Lab - Using the EXIFtool to Read and Write EXIF Tags

Overview

This lab will learn how to use the EXIFtool to examine the tagging and metadata information within an image file. EXIF stands for "**Exchangeable Image File Format**."

Exiftool was developed by Phil Harvey. It is a platform-independent Perl library coupled with a full-featured command-line implementation for reading, writing, and manipulating the metadata across a broad range of files, particularly JPEG images. This metadata can include the camera make, file type, permissions, file size, etc. Exiftool further offers more details about the photograph, like the exposure, the shutter speed, and whether the flash fired or not.

Though some metadata is readily available viewing the property tab of an image, this is just a small subset of the metadata tags available under the hood of an image file. The EXIF tool is a free and open-source software program for reading, writing, and manipulating an image, audio, video, and PDF metadata.

Lab Requirements

In this lab, I am using **CSI Linux**. **CSI Linux** comes with Exiftool preinstalled, and I find it more conducive for conducting digital analysis. This is not to say you cannot use Kali and get the same results. I find that getting the Exiftool to run and work correctly in Kali takes some troubleshooting.

To install the Exiftool onto **Kali**, you first need to clone it from Github.

```
git clone https://github.com/exiftool/exiftool.git
```

In addition, you will need to install the necessary Pearl package to run it.

```
sudo apt-get install libimage-exiftool-perl
```

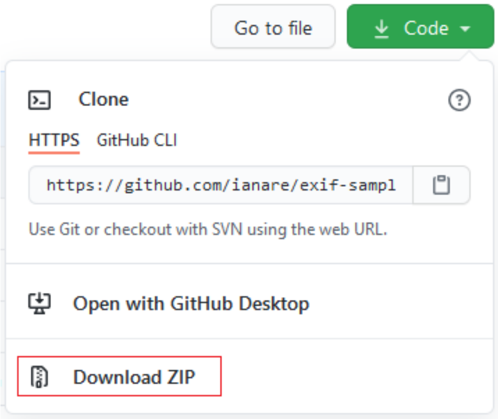
For your CSI or Kali desktop, download the following images for Exiftool to work with. Once you have the images downloaded, you can extract the archive to your desktop for this lab.

What follows is the instructions for downloading and extracting the image files from Dropbox.

From your Kali or CSI Desktop, open a browser and paste the following URL into the address bar.

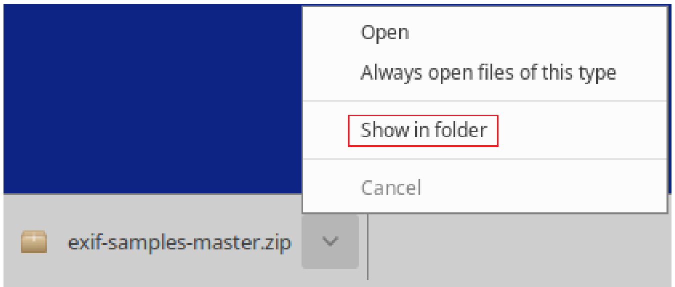
https://github.com/ianare/exif-samples

Scroll to the right side of the page and click on the green button that says Code. From the context menu, select the open to download as a zip file.

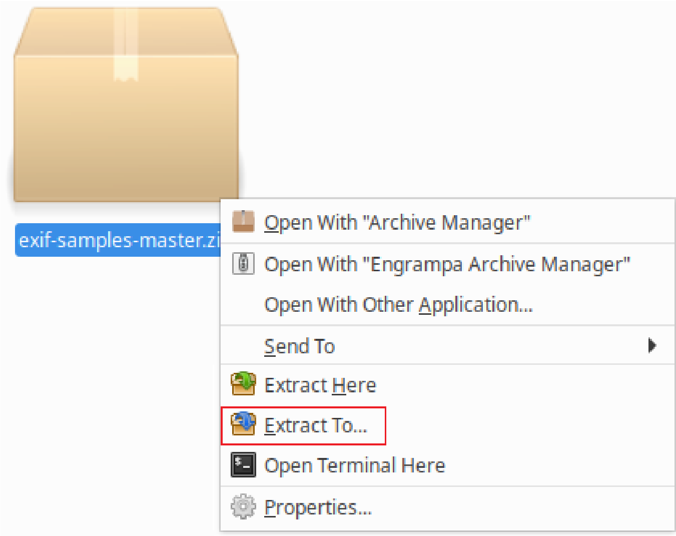


Use Git or checkout with SVN using the web URL.

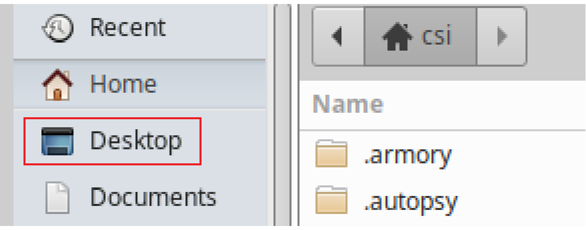
Scroll to the bottom of your browser window, find the download, click on the down arrow, and from the context menu, select, **Show in folder**.



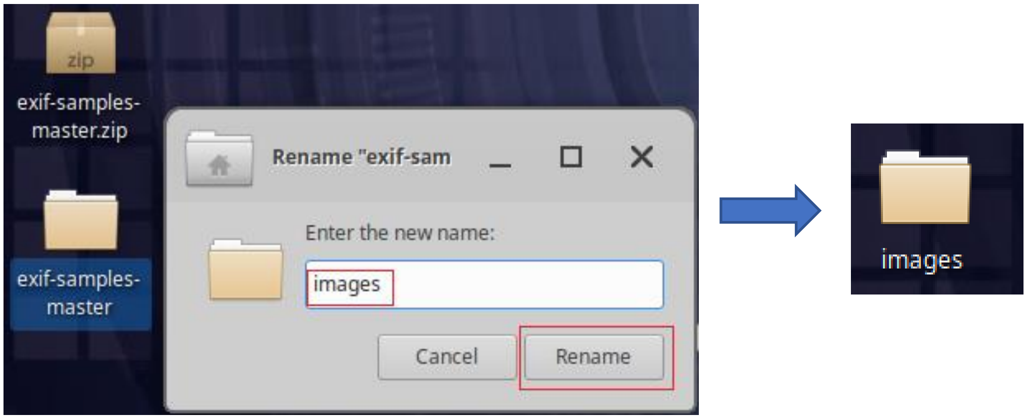
Right-click on the downloaded archive.


exif-samples-master.zi
Open With "Archive Manager"
Open With "Engrampa Archive Manager"
Open With Other Application...
Send To
Extract Here
Extract To...
Open Terminal Here
Properties...

From the menu on the left, select the Desktop as the location to extract to.



Locate the extracted folder on your Desktop. Right-click and rename the extracted folder, **images**, all lower case.



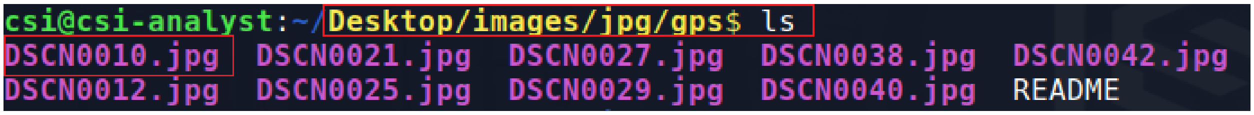
Begin the lab!

From the desktop, launch a terminal. At the prompt, we need to change the directory location to where our target image is located.

Change directory location to the following location:

```
cd Desktop/images/jpg/gps
```

At the prompt, type `ls` to see the contents of the `gps` directory.

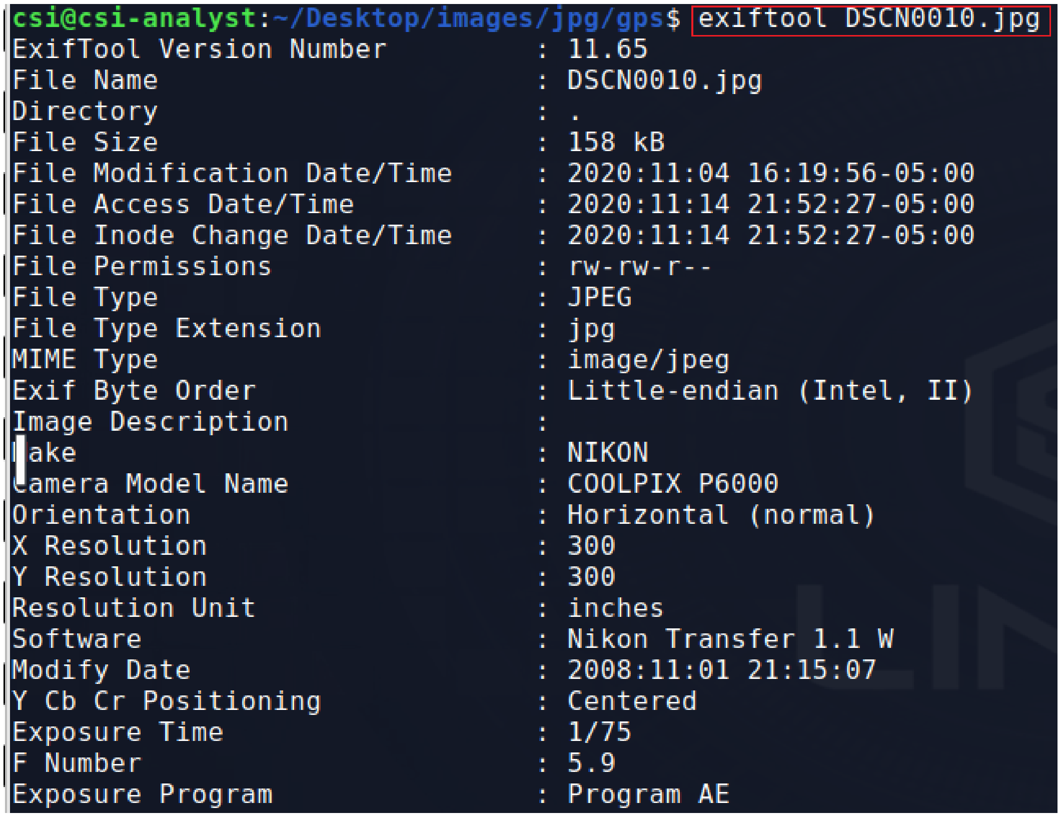


```
csi@csi-analyst:~/Desktop/images/jpg/gps$ ls
DSCN0010.jpg  DSCN0021.jpg  DSCN0027.jpg  DSCN0038.jpg  DSCN0042.jpg
DSCN0012.jpg  DSCN0025.jpg  DSCN0029.jpg  DSCN0040.jpg  README
```

Copy and paste the name of the first image.

At the terminal prompt, to launch the ExifTool, type exiftool followed by the name of the image.

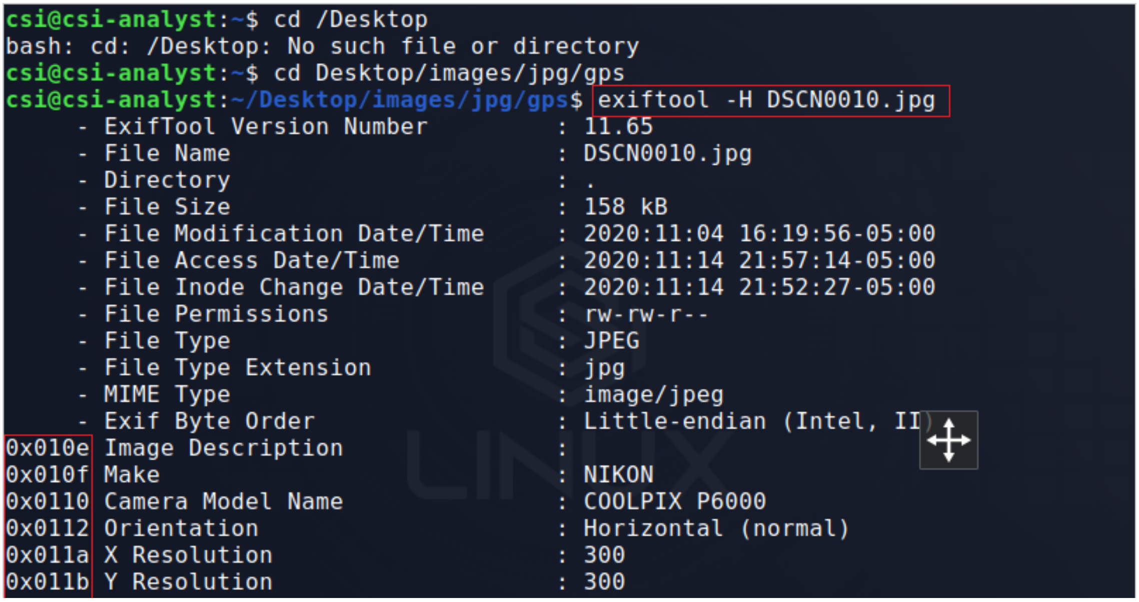
```
exiftool DSCN0010.jpg
```



```
csi@csi-analyst:~/Desktop/images/jpg/gps$ exiftool DSCN0010.jpg
ExifTool Version Number         : 11.65
File Name                       : DSCN0010.jpg
Directory                       : .
File Size                       : 158 kB
File Modification Date/Time     : 2020:11:04 16:19:56-05:00
File Access Date/Time           : 2020:11:14 21:52:27-05:00
File Inode Change Date/Time     : 2020:11:14 21:52:27-05:00
File Permissions                : rw-rw-r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Little-endian (Intel, II)
Image Description               :
Make                            : NIKON
Camera Model Name               : COOLPIX P6000
Orientation                     : Horizontal (normal)
X Resolution                    : 300
Y Resolution                    : 300
Resolution Unit                 : inches
Software                        : Nikon Transfer 1.1 W
Modify Date                     : 2008:11:01 21:15:07
Y Cb Cr Positioning             : Centered
Exposure Time                   : 1/75
F Number                        : 5.9
Exposure Program                : Program AE
```

To show the IDs and exif tags in a Hexa-Decimal format, we can run the following command.

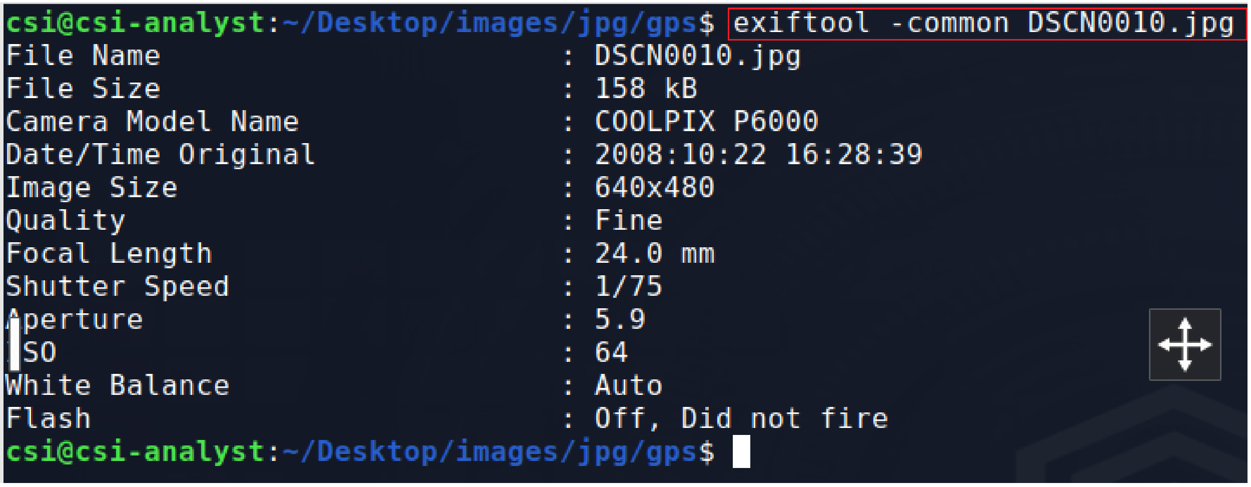
`exiftool -H DSCN0010.jpg`



```
csi@csi-analyst:~$ cd /Desktop
bash: cd: /Desktop: No such file or directory
csi@csi-analyst:~$ cd Desktop/images/jpg/gps
csi@csi-analyst:~/Desktop/images/jpg/gps$ exiftool -H DSCN0010.jpg
     - ExifTool Version Number         : 11.65
     - File Name                       : DSCN0010.jpg
     - Directory                       : .
     - File Size                       : 158 kB
     - File Modification Date/Time     : 2020:11:04 16:19:56-05:00
     - File Access Date/Time           : 2020:11:14 21:57:14-05:00
     - File Inode Change Date/Time     : 2020:11:14 21:52:27-05:00
     - File Permissions                : rw-rw-r--
     - File Type                       : JPEG
     - File Type Extension             : jpg
     - MIME Type                       : image/jpeg
     - Exif Byte Order                 : Little-endian (Intel, II)
0x010e Image Description               :
0x010f Make                            : NIKON
0x0110 Camera Model Name               : COOLPIX P6000
0x0112 Orientation                     : Horizontal (normal)
0x011a X Resolution                    : 300
0x011b Y Resolution                    : 300
```

To see just a subset of the most common Exif tags of the image file, type the following command.

`exiftool -common DSCN0010.jpg`

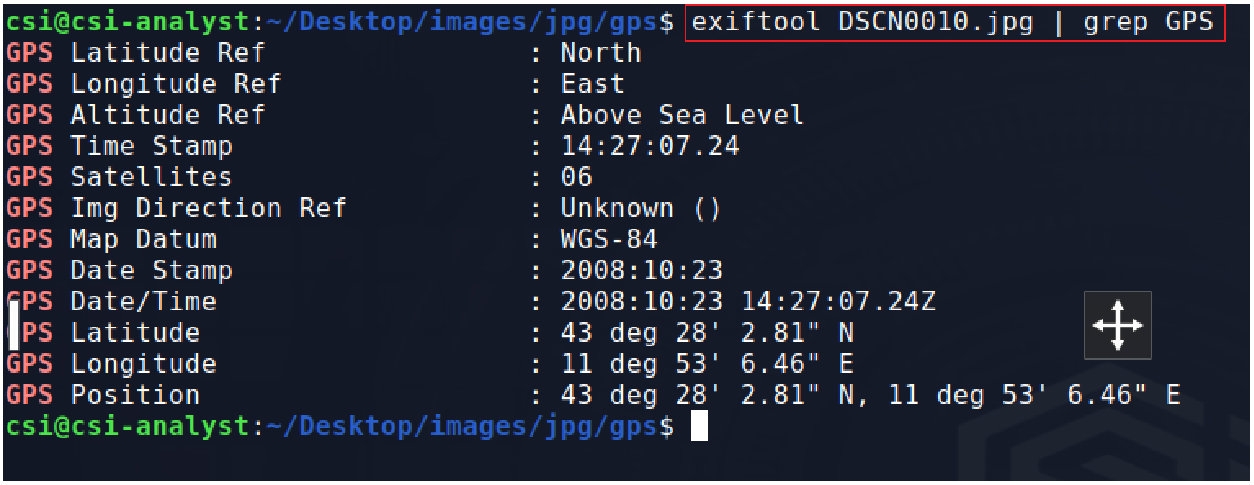


```
csi@csi-analyst:~/Desktop/images/jpg/gps$ exiftool -common DSCN0010.jpg
File Name                       : DSCN0010.jpg
File Size                       : 158 kB
Camera Model Name               : COOLPIX P6000
Date/Time Original              : 2008:10:22 16:28:39
Image Size                      : 640x480
Quality                         : Fine
Focal Length                    : 24.0 mm
Shutter Speed                   : 1/75
Aperture                        : 5.9
ISO                             : 64
White Balance                   : Auto
Flash                           : Off, Did not fire
csi@csi-analyst:~/Desktop/images/jpg/gps$
```

If the image was taken using a smartphone or a camera with the GPS information embedded in the device, this to can be extracted.

To see just the GPS information, type the following command.

exiftool DSCN0010.jpg | grep GPS

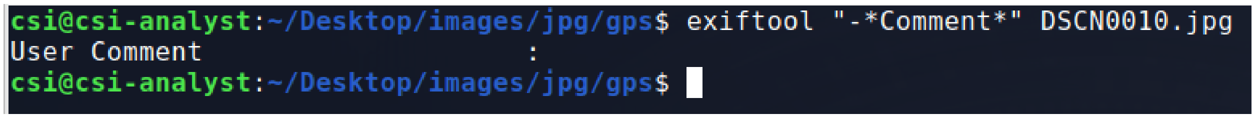


```
csi@csi-analyst:~/Desktop/images/jpg/gps$ exiftool DSCN0010.jpg | grep GPS
GPS Latitude Ref                : North
GPS Longitude Ref               : East
GPS Altitude Ref                : Above Sea Level
GPS Time Stamp                  : 14:27:07.24
GPS Satellites                  : 06
GPS Img Direction Ref           : Unknown ()
GPS Map Datum                   : WGS-84
GPS Date Stamp                  : 2008:10:23
GPS Date/Time                   : 2008:10:23 14:27:07.24Z
GPS Latitude                    : 43 deg 28' 2.81" N
GPS Longitude                   : 11 deg 53' 6.46" E
GPS Position                    : 43 deg 28' 2.81" N, 11 deg 53' 6.46" E
csi@csi-analyst:~/Desktop/images/jpg/gps$
```

With Exiftool, we can also conduct a keyword search to look for a particular tag being present among the metadata. In this example, I am looking for any tag with the keyword ‘comment’ as being present.

exiftool "-*Comment*" DSCN0010.jpg

In this example, the asterisk character (*) is being used as a wildcard in the search.

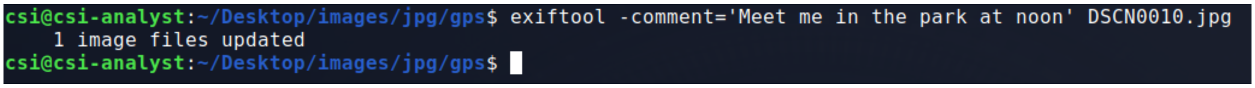


```
csi@csi-analyst:~/Desktop/images/jpg/gps$ exiftool "-*Comment*" DSCN0010.jpg
User Comment                    :
csi@csi-analyst:~/Desktop/images/jpg/gps$
```

Exiftool also allows us to write to certain metadata tags that are not restricted. Restricted tags would be any tag that has anything to do with the physical characteristics of the image file, such as the compression ratio.

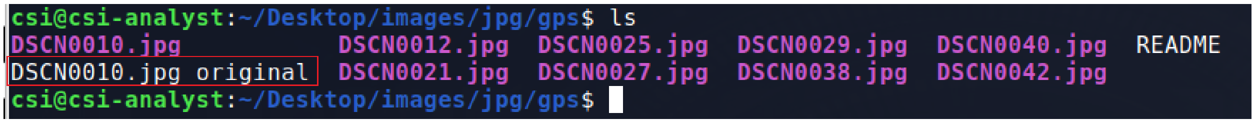
In this example, I added a message to the comment tag. This would be an example of someone hiding a message within the metadata of the image.

```
exiftool -comment='Meet me in the park at noon’ DSCN0010.jpg
```



```
csi@csi-analyst:~/Desktop/images/jpg/gps$ exiftool -comment='Meet me in the park at noon' DSCN0010.jpg
    1 image files updated
csi@csi-analyst:~/Desktop/images/jpg/gps$ 
```

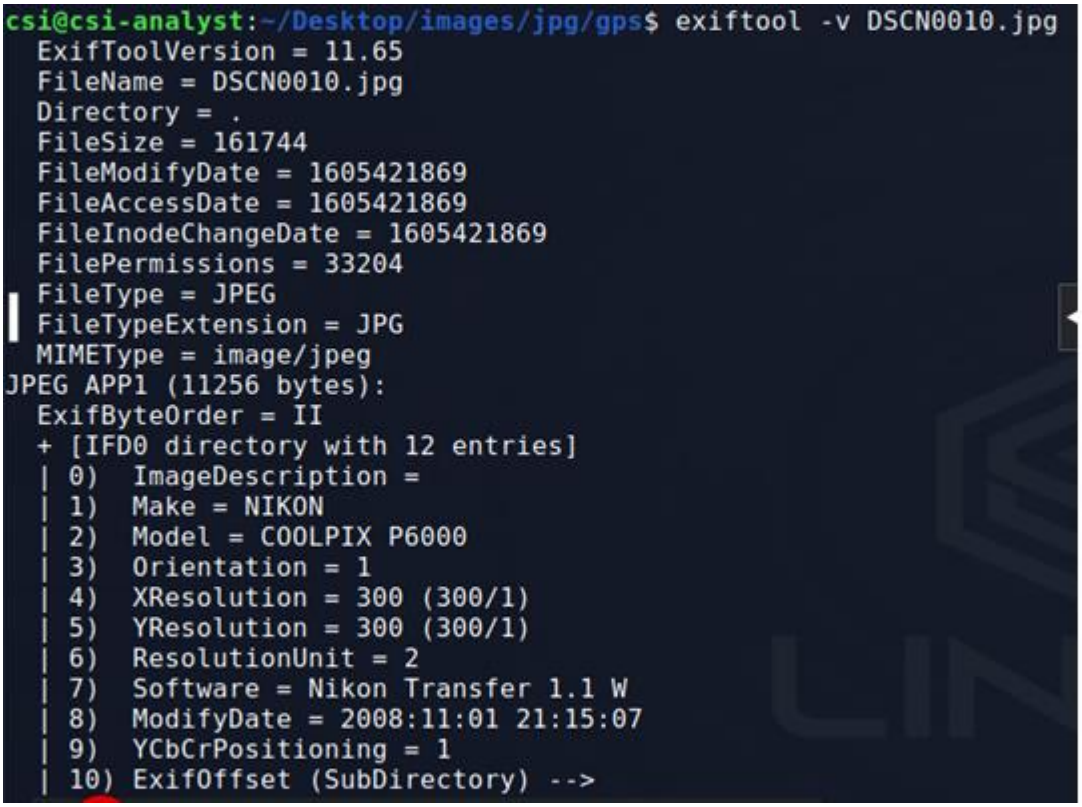
Anytime you modify an image’s original metadata with ExifTool, a copy of the original file is backed up.



```
csi@csi-analyst:~/Desktop/images/jpg/gps$ ls
DSCN0010.jpg            DSCN0012.jpg  DSCN0025.jpg  DSCN0029.jpg  DSCN0040.jpg  README
DSCN0010.jpg original   DSCN0021.jpg  DSCN0027.jpg  DSCN0038.jpg  DSCN0042.jpg
csi@csi-analyst:~/Desktop/images/jpg/gps$ 
```

Exiftool has a verbose feature (-v) to provide more comprehensive data about the process being performed.

```
exiftool -v DSCN0010.jpg
```

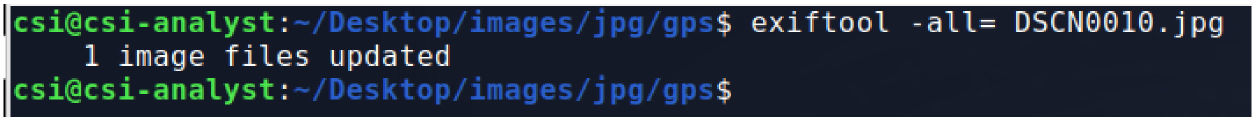


```
csi@csi-analyst:~/Desktop/images/jpg/gps$ exiftool -v DSCN0010.jpg
  ExifToolVersion = 11.65
  FileName = DSCN0010.jpg
  Directory = .
  FileSize = 161744
  FileModifyDate = 1605421869
  FileAccessDate = 1605421869
  FileInodeChangeDate = 1605421869
  FilePermissions = 33204
  FileType = JPEG
  FileTypeExtension = JPG
  MIMEType = image/jpeg
JPEG APP1 (11256 bytes):
  ExifByteOrder = II
  + [IFD0 directory with 12 entries]
  | 0)  ImageDescription =
  | 1)  Make = NIKON
  | 2)  Model = COOLPIX P6000
  | 3)  Orientation = 1
  | 4)  XResolution = 300 (300/1)
  | 5)  YResolution = 300 (300/1)
  | 6)  ResolutionUnit = 2
  | 7)  Software = Nikon Transfer 1.1 W
  | 8)  ModifyDate = 2008:11:01 21:15:07
  | 9)  YCbCrPositioning = 1
  | 10) ExifOffset (SubDirectory) -->
```

Exiftool can also remove the metadata for an image file leaving only a small subset of information.

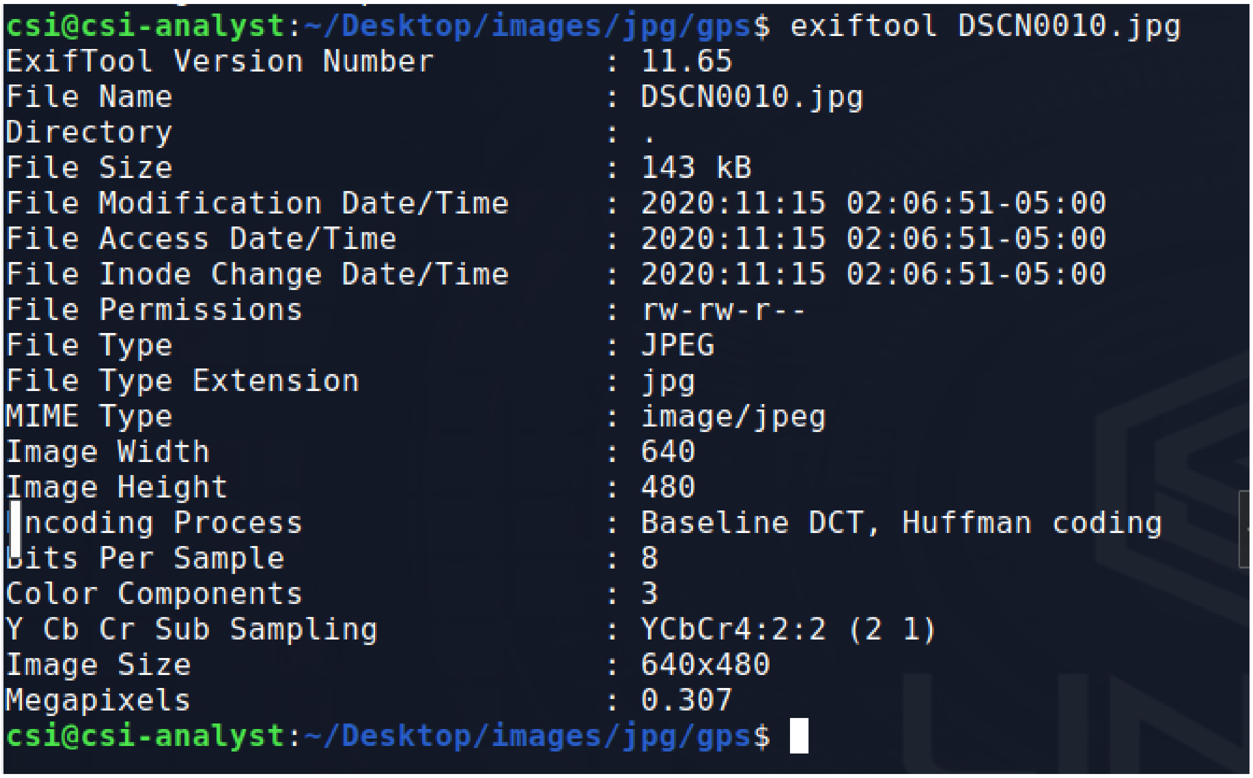
To remove the metadata from an image, type the following command.

`exiftool -all= DSCN0010.jpg`



```
csi@csi-analyst:~/Desktop/images/jpg/gps$ exiftool -all= DSCN0010.jpg
    1 image files updated
csi@csi-analyst:~/Desktop/images/jpg/gps$
```

After the removal….



```
csi@csi-analyst:~/Desktop/images/jpg/gps$ exiftool DSCN0010.jpg
ExifTool Version Number         : 11.65
File Name                       : DSCN0010.jpg
Directory                       : .
File Size                       : 143 kB
File Modification Date/Time     : 2020:11:15 02:06:51-05:00
File Access Date/Time           : 2020:11:15 02:06:51-05:00
File Inode Change Date/Time     : 2020:11:15 02:06:51-05:00
File Permissions                : rw-rw-r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Image Width                     : 640
Image Height                    : 480
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:2 (2 1)
Image Size                      : 640x480
Megapixels                      : 0.307
csi@csi-analyst:~/Desktop/images/jpg/gps$
```