5.1 Introduction to Forensic Duplication

5.2 Rules of Forensic Duplication (Thumb Rule)

5.3 Necessity of Forensic Duplication

5.4 Forensic Duplicates as Admissible Evidence

5.5 Important Terms in Forensic Duplicate

5.6 Forensic Image Formats

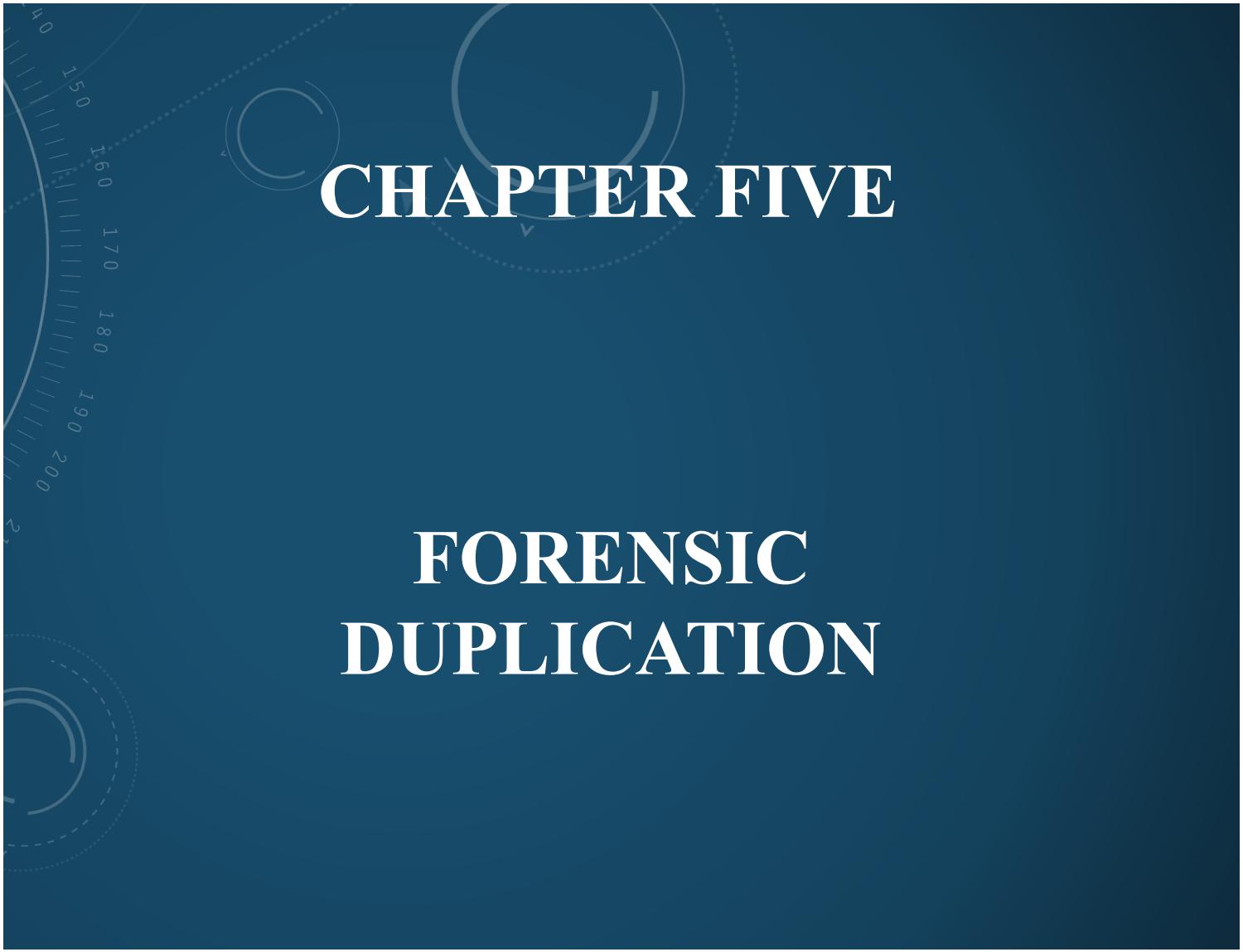
5.7 Traditional Duplication

5.8 Live System Duplication

5.9 Forensic Duplication Tool Requirements

5.10 Creating a Forensic Duplicate of a Hard Drive

5.11 Creating a Qualified Forensic Duplicate of a Hard Drive



Introduction To Forensic Duplication :

A forensic duplicate contains the same digital data as the original piece of evidence. Many times, with data collection process, forensic duplication process also gets started, which is based on response strategy already formulated.

Rules of Forensic Duplication :

1. Make two copies of the original media (digital evidence).
- **(a)** One copy becomes the working copy on which investigation will be done.
- **(b)** One copy is a library/control copy for future reference.
- **(c)** Verify the integrity of the copies.

2. The working copy is used for the analysis.
3. The library copy is stored for disclosure purposes or in the event that the working copy becomes corrupted.
4. If performing a drive to drive imaging (not an image file), use clean media to copy to:
5. Verify the integrity of all images using hash values.

Necessity of Forensic Duplication :

Forensic duplication importance can be summarized as:

1. Working from a duplicate image provides following features:

(a) Preserves the original digital evidences.

(b) Prevents inadvertent alteration of original digital evidence during examination.

(c) Allows recreation of the duplicate image, if necessary.

2. Digital evidence can be duplicated with no degradation from copy to copy:

(a) This is not the case with most other forms of evidence.

Forensic Duplicates as Admissible Evidence :

Digital evidence should satisfy minimum criteria of legal standards. Some standards are given by the United States, known as Federal Rules of Evidence (FRE).

1. FRE §1002 requires an original to prove the content of a writing, record, or photograph. This means
the item or information presented in court must be original. It follows from the best evidence rule:
Copying can introduce errors.

2. FRE §1001 (3) states that if data are deposited in a computer or alike device, any printout or other
output readable by sight, shown to reflect the data precisely is an “original.”

3. FRE §1003 states that a duplicate is admissible to the same extent as an original if:

(a) An honest question is elevated to the authenticity of the original or

(b) In the circumstances, it would be partial to confess the identical in lieu of the original.

Important Terms in Forensic Duplicate :

1. Forensic Duplicate : Forensic duplicate stores every bit of information from source in a raw bitstream format. In a process of forensic duplication, 5GB of drive results in 5GB of forensic data.

2. Qualified Forensic Duplicate : The file that stores every bit of information from the source is referred to as qualified forensic duplicate in the altered form. In-band hashes and empty sector compression are the example of two altered forms. In some tools, it may read a number of sectors from the source. SafeBack and EnCase can be used to generate qualified forensic duplicate.

3. Restored Image : Restoration of a forensic duplicate or qualified forensic duplicate to another storage media results in restored image. It is a complicated process. As the forensic duplicate is restored to the destination hard drive, the partition tables are updated with the new values.

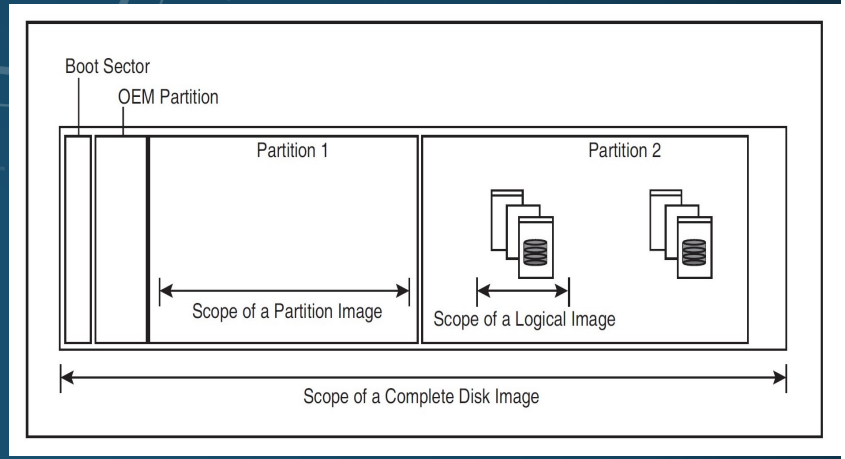
4. Mirror Image : A hardware that does a bit-for-bit copy from one HDD to another is used to generate a mirror image.
Generating mirror image presents an extra step in forensic investigation process.

Forensic Image Formats :

1. Complete Disk Image : The process for getting a "complete disk image" is meant to duplicate each addressable computer memory unit on the medium. This includes Host Protected Areas (HPAs) and Drive Configuration Overlays (DCOs).

2. Partition Image : Most forensic imaging tools permit you specify a personal partition, or volume, as the source for a picture.

A partition image may be a set of a whole disk image and contains all of the allocation units from a personal
partition on a drive. This includes the unallocated space and file slack present within that partition.



Forensic Image Formats :

3. Logical Image : A logical image is a smaller amount of Associate in Nursing "image" and additional of a straightforward copy. A logical image is less of an "image" and more of a simple copy.

4. Image Integrity : When a forensic image is formed, cryptologic checksums are generated for two reasons. First, once the image
is taken from a drive, which is offline (static) and preserved, the hash is employed to verify and demonstrate
that the forensic image could be a true and correct illustration of the initial. Second, the hash is employed to
sight if the info was changed since the purpose of your time at which the image was created.

Traditional Duplication :

1. Hardware Write Blockers :
The write blockers are generally protocol bridges that contain changed code or an ASIC designed to intercept a set of the protocol's commands. With these in your kit, you will faithfully duplicate SATA, PATA, SCSI, SAS, and USB devices.

2. Image Creation Tools :
The three main tools we tend to use are a unit DC3dd, AccessData's FTK Imager, and steering Software's incase. Each has its pros and cons that build it additional or less appropriate for a given scenario.

Live System Duplication :

The creation of an image of media in a system that is actively running is the example of a live system duplication. This case is not most popular; however, it is usually the only alternative. The system could also be a particularly business-critical system that cannot be taken down except throughout terribly short maintenance windows. Make sure to document precisely what you probably did, as well as the tool you used, the procedure you followed, what services could also be running, and the actual dates and times. You may need that info just in case somebody "challenges" the actual fact that you changed the system. Such challenges are simply refuted if you have got the proper documentation

Forensic Duplication Tool Requirements :

Forensic duplication tools must satisfy the following criteria:

1. The tool shall make a bitstream duplicate or an image of an original disk or partition.
2. The tool shall not alter the original disk.
3. The tool will be able to verify the integrity of a disk image file.
4. The tool shall log I/O errors.
5. The tool's documentation shall be correct.
6. The tool should create a mirror image or forensic duplicate of the original storage media.
7. The tool must be able handle read errors.
8. The tool should not make any changes to the source medium.
9. The tool must have the capability to be held up to scientific review. Results must be verifiable by a third party.
10. If there are no errors accessing the source, then the tool shall create a bitstream duplicate or image of the source.
11. If there are I/O errors accessing the source, then the tool shall create a qualified bitstream duplicate or image of the source.
12. The tool shall log I/O errors in an accessible and readable form, including the type of error and location of the error.

Forensic Duplication Tool Requirements :

13. The tool shall be able to access disk drives through one or more well-defined interfaces.
14. Documentation shall be correct, insofar as the mandatory and any implemented optional requirements are concerned, that is, if a user following the tool's documented procedures produces the expected result,
then the documentation is deemed correct.
15. If the tool copies a source to a destination that is larger than the source, then it will document the
contents of the areas on the destination that are not part of the copy.
16. If the tool copies a source to a destination that is smaller than the source, then the tool will notify the
user, truncate the copy, and log this action.
Some Examples of forensic duplication tools are:

- **a.** SafeBack (www.forensics-intl.com)
- **b.** Ghost (www.symantec.com)
- **c.** DD (standard UNIX/Linux utility)
- **d.** Encase (www.encase.com)
- **e.** Mareware
- **f.** FTK (www.accessdata.com)
- **g.** ProDiscover Basic

Creating a Forensic Duplicate of a Hard Drive :

1. Duplicating with dd and dcfldd : For creating a true forensic duplicate image, dd utility is the most efficient tool. ddwill perform bit-for-bit copy of the original, as long as the operating system kernel recognizes the storage medium. However, it is expensive.
2. Creating a Linux Boot Media : Preparation for duplication using Linux is difficult from the methods that we discuss in this section. But using Linux is worthy, as it can be the most flexible boot environment in the toolbox.
3. Performing a Duplication with dd : Sometimes, to fit on a specific media type, such as CD/DVD or file systems with files fewer than 2.1 GB, duplication will be stored in a series of files. This is usually referred to as segmented image.
4. Duplicating with the Open Data Duplicator : The new open source tool is ODD. To perform forensic duplication simultaneously on a number of computers over a Local LAN, the client-server model is followed by this tool. To use the software on single forensic workstations, you need to run both halves on the same computer.
Three portions of ODD are:
1. Bootable CD-ROMs: This is similar to Trinux Linux Distributions;
2. Server-side applications: Most of the duplications, such as string searches, calculation of hashes, and
storage of true forensic duplications, will be done by the server.
3. Client-side applications: If you are duplicating drives on forensic workstations, this portion may be run
locally.

Creating a Qualified Forensic Duplicate of a Hard Drive :

1. Creating a Boot Disk :

Clean operating environment is required for imaging a system. You must create an MS DOS boot disk when imaging drives using DOS applications such as SafeBack or EnCase.

2. Creating a Qualified Forensic Duplicate with SafeBack :

New Technology Inc. (NTI) offers SafeBack. It is used to make qualified forensic duplication of any hard drive. You need to have a clear environment ready on the floppy for SafeBack application because it runs from DOS boot floppy.

3. Creating a Qualified Forensic Duplicate with EnCase :

The most popular commercially available forensic tool is EnCase from Guidance Software. It provides ‘easy-to-navigate’ GUI. Allowing the examiner to customize the types of searches performed by the tool, a flexible scripting language in included. Preview option is the most significant feature of EnCase. You can use the preview function to quickly ascertain whether a computer system is material to the issue being investigated, during the first stages of the investigation.