

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

Evaluating Computer Forensics Tool Needs

- Look for versatility, flexibility, and robustness
 - OS
 - File system(s)
 - Script capabilities
 - Automated features
 - Vendor's reputation for support
- 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



Logicube Talon
(link Ch 7a)

Tasks Performed by Computer Forensics Tools

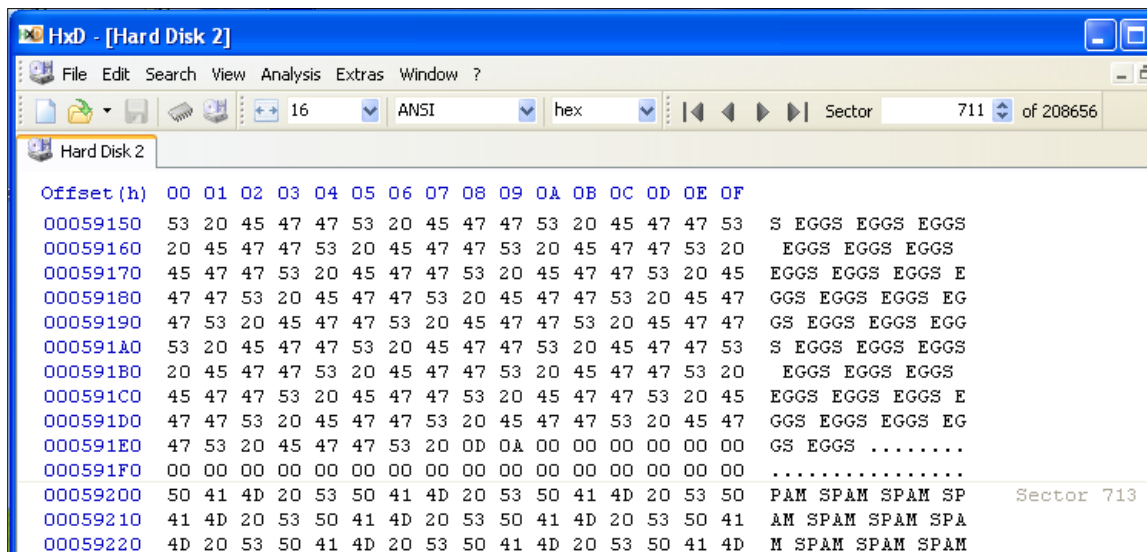
- Five major categories:
 - Acquisition
 - Validation and discrimination
 - Extraction
 - Reconstruction
 - Reporting

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

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



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

Validation and discrimination

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

Validation and discrimination (continued)

- Subfunctions
 - Hashing
 - CRC-32, MD5, Secure Hash Algorithms
 - Filtering
 - Known system files can be ignored
 - 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)

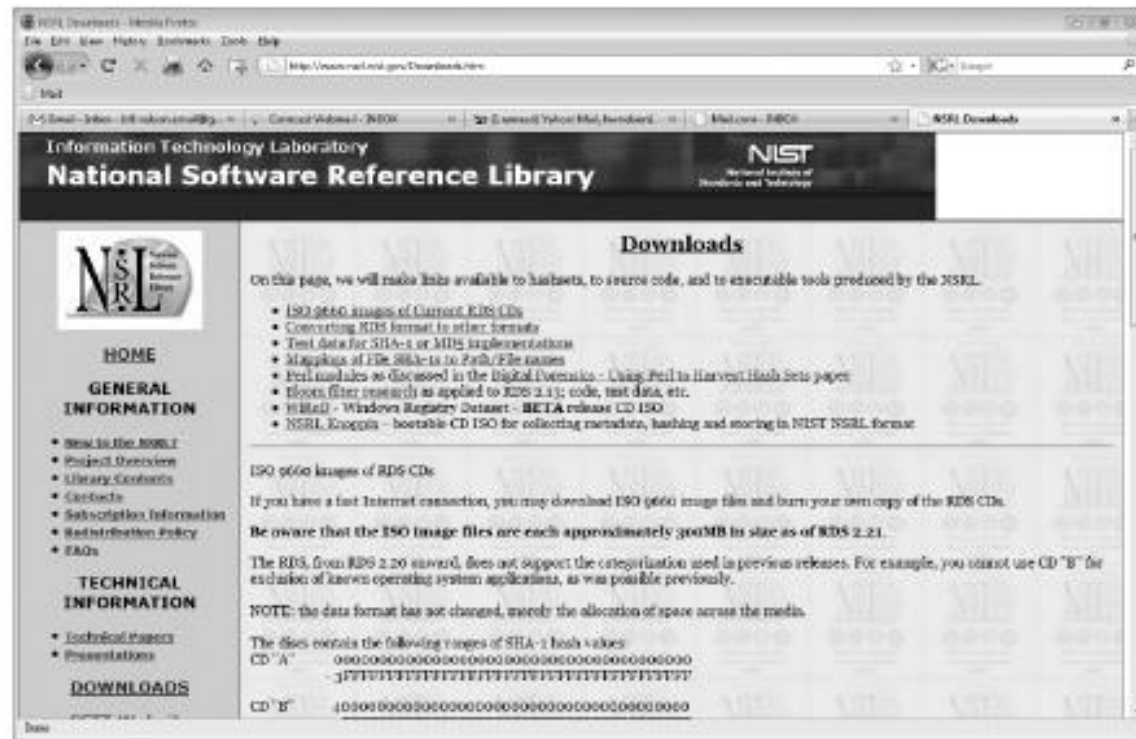


Figure 7-2 The download page of the National Software Reference Library

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

Indicates a .jpeg file

The screenshot shows the WinHex application window with Drive K selected. The file list on the left includes 'ForensicData.doc.jpg'. The main pane displays a hex dump of the file's content. The first few bytes of the hex dump are: FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 60. These bytes correspond to the JPEG file signature (FF D8) followed by the JFIF marker (FF E0) and the JFIF header (00 00 10 4A 46 49 46 00 01 01 01 00 60). The text 'JFIF' is highlighted in the hex dump, and an arrow points from the text 'Indicates a .jpeg file' to this highlight.

Name	Ext.	Size	Created	Modified	Accessed	Attr.	File sector
EF6.txt	txt	56 B	01/22/2009 12:55:17	01/22/2009 12:15:52	01/24/2009 10:48:59	A	75275
EF7.txt	txt	59 B	01/22/2009 12:55:17	01/22/2009 12:16:20	01/24/2009 10:48:59	A	75277
desktop.ini	ini	0 B	01/21/2009 12:41:45	04/28/2008 12:22:51	01/21/2009 12:41:45	A	
Eiffel Tower Google.kmz	kmz	0.6 KB	01/21/2009 12:41:45	04/28/2008 12:09:50	01/22/2009 12:54:23	A	107372
ForensicData.doc.jpg	jpg	47.8 KB	01/28/2009 19:31:37	01/28/2009 19:31:37	01/28/2009 19:31:37	A	122250
Yahoo! Briefcase.url	url	206 B	01/21/2009 12:41:45	04/28/2008 12:09:50	01/24/2009 19:12:57	A	75279

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Hex	ASCII
03AB7400	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	60	FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 60	JFIF
03AB7410	00	00	00	00	FF	DB	00	43	00	08	06	06	07	06	05	08	00 00 00 00 FF DB 00 43 00 08 06 06 07 06 05 08	
03AB7420	07	07	07	09	09	08	0A	0C	14	0D	0C	0B	0B	0C	19	12	07 07 07 09 09 08 0A 0C 14 0D 0C 0B 0B 0C 19 12	
03AB7430	13	0F	14	1D	1A	1F	1E	1D	1A	1C	1C	20	24	2E	27	20	13 0F 14 1D 1A 1F 1E 1D 1A 1C 1C 20 24 2E 27 20	
03AB7440	22	2C	23	1C	1C	28	37	29	2C	30	31	34	34	34	1F	27	22 2C 23 1C 1C 28 37 29 2C 30 31 34 34 34 1F 27	
03AB7450	39	3D	38	32	3C	2E	33	34	32	FF	DB	00	43	01	09	09	39 3D 38 32 3C 2E 33 34 32 FF DB 00 43 01 09 09	
03AB7460	09	0C	0B	0C	18	0D	0D	18	32	21	1C	21	32	32	32	32	09 0C 0B 0C 18 0D 0D 18 32 21 1C 21 32 32 32 32	
03AB7470	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32 32 32 32 32 32 32 32 32 32 32 32 32 32	
03AB7480	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32 32 32 32 32 32 32 32 32 32 32 32 32 32	
03AB7490	32	32	32	32	32	32	32	32	32	32	32	32	32	32	FF	C0	32 32 32 32 32 32 32 32 32 32 32 32 FF C0	
03AB74A0	00	11	08	02	58	03	80	03	01	22	00	02	11	01	03	11	00 11 08 02 58 03 80 03 01 22 00 02 11 01 03 11	
03AB74B0	01	FF	C4	00	1F	00	00	01	05	01	01	01	01	01	01	00	01 FF C4 00 1F 00 00 01 05 01 01 01 01 01 01 00	
03AB74C0	00	00	00	00	00	00	00	01	02	03	04	05	06	07	08	09	00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09	
03AB74D0	0A	0B	FF	C4	00	B5	10	00	02	01	03	03	02	04	03	05	0A 0B FF C4 00 B5 10 00 02 01 03 03 02 04 03 05	
03AB74E0	05	04	04	00	00	01	7D	01	02	03	00	04	11	05	12	21	05 04 04 00 00 01 7D 01 02 03 00 04 11 05 12 21	
03AB74F0	31	41	06	13	51	61	07	22	71	14	32	81	91	A1	08	23	31 41 06 13 51 61 07 22 71 14 32 81 91 A1 08 23	
03AB7500	42	B1	C1	15	52	D1	F0	24	33	62	72	82	09	0A	16	17	42 B1 C1 15 52 D1 F0 24 33 62 72 82 09 0A 16 17	
03AB7510	18	19	1A	25	26	27	28	29	2A	34	35	36	37	38	39	3A	18 19 1A 25 26 27 28 29 2A 34 35 36 37 38 39 3A	
03AB7520	43	44	45	46	47	48	49	4A	53	54	55	56	57	58	59	5A	43 44 45 46 47 48 49 4A 53 54 55 56 57 58 59 5A	

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

Tasks Performed by Computer Forensics Tools (continued)

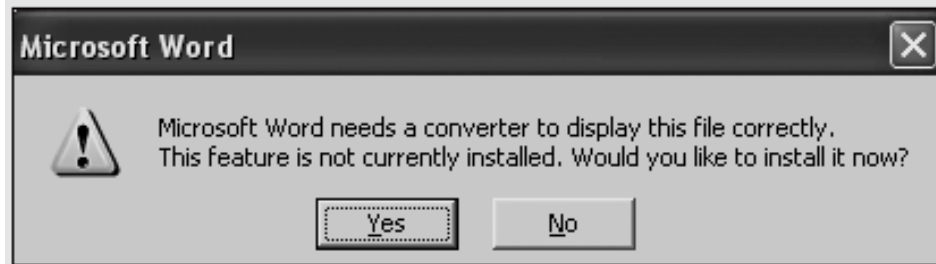


Figure 7-4 Error message displayed when trying to open a JPEG file in Word



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

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

Extraction (continued)

- Subfunctions
 - Data viewing
 - Keyword searching
 - Decompressing
 - Carving (reconstructing file fragments)
 - Decrypting
 - Bookmarking
- **Keyword search** speeds up analysis for investigators

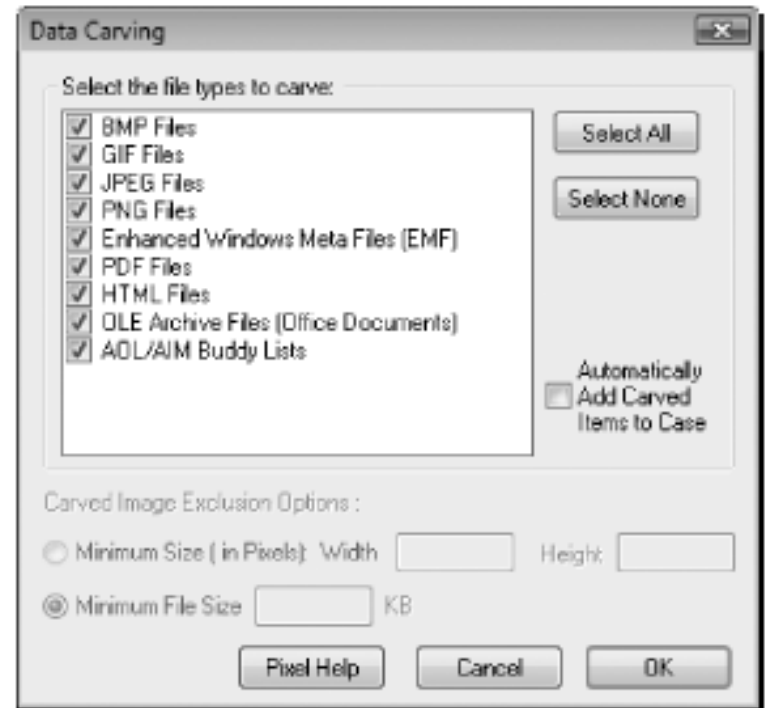
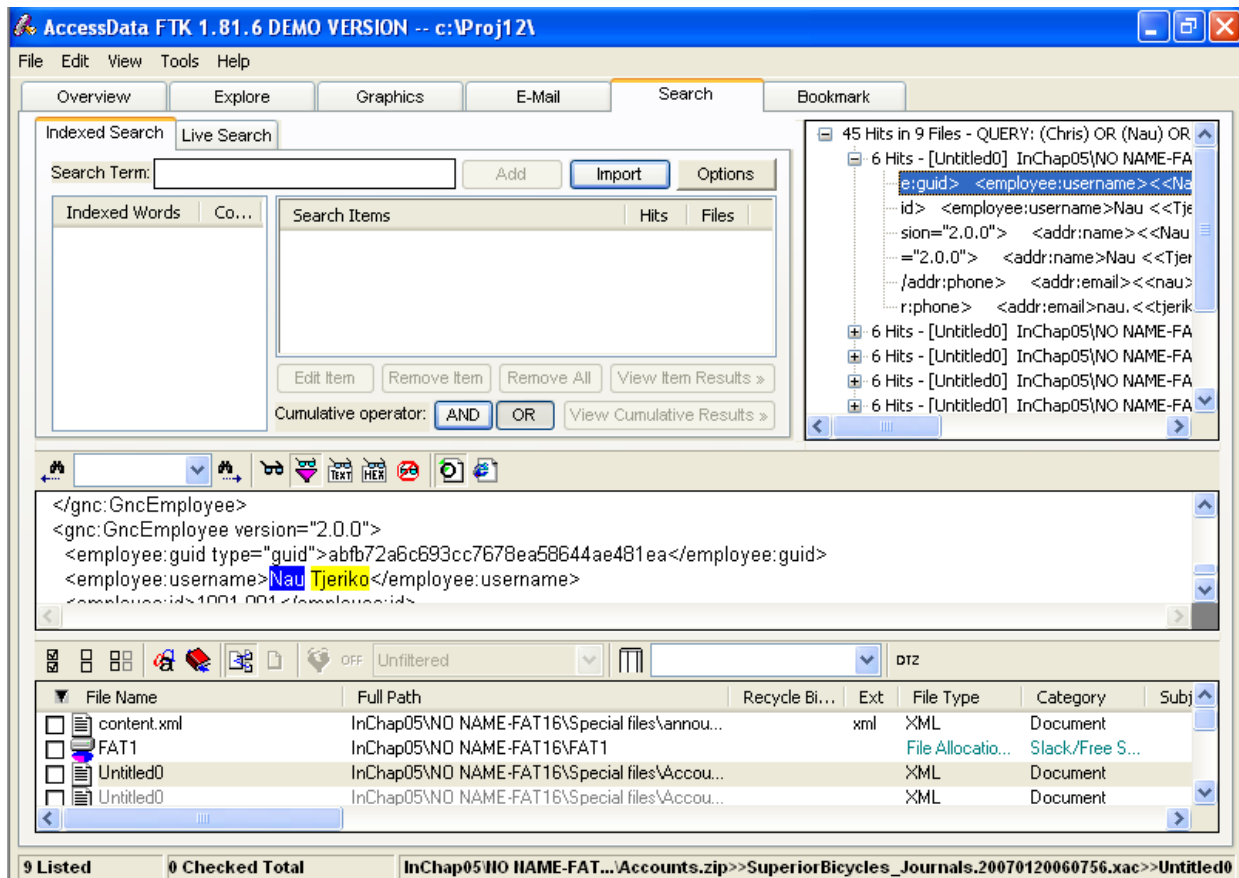


Figure 7-7 Data-carving options in FTK

FTK's Search Pane



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**

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
- This is easiest if a matching blank hard disk is available, same make and model

Reconstruction (continued)

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


VOOM Shadow 2

- For write-blocked courtroom demos using real original drive, use Voom Shadow 2 (link Ch 7b)

A black, rectangular hardware device with a front panel. The top of the panel features the text 'VOOM Technologies, Inc.' and 'SHADOW 2'. Below this, there are four indicator lights: a green light labeled 'PWR', a yellow light labeled 'LOCK', a red light labeled 'HDD', and a small green light labeled 'PWR'. At the bottom of the front panel, there is a small label that reads 'To Activate & Enable Function Press Button 3 Times & Repeat Subsequent'. The device has a standard 3.5-inch floppy disk drive on the left side and a USB port on the right side.

[previous](#) | [up](#) | [next](#)

VOOM Shadow 2

 [E-mail this product to a friend](#)

The Shadow 2 provides read/write access from the host computer's perspective, while maintaining the original HDD unchanged and forensically sound. The Shadow redirects all writes to its internal drive, at the host-to-drive interface level. Clear ('zero') the Shadow's drive at anytime and begin a clean investigation of the suspect computer within seconds.

Simply connect the Shadow and turn it on, after a few seconds (green light) boot the suspect computer. Operate the suspect computer in the same fashion as any user would. The Shadow ensures the suspect computer never receives a write and remains forensically sound. Since the Shadow only writes to its own internal drive, when it is removed the suspect computer remains in this pristine, unaltered state.

VOOM Shadow 2
SKU:
Price: **\$1,600.00**

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

Computer Forensics Software Tools

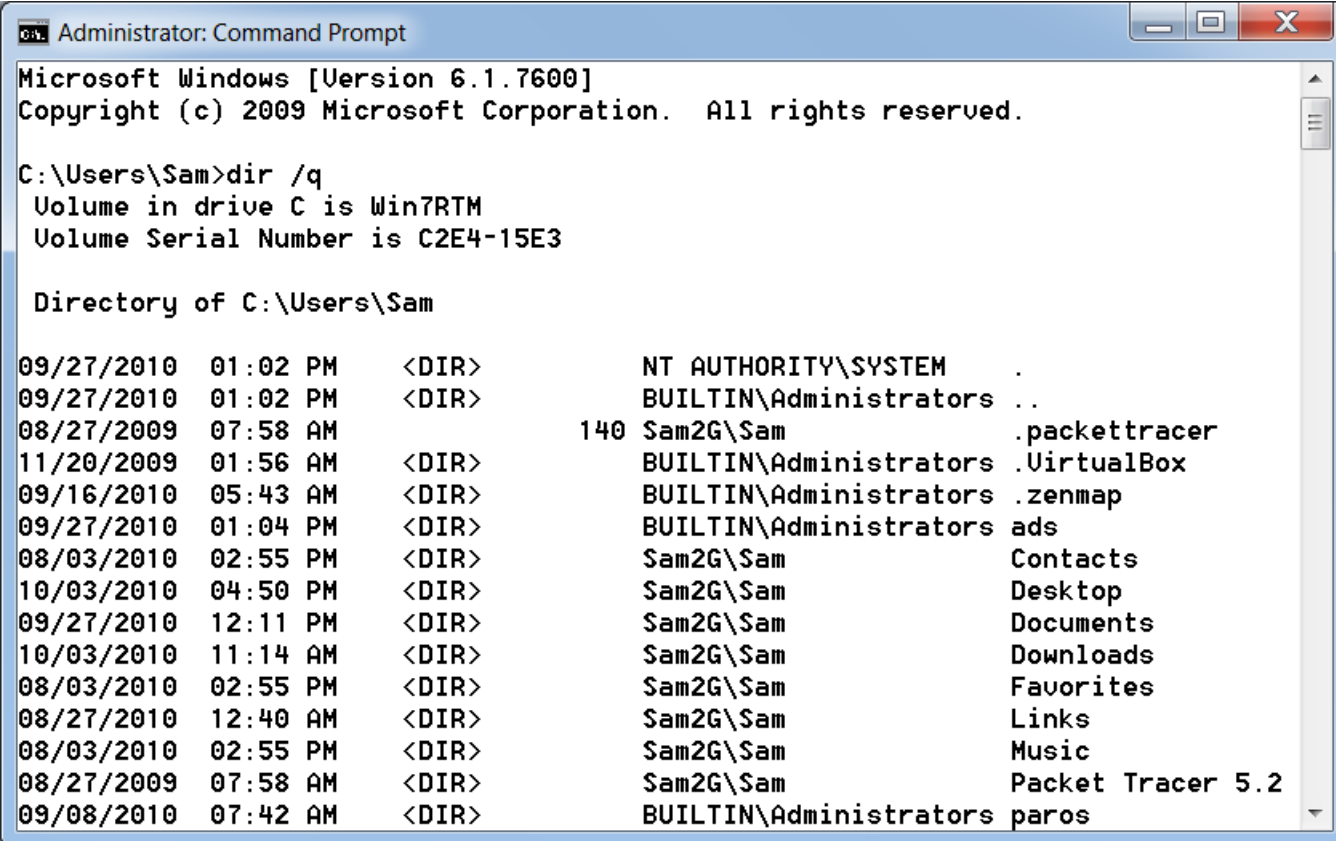
- The following sections explore some options for command-line and GUI tools in both Windows and UNIX/Linux

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

DIR /Q

- Shows file owner



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Sam>dir /q
Volume in drive C is Win7RTM
Volume Serial Number is C2E4-15E3

Directory of C:\Users\Sam

09/27/2010  01:02 PM    <DIR>          NT AUTHORITY\SYSTEM      .
09/27/2010  01:02 PM    <DIR>          BUILTIN\Administrators  ..
08/27/2009  07:58 AM      140 Sam2G\Sam             .packettracer
11/20/2009  01:56 AM    <DIR>          BUILTIN\Administrators  .VirtualBox
09/16/2010  05:43 AM    <DIR>          BUILTIN\Administrators  .zenmap
09/27/2010  01:04 PM    <DIR>          BUILTIN\Administrators  ads
08/03/2010  02:55 PM    <DIR>          Sam2G\Sam                Contacts
10/03/2010  04:50 PM    <DIR>          Sam2G\Sam                Desktop
09/27/2010  12:11 PM    <DIR>          Sam2G\Sam                Documents
10/03/2010  11:14 AM    <DIR>          Sam2G\Sam                Downloads
08/03/2010  02:55 PM    <DIR>          Sam2G\Sam                Favorites
08/27/2010  12:40 AM    <DIR>          Sam2G\Sam                Links
08/03/2010  02:55 PM    <DIR>          Sam2G\Sam                Music
08/27/2009  07:58 AM    <DIR>          Sam2G\Sam                Packet Tracer 5.2
09/08/2010  07:42 AM    <DIR>          BUILTIN\Administrators  paros
```

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
 - Link Ch 7d

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

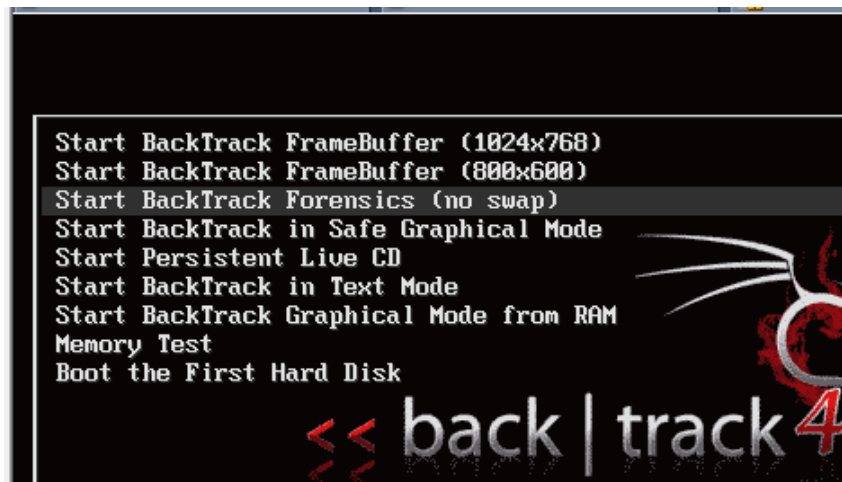


Figure 7-8 The Helix menu

UNIX/Linux Forensic Tools (continued)

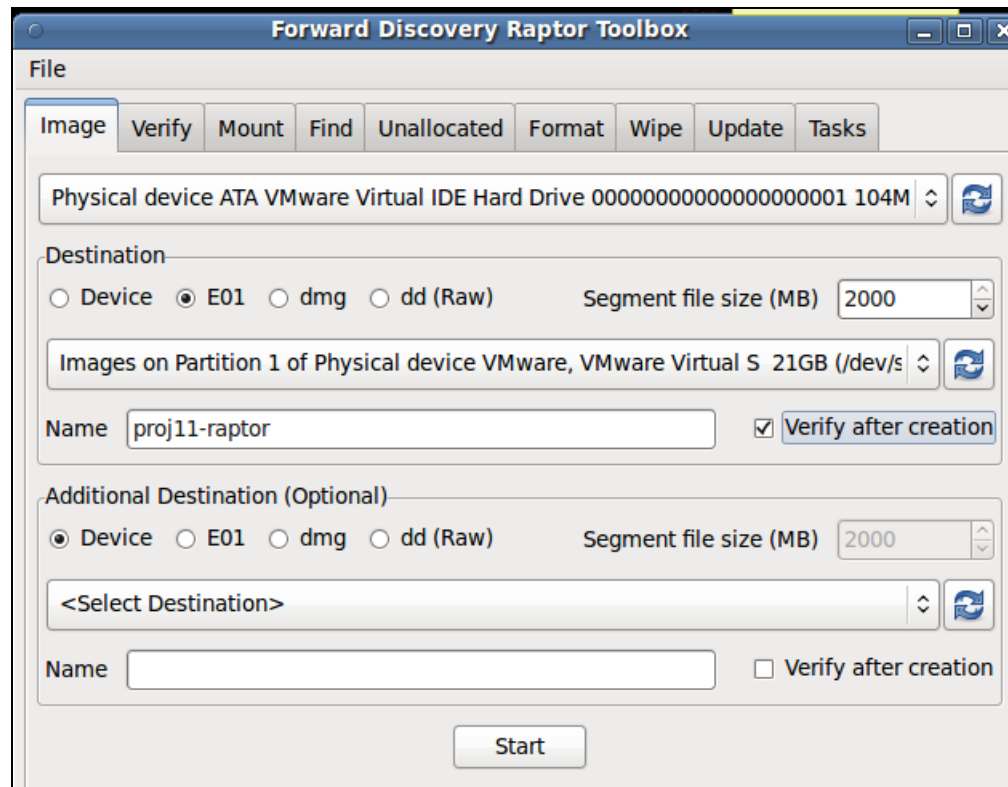
- Knoppix-STD
 - Knoppix Security Tools Distribution (STD)
 - A collection of tools for configuring security measures, including computer and network forensics
 - Knoppix-STD is forensically sound
 - Doesn't allow you to alter or damage the system you're analyzing
 - Knoppix-STD is a Linux bootable CD

BackTrack



- BackTrack 4 has a Forensics Mode
- But it's not the default boot mode, so you need to be careful

Raptor



- Forensic LiveCD (link Ch 7e)

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

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

Building your Own Forensic Workstation

- 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

Purchasing a Forensic Workstation

- 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
 - DOS only, not Windows (link Ch 6f)
- 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

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
 - See link Ch 7g

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
 - But it won't work with encrypted or compressed files

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
 - Usually FTK or EnCase
 - Verify your results with a disk editor
 - If a file is recovered, 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