Technical White Paper

October 12, 2004 www.TechPathways.com
Christopher L. T. Brown, CISSP
clbrown@techpathways.com

Exchangeable Image file Format (ExIF)

Abstract

The Japanese Electronic Industry Development Association (JEIDA) created a standard for the storage of camera and image metadata in JPEG and TIFF files. Most digital camera manufacturers have implemented this standard and now store camera metadata along with the digital image. This metadata can potentially provide vital evidence to investigators such as when the picture was taken, what camera was used in capturing the image and in some cases, who took the image or where the image was captured.

Background

In 1992, the first JPEG file format standard (JFIF) was defined to enable the interchange of JPEG bit streams between a wide variety of applications and platforms. In conformity with the JPEG specification, JFIF added key information to the file such as resolution and standardized color space, and provided for the addition of a thumbnail image. In June, 1998, the JEIDA developed a new standard to allow camera manufacturers to embed camera and image metadata into a JPEG file in conformity with the existing JPEG specification. This standard, called the Exchangeable Image file Format (ExIF) enabled digital camera manufacturers to include information such as camera make and model, camera settings, time, author, copyright and other information directly into the image file so that the photographer would have a permanent record of this information preserved along with the image. By early 2001, most camera manufacturers had implemented this capability into the camera they marketed worldwide. This information can be extracted from the image and may provide vital clues and evidence to investigators.

Every JPEG file begins with "FFD8" which is defined as the SOI (Start of Image) Marker and ends with "FFD9" which is the EOI (End of Image) marker. In between these two markers, the data is divided into several segments, each of which is defined by a specific marker.   The length of each segment is defined within the segment to provide the maximum flexibility and still allow applications to separate and examine each segment. This flexible file structure has allowed the creation of standards such as JFIF and ExIF which add specific markers and segments to store data while still conforming to the overall JPEG specification. The diagram below shows this generalized structure.

SOI Marker	Marker XX size=SSSS	Marker YY size=TTTT	SOS Marker size=UUUU	Image stream	EOI Marker
FFD8	FFXX SSSS DDDD......	FFYY TTTT DDDD......	FFDA UUUU DDDD....	1111....	FFD9

The original JPEG specification defined a set of markers called application markers which range from FFE0 to FFEF that allow for the addition of application specific information. This information is not needed to decode the JPEG image, but rather, add information to be used by specific applications. JFIF was the first to employ these application markers and used the APP0 marker (FFE0) to identify the segment which contained the information added by JFIF. The newer ExIF specification uses the APP1 marker (FFE1) to mark the additional metadata information to be added to a file. This APP1 marker must follow directly after the SOI marker. The file format for ExIF approximately is as follows:

FFD8	Start of Image Marker				
FFE1	APP1 Marker				
SSSS		APP1 Data Size			
45786966 0000		ExIF Header			
49492A00 08000000		TIFF Header			
XXXX. . . .					Directory
LLLLLLLL		IFD0 (main image)			Link to ExIF IDF
LLLLLLLL		(See IFD0 Tags table below)			Link to GPS IDF
LLLLLLLL					Next IFD Pointer
XXXX. . . .		Data area of IFD0			
XXXX. . . .			ExIF SubIFD		ExIF Version
00000000			(See ExIF SubIDF Tags table below)		End of Link
XXXX. . . .			Data area of ExIF SubIFD		
XXXX. . . .	APP1 Data			Interoperability IFD	Directory
00000000					End of Link
XXXX. . . .				Data area of Interoperability IFD	
XXXX. . . .				Makernote IFD	Directory
00000000					End of Link
XXXX. . . .				Data area of Makernote IFD	
XXXX. . . .		GPS IDF			GPS Version
00000000		(See Misc Tags table below)			End of Link
XXXX. . . .		Data area of GPS IFD			
XXXX. . . .		IFD1(thumbnail image)			Directory
00000000					End of Link
XXXX. . . .		Data area of IFD1			
FFD8XXXX. . . XXXXFFD9		Thumbnail image			
FFXX	Other Marker(s)				
TTTT		Data Size			
DDDD		Data Area			
FFDA	Start of Stream Marker				
UUUU		Stream Size			
DDDD		Data			
IIII	Image Stream				
FFD9	End of Image Marker				

ExIF Tag Information

The real benefit to the investigator of the ExIF standard is the information that may be provided in the Tags fields. The tables below list the Tags defined by the ExIF standard for the IFD0, ExIF sub IDF fields as well as the miscellaneous ExIF Tags. Investigators should note, Tag fields may or may not have meaningful information stored in them. Tag field use is implementation dependant and varies from manufacturer to manufacture.

Tag No.	Tag Name	Format	Desc.
0x010e	ImageDescription	ASCII string	Describes image. Two-byte character code such as Chinese/Korean/Japanese cannot be used.
0x010f	Make	ASCII string	Shows manufacturer of digital cameras. In the ExIF standard, this tag is optional, but it is mandatory for DCF.
0x0110	Model	ASCII string	Shows model number of digital cameras. In the ExIF standard, this tag is optional, but it is mandatory for DCF.
0x0112	Orientation	unsigned short	The orientation of the camera relative to the scene, when the image was captured. The relation of the '0th row' and '0th column' to visual position is shown as right. Value 0th Row 0th Column 1 top left side 2 top right side 3 bottom right side 4 bottom left side 5 left side top 6 right side top 7 right side bottom 8 left side bottom
0x011a	XResolution	unsigned rational	Display/Print resolution of image. Default value is 1/72inch, but it has no mean because personal computer doesn't use this value to display/print out.
0x011b	YResolution	unsigned rational	
0x0128	ResolutionUnit	unsigned short	Unit of XResolution(0x011a)/YResolution(0x011b). '1' means no-unit, '2' means inch, '3' means centimeter. Default value is '2'(inch).
0x0131	Software	ASCII string	Shows firmware (internal software of digital cameras) version number.
0x0132	DateTime	ASCII string	Date/Time of image was last modified. Data format is "YYYY:MM:DD HH:MM:SS"+0x00, total 20bytes. If clock has not set or digital cameras doesn't have clock, the field may be filled with spaces. In usual, it has the same value of DateTimeOriginal(0x9003)
0x013e	WhitePoint	unsigned rational	Defines chromaticity of white point of the image. If the image uses CIE Standard Illumination D65(known as international standard of 'daylight'), the values are '3127/10000,3290/10000'.
0x013f	PrimaryChromaticities	unsigned rational	Defines chromaticity of the primaries of the image. If the image uses CCIR Recommendation 709 primaries, values are '640/1000, 330/1000, 300/1000, 600/1000, 150/1000, 0/1000'.
0x0211	YCbCrCoefficients	unsigned rational	When image format is YCbCr, this value shows a constant to translate it to RGB format. In usual, values are '0.299/0.587/0.114'.
0x0213	YCbCrPositioning	unsigned short	When image format is YCbCr and uses 'Subsampling'(cropping of chroma data, all the digital cameras do that), defines the chroma sample point of subsampling pixel array. '1' means the center of pixel array, '2' means the datum point.
0x0214	ReferenceBlackWhite	unsigned rational	Shows reference value of black point/white point. In case of YCbCr format, first 2 show black/white of Y, next 2 are Cb, last 2 are Cr. In case of RGB format, first 2 show black/white of R, next 2 are G, last 2 are B.
0x8298	Copyright	ASCII string	Shows copyright information
0x8769	ExIFOffset	unsigned long	Offset to ExIF Sub IFD

Tag No.	Tag Name	Format	Desc.
0x829a	ExposureTime	unsigned	Exposure time (reciprocal of shutter speed). Unit is second.

		rational	
0x829d	FNumber	unsigned rational	The actual F-number (F-stop) of lens when the image was taken.
0x8822	ExposureProgram	unsigned short	Exposure program that the camera used when image was taken. '1' means manual control, '2' program normal, '3' aperture priority, '4' shutter priority, '5' program creative (slow program), '6' program action(high-speed program), '7' portrait mode, '8' landscape mode.
0x8827	ISOSpeedRatings	unsigned short	CCD sensitivity equivalent to Ag-Hr film speedrate.
0x9000	ExIFVersion	undefined	ExIF version number. Stored as 4bytes of ASCII character. If the picture is based on ExIF V2.1, value is “0210”. Since the type is 'undefined', there is no NULL (0x00) for termination.
0x9003	DateTimeOriginal	ascii string	Date/Time of original image taken. This value should not be modified by user program. Data format is “YYYY:MM:DD HH:MM:SS”+0x00, total 20bytes. If clock has not set or digital cameras doesn't have clock, the field may be filled with spaces. In the ExIF standard, this tag is optional, but it is mandatory for DCF.
0x9004	DateTimeDigitized	ascii string	Date/Time of image digitized. Usually, it contains the same value of DateTimeOriginal(0x9003). Data format is “YYYY:MM:DD HH:MM:SS”+0x00, total 20bytes. If clock has not set or digital cameras doesn't have clock, the field may be filled with spaces. In the ExIF standard, this tag is optional, but it is mandatory for DCF.
0x9101	ComponentsConfiguration	undefined	Shows the order of pixel data. Most of case '0x04,0x05,0x06,0x00' is used for RGB-format and '0x01,0x02,0x03,0x00' for YCbCr-format. 0x00:does not exist, 0x01:Y, 0x02:Cb, 0x03:Cr, 0x04:Red, 0x05:Green, 0x06:Bllue.
0x9102	CompressedBitsPerPixel	unsigned rational	The average compression ratio of JPEG (rough estimate).
0x9201	ShutterSpeedValue	signed rational	Shutter speed by APEX value. To convert this value to ordinary 'Shutter Speed'; calculate this value's power of 2, then reciprocal. For example, if the ShutterSpeedValue is '4', shutter speed is $1/(2^4)=1/16$ second.
0x9202	ApertureValue	unsigned rational	The actual aperture value of lens when the image was taken. Unit is APEX. To convert this value to ordinary F-number (F-stop), calculate this value's power of root 2 (=1.4142). For example, if the ApertureValue is '5', F-number is 1.4142^5 = F5.6.
0x9203	BrightnessValue	signed rational	Brightness of taken subject, unit is APEX. To calculate Exposure(Ev) from BrigtnessValue(Bv), you must add SensitivityValue(Sv). Ev=Bv+Sv Sv=$\log_2$(ISOSpeedRating/3.125) ISO100:Sv=5, ISO200:Sv=6, ISO400:Sv=7, ISO125:Sv=5.32.
0x9204	ExposureBiasValue	signed rational	Exposure bias (compensation) value of taking picture. Unit is APEX (EV).
0x9205	MaxApertureValue	unsigned rational	Maximum aperture value of lens. You can convert to F-number by calculating power of root 2 (same process of ApertureValue:0x9202).
0x9206	SubjectDistance	signed rational	Distance to focus point, unit is meter.
0x9207	MeteringMode	unsigned short	Exposure metering method. '0' means unknown, '1' average, '2' center weighted average, '3' spot, '4' multi-spot, '5' multi-segment, '6' partial, '255' other.
0x9208	LightSource	unsigned short	Light source, actually this means white balance setting. '0' means unknown, '1' daylight, '2' fluorescent, '3' tungsten, '10' flash, '17' standard light A, '18' standard light B, '19' standard light C, '20' D55, '21' D65, '22' D75, '255' other.
0x9209	Flash	unsigned short	'0' means flash did not fire, '1' flash fired, '5' flash fired but strobe return light not detected, '7' flash fired and strobe return light detected.
0x920a	FocalLength	unsigned rational	Focal length of lens used to take image. Unit is millimeter.
0x927c	MakerNote	undefined	Maker dependent internal data. Some of maker such as Olympus/Nikon/Sanyo etc. uses IFD format for this area.
0x9286	UserComment	undefined	Stores user comment. This tag allows to use two-byte character code or Unicode. First 8 bytes describe the character code. 'JIS' is a Japanese character code (known as Kanji). '0x41,0x53,0x43,0x49,0x49,0x00,0x00,0x00':ASCII '0x4a,0x49,0x53,0x00,0x00,0x00,0x00,0x00':JIS '0x55,0x4e,0x49,0x43,0x4f,0x44,0x45,0x00':Unicode '0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00':Undefined
0x9290	SubsecTime	ASCII string	Some of digital cameras can take 2~30 pictures per second, but DateTime/DateTimeOriginal/DateTimeDigitized tag can't record the sub-second time. SubsecTime tag is used to record it. For example, DateTimeOriginal = “1996:09:01 09:15:30”, SubSecTimeOriginal = “130”, Combined original time is “1996:09:01 09:15:30.130”
0x9291	SubsecTimeOriginal	ASCII string	
0x9292	SubsecTimeDigitized	ASCII	

<table>
<tr><td></td><td></td><td>string</td><td></td></tr>
<tr><td>0xa000</td><td>FlashPixVersion</td><td>undefined</td><td>Stores FlashPix version. If the image data is based on FlashPix former Ver.1.0, value is “0100”. Since the type is 'undefined', there is no NULL(0x00) for termination.</td></tr>
<tr><td>0xa001</td><td>ColorSpace</td><td>unsigned short</td><td>Defines Color Space. DCF image must use sRGB color space so value is always '1'. If the picture uses the other color space, value is '65535':Uncalibrated.</td></tr>
<tr><td>0xa002</td><td>ExIFImageWidth</td><td>unsigned short/long</td><td>Size of main image.</td></tr>
<tr><td>0xa003</td><td>ExIFImageHeight</td><td>unsigned short/long</td><td></td></tr>
<tr><td>0xa004</td><td>RelatedSoundFile</td><td>ASCII string</td><td>If this digital camera can record audio data with image, shows name of audio data.</td></tr>
<tr><td>0xa005</td><td>ExIFInteroperabilityOffset</td><td>unsigned long</td><td>Extension of “ExIFR98”, detail is unknown. This value is offset to IFD format data. Currently there are 2 directory entries, first one is Tag0x0001, value is “R98”, next is Tag0x0002, value is “0100”.</td></tr>
<tr><td>0xa20e</td><td>FocalPlaneXResolution</td><td>unsigned rational</td><td>Pixel density at CCD's position. If you have MegaPixel digital cameras and take a picture by lower resolution (e.g.VGA mode), this value is re-sampled by picture resolution. In such case, FocalPlaneResolution is not same as CCD's actual resolution.</td></tr>
<tr><td>0xa20f</td><td>FocalPlaneYResolution</td><td>unsigned rational</td><td></td></tr>
<tr><td>0xa210</td><td>FocalPlaneResolutionUnit</td><td>unsigned short</td><td>Unit of FocalPlaneXResoluton/FocalPlaneYResolution. '1' means no-unit, '2' inch, '3' centimeter.
Note: Some of Fujifilm's digital cameras (e.g.FX2700,FX2900,Finepix4700Z/40i etc) uses value '3' so it must be 'centimeter', but it seems that they use a '8.3mm?'(1/3in.?) to their ResolutionUnit. Fuji's BUG? Finepix4900Z has been changed to use value '2' but it doesn't match to actual value also.</td></tr>
<tr><td>0xa215</td><td>ExposureIndex</td><td>unsigned rational</td><td>Same as ISOSpeedRatings(0x8827) but data type is unsigned rational. Only Kodak's digital cameras uses this tag instead of ISOSpeedRating, I don't know why(historical reason?).</td></tr>
<tr><td>0xa217</td><td>SensingMethod</td><td>unsigned short</td><td>Shows type of image sensor unit. '2' means 1 chip color area sensor, most of all digital cameras use this type.</td></tr>
<tr><td>0xa300</td><td>FileSource</td><td>undefined</td><td>Indicates the image source. Value '0x03' means the image source is digital still camera.</td></tr>
<tr><td>0xa301</td><td>SceneType</td><td>undefined</td><td>Indicates the type of scene. Value '0x01' means that the image was directly photographed.</td></tr>
<tr><td>0xa302</td><td>CFAPattern</td><td>undefined</td><td>Indicates the Color filter array (CFA) geometric pattern.
<table>
<tr><th>Length</th><th>Type</th><th>Meaning</th></tr>
<tr><td>2</td><td>short</td><td>Horizontal repeat pixel unit = n</td></tr>
<tr><td>2</td><td>short</td><td>Vertical repeat pixel unit = m</td></tr>
<tr><td>1</td><td>byte</td><td>CFA value[0,0]</td></tr>
<tr><td>:</td><td>:</td><td>:</td></tr>
<tr><td>1</td><td>byte</td><td>CFA value[n-1,0]</td></tr>
<tr><td>1</td><td>byte</td><td>CFA value[0,1]</td></tr>
<tr><td>:</td><td>:</td><td>:</td></tr>
<tr><td>1</td><td>byte</td><td>CFA value[n-1,m-1]</td></tr>
</table>
The relation of filter color to CFA value is shown below.
<table>
<tr><td>Filter Color</td><td>Red</td><td>Green</td><td>Blue</td><td>Cyan</td><td>Magenta</td><td>Yellow</td><td>White</td></tr>
<tr><td>CFA value</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td></tr>
</table>
</td></tr>
</table>

Misc. Tags

Tag No.	Tag Name	Format
0x00fe	NewSubfileType	unsigned long
0x00ff	SubfileType	unsigned short
0x012d	TransferFunction	unsigned short
0x013b	Artist	ASCII string

0x013d	Predictor	unsigned short
0x0142	TileWidth	unsigned short
0x0143	TileLength	unsigned short
0x0144	TileOffsets	unsigned long
0x0145	TileByteCounts	unsigned short
0x014a	SubIFDs	unsigned long
0x015b	JPEGTables	undefined
0x828d	CFARepeatPatternDim	unsigned short
0x828e	CFAPattern	unsigned byte
0x828f	BatteryLevel	unsigned rational
0x83bb	IPTC/NAA	unsigned long
0x8773	InterColorProfile	undefined
0x8824	SpectralSensitivity	ASCII string
0x8825	GPSInfo	unsigned long
0x8828	OECF	undefined
0x8829	Interlace	unsigned short
0x882a	TimeZoneOffset	signed short
0x882b	SelfTimerMode	unsigned short
0x920b	FlashEnergy	unsigned rational
0x920c	SpatialFrequencyResponse	undefined
0x920d	Noise	undefined
0x9211	ImageNumber	unsigned long
0x9212	SecurityClassification	ASCII string
0x9213	ImageHistory	ASCII string
0x9214	SubjectLocation	unsigned short
0x9215	ExposureIndex	unsigned rational
0x9216	TIFF/EPStandardID	unsigned byte
0xa20b	FlashEnergy	unsigned rational
0xa20c	SpatialFrequencyResponse	unsigned short
0xa214	SubjectLocation	unsigned short

It is apparent from the tables above a vast amount of data that may be stored in the ExIF Metadata. While some data, like make and model of the camera used, date and time of original, copyright, user comments, Artist, Time Zone offset, GPS Information, Image History, and Subject Location have obvious benefits to an investigator if present, other fields may be helpful in comparing multiple images taken at or near the same time to establish that they were taken with the same camera. This may allow one image with identifying information to tie back to another image and more importantly the images to the device.

Elimination of ExIF Metadata

ExIF metadata may be stripped or eliminated using software. Applications such as Photoshop may not save this information if a JPEG file is open and then later saved by that application. Although many software manufacturers are moving to support the standard and preserve this information, older versions of the software may be used intentionally or unintentionally to eliminate this information. Sophisticated individuals may even use simple tools such as hex editors to eliminate data from ExIF files.

Conclusion

The Tag tables above provide a tremendous amount of potentially useful information if contained in the ExIF section of a JPEG file. While it is cumbersome to try to pull this data manually from the file, programs exist today to extract this data for the investigator. Programs such as EXIFutils or IMatch can be used to view this information. Technology Pathways forensic tool, ProDiscover will automatically extract and report this information for investigators if desired for all JPEG and TIFF files marked as evidence of interest. This can open up a whole new avenue for investigators and capture ExIF metadata in an evidentiary quality manner to be used in court at a latter date.