UNIT IV
EVIDENCE COLLECTION AND FORENSICS TOOLS

Processing Crime and Incident Scenes

Objectives

- Explain the **rules** for digital evidence
- Describe how to **collect** evidence at private-sector incident scenes
- Explain **guidelines for processing** law enforcement crime scenes
- List the steps in **preparing** for an evidence search
- Describe how to **secure** a computer incident or crime scene
- Explain guidelines for **seizing** digital evidence at the scene
- List procedures for **storing** digital evidence
- Explain how to **obtain a digital hash**
- Review a case to identify requirements and plan your investigation

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

Identifying Digital Evidence

- The following are two groups that set standards for recovering, preserving, and examining digital evidence
  - Scientific Working Group on Digital Evidence (SWGDE)
  - International Organization on Computer Evidence (IOCE)

Identifying Digital Evidence

- 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

Identifying Digital Evidence

- Collecting computers and processing an incident must be done **systematically**
  - Minimize confusion by avoiding losing and damaging evidence
  - only **one person** should collect and catalog
  - If there's too much evidence or too many then all examiners must follow the same procedures, and a **lead or managing examiner** should control collecting and cataloging evidence
  - consistently handle evidence in a **safe, secure manner**
  - **Great challenge** - establishing recognized standards for digital evidence

Understanding Rules of Evidence

- **Handle all evidence consistently**
  - help verify your work and enhance your credibility
  - Apply the same security and accountability controls
- **Comply with rules** of evidence
  - State's rules of evidence
  - Federal Rules of Evidence
- Evidence admitted in a criminal case can be used in a civil suit, and vice versa
- **Follow latest rules** on collecting, processing, storing, and admitting digital evidence

Understanding Rules of Evidence

- Digital evidence **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

- **Twenty-four exceptions** - in the federal rules don't require proof
  - 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

Understanding Rules of Evidence

- Computer records are usually divided into:
  - **Computer-generated records**
    - Records (data) the system maintains - **Log files**
  - **Computer-stored records**
    - Records person creates and saves on a computer - **Word doc, spreadsheet**

Understanding Rules of Evidence

- Computer records must be shown to be **authentic** and trustworthy
  - To be admitted into court
- **Computer-generated records** are authentic
  - If the program that created the output **is functioning correctly**
- **Computer-stored records** are authentic
  - the person offering must demonstrate that a person created the data and the data is reliable and trustworthy—in other words, that **it wasn't altered** when it was acquired or afterward

Understanding Rules of Evidence

- Collecting *evidence* according to the **proper steps** of evidence control helps **ensure** that the computer evidence is **authentic**

Understanding Rules of Evidence

- 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

- The author of a Microsoft Word document can be identified by using file metadata
  - Text that is formatted as hidden (a font effect that is available in the **Font** dialog box)
  - **Word 2007**
    - Click **Menus** tab
    - On **File** menu, choose **Prepare**
    - Click **Property** in the drop down menu, you will see the **document properties panel**

Understanding Rules of Evidence

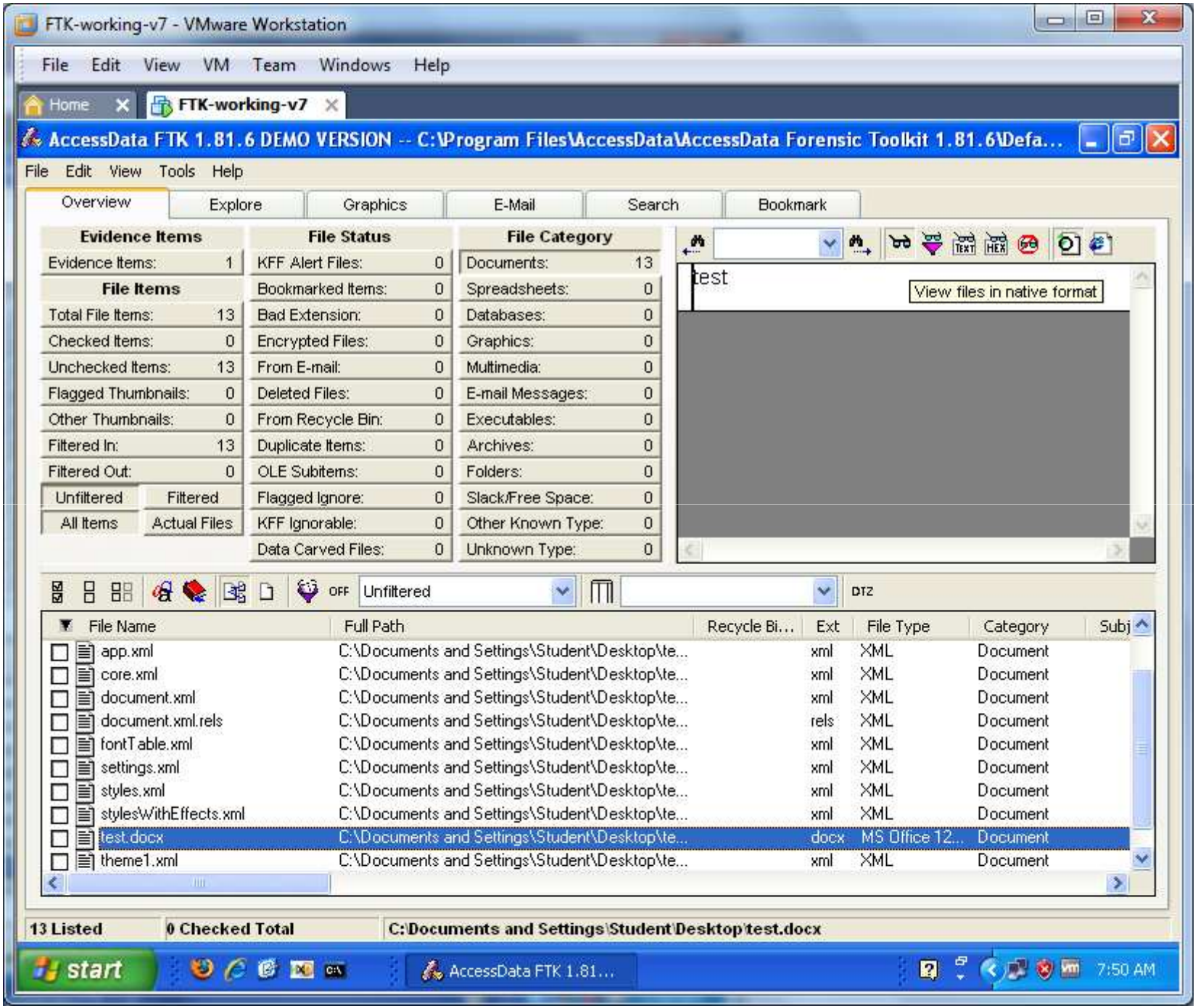
- **Word 2010 and 2013:**
  - Click **File** tab
  - On **Info** part, move to **Properties** in the right side of the pane
  - Click the down arrow, and choose **Advanced Properties** in the menu
  - You will get a pop up window, where you can make change in the dialog

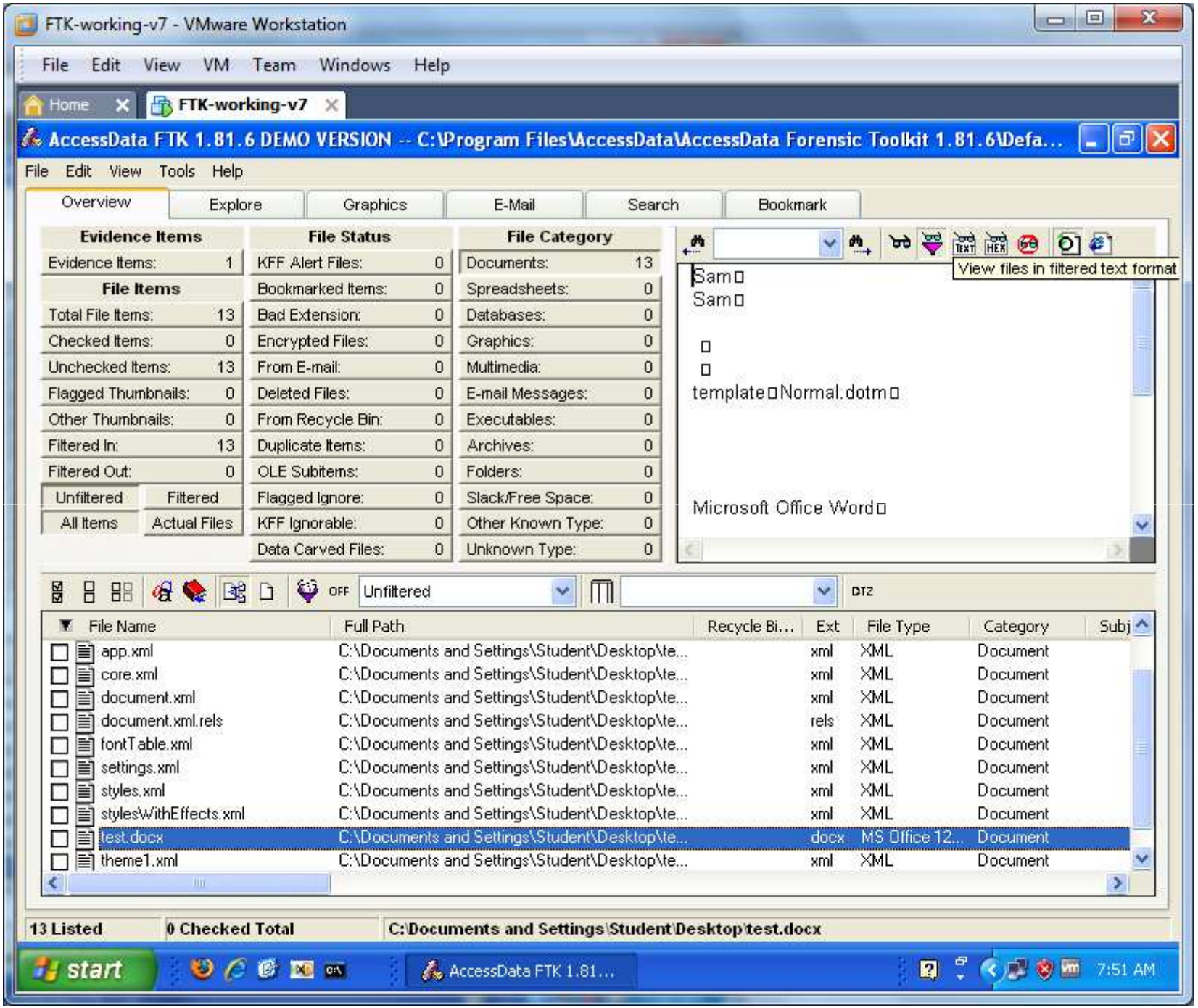
Demo: Metadata in FTK

- Save a Word document
- In FTK:
  - Click **No**, **OK**, **OK** through the demo warning boxes
  - Go directly to working with program
  - **File**, **Add Evidence**
  - Enter your name, **Next**, **Next**
  - Click "**Add Evidence**" button
  - Click "**Individual File**", **Continue**
  - Navigate to Word document,double-click it
  - **OK**, **Next**, **Continue**

FTK Demo

- In "File Category", click the **Documents** button
- Select the document in the lower pane
- "**View files in native format**" shows the text typed into the Word document
- "**View files in filtered text format**" shows the metadata, such as the registered owner of the program


FTK-working-v7 - VMware Workstation
File Edit View VM Team Windows Help
Home
FTK-working-v7
AccessData FTK 1.81.6 DEMO VERSION -- C:\Program Files\AccessData\AccessData Forensic Toolkit 1.81.6\Defa...
File Edit View Tools Help
Overview
Explore
Graphics
E-Mail
Search
Bookmark
Evidence Items
Evidence Items: 1
File Items
Total File Items: 13
Checked Items: 0
Unchecked Items: 13
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 13
Filtered Out: 0
Unfiltered
Filtered
All Items
Actual Files
File Status
KFF Alert Files: 0
Bookmarked Items: 0
Bad Extension: 0
Encrypted Files: 0
From E-mail: 0
Deleted Files: 0
From Recycle Bin: 0
Duplicate Items: 0
OLE Subitems: 0
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 0
File Category
Documents: 13
Spreadsheets: 0
Databases: 0
Graphics: 0
Multimedia: 0
E-mail Messages: 0
Executables: 0
Archives: 0
Folders: 0
Slack/Free Space: 0
Other Known Type: 0
Unknown Type: 0
test
View files in native format
OFF
Unfiltered
DTZ
File Name
Full Path
Recycle Bi...
Ext
File Type
Category
Subj
app.xml C:\Documents and Settings\Student\Desktop\te... xml XML Document
core.xml C:\Documents and Settings\Student\Desktop\te... xml XML Document
document.xml C:\Documents and Settings\Student\Desktop\te... xml XML Document
document.xml.rels C:\Documents and Settings\Student\Desktop\te... rels XML Document
fontTable.xml C:\Documents and Settings\Student\Desktop\te... xml XML Document
settings.xml C:\Documents and Settings\Student\Desktop\te... xml XML Document
styles.xml C:\Documents and Settings\Student\Desktop\te... xml XML Document
stylesWithEffects.xml C:\Documents and Settings\Student\Desktop\te... xml XML Document
test.docx C:\Documents and Settings\Student\Desktop\te... docx MS Office 12... Document
theme1.xml C:\Documents and Settings\Student\Desktop\te... xml XML Document
13 Listed
0 Checked Total
C:\Documents and Settings\Student\Desktop\test.docx
start
AccessData FTK 1.81...
7:50 AM


FTK-working-v7 - VMware Workstation
File Edit View VM Team Windows Help
Home
FTK-working-v7
AccessData FTK 1.81.6 DEMO VERSION -- C:\Program Files\AccessData\AccessData Forensic Toolkit 1.81.6\Defa...
File Edit View Tools Help
Overview
Explore
Graphics
E-Mail
Search
Bookmark
Evidence Items
Evidence Items: 1
File Items
Total File Items: 13
Checked Items: 0
Unchecked Items: 13
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 13
Filtered Out: 0
Unfiltered
Filtered
All Items
Actual Files
File Status
KFF Alert Files: 0
Bookmarked Items: 0
Bad Extension: 0
Encrypted Files: 0
From E-mail: 0
Deleted Files: 0
From Recycle Bin: 0
Duplicate Items: 0
OLE Subitems: 0
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 0
File Category
Documents: 13
Spreadsheets: 0
Databases: 0
Graphics: 0
Multimedia: 0
E-mail Messages: 0
Executables: 0
Archives: 0
Folders: 0
Slack/Free Space: 0
Other Known Type: 0
Unknown Type: 0
View files in filtered text format
Sam
Sam
template Normal.dotm
Microsoft Office Word
OFF
Unfiltered
DTZ
File Name
Full Path
Recycle Bi...
Ext
File Type
Category
Subj
app.xml C:\Documents and Settings\Student\Desktop\te... xml XML Document
core.xml C:\Documents and Settings\Student\Desktop\te... xml XML Document
document.xml C:\Documents and Settings\Student\Desktop\te... xml XML Document
document.xml.rels C:\Documents and Settings\Student\Desktop\te... rels XML Document
fontTable.xml C:\Documents and Settings\Student\Desktop\te... xml XML Document
settings.xml C:\Documents and Settings\Student\Desktop\te... xml XML Document
styles.xml C:\Documents and Settings\Student\Desktop\te... xml XML Document
stylesWithEffects.xml C:\Documents and Settings\Student\Desktop\te... xml XML Document
test.docx C:\Documents and Settings\Student\Desktop\te... docx MS Office 12... Document
theme1.xml C:\Documents and Settings\Student\Desktop\te... xml XML Document
13 Listed
0 Checked Total
C:\Documents and Settings\Student\Desktop\test.docx
start
AccessData FTK 1.81...
7:51 AM

Understanding Rules of Evidence

- 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, **original** writing, recording, or photograph is **required**

Understanding Rules of Evidence

- **Computer-generated records**, such as system logs or the results of a mathematical formula in a spreadsheet, **aren’t hearsay**

- **Computer-stored records** that a person generates are subject to rules governing hearsay

Understanding Rules of Evidence

- 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

When a Copy is All You Have

- Example of not being able to use original evidence is investigations involving network Servers
- If the hard drive crashes after you make the copy
- If removing the original computers is not possible, because it would cause harm to a business or its owner, who might be an innocent bystander
  - Steve Jackson Games was harmed in this manner when the Secret Service seized all computers because BBS users placed evidence of a crime on them
  - The company sued and won

Collecting Evidence in Private-Sector Incident Scenes

Collecting Evidence in Private-Sector Incident Scenes

- Private-sector organizations include:
  - Businesses and government agencies that aren’t involved in law enforcement
- Agencies must comply with state public disclosure and federal Freedom of Information Act (FOIA) laws
  - And make certain documents available as public records
- FOIA allows citizens to request copies of public documents created by federal agencies

Collecting Evidence in Private-Sector Incident Scenes

- A special category of private-sector businesses includes ISPs and other communication companies
- ISPs can investigate computer abuse committed by their employees, but not by customers
  - Except for activities that are deemed to create an emergency situation
- Investigating and controlling computer incident scenes in the corporate environment
  - Much easier than in the criminal environment
  - Incident scene is often a workplace

Collecting Evidence in Private-Sector Incident Scenes

- Typically, businesses have inventory databases of computer hardware and software
  - Help identify the computer forensics tools needed to analyze a policy violation
    - And the best way to conduct the analysis
- Corporate policy statement about misuse of computing assets
  - Allows corporate investigators to conduct covert surveillance with little or no cause
  - And access company systems without a warrant

Collecting Evidence in Private-Sector Incident Scenes

- Companies should display a warning banner or publish a policy, or both
  - Stating that they reserve the right to inspect computing assets at will
- Corporate investigators should know under what circumstances they can examine an employee's computer
  - Every organization must have a well-defined process describing when an investigation can be initiated

Collecting Evidence in Private-Sector Incident Scenes

- If a corporate investigator finds that an employee is committing or has committed a crime
  - Employer can file a criminal complaint with the police
- Employers are usually interested in enforcing company policy
  - Not seeking out and prosecuting employees
- Corporate investigators are, therefore, primarily concerned with protecting company assets

Collecting Evidence in Private-Sector Incident Scenes

- If you discover evidence of a crime during a company policy investigation
  - Determine whether the incident meets the elements of criminal law
  - Inform management of the incident
  - Stop your investigation to make sure you don’t violate Fourth Amendment restrictions on obtaining evidence
  - Work with the corporate attorney to write an affidavit confirming your findings

Becoming an Agent of Law Enforcement

- If law enforcement officers ask you to find more information, you are at legal risk
  - Don’t do any further investigation until you receive a subpoena or court order