Explainer: how law enforcement decodes your photos

June 23 2017, by Richard Matthews

Your photos can tell law enforcement a lot about you. Credit: allen/Flickr, CC BY-ND

For as long as humans have been making images, we have also been manipulating them.

Complex darkroom techniques were once required to modify images but now anyone with a smartphone can apply hundreds of changes using freely available tools.

While this may be convenient for your Instagram feed, it presents a unique challenge for law enforcement. Images cannot always be trusted as an accurate depiction of what occurred.

For example, I recently analysed several photos for the RSPCA showing a duck with a knife embedded in its head to determine if they were photoshopped.

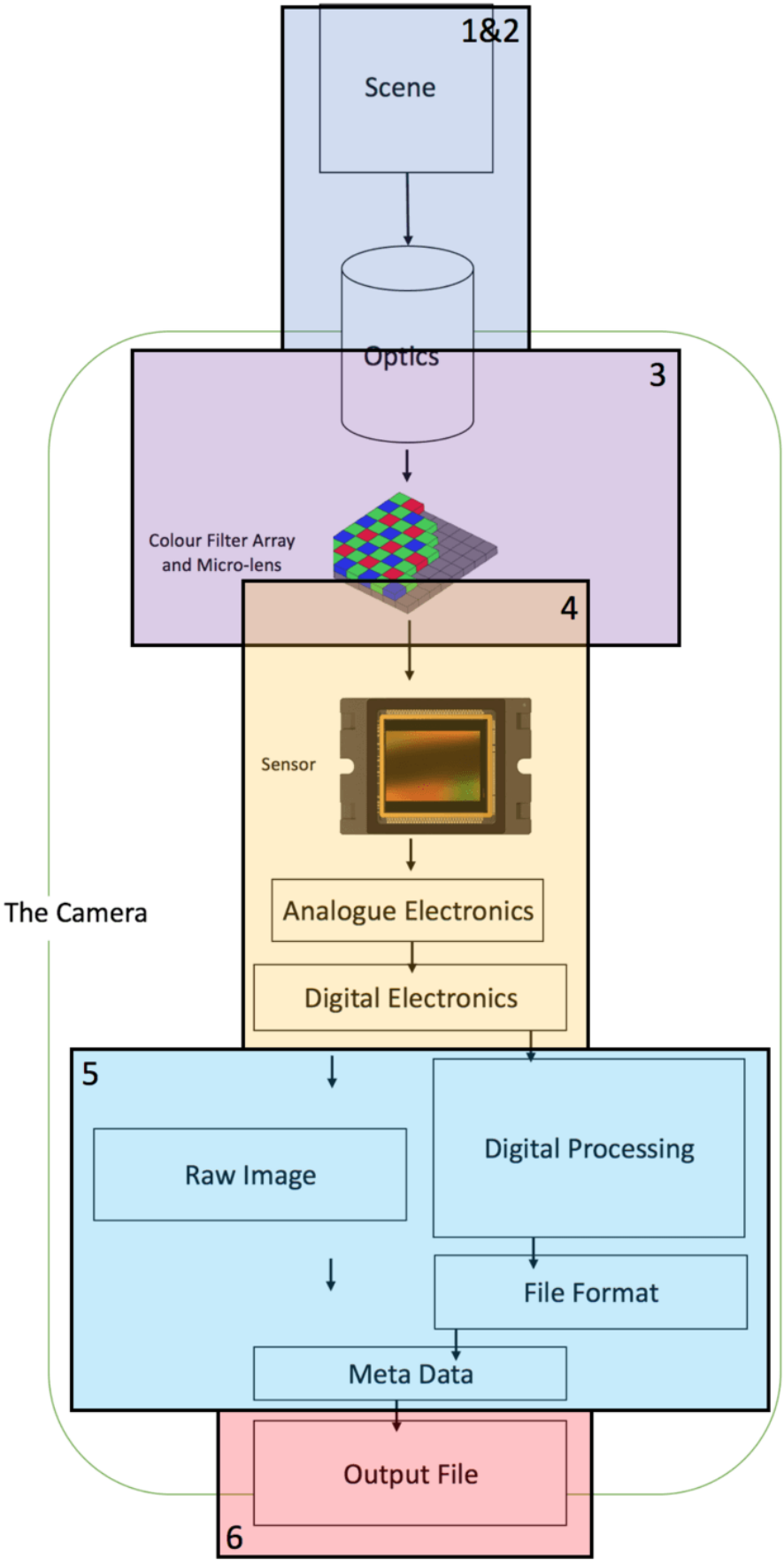
Authorities are increasingly asking images to be verified by forensic experts, but how is this done and where is it headed?

The image pipeline

Analysts currently rely on knowledge of the "image pipeline" to inspect and validate images.

This pipeline is often broken down into six key areas:

1. Physics: shadows, lighting and reflections
2. Geometry: vanishing points, distances within the image and 3-D models
3. Optical: lens distortion or aberrations
4. Image Sensor: fixed pattern noise and colour filter defects
5. File format: metadata, file compression, thumbnails and markers
6. Pixel: scaling, cropping, cloned or resaving


1&2
Scene
Optics
3
Colour Filter Array
and Micro-lens
4
Sensor
The Camera
Analogue Electronics
Digital Electronics
5
Raw Image
Digital Processing
File Format
Meta Data
Output File
6

The image pipeline with each section numerically allocated based on features that investigators are likely to analyse. Credit: Richard Matthews, Author provided

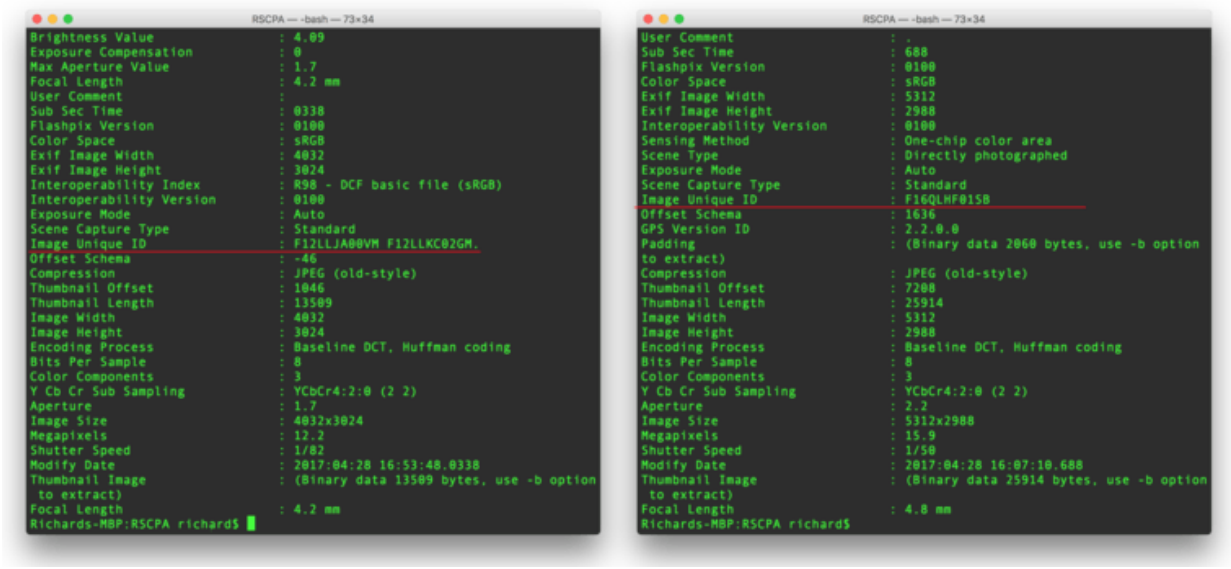
It is often the unseen that begins our investigation rather than the seen. Here we'll be focusing on the metadata captured in images (level 5 in the schema above).

File format forensics: metadata

When an image is saved, the file typically contains data about the image, known as metadata.

There are more than 460 metadata tags within the exchangeable image file format for digital still cameras (EXIF 2.3). This specification helps cameras use formats that can be exchanged between devices – for example, ensuring an iPhone photo appears correctly on a Samsung device.

Tags can include image size, location data, a smaller thumbnail of the image and even the make and model of the camera.



Metadata of one of the images from the left above and the image from the right. These show two separate unique image identifiers which were correlated to a phone camera firmware. Credit: Richard Matthews

Determining which camera took what photo

In a recent investigation, we were able to validate a group of images known as the Byethorne duck.

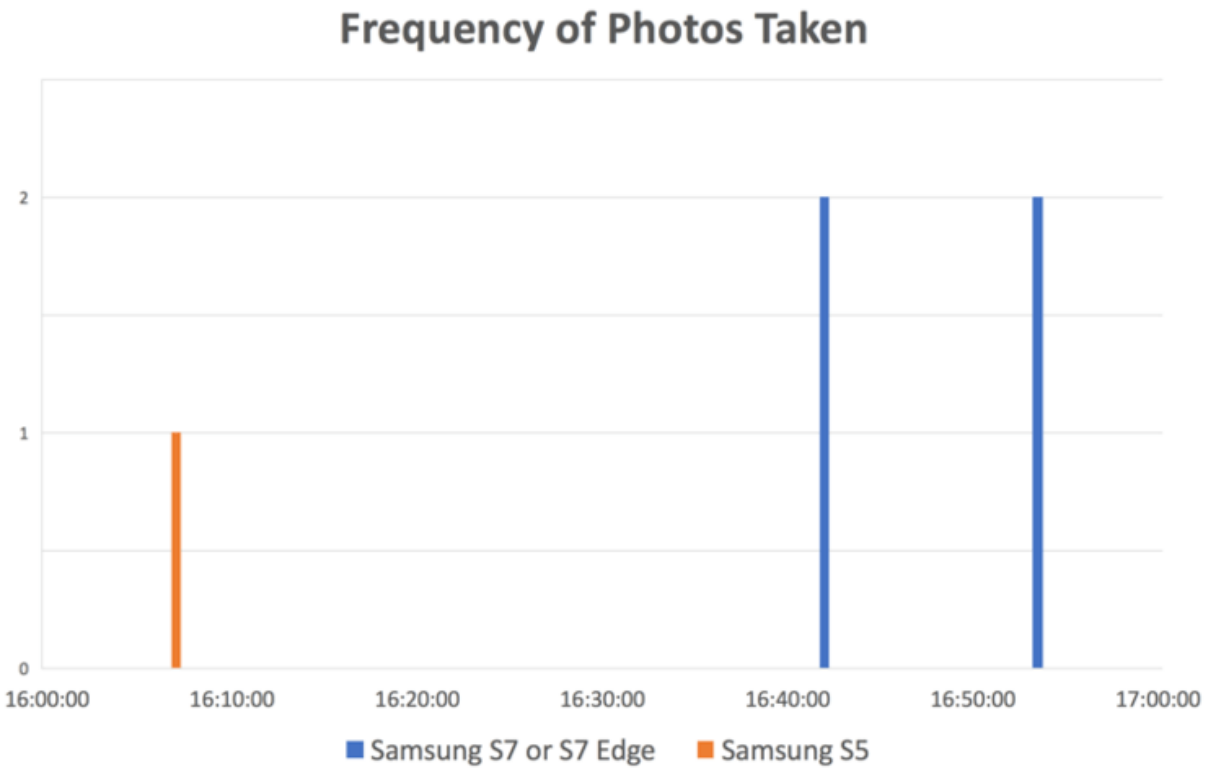
The images supplied by the RSPCA to The Advertiser showed a duck with a knife impaled into its head. Accusations soon emerged that the image was photoshopped.

We inspected the images using Phil Harvey's ExifTool and were able to determine that four of the images (left above) were taken by one camera, with the remainder taken by another.

This was verified using sensor pattern noise and statistical methods. We

extracted a unique fingerprint from each image using signal processing filters and compared how similar they were to each another.

A high value indicates they are very similar and probably correlated, while a low value indicates that they are dissimilar and unlikely to be correlated.



Time the photos were taken and by which camera. Credit: Richard Matthews

When we compared four of the five image fingerprints, we obtained values well above 2,000. Given they're correlated, we can say the images likely came from the same camera.

When we tested the fifth image, the similarity value we obtained was close to zero.

The unique image ID field also contained the camera firmware number. By cross referencing with image and sensor size also contained in the metadata, we suggested that either a Samsung Galaxy S7 or S7 Edge was used to capture the first four images and a Samsung Galaxy S5 was used to capture the fifth.

The time the images were taken was also shown in the metadata, allowing a timeline of when the images were taken and by who to emerge.

Since the photos were taken by two different cameras across the span of around one hour, it is highly unlikely the images were fake.

An RSPCA spokesperson confirmed it received images of the duck from two separate people, which aligns with these findings. To date, there has been insufficient evidence to determine the identity of a perpetrator.

A selection of books on the author's desk. Credit: Richard Matthews

Finding a person's location from an image

The camera model isn't the only thing that can be obtained from metadata.

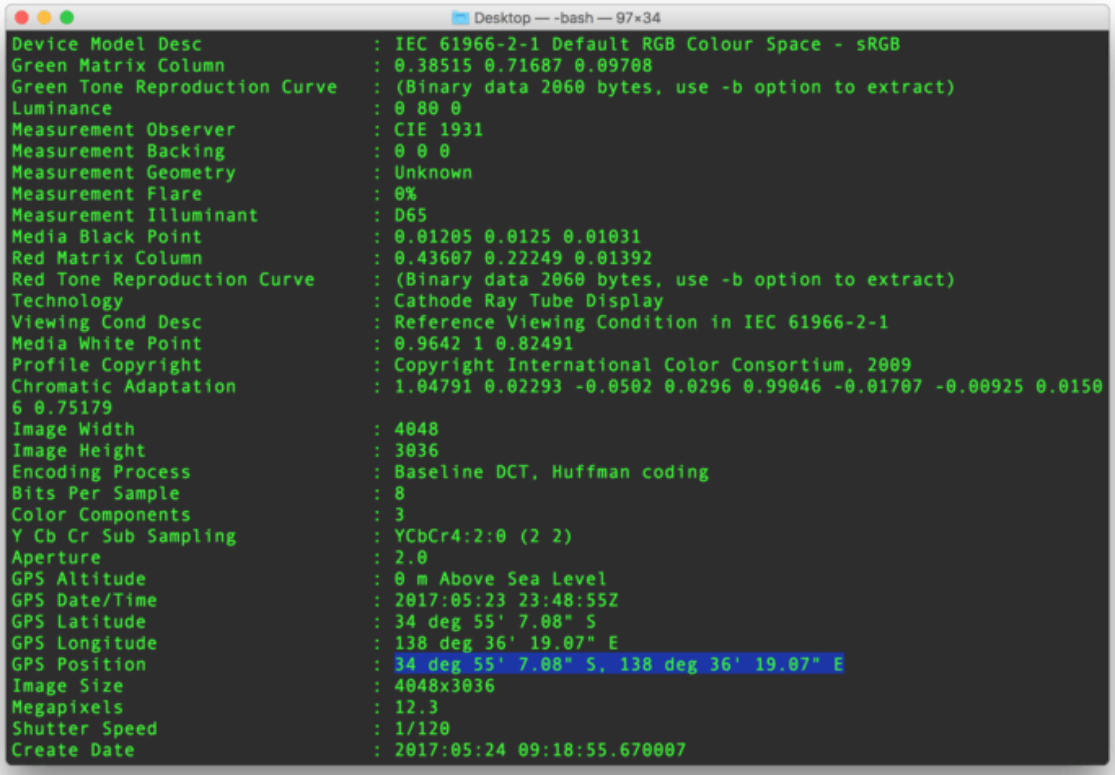
We can see where my office is located by analysing this image of books taken at my desk.

The GPS coordinates are embedded directly in the image metadata. By

placing these coordinates into Google Maps, the exact location of my office is displayed.

This obvious privacy concern is why Facebook, for example, typically removes metadata from uploaded images.

According to a Facebook spokesperson, information including GPS data is automatically removed from photos uploaded onto the platform to protect people "from accidentally sharing private information, such as their location".



Metadata viewed in ExifTool for the bookshelf image. Credit: Richard Matthews

The future of image forensics

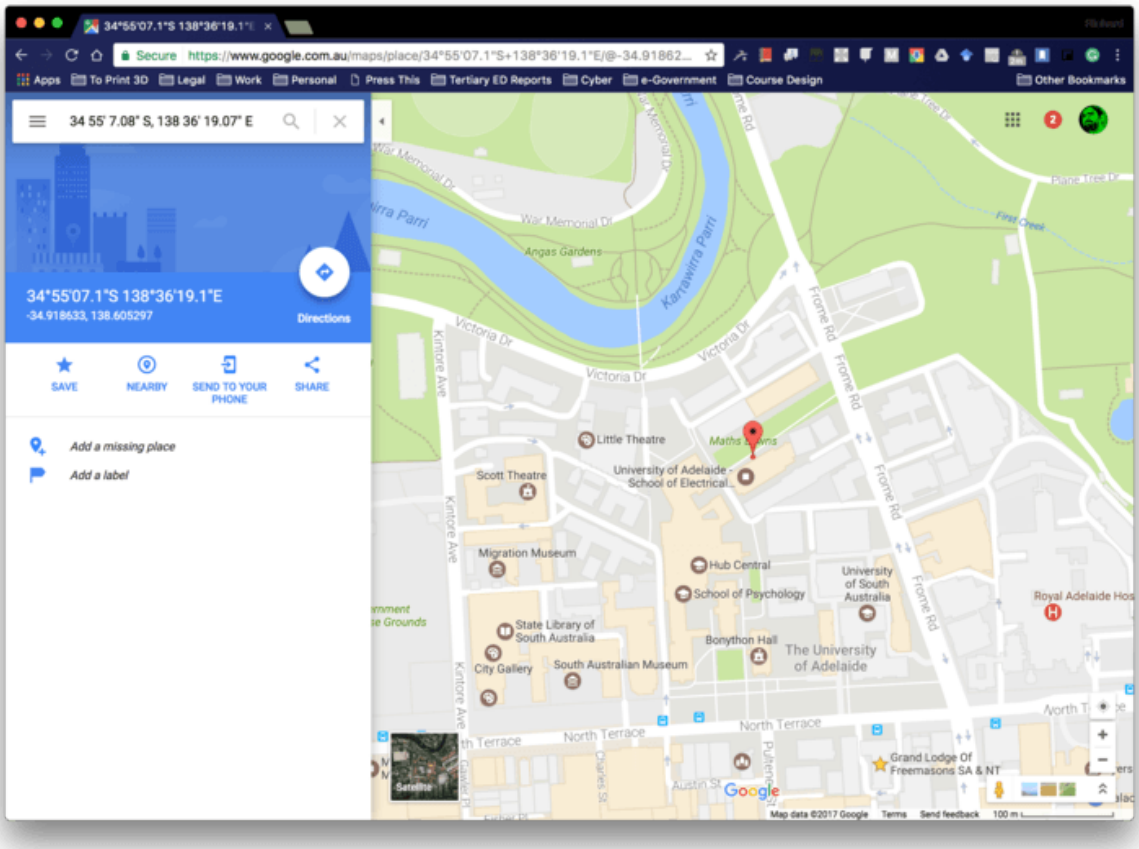
Metadata is never used in isolation.

Authenticating an image to ensure it hasn't been modified and upholding the chain of custody – the paper trail or provenance documentation that goes along with a piece of evidence – is increasingly important to police.

In the future, tools to assist police with this could include audit logs built directly into the camera, or the insertion of a watermark.

I am currently expanding on previous research that suggests each image sensor (the electronic device that actually takes the image) has a unique fingerprint due to the way it reacts non-uniformly to light.

Next time you take a photo, just think about the story it could tell.



The precise location of Richard's office at the University of Adelaide is discovered using the metadata contained within the bookshelf photo. Credit: Richard Matthews

But what happened to the duck? A spokesperson at the RSPCA said:

"We believe the knife may have dislodged shortly after the photos were taken. A duck believed to be the same duck in the photograph has been viewed swimming and behaving normally in the days after giving us the belief that the knife did not penetrate deeply enough to cause significant injury."