Forensic Duplication

FORENSIC DUPLICATES AS ADMISSIBLE EVIDENCE

- U.S. Federal Rules of Evidence (FRE) §1002 states that the item or **information presented in court must be the original**

FORENSIC DUPLICATES AS ADMISSIBLE EVIDENCE

- Best evidence rule: Copying can introduce **errors**
- The examination can **destroy** evidence inadvertently.
- The original computer system might only be **available for capturing**
- Originals themselves **cannot be obtained** due to business needs

FORENSIC DUPLICATES AS ADMISSIBLE EVIDENCE

- Relevant Exceptions
  - FRE §1001-3, Definitions and Duplicates:
    - *"If data are stored by computer or* similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an original."
  - FRE §1003, Admissibility of Duplicates:
    - "A duplicate is admissible to the same extent as an original unless
      - a genuine question is raised as to the authenticity of the original or
      - in the circumstances it would be unfair to admit the duplicate in lieu of the original."

Duplicate

- Forensic Duplicate: File that contains every bit of information from the source in a raw bit stream format
  - Unix dd command and dfcldd command
  - Open-source - Open Data Duplicator
- Qualified Duplicate: Same as above, but allows embedded metadata or certain types of compression
  - SafeBack and EnCase

What Is a Forensic Duplicate?

- Produce identical byte stream from duplicate as from the original
- A forensic duplicate is a file that contains every bit of information from the source, in a **raw bit stream format**
  - A 5GB hard drive would result in a 5GB forensic duplicate
- A forensic duplicate may be compressed after the duplication process
- Two tools that create a forensic duplicate
  - Unix dd command and dfcldd command
  - Open-source Open Data Duplicator

What Is a Qualified Forensic Duplicate?

- File that contains every bit of information from the source
- Stored in an altered forms
  - in-band hashes
  - empty sector compression
- Sector(in-band hashes)
  - Tools read some number of sectors from the source, generate a hash and store the sectors followed by hash to output file
  - Even if sector group fails even then restoration can continue
  - This is not possible when storing a file

What Is a Qualified Forensic Duplicate?

- Empty sector compression
  - Minimizing the size of the output file
  - If the tool comes across 500 sectors, all filled with zeros, it will make a special entry in the output file that the restoration program will recognize
- Tools that create qualified forensic duplicate output files are SafeBack and EnCase

Definitions

- **Restored Image:**
  - A forensic duplicate or qualified forensic duplicate restored to another storage medium

    - Difficult to do if second hard drive does not have the same geometry as the previous one

Definitions

- **Mirror Image**
  - Created from hardware that does a bit-to-bit copy from one hard drive to another (copy even the OS)

FORENSIC DUPLICATION TOOL REQUIREMENTS

- The tool must have the ability to image every bit of data on the storage medium
  - The tool must create a forensic duplicate or mirror image
  - The tool must handle read errors
  - The tool must not make any changes to the source medium
  - The tool must have the ability to be held up to scientific and peer review

Creating a Forensics Duplicate of a Hard Drive

Software tools:

- Unix dd
  - Tested and proven
  - Runs on Unix/Linux/Mac OS X which can recognize almost any hardware
  - Free

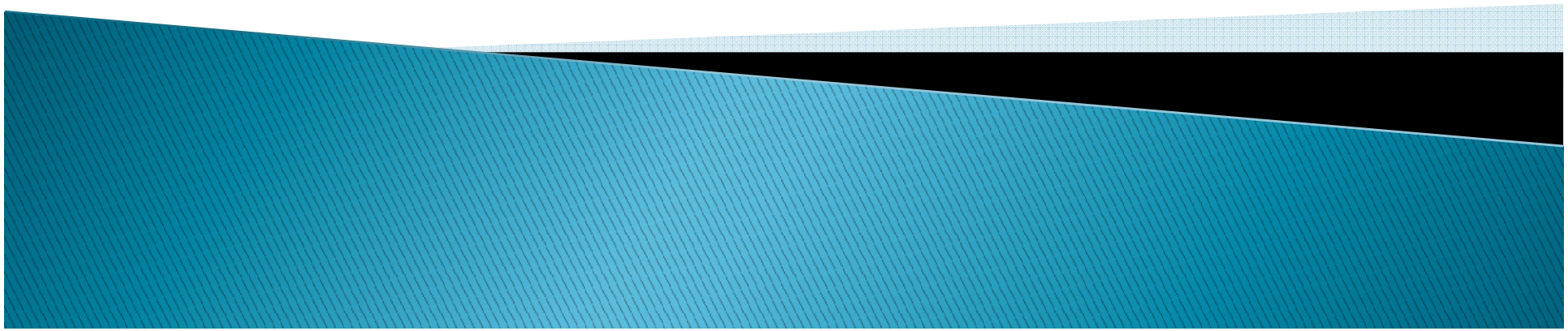
Creating a Forensics Duplicate of a Hard Drive

Software tools: Encase

- Expensive
- Full Suite of Forensics Tools
- Great Market Penetration
- Based on Windows

- Software Tools: Safeback
  - Specialized Imaging Tool
  - Uses DOS

CREATING A RESPONSE TOOLKIT



CREATING A RESPONSE TOOLKIT

- Approach for an initial response need to be planned
- Such that
  - Obtain all the information
  - Without affecting any potential evidence
    - Because commands used will be with administrator rights on the victim system
- The best way to meet this goal is to prepare a **complete response toolkit**

CREATING A RESPONSE TOOLKIT

- Creating a response toolkit is
  - important
  - Monotonous
  - laborious step
    - By spending the time to collect the trusted files and burn them onto
- Helps to
  - respond quickly
  - Professionally
  - successfully

CREATING A RESPONSE TOOLKIT

- **Gathering the Tools**
  - Use trusted commands
  - Maintain a CD
- **Preparing the Toolkit**

CREATING A RESPONSE TOOLKIT

- **Preparing the Toolkit**
  - Ensure that toolkit will function exactly as intended
  - Do not alter the target system
  - Steps to prepare toolkits for initial response:
    - **Label the response toolkit media**
    - **Check for dependencies with Filemon (** Process Monitor**)**
    - **Create a checksum for the response toolkit**
    - **Write-protect any toolkit floppies**

CREATING A RESPONSE TOOLKIT

- Label the response toolkit media
  - A first step in evidence collection
  - Document the collection itself
  - Label response toolkit CD-ROM or floppy disks
  - Helps to identify this part of investigation
  - For example
    - Case number
    - Time and date
    - Name of the investigator who created the response media
    - Name of the investigator using the response media
    - Whether or not the response media (usually a floppy disk) contains output files or evidence from the victim system

CREATING A RESPONSE TOOLKIT

- **Check for dependencies with Filemon**
  - It is important to determine which DLLs and files your response tools depend on
  - We use Filemon to determine all the files accessed and affected by each of the utilities in our toolkit
  - It is good to know which tools change access times on files on the target system

CREATING A RESPONSE TOOLKIT

- **Create a checksum for the response toolkit**
  - One of the files on response kit floppy (and CD and USB drive) is a text file with a checksum of all the commands on it

CREATING A RESPONSE TOOLKIT

- **Write-protect any toolkit floppies**
  - If you use floppy disks, be sure to write protect the floppy after it is created
  - If you store evidentiary files on the response floppy during an incident, you need to write-protect it after you accumulate data and begin the chain of custody
  - The **chain of custody tags** should be filled out for each response floppy or CD, whether or not it contains evidence files