

Computer Forensics Tutorials

Instructor	Dr.Abdul Rehman Al-Ghamdi	Phone	+966-503770707
Office	CCIT	Version	Three
Office Hours	0800 – 1400Hours	Email	

3.1 Introduction

For a student just getting started in digital forensics, concepts regarding forensic images can be confusing. Terminology like images, clones, bit-stream copies and forensic images are often used incorrectly, further complicating the issue. This tutorial will attempt to clear up the confusion. We will present an instructive clarification of what a forensic image is as well as what it is not. In addition, we will provide a comprehensive look at the many different ways to access data on forensic images using mostly open source tools on both Windows and kali Linux platforms.

3.2 Disk image

Digital forensic investigations often involve creating and examining disk images. A disk image is a bit-for-bit copy of a full disk or a single partition from a disk.

3.3 Forensic image

Forensic examiners use imaging techniques to acquire data from a disk as opposed to copying files because an image contains every bit of data from the source disk and a copy operation will only retrieve currently accessible files.

A **forensic image** will contain current files as well as **slack space** and **unallocated space**.

Relevant forensic artifacts such as, deleted files, deleted file fragments and hidden data may be found in slack and unallocated space.

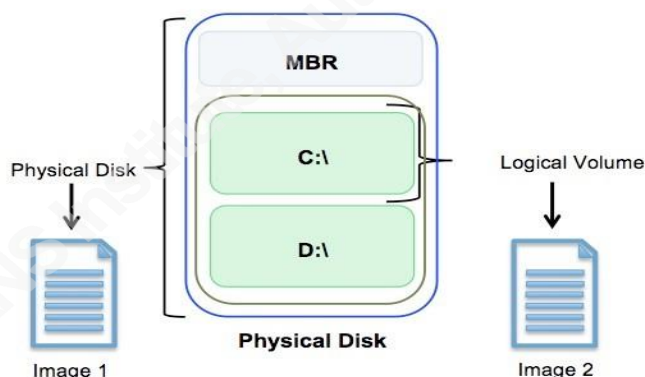
3.4 Disk Image Sources

The physical disk shown in Figure 1 contains a **master boot record (MBR)** and a partition with two logical volumes, each formatted with a file system.

The master boot record contains metadata about the layout of the disk including where the partitions begin and end.

The source of the image could also be a logical volume within a physical disk, such as Volume C:\ and Image 2. In both cases, an image is a file that will always contain an exact copy of the data that represents a snapshot of the source at the point in time when it was copied.

Figure 1: Logical volumes contain file systems within a physical disk



In forensics, **embedded images** are disk images that contain metadata about the image such as a timestamp when the image was created and a **cryptographic hash** acting as a **fingerprint** for the image.

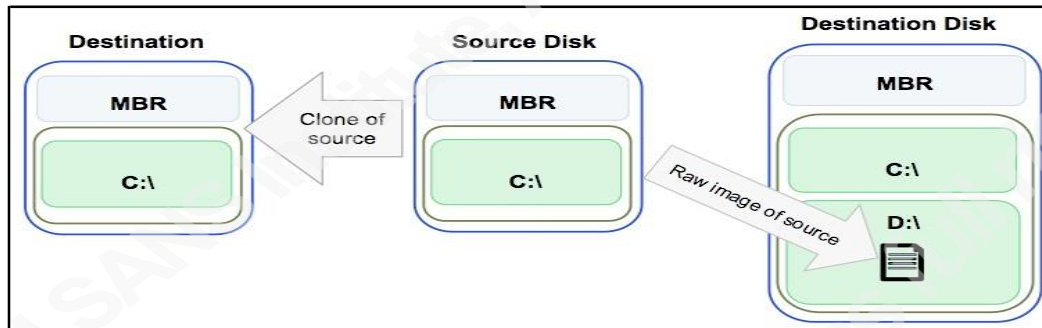
3.5 Image vs. Clone

The terms **image** and **clone** are not synonymous. A forensic image is a **duplicate of a** physical drive that is written to a file. The file can be stored on an internal disk, on an external disk, on a network storage server or on optical storage, etc.

A disk clone is a bit-for-bit copy of a physical disk directly on to another disk. The original and the clone are identical and interchangeable. Cloning is usually used to make a backup or duplicate of the operating system drive because it can be very quickly replaced in the case of drive failure.

Figure 2 compares a cloned disk to a disk image. On the left, the output from the cloning process is another entire disk that is an exact copy of the source, including the metadata in the MBR. On the right, the output of the imaging process is an image file, stored on another disk. Inside that image file is the exact copy of the source disk, including the metadata in the MBR.

Figure 2: A *clone* is a duplicate disk and an *image* is a duplicate of the data from the disk that is written to a file



3.6 Image File Formats

Two formats are most widely used today are the **Encase evidence file format (often called Expert Witness format or E01 images)** and **raw image** file formats.

3.6.1 Raw images

As described in earlier a raw image contains only the data from the source **disk**.

There is no header or metadata included in the image file but **some utilities may include** a separate file with metadata.



Raw images can be created by several different utilities and frequently will use the following file extensions:

.dd .raw .img




3.6.2 Encase 6 evidence file images (E01)

The popular commercial forensics suite, EnCase, developed a proprietary format called EnCase Evidence File format. EnCase Evidence Files use the file extension, E01, and are based on the Expert Witness Format (EWF) by ASR Data. These image files are commonly referred to as Expert Witness, E01 or EWF files.

E01 files have both a header and footer containing metadata about the image. The metadata includes the drive type, the version of EnCase that created the image, the source disk operating system, timestamps and a cryptographic hashes over the data portion of the image.

3.7 Image Creation Tools

Table 1 summarizes the common tools that can be used to create image files along with the platforms on which each can be executed.

Tool	Platform			Input Sources				Encoding		Output Formats			
				Physical Disk	Logical Volume	Files	Folders	Compression	Encryption	Raw	E01	Ex01	Split
FTK Imager 3.2	✓			✓	✓		✓	✓	✓	✓	✓		✓
FTK Imager CLI 3.1.1	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓		✓
EnCase Forensic Imager 7.0	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
dd		✓	✓	✓	✓	✓	✓			✓			
dcfldd		✓		✓	✓	✓	✓			✓			✓
dd_rescue		✓		✓	✓	✓	✓			✓			
dd.exe	✓			✓	✓	✓	✓	✓	✓	✓			
dc3dd	✓	✓		✓	✓	✓	✓			✓			✓
ewf_acquire		✓	✓	✓	✓					✓	✓	✓	✓

Answer the following questions

1. What is a forensics image?

2. Explain disk image

3. What is the difference between an image and clone

4. What is cryptographically hash value?

5. Explain image formats

6. What is raw image?

7. List five image creation tools?

