

THOMSON



COURSE TECHNOLOGY

# **Guide to Computer Forensics and Investigations, Second Edition**

*Chapter 2*

*Understanding Computer Investigation*

# Objectives

- Prepare a case
- Begin an investigation
- Understand computer forensics workstations and software

# Objectives (continued)

- Conduct an investigation
- Complete a case
- Critique a case

# Preparing a Computer Investigation

- Role of computer forensics professional: gather evidence to prove a suspect committed a crime or violated a company policy
- Collect evidence that can be offered in court or at a corporate inquiry
  - Investigate the suspect's computer
  - Preserve the evidence on a different computer

# Preparing a Computer Investigation (continued)

- Follow an accepted procedure to prepare a case
- The U.S. Department of Justice has a document you can download that reviews proper acquisition of electronic evidence
- 
- Chain of custody
  - Route the evidence takes from the time you find it until the case is closed or goes to court

# Examining a Computer Crime

- Computers can contain information that helps law enforcement determine:
  - Chain of events leading to a crime
  - Evidence that can lead to a conviction
- Law enforcement officers should follow proper procedure when acquiring the evidence
  - Digital evidence can be easily altered by an overeager investigator

# Examining a Computer Crime (Example page 30)



Figure 2-1 The crime scene

# Examining a Company Policy Violation

- Companies often establish policies for computer use by employees.
- Employees misusing resources can cost companies millions of dollars
- Misuse includes:
  - Surfing the Internet
  - Sending personal e-mails
  - Using company computers for personal tasks

# Taking a Systematic Approach

- Steps for problem solving:
  - Make an initial assessment about the type of case you are investigating
  - Determine a preliminary design or approach to the case
  - Create a detailed design
  - Determine the resources you need
  - Obtain and copy an evidence disk drive

# Taking a Systematic Approach (continued)

- Steps for problem solving (continued):
  - Identify the risks
  - Mitigate or minimize the risks
  - Test the design
  - Analyze and recover the digital evidence
  - Investigate the data you recovered
  - Complete the case report
  - Critique the case

# Assessing the Case

- Systematically outline the case details:
  - Situation
  - Nature of the case
  - Specifics about the case
  - Type of evidence
  - OS
  - Known disk format
  - Location of evidence

# Assessing the Case (continued)

- Based on case details, you can determine the case requirements:
  - Type of evidence
  - Computer forensics tools
  - Special OSs

# Planning your Investigation

- A basic investigation plan should include the following activities:
  - Acquire the evidence
  - Complete an evidence form and establish a chain of custody
  - Transport evidence to a computer forensics lab
  - Secure evidence in an approved secure container

# Planning your Investigation (continued)

- A basic investigation plan (continued):
  - Prepare a forensics workstation
  - Obtain the evidence from the secure container
  - Make a forensic copy of the evidence
  - Return the evidence to the secure container
  - Process the copied evidence with computer forensics tools

# Planning your Investigation (continued)

- An evidence custody form helps you document what has been done with the original evidence and its forensics copies
- There are two types:
  - Single-evidence form
  - Multi-evidence form





# Securing your Evidence

- Use evidence bags to secure and catalog the evidence
- Use computer safe products
  - Antistatic bags
  - Antistatic pads
- Use well-padded containers

# Securing your Evidence (continued)

- Use evidence tape to seal all openings
  - Floppy disk or CD drives
  - Power supply electrical cord
- Write your initials on tape to prove that evidence has not been tampered
- Consider computer-specific temperature and humidity ranges

# Understanding Data-Recovery Workstations and Software

- Investigations are conducted on a computer forensics lab (or data-recovery lab)
- Computer forensics and data-recovery are related but different
- Computer forensics workstation
  - Specially configured personal computer
- To avoid altering the evidence, use:
  - Forensics boot floppy disk
  - Write-blockers devices

# Setting Up your Workstation for Computer Forensics

- Set up Windows 98 workstation to boot into MS-DOS
  - Display a Startup menu
  - Modify Msdos.sys file using any text editor
- Install a computer forensics tool
  - DriveSpy and Image

# Setting Up your Workstation for Computer Forensics (continued)



Figure 2-5 The Advanced Troubleshooting Settings dialog box



# Conducting an Investigation

- Begin by copying the evidence using a variety of methods
  - Recall that no single method retrieves all data
  - The more methods you use, the better

# Gathering the Evidence

- Take all necessary measures to avoid damaging the evidence
  - Place the evidence in a secure container
- Complete the evidence custody form
- Transport the evidence to the computer forensics lab
- Create forensics copies (if possible)
- Secure evidence by locking the container

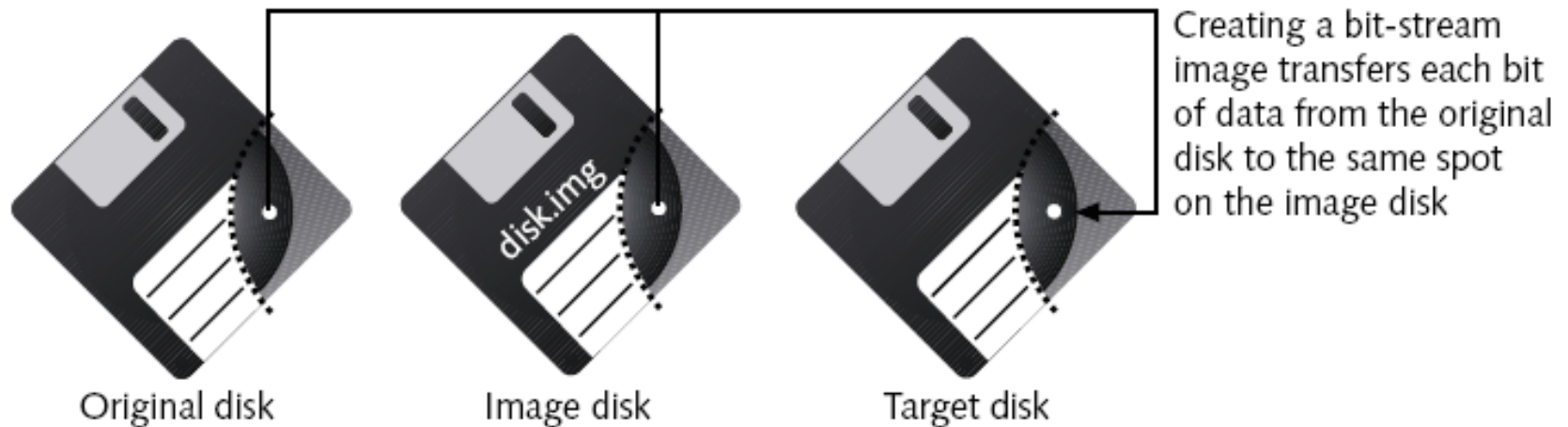
# Understanding Bit-stream Copies

- Bit-by-bit copy of the original storage medium
- Exact copy of the original disk
- Different from a simple backup copy
  - Backup software only copy known files
  - Backup software cannot copy deleted files or e-mail messages, or recover file fragments

# Understanding Bit-stream Copies (continued)

- A bit-stream image file contains the bit-stream copy of all data on a disk or partition
- Preferable to copy the image file to a target disk that matches the original disk's manufacturer, size, and model

# Understanding Bit-stream Copies (continued)



**Figure 2-8** Transfer of data from original to bit-stream image to target

# Creating a Forensic Boot Floppy Disk

- Goal is not to alter the original data on a disk
- Preferred way to preserve the original data is to never examine it
  - Make forensic copies
  - Create a special boot floppy disk that prevents OS from altering the data when the computer starts up
  - Windows 9x can also alter other files, especially if DriveSpace is implemented on a file allocation table (FAT) 16 disk

# Assembling the Tools for a Forensic Boot Floppy Disk

- Tools:
  - Disk editor such as Norton Disk Edit or Hex Workshop
  - Floppy disk
  - MS-DOS OS
  - Computer that can boot to a true MS-DOS level
  - Forensics acquisition tool
  - Write-block tool

# Assembling the Tools for a Forensic Boot Floppy Disk (continued)

- Steps:
  - Make the floppy disk bootable
  - Update the OS files to remove any reference to the hard disk (using Hex Workshop or Norton Disk Edit)
    - Modify the command.com file on the floppy disk
    - Modify the io.sys file on the floppy disk
  - Add computer forensic tools
  - Test your floppy disk
  - Create several backup copies

# Assembling the Tools for a Forensic Boot Floppy Disk (continued)

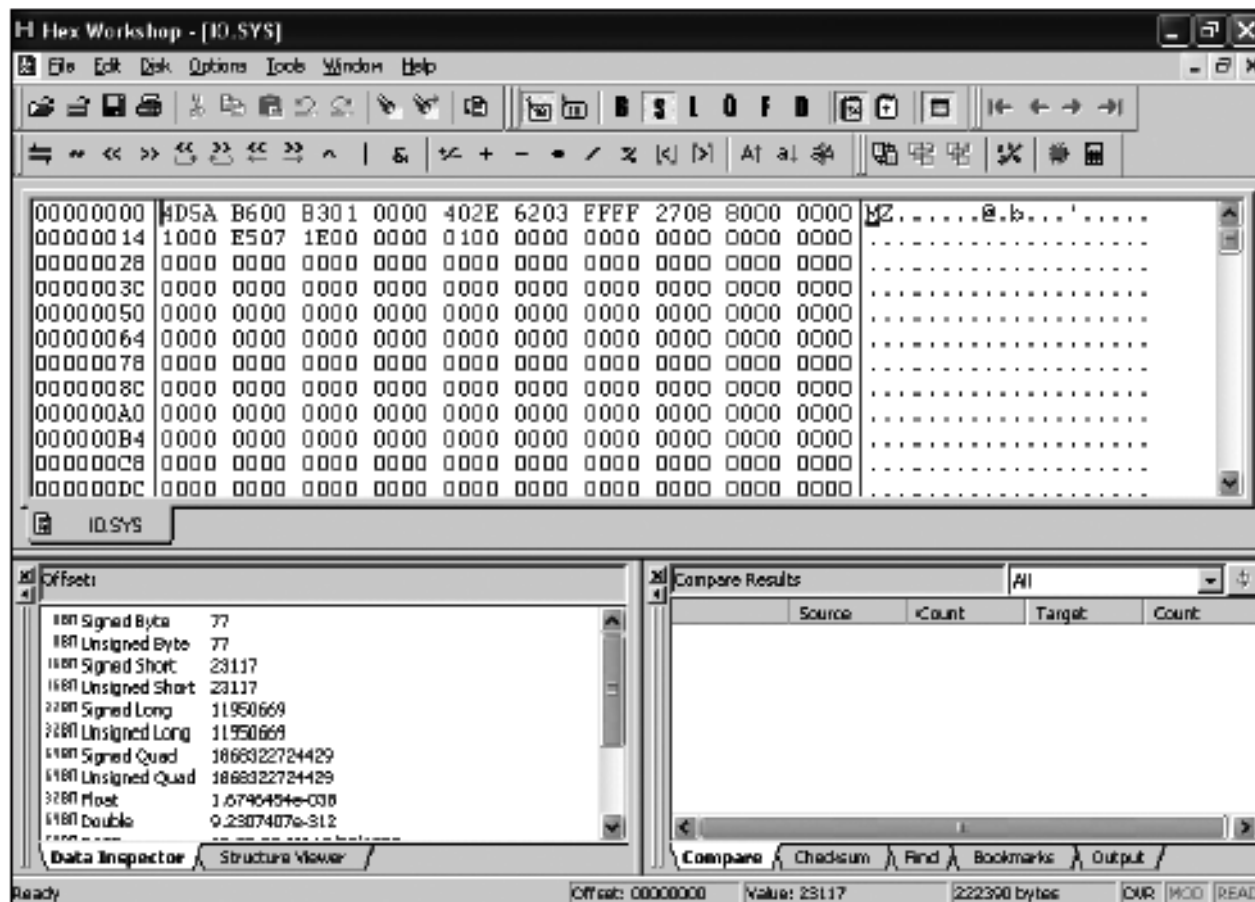


Figure 2-11 Io.sys open in Hex Workshop

# Retrieving Evidence Data Using a Remote Network Connection

- Bit-stream image copies can also be retrieved from a workstation's network connection
- Software:
  - SnapBack
  - EnCase
  - R-Tools
- Can be a time-consuming process even with a 1000-Mb connection
- It takes less using a NIC-to-NIC connection

# Copying the Evidence Disk

- A forensic copy is an exact duplicate of the original data
- Create a forensic copy using:
  - MS-DOS
  - Specialized tool such as Digital Intelligence's Image
    - First, create a bit-stream image
    - Then, copy the image to a target disk

# Creating a Bit-stream Image with FTK Imager

- Start Forensic Toolkit (FTK) Imager by double-clicking the icon on your desktop
- Click File, Image Drive from the menu; insert floppy disk labeled “Domain Name working copy #2”
- In the dialog box that opens, click the A: drive to select a local drive, then click OK

# Creating a Bit-stream Image with FTK Imager (continued)

- A wizard walks you through the steps
  - Accept all the defaults
  - Specify the destination folder
  - If necessary, create a folder called Forensics Files
  - Name the file Bootimage.1

# Analyzing Your Digital Evidence

- Your job is to recover data from:
  - Deleted files
  - File fragments
  - Complete files
- Deleted files linger on the disk until new data is saved on the same physical location
- Tools:
  - Digital Intelligence's DriveSpy
  - AccessData's FTK

# Analyzing Your Digital Evidence (continued)

- DriveSpy is a powerful tool that recovers and analyzes data on FAT12, FAT16, and FAT32 disks
  - Can search for altered files and keywords
- FTK is an easy-to-use GUI application for FAT12, FAT16, FAT32, and new technology file system (NTFS) disks
  - FTK Imager
  - Registry Viewer
  - Password Recovery Toolkit

# Analyzing Your Digital Evidence (continued)

```
DRIVESPY V1.62:
Copyright 1998,1999,2000,2001 Digital Intelligence, Inc., All Rights Reserved

This copy of DRIVESPY licensed to:

Type "HELP" for online help

ECHO is OFF: Sun Jul 21 22:10:30 2002
PAGE is ON

Physical Drives on this System:

Drive | Mode | Cylinders | Heads | Sectors | Length | Size (Mb)
-----|-----|-----|-----|-----|-----|-----
  0   | LBA  |           |       |         | 8452080 | 4126
      | CHS  | 525       | 255   | 63      | 8434125 | 4118

Note: CHS values are not displayed for LBA drives which do not provide
the associated information via Interrupt 13 Extensions. This will
in no way adversely effect the performance or accuracy of DRIVESPY.

SYS>
```

SYS prompt where you type DriveSpy commands

Figure 2-13 The opening screen for DriveSpy

# Analyzing Your Digital Evidence (continued)

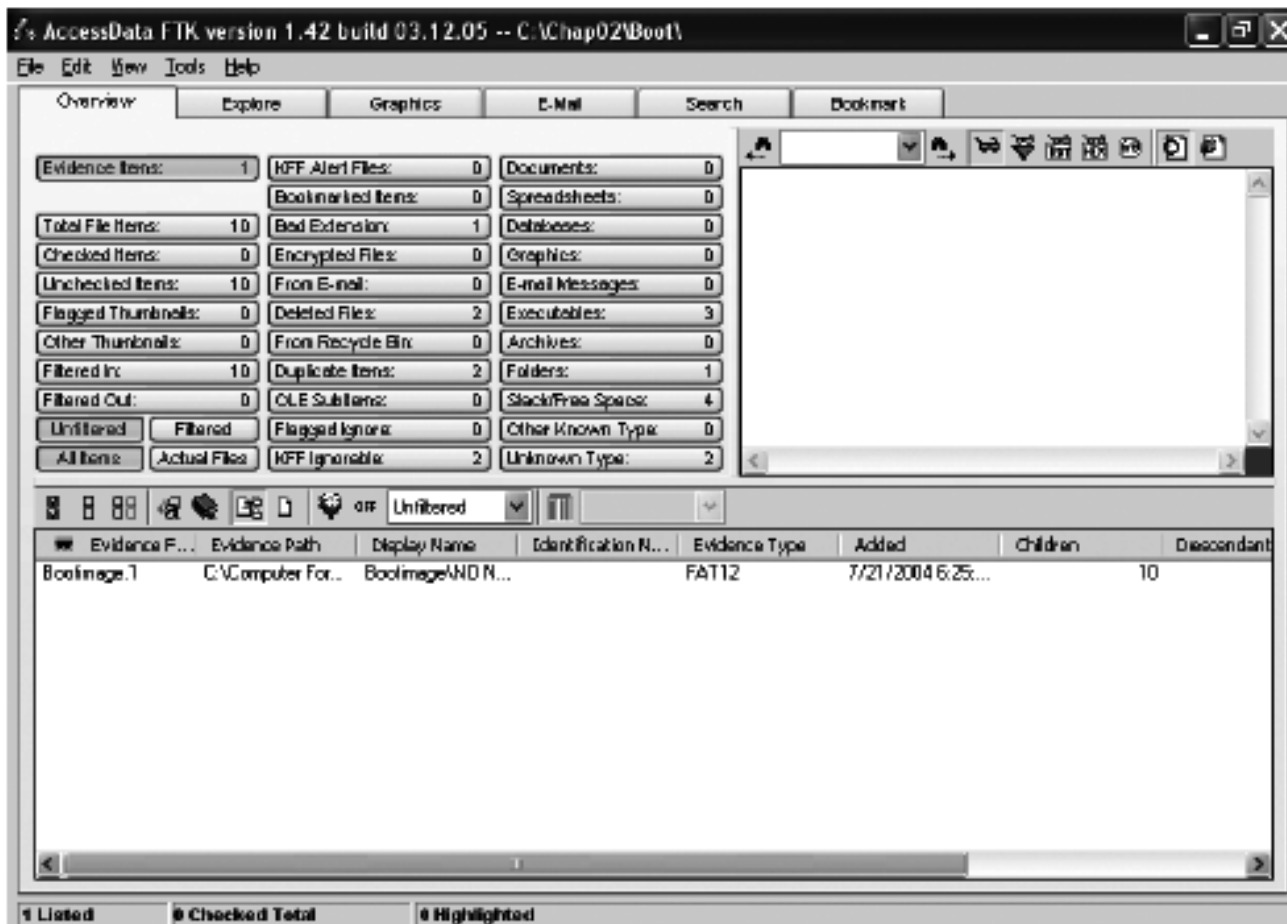


Figure 2-21 FTK's Overview window

# Completing the Case

- You need to produce a final report
  - State what you did and what you found
- You can even include logs from the forensic tools you used
- If required, use a report template
- The report should show conclusive evidence that the suspect did or did not commit a crime or violate a company policy

# Critiquing the Case

- Ask yourself the following questions:
  - How could you improve your participation in the case?
  - Did you expect the results you found?
  - Did the case develop in ways you did not expect?
  - Was the documentation as thorough as it could have been?

# Critiquing the Case (continued)

- Questions continued:
  - What feedback has been received from the requesting source?
  - Did you discover any new problems? What are they?
  - Did you use new techniques during the case or during research?

# Summary

- Use a systematic approach to investigations
- Plan a case by taking into account:
  - Nature of the case
  - Case requirements
  - Gathering evidence techniques
- Do not forget that every case can go to court
- Apply standard problem-solving techniques

# Summary (continued)

- Keep track of the chain of custody of your evidence
- Create bit-stream copies of the original data
- Use the duplicates whenever possible
- Some tools: DriveSpy and Image, FTK, MS-DOS commands
- Produce a final report detailing what you did and found

# Summary (continued)

- Always critique your work as a way of improving it
- Apply these lessons to future cases