WYSIWYG – Or is it?
The Need for a Standard for Secure Digital Photography in Accident Investigation

Corey Stephens & Chris Baum
Air Line Pilots Association, International

Author Biographies:
Corey Stephens is a Staff Engineer with the Engineering & Air Safety Department of the Air Line Pilots Association, International (ALPA). His current duties include participating in all of ALPA's accident investigation activity and he is the staff lead for ALPA's Advanced Accident Investigation Course. Corey has been with ALPA for 6 years and has worked on accidents in the US and Canada. He has also assisted the International Federation of Air Line Pilot Associations (IFALPA) with technical expertise on international accidents. Corey has also worked in the safety department of United Airlines and with the US National Transportation Safety Board.

Chris Baum is the Manager of Engineering and Accident Investigation Section in the Engineering and Air Safety Department of the Air Line Pilots Association, International (ALPA). Chris supervises all support activities associated with ALPA's accident investigation efforts. He has been with ALPA for 8 years and has served in several positions in the Engineering and Air Safety Department. Prior to coming to ALPA, Chris spent 23 years in the US Air Force in a variety of operational and staff positions.

WYSIWYG – Or is it?

The Need for a Standard for Secure Digital Photography in Accident Investigation

By
Mr. Corey Stephens
and
Mr. Chris Baum

Engineering and Air Safety Department
Air Line Pilots Association, International

1. Introduction

One has only to stop and look around at any contemporary major accident investigation site to realize that digital devices are in widespread use in the accident investigation community. Among these are an ever-increasing number of digital cameras, in many cases outnumbering film cameras as the tool of choice for recording the entire spectrum of accident scenes, from close-ups of failed components to aerial views of the accident site. Notwithstanding the completely valid school of thought which advocates disposable film cameras over any other type (cheaper, simpler, readily available, zero maintenance, no training required, low probability of error, etc.), digital cameras appear to be here to stay; at least until replaced by the next quantum leap in photographic technology.

Similarly, one has only to review current published government guidance on the conduct of an investigation to realize that no specific accommodations are generally being made to account for the different character of the digital medium vis-à-vis the optical (film) one. In the United States and Canada, there are no specific chain-of-custody requirements to ensure that the computer file representing the digital image is not copied illicitly, altered, or destroyed. Similarly, there is no guidance on use of any particular format for digital imaging, and no format yet exists that would allow investigators or other users of digital photography to positively check the validity of an image and identify any changes made to it (as well as when such changes were made, what they were, and who made them).

This paper will attempt to address the need for such a standard to verify the authenticity of digital photographs. We will begin with a discussion of how film cameras have been used and misused in investigations of various types over time, and how digital cameras have come to be used in the field of aircraft accident investigation today. We will attempt to identify at a high level some of the problems the authors perceive in the use of digital photography, including the possibility of undetectable alteration leading to erroneous conclusions. We will review the current state of various other agencies' (e.g.

law enforcement) research and concerns in the subject because for a “secure” digital standard to be developed, it will be necessary, if for no other reason than efficiency, to enlist the participation of a variety of disciplines who can be considered stakeholders in this discussion. We will look at part of the spectrum of existing file formats in use for digital photography at both the amateur and professional level and attempt to describe how these or other formats would need to accommodate the needs of the investigation community to be able to have high confidence that the image they are viewing months after the accident is the same was viewed by investigators on scene. Finally, we will propose that the solution to developing a set of standards for camera, recording media, and related processes is for government and industry to work cooperatively to review the need, identify the requirements, and set the processes in motion that will lead to such standards

2. History of film cameras in investigations and film photo fakery

The following is quoted from a review of the book Photo Fakery: The History and Techniques of Photographic Manipulation, by Dino A. Brugioni. The review was found posted on FCW.com (Federal Computer World)

> Since the early 19th century, people have come to accept what they see in photographs as reality. The adage that "the camera never lies" has come to be accepted as historical fact, buttressed by the faith taken daily by all who read a newspaper or magazine that what is depicted in photos actually happened. …..
>
> The art of producing fake photography predates the computer by almost a century, and some of America's well-known and most beloved figures have not gone unscathed, according to Brugioni.
>
> For example, when photographer Matthew Brady first photographed President John Calhoun, he had no idea that an eager entrepreneur would later take a reversed image of Abraham Lincoln's head and graft it onto Calhoun's body for a new engraving. Not only was Lincoln's head also substituted on the bodies of Alexander Hamilton and Martin Van Buren, but the famous photo of "The Martyr Lincoln," which depicts Lincoln in his casket, has since been proven to be fraudulent, Brugioni writes.
>
> Other well-known doctored photographs include the recently de-bunked 1934 depiction of the Loch Ness monster that appeared in a London newspaper; a studio portrait of American literary giant Walt Whitman that was used as the frontispiece to Leaves of Grass; and an 1865 portrait of Union Army Gen. William Sherman and his staff. More recent examples of tampering illustrated by Brugioni include the controversial darkening of O.J. Simpson's face on the cover of Time magazine and the less sinister yet commonplace touchups done to the faces, teeth and bust lines of today's supermodels.
>
> According to Brugioni, "the invention of the Eastman portable camera in 1888, followed by the box camera, opened photography to people in all walks of life." Now, a little more than 100 years later, the same can be said of the computer. Brugioni's book appears at a time when the technology is readily available for almost anybody with a modicum of computer skills to re-touch, change or forge photos. …..

> Likewise, Brugioni uses the mind-boggling pace of technology to paint a bleak picture of the future. "We can see how photo fakery has made most of us doubters rather than believers," Brugioni writes. "With the new and expanding technology, faith in photography as the purveyor of truth has been weakened and, in the future, it will be further weakened rather than strengthened."
>
> Brugioni suggests that in this age of the "electronic darkroom," ethics must become "an important part of a course in digital imaging taught at DOD's Joint Defense Photography School in Pensacola, Fla." The concern, according to Brugioni, is that the ability to alter photos through electronic manipulation raises moral, legal and ethical issues for members of the intelligence community who are responsible for providing imagery intelligence to high-level decision-makers in government, including the president.
>
> Readers are left hanging, however, wondering what, if anything, can be done to avoid a future where nothing can be believed. Brugioni puts forth a strong argument in favor of distrusting the pictures shown in newspapers, in magazines, on television and on the Internet….[1]

It should not come as a surprise to any accident investigator working today that the idea of presenting a photograph to support a textual or other description of some aspect of an investigation is not new. Virtually any modern major aircraft accident investigation will have photographs of wreckage, ground scars, general overview of the accident site, and so on. Such use of photography has become routine and is expected. However, a review of the published accident investigation manuals of the United States, Canada, and ICAO reveal that surprisingly little is written in these texts regarding the use of photographs in the course of an investigation. All the aforementioned works refer to photography, suggesting that its use is expected and condoned, but none of these manuals make any mention of the need to verify the validity of photographs prior to using them to support analysis and develop conclusions as to accident causation. The maturity of all these documents suggests that this omission is not an oversight, but rather a reflection of a presumption on the part of the State that the Investigator In Charge will be able to exercise sufficient control over the investigation that he or she will, through the normal investigative process, have confidence that photographs taken in the field will be controlled sufficiently to prevent fraudulent use of altered photographs. This is likely a valid assumption in the case of traditional optical photographs. While it would not be impossible to take optical photographs of, for example, a suspect component, and in about the same time as would be required for normal developing, remove the film and surreptitiously alter the photograph, the normal processes for controlling access to evidence would tend to prevent such activity (or at least make it obvious). Conversely, however, the expanding use of digital photography in investigations does not have the same inherent characteristics that resist tampering. Accident sites at most recent major investigations are virtually awash in computers and related equipment. Each and every one of these devices is potentially an “electronic darkroom” that can be used, in real time, to retrieve, retain a copy of, and display digital photographs. That fact alone means that the possibility of a digital photograph being altered, through either a deliberate act, carelessness, or honest error is far greater than in the optical photography case.

[1] Sometimes seeing is not believing BY DANIEL VERTON Dec. 20, 1999

Add to this the fact that digital cameras are increasing in popularity, increasing in capability, and decreasing in price and the fact that computer software whose legitimate purpose is to *change* digital photographs is doing the same thing, and it becomes easy to see that a potential problem exists that must be managed.

3. How are digital cameras used in the field today and what are the benefits

Clearly, photography in general has established its place as a valuable investigative tool. It's difficult to imagine any modern investigation being conducted without photo documentation of the overall site, individual failed components, and so forth. Digital photography, however, is a subset that is still evolving. Subjectively, it appears that in the early years of the technology, it was viewed by investigators as simply a new type of camera, and it was too soon to tell if the legacy would be "state of the art" or "flash in the pan." Early models were expensive and the quality was inferior to optical cameras. Nevertheless, as investigators became more and more used to using automation in their daily business, and then in the field, the appeal of a device that would allow the immediate review of photographs as well as the ability to copy and move them easily, was compelling. The emerging prevalence, if not the advantages, of digital photography made it evident to investigative agencies that this technology had a place in field work. The problem, of course, was that this was not a decision driven by the needs of investigators, but rather one reacting to the marketing blitz that accompanied the emergence of digital cameras.

On a very basic level, digital cameras are used in essentially the same manner as their optical cousins. The camera as an investigative tool is used to record pertinent details of fractures, burns, scars, switch positions and so forth. It is used to help the investigator recall the overall orientation of objects, and to enable study of views that may only be obtainable in a transient manner (such as an overhead view from a helicopter). Beyond that, however, there are significant differences between digital and optical that should be examined and understood if the risks and benefits are to be properly balanced.

Perhaps the most evident benefit of digital photography is that it gives the photographer/investigator the ability to immediately see what he or she has just shot, evaluate the picture, make adjustments, and reshoot if necessary. Some later model cameras have this capability built in to the programming and can automatically take a short series of photos, varying the exposure or other parameters slightly for each shot. In theory, this should result in photographs that are generally more useful to the investigator. On the other hand, however, this same capability introduces some new variables. Optical processing in general results in a relatively consistent product. Digital images, however, may vary considerably based only on the output device (e.g. the camera's own LCD screen vs. a laptop's processed video signal vs. a printer's "version" of the image). Depending on the desired subject of the image, these differences may or may not be significant.

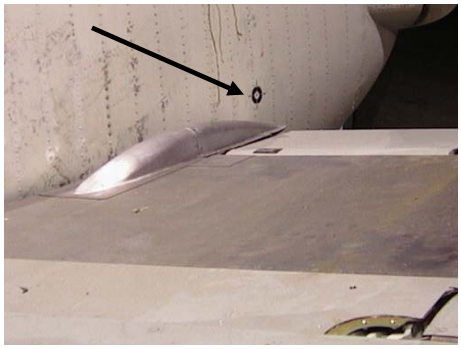
Another feature of digital cameras (generally viewed as an advantage) is the elimination of the need for film. In reality, however, the digital device has essentially the same limitations as the optical device – there is a finite amount of storage for the images and when that is used up, the photographer must take some action. The difference, of course, is in scale. The capacity of storage media continues to go up and the price continues to go down. At the same time, however, the capability of the camera to use large quantities of storage also continues to skyrocket. This is, on balance, a benefit. The upper limit of quality of digital photography (in terms of the image resolution – megapixels) continues to climb, allowing digital images to be made that are nearly indistinguishable in quality from the optical versions and are generally more than satisfactory for most investigative uses. The net result of the advances in picture quality (as indicated by pixel density) and storage availability clearly favors digital. The photographer can use media that allow recording of tens, if not hundreds of pictures on devices that can be stored in a pocket, are more robust than traditional film cartridges, can be emptied of their data contents and reused, can be shared among users almost at will (although it is sometimes necessary to have a reading device) and have virtually no expiration date.

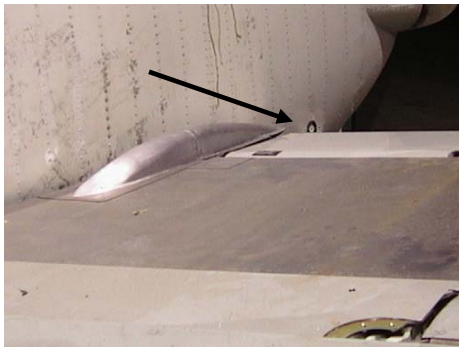
4. What are the potential problems

With so many advantages in capacity, immediacy, and portability, one might be inclined to look at digital photography as an invaluable investigative tool. That may well be, but as with any other beneficial item, costs exists that must be balanced and drawbacks exist that must be evaluated to see if they should be mitigated before using the technology. On a very basic level, the problems associated with digital photography are essentially the same as for optical photography in investigations. For example, it is equally important, whether the medium is film or digital, to ensure that photographs taken as evidence that leads to determinations of an accident cause can be preserved for proper use by safety investigators, can be validated and their authenticity verified, and so on. There are few new protocols that need to be developed for use of digital photography. Implementing those protocols, however, may be significantly more difficult when using digital media.

Image manipulation is perhaps the biggest threat to the use of digital photography. If one were to set out to falsify optical photographs convincingly, one would likely need to have (or have access to) relatively sophisticated darkroom equipment and would also require the expertise to use it. On the other hand, current software is available for relatively little money that not only enables even a novice to alter digital photographs but also will frequently perform the task itself! If one wanted to be in the business of altering digital photographs, and was willing to make an investment in that process, far more sophisticated software is available. One of the photographs taken below was taken to illustrate the relationship between the aircraft elevator trailing edge and a manufacturer's alignment mark installed to enable proper elevator rigging. The other was adjusted to change the position of the alignment mark relative to the elevator. The adjustment required software available at any retail computer store and about 15 minutes of effort. Granted, this is a simplistic example and in an actual investigation, there would likely be a number of ways the deception could be uncovered. If the photos were electronically

embedded in the document and the document was retained electronically, it might actually be possible to enlarge each photo and clearly see the changes. However, if the photos were printed in a report, such recovery would not be possible. In spite of the simplicity of this example, it illustrates the ease with which a photograph, taken to illustrate a point, can be changed to create an impression quite different from reality.





As with any piece of evidence, a chain of custody is important to ensure that the evidence remains under the control of the Investigator in Charge or other official of the State investigative agency. With physical objects, this is a straightforward process. Even with conventional photographic film, the process that generates a photographic negative can be monitored and the negatives can then be retained for safekeeping. Such a chain of custody is not as simple or straightforward with digital media. Given that the "photograph" takes the form of a computer file, duplicates of which can be indistinguishable from the original, identification of source material from copies becomes a significant issue. Even the storage device itself may not be identifiable as an original unless measures are taken initially to do so (e.g. initialed by an investigator or placed in a container with a tamper-evident seal. The file that contains a digital image can be moved both from and to many types of storage. As a result, it is possible to capture an image with a camera, store it to a digital storage medium, move it from that medium to a computer for processing, change it and move it back to the storage medium as a different image. Most computer users realize that files have attributes, and among those attributes is a date and time. This is frequently the information used to distinguish one version of a file from a later, presumably changed, version. This feature may be of value in determining if a file has a date and time in consistent with its "status" as an original investigation artifact. However, depending on the software used, the file date and time on a computer may be the date and time the file was downloaded off the medium onto a computer for legitimate investigative use, even if the file was unchanged. Thus, the presence of a date and time later than the field phase of the investigation is not explicitly indicative that the file has been changed.

Finally, one must consider the volatility and fragility of a digital image. As a rule, digital storage media are robust and relatively resistant to mechanical damage. They are, however, not impervious to mistakes, mishandling, or other hazards. If a role of conventional photographic film is somehow damaged, portions of the images on the film

may be recoverable. If the digital medium is mechanically damaged, it is far less likely that any information is recoverable. In addition, as most computer users know, there is the distinct possibility of human error causing loss of data. The difference between "Erase All – Yes" and "Erase All – No" may be so slight as to allow the user to defeat the manufacturer's safeguards. And as every computer user also knows, once a file is truly gone, it is generally gone forever.

5. How are other organizations and agencies handling this

Aviation accident investigators are not the only ones facing these problems. The Federal Bureau of Investigations in the United States has been looking at these same issues. An examiner in the FBI Laboratory's Special Photographic Unit, Special Agent Douglas A. Goodin, described in February 1996 in a paper entitled Image Security and Integrity: "The ease with which images can be changed is the central issue in image integrity. The impermanent recording of an image by rearranging a bunch of magnetic particles and corresponding pixels seems to lack the security and integrity of good old film." Special Agent Goodin believes that at a crime scene when a digital camera is used a greater problem for law enforcers may surface. "The photographer may have been the only one there at the time. A particularly damning piece of evidence could be later undetectably inserted into the images through an image-processing program. As digital photography becomes more widespread in law enforcement, I could see this becoming a problem for overzealous or dishonest officers." In a recent case in the United States the prosecution team in a trial was accused of photo manipulation. During the O.J. Simpson murder trial, prosecutors entered into evidence a picture of Simpson wearing the now infamous Bruno Magli shoes. The defense claimed Simpson didn't wear those shoes and the photograph was manipulated, and thus objected. Expert witnesses were then called in. Two experts gave their analysis of the photos, but each gave a different view. This issue was finally settled when a roll of film that contained pictures of Simpson wearing the Bruno Maglis was discovered and entered into evidence. If not for that roll of film, or had the original image been digital, the original photograph probably wouldn't have held up as evidence.

In June 2002, the Scientific Working Group on Imaging Technologies (SWGIT), of which the FBI is involved, released Version 1.2 of their recommendations and guidelines for the use of digital image processing in the criminal justice system. Their objective is "…to ensure the successful introduction of forensic imagery as evidence in a court of law." Their work includes brief descriptions of advantages, disadvantages, and potential limitations of each major digital imaging process. They see digital image processing as a necessary and accepted practice in forensic science. The SWGIT group feels that any changes to an image made through digital image processing are acceptable in forensic applications provided the following criteria are met:

- The original image is preserved
- The processing steps are logged when they include techniques other than those used in a traditional photographic darkroom
- The end result is presented as an enhanced image, which may be reproduced by applying the logged steps to the original image

SWGIT has continued their work by releasing “Minimum Best Practices for Documenting Image Enhancement - Version 1.1” on March 4, 2004. The purpose of this document is to describe the “best practice” documentation of image enhancement used in the criminal justice system. The objective of SWGIT with these standards is to provide laboratory personnel with instruction regarding the level of documentation that is appropriate when performing enhancement operations on still images, regardless of the tools and devices used to perform the enhancement. SWGIT is using this documentation of image enhancement techniques to help satisfy the legal requirements for the introduction of forensic images as evidence in a court of law. SWGIT has developed two categories by which images can be enhanced; Category 1 and Category 2. Category 1 images include “Images utilized to demonstrate what the photographer or recording device witnessed but not analyzed by subject matter experts.” This would include: General crime scene or investigative images, surveillance images, autopsy images, documentation of items of evidence in a laboratory, and arrest photographs ("mug shots"). Category 2 images include “images utilized for scientific analysis by subject matter experts.” This would include: latent prints, questioned documents, impression evidence, Category 1 images to be subjected to analysis, and patterned evidence. SWGIT suggests that Category 1 images need only rudimentary documentation that would describe what type of enhancement(s) was used. Category 2 images require a more detailed description of the enhancement, so that any changes would be clearly spelled out to an expert. SWGIT has also developed a number of standard operating practices (SOP) for digital and film based photography. These SOPs cover issues such as first responder photography, surveillance photography, tactical survey photography, HAZMAT scene photography, aerial photography, and accident scene photography.

The FBI and other agencies have already done much work, and we can benefit from that. ISASI could develop SOPs and “best practices” documentation for the accident investigation community. By using this work as a foundation, we can make digital photography more beneficial and reliable as evidence.

6. Current File Formats

There are some file formats that currently support supplemental information about the recorded image. These include Joint Photographic Experts Group (JPEG) and Tagged Image File Format (TIFF) Exchangeable Image File format (EXIF) and TIFF extensions. The need for a uniform file format standard for image data stored by digital still cameras has increased as these cameras have grown in popularity. At the same time, with the broadening application of this technology, a similar need has arisen for uniformity of the attribute information that can be recorded in a file. We will not go into a history of JPEG and TIFF file formats here, but we will discuss the EXIF and TIFF attribute information that can currently be recorded.

EXIF was developed by the Japan Electronic Industry Development Association (JEIDA) to be used in digital still cameras and related systems. Version 1.0 was first published in October 1996. Over time, changes have been made to make improvements to the EXIF

format for greater ease of use, while still allowing backward compatibility with products of manufacturers currently implementing EXIF Version 1.x or considering its future implementation. Version 2.1 contains the current recommended EXIF standards. The file-recording format is based on existing formats. Compressed files are recorded as JPEG (ISO/IEC 10918-1iv). Uncompressed files are recorded in TIFF Rev. 6.0v format. By using existing formats, photos taken using a digital still camera or related system can be read directly by commercial applications (ex: Adobe PhotoShop), and makes viewing and manipulating of the images possible. Related attribute information for both compressed and uncompressed files is stored in the tag information format defined in TIFF Rev. 6.0. Information specific to the camera system and not defined in TIFF is stored in private (manufacturer) tags registered for EXIF. The reason for using the TIFF Rev. 6.0 tag format in the compressed file is to facilitate exchange of attribute data between EXIF compressed and uncompressed files. A feature of EXIF image files is their compatibility with standard formats in wide use today, enabling them to be used on personal computers and in other information systems. The intention of JEIDA is to promote widespread use of digital still cameras. Figure 1 below shows what data are recorded under the TIFF Rev. 6.0 Attribute Information tags. Figures 2 & 3 show the fields that are recorded under EXIF. For a full description of all fields, please reference "Digital Still Camera Image File Format Standard (Exchangeable image file format for Digital Still Camera:EXIF), Version 2.1, JEIDA-49-1998)

EXIF allows more than just the recording of image specific attributes. EXIF also allows the recording of specific location information acquired by a GPS receiver. This is feature can be very beneficial in an accident investigation. Not only is latitude and longitude information captured, but other references such as GPS time (atomic clock), and reference points used to determine direction of movement and direction of image. Figure 4 shows a complete list of GPS attributes that can be recorded under EXIF.

While EXIF and TIFF extensions are very useful, they do have some limitations. If the images are opened in an application that does not support the readout of attributes, and then saved, the information will be lost. If that is the only copy of the image, then all electronically recorded history of that file will be lost. Another limitation is garbage-in garbage-out (GIGO). If the settings in the camera (ex: time and date) are not correct, then the values will be recorded incorrectly. Also, many camera manufacturers release firmware updates to fix minor "bugs" the camera's operating system. If there is a firmware problem, it is possible the correct data will not be recorded. Likewise the GPS location information will be limited to the accuracy of the data source. If a differential GPS system is not used, then the investigator runs the risk of the photos not matching up with the survey locations.

Figure 1

Tag Name	Field Name	Tag ID		Type	Count
		Dec	Hex		
A. Tags relating to image data structure					
Image width	ImageWidth	256	100	SHORT or LONG	1
Image height	ImageLength	257	101	SHORT or LONG	1
Number of bits per component	BitsPerSample	258	102	SHORT	3
Compression scheme	Compression	259	103	SHORT	1
Pixel composition	PhotometricInterpretation	262	106	SHORT	1
Orientation of image	Orientation	274	112	SHORT	1
Number of components	SamplesPerPixel	277	115	SHORT	1
Image data arrangement	PlanarConfiguration	284	11C	SHORT	1
Subsampling ratio of Y to C	YCbCrSubSampling	530	212	SHORT	2
Y and C positioning	YCbCrPositioning	531	213	SHORT	1
Image resolution in width direction	XResolution	282	11A	RATIONAL	1
Image resolution in height direction	YResolution	283	11B	RATIONAL	1
Unit of X and Y resolution	ResolutionUnit	296	128	SHORT	1
B. Tags relating to recording offset					
Image data location	StripOffsets	273	111	SHORT or LONG	*S
Number of rows per strip	RowsPerStrip	278	116	SHORT or LONG	1
Bytes per compressed strip	StripByteCounts	279	117	SHORT or LONG	*S
Offset to JPEG SOI	JPEGInterchangeFormat	513	201	LONG	1
Bytes of JPEG data	JPEGInterchangeFormatLength	514	202	LONG	1
C. Tags relating to image data characteristics					
Transfer function	TransferFunction	301	12D	SHORT	3 * 256
White point chromaticity	WhitePoint	318	13E	RATIONAL	2
Chromaticities of primaries	PrimaryChromaticities	319	13F	RATIONAL	6
Color space transformation matrix coefficients	YCbCrCoefficients	529	211	RATIONAL	3
Pair of black and white reference values	ReferenceBlackWhite	532	214	RATIONAL	6
D. Other tags					
File change date and time	DateTime	306	132	ASCII	20
Image title	ImageDescription	270	10E	ASCII	Any
Image input equipment manufacturer	Make	271	10F	ASCII	Any
Image input equipment model	Model	272	110	ASCII	Any
Software used	Software	305	131	ASCII	Any
Person who created the image	Artist	315	13B	ASCII	Any
Copyright holder	Copyright	3432	8298	ASCII	Any

Figure 2

Tag Name	Field Name	Tag ID Dec	Tag ID Hex	Type	Count
A. Tags Relating to Version					
Exif version	ExifVersion	36864	9000	UNDEFINED	4
Supported FlashPix version	FlashPixVersion	40960	A000	UNDEFINED	4
B. Tag Relating to Image Data Characteristics					
Color space information	ColorSpace	40961	A001	SHORT	1
C. Tags Relating to Image Configuration					
Meaning of each component	ComponentsConfiguration	37121	9101	UNDEFINED	4
Image compression mode	CompressedBitsPerPixel	37122	9102	RATIONAL	1
Valid image width	PixelXDimension	40962	A002	SHORT or LONG	1
Valid image height	PixelYDimension	40963	A003	SHORT or LONG	1
D. Tags Relating to User Information					
Manufacturer notes	MakerNote	37500	927C	UNDEFINED	Any
User comments	UserComment	37510	9286	UNDEFINED	Any
E. Tag Relating to Related File Information					
Related audio file	RelatedSoundFile	40964	A004	ASCII	13
F. Tags Relating to Date and Time					
Date and time of original data generation	DateTimeOriginal	36867	9003	ASCII	20
Date and time of digital data generation	DateTimeDigitized	36868	9004	ASCII	20
DateTime subseconds	SubSecTime	37520	9290	ASCII	Any
DateTimeOriginal subseconds	SubSecTimeOriginal	37521	9291	ASCII	Any
DateTimeDigitized subseconds	SubSecTimeDigitized	37522	9292	ASCII	Any
G. Tags Relating to Picture-Taking Conditions					
See Table 5					
H. Tags Relating to Date and Time					
Pointer of Interoperability IFD	Interoperability IFD Pointer	40965	A005	LONG	1

Figure 3

G. Tags Relating to Picture-Taking Conditions					
Exposure time	ExposureTime	33434	829A	RATIONAL	1
F number	FNumber	33437	829D	RATIONAL	1
Exposure program	ExposureProgram	34850	8822	SHORT	1
Spectral sensitivity	SpectralSensitivity	34852	8824	ASCII	Any
ISO speed rating	ISOSpeedRatings	34855	8827	SHORT	Any
Optoelectric conversion factor	OECF	34856	8828	UNDEFINED	Any
Shutter speed	ShutterSpeedValue	37377	9201	SRATIONAL	1
Aperture	ApertureValue	37378	9202	RATIONAL	1
Brightness	BrightnessValue	37379	9203	SRATIONAL	1
Exposure bias	ExposureBiasValue	37380	9204	SRATIONAL	1
Maximum lens aperture	MaxApertureValue	37381	9205	RATIONAL	1
Subject distance	SubjectDistance	37382	9206	RATIONAL	1
Metering mode	MeteringMode	37383	9207	SHORT	1
Light source	LightSource	37384	9208	SHORT	1
Flash	Flash	37385	9209	SHORT	1
Lens focal length	FocalLength	37386	920A	RATIONAL	1
Flash energy	FlashEnergy	41483	A20B	RATIONAL	1
Spatial frequency response	SpatialFrequencyResponse	41484	A20C	UNDEFINED	Any
Focal plane X resolution	FocalPlaneXResolution	41486	A20E	RATIONAL	1
Focal plane Y resolution	FocalPlaneYResolution	41487	A20F	RATIONAL	1
Focal plane resolution unit	FocalPlaneResolutionUnit	41488	A210	SHORT	1
Subject location	SubjectLocation	41492	A214	SHORT	2
Exposure index	ExposureIndex	41493	A215	RATIONAL	1
Sensing method	SensingMethod	41495	A217	SHORT	1
File source	FileSource	41728	A300	UNDEFINED	1
Scene type	SceneType	41729	A301	UNDEFINED	1
CFA pattern	CFAPattern	41730	A302	UNDEFINED	Any

Figure 4

Tag Name	Field Name	Tag ID		Type	Count
		Dec	Hex		
A. Tags Relating to GPS					
GPS tag version	GPSVersionID	0	0	BYTE	4
North or South Latitude	GPSLatitudeRef	1	1	ASCII	2
Latitude	GPSLatitude	2	2	RATIONAL	3
East or West Longitude	GPSLongitudeRef	3	3	ASCII	2
Longitude	GPSLongitude	4	4	RATIONAL	3
Altitude reference	GPSAltitudeRef	5	5	BYTE	1
Altitude	GPSAltitude	6	6	RATIONAL	1
GPS time (atomic clock)	GPSTimeStamp	7	7	RATIONAL	3
GPS satellites used for measurement	GPSSatellites	8	8	ASCII	Any
GPS receiver status	GPSStatus	9	9	ASCII	2
GPS measurement mode	GPSMeasureMode	10	A	ASCII	2
Measurement precision	GPSDOP	11	B	RATIONAL	1
Speed unit	GPSSpeedRef	12	C	ASCII	2
Speed of GPS receiver	GPSSpeed	13	D	RATIONAL	1
Reference for direction of movement	GPSTrackRef	14	E	ASCII	2
Direction of movement	GPSTrack	15	F	RATIONAL	1
Reference for direction of image	GPSImgDirectionRef	16	10	ASCII	2
Direction of image	GPSImgDirection	17	11	RATIONAL	1
Geodetic survey data used	GPSMapDatum	18	12	ASCII	Any
Reference for latitude of destination	GPSDestLatitudeRef	19	13	ASCII	2
Latitude of destination	GPSDestLatitude	20	14	RATIONAL	3
Reference for longitude of destination	GPSDestLongitudeRef	21	15	ASCII	2
Longitude of destination	GPSDestLongitude	22	16	RATIONAL	3
Reference for bearing of destination	GPSDestBearingRef	23	17	ASCII	2
Bearing of destination	GPSDestBearing	24	18	RATIONAL	1
Reference for distance to destination	GPSDestDistanceRef	25	19	ASCII	2
Distance to destination	GPSDestDistance	26	1A	RATIONAL	1

7. What is needed in a standard for investigations

Now that we have looked at the attributes that are currently recordable for digital photos, let's look at what attributes would be considered essential for accident investigation. These include: date and time the photo was taken, camera settings (exposure, etc), where taken (GPS info), the name of the photographer, notification of any alterations of the file, and a layer of the image that shows the original unaltered image.

Date and time are important and easily recorded. Validity of this data, however, must be assured as well and is not quite as straightforward. The source of this data can be the camera's internal clock or GPS input. The GPS input would be preferable as it cannot be set incorrectly. If the internal clock is used, then it should be adjusted to the same time format and zone that the investigating agency is using (ex: local or ZULU). Camera (equipment type) information is recorded under both the TIFF extensions and EXIF, but camera settings and condition information is only available under EXIF. This type of data includes: exposure time, F number, ISO speed rating, shutter speed, flash, exposure program, light source, etc. (For a detailed list see Figures 2 and 3 in the preceding section. When the image file is opened in an application that supports EXIF, this data can be viewed, making highly detailed log sheets in the field unnecessary. Information such as the exact location of where a photo was taken and direction are also very

important to know. With investigations increasingly using more digitized data from the surveys of accident sites, the ability to bring in latitude and longitude information, as well as the direction the photo was taken becomes even more valuable. Being able to map out the location of a photo in respect to a specific part or piece of wreckage using precise (differential GPS) measurements is very valuable in post field activities. If the camera is set properly, both TIFF extensions and EXIF can record the name of the photographer. This is very important in investigations involving multiple parties or agencies, in order to keep the source known. If all that is left at the end of an investigation is a CD full of JPEG files, and no information on the photographer, you cannot be assured of the chain of custody of the images.

There are two other requirements for digital images used in an investigation that are not currently addressed under these formats. The first is the ability to log any alterations or modifications of the file. Any time there is a modification, or a filter is used on an image in an application, there must be a log of those changes. This would allow anyone in the investigation to determine the authenticity of an image. The second is a "layer" of the image that would remain unaltered. This would be similar to Adobe PhotoShop's layering system, except that the base layer would never change. Notations, filters, or other processes could be done on the photo, but the base photo cannot be changed. This allows all parties to recover the original, unaltered image. By using these two features together, the history of a digital image could be viewed by anyone examining the electronic version of an image. It should be noted, though, that these safeguards would not prevent an illicitly altered image from being printed and represented as accurate. Ultimately, a process would have to be developed that not only made the electronic image's authenticity verifiable, but also prevented an altered image from being printed without an indication that it had been altered.

8. An industry group is needed to define and develop the standard

In order to address the issues identified above, a series of standards is necessary. These standards would encompass a format for digital media that allows "audit" of the authenticity as well as a number of processes that would ensure that authenticity of both the electronic and printed form of digital photographs could be verified. As noted above, the need for this "secure video" capability extends beyond the aircraft accident investigation community. Any discipline that relies on authentic photographs would be affected. All modes of transportation accident investigation, law enforcement and insurance companies all have similar interests, as would a variety of government agencies. Representatives of these groups, along with camera and image processing experts, should be brought together in a cooperative government-industry group to develop standards for "secure" digital photographs. These standards and processes would ultimately result in a means to take, store, enhance, clarify, edit, copy and print digital photographs while maintaining the capability to recover the original image and identify all changes made to it.

Standards setting is never easy – competing interests must be balanced and somebody has to pay for the changes to the status quo. Nevertheless, absence of a means to ensure that photographs taken cannot be altered without irrevocable evidence of that alteration has the potential to result in significant cost to the industry if manufacturing and operations are affected by erroneous conclusions drawn from and investigation based on flawed evidence. As the capability to take extremely high quality digital photographs and distribute them instantly around the world expands; as the capability to make changes to digital photographs becomes ever more sophisticated; and as the potential cost of accidents becomes higher, the need for digital photographs whose authenticity can be positively determined will similarly increase. The characteristics identified by the SWGIT group and listed above (Section 5) are straightforward. The original image must be preserved and be recoverable; change must be allowed but must also be logged or tracked; and the enhanced or changed image must be clearly identifiable as such. Defining the changes necessary to hardware, software and processes would not be difficult. Implementing them in an industry-standard form would be. A standard is nevertheless needed that can be applied to newly manufactured cameras, retrofit into existing ones, and supported by image editing software. The aircraft accident investigation community has before it an opportunity to take a leadership role in an effort to proactively improve upon a technology to the benefit of all investigations and related activity. We should act on that opportunity now.