Image Verification

CSC 485/585

Objectives

- Understand why a computer forensic examiner verifies their forensic images.
- Understand how to verify a Raw Bit Stream (RBS) image.
- Understand how to verify an .E01 format image.
- Understand verification errors and related issues.

2

Why we verify forensic images?

- To ensure that the data read from a source disk is the same as the data written to our target disk.
  - Bad Sectors, I/O data transfer problems, cached data writes not synced to target disk, etc.
- You don't want to image on-site and leave thinking you have a "good" image, only to get back to your office to find out it is corrupt or otherwise unusable.
- To re-validate image integrity to ensure that data corruption or disk failure has not taken place as evidence drives are stored for extended periods of time.
- In the event of data corruption or failure, to identify the specific corrupted blocks of data within an .e01, thereby refuting defense claims that evidence found in uncorrupted portions of the forensic image are not valid.
- To ensure that subsequent copies of the original forensic image are identical to the original.

3

Why we verify forensic images?

- Probably the most common reason for bad images is due to unknown I/O errors during the imaging process, most frequently caused by faulty, over-used and worn data ribbon cables. These get easily crimped, bent, and cut causing such errors.

4

Verifying an RBS image

- Verifying an RBS image simply means calculating a hash value of the RBS image and comparing that hash value against a previously calculated hash value that you recorded for later comparison.
- If you took no hash value of the original disk, then there is nothing to verify against other than calculating a hash value to ensure any later copies of the RBS image are the same.

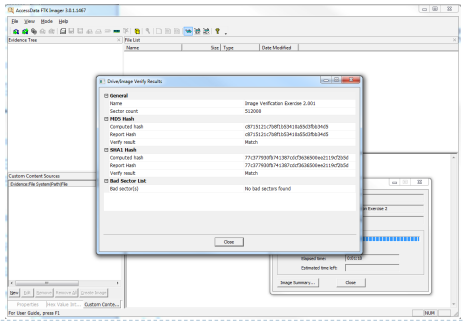
5

RBS data corruption issues?

- We know that a single byte of data changed will result in a completely different hash value.
- The problem with verifying an RBS image is that our hashing tool will only allow us to know if the current hash is the same as any previously recorded hash or it is different…..not how many changes or where the changes are.
- There is no additional metadata or checksum data added to an RBS image to tell us where things changed, unlike proprietary image formats such as .E01 images.
- Your verification tool will not ever know or tell you that there is a problem, other than your manual comparison of the hash values from the original data to the computed hash of the corrupted data.

6

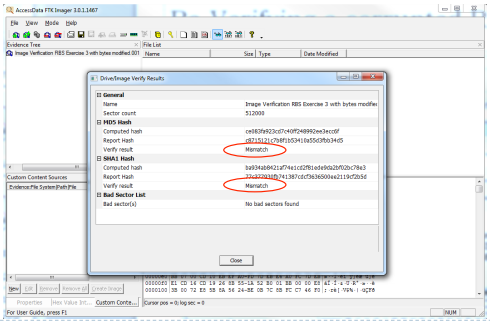
Verifying an RBS image during imaging



7

Re-Verifying a corrupted RBS image

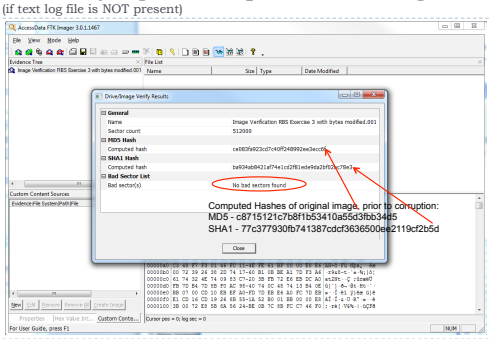
(if text log file is present)



8

Re-Verifying a corrupted RBS image

(if text log file is NOT present)



9

Verifying an .E01 image

- An .E01 format image file contains a variety of "metadata" inside the image file, in addition to the original data captured from the original evidence disk.
- Data captured within an .E01 is broken into "blocks" that are typically 64 sectors (default) in size.
- A CRC is calculated for each "block" of data and individual CRC values are stored with each block throughout the .E01 image.
- An overall MD5 and/or SHA1 is also captured for the entire original data (without any EnCase metadata, just the same as an RBS image) and stored within the .E01 image for future verification.

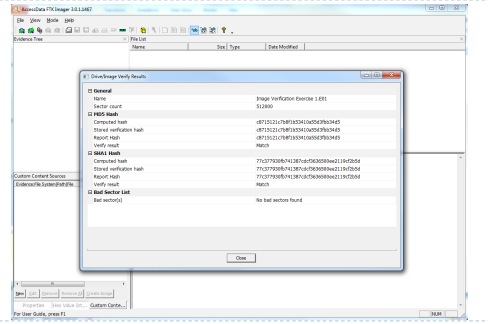
10

Verifying an .E01 image

- When EnCase or other forensic tool verifies an .E01 image file, it does two things:
  - Re-calculates a CRC for each block of data in the .E01 and compares the calculated CRC with the CRC stored in the .E01 for each block.
  - Re-calculates an overall MD5/SHA1 for all of the data within the .E01 (excluding any metadata or additional info not part of the original disk) and compares the overall value calculated with the overall hash stored inside the .E01 image file.
- Any mis-match of ANY individual CRCs or the overall MD5/SHA1 will result in a verification failure.

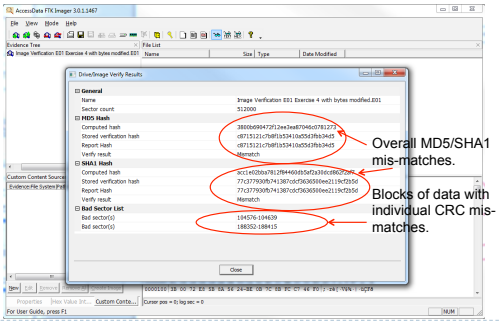
11

Verifying an .e01 image during imaging



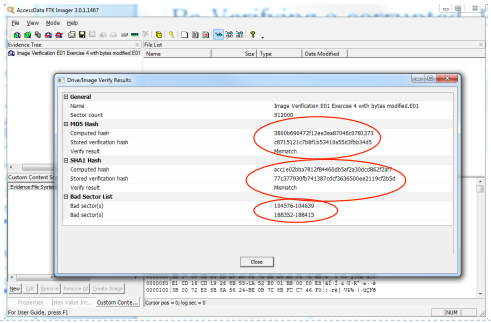
12

Re-Verifying a corrupted .E01 image
(if text log file is present)



13

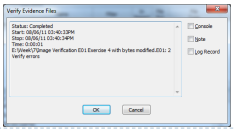
Re-Verifying a corrupted .E01 image
(if text log file is NOT present)



14

Re-Verifying a corrupted .E01 image

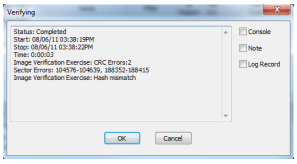
- Any individual .e01 image segment may be verified in EnCase Acquisition mode, using the menu option Tools\Verify Evidence Files.
- Used only to quickly verify individual image segments and not an entire image set. Provides minimal information other than there are errors.



15

Re-Verifying a corrupted .E01 image

- In Full mode of EnCase, you are provided with more detailed info and reports about the physical sector location of the corrupted data.



CRC Errors

Start	Count
104,576	64
188,352	64

The integrity of the following sector groups could not be verified
Image Verification E01 Exercise 4 with bytes modified.E01: 104576-104639,188352-188415

16

Refuting Claims of Invalid Evidence

- In "Disk View" of EnCase (license required, can't be done in Acquisition Mode), you can go to the exact physical sectors identified as corrupted data and identify which file(s) sit on those sectors, thereby refuting any claims that other files of evidentiary value (outside of these corrupted sectors) are invalid.
- The same thing can be done in most forensic software that can read and interpret an .E01 file, such as FTK and X-Ways Forensics.

17

Questions ???

…as usual, use the discussion board!