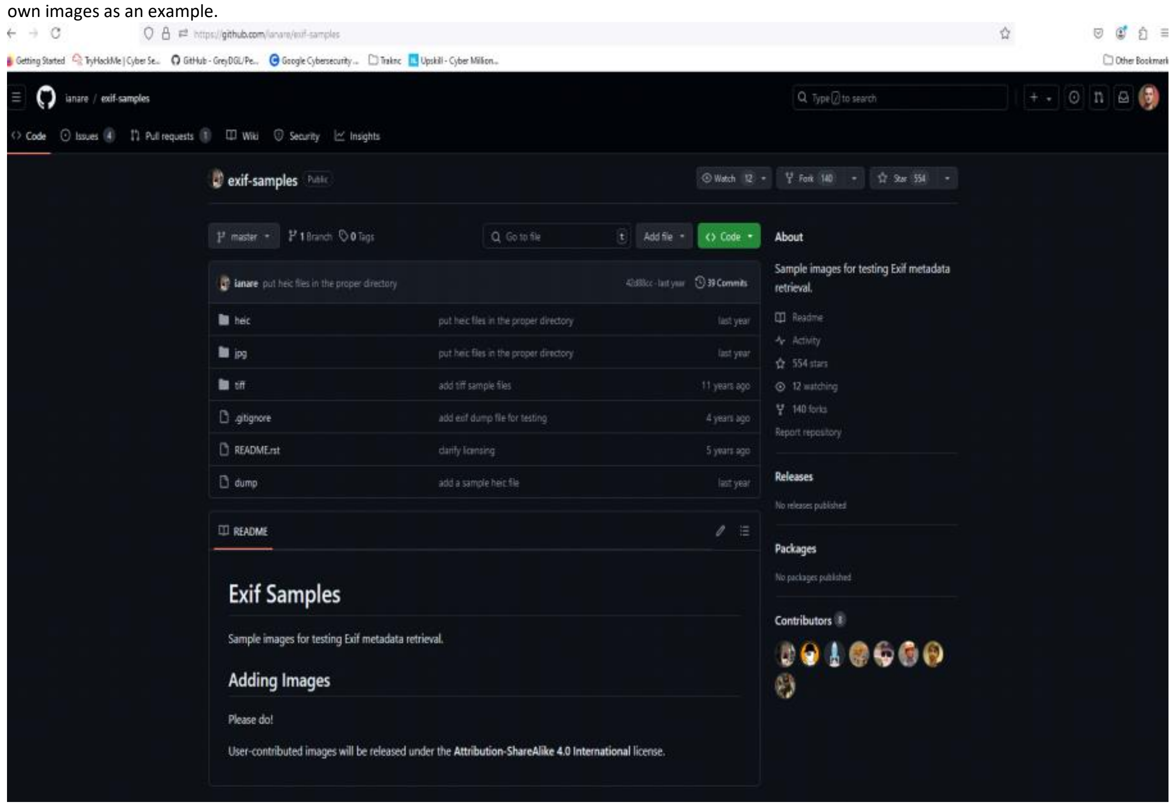
Hello everyone! I hope you are doing well. Thank you for checking this out.

I just wanted to give a little step by step instruction on how to utilize the Exiftool in Kali Linux. If you are not familiar with Exiftool, it comes with your Kali Linux VM or physical machine with the Kali Linux OS.

It is a tool that is used to gather metadata information. The types of files you can gather metadata from include image files (jpeg, PNG, BMP etc.), audio files (mp3, WAV, WMA etc.), video files (MP4, MOV, WebM etc.), document files (PDF, DOC/DOCX, XLS/XLSX etc.) and archive files (ZIP, RAR and 7z). You can also gather metadata from XMP sidecar files and ICC profiles.

This tool is mainly used for forensic purposes. It can verify file authenticity, be used for geolocation purposes, give you camera details such as the make and model and provide the author and editing history. Exiftool is a great resource to utilize in your investigations as it will reveal a lot about a specific file and can help you track down a threat actor.

I will be now showing you some screen shots on how to use Exiftool. I used a sample image from GitHub that was allowed to be used for practice. I did not use anyone's personal files for this demonstration as a disclaimer. Also DO NOT save any type of file to your physical machine that could potentially contain malicious materials. If you are uncertain about this, conduct further investigation into the file by utilizing other means such as VirusTotal and other resources. This is the link https://github.com/ianare/exif-samples

1. First you will want to open your Kali Linux VM or boot up your machine if it isn't already.
2. Once you are at the main screen of your machine, head on over to the link I provided above or use one of your own images as an example.
3. 

https://github.com/ianare/exif-samples

ianare / exif-samples

exif-samples Public

ianare put heic files in the proper directory 42d88cc · last year 39 Commits

heic	put heic files in the proper directory	last year
jpg	put heic files in the proper directory	last year
tiff	add tiff sample files	11 years ago
.gitignore	add exif dump file for testing	4 years ago
README.rst	clarify licensing	5 years ago
dump	add a sample heic file	last year

README

Exif Samples

Sample images for testing Exif metadata retrieval.

Adding Images

Please do!

User-contributed images will be released under the **Attribution-ShareAlike 4.0 International** license.

About

Sample images for testing Exif metadata retrieval.

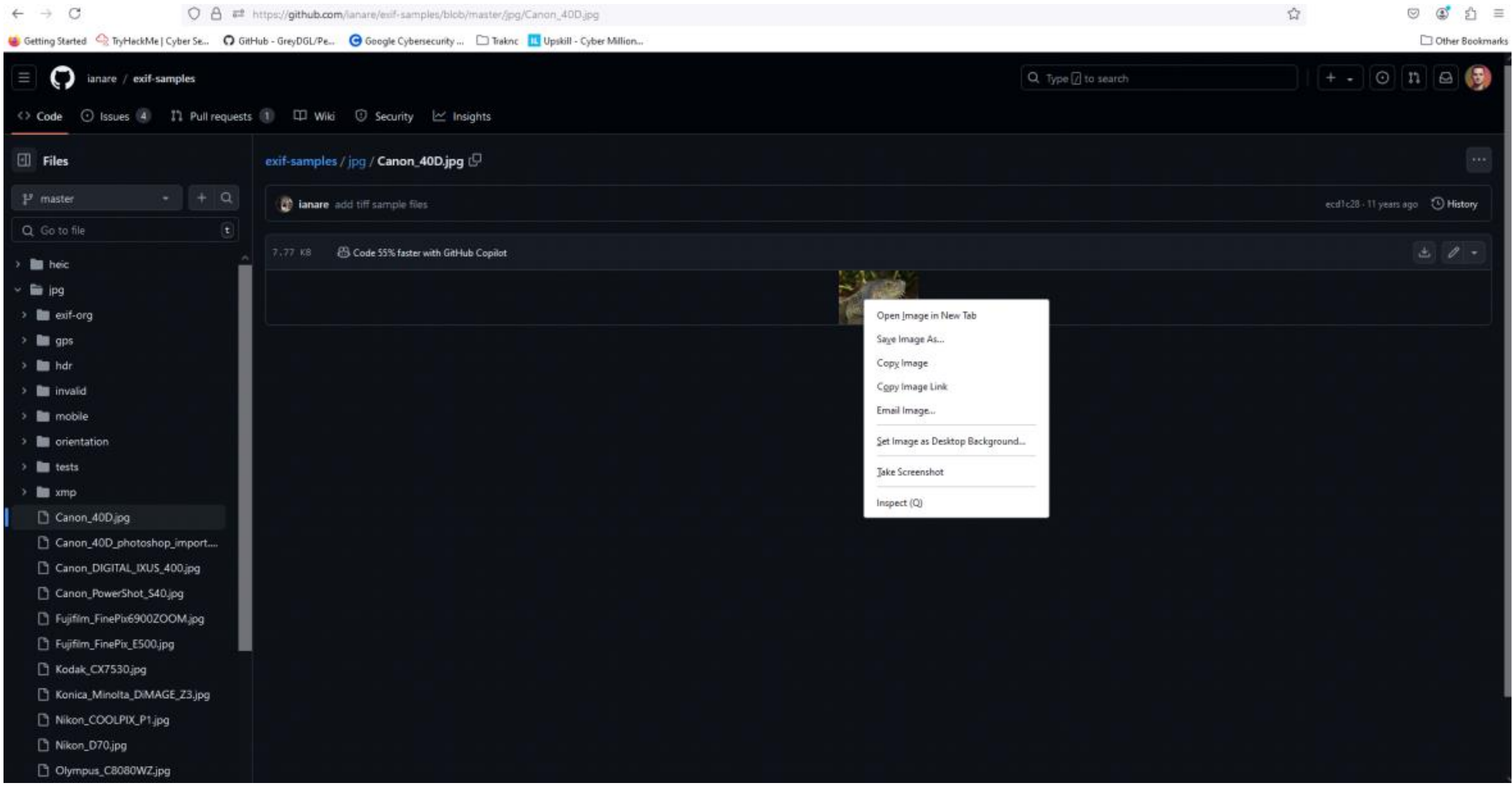
Releases

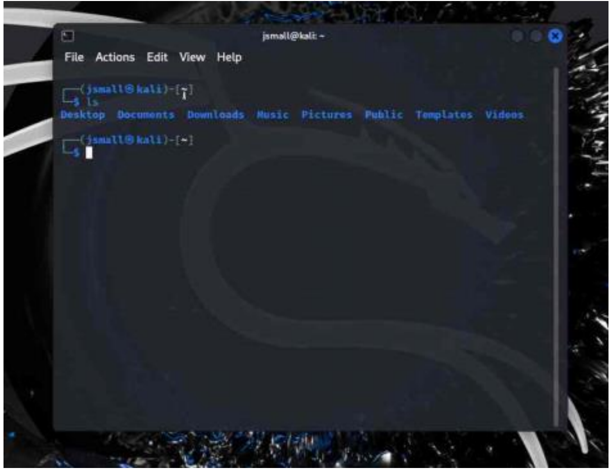
No releases published

Packages

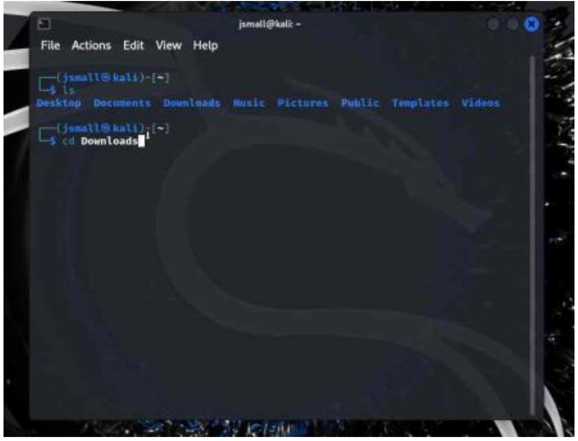
No packages published

4. Choose and image and save it to your machine.

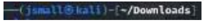
5. 

6. Next, you will want to open your command prompt. Then you want to use the **ls** command to see your directories
7. 

```
┌──(jsmall㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(jsmall㉿kali)-[~]
└─$ 
```

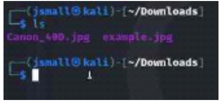
8. Navigate to your Downloads directory or the directory to where you saved the image. By default, the image should have been saved to Downloads. For this demo, the command to change directories into the Downloads folder is **cd Downloads** and press ENTER
9. 

```
┌──(jsmall㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(jsmall㉿kali)-[~]
└─$ cd Downloads
```

10. You should see this in your command prompt if you have successfully navigated to your Downloads directory
11. 

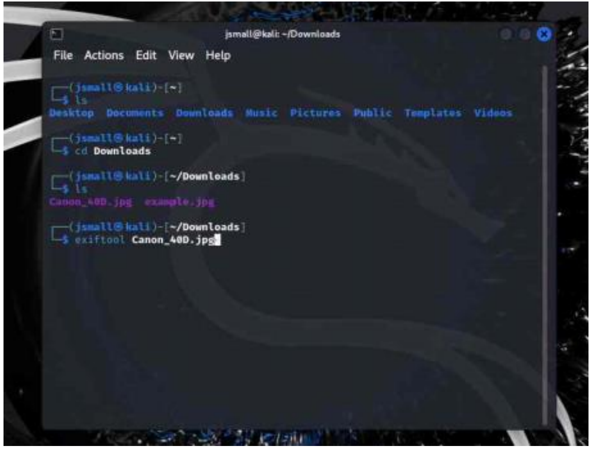
```
┌──(jsmall㉿kali)-[~/Downloads]
```

12. If you want to verify that the jpeg file you're looking for is in that directory, simply type the **ls** command and press enter. For this demo, I saved the sample image named Canon_40D.jpeg and you can see it listed with another example photo of my own in this directory.

13. 

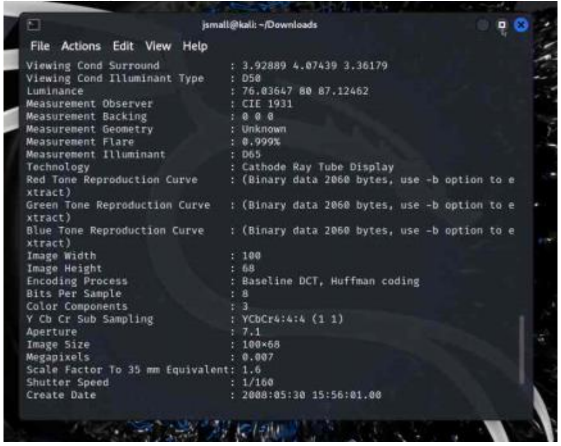
```
┌──(jsmall㉿kali)-[~/Downloads]
└─$ ls
Canon_40D.jpg  example.jpg

┌──(jsmall㉿kali)-[~/Downloads]
└─$ █
```

14. To execute the power of Exiftool on the desired file, simply use the command line exiftool Canon_40D.jpeg and press ENTER

15. 

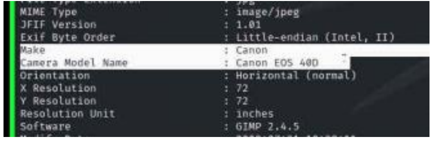
```
┌──(jsmall㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(jsmall㉿kali)-[~]
└─$ cd Downloads

┌──(jsmall㉿kali)-[~/Downloads]
└─$ ls
Canon_40D.jpg  example.jpg

┌──(jsmall㉿kali)-[~/Downloads]
└─$ exiftool Canon_40D.jpg█
```

16. You will then see a similar screen to this one and it will have populated all kinds of metadata about this particular jpeg file.

17. 

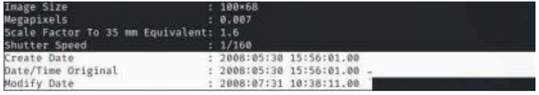
```
Viewing Cond Surround           : 3.92889 4.07439 3.36179
Viewing Cond Illuminant Type    : D50
Luminance                       : 76.03647 80 87.12462
Measurement Observer            : CIE 1931
Measurement Backing             : 0 0 0
Measurement Geometry            : Unknown
Measurement Flare               : 0.999%
Measurement Illuminant          : D65
Technology                      : Cathode Ray Tube Display
Red Tone Reproduction Curve     : (Binary data 2060 bytes, use -b option to e
xtract)
Green Tone Reproduction Curve   : (Binary data 2060 bytes, use -b option to e
xtract)
Blue Tone Reproduction Curve    : (Binary data 2060 bytes, use -b option to e
xtract)
Image Width                     : 100
Image Height                    : 68
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:4:4 (1 1)
Aperture                        : 7.1
Image Size                      : 100×68
Megapixels                      : 0.007
Scale Factor To 35 mm Equivalent: 1.6
Shutter Speed                   : 1/160
Create Date                     : 2008:05:30 15:56:01.00
```

18. If you wanted to see what the camera make and model that was used to take this picture, simply scroll through and you will find it

19. 

```
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Exif Byte Order                 : Little-endian (Intel, II)
Make                            : Canon
Camera Model Name               : Canon EOS 40D
Orientation                     : Horizontal (normal)
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Software                        : GIMP 2.4.5
```

20. You can even find things such as the image size and date and time it was taken. You can even see that at a later date and time, the image was altered from its original state under Modify Date.

21. 

```
Image Size                      : 100×68
Megapixels                      : 0.007
Scale Factor To 35 mm Equivalent: 1.6
Shutter Speed                   : 1/160
Create Date                     : 2008:05:30 15:56:01.00
Date/Time Original              : 2008:05:30 15:56:01.00
Modify Date                     : 2008:07:31 10:38:11.00
```

Again, this was meant to be a short demo on how to use Exiftool. There is so much more you can do and use Exiftool for in your investigations. I can make more tutorials if you would like later using different types of files. I hope this brief tutorial has helped you learn something you did not know. Stay safe and have fun playing around with Exiftool!