

Cyber Investigation for Metadata

TOUTES LES FICHES

par Roseline Faliph



PUBLIC



PARTICIPANTS



ANIMATEURS



NIVEAU



PRÉPARATION



ACTIVITÉ

Description

This workshop mixes theoretical notions with a game-based approach to help participants to understand the idea and utility of metadata. This, in an era where the internet is teeming with a practically endless amount of images.

Objectifs

- Data and metadata
- Digital footprint and metadata
- Websites and debate on metadata

Matériel

- computer for two participants
- a file containing at least a dozen photos
- a good internet connection
- a printed world map
- a projector
- USB keys (one per group)
- pens or markers

Contenus utilisés

<http://exif.regex.info/exif.cgi>

Pré-requis

- Understanding of the file formats used: jpg, mp3, pdf...
- Having notions of latitude and longitude

WORKFLOW

1

What is Metadata?

Image metadata is information (date, place, author, camera type, editing history) registered every time a photo is taken. These data are difficult to access and this is why most people are not aware that their phone or camera stores them

(For older groups: three formats work together to contain information. Without going into detail, EXIF is the one most focused on material aspects, IPTC to copyright and XMP is a modernised extension of IPTC)

All cameras and phones record metadata but these are not always the same. According to your device's settings and characteristics some data won't be registered. For example, geolocation data will not be registered if you don't have deactivated your GPS.

Image format like TIFF or JPEG are some of the most talkative!

But for what?

Metadata means that photographers can easily categorise their photos by place taken, date, etc. It can also reveal details surrounding technical choices taken for photos (speed, lens diaphragm, aperture, exposure, etc.)

In the era of digitisation and internet, where photos are shared everywhere by everyone and often taken out of their original context, metadata also allows photographers to leave an indisputable trace of the authorship of their photos and of the context of the original shot. In this way it is a vital tool for the protection for of copyright and the photographer's authorship.

It is also of course an important means for users to discover the origin of a photograph.

2

Are we all cyber-detectives?

To understand metadata, we will refer to [a website](#) that will unveil all hidden information on a photograph. (Display the site using the projector).

This site was created by an amateur photographer to make it easier to access metadata.

Jeffrey's Image Metadata Viewer

URL:

or...
File: Aucun fichier sélectionné.

☐ Je ne suis pas un robot 
Confidentialité - Conditions

Jeffrey Friedl's Image Metadata Viewer
(How to use)

Some of my other stuff
· My Blog · Lightroom plugins · Pretty Photos
· "Photo Tech"

Demonstration

Demonstrate with some photographs so everyone can understand how to bring up the metadata. Explain that there are two ways to proceed:

- You can analyse metadata of an image found online by giving its url
- You can analyse an image saved on your computer's hard drive through the 'browse' button.

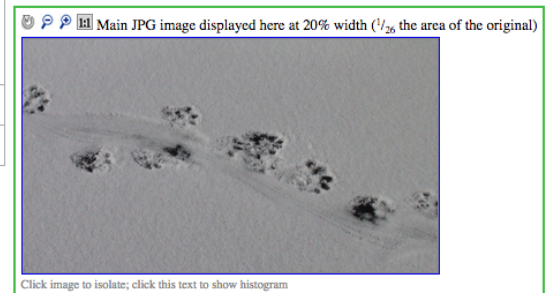
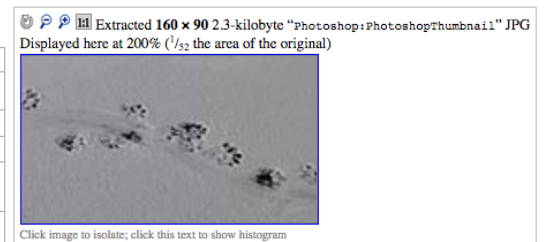
Don't forget to tick the 'I am not a robot' box!

Analyse with participants the different types of information that appear: camera, lens, exposure, flash, date of taking, location (with a link to OpenStreetMap to show the place on a map), size of the file, colour encoding system.

Basic Image Information

Target file: IMG5.jpg

Camera:	Sony HDR-XR200V
Lens:	5.5 mm (Max aperture f/1.8)
Exposure:	Auto exposure, Program AE, 1/250 sec, f/4
Flash:	Auto, Did not fire
Date:	April 10, 2013 9:02:19AM (timezone not specified) (5 years, 7 months, 23 days, 16 hours, 50 minutes, 6 seconds ago, assuming image timezone of 7 hours behind GMT)
Location:	Latitude/longitude: 39° 59' 48.1" North, 106° 22' 52.1" West (39.996685, -106.381150) Map via embedded coordinates at: Google, Yahoo, WikiMapia, OpenStreetMap, Bing (also see the Google Maps pane below) Altitude: 2,281 meters (7,485 feet) Timezone guess from earthtools.org: 7 hours behind GMT
File:	2,304 x 1,296 JPEG (3.0 megapixels) 379,437 bytes (371 kilobytes)
Color Encoding:	Embedded color profile: "sRGB"



We will focus on two data points: the date and the location. Using these two elements we will be able to lead a real cyber-investigation.

The CyberInvestigation scenario

'Gerard Marco is a famous thief who disappeared mysteriously 12 years ago along with many priceless stolen items. He was discovered dead yesterday, but the items were not recovered. A team of international cyber-detectives have gotten their hands on the only piece of proof: a USB key containing some of his data. This is the only

lead we have — the only hope we have of finding the hiding place of the missing objects.

This key contains a series of undated unnamed photographs of seemingly no relation to each other. Thanks to metadata, our cyberdetectives will be able to solve the mystery of these photos'

Off you go!

3

The hunt for metadata!

The hunt for metadata!

Participants will be divided into groups of two. Each group should have:

- a computer with internet access with link towards the site exif.regex.info/exif.cgi
- a printed world map
- a pen/marker

Each group will need to lead the investigation by researching the origin of each photo (date and place) by classing them in order to find where Gerard Marco hid the stolen objects.

This should take around 20 minutes (depending on the level of participants)./

Following this, you can see what each group came up with!

Alternative: give different images to every group and have one world map displayed on the wall. Groups will need to collaborate to retrace the steps for the thief to re-establish the correct chronology between the taking of each photo.

4

Conclusion(s)

Image metadata are another source of personal data we leave online when we share photos. They can contain a huge amount of personal information such as our address and can give away details about our routines or habits.

However, metadata can be precious for photographers in order for them to retain rights over images they have authored! This is also the case for journalists who need to know the source of an image (particularly during this era when such a large amount of false information – fake news – is constantly circulating) or indeed for detectives.

It is also worrying to realise that today, almost 85% of images posted online no longer

contain metadata (<https://www.imatag.com/en/blog/2018/05/11/state-of-image-metadata-in-2018/>). They are mostly being erased to optimise the performance of websites and not being replaced out of ignorance. This is also happening on social media platforms that systematically delete metadata and rename uploaded photos.

How to find the origin of an image without metadata

Use a reverse image search on either:

- [Google](#)
- [Tineye](#)

Be aware that sometimes these searches don't take into account images shared on social media platforms (who often do not allow developers or the public to access their images)!

Always be conscientious when sharing images and photos

Advice:

If you would like to go about subjecting your own photos for a cyberinvestigation, take them yourself with a device equipped with GPS (most current cameras or phones will have one).