Lecture #32: Forensic Duplication

Dr.Ramchandra Mangrulkar

October 8, 2020

Forensic Duplication

1. During an incident, a significant amount of data is gathered, preserved, cataloged, and analyzed.
2. The most comprehensive sources of information is a forensic image of an affected or suspect computer system.
3. Processes, formats, and tools that are used by the forensic community to properly duplicate data.
4. A court may find that the best available duplication acceptable and render it admissible.

Types of Forensic Duplication

- A simple duplication consists of making a copy of specific data. The data may consist of a single file, a group of files, a partition on a hard drive, an entire hard drive, or other elements of data storage devices and the information stored on them.
- A forensic duplication is an accurate copy of data that is created with the goal of being admissible as evidence in legal proceedings. Furthermore, we define forensic duplication as an image of every accessible bit from the source medium.

Characteristics of Forensic Duplication Tools

- ability to image or account for every bit of accessible. data on the storage medium.
- must create a forensic duplicate of the original storage medium.
- must handle read errors in a robust and graceful manner.
- the process must not make any changes to the original storage medium.
- must generate results that are repeatable and verifiable by a third party.
- must generate logs that detail the actions requested and any errors encountered.

Forensics Image Format

IR teams will create and process three primary types of forensic images

- Complete Disk Image
- Partition Image
- Logical Image

Complete Disk Image

- A “complete disk image” is intended to duplicate every addressable allocation unit on the storage medium.
- includes Host Protected Areas (HPAs) and Drive Configuration Overlays (DCOs).
- complete disk image, the output file contains every allocation unit, or sector, accessible to the imaging software.

Overview of the Disk Areas

A service area is a logical area on the hard-drive (residing on the platters) set aside by hard-drive vendors for internally managing the drive. These areas are outside the hard-drive's Logical Block Address (LBA) space and as such are non-addressable and inaccessible via the standard ATA commands. The service area contains both code and data modules, such as defect management modules, SMART data modules, self-test modules and much more.

Disk Areas

- Disk Firmware Area (DPA)
  The firmware is composed of a series of modules. Examples are: SECU (Security System Module), P-List, G-List, T-List, SMART Attributes, and U-List (Firmware Zone Translator).
- The Host Protected Area (HPA)
  is used for holding diagnostics and other utilities required by the manufacturer such as the boot sector, the user addressable sectors, start of the reserved area, and the code for the boot.
- A Device Configuration Overlay (DCO) is similar to the HPA, but is used by manufacturers to configure drive sizes, to enable and disable features on the disk.

Case Study

Eye Witness Report

A couple of years ago, we participated in an internal investigation of an employee who was thought to have gained unauthorized access to financial statements prior to an SEC filing. The subject's primary system (an Apple MacBook Pro) was duplicated and the complete disk image was provided for analysis. The investigators had information from server logs that showed that a specific browser version, identifiable by a user agent string, was used to access the restricted data.

The subject knew that he was going to be investigated and attempted to cover his

Case Study

tracks by downgrading his entire system to end up with a browser version that predated the one identified by the investigators. He had also researched common forensic analysis techniques and understood the problems he would have with date and time stamps on the file system. Examination revealed that the subject attempted to deceive the investigators by taking the following steps:

1. He modified the system log files to remove evidence of computer use during the incident.
2. He resized the primary partition to make room for a second.
3. He changed the time and date of the computer.
4. He installed an older version of the operating system on the second partition.
5. He migrated user data.
6. He migrated the modified log files.
7. He removed access to the first, original partition to ensure it would not boot or be automounted.
8. He restored the time and date of the computer.
9. He restarted and began to use the new, but apparently older, partition to accumulate recent activity.

Despite his attempts, the amount of artifacts left behind during this process were numerous; however, most were on the original partition. He had done a good enough job on the recently installed partition that if the investigators had only obtained a partition image of the active partition, they would have been able to

Partition Image

- Tools allow you specify an individual partition, or volume, as the source for an image.
- A partition image is a subset of a complete disk image and contains all of the allocation units from an individual partition on a drive.
- A partition image still affords you the opportunity to perform low-level analysis and attempt to undelete files and examine slack space from that partition.
- Because a partition image does not capture all the data on a drive, it is taken only under special circumstances.

Logical Image

- A logical image is less of an "image" and more of a simple copy, and it's the type of duplication we referred to previously as a "simple duplication."
- Both FTK Imager and EnCase have the ability to create evidence containers for logical files.

Image Integrity

- When a forensic image is created, cryptographic checksums are generated for two reasons.
- First, when the image is taken from a drive that is offline (static) and preserved, the hash is used to verify and demonstrate that the forensic image is a true and accurate representation of the original.
- Second, the hash is used to detect if the data was modified since the point of time at which the image was created.
- The hash is simply used to ensure that the integrity has been maintained throughout the life of the image.

Traditional Duplication

[1] Traditional imaging is performed on static drives (that is, hard drives that are not part of an active, running system

- Hardware Write Blockers
  The best way to ensure that the source media is not modified in any way is to use specialized hardware that prohibits write commands from reaching the drive controller. A set of these write blockers should be in every IR team's kit.
- The write blockers are typically protocol bridges that contain modified firmware or an ASIC designed to intercept a subset of the protocol's commands.

[1] Incident Response Computer Forensics, Third Edition

Case Study

Figure 8-2 Write blocker hardware

Case Study

Figure 8-3. eSATA write blocker hardware

Image Creation Tools

- The most common method to create a forensic duplicate is via software. The three main tools we use are DC3dd, AccessData's FTK Imager, and Guidance Software's EnCase
- dd, DCFLdd, and DC3dd

Live System Duplication

A live system duplication is defined as the creation of an image of media in a system that is actively running.

- the system may be an extremely business-critical system that cannot be taken down.
- Performing a live image will make minor modifications to the system, but you will be able to get an image.
- Be sure to document exactly what you did, including the tool you used, the procedure you followed, what services may be running, and the exact dates and times.
- If “challenged” , the fact that you modified the system. Such challenges are more easily refuted if you have the proper documentation.

Duplication of Enterprise Asset

- the evidence that is part of an investigation resides on a very large RAID, SAN, NAS, or other massive central storage system.
- it's infeasible to make a complete duplicate of the entire original source due to the sheer volume of data or the complexity of the storage configuration.
- formulate an appropriate plan to create a logical copy of only the relevant data