Chapter 1

Forensic Data

Today there are three fundamental kinds of forensic data:

* Disk Images
* Memory Images
* Packets intercepted on a network.

Most research to date has been done with Disk images. Most data is stored on disk, and most forensic investigations have been for the purpose of finding information that is on a disk (such as in the case of a child pornography investigation), or in trying to understand information left behind on a disk (for example, after an intrusion or malware incident).

It is also common to find the other kinds of information on disk images. Memory is frequently stored on disk images from swapping (e.g. PAGEFILE.SYS on Windows) or system hibernation (HIBER.SYS). Packets are found on image files when the disks were used to store the results of a network interception.

Working with image files can consist of these activities:

* Copying the data from the source drive into the image file, a process called drive imaging.
* Computing the checksum of the disk image.
* Validating the copy against the original.
* Creating a digital signature for the disk image.
* Self-validating the copy.
* Making backup copies of the disk image and validating the integrity of the backups.
* Converting the disk image into a form that can be used by your forensic tool.

On the digitalcorpora.org website there are several disk images with which you can work. We’re going to do our initial work with the image nps-2009- canon2-gen6. This image is usually stored in the directory /corp/images/nps/nps- 2009-canon2/.

The nps-2009-canon2 disk images are a series of images created with a Canon digital camera and a 32MB SD card. First the card was cleared using —dd— on a Linux computer. The card was then inserted into the digital camera, a series of photos were taken, and the card was removed and imaged. The card was put back into the camera, some of the photos were deleted, and new photos were taken. This process was repeated five times, creating a total of six disk images, nps-2009-canon2-gen1 through nps-2009-canon2-gen6.

The SD card contained 60,800 512-byte sectors, for a total of 31,129,600 bytes (30,400 KiB).

For each disk image four files are distributed:

.raw – a DD disk image that’s 31,129,600 bytes in length

.aff – an AFF disk image of the same file created with [?]

.E01 – An EnCase E01 file of the disk image created with [?]

.xml – A digital forensics XML file describing the files resident in the disk image.

It is customary in digital forensics to use cryptographic hashes to verify the integrity of a disk image. When the disk is first imaged the hash is recorded in a secure manner (typically written in the investigator’s notebook). From that point forward, the image can be manually validated by recomputing the hash and comparing it to the one originally recorded.

The hash of a raw file can be easily calculated with the “openssl” command:

**$ openssl md5 /corp/images/nps/nps-2009-canon2/nps-2009-canon2-gen6.raw MD5(/corp/images/nps/nps-2009-canon2/nps-2009-canon2-gen6.raw)=750b509d8fbed37a5213**

**$**

You can’t calculate the hash of an AFF or E01 file in this manner, however, because these files contain additional metadata that is not part of the disk image. Both of these formats also store hash codes directly in the disk image. This allows you to validate the contents of a disk image with a command that calculates the hash by examining the data and comparing it with the stored value.

1.0.1 E01 Files for Viewing the EnCase File of the SD Card Disk Image

You can use the ewfinfo command to view the metadata information of a disk image:

**% ewfinfo /corp/images/nps/nps-2009-canon2/nps-2009-canon2-gen6.E01 ewfinfo 20090927 (libewf 20090927, libuna 20090901, libbfio 20090927, zlib 1.2.3, l**

**Acquiry information**

**Acquiry date:Mon Apr 12 08:12:32 2010**

**System date:Mon Apr 12 08:12:32 2010**

**Operating system used:Darwin**

**Software version used:20090927 Password:N/A**

**EWF information**

**File format:EnCase 6**

**Sectors per chunk:64**

**Error granularity:64**

**Compression type:no compression**

**GUID:dc032794-bef0-2c45-8ede-8cc01ed31683**

**Media information**

**Media type:removable disk**

**Is physical:no**

**Bytes per sector:512**

**Amount of sectors:60800**

**Media size:29 MiB (31129600 bytes)**

**Digest hash information**

**MD5:750b509d8fbed37a5213480aaccfdc61**

**%**

You can verify the contents of an E01 file using the ewfverify command:

**$ ewfverify /corp/images/nps/nps-2009-canon2/nps-2009-canon2-gen6.E01 ewfverify 20090927 (libewf 20090927, libuna 20090901, libbfio 20090927, zlib 1.2.3, libcrypto 0.9.8)**

**Verify started at: Mon Jun 7 14:20:20 2010**

**This could take a while.**

**Status: at 0%. verified**

**32 KiB (32768 bytes) of total 29 MiB (31129600 bytes).**

**...**

**Status: at 100%. verified**

**29 MiB (31129600 bytes) of total 29 MiB (31129600 bytes).**

**Verify completed at: Mon Jun 7 14:20:20 2010**

**Read: 29 MiB (31129600 bytes) in 0 second(s).**

**MD5 hash stored in file:750b509d8fbed37a5213480aaccfdc61**

**MD5 hash calculated over data:750b509d8fbed37a5213480aaccfdc61**

**ewfverify: SUCCESS**

**$**

1.0.2 AFF1 Files for Viewing the AFF File of the SD Card Disk Image

AFF1 files can store MD5 and SHA1 inside. You can display the information with the afinfo command:

**% afinfo -a /corp/images/nps/nps-2009-canon2/nps-2009-canon2-gen6.aff /corp/images/nps/nps-2009-canon2/nps-2009-canon2-gen6.aff is a AFF file**

**/corp/images/nps/nps-2009-canon2/nps-2009-canon2-gen6.aff data**

**{omitted for clarification sake, table did not import correctly}**

The afverify command can be used to verify that the hash in the file matches the hash of the pages:

**% afverify /corp/images/nps/nps-2009-canon2/nps-2009-canon2-gen6.aff /corp/images/nps/nps-2009-canon2/nps-2009-canon2-gen6.aff: no signing certificate present.**

**SHA1 stored in file: 4742c325f10583dab1eb4c55d0d45ab3beb99eb3**

**MD5 stored in file: 750b509d8fbed37a5213480aaccfdc61**

**Read 0/ 31129600 bytes; done in n/a**

**Read 16777216/ 31129600 bytes; done in 00:00:00**

**Calculated SHA1: 4742c325f10583dab1eb4c55d0d45ab3beb99eb3 VERIFIES**

**Calculated MD5: 750b509d8fbed37a5213480aaccfdc61 VERIFIES**

**%**

1.0.3 Exercises

* Download an install the following programs in this order: Comments
  + libewf
  + afflib
  + sleuthkit
* Download nps-2009-canon2-gen6.aff, nps-2009-canon2-gen6.e01 and nps- 2009-canon2-gen6.raw Comments
* Verify the SHA1 of each file. Verify the RAW with the openSSL command and make sure that it matches what is in this book. Use the ewfverify and afverify commands to verify that the hash codes stored in the AFF and E01 files match the computed values.
* Convert the RAW file to an AFF and E01 files. Notice that the files are different than the distribution AFF and E01 files. Comments
* Verify your converted files using SHA1 as you did above.
* Convert the distribution AFF and E01 files back to raw files using tool [?] and use the Unix —cmp— command to show that the resulting files match the distribution raw file.