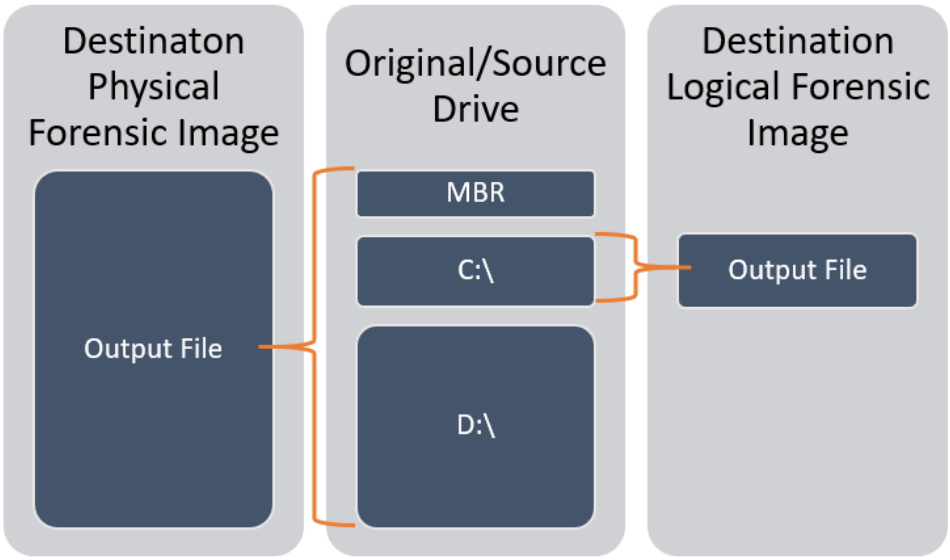
Forensic Imaging Processes, Procedures and Type Comparisons

USAForensic Standards for Proper Handling of Evidence Drives:

- Hot/Live forensic anti-stat extraction of any computers already powered on, or those in a hibernation or sleep-mode to gather active RAM & cache data.
    - RAM & cache data hold temporary information that is queued up for quick access while the computer is running. When the computer is turned off, RAM clears itself and most key cache files also reset.
    - Gathering this information, in the event the computer is *not* turned off, is crucial to getting the most data from the computer being examined.
- Dead forensic image using the latest Tableau hardware write blocker (or similar) with most current certified-stable firmware for cloning. This is for any computer that is already powered off when discovered.
    - Hardware write blockers ensure no data can be written back to the source drive. This is a critical piece to preserving evidence in its original state.
    - Software write blockers are not acceptable for forensic images, as they are just not as reliable as hardware (physical) write blockers.
- Use RAW(DD) format when creating a forensic image of original drive(s).
    - RAW(DD) forensic images are a sector-for-sector copy of the original drive. There is *zero* compression natively with this format, and the sector order is identical to the source drive.
    - Studies have shown that compressed forensic images of all types have the potential to destroy data through the process used to compress files (bzip, zlib for example).
- Use Western Digital Pro Red 7200RPM drives for the forensic images, which we will provide.
    - There's a much lower fail and read/write error rate when using better drives. This means both faster analysis, and more accurate analysis than with traditional "budget" drives.
    - 7200RPM drives with 128MB cache will speed up forensic image creation and data analysis, which saves time and money in the long run.
- Use the latest version of AccessData's FTK Imager for forensic image creation.
    - This widely-used and well-respected program creates forensic images with dependable results.

Physical vs Logical Forensic Images:

When beginning the forensic imaging process, the forensic expert must choose either a Physical or Logical source. Physical images target the entire source drive's contents, not just a portion of it. Logical Images are restricted to a single partition on the source drive. On a modern drive with Windows 10, a standard system has 3 partitions. On an advanced user's computer, there can be several more partitions. To eliminate any potential for missing data during forensic imaging, Physical images are always the preferred choice.



Forensic Image Types:

There are several Forensic Image format options available when making copies of evidence. The primary 2 are discussed within this document and are listed below in green and blue. The other formats listed are frankly not relevant or applicable, but potentially still used in the forensic field in rare/specific situations. Snippets from a published Harvard study are included throughout this document, and these formats are compared to one another.

RAW (IMG, DD)
EWF-E01 (EWCF-ASR02)
ISO
BIN/CUE
AFFv1-3 (AFF, AFD, AFM)
EWF-L01
S01 (.001)
AFF4
EWF2-Lx01
EWF2-Ex01

Forensic Image Type Details:

RAW(DD) Forensic Images
Description: Raw formats represent unstructured byte sequences captured from physical or logical volumes. Many extensions have been used in the past when raw disk images were created. .raw, .dd, .img and .001 are some of the more popular file extensions. These represent any image that is solely an uncompressed sector-by-sector copy of stored bits (with no additional headers/footers/structure/metadata). Raw(DD) forensic images are a sector-by-sector copy of the source drive. During the forensic imaging process, the source drive's individual sectors are read in order starting at the beginning, then written to the destination file(s) in the exact same order in which they exist on the source drive. The application handling this process does not rearrange the sectors or try to optimize data in any way. The resulting data set is an identical copy of the original, and easily readable by the examiner. This format is fully compatible with the common forensic analysis tools (such as EnCase, Autopsy, X-Ways, etc.), and is not proprietary to one specific brand or platform. This format also supports mounting the image as a virtual drive, for manual navigation through the filesystem by a forensic expert. This is a key feature, as the "push-button forensic" programs commonly used by Law Enforcement often don't have the methods/tools necessary to parse buried data, or the means to fully track the origins of a file.

Output File(s)/Image Segments:

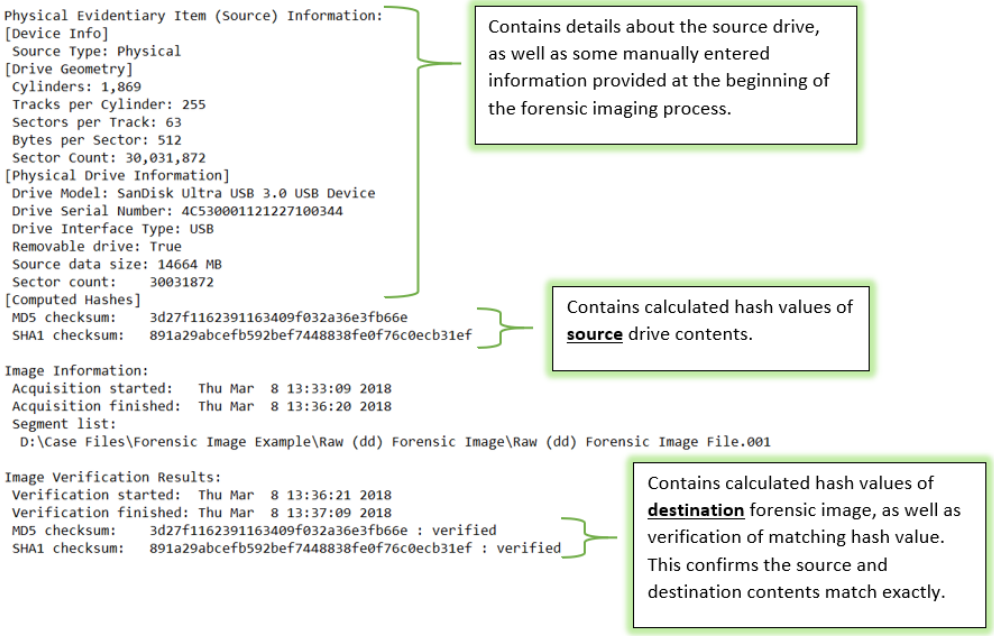
Raw(DD) forensic images can be written to a single file or several "segmented" files. Segment sizes are defined by the examiner at the start of the forensic imaging process. Segments can vary in size and the application will create as many segments as necessary until all data is written to the destination. Segmenting can also be disabled, which is preferable in normal circumstances. Without segments, the output file will be '*filename*.001'. With segments enabled, output filenames will start with '*filename*.001' and continue to create segments in numerical order until the process is completed ('*filename*.002', '*filename*.003', etc.).

Compression:

Raw(DD) format does not natively use compression in the process of creating a forensic image. This is one of the key factors that make this format so dependable and accurate. Anti-forensic programs, such as those using steganography, are often made to destroy themselves when compression is used to store the data. In this instance, the original file hiding the hidden message/data can be restored, but the hidden content is destroyed.

Image Verification with Hash Values & Metadata:

The below snapshot is from a successfully completed RAW(DD) Forensic Image. This image was created in the USA Forensic Lab using 'AccessData FTK Imager'. MD5 & SHA1 Hash Values are calculated on both source and destination files to confirm a successful forensic image has been created. Metadata for the source drive is stored in this external file only, and not within the forensic image.



EWF-E01 Forensic Images

Description:

This format, as a proprietary format of EnCase and ASR Data has been basically deprecated, however, the opensource community has reverse engineered the format and published a stable specification that is used in libewf software libraries. It is designed to support arbitrary offset access within compressed data streams and it uses Cyclic Redundancy Checks (CRCs) for integrity validation. EnCase v.7 recently moved to a new version of this format (Ex01) but has since switched back to the previous format of E01 with the release of EnCase v.8 (using zlib compression). The EnCase v.7 Ex01 format was noticeably slower to process than the already slower than normal predecessor E01, as it was built to use 'bzip2' compression in place of 'zlib'.

Output File(s)/Image Segments:

E01 forensic images can be written to a single file or several "segmented" files. Segment sizes are defined by the examiner at the start of the forensic imaging process. Segments can vary in size and the application will create as many segments as necessary until all data is written to the destination. Segmenting can also be disabled, which is

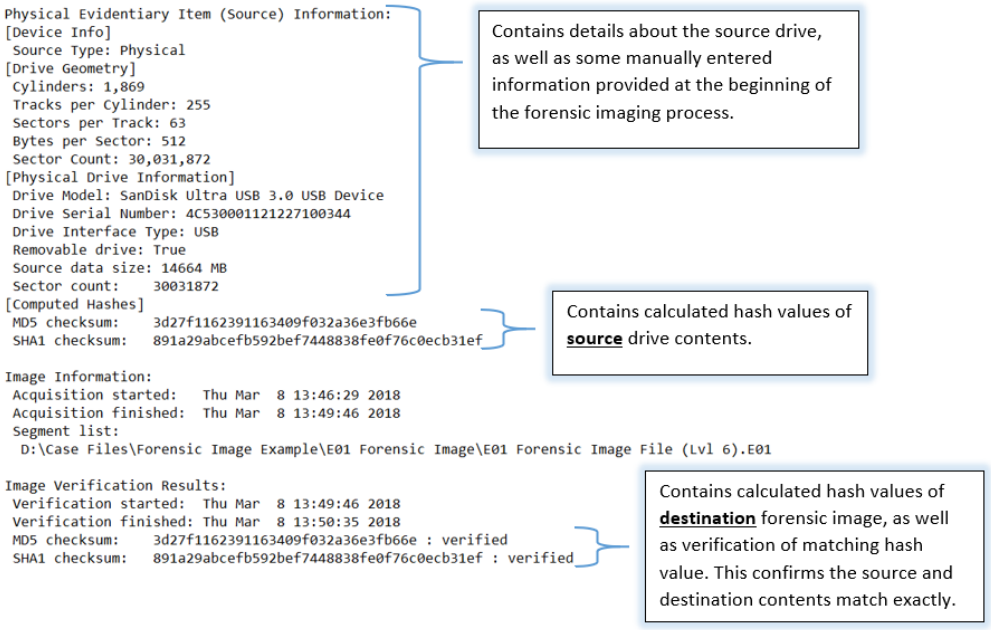
preferable in normal circumstances. Without segments, the output file will be '*filename*.E01'. With segments enabled, output filenames will start with '*filename*.E01' and continue to create segments in numerical order until the process is completed ('*filename*.E02', '*filename*.E03', etc.).

Compression:

The current version of E01 uses 'zlib' by default. Compression can be disabled for the forensic image process, but a novice user may not know to run the drive without compression. The only benefit to compression is the ability to store the forensic image on a smaller drive. To analyze a compressed E01 file, forensic analysis tools must decompress the files as it processes them. This takes significantly longer to analyze for a forensic expert, and the cost savings with a smaller drive is eliminated in time investment. Anti-forensic programs, such as those using steganography, are often made to destroy themselves when compression is used to store the data. In this instance, the original file hiding the hidden message/data can be restored, but the hidden content is destroyed. This factor alone makes this format unacceptable for use in the scientific or forensic world.

Image Verification with Hash Values:

The below image is from a successfully completed E01 Forensic Image with standard Level 6 compression. This image was created in the USA Forensic Lab using 'AccessData FTK Imager'. MD5 & SHA1 Hash Values are calculated on both source and destination files to confirm a successful forensic image has been created. Metadata for the source drive is stored both within the destination file(s), and externally in a separate file. Cyclic Redundancy Checks (CRCs) are processed for every 64 sectors of data, and appropriate metadata is stored within the destination file(s).



Forensic Image Study Results by Harvard *(1)*:

Analysis Outcome

A matrix of the scores and final classifications follows. Green rows indicate our recommendations for Class A formats based on the analysis completed in this phase of the disk image content modeling project (these selections were determined in accordance with HL team members). AVPreserve and HL team members agreed that there is no need for B formats in this case, preferring to support only one "forensic" use-case format at this point. Red rows indicate the formats that were not considered stable enough for inclusion in the HL DRS at this point. Because of the slight instability in the forensic format environment, AVPreserve recommends a continued analysis of the changes in this area over the next five years.

	Standard Weighted Score	HL Color Coded Weighting	AVPreserve Weighting	Classification
RAW (IMG, DD)	24.5	51	56.5	A
ISO	21.75	44.5	49.25	A
BIN/CUE	20.5	41.75	49.25	A
EWF-E01 (EWCF-ASR02)	19.25	38.5	45.25	A
AFFv1-3 (AFF, AFD, AFM)	*17.25*	*35.75*	*42*	
EWF-L01	*17.75*	*35*	*43.25*	
S01 (.001)	*16*	*32.25*	*38.75*	
AFF4	*14.75*	*31.25*	*33.75*	
EWF2-Lx01	*14.5*	*29.5*	*36.5*	
EWF2-Ex01	*13.75*	*27.75*	*33.75*	

Forensic Image Comparison Notes from DME Forensic Article *(2)*:

Results

Filetype	Time to Image	Space Savings	Time to Search
E01	1:27:06	32 GB (7%)	~ 1:53:00
DD	1:24:44	N/A	~ 1:06:00

Obviously the time to create the image was about the same, and we didn't save much space (less than 7%) by using E01. Looking at the searching performance numbers however, you'll notice that our searching was about 42% faster by utilizing the raw DD format over E01. That was just on one search, so if you are doing a lot of analysis on this data, that performance increase can really make a difference over the course of the examination.

(1) *Harvard Article titled "Disk Image Formats", Published Oct 31st, 2016, Author Andrea Goethals.*

(2) *DME Forensic Article titled "Forensic Images for DVR Analysis - E01 or DD", Published May 27th, 2014, Author DME Forensics.*


602 740-6128
USAForensic.com
USA FORENSIC
Bryan@USAForensic.com
USA FORENSIC
LLC
Matt@USAForensic.com