Guide to Computer Forensics and Investigations Fourth Edition

Chapter 7

Current Computer Forensics Tools

Objectives

- Explain how to evaluate needs for computer forensics tools
- Describe available computer forensics software tools
- List some considerations for computer forensics hardware tools
- Describe methods for validating and testing computer forensics tools

Evaluating Computer Forensics Tool Needs

- Look for versatility, flexibility, and robustness
  - OS
  - File system
  - Script capabilities
  - Automated features
  - Vendor's reputation
- Keep in mind what application files you will be analyzing

Types of Computer Forensics Tools

- Hardware forensic tools
  - Range from single-purpose components to complete computer systems and servers
- Software forensic tools
  - Types
    - Command-line applications
    - GUI applications
  - Commonly used to copy data from a suspect's disk drive to an image file

Tasks Performed by Computer Forensics Tools

- Five major categories:
  - Acquisition
  - Validation and discrimination
  - Extraction
  - Reconstruction
  - Reporting

Tasks Performed by Computer Forensics Tools (continued)

- **Acquisition**
  - Making a copy of the original drive
- Acquisition subfunctions:
  - Physical data copy
  - Logical data copy
  - Data acquisition format
  - Command-line acquisition
  - GUI acquisition
  - Remote acquisition
  - Verification

Tasks Performed by Computer Forensics Tools (continued)

- Acquisition (continued)
  - Two types of data-copying methods are used in software acquisitions:
    - Physical copying of the entire drive
    - Logical copying of a disk partition
  - The formats for disk acquisitions vary
    - From raw data to vendor-specific proprietary compressed data
  - You can view the contents of a raw image file with any hexadecimal editor

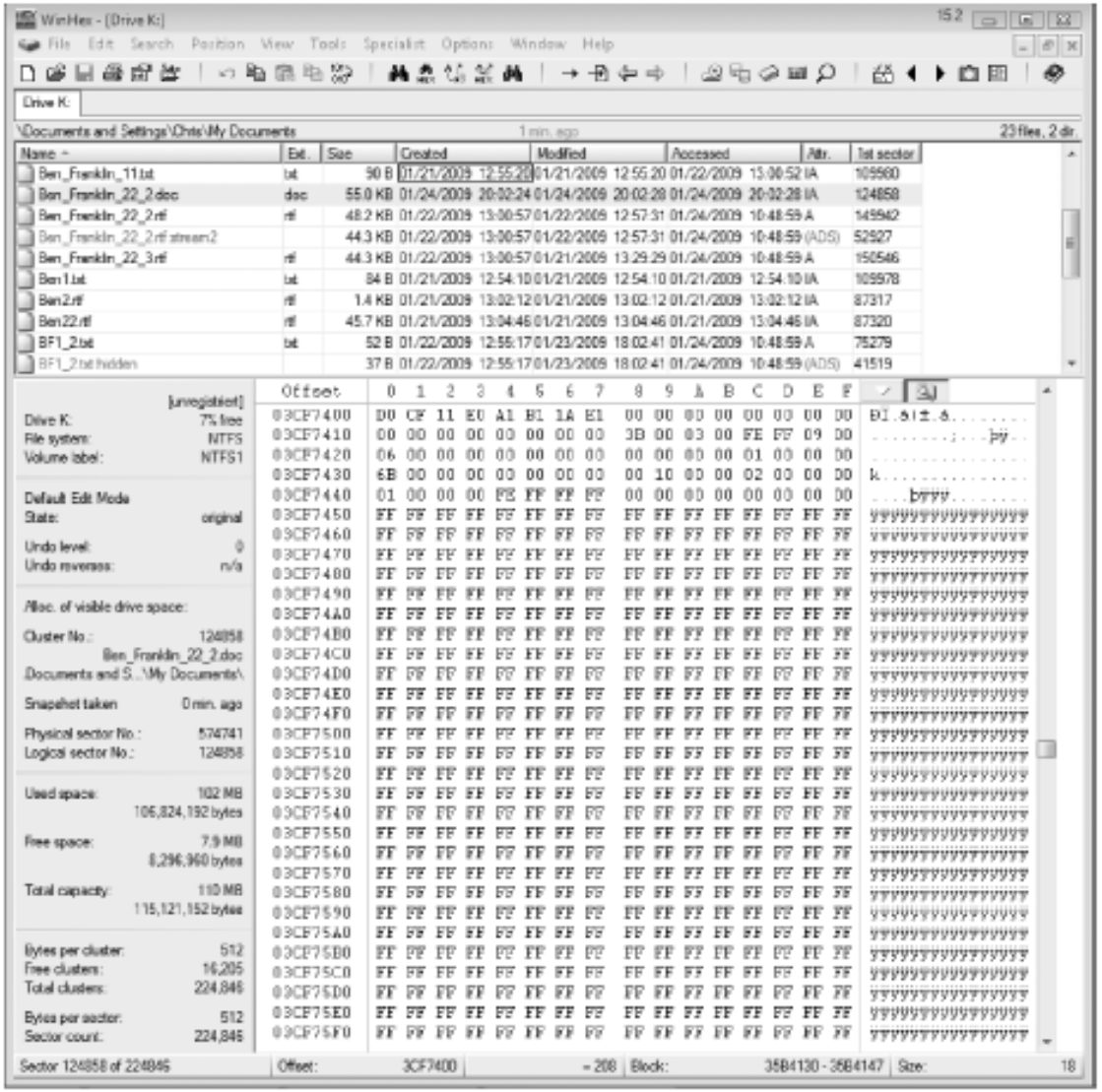

Figure 7-1 Viewing data in a hexadecimal editor

Tasks Performed by Computer Forensics Tools (continued)

- Acquisition (continued)
  - Creating smaller segmented files is a typical feature in vendor acquisition tools
  - All computer forensics acquisition tools have a method for verification of the data-copying process
    - That compares the original drive with the image

Tasks Performed by Computer Forensics Tools (continued)

- Validation and discrimination
  - **Validation**
    - Ensuring the integrity of data being copied
  - **Discrimination** of data
    - Involves sorting and searching through all investigation data

Tasks Performed by Computer Forensics Tools (continued)

- Validation and discrimination (continued)
  - Subfunctions
    - Hashing
      - CRC-32, MD5, Secure Hash Algorithms
    - Filtering
      - Based on hash value sets
    - Analyzing file headers
      - Discriminate files based on their types
  - National Software Reference Library (NSRL) has compiled a list of known file hashes
    - For a variety of OSs, applications, and images

Tasks Performed by Computer Forensics Tools (continued)

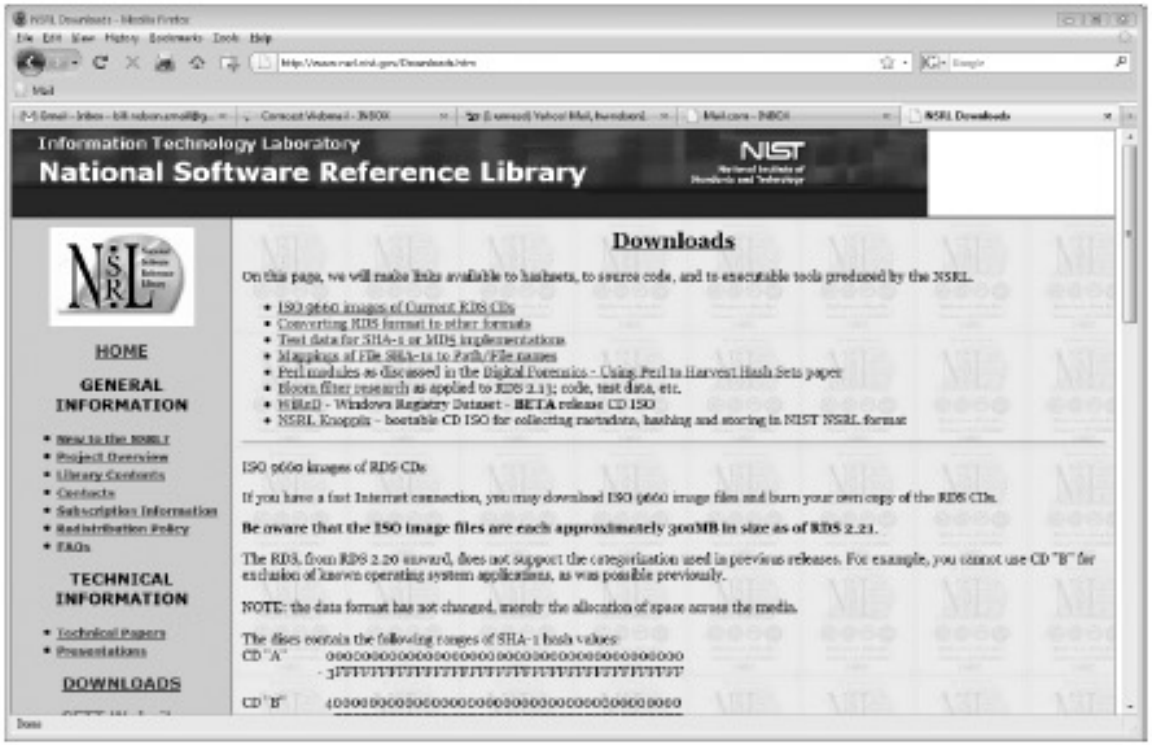

Figure 7-2 The download page of the National Software Reference Library

Tasks Performed by Computer Forensics Tools (continued)

- Validation and discrimination (continued)
  - Many computer forensics programs include a list of common header values
    - With this information, you can see whether a file extension is incorrect for the file type
  - Most forensics tools can identify header values

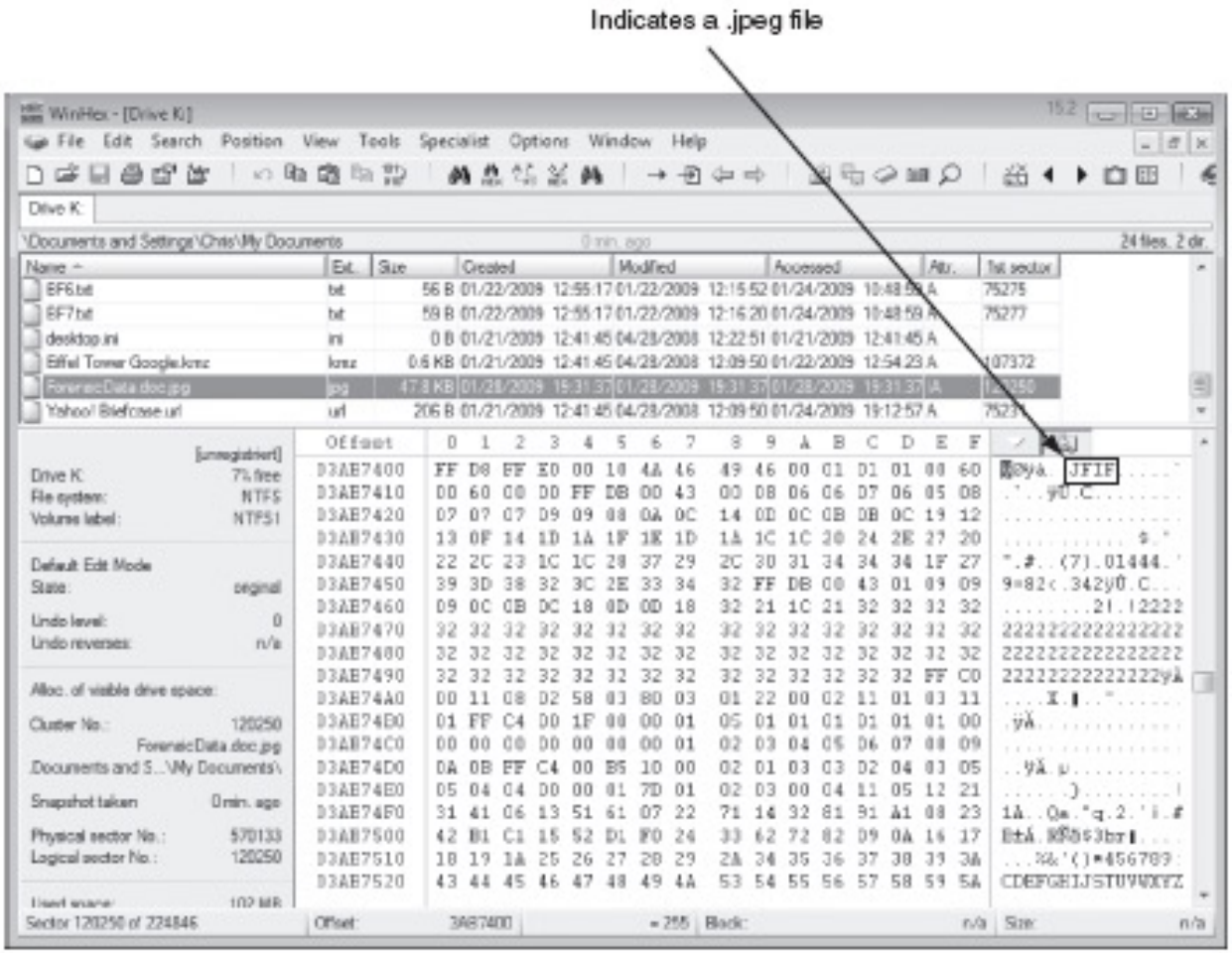

Figure 7-3 The file header indicates a .jpeg file

Tasks Performed by Computer Forensics Tools (continued)

Figure 7-4 Error message displayed when trying to open a JPEG file in Word

Figure 7-5 ForensicData.doc open in an image viewer

Tasks Performed by Computer Forensics Tools (continued)

- **Extraction**
  - Recovery task in a computing investigation
  - Most demanding of all tasks to master
  - Recovering data is the first step in analyzing an investigation's data

Tasks Performed by Computer Forensics Tools (continued)

- Extraction (continued)
  - Subfunctions
    - Data viewing
    - Keyword searching
    - Decompressing
    - Carving
    - Decrypting
    - Bookmarking
  - **Keyword search** speeds up analysis for investigators

Figure 7-6 The Indexed Search feature in FTK

Tasks Performed by Computer Forensics Tools (continued)

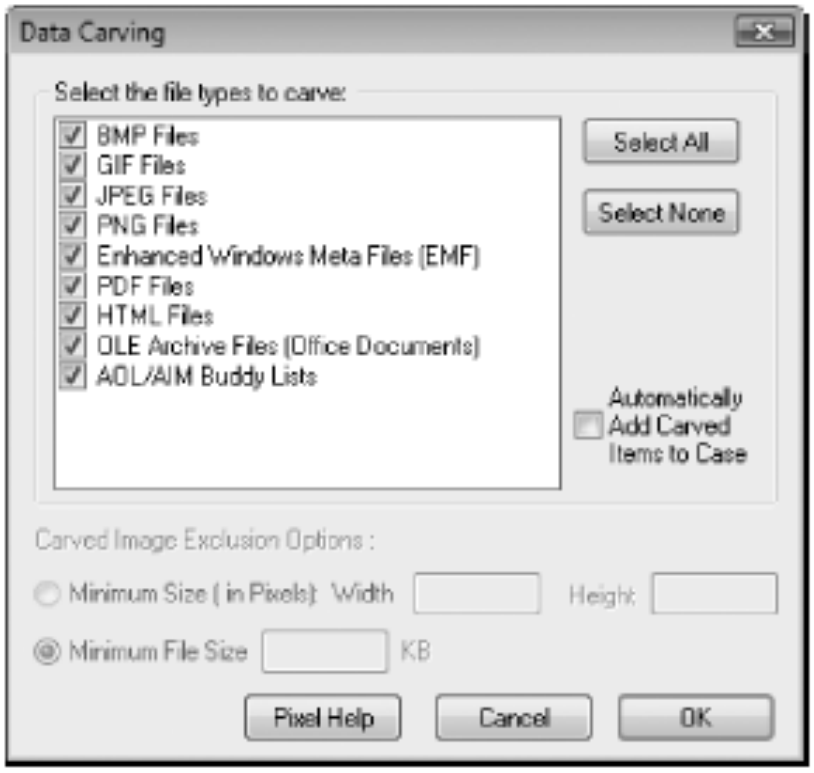

Figure 7-7 Data-carving options in FTK

Tasks Performed by Computer Forensics Tools (continued)

- Extraction (continued)
  - From an investigation perspective, encrypted files and systems are a problem
  - Many password recovery tools have a feature for generating potential password lists
    - For a **password dictionary attack**
  - If a password dictionary attack fails, you can run a **brute-force attack**

Tasks Performed by Computer Forensics Tools (continued)

- **Reconstruction**
  - Re-create a suspect drive to show what happened during a crime or an incident
  - Subfunctions
    - Disk-to-disk copy
    - Image-to-disk copy
    - Partition-to-partition copy
    - Image-to-partition copy

Tasks Performed by Computer Forensics Tools (continued)

- Reconstruction (continued)
  - Some tools that perform an image-to-disk copy:
    - SafeBack
    - SnapBack
    - EnCase
    - FTK Imager
    - ProDiscover

Tasks Performed by Computer Forensics Tools (continued)

- Reporting
  - To complete a forensics disk analysis and examination, you need to create a report
  - Subfunctions
    - Log reports
    - Report generator
  - Use this information when producing a final report for your investigation

Tool Comparisons

Table 7-1 Comparison of forensics tool functions

Function	ProDiscover Basic	AccessData Ultimate Toolkit	Guidance Software EnCase
Acquisition			
Physical data copy	√	√	√
Logical data copy	√	√	√
Data acquisition formats	√	√	√
Command-line process			√
GUI process	√	√	√
Remote acquisition			√*
Verification	√	√	√
Validation and discrimination			
Hashing	√	√**	√**
Filtering		√	√
Analyzing file headers		√	√
Extraction			
Data viewing	√	√***	√***
Keyword searching	√	√	√
Decompressing		√	√
Carving		√	√
Decrypting		√	
Bookmarking	√	√	√
Reconstruction			
Disk-to-disk copy	√	√	√
Image-to-disk copy	√	√	√
Partition-to-partition copy	√		√
Image-to-partition copy	√		√
Reporting			
Log reports		√	√
Report generator	√	√	

Other Considerations for Tools

- Considerations
  - Flexibility
  - Reliability
  - Expandability
  - Keep a library with older version of your tools
- Create a software library containing older versions of forensics utilities, OSs, and other programs

Computer Forensics Software Tools

- The following sections explore some options for command-line and GUI tools in both Windows and UNIX/Linux

Command-line Forensic Tools

- The first tools that analyzed and extracted data from floppy disks and hard disks were MS-DOS tools for IBM PC file systems
- Norton DiskEdit
  - One of the first MS-DOS tools used for computer investigations
- Advantage
  - Command-line tools require few system resources
    - Designed to run in minimal configurations

UNIX/Linux Forensic Tools

- *nix platforms have long been the primary command-line OSs
- SMART
  - Designed to be installed on numerous Linux versions
  - Can analyze a variety of file systems with SMART
  - Many plug-in utilities are included with SMART
  - Another useful option in SMART is its hex viewer

UNIX/Linux Forensic Tools (continued)

- Helix
  - One of the easiest suites to begin with
  - You can load it on a live Windows system
    - Loads as a bootable Linux OS from a cold boot
- Autopsy and SleuthKit
  - Sleuth Kit is a Linux forensics tool
  - Autopsy is the GUI/browser interface used to access Sleuth Kit's tools

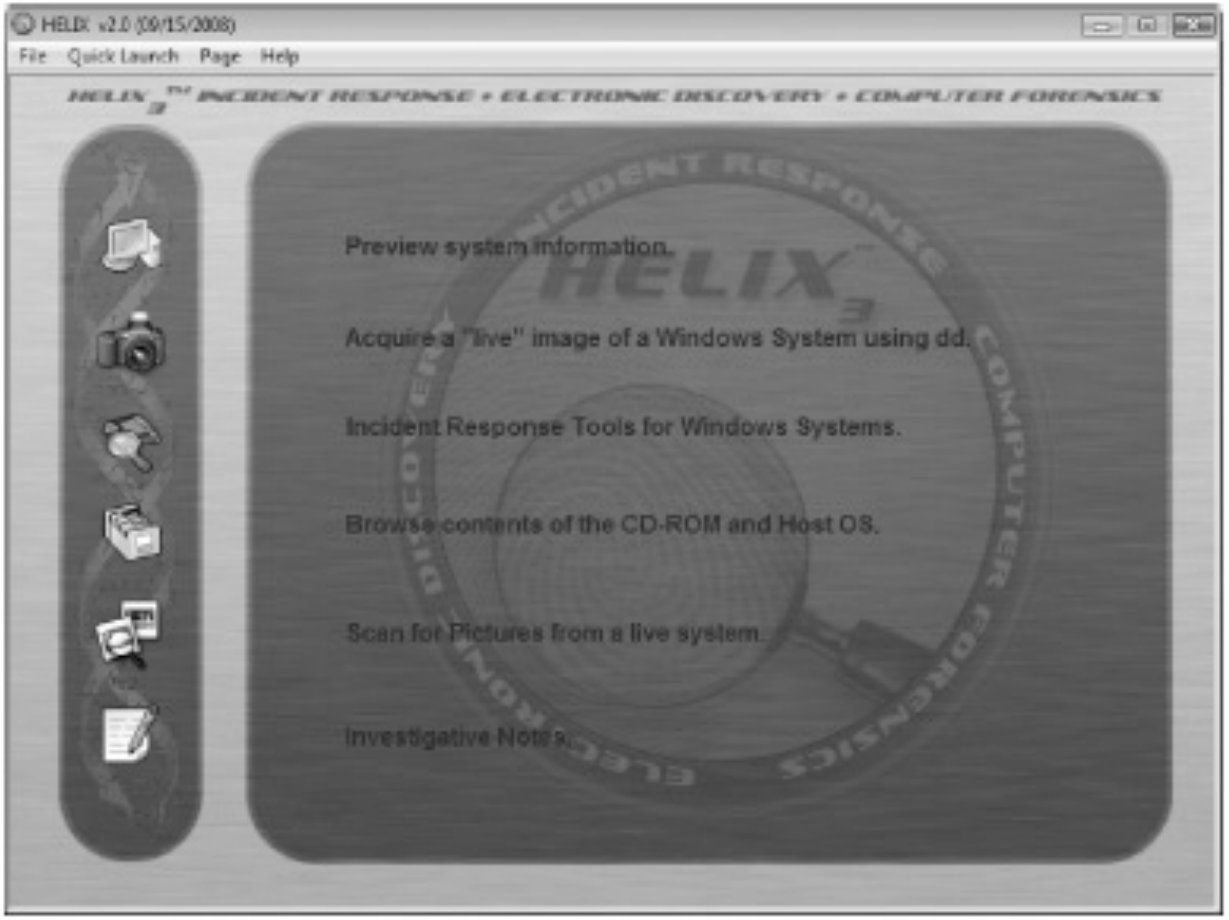

Figure 7-8 The Helix menu

UNIX/Linux Forensic Tools (continued)

- Knoppix-STD
  - Knoppix Security Tools Distribution (STD)
    - A collection of tools for configuring security measures, including computer and network forensics
  - Knoppix-STD is forensically sound
    - Doesn’t allow you to alter or damage the system you’re analyzing
  - Knoppix-STD is a Linux bootable CD

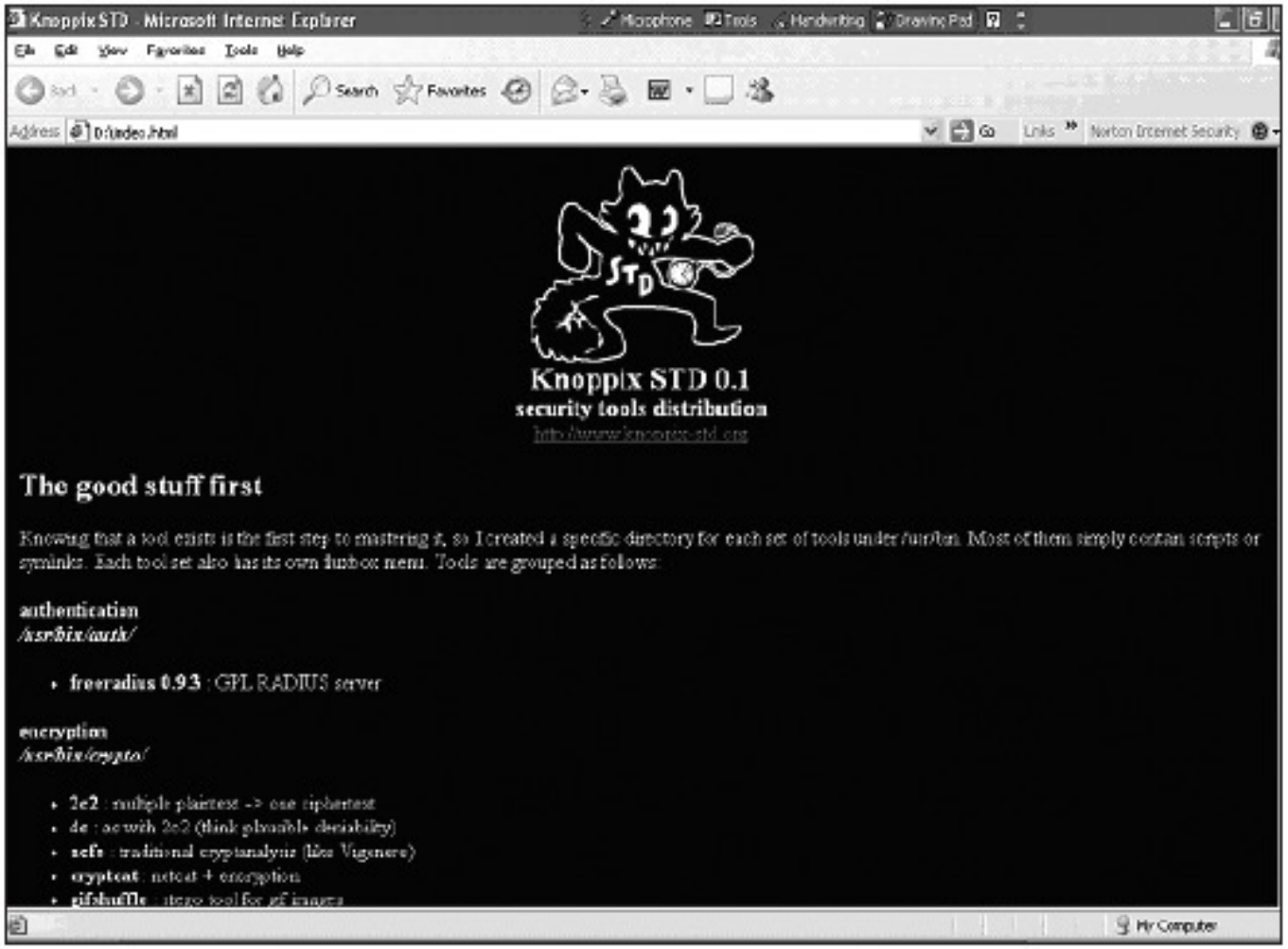

Figure 7-9 The Knoppix-STD information window in Windows

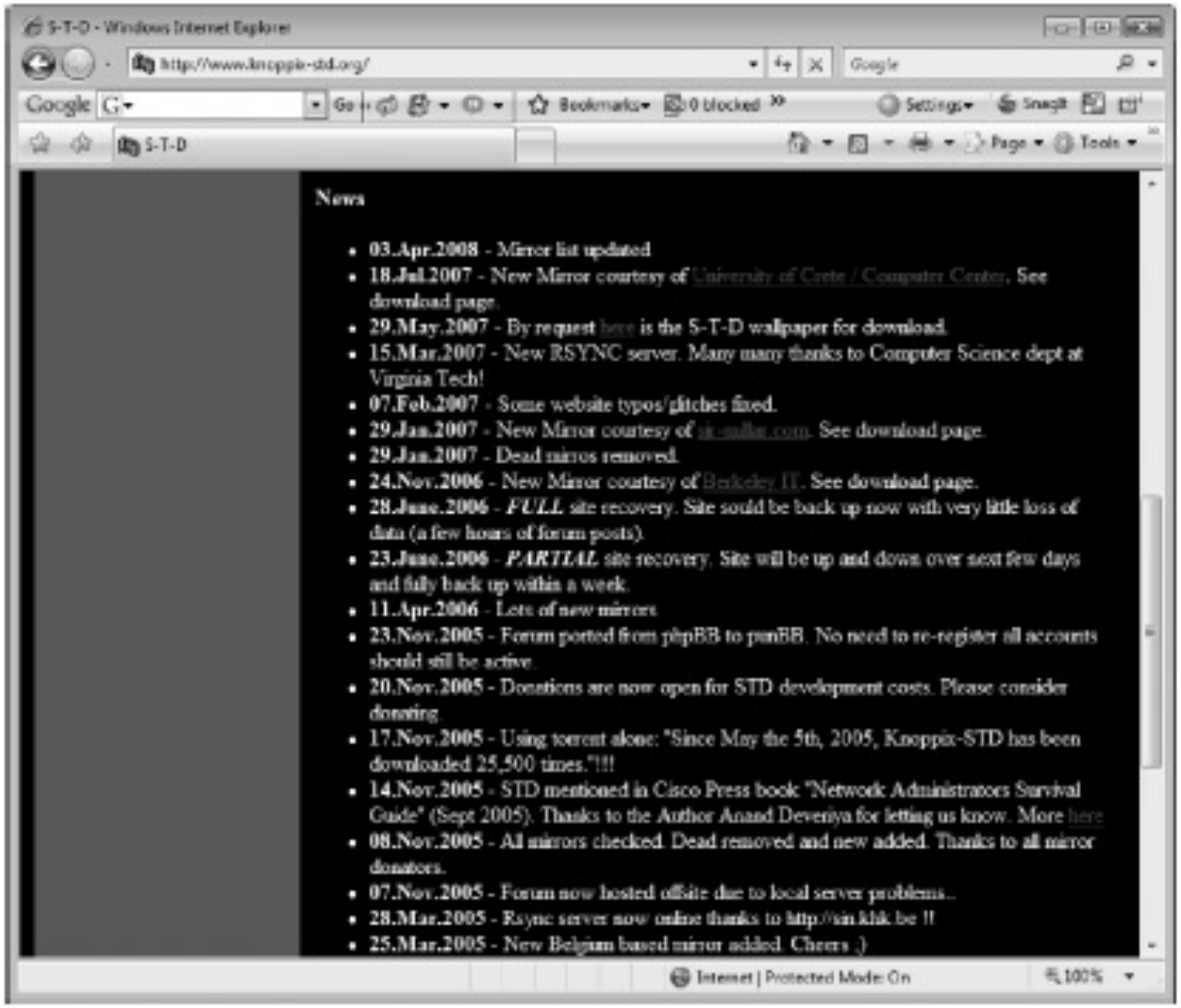

Figure 7-10 A list of forensics tools available in Knoppix-STD

Other GUI Forensic Tools

- Simplify computer forensics investigations
- Help training beginning investigators
- Most of them come into suites of tools
- Advantages
  - Ease of use
  - Multitasking
  - No need for learning older OSs

Other GUI Forensic Tools (continued)

- Disadvantages
  - Excessive resource requirements
  - Produce inconsistent results
  - Create tool dependencies

Computer Forensics Hardware Tools

- Technology changes rapidly
- Hardware eventually fails
  - Schedule equipment replacements
- When planning your budget consider:
  - Failures
  - Consultant and vendor fees
  - Anticipate equipment replacement

Forensic Workstations

- Carefully consider what you need
- Categories
  - Stationary
  - Portable
  - Lightweight
- Balance what you need and what your system can handle

Forensic Workstations (continued)

- Police agency labs
  - Need many options
  - Use several PC configurations
- Private corporation labs
  - Handle only system types used in the organization
- Keep a hardware library in addition to your software library

Forensic Workstations (continued)

- Not as difficult as it sounds
- Advantages
  - Customized to your needs
  - Save money
- Disadvantages
  - Hard to find support for problems
  - Can become expensive if careless
- Also need to identify what you intend to analyze

Forensic Workstations (continued)

- You can buy one from a vendor as an alternative
- Examples
  - F.R.E.D.
  - F.I.R.E. IDE
- Having vendor support can save you time and frustration when you have problems
- Can mix and match components to get the capabilities you need for your forensic workstation

Using a Write-Blocker

- **Write-blocker**
  - Prevents data writes to a hard disk
- Software-enabled blockers
  - Software write-blockers are OS dependant
  - Example: PDBlock from Digital Intelligence
- Hardware options
  - Ideal for GUI forensic tools
  - Act as a bridge between the suspect drive and the forensic workstation

Using a Write-Blocker (continued)

- Can navigate to the blocked drive with any application
- Discards the written data
  - For the OS the data copy is successful
- Connecting technologies
  - FireWire
  - USB 2.0
  - SCSI controllers

Recommendations for a Forensic Workstation

- Determine where data acquisitions will take place
- Data acquisition techniques
  - USB 2.0
  - FireWire
- Expansion devices requirements
- Power supply with battery backup
- Extra power and data cables

Recommendations for a Forensic Workstation (continued)

- External FireWire and USB 2.0 ports
- Assortment of drive adapter bridges
- Ergonomic considerations
  - Keyboard and mouse
  - A good video card with at least a 17-inch monitor
- High-end video card and monitor
- If you have a limited budget, one option for outfitting your lab is to use high-end game PCs

Validating and Testing Forensic Software

- Make sure the evidence you recover and analyze can be admitted in court
- Test and validate your software to prevent damaging the evidence

Using National Institute of Standards and Technology (NIST) Tools

- **Computer Forensics Tool Testing (CFTT)** program
  - Manages research on computer forensics tools
- NIST has created criteria for testing computer forensics tools based on:
  - Standard testing methods
  - ISO 17025 criteria for testing items that have no current standards
  - ISO 5725

Using National Institute of Standards and Technology (NIST) Tools (continued)

- Your lab must meet the following criteria
  - Establish categories for computer forensics tools
  - Identify computer forensics category requirements
  - Develop test assertions
  - Identify test cases
  - Establish a test method
  - Report test results
- Also evaluates drive-imaging tools using
  - Forensic Software Testing Support Tools (FS-TST)

Using National Institute of Standards and Technology (NIST) Tools (continued)

- **National Software Reference Library (NSRL)** project
  - Collects all known hash values for commercial software applications and OS files
    - Uses SHA-1 to generate a known set of digital signatures called the Reference Data Set (RDS)
  - Helps filtering known information
  - Can use RDS to locate and identify known bad files

Using Validation Protocols

- Always verify your results
- Use at least two tools
  - Retrieving and examination
  - Verification
- Understand how tools work
- One way to compare results and verify a new tool is by using a disk editor
  - Such as Hex Workshop or WinHex

Using Validation Protocols (continued)

- Disk editors
  - Do not have a flashy interface
  - Reliable tools
  - Can access raw data
- Computer Forensics Examination Protocol
  - Perform the investigation with a GUI tool
  - Verify your results with a disk editor
  - Compare hash values obtained with both tools

Using Validation Protocols (continued)

- Computer Forensics Tool Upgrade Protocol
  - Test
    - New releases
    - OS patches and upgrades
  - If you find a problem, report it to forensics tool vendor
    - Do not use the forensics tool until the problem has been fixed
  - Use a test hard disk for validation purposes
  - Check the Web for new editions, updates, patches, and validation tests for your tools

Summary

- Create a business plan to get the best hardware and software
- Computer forensics tools functions
  - Acquisition
  - Validation and discrimination
  - Extraction
  - Reconstruction
  - Reporting
- Maintain a software library on your lab

Summary (continued)

- Computer Forensics tools types
  - Software
  - Hardware
- Forensics software
  - Command-line
  - GUI
- Forensics hardware
  - Customized equipment
  - Commercial options
  - Include workstations and write-blockers

Summary (continued)

- Tools that run in Windows and other GUI environments don’t require the same level of computing expertise as command-line tools
- Always test your forensics tools