Afternoon Session:

Image and EXIF Forensics

Cyber Taster - Digital Forensics

14/05/2019 – 13:00-15:00

Learning Outcomes

Morning:

- Gain a high level understanding of what Digital Forensics entails
- Develop an understanding of Web Browser Forensics

Afternoon:

- Develop an understanding of Image and EXIF metadata forensics

Structure of Session

- Morning Session: 10:00-12:00
  - Presentation: 45 minutes
    - Introduction to Forensics
    - Web Browser Forensics
  - Workshop: 70 minutes
    - Browser Forensics

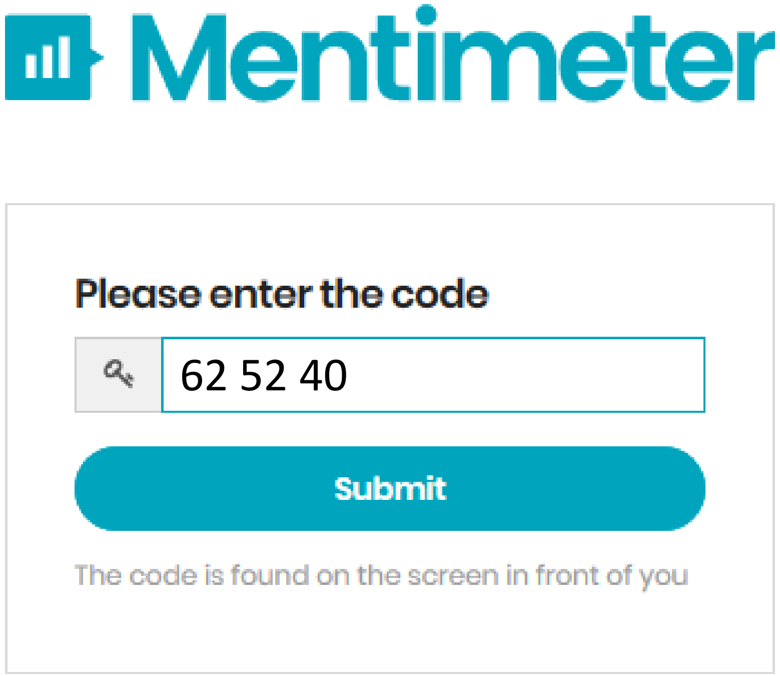
- Afternoon Session : 13:00-15:00
  - Presentation: 45 minutes
    - Image and EXIF Forensics
  - Workshop: 70 minutes
    - Image and EXIF Forensics

All resources for today can be found at:
https://github.com/smck1/taste_of_cyber

Questions

- Submit a question

- Go to: menti.com
- Code: 62 52 40



Please enter the code

62 52 40

The code is found on the screen in front of you

Image Forensics

Why Image Forensics?

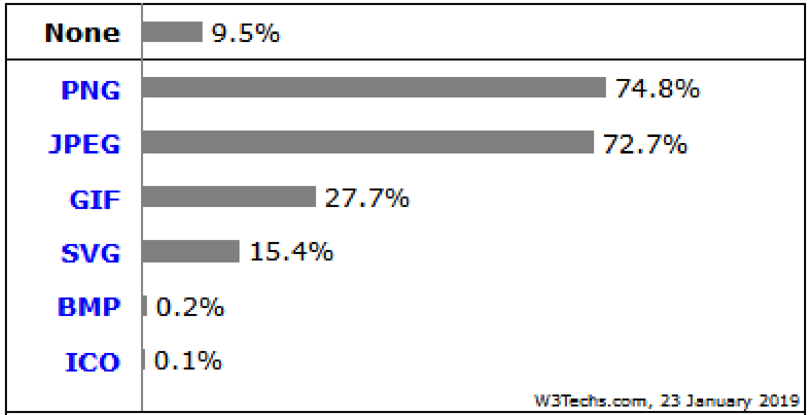
- Most public sector forensics deals with the analysis of illegal images/videos
- Understanding the fundamentals of how images are stored allows the forensics expert to better comprehend such forensic artefacts
  - Structure of files as you would expect on disk
  - How manipulations could affect the evidence
  - Verify the authenticity / source of an image

A note on compression

- Uncompressed
  - No tricks are used to reduce the size of the data as it is stored
  - E.g. filetypes: DD, RAW, WAV
- Lossless compression
  - Data reduction does not involve any loss of signal / resolution
    - i.e. compressing and uncompressing the data results in the same data
  - E.g. filetypes: EO1, PNG, FLAC
- Lossy compression
  - Some of the signal is lost during the compression process and cannot be recovered
  - E.g. filetypes: JPEG, MP3, video codecs (h264)

JPEG – The De-facto Image Standard

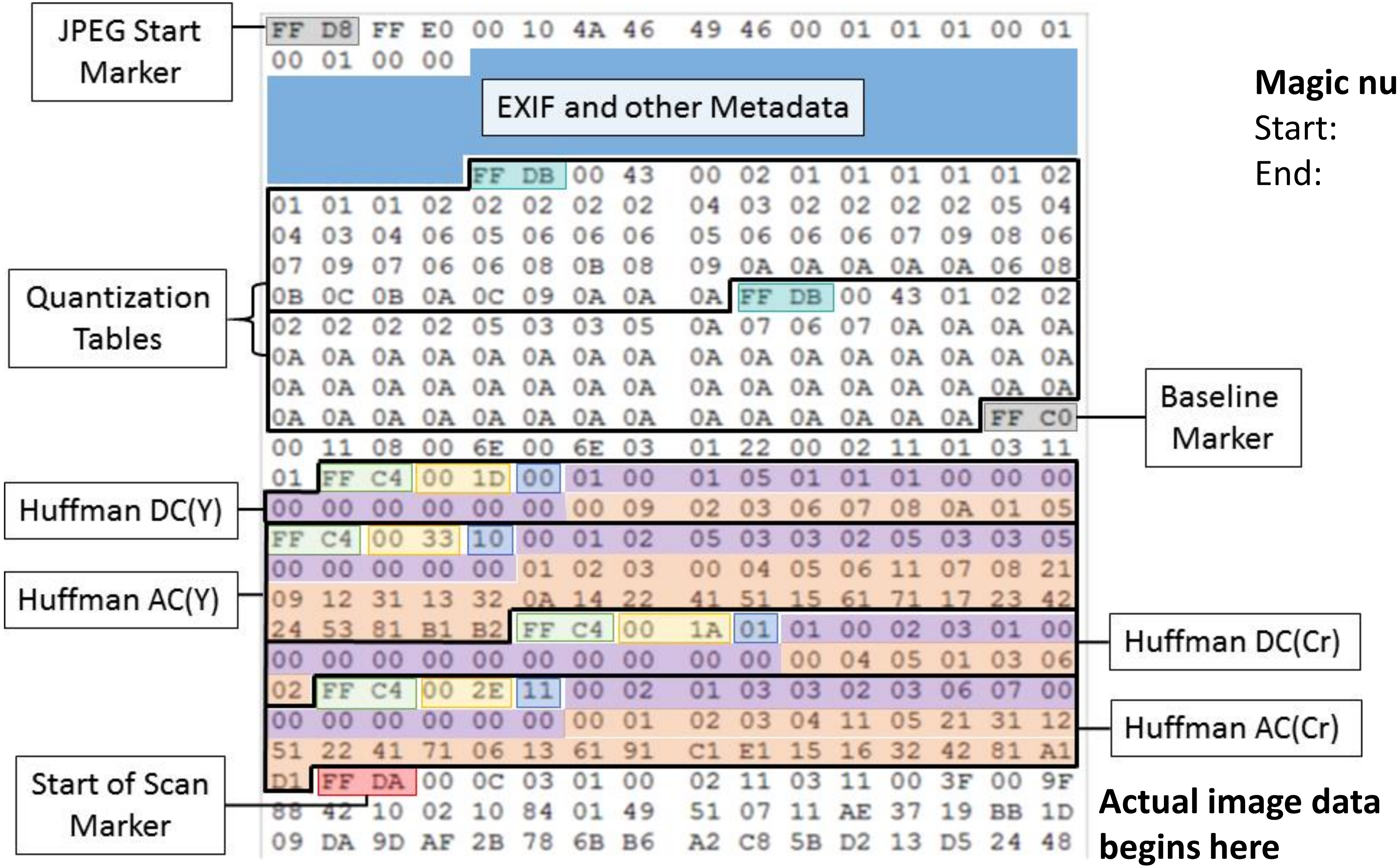
- JPEG is currently the most common lossy image compression scheme in existence
  - Technically also has a seldom used lossless mode
- Used by most cameras (though some use RAW format)
- Very widespread on the internet
- Much smaller file sizes than BMP / PNG (for natural images)



Percentages of websites using various image file formats
Note: a website may use more than one image file format

JPEG compression artefacts

JPEG Structure on Disk



```
FF D8 FF E0 00 10 4A 46  49 46 00 01 01 01 00 01
00 01 00 00
            FF DB 00 43  00 02 01 01 01 01 01 02
01 01 01 02 02 02 02 02  04 03 02 02 02 02 05 04
04 03 04 06 05 06 06 06  05 06 06 06 07 09 08 06
07 09 07 06 06 08 0B 08  09 0A 0A 0A 0A 0A 06 08
0B 0C 0B 0A 0C 09 0A 0A  0A FF DB 00 43 01 02 02
02 02 02 02 05 03 03 05  0A 07 06 07 0A 0A 0A 0A
0A 0A 0A 0A 0A 0A 0A 0A  0A 0A 0A 0A 0A 0A 0A 0A
0A 0A 0A 0A 0A 0A 0A 0A  0A 0A 0A 0A 0A 0A 0A 0A
0A 0A 0A 0A 0A 0A 0A 0A  0A 0A 0A 0A 0A 0A FF C0
00 11 08 00 6E 00 6E 03  01 22 00 02 11 01 03 11
01 FF C4 00 1D 00 01 00  01 05 01 01 01 00 00 00
00 00 00 00 00 00 00 09  02 03 06 07 08 0A 01 05
FF C4 00 33 10 00 01 02  05 03 03 02 05 03 03 05
00 00 00 00 00 01 02 03  00 04 05 06 11 07 08 21
09 12 31 13 32 0A 14 22  41 51 15 61 71 17 23 42
24 53 81 B1 B2 FF C4 00  1A 01 01 00 02 03 01 00
00 00 00 00 00 00 00 00  00 00 00 04 05 01 03 06
02 FF C4 00 2E 11 00 02  01 03 03 02 03 06 07 00
00 00 00 00 00 00 00 01  02 03 04 11 05 21 31 12
51 22 41 71 06 13 61 91  C1 E1 15 16 32 42 81 A1
D1 FF DA 00 0C 03 01 00  02 11 03 11 00 3F 00 9F
88 42 10 02 10 84 01 49  51 07 11 AE 37 19 BB 1D
09 DA 9D AF 2B 78 6B B6  A2 C8 5B D2 13 D5 24 48
```

Magic numbers:

Start:	0xFF D8
End:	0xFF D9

Other Image Formats

Something other than JPEG

Common Image Formats – bmp/gif

- **BMP** (.bmp, .dib) – Bitmap
  - Lossless or no compression
  - Contains an array of all pixel colours
  - Colour information and ICC profiles as metadata

```
Header:     42 4D     BM

Windows (or device-
independent) bitmap image

No Footer: Bytes 2-5 contain
the file length in little-
endian order.
```

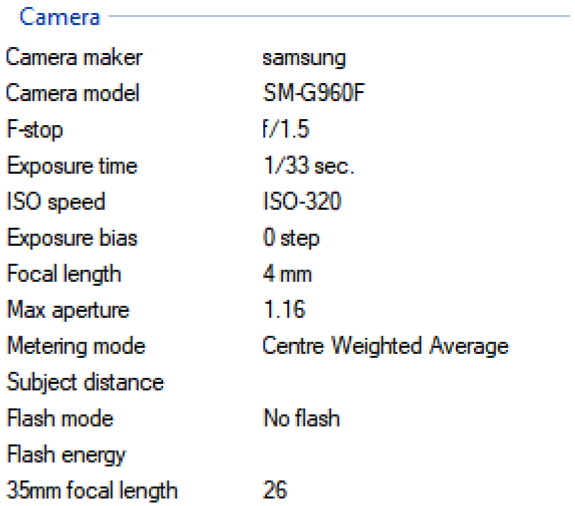
- **GIF** (.gif) – Graphics Interchange Format
  - Two versions, 1987/1989
  - Palette based
  - Limited colours
  - LZW encoding
  - Supports animation (89a) using multiple image frames rendered with a delay

```
Header:  47 49 46 38 37 61     GIF87a
     or  47 49 46 38 39 61     GIF89a
Footer:  00 3B                 .;
```

Common Image Formats - png

- **PNG** (.png) – Portable Network Graphics
  - Lossless compression
  - Breaks file into metadata and data “chunks”
  - Each line of pixels is encoded separately, data is stored in “IDAT” chunks
  - IDAT chunks are ZLIB containers using the DEFLATE algorithm
  - Supports transparency, good at solid colours
  - Has an animated variant! (APNG)

```
Header:   89 50 4E 47 0D 0A 1A 0A     ‰PNG....
Trailer:  49 45 4E 44 AE 42 60 82     IEND®B`,
```



Camera

Camera maker	samsung
Camera model	SM-G960F
F-stop	f/1.5
Exposure time	1/33 sec.
ISO speed	ISO-320
Exposure bias	0 step
Focal length	4 mm
Max aperture	1.16
Metering mode	Centre Weighted Average
Subject distance	
Flash mode	No flash
Flash energy	
35mm focal length	26

Image Metadata

Data about data

What is Metadata?

- Metadata is data about data.
  - It can provide corroborating information about the document data itself
  - It can reveal information that someone tried to hide, delete, or obscure.
  - It can be used to automatically correlate documents from different sources

- Some kinds of metadata that are interesting in computer forensics:
  - File system metadata (e.g. MAC times, access control lists, etc.)
  - Digital image metadata. Although information such as the image size and number of colours are technically metadata, JPEG and other file formats store additional data about the photo or the device that acquired it
  - Document metadata, such as the creator of a document, it's last print time, etc.

http://www.forensicswiki.org

Common JPEG APP Markers

APP0 – **JFIF**: version no./aspect ratio/pixel density

APP1 – **EXIF**: camera/phone metadata such as model numbers, settings, geolocation, thumbnail

APP1 – **XMP**: Adobe metadata format

APP2 – **ICC**: colour profiles for displaying the image

APP3 – **META**: same format as EXIF

APP13 – **Photoshop**: Software version, other metadata, thumbnail

APP14 – **Adobe**: Some extra decoding information

EXIF Metadata Includes

Date and Time – Most digital cameras will record the current date and time.

Physical Location – GPS enabled cameras, especially smartphones can geotag photos with exact GPS co-ordinates of where the photo was taken.

Dimensions – Image resolution, compression, width and height (measured in pixels).

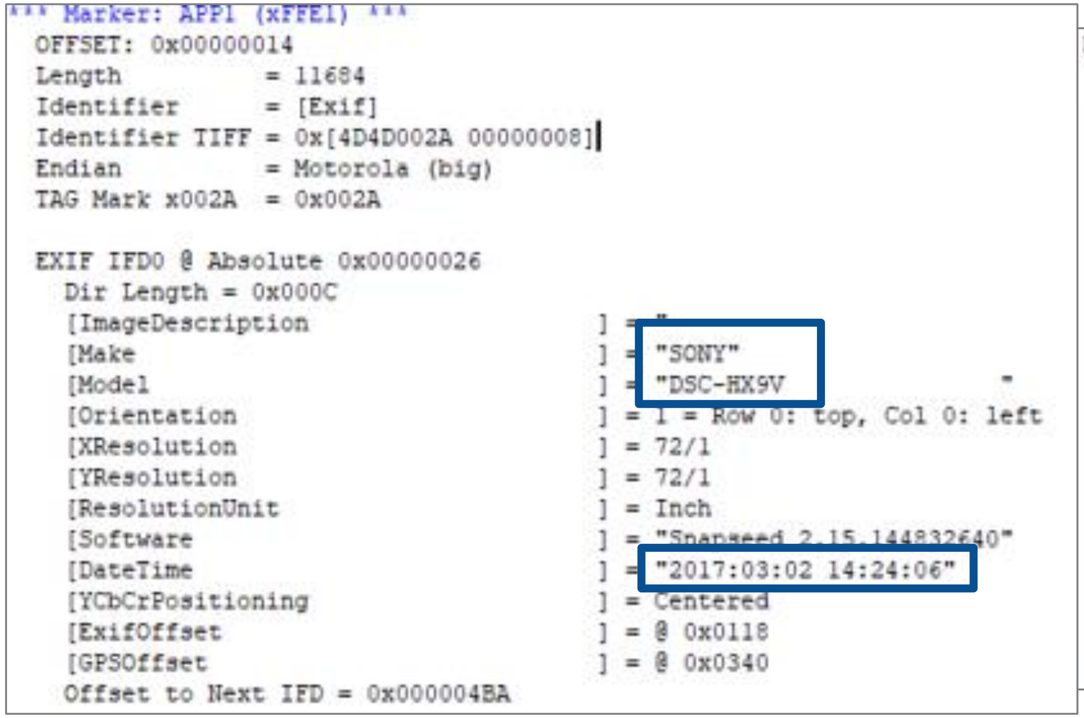
Variable Camera Settings – including the shutter speed, exposure time, aperture, focal length, metering mode, ISO speed, and camera orientation (rotation) at the time the photo was taken and whether or not a flash was used.

Fixed Camera Information – such as the make, model, serial number and if a lens was used it may also store information about the lens as well.

Thumbnail – a smaller version of the original image is stored for quick viewing on the camera’s LCD screen, file managers and photo manipulation software.

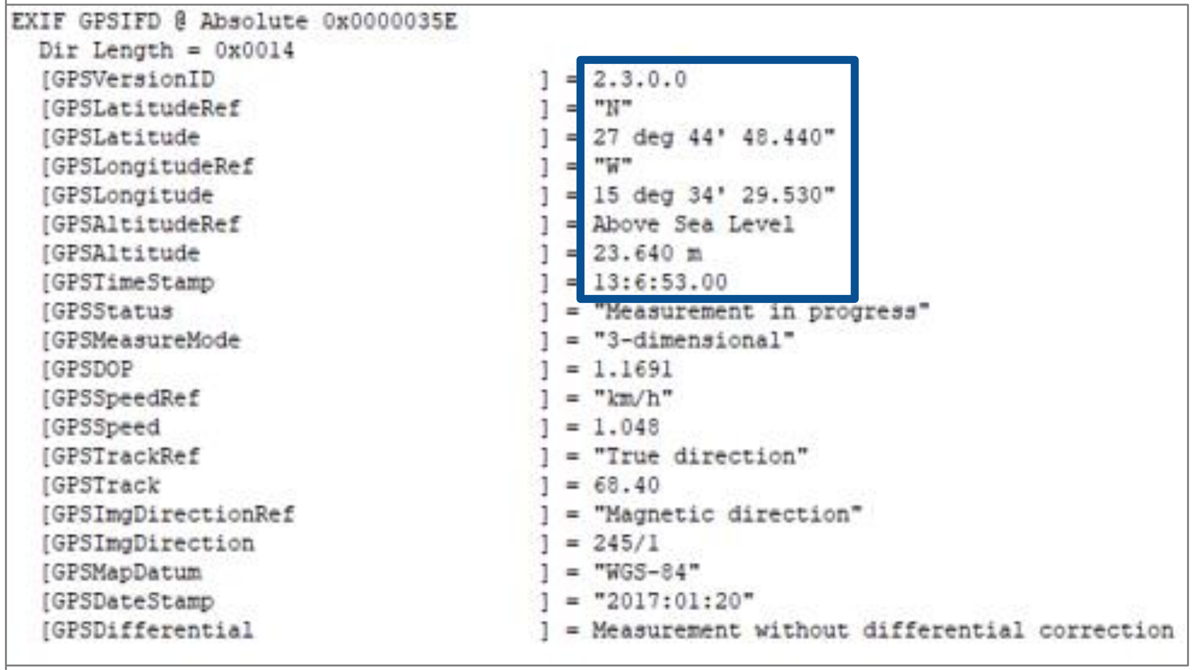
Copyright notice – if set in the camera settings

Example EXIF (JPEGsnoop)

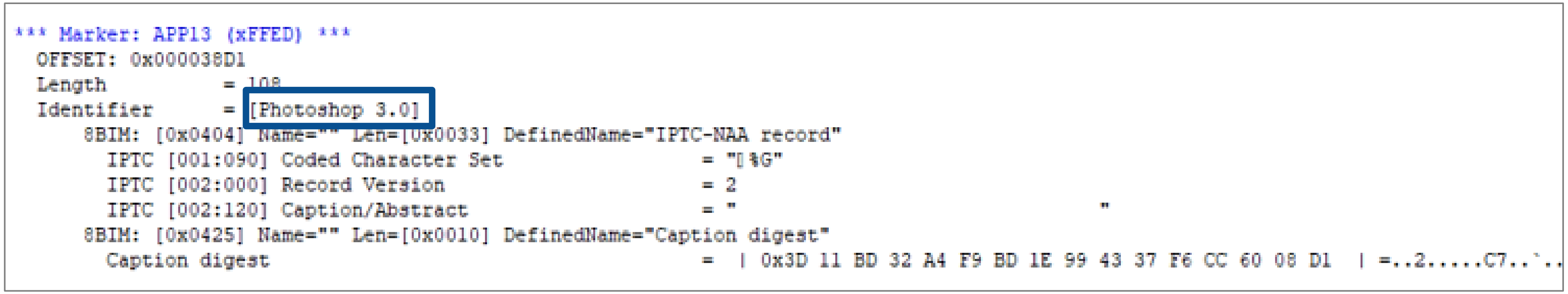


```
*** Marker: APP1 (xFFE1) ***
  OFFSET: 0x00000014
  Length          = 11684
  Identifier      = [Exif]
  Identifier TIFF = 0x[4D4D002A 00000008]
  Endian          = Motorola (big)
  TAG Mark x002A  = 0x002A

  EXIF IFD0 @ Absolute 0x00000026
    Dir Length = 0x000C
    [ImageDescription                    ] = "
    [Make                                ] = "SONY"
    [Model                               ] = "DSC-HX9V                  "
    [Orientation                         ] = 1 = Row 0: top, Col 0: left
    [XResolution                         ] = 72/1
    [YResolution                         ] = 72/1
    [ResolutionUnit                      ] = Inch
    [Software                            ] = "Snapseed 2.15.144832640"
    [DateTime                            ] = "2017:03:02 14:24:06"
    [YCbCrPositioning                    ] = Centered
    [ExifOffset                          ] = @ 0x0118
    [GPSOffset                           ] = @ 0x0340
    Offset to Next IFD = 0x000004BA
```



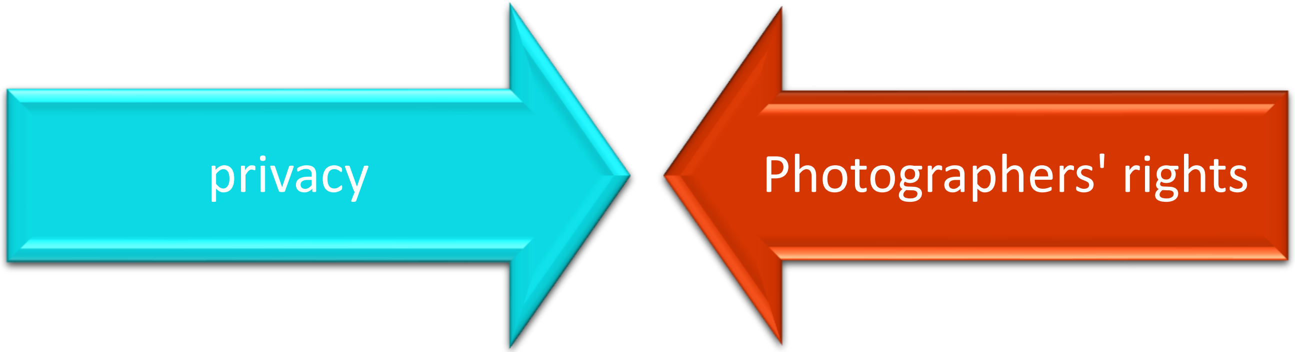
```
EXIF GPSIFD @ Absolute 0x0000035E
  Dir Length = 0x0014
  [GPSVersionID                    ] = 2.3.0.0
  [GPSLatitudeRef                  ] = "N"
  [GPSLatitude                     ] = 27 deg 44' 48.440"
  [GPSLongitudeRef                 ] = "W"
  [GPSLongitude                    ] = 15 deg 34' 29.530"
  [GPSAltitudeRef                  ] = Above Sea Level
  [GPSAltitude                     ] = 23.640 m
  [GPSTimeStamp                    ] = 13:6:53.00
  [GPSStatus                       ] = "Measurement in progress"
  [GPSMeasureMode                  ] = "3-dimensional"
  [GPSDOP                          ] = 1.1691
  [GPSSpeedRef                     ] = "km/h"
  [GPSSpeed                        ] = 1.048
  [GPSTrackRef                     ] = "True direction"
  [GPSTrack                        ] = 68.40
  [GPSImgDirectionRef              ] = "Magnetic direction"
  [GPSImgDirection                 ] = 245/1
  [GPSMapDatum                     ] = "WGS-84"
  [GPSDateStamp                    ] = "2017:01:20"
  [GPSDifferential                 ] = Measurement without differential correction
```



```
*** Marker: APP13 (xFFED) ***
  OFFSET: 0x000038D1
  Length          = 108
  Identifier      = [Photoshop 3.0]
      8BIM: [0x0404] Name="" Len=[0x0033] DefinedName="IPTC-NAA record"
        IPTC [001:090] Coded Character Set                  = "[%G"
        IPTC [002:000] Record Version                       = 2
        IPTC [002:120] Caption/Abstract                     = "                              "
      8BIM: [0x0425] Name="" Len=[0x0010] DefinedName="Caption digest"
        Caption digest                                      =  | 0x3D 11 BD 32 A4 F9 BD 1E 99 43 37 F6 CC 60 08 D1  | =..2.....C7..`..
```

EXIF and Social Media

- What happens when you upload a photo to social media?
- Depending on the site, photo may be resized and EXIF info stripped out
  - e.g. Facebook will strip, but retain any copyright notice
  - Google+ retains all metadata (still?)

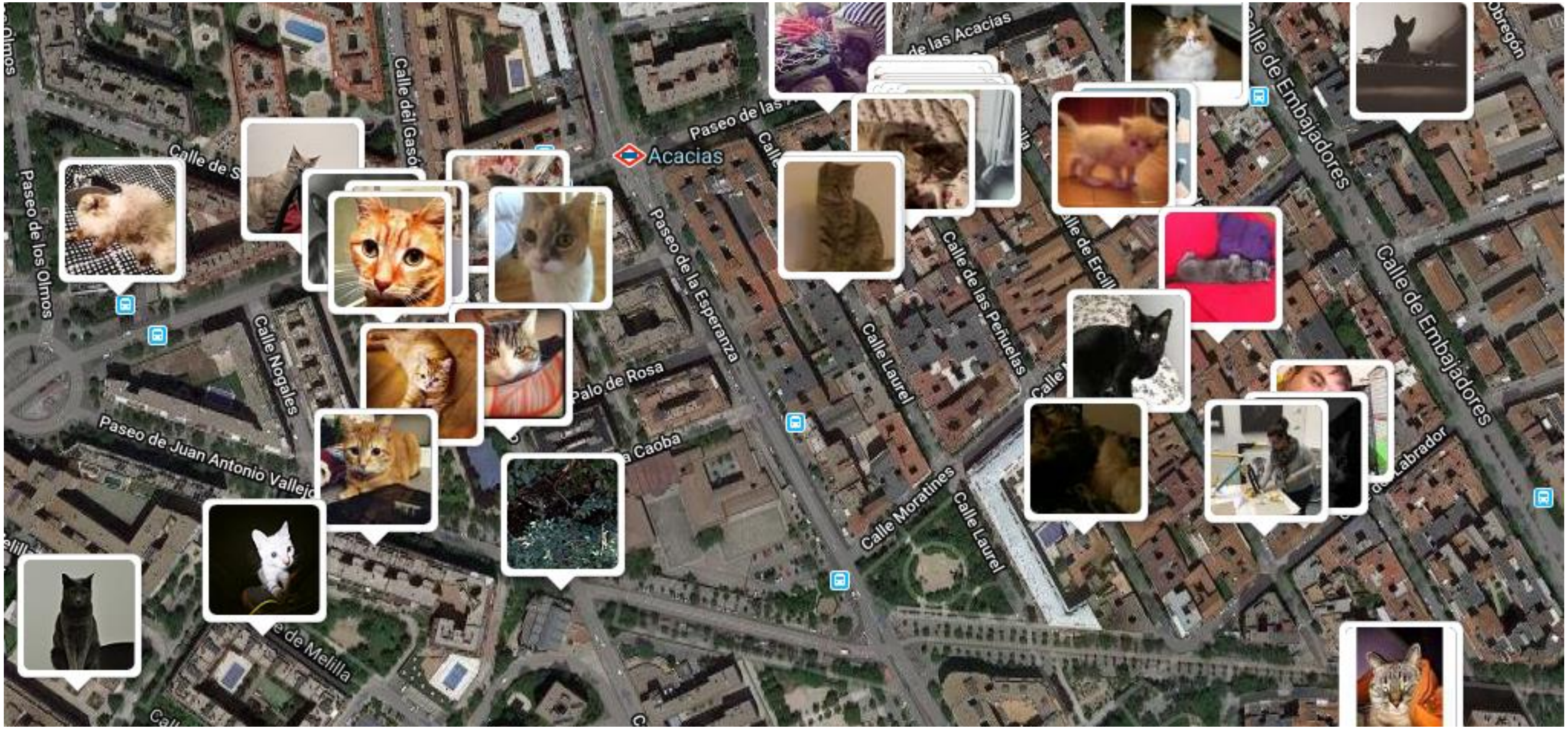


privacy

Photographers' rights

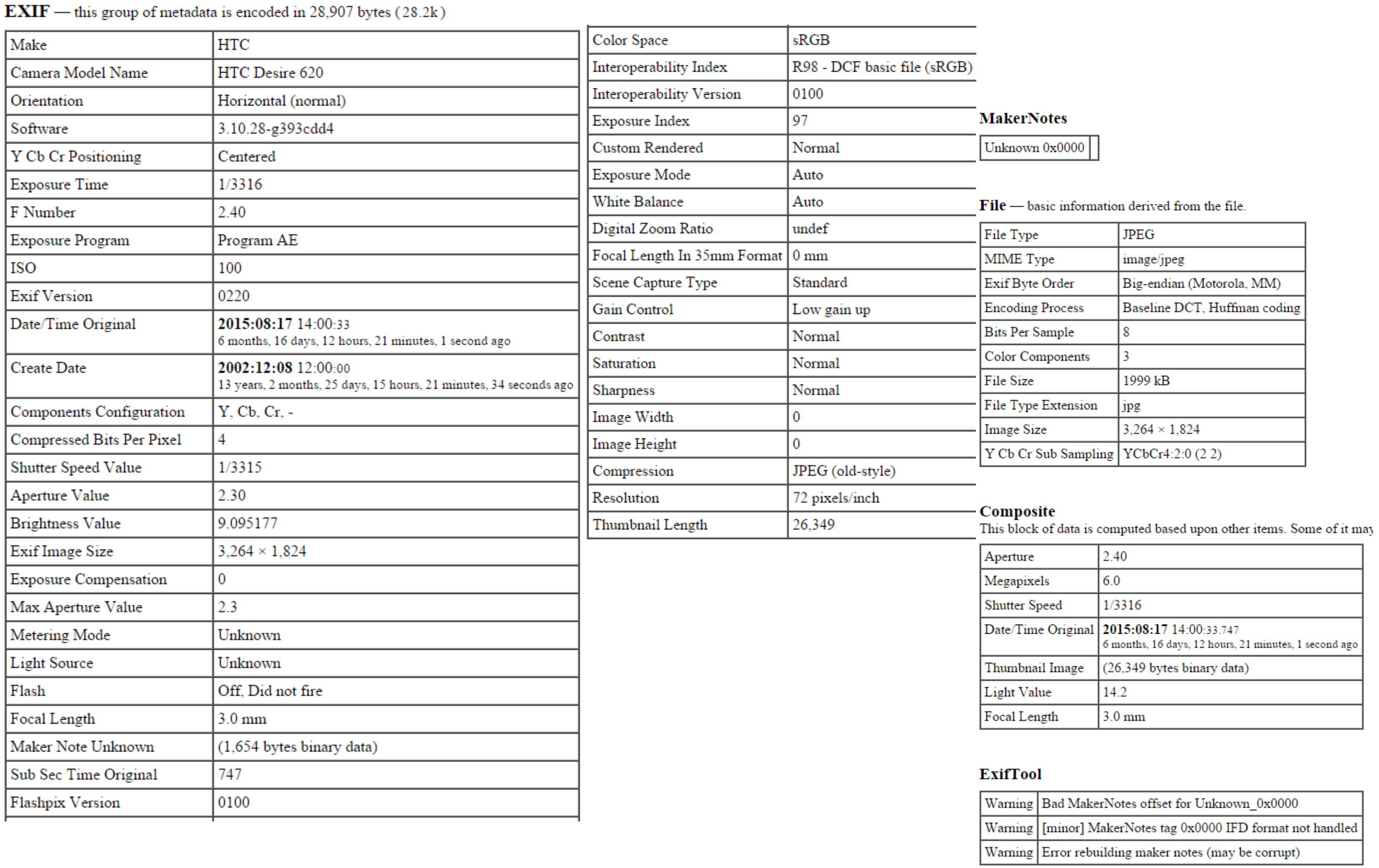
I Know Where Your Cat Lives

https://iknowwhereyourcatlives.com/



Stripped Metadata Example

Original



EXIF — this group of metadata is encoded in 28,907 bytes (28.2k)

Make	HTC
Camera Model Name	HTC Desire 620
Orientation	Horizontal (normal)
Software	3.10.28-g393cdd4
Y Cb Cr Positioning	Centered
Exposure Time	1/3316
F Number	2.40
Exposure Program	Program AE
ISO	100
Exif Version	0220
Date/Time Original	**2015:08:17** 14:00:33 6 months, 16 days, 12 hours, 21 minutes, 1 second ago
Create Date	**2002:12:08** 12:00:00 13 years, 2 months, 25 days, 15 hours, 21 minutes, 34 seconds ago
Components Configuration	Y, Cb, Cr, -
Compressed Bits Per Pixel	4
Shutter Speed Value	1/3315
Aperture Value	2.30
Brightness Value	9.095177
Exif Image Size	3,264 × 1,824
Exposure Compensation	0
Max Aperture Value	2.3
Metering Mode	Unknown
Light Source	Unknown
Flash	Off, Did not fire
Focal Length	3.0 mm
Maker Note Unknown	(1,654 bytes binary data)
Sub Sec Time Original	747
Flashpix Version	0100

Color Space	sRGB
Interoperability Index	R98 - DCF basic file (sRGB)
Interoperability Version	0100
Exposure Index	97
Custom Rendered	Normal
Exposure Mode	Auto
White Balance	Auto
Digital Zoom Ratio	undef
Focal Length In 35mm Format	0 mm
Scene Capture Type	Standard
Gain Control	Low gain up
Contrast	Normal
Saturation	Normal
Sharpness	Normal
Image Width	0
Image Height	0
Compression	JPEG (old-style)
Resolution	72 pixels/inch
Thumbnail Length	26,349

MakerNotes

Unknown 0x0000

File — basic information derived from the file.

File Type	JPEG
MIME Type	image/jpeg
Exif Byte Order	Big-endian (Motorola, MM)
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
File Size	1999 kB
File Type Extension	jpg
Image Size	3,264 × 1,824
Y Cb Cr Sub Sampling	YCbCr4:2:0 (2 2)

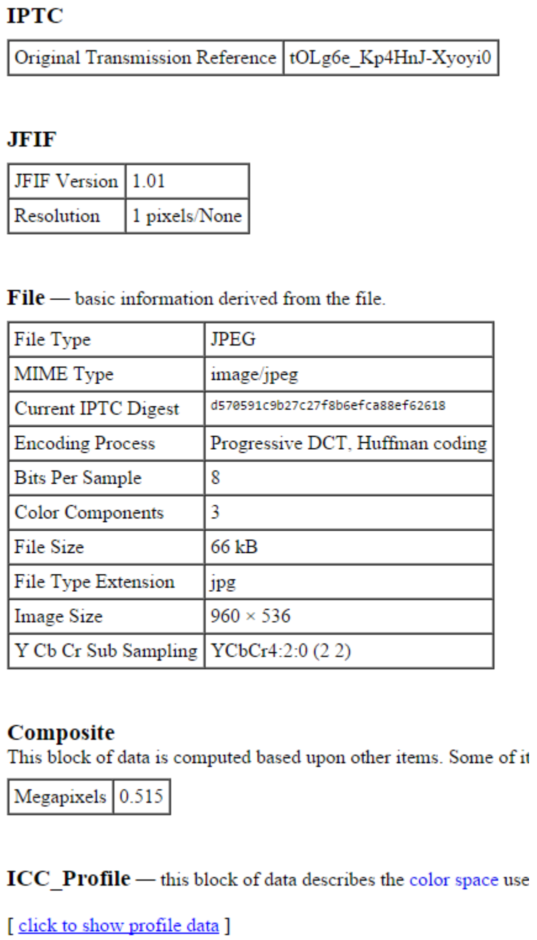
Composite
This block of data is computed based upon other items. Some of it may

Aperture	2.40
Megapixels	6.0
Shutter Speed	1/3316
Date/Time Original	**2015:08:17** 14:00:33.747 6 months, 16 days, 12 hours, 21 minutes, 1 second ago
Thumbnail Image	(26,349 bytes binary data)
Light Value	14.2
Focal Length	3.0 mm

ExifTool

Warning	Bad MakerNotes offset for Unknown_0x0000
Warning	[minor] MakerNotes tag 0x0000 IFD format not handled
Warning	Error rebuilding maker notes (may be corrupt)

Facebook



IPTC

Original Transmission Reference	tOLg6e_Kp4HnJ-Xyoyi0

JFIF

JFIF Version	1.01
Resolution	1 pixels/None

File — basic information derived from the file.

File Type	JPEG
MIME Type	image/jpeg
Current IPTC Digest	d570591c9b27c27f8b6efca88ef62618
Encoding Process	Progressive DCT, Huffman coding
Bits Per Sample	8
Color Components	3
File Size	66 kB
File Type Extension	jpg
Image Size	960 × 536
Y Cb Cr Sub Sampling	YCbCr4:2:0 (2 2)

Composite
This block of data is computed based upon other items. Some of it

Megapixels	0.515

ICC_Profile — this block of data describes the color space use

[click to show profile data]

Image Source Verification

Image Source and Modification

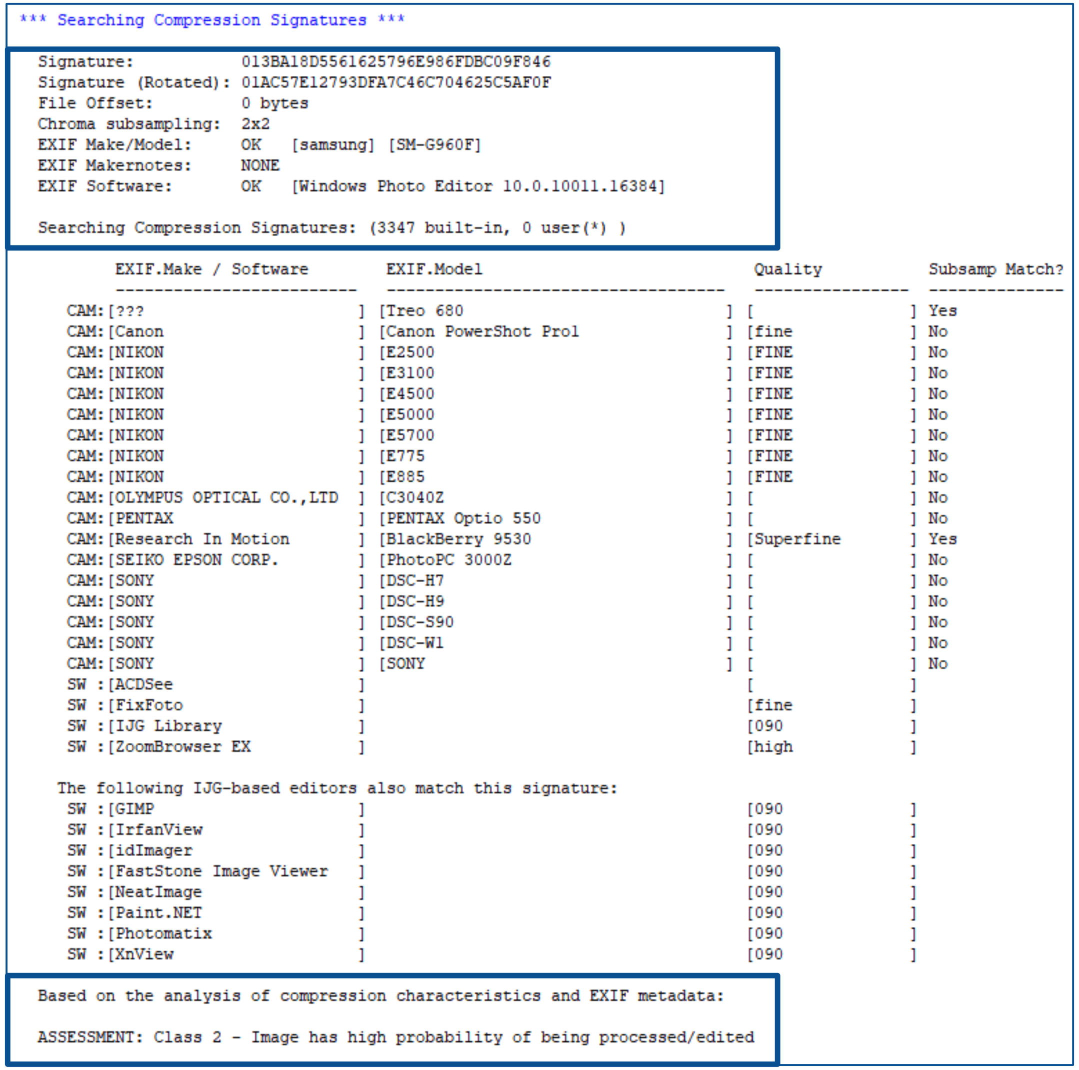
- An important part of forensics is image verification
  - Where did it come from?
  - Is it original?
  - Has it been edited?
- Our knowledge about how JPEG works helps us answer these questions
  - Do the quantization tables match the camera reported in EXIF? Do they match Photoshop’s tables?
  - Are the Huffman tables what we expect?
  - Is the structure of the metadata what we expect?

Signature Databases

- Possible to build databases for common software and cameras

- JPEGsnoop is decent at detecting the source and determining if modification has occurred

- Can we trust these signatures?



```
*** Searching Compression Signatures ***

  Signature:           013BA18D5561625796E986FDBC09F846
  Signature (Rotated): 01AC57E12793DFA7C46C704625C5AF0F
  File Offset:         0 bytes
  Chroma subsampling:  2x2
  EXIF Make/Model:     OK   [samsung] [SM-G960F]
  EXIF Makernotes:     NONE
  EXIF Software:       OK   [Windows Photo Editor 10.0.10011.16384]

  Searching Compression Signatures: (3347 built-in, 0 user(*) )

         EXIF.Make / Software       EXIF.Model                             Quality          Subsamp Match?
         ------------------------   ------------------------------------   ----------------  --------------
    CAM:[???                     ] [Treo 680                            ] [                ] Yes
    CAM:[Canon                   ] [Canon PowerShot Pro1                ] [fine            ] No
    CAM:[NIKON                   ] [E2500                               ] [FINE            ] No
    CAM:[NIKON                   ] [E3100                               ] [FINE            ] No
    CAM:[NIKON                   ] [E4500                               ] [FINE            ] No
    CAM:[NIKON                   ] [E5000                               ] [FINE            ] No
    CAM:[NIKON                   ] [E5700                               ] [FINE            ] No
    CAM:[NIKON                   ] [E775                                ] [FINE            ] No
    CAM:[NIKON                   ] [E885                                ] [FINE            ] No
    CAM:[OLYMPUS OPTICAL CO.,LTD ] [C3040Z                              ] [                ] No
    CAM:[PENTAX                  ] [PENTAX Optio 550                    ] [                ] No
    CAM:[Research In Motion      ] [BlackBerry 9530                     ] [Superfine       ] Yes
    CAM:[SEIKO EPSON CORP.       ] [PhotoPC 3000Z                       ] [                ] No
    CAM:[SONY                    ] [DSC-H7                              ] [                ] No
    CAM:[SONY                    ] [DSC-H9                              ] [                ] No
    CAM:[SONY                    ] [DSC-S90                             ] [                ] No
    CAM:[SONY                    ] [DSC-W1                              ] [                ] No
    CAM:[SONY                    ] [SONY                                ] [                ] No
    SW :[ACDSee                  ]                                        [                ]
    SW :[FixFoto                 ]                                        [fine            ]
    SW :[IJG Library             ]                                        [090             ]
    SW :[ZoomBrowser EX          ]                                        [high            ]

   The following IJG-based editors also match this signature:
    SW :[GIMP                    ]                                        [090             ]
    SW :[IrfanView               ]                                        [090             ]
    SW :[idImager                ]                                        [090             ]
    SW :[FastStone Image Viewer  ]                                        [090             ]
    SW :[NeatImage               ]                                        [090             ]
    SW :[Paint.NET               ]                                        [090             ]
    SW :[Photomatix              ]                                        [090             ]
    SW :[XnView                  ]                                        [090             ]

  Based on the analysis of compression characteristics and EXIF metadata:

  ASSESSMENT: Class 2 - Image has high probability of being processed/edited
```

Pixel Level Verification

- Another approach is to make use of the imperfections inherent to camera technologies
- Like a fingerprint no camera is identical – signatures left by:
  - Camera lenses, Image sensors
  - Colour filters, Image post-processing
- However this takes much more effort to verify, requiring the original camera
  - Requires reference images taken in completely dark and completely white scenarios

Thumbnails

Embedded in files and OS caches

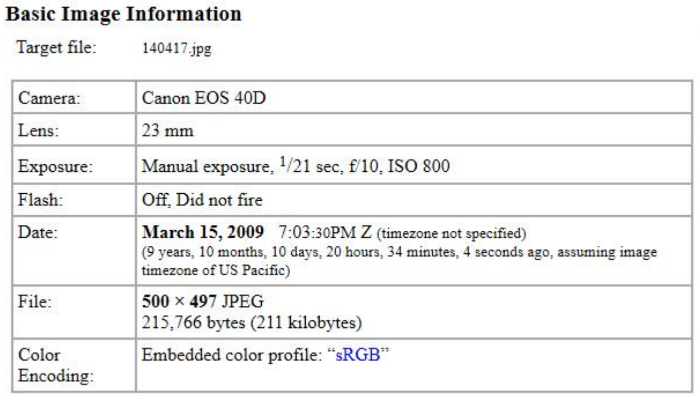
Embedded Thumbnails

- Lower resolution image previews (thumbnails) are frequently embedded in a file for use by cameras/software

- In JPEG this can appear in at least three different APP markers:
  - **APP1 (JFIF)** / **APP2 (EXIF)** / **APP13 (Photoshop)**
  - A smaller, complete, JPEG within a JPEG (JPEGception)

Embedded Thumbnail Example

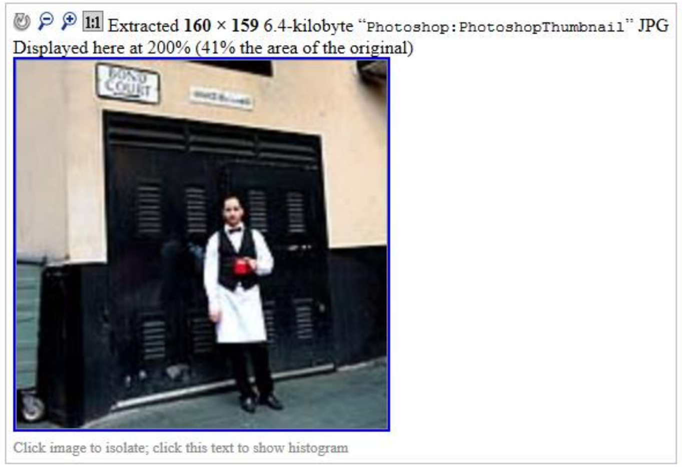
- Stored in APP13 (Photoshop)



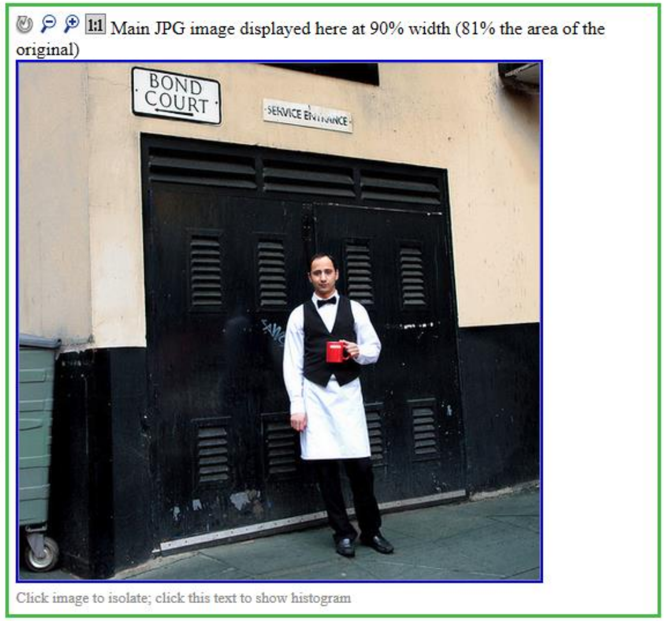
Basic Image Information

Target file: 140417.jpg

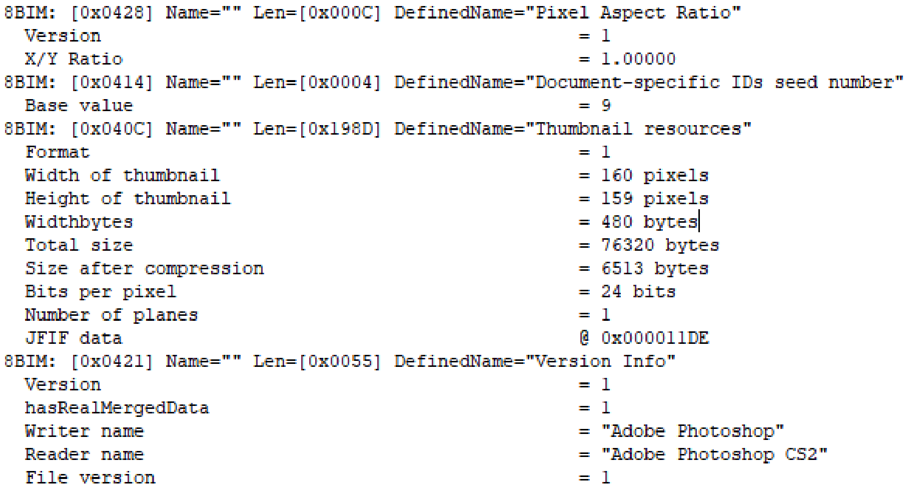
Camera:	Canon EOS 40D
Lens:	23 mm
Exposure:	Manual exposure, 1/21 sec, f/10, ISO 800
Flash:	Off, Did not fire
Date:	**March 15, 2009** 7:03:30PM Z (timezone not specified) (9 years, 10 months, 10 days, 20 hours, 34 minutes, 4 seconds ago, assuming image timezone of US Pacific)
File:	**500 × 497** JPEG 215,766 bytes (211 kilobytes)
Color Encoding:	Embedded color profile: “sRGB”



Extracted **160 × 159** 6.4-kilobyte “Photoshop:PhotoshopThumbnail” JPG Displayed here at 200% (41% the area of the original)



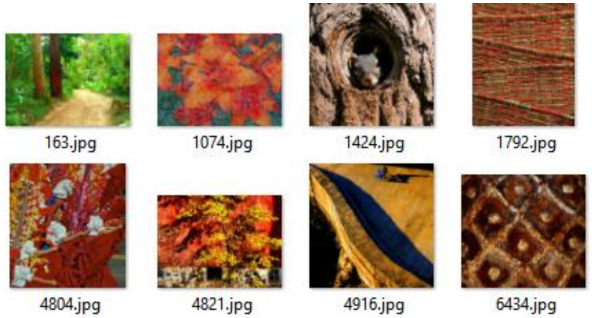
Main JPG image displayed here at 90% width (81% the area of the original)



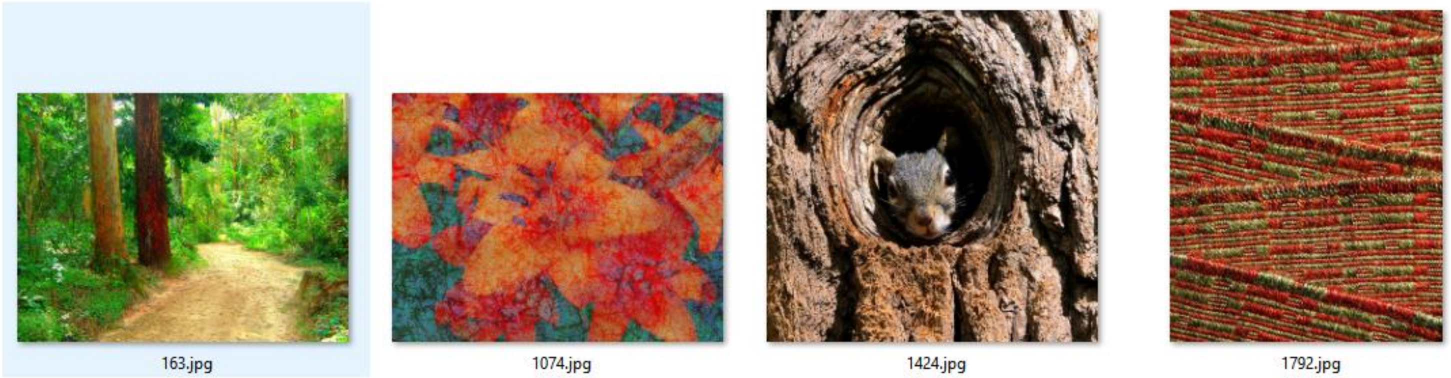
```
8BIM: [0x0428] Name="" Len=[0x000C] DefinedName="Pixel Aspect Ratio"
  Version                                          = 1
  X/Y Ratio                                        = 1.00000
8BIM: [0x0414] Name="" Len=[0x0004] DefinedName="Document-specific IDs seed number"
  Base value                                       = 9
8BIM: [0x040C] Name="" Len=[0x198D] DefinedName="Thumbnail resources"
  Format                                           = 1
  Width of thumbnail                               = 160 pixels
  Height of thumbnail                              = 159 pixels
  Widthbytes                                       = 480 bytes
  Total size                                       = 76320 bytes
  Size after compression                           = 6513 bytes
  Bits per pixel                                   = 24 bits
  Number of planes                                 = 1
  JFIF data                                        @ 0x000011DE
8BIM: [0x0421] Name="" Len=[0x0055] DefinedName="Version Info"
  Version                                          = 1
  hasRealMergedData                                = 1
  Writer name                                      = "Adobe Photoshop"
  Reader name                                      = "Adobe Photoshop CS2"
  File version                                     = 1
```

OS Thumbnail Caches

Windows 10 Large Icons View



Windows 10 Extra-Large Icons View



- Thumbnails are also generated by **Operating Systems** for use when browsing directories/folders
  - Usually store different thumbnail sizes for different folder views
  - Don’t need to generate preview every time the folder is opened, do it once, or when file is modified
- Many modern Operating Systems have a **centralised thumbnail store** for the entire file system/user
  - True for Windows (Vista+), Linux, Android, OS X

OS Thumbnails – Forensic Relevance

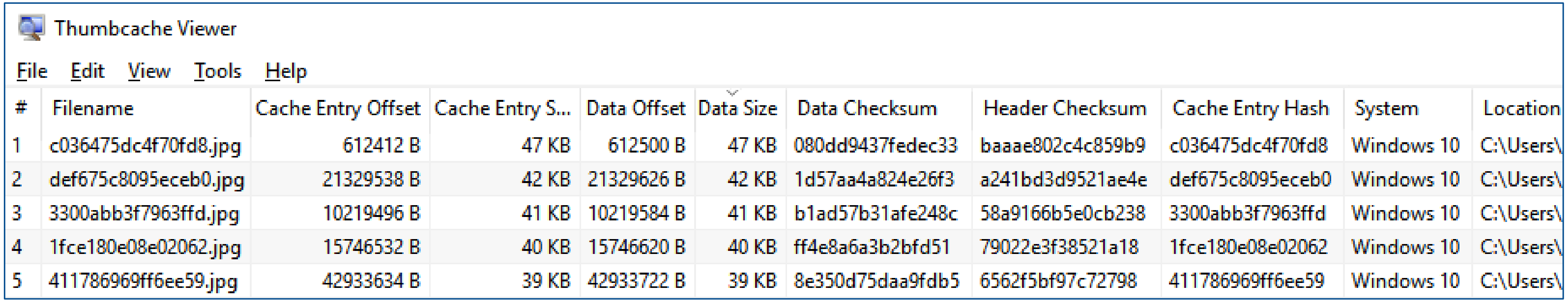
- **Deleted images** or those from **removable media** may still be **cached by the OS**
- Images may also be cached for **networked resources**, such as a Samba Drive.
- Thumbnail caches have frequently been used for convictions in the absence of the original file
- Provides a single “catalogue” of images for the entire device
- **Caveats**:
  - Not all images may be cached
  - Some cached images may never have been viewed

Thumbcache Viewer

- Thumbcache files are user specific, located at:

  [Drive]:/Users/[Username]/AppData/Local/Microsoft/Windows/Explorer/

- Databases can be viewed in Windows using the Thumbcache Viewer application

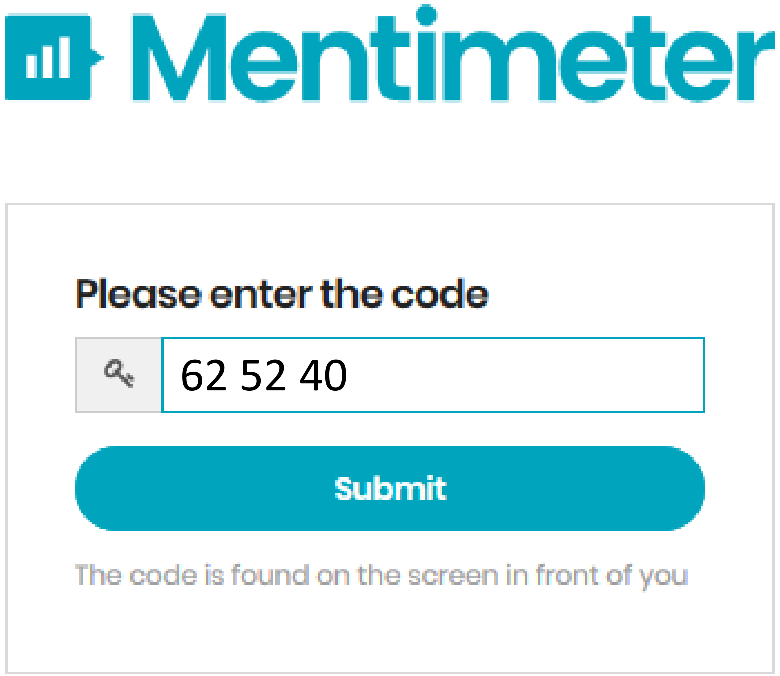


#	Filename	Cache Entry Offset	Cache Entry S...	Data Offset	Data Size	Data Checksum	Header Checksum	Cache Entry Hash	System	Location
1	c036475dc4f70fd8.jpg	612412 B	47 KB	612500 B	47 KB	080dd9437fedec33	baaae802c4c859b9	c036475dc4f70fd8	Windows 10	C:\Users\
2	def675c8095eceb0.jpg	21329538 B	42 KB	21329626 B	42 KB	1d57aa4a824e26f3	a241bd3d9521ae4e	def675c8095eceb0	Windows 10	C:\Users\
3	3300abb3f7963ffd.jpg	10219496 B	41 KB	10219584 B	41 KB	b1ad57b31afe248c	58a9166b5e0cb238	3300abb3f7963ffd	Windows 10	C:\Users\
4	1fce180e08e02062.jpg	15746532 B	40 KB	15746620 B	40 KB	ff4e8a6a3b2bfd51	79022e3f38521a18	1fce180e08e02062	Windows 10	C:\Users\
5	411786969ff6ee59.jpg	42933634 B	39 KB	42933722 B	39 KB	8e350d75daa9fdb5	6562f5bf97c72798	411786969ff6ee59	Windows 10	C:\Users\

Questions

- Submit a question

- Go to: menti.com
- Code: 62 52 40



Please enter the code

62 52 40

The code is found on the screen in front of you

Appendix

Reading and references

EXIF Extras

http://forensicsfromthesausagefactory.blogspot.co.uk/2013/03/location-data-within-jpgs.html

http://windowsitpro.com/blog/how-facebook-handles-image-exif-data

https://scotthelme.co.uk/exif-and-geotagging/

http://www.techfleece.com/2013/03/19/iptc-release-study-on-which-social-media-sites-retain-photographers-copyright-information-exif-data/

Detailed test results http://www.embeddedmetadata.org/social-media-test-results.php (most tested late 2015)

Detailed breakdown of EXIF data storage
http://www.codeproject.com/Articles/43665/ExifLibrary-for-NET.

Workshop Resources

- **https://github.com/smck1/taste_of_cyber**