Survey of Disk Image Storage Formats

Version 1.0

Common Digital Evidence Storage Format Working Group
Digital Forensic Research Workshop

September 1, 2006

Digital data that could be used as evidence are typically stored in specialized and closed formats, which typically also include metadata about the evidence. Closed formats limit the number of tools and analysis techniques that can be used on the data. The goal of the Common Digital Evidence Storage Format (CDESF) working group is to define a storage format that is open and accepted by the community.

The first step in this process is to define what currently exists. To assess the state of the field, the CDESF working group surveyed the following disk image formats: raw, AFF, DEB (Qinetiq), EnCase, Expert Witness, gfzip, ProDiscover, and SMART. This document contains the working group findings after evaluating the storage formats using several criteria, such as publication status, extensibility, and metadata that are stored. A survey table for each format can be found in the Appendix.

Overview of Formats

The details of the various formats will be described in the following sections. This section provides a brief overview of each format that is addressed in this document and links to web sites that documents that have more information.

The Advanced Forensic Format (AFF) is from Simson Garfinkel and Basis Technology. The format is open and comes in three variants: AFF, AFD, and AFM. AFF stores all data and metadata in a single file, AFD stores the data and metadata in multiple small files, and AFM stores the data in a raw format and the metadata is stored in a separate file.

http://www.afflib.org

There are two independent formats that use the name Digital Evidence Bag (DEB). The first one we discuss is from Philip Turner and Qinetiq. The format is open and was first presented in a paper at DFRWS 2005. It uses a number of files to store the evidence and associated metadata. The metadata are stored in ASCII files. Tools for the format have not been publicly released.

The second DEB format is from Wetstone Technology. This format uses XML to store the evidence and metadata. The format was developed as research for the Air Force

Research Labs and will be made available. It is not currently used for storing disk images and therefore is not mentioned elsewhere in this survey.

The EnCase format is a closed format that is defined by Guidance Software for use in their EnCase tool to store hard drive images and individual files. Its predecessor format is the Expert Witness format, which has been publicly documented. The EnCase format has added new metadata to the original Expert Witness format.

http://www.encase.com
http://www.asrdata.com/SMART/whitepaper.html
EnCase Legal Journal, November 2005.
http://www.guidancesoftware.com/commercial/legalresources.asp

The Generic Forensic Zip (Gfzip) format is from Rob J Meijer. Its design is open and uses data structures similar to AFF. The metadata and storage approach are different though. A gfzip file can be 'raw' compatible so that the metadata is stored after the evidence data and it also offers a 'packed' mode where redundant blocks of data are not stored.

http://savannah.nongnu.org/projects/gfzip/

The iXImager format is used by the iLook tool, which is developed by the U.S. Internal Revenue Service (IRS) and is restricted to law enforcement and government use only. The format is proprietary and the iLook team would not verify the information we collected about the format. Therefore, it is not included in the survey.

http://www.ilook-forensics.org/

The ProDiscover format was defined by Technology Pathways for use in their products to store hard drive images. The format is open and has a published specification.

http://www.techpathways.com/uploads/ProDiscoverImageFileFormatv4.pdf

The raw format is simply a file that contains the exact data that needs to be stored and the file could contain any type of data, including hard disk sectors, files, and network packets. Raw files can be easily created and read by any tool, but they do not store any metadata and are not compressed.

There are two SMART formats, which are defined by ASR Data for their products to store hard drive data. The default format stores the metadata in a separate text file where the contents can be easily viewed, but the exact layout has not been published. The second format, which we will call the SMART Expert Witness Compression format, is based on the original Expert Witness format.

http://www.asrdata.com/

Publication and Patent Status

Storage formats whose details have not been published can create difficulties for individuals who do not have the access or ability to use the limited number of tools that can read such files. Converting between proprietary formats may result in incorrect data,

missing metadata, and lost time. Even open file formats that are well documented can be data prisons if the format lacks sufficient expressiveness for the information the investigator needs to embody, or if the standard is so complicated it cannot be implemented correctly.

The AFF, Expert Witness, Gfzip, and ProDiscover formats are published and are not covered by any patents that we know of. The Qinetiq DEB format is published and patent pending. The EnCase and SMART Expert Witness Compressed image formats are not published. The default SMART format uses a raw file to store the data and the metadata are stored in a text file that is organized using a proplist structure, but the properties that are defined in the file have not been published. Open source implementations of AFF, Expert Witness, EnCase, and Gfzip exist (although not all are by the format's designers). Technology Pathways will provide an implementation of its ProDiscover format upon request.

Software Support

The majority of forensic analysis applications can read the raw format, making it the de facto standard. The other formats that were surveyed can only be read by a limited number of tools apart from those used to create them. Table 1 shows which storage formats can be read using various publicly available tools. Note that any tool that supports the raw format can read the raw data in the AFM, gfzip, and SMART default formats, but those tools are not listed in the table because they are not reading the metadata in the format. A check exists only if the tool reads the metadata, if it exists.

Table 1: Matrix of file formats and the tools that support them.

	AFF	DEB (Qinetiq)	EnCase	Expert Witness	Gfzip	ProDisc	Raw	SMART Default	SMART Comp
AFFlib:	✓		✓	✓	[1]		✓		
EnCase:			✓	✓			✓		
FTK:			✓	✓			✓		✓
ProDiscover:						✓	✓		
Sleuth Kit	✓		✓	✓	[1]		✓		
SMART:			✓	✓			✓	✓	✓
X-Ways:			✓	✓			✓		

[1]: Gfzip has an AFF compatibility mode.

Metadata

One of the benefits of using a specialized storage format is the ability to store metadata about the data. All forensic image storage formats, except the raw format, have this feature. For example, we may want to store a hard drive's serial number, the date and place that the drive was imaged, and a digital signature or cryptographic checksum to verify the data's integrity. This section describes a high level overview of where the metadata are stored and what metadata are stored.

There are two basic approaches to storing metadata. One is to embed the metadata in the same file as the evidence and the second is to store the metadata in a separate file (which

means that the evidence could be in a raw format). The AFF (specifically the AFF and AFD formats), EnCase, Gfzip, ProDiscover, SMART Expert Witness formats use the first approach and embed the metadata in the same file as the evidence. The AFM (a type of AFF), Qinetiq DEB, and SMART default formats use one or more separate files for the metadata. Gfzip can embed metadata using the same approach as AFF or it can embed the metadata at the end of the file. In the latter case, there is no Gfzip header and the file starts with the raw evidence. Therefore, tools that support the raw format can read the evidence from this file, although keyword searches may find hits in the metadata section if the tool is not aware of the Gfzip format.

Most formats have a limited number of metadata types that can be stored. Common metadata includes case and evidence numbers, examiner name, description, time, and integrity information (e.g., MD5 hash of the data). Some formats allow only ASCII characters to be used and others support Unicode. AFF and Gfzip seem to be unique in that they allow arbitrary metadata to be stored. Note that some of the other formats may be capable of storing arbitrary metadata, but we were not aware of the feature because the format was not open and we did not know the internal data structures.

Qinetiq DEB was the only format surveyed that already included support for a log to record chain of custody information.

Splitting

The amount of data that must be stored can be very large and it may need to be broken up into multiple files. This occurs when the data are stored to a FAT32 file system or when the data are written to an optical drive for backup.

All of the surveyed formats allow the data to be broken into smaller segments (a.k.a. splits). The file name extension is typically used to order the files. In the case of AFF, the AFD format must be used, which stores the split files in a directory. EnCase supports splitting and numbers each segment with a sequential extension (E01... Enn). In addition, each file has information to determine its sequence number. Similarly, the SMART Expert Witness format numbers each segment with a sequential extension (S01... Snn) and the SMART Default format uses numbers in its extension, starting with .001. ProDiscover creates a separate file that contains information about the split files, and also embeds the “current split image number” and “total number of splits” within each segment.

Compression

It can be useful to compress data that are being stored. This reduces the amount of storage space that is required to store the evidence, but it may cause the acquisition time to increase as well as the time to read data from the image.

With the exception of the raw format, all storage formats support some level of compression. In most cases, the exact algorithm is not known. The tool that creates the storage files will typically provide an option to control how much to compress the data based on the time to compress versus storage size tradeoff.

Gfzip can "pack" images by creating an index of blocks of data. Each unique block is stored only once and is referenced when it occurs in the evidence. This means that redundant blocks are not stored.

Integrity Information

If a storage format becomes corrupt, then it is important for the investigator to determine this and isolate the damage. With existing formats, this is performed by calculating and storing hash values for chunks of data. If a chunk becomes corrupt then an analysis tool can choose to not use the data in that chunk, but can still use other data. AFF, DEB, EnCase, Expert Witness, and SMART all provide this feature using a combination of CRC and MD5 hashes.

To prove the integrity of data, a cryptographic signature is also needed because a malicious person could modify the evidence and simply recalculate the corresponding hash values. A cryptographic signature from a properly secured key could make this much more difficult. Of the surveyed formats, only the default SMART format includes a cryptographic signature. Plans exist for AFF and gfzip to include a signature in future versions.

Error Information

In some cases, errors may occur when trying to read the data that will be stored in the storage format. For example, if the contents of a disk are being stored then there could be a hardware issue that prevents data from being read.

When the raw format is being used, a common approach is to store 0s in place of the data that could not be read. However, this prevents the investigator and tools from being able to distinguish between sectors that contain all 0s and those that could not be read.

Some formats record information about bad sectors that were encountered and other I/O errors. For instance, EnCase, Expert Witness, and SMART store a comprehensive list of bad sectors. The last part of the ProDiscover image file contains any I/O errors encountered during image capture. AFF 1.0 has a system called "badflag" which is a per-image flag to denote bad data. Future versions of AFF will have a bitfield per page denoting which sectors are bad, weren't read, or have been redacted. The Gfzip format can also flag sections as bad.

Other Features

There are other features of each format that did not fit into the previous categories. One advantage of the raw format is that it can be accessed directly, without additional transformation/interpretation methods, by hardware. This reduces the places that errors can be introduced. EnCase uses password access control, but the data are not encrypted and the password can therefore be bypassed. The ProDiscover format can also include a

password, but, like Encase, it can be bypassed. The gfzip format currently includes a draft proposal for encrypted image files.

Acknowledgements

Members of the CDESF working group collected the survey data. A draft of the survey was sent to the vendors. Thanks to Andy Rosen and Jeff Meininger at ASR Data, Christopher Brown at Technology Pathways, and Robert Miejer for their review and clarifications.

Working Group Members

Frank Adelstein (ATC-NY)
Brian Carrier (Basis Technology)
Eoghan Casey (Stroz Friedberg, LLC)
Simson L. Garfinkel (Harvard University)
Chet Hosmer (Wetstone Technologies, Inc.)
Jesse Kornblum (ManTech CFIA)
Jim Lyle (National Institute of Standards and Technology)
Marcus Rogers (Purdue University)
Phil Turner (Qinetiq)

Appendix – Surveys

Raw Format

Format Name:	Raw
Version:	n/a
Supporting Organization:	Many
Is the format published?	No
Is the format covered by any patents or license? If so, which ones?	No
What products currently create or read the format?	All forensic programs surveyed read the raw format. Raw images can be created using Unix/Linux 'dd' utility, Access Data FTK Imager, ProDiscover, and SMART.
What types of digital evidence can it store (i.e. disk images, files, network packets, tool output, arbitrary)?	Disk images of any block device, including hard drives, logical volumes, and device memory
Can the evidence be broken up into multiple files? If so, what file name and extension requirements exist?	Yes using Unix/Linux 'split' utility, FTK Imager option. No standard file name or extension requirements exist.
Does the format also store metadata? (if not, then stop)	No
Are the metadata and digital evidence stored in a single file, multiple files, or either?	n/a
If multiple files, is the evidence in a separate file from the metadata?	n/a
If multiple files, what format is the evidence stored as?	n/a
Can arbitrary metadata be stored?	n/a
What provenance metadata can be stored (i.e. acquisition date, drive id)?	n/a
What integrity metadata can be stored (i.e. hashes, digital signatures)?	n/a
What access / chain of custody metadata can be stored?	n/a
What distributed processing metadata can be stored?	n/a
What other metadata can be stored (i.e. version format number)?	
What format is used to encode the metadata (i.e. ASCII, XML, linked list)?	n/a
Does the format support metadata with international characters (i.e. Unicode)?	n/a
Can the format document which locations in the	n/a

evidence could not be read because of bad media?	
If the format has evidence integrity metadata, is there one piece of integrity information for the evidence as a whole or for smaller pieces to isolate problems?	n/a
Does the format allow the evidence to be compressed? If so, what algorithms are supported?	n/a
What other unique characteristics does this format have?	n/a

AFF

Format Name:	Advanced Forensic Format (AFF)
Version:	1.0
Supporting Organization:	Simson Garfinkel & Basis Technology Corp.
Is the format published?	Yes
Is the format covered by any patents or license? If so, which ones?	No
What products currently create or read the format?	AFF tools.
What types of digital evidence can it store (i.e. disk images, files, network packets, tool output, arbitrary)?	Currently schemas are defined for disk images. Can be extended to store any type of digital evidence.
Can the evidence be broken up into multiple files? If so, what file name and extension requirements exist?	Yes. The AFF library will automatically treat all AFF files stored in a single ".afd" directory as multiple files for a single "meta-file."
Does the format also store metadata? (if not, then stop)	Yes
Are the metadata and digital evidence stored in a single file, multiple files, or either?	Either
If multiple files, is the evidence in a separate file from the metadata?	User defined. Metadata can be stored in the same file as evidence, or in a separate file.
If multiple files, what format is the evidence stored as?	AFF binary format or AFF XML format.
Can arbitrary metadata be stored?	Yes. Any number of name/value pairs.
What provenance metadata can be stored (i.e. acquisition date, drive id)?	Case Number, Examiner, Evidence Number, Unique Description, Serial Number, Current Time, Notes, and any other information that you want to

	define in the aimage configuration file.
What integrity metadata can be stored (i.e. hashes, digital signatures)?	MD5 hash over whole image, MD5 over individual "pages," MD5 over metadata segments.
What access / chain of custody metadata can be stored?	User defined. Any number of name/value pairs.
What distributed processing metadata can be stored?	User defined. Any number of name/value pairs.
What other metadata can be stored (i.e. version format number)?	User defined. Any number of name/value pairs.
What format is used to encode the metadata (i.e. ASCII, XML, linked list)?	UTF8, which can be stored in AFF binary or XML.
Does the format support metadata with international characters (i.e. Unicode)?	Yes
Can the format document which locations in the evidence could not be read because of bad media?	Yes
If the format has evidence integrity metadata, is there one piece of integrity information for the evidence as a whole or for smaller pieces to isolate problems?	MD5 hash over whole image, and of individual pages.
Does the format allow the evidence to be compressed? If so, what algorithms are supported?	Yes: zlib with compression levels of 1 through 9.
What other unique characteristics does this format have?	

DEB

Format Name:	Digital Evidence Bags (DEB)
Version:	0.81
Supporting Organization:	QinetiQ
Is the format published?	Yes, limited release
Is the format covered by any patents or license? If so, which ones?	
What products currently create or read the format?	DEB Viewer, DEB Selective Imager, DEB command line application wrapper
What types of digital evidence can it store (i.e. disk images, files, network packets, tool output, arbitrary)?	Potentially anything but at the moment disk images, files, tool output, logs etc.
Can the evidence be broken up into multiple files? If so, what file name and extension requirements exist?	Yes .Inn = numbered Index files, .Bnn = numbered Bag files

Does the format also store metadata? (if not, then stop)	Yes
Are the metadata and digital evidence stored in a single file, multiple files, or either?	Multiple.
If multiple files, is the evidence in a separate file from the metadata?	Yes - evidence in Bag file, metadata in Tag and Index files.
If multiple files, what format is the evidence stored as?	Binary dump in bag file. The Bag file may be compressed / encrypted but this is not implemented yet.
Can arbitrary metadata be stored?	Yes.
What provenance metadata can be stored (i.e. acquisition date, drive id)?	Investigating Agency, Investigating Officer, Exhibit, Description, Location, Task Reference, DEB Created Date & Time, Host ID, Device Descriptor, Device Manufacturer, Device model, Device Serial Number
What integrity metadata can be stored (i.e. hashes, digital signatures)?	Hashes. Encryption to be supported.
What access / chain of custody metadata can be stored?	Date & Time, Application ID, Application Version, Application Signature, Application Function, Host ID, DEB Components Accessed
What distributed processing metadata can be stored?	Host ID
What other metadata can be stored (i.e. version format number)?	Version ID
What format is used to encode the metadata (i.e. ASCII, XML, linked list)?	ASCII
Does the format support metadata with international characters (i.e. Unicode)?	Not currently.
Can the format document which locations in the evidence could not be read because of bad media?	Not currently.
If the format has evidence integrity metadata, is there one piece of integrity information for the evidence as a whole or for smaller pieces to isolate problems?	Yes - a hashes over the tag, index and bag files and hashes over individual components with the bag file.
Does the format allow the evidence to be compressed? If so, what algorithms are supported?	Compression is supported, but not implemented yet.
What other unique characteristics does this format have?	The DEB format could be used to store data from any arbitrary source, whether from a static environment or real time packet capture or command line application. The format could be used as a wrapper for existing formats

	thus providing a migration path for current systems and formats.

EnCase

Format Name:	EnCase Evidence File - E01
Version:	v3 /v4 /v5
Supporting Organization:	Guidance Software Inc.
Is the format published?	Partially
Is the format covered by any patents or license? If so, which ones?	Unknown
What products currently create or read the format?	Encase and FTK Imager can create EnCase image files in this format. AFF, EnCase, FTK, SMART, Sleuth Kit, X-Ways can read this format.
What types of digital evidence can it store (i.e. disk images, files, network packets, tool output, arbitrary)?	Disk images and Palm Pilot memory
Can the evidence be broken up into multiple files? If so, what file name and extension requirements exist?	Yes, with file extension E01.. Enn
Does the format also store metadata? (if not, then stop)	Yes
Are the metadata and digital evidence stored in a single file, multiple files, or either?	Either
If multiple files, is the evidence in a separate file from the metadata?	No
If multiple files, what format is the evidence stored as?	n/a
Can arbitrary metadata be stored?	A notes field exists for arbitrary text.
What provenance metadata can be stored (i.e. acquisition date, drive id)?	Case Number, Examiner, Evidence Number, Unique Description, Current Time, Notes
What integrity metadata can be stored (i.e. hashes, digital signatures)?	MD5 hash over whole image, CRC over 32K(Encase v3, V4) block, User selectable block size - V5
What access / chain of custody metadata can be stored?	None
What distributed processing metadata can be stored?	None
What other metadata can be stored (i.e. version format number)?	None
What format is used to encode the metadata	Special data structures

(i.e. ASCII, XML, linked list)?	
Does the format support metadata with international characters (i.e. Unicode)?	Yes
Can the format document which locations in the evidence could not be read because of bad media?	Yes
If the format has evidence integrity metadata, is there one piece of integrity information for the evidence as a whole or for smaller pieces to isolate problems?	MD5 hash over whole image, CRC over 32K(Encase v3, V4) block, User selectable block size - V5
Does the format allow the evidence to be compressed? If so, what algorithms are supported?	Yes: Zlib (“good” and “best”)
What other unique characteristics does this format have?	Password access control for use with GSI applications

Gfzip

Format Name:	Generic Forensic Zip (gfzip)
Version:	1.0 draft version 5 (encryption is still in potential state of flux)
Supporting Organization:	
Is the format published?	Yes
Is the format covered by any patents or license? If so, which ones?	No
What products currently create or read the format?	Last addition (encryption) currently in peer review, libgfz is to be build based on the final 1.0 file format specification.
What types of digital evidence can it store (i.e. disk images, files, network packets, tool output, arbitrary)?	Images of block devices, both as separate images and in packed archives.
Can the evidence be broken up into multiple files? If so, what file name and extension requirements exist?	Yes. But only by using packed archives that are meant to store multiple images.
Does the format also store metadata? (if not, then stop)	Yes
Are the metadata and digital evidence stored in a single file, multiple files, or either?	The metadata is always stored in the image file, the digital evidence optionally in a packed archive file.
If multiple files, is the evidence in a separate file from the metadata?	Configurable. Metadata can be stored in the same file as evidence, or in a 'shared' packed archive that consists of multiple files.

If multiple files, what format is the evidence stored as?	In packed archive files containing digest ordered compressed data chunks that are referred to from the image files.
Can arbitrary metadata be stored?	Yes. See AFF
What provenance metadata can be stored (i.e. acquisition date, drive id)?	See AFF.
What integrity metadata can be stored (i.e. hashes, digital signatures)?	For legacy purposes SHA1 and MD5 of the full image. All 'real' integrity guards are provided by SHA256 digests, x509 and crypto graphical signing. This includes chain of custody guards provided by cryptographic file partition chaining.
What access / chain of custody metadata can be stored?	Chain of custody is provided by individually signed metadata partitions that are cryptographically chained together to represent the chain of custody.
What distributed processing metadata can be stored?	User defined. Any number of name/value pairs.
What other metadata can be stored (i.e. version format number)?	User defined. Any number of name/value pairs.
What format is used to encode the metadata (i.e. ASCII, XML, linked list)?	UTF, x509 certificates.
Does the format support metadata with international characters (i.e. Unicode)?	Yes
Can the format document which locations in the evidence could not be read because of bad media?	Yes
If the format has evidence integrity metadata, is there one piece of integrity information for the evidence as a whole or for smaller pieces to isolate problems?	SHA1,MD5 for AFF compatibility, SHA256 as 'real' guard suitable also for packed archive usage, used at multiple levels, SHA256,x509 and cryptographic signing for file partitions and chaining of file partitions for chain of custody recording purposes.
Does the format allow the evidence to be compressed? If so, what algorithms are supported?	Yes: zlib on a per block level and SHA256 indexed packing.

What other unique characteristics does this format have?	• Support for packed archives. • Data first compatibility modes for raw and aff compatibility. • X509 pki integration for integrity and chain of custody • Cryptographic chain of custody guarding. • Abandoning of legacy digest algoritms. • (Draft) support for x509 pki based encrypted storage.

ProDiscover

Format Name:	ProDiscover
Version:	1.3
Supporting Organization:	ProDiscover
Is the format published?	Yes
Is the format covered by any patents or license? If so, which ones?	No patents. The specification is copyright protected.
What products currently create or read the format?	ProDiscover.
What types of digital evidence can it store (i.e. disk images, files, network packets, tool output, arbitrary)?	Physical Disk, Physical Partition, Raw Physical Memory, Raw CMOS, and Raw BIOS
Can the evidence be broken up into multiple files? If so, what file name and extension requirements exist?	Yes. List of segments are stored in a separate file, and each segment stores the current segment number and total number of segment.
Does the format also store metadata? (if not, then stop)	Yes
Are the metadata and digital evidence stored in a single file, multiple files, or either?	Either
If multiple files, is the evidence in a separate file from the metadata?	No
If multiple files, what format is the evidence stored as?	n/a
Can arbitrary metadata be stored?	No
What provenance metadata can be stored (i.e. acquisition date, drive id)?	Image Number, Examiner name, Unique Description, Image Capture Time, Image System Time, the name of source disk, a hard disk make string, time zone information.
What integrity metadata can be stored (i.e.	MD5, SHA1, and/or SHA256 hash of

hashes, digital signatures)?	whole image
What access / chain of custody metadata can be stored?	None
What distributed processing metadata can be stored?	None
What other metadata can be stored (i.e. version format number)?	Total number of sector, original data size, starting sector of ATA host protected area, file system type, etc. (see documentation for more)
What format is used to encode the metadata (i.e. ASCII, XML, linked list)?	Special data structures
Does the format support metadata with international characters (i.e. Unicode)?	No
Can the format document which locations in the evidence could not be read because of bad media?	Yes
If the format has evidence integrity metadata, is there one piece of integrity information for the evidence as a whole or for smaller pieces to isolate problems?	No
Does the format allow the evidence to be compressed? If so, what algorithms are supported?	Yes. aPLib 32 bit Compression Library
What other unique characteristics does this format have?	Password access control for use with ProDiscover products

SMART Default

Format Name:	SMART Default
Version:	n/a
Supporting Organization:	ASR Data
Is the format published?	No, but metadata are stored in text proplist format
Is the format covered by any patents or license? If so, which ones?	Unknown
What products currently create or read the format?	SMART
What types of digital evidence can it store (i.e. disk images, files, network packets, tool output, arbitrary)?	Disk images, including hard drives and logical volumes
Can the evidence be broken up into multiple files? If so, what file name and extension requirements exist?	Yes, with names image.001, .image.002 (...) for data and .image.info for metadata.
Does the format also store metadata? (if not,	Yes

then stop)	
Are the metadata and digital evidence stored in a single file, multiple files, or either?	Multiple
If multiple files, is the evidence in a separate file from the metadata?	Yes
If multiple files, what format is the evidence stored as?	Raw, with option for compression
Can arbitrary metadata be stored?	Only limited amount in Notes field
What provenance metadata can be stored (i.e. acquisition date, drive id)?	Case Number, Examiner, Evidence Number, Unique Description, Current Time, Notes
What integrity metadata can be stored (i.e. hashes, digital signatures)?	MD5, CRC32, and SHA1 hashes of whole disk, image segment files, partition and partition waste space spans, and hashes of contiguous error-free data segments if there are read errors. Also, metadata is protected by a signature.
What access / chain of custody metadata can be stored?	None
What distributed processing metadata can be stored?	None
What other metadata can be stored (i.e. version format number)?	None
What format is used to encode the metadata (i.e. ASCII, XML, linked list)?	ASCII, in proplist format
Does the format support metadata with international characters (i.e. Unicode)?	No
Can the format document which locations in the evidence could not be read because of bad media?	Unknown
If the format has evidence integrity metadata, is there one piece of integrity information for the evidence as a whole or for smaller pieces to isolate problems?	MD5 hash over whole image, CRC over 32K block
Does the format allow the evidence to be compressed? If so, what algorithms are supported?	Yes: zlib (gz) and bzip2.
What other unique characteristics does this format have?	n/a

SMART Expert Witness Compressed

Format Name:	SMART Expert Witness Compress
Version:	n/a

Supporting Organization:	ASR Data
Is the format published?	Partially
Is the format covered by any patents or license? If so, which ones?	Unknown
What products currently create or read the format?	SMART and FTK Imager
What types of digital evidence can it store (i.e. disk images, files, network packets, tool output, arbitrary)?	Disk images, including hard drives and logical volumes
Can the evidence be broken up into multiple files? If so, what file name and extension requirements exist?	Yes, with file extension S01.. Snn
Does the format also store metadata? (if not, then stop)	Yes
Are the metadata and digital evidence stored in a single file, multiple files, or either?	Multiple
If multiple files, is the evidence in a separate file from the metadata?	Yes
If multiple files, what format is the evidence stored as?	Compressed raw
Can arbitrary metadata be stored?	Only limited amount in Notes field
What provenance metadata can be stored (i.e. acquisition date, drive id)?	Case Number, Examiner, Evidence Number, Unique Description, Current Time, Notes
What integrity metadata can be stored (i.e. hashes, digital signatures)?	MD5 hash over whole image, CRC over 32K block
What access / chain of custody metadata can be stored?	None
What distributed processing metadata can be stored?	None
What other metadata can be stored (i.e. version format number)?	None
What format is used to encode the metadata (i.e. ASCII, XML, linked list)?	Internal data structures
Does the format support metadata with international characters (i.e. Unicode)?	No
Can the format document which locations in the evidence could not be read because of bad media?	Unknown
If the format has evidence integrity metadata, is there one piece of integrity information for the evidence as a whole or for smaller pieces to isolate problems?	MD5 hash over whole image, CRC over 32K block
Does the format allow the evidence to be compressed? If so, what algorithms are	Yes: zlib (fastest)

supported?	
What other unique characteristics does this format have?	n/a