Exiftool Exercise

BitCuratorEdu

Last Updated: January 18, 2022

About This Exercise

Author
Cal Lee

Description
This exercise is meant to introduce students to EXIF metadata and give them hands-on experience using Exiftool in the BitCurator environment. These slides are excerpted from Cal Lee's SAA "Advanced Digital Forensics" class.

Learning object type
Lesson plan/materials

Learning objectives
This learning object might be used in a lesson to satisfy the following learning objectives:

- Practice using tools in the BitCurator Environment.

Exchangeable Image File Format (EXIF)

- Possible tags:

https://exiftool.org/TagNames/EXIF.html

Example of EXIF Metadata from a JPEG File (Generated Using exiftool*)

```
---- ExifTool ----
ExifTool Version Number         : 9.38
---- System ----
File Name                       : IMG_20130823_151811.jpg
Directory                       : C:/Users/callee/Documents/images/digital-forensics-lab
File Size                       : 1785 kB
File Modification Date/Time     : 2013:08:23 16:36:44-04:00
File Access Date/Time           : 2013:10:14 17:13:02-04:00
File Creation Date/Time         : 2013:08:23 16:36:44-04:00
File Permissions                : rw-rw-rw-
---- File ----
File Type                       : JPEG
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
Image Width                     : 2592
Image Height                    : 1944
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
---- GPS ----
GPS Img Direction               : 83
GPS Img Direction Ref           : Magnetic North
GPS Latitude Ref                : North
GPS Latitude                    : 35 deg 55' 2.24"
GPS Longitude Ref               : West
GPS Longitude                   : 79 deg 2' 57.55"
GPS Altitude Ref                : Above Sea Level
GPS Altitude                    : 0 m
GPS Time Stamp                  : 19:18:06
GPS Processing Method           : NETWORK
GPS Date Stamp                  : 2013:08:23
---- IFD0 ----
Orientation                     : Unknown (0)
Camera Model Name               : Galaxy Nexus
Modify Date                     : 2013:08:23 15:18:11
Y Cb Cr Positioning             : Centered
Y Resolution                    : 72
Resolution Unit                 : inches
X Resolution                    : 72
Make                            : Samsung
---- ExifIFD ----
Create Date                     : 2013:08:23 15:18:11
Date/Time Original              : 2013:08:23 15:18:11
Exif Version                    : 0220
Flash Energy                    : 0
Image Unique ID                 : OAEL01
Exposure Time                   : 1/17
ISO                             : 125, 0, 0
Scene Type                      : Directly photographed
Exposure Index                  : undef
Components Configuration        : Y, Cb, Cr, -
F Number                        : 2.8
Compressed Bits Per Pixel       : 0
Sensing Method                  : One-chip color area
Exposure Program                : Aperture-priority AE
Aperture Value                  : 2.6
Brightness Value                : 0
Subject Distance Range          : Unknown
Shutter Speed Value             : 1/15
Subject Distance                : 0 m
Saturation                      : Normal
Color Space                     : sRGB
Contrast                        : Normal
Metering Mode                   : Multi-spot
Flashpix Version                :
Exposure Compensation           : 0
Exif Image Height               : 1944
Max Aperture Value              : 2.6
Sharpness                       : Normal
Exif Image Width                : 2592
Focal Length                    : 3.4 mm
Digital Zoom Ratio              : 1
Light Source                    : Fluorescent
Scene Capture Type              : Standard
Flash                           : Off, Did not fire
Custom Rendered                 : Custom
White Balance                   : Auto
Exposure Mode                   : Auto
---- IFD1 ----
Compression                     : JPEG (old-style)
Image Width                     : 160
Image Height                    : 120
Thumbnail Offset                : 1239
Thumbnail Length                : 7164
---- Composite ----
Aperture                        : 2.8
GPS Altitude                    : 0 m Above Sea Level
GPS Date/Time                   : 2013:08:23 19:18:06Z
GPS Latitude                    : 35 deg 55' 2.24" N
GPS Longitude                   : 79 deg 2' 57.55" W
GPS Position                    : 35 deg 55' 2.24" N, 79 deg 2' 57.55" W
Image Size                      : 2592x1944
Shutter Speed                   : 1/17
Thumbnail Image                 : (Binary data 7164 bytes, use -b option to extract)
Focal Length                    : 3.4 mm
Light Value                     : 6.7
```

*http://www.sno.phy.queensu.ca/~phil/exiftool/ (Also available through the BitCurator environment)

Exiftool Exercise (BitCurator)

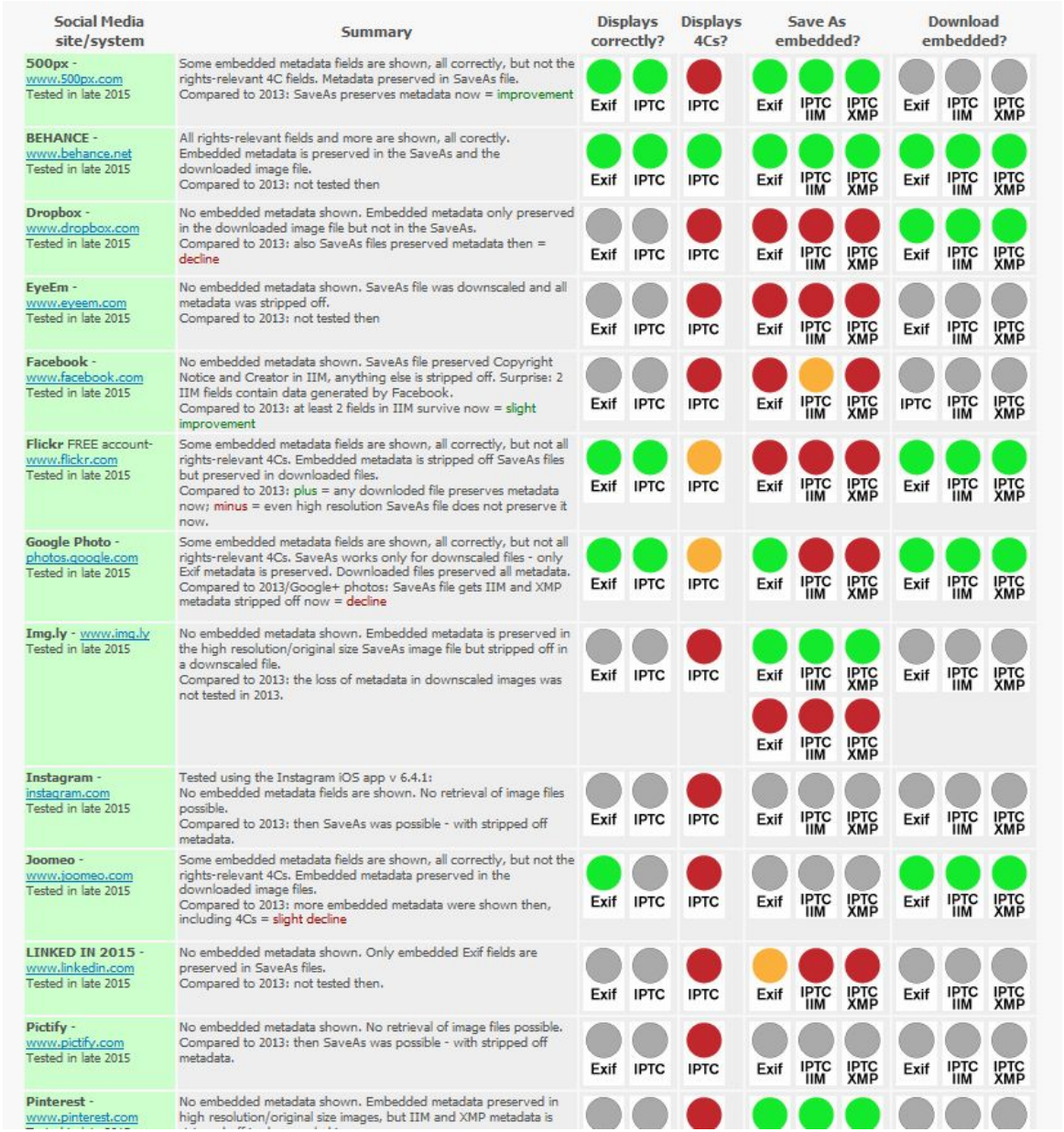
- Start up the BitCurator VM
- Download one or more pictures to your desktop that you'd like to examine
- Options for viewing EXIF:
  1. PyEXIFToolGUI:
     - Navigate to Desktop > Forensics Tools > PyEXIFToolGUI
     - Open the tool and select File > Load Images
     - Let's also add some GPS coordinates: Select Edit Data, enter the values, then select Save to Selected Image(s) [Make sure that the image is selected]
  2. File info menu:
     - Navigate to the image file
     - Right click on it and select Scripts > File Info > Meta Information [Pick EXIF Data]
  3. exiftool at the command line:
     - Open a command prompt window
     - Navigate to where you stored the image (e.g. cd Desktop)
     - Type: *exiftool [Filename]*
     - Note: You can scroll up and down by using Shift + Page Up/Page Down, or you can invoke the command as *exiftool [Filename]* | *less* (type "q" to quit)

Optional Exiftool Exercise (Windows or Mac)

- Download one or more pictures to your desktop that you'd like to examine
- Download and unzip Windows Executable or MacOS Package: https://exiftool.org/
- Save exiftool(-k).exe to your desktop
  - Change file name to: exiftool(-k -a -u -g1 -w txt).exe [NOTE: This is changing the parameters for running the software – same as if you were to add these switches at the command line. This trick might not work on a Mac, but you can always issue the commands directly.]
    - -k = pause the program before terminating
    - -a = allow extraction of duplicate tags
    - -u = extract unknown tags
    - -g1 = organize output by tag group
    - -w = write output text file
- Drag and drop pictures onto the exiftool icon and examine the results
- Change file name to: exiftool(**-X** -k -a -u -g1 -w **xml**).exe
- Drag and drop pictures onto the exiftool icon and examine the results

For more about exiftool, see: https://exiftool.org/

Stripping of Metadata from Images



Social Media site/system	Summary	Displays correctly?		Displays 4Cs?	Save As embedded?			Download embedded?		
500px - www.500px.com Tested in late 2015	Some embedded metadata fields are shown, all correctly, but not the rights-relevant 4C fields. Metadata preserved in SaveAs file. Compared to 2013: SaveAs preserves metadata now = improvement	Exif	IPTC	IPTC	Exif	IPTC IIM	IPTC XMP	Exif	IPTC IIM	IPTC XMP
BEHANCE - www.behance.net Tested in late 2015	All rights-relevant fields and more are shown, all corectly. Embedded metadata is preserved in the SaveAs and the downloaded image file. Compared to 2013: not tested then	Exif	IPTC	IPTC	Exif	IPTC IIM	IPTC XMP	Exif	IPTC IIM	IPTC XMP
Dropbox - www.dropbox.com Tested in late 2015	No embedded metadata shown. Embedded metadata only preserved in the downloaded image file but not in the SaveAs. Compared to 2013: also SaveAs files preserved metadata then = decline	Exif	IPTC	IPTC	Exif	IPTC IIM	IPTC XMP	Exif	IPTC IIM	IPTC XMP
EyeEm - www.eyeem.com Tested in late 2015	No embedded metadata shown. SaveAs file was downscaled and all metadata was stripped off. Compared to 2013: not tested then	Exif	IPTC	IPTC	Exif	IPTC IIM	IPTC XMP	Exif	IPTC IIM	IPTC XMP
Facebook - www.facebook.com Tested in late 2015	No embedded metadata shown. SaveAs file preserved Copyright Notice and Creator in IIM, anything else is stripped off. Surprise: 2 IIM fields contain data generated by Facebook. Compared to 2013: at least 2 fields in IIM survive now = slight improvement	Exif	IPTC	IPTC	Exif	IPTC IIM	IPTC XMP	IPTC	IPTC IIM	IPTC XMP
Flickr FREE account- www.flickr.com Tested in late 2015	Some embedded metadata fields are shown, all correctly, but not all rights-relevant 4Cs. Embedded metadata is stripped off SaveAs files but preserved in downloaded files. Compared to 2013: plus = any downloded file preserves metadata now; minus = even high resolution SaveAs file does not preserve it now.	Exif	IPTC	IPTC	Exif	IPTC IIM	IPTC XMP	Exif	IPTC IIM	IPTC XMP
Google Photo - photos.google.com Tested in late 2015	Some embedded metadata fields are shown, all correctly, but not all rights-relevant 4Cs. SaveAs works only for downscaled files - only Exif metadata is preserved. Downloaded files preserved all metadata. Compared to 2013/Google+ photos: SaveAs file gets IIM and XMP metadata stripped off now = decline	Exif	IPTC	IPTC	Exif	IPTC IIM	IPTC XMP	Exif	IPTC IIM	IPTC XMP
Img.ly - www.img.ly Tested in late 2015	No embedded metadata shown. Embedded metadata is preserved in the high resolution/original size SaveAs image file but stripped off in a downscaled file. Compared to 2013: the loss of metadata in downscaled images was not tested in 2013.	Exif	IPTC	IPTC	Exif Exif	IPTC IIM IPTC IIM	IPTC XMP IPTC XMP	Exif	IPTC IIM	IPTC XMP
Instagram - instagram.com Tested in late 2015	Tested using the Instagram iOS app v 6.4.1: No embedded metadata fields are shown. No retrieval of image files possible. Compared to 2013: then SaveAs was possible - with stripped off metadata.	Exif	IPTC	IPTC	Exif	IPTC IIM	IPTC XMP	Exif	IPTC IIM	IPTC XMP
Joomeo - www.joomeo.com Tested in late 2015	Some embedded metadata fields are shown, all correctly, but not the rights-relevant 4Cs. Embedded metadata preserved in the downloaded image files. Compared to 2013: more embedded metadata were shown then, including 4Cs = slight decline	Exif	IPTC	IPTC	Exif	IPTC IIM	IPTC XMP	Exif	IPTC IIM	IPTC XMP
LINKED IN 2015 - www.linkedin.com Tested in late 2015	No embedded metadata shown. Only embedded Exif fields are preserved in SaveAs files. Compared to 2013: not tested then.	Exif	IPTC	IPTC	Exif	IPTC IIM	IPTC XMP	Exif	IPTC IIM	IPTC XMP
Pictify - www.pictify.com Tested in late 2015	No embedded metadata shown. No retrieval of image files possible. Compared to 2013: then SaveAs was possible - with stripped off metadata.	Exif	IPTC	IPTC	Exif	IPTC IIM	IPTC XMP	Exif	IPTC IIM	IPTC XMP
Pinterest - www.pinterest.com	No embedded metadata shown. Embedded metadata preserved in high resolution/original size images, but IIM and XMP metadata is									

http://www.embeddedmetadata.org/social-media-test-results.php

Most resources from the BitCuratorEdu project are intentionally left with basic formatting and without project branding. We encourage educators, practitioners, and students to adapt these materials as much as needed and share them widely.

The BitCuratorEdu project is a three-year effort funded by the Institute of Museum and Library Services (IMLS) to study and advance the adoption of digital forensics tools and methods in libraries and archives through professional education efforts. This project is a partnership between Educopia Institute and the School of Information and Library Science at the University of North Carolina at Chapel Hill, along with the Council of State Archivists (CoSA) and several Masters-level programs in library and information science.