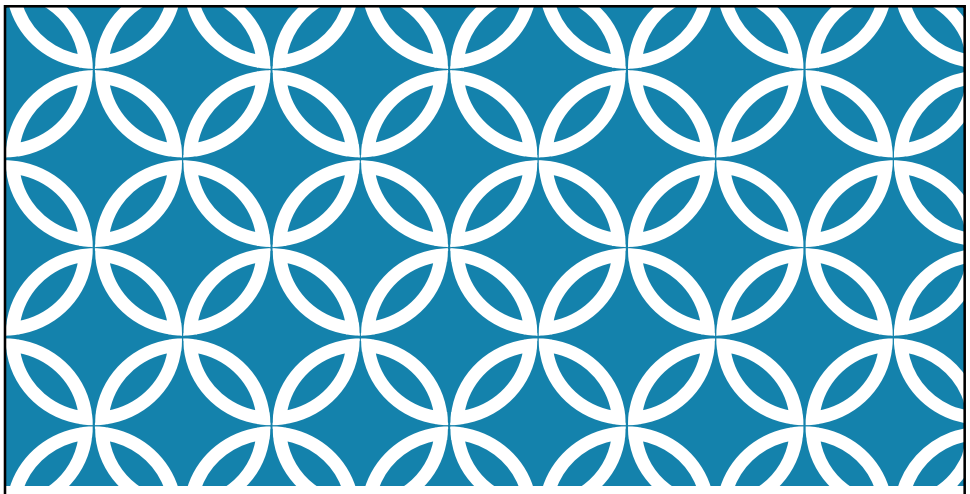
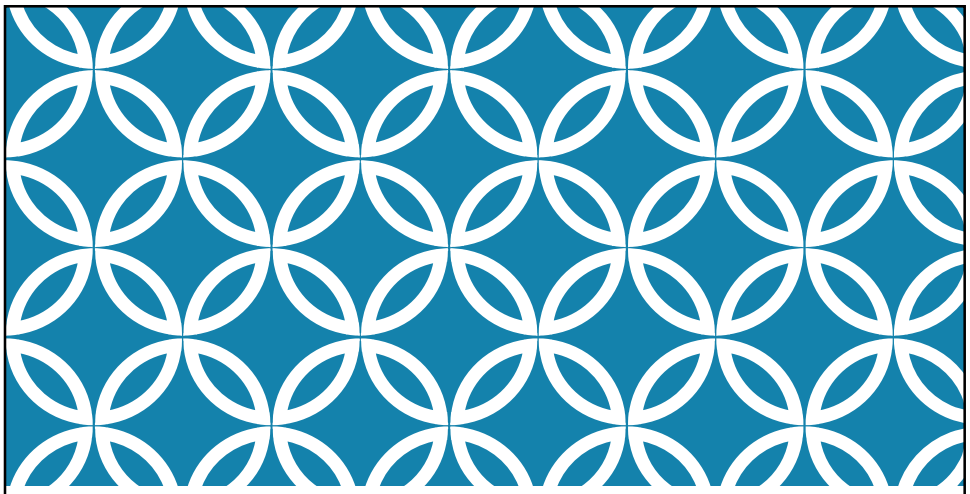


DIGITAL EVIDENCE CONTROL | *Chapter 6*

OBJECTIVES

- Explain the rules for digital evidence
- Describe how to secure digital evidence at an incident or crime scene
- List procedures for storing digital evidence



IDENTIFYING DIGITAL EVIDENCE

IDENTIFYING DIGITAL EVIDENCE

- Digital evidence
  - Can be any information stored or transmitted in digital form
- U.S. courts accept digital evidence as physical evidence
  - Digital data is a tangible object
- Some require that all digital evidence be printed out to be presented in court
- Groups
  - Scientific Working Group on Digital Evidence (SWGDE) Active law enforcement only
  - International Organization on Computer Evidence (IOCE)

IDENTIFYING DIGITAL EVIDENCE (CONTINUED)

- General tasks investigators perform when working with digital evidence:
  - Identify digital information or artifacts that can be used as evidence
  - Collect, preserve, and document evidence
  - Analyze, identify, and organize evidence
  - Rebuild evidence or repeat a situation to verify that the results can be reproduced reliably
- Collecting computers and processing a criminal or incident scene must be done systematically

UNDERSTANDING RULES OF EVIDENCE

- Consistent practices help verify your work and enhance your credibility
- Comply with your state's rules of evidence or with the Federal Rules of Evidence
- Evidence admitted in a criminal case can be used in a civil suit, and vice versa
- Keep current on the latest rulings and directives on collecting, processing, storing, and admitting digital evidence

UNDERSTANDING RULES OF EVIDENCE (CONTINUED)

- Data you discover from a forensic examination falls under your state's rules of evidence
  - Or the Federal Rules of Evidence
- Digital evidence is unlike other physical evidence because it can be changed more easily
  - The only way to detect these changes is to compare the original data with a duplicate
- Most federal courts have interpreted computer records as hearsay evidence
  - Hearsay is secondhand or indirect evidence

UNDERSTANDING RULES OF EVIDENCE (CONTINUED)

- Business-record exception
  - Allows "records of regularly conducted activity," such as business memos, reports, records, or data compilations
- Generally, computer records are considered admissible if they qualify as a business record
- Computer records are usually divided into:
  - **Computer-generated records**
  - **Computer-stored records**

UNDERSTANDING RULES OF EVIDENCE (CONTINUED)

- Computer records must be shown to be authentic and trustworthy
  - To be admitted into court
- Computer-generated records are considered authentic
  - If the program that created the output is functioning correctly
- Collecting evidence according to the proper steps of evidence control helps ensure that the computer evidence is authentic

UNDERSTANDING RULES OF EVIDENCE (CONTINUED)

- When attorneys challenge digital evidence
  - Often they raise the issue of whether computer-generated records were altered
    - Or damaged after they were created
- One test to prove that computer-stored records are authentic is to demonstrate that a specific person created the records
  - The author of a Microsoft Word document can be identified by using file metadata

UNDERSTANDING RULES OF EVIDENCE (CONTINUED)

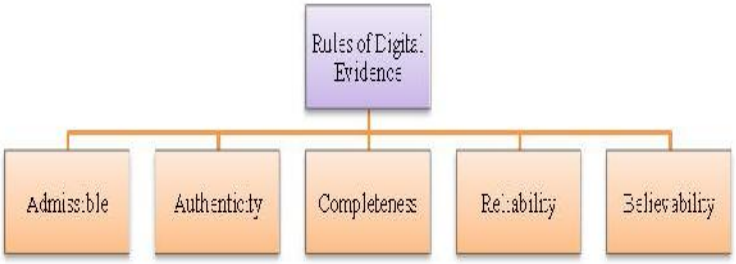
- The process of establishing digital evidence's trustworthiness originated with written documents and the best evidence rule
- Best evidence rule states:
  - To prove the content of a written document, recording, or photograph, ordinarily the original writing, recording, or photograph is required

UNDERSTANDING RULES OF EVIDENCE (CONTINUED)

- Federal Rules of Evidence
  - Allow a duplicate instead of originals when it is "produced by the same impression as the original … by mechanical or electronic re- recording … or by other equivalent techniques which accurately reproduce the original."
- As long as bit-stream copies of data are created and maintained properly
  - The copies can be admitted in court, although they aren't considered best evidence

RULES OF EVIDENCE

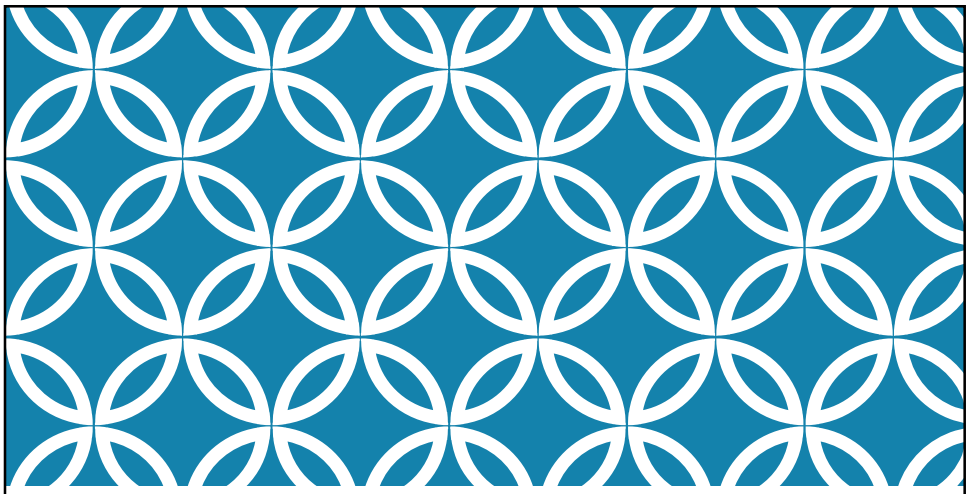
Any data or information that is stored or transmitted in digital form can be accepted as digital evidence in a court of law if it passes the test of admissibility and weight which is known as digital evidence criteria discussed in Sommer (1999) and Kozushko (2003).



13

RULES OF EVIDENCE

- 1st Rule: digital evidence **must be able to be used in court (admissible)**. Failure to comply with this rule is equivalent to not collecting the evidence in the first place.
- 2nd Rule: digital evidence **must be authentic**. In this rule, digital evidence must be tied to the incident in order to prove something. The digital evidence must be shown to relate to the incident in a relevant way.
- 3rd Rule: the evidence **must be complete** to affect the admissibility of the digital evidence. It is not sufficient to collect digital evidence that only shows one perspective of the incident. Therefore, the digital evidence should be collected not only to prove an attacker's actions, but also to prove their innocence. For instance, if it can be shown that the attacker logged in at the time of the incident, it also needs to be shown who else were logged in or not, so as to possibly prove the innocence of another person. This is called **exculpatory evidence** and it is an important part of proving a case.
- 4th Rule: is **reliability** and more specifically, the evidence collection and analysis procedures must not cast doubt on the evidence's authenticity and accuracy.
- 5th Rule: is **believability**. The evidence that is presented should be clearly understandable and believable by a jury.



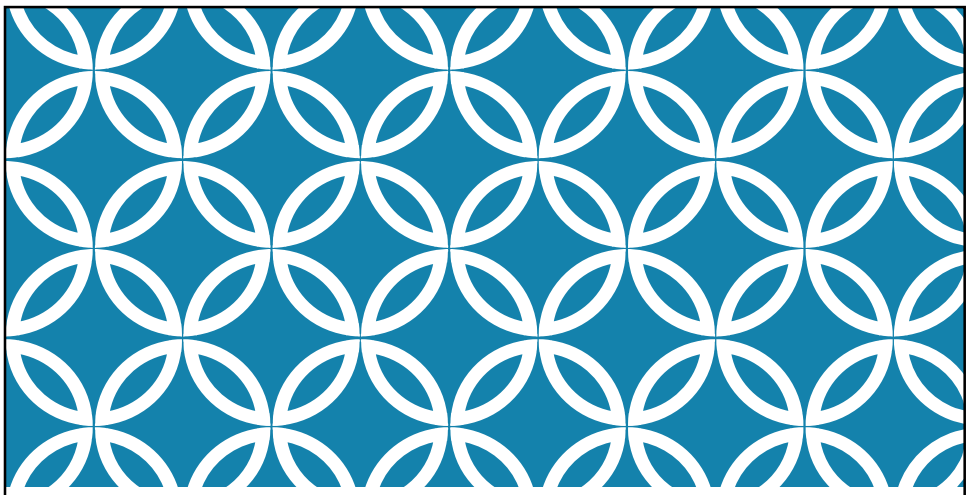
SECURING DIGITAL EVIDENCE AT AN INCIDENT SCENE

SECURING DIGITAL EVIDENCE AT AN INCIDENT SCENE

- Depends on the nature of the case
- Considerations:
  - Do you need to take the entire computer system?
  - Is the computer powered on when you arrive?
  - Is the suspect near the area of the computer?

SECURING DIGITAL EVIDENCE AT AN INCIDENT SCENE (CONTINUED)

- Guidelines:
  - Create a forensics copy
  - Handling a powered-on computer
    - Photograph the screen contents first
    - Save active data to removable media
    - Shutdown the computer
  - Still- and video-record the scene
  - Be invisible



CATALOGING DIGITAL EVIDENCE

CATALOGING DIGITAL EVIDENCE

- If the computer is turned off:
  - Identify the type of computer
  - Photograph all cable connections
  - Label cables with evidence tags
  - Assign one person to collect and log evidence
  - Tagging
    - Current date and time
    - Serial numbers
    - Make and model

CATALOGING DIGITAL EVIDENCE (CONTINUED)

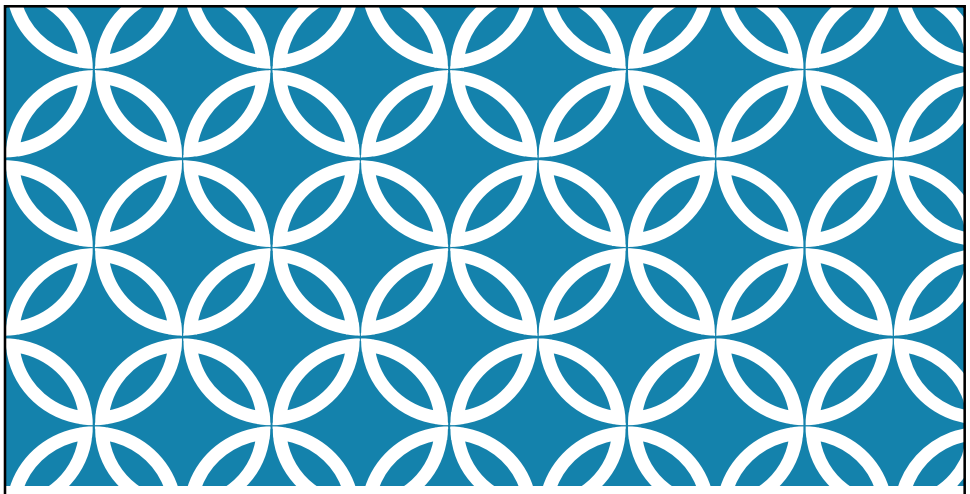
- If the computer is turned off (continued):
  - Maintain two separated logs for backup purposes
  - Maintain constant control of the evidence collected and the scene
- Additional steps if the computer is turned on:
  - Copy any application data on screens
  - Save RAM data to removable media
  - Shutdown the computer
  - Use another OS to examine hard disk data
  - Create a bit-stream copy of the suspect's hard disk
  - Verify integrity of the forensic copy

LAB EVIDENCE CONSIDERATIONS

- Transport evidence to your lab
  - Ensure security and integrity of digital evidence
- Record your activities and findings
- Goal
  - Reproduce the same results
- Save your journal for future references
  - At court
  - Training

PROCESSING AND HANDLING DIGITAL EVIDENCE

- Create a bit-stream copy
  - Use a write-blocking device
- Preserve the image file
- Steps:
  - Copy all bit-stream images to a large hard disk
  - Start forensics tools
  - Check bit-stream image file integrity
  - Place the original media in an evidence locker



STORING DIGITAL EVIDENCE

STORING DIGITAL EVIDENCE

- The media you use to store digital evidence usually depends on how long you need to keep it
- CD-Rs or DVDs
  - The ideal media
  - Capacity: up to 17 GB
  - Lifespan: 2 to 5 years
- Magnetic tapes
  - Capacity: 40 to 72 GB
  - Lifespan: 30 years
  - Costs: drive: $400 to $800; tape: $40

STORING DIGITAL EVIDENCE (CONTINUED)

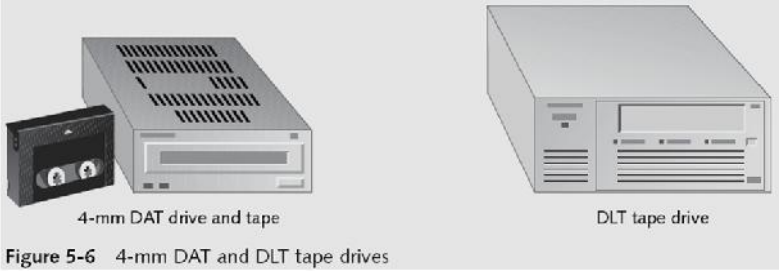


Figure 5-6 4-mm DAT and DLT tape drives

EVIDENCE RETENTION AND MEDIA STORAGE NEEDS

- To help maintain the chain of custody for digital evidence
  - Restrict access to lab and evidence storage area
- Lab should have a sign-in roster for all visitors
  - Maintain logs for a period based on legal requirements
- You might need to retain evidence indefinitely
  - Check with your local prosecuting attorney's office or state laws to make sure you're in compliance
  - You cannot retain child pornography evidence, however

EVIDENCE RETENTION AND MEDIA STORAGE NEEDS (CONTINUED)

Item description:				
Item tag number:				
Person	Date logged out	Time logged out	Date logged in	Time logged in

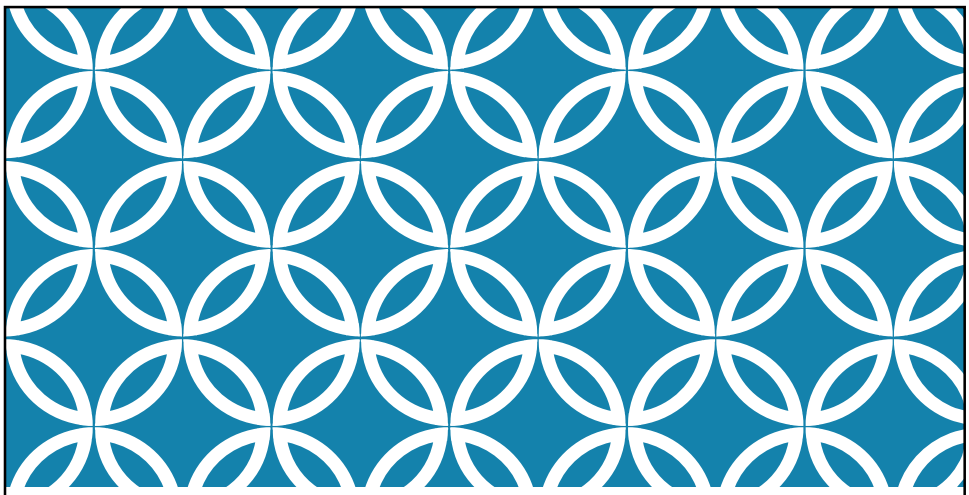
Figure 5-7 A sample log file

DOCUMENTING EVIDENCE

- Create or use an evidence custody form
- An evidence custody form serves the following functions:
  - Identifies the evidence
  - Identifies who has handled the evidence
  - Lists dates and times the evidence was handled
- You can add more information to your form
  - Such as a section listing MD5 and SHA-1 hash values

DOCUMENTING EVIDENCE (CONTINUED)

- Include any detailed information you might need to reference
- Evidence bags also include labels or evidence forms you can use to document your evidence



OBTAINING A DIGITAL HASH

OBTAINING A DIGITAL HASH

- Obtain a unique identity for file data
- Digital hash changes if a bit or byte changes
  - Verification process
  - Create a hash value
  - Analyze data
  - Create a second hash value
  - Compare hash values

OBTAINING A DIGITAL HASH (CONTINUED)

- Secure Hash Algorithm (SHA)
  - Developed by NIST
- Digital hashes are like digital fingerprints
- Non-keyed hash set can identify known programs
- Keyed hash set can produce a unique fingerprint

OBTAINING A DIGITAL HASH (CONTINUED)

- Example:
  - Create a file with Notepad
  - Obtain its hash value with DriveSpy
  - Modify the file
  - Recompute its hash value
  - Compare hash values

OBTAINING A DIGITAL HASH (CONTINUED)

- **Cyclic Redundancy Check (CRC)**
  - Mathematical algorithm that determines whether a file's contents have changed
  - Most recent version is CRC-32
  - Not considered a forensic hashing algorithm
- **Message Digest 5 (MD5)**
  - Mathematical formula that translates a file into a hexadecimal code value, or a hash value
  - If a bit or byte in the file changes, it alters the **digital hash**

OBTAINING A DIGITAL HASH (CONTINUED)

- Three rules for forensic hashes:
  - You can't predict the hash value of a file or device
  - No two hash values can be the same
  - If anything changes in the file or device, the hash value must change
- **Secure Hash Algorithm version 1 (SHA-1)**
  - A newer hashing algorithm
  - Developed by the **National Institute of Standards and Technology (NIST)**

OBTAINING A DIGITAL HASH (CONTINUED)

- In both **MD5** and **SHA-1**, collisions have occurred
- Most computer forensics hashing needs can be satisfied with a non-keyed hash set
  - A unique hash number generated by a software tool, such as the Linux md5sum command
- **Keyed hash set**
  - Created by an encryption utility's secret key
- You can use the MD5 function in FTK Imager to obtain the digital signature of a file
  - Or an entire drive

OBTAINING A DIGITAL HASH (CONTINUED)

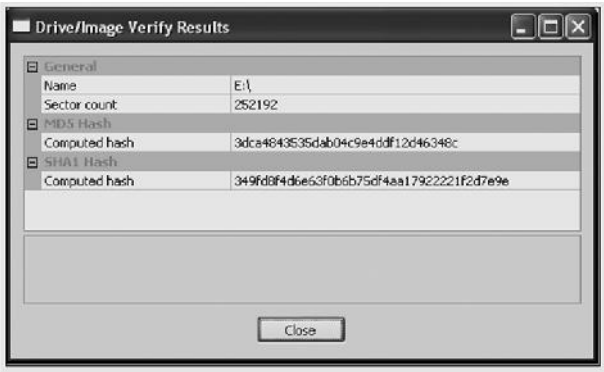


Figure 5-8 Using FTK Imager to verify hash values

SUMMARY

- Digital evidence
  - Information stored or transmitted on electronic or optical media
  - Fragile and easy to alter
- Working with digital evidence
  - Identify potential evidence
  - Collect, preserve, document, analyze, and organize the evidence

SUMMARY (CONTINUED)

- Handle evidence consistently for criminal or civil investigations
- Catalog or document evidence you find on a crime scene
- Store evidence
- Create forensic copies of your evidence
- Use digital signatures to verify evidence integrity