Forensics
Week 3 – EXIF Metadata

Date: 3rd October 2025

Course Code: TU856 / TU857 / TU858 yr 4.

TU Dublin – Grangegorman Campus

School of Computer Science

Overview

- What is EXIF Data?

- What does EXIF store?

- Categories of Data Stored in EXIF

- Forensic Importance

- Forensics Usefulness

- EXIF – What to look for

- In-Class Demo

What is EXIF Data?

- EXIF stands for Exchangeable Image File Format.

- It's a metadata standard that stores information about a digital image or media file, usually embedded directly into the file itself.

- Exif is supported by almost all camera manufacturers.

- Example:
  - When you take a photo with a digital camera or smartphone, the device automatically records details about the picture — this is the EXIF metadata.

What does EXIF store

- The metadata tags defined in the Exif standard cover a wide range:
  - Camera settings (camera model and make, lens, shutter speed etc...)
  - Image metrics (Pixel dimensions, resolution, colorspace, and filesize)
  - Date and time information
  - Location Information
  - A thumbnail for previewing the picture
  - Description (text)
  - Copyright Info

Categories of Data Stored in EXIF

- Camera / Device Information
  - Camera make and model (e.g., Nikon D3500, iPhone 14 Pro)
  - Lens type and serial number
  - Firmware or software version

- Image Capture Settings
  - Resolution and dimensions (e.g., 4000 × 3000 pixels)
  - Orientation (portrait/landscape)
  - Exposure time (shutter speed)
  - Aperture (f-stop)
  - ISO sensitivity
  - White balance
  - Focal length
  - Flash (on/off, fired/not fired)

- Date & Time
  - Date and time of capture
  - Time zone (sometimes)

- Geolocation (if GPS is enabled)
  - Latitude & longitude
  - Altitude
  - GPS timestamp
  - Direction (compass heading)

- File & Image Info
  - File size
  - Compression type (JPEG, RAW, etc.)
  - Color space (sRGB, Adobe RGB)
  - Thumbnail preview image

- Editing / Software Info
  - Software used to edit/save the photo (e.g., Adobe Photoshop, GIMP, Snapseed)
  - History of edits (sometimes limited)

Forensic Importance

- Identify device used (helps link suspect's phone/camera to photos).

- Reconstruct events (timestamps, GPS tags).

- Detect tampering (metadata inconsistencies → possible manipulation).

- Chain of evidence (proves authenticity if metadata aligns with logs).

Forensics Usefulness

- What can be useful to a forensic investigation:

- Camera make and model

- Device name

- Time when the picture was taken

- GPS coordinates describing where the picture was taken

- Serial number of the device that took the picture

- Name of the person who took the image

- EXIF data is the information that was available to the device when the picture was taken.

EXIF – What to look for

- Some EXIF data features can be turned off.

- When files are uploaded to web platforms the EXIF metadata can be removed.

- For a forensic investigation it is always good to find pictures relating to the case.

- It will be important to determine where, when, and with what device the pictures were taken.

Example – EXIF Data

- In-Class Demo

Questions