#### 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

#### 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

10日間部時に 20日	a a a 🔅	1.		15	ž d	1	-	-12	4	Þ	3	9	0	101 J	ρ	₩ 4	▶白田	0
Drive K:																		
Documents and Settings\Chris\My Docu	ments					1 min	890										23 fik	w.2d
lane ~	Ed. Sec		Creat	ed		M	odifie	d .		Ac	cesso	bd		10	r.	1st sector		
Ben_Franklin_11.txt	bit	90 B	01/2	1/2008	12.55	2001	/21/3	2009	12:55:2	0 01.	122/2	600	13:00	52 IA		105560	1	
Bon_Franklin_22_2.doc	dec 5	5.0 KB	01/24	1/2009	20:02:	24 01	/24/2	6009	20:02:2	8 01.	/24/2	009 :	20:02	28 IA		124858		
Ben_Frenklin_22_2rtf	r# 4	8.2 KB	01/22	2/2009	13:00	57/01	m	2009	12:57:3	1 01.	24/2	600	10:48	-59 A		149942		- 1
Ben Franklin 22 2rtf stream2		4.3 KB	01/22	2/2009	13:00:	57 01	/22/2	2009	12:57:3	1 01.	/24/2	600	10:48	59 (A)	05)	52527		
Ben Franklin 22 3rtf	18 4	4.3 KB	01/22	2/2009	13:00	57 01	/21/2	2009	13:29:2	9 01.	24/2	009	10:48	59 A		150546		
Ben1.tat	tet .	84 B	01/21	/2009	12:54	10 01	/21/2	2009	12.54.1	0.01.	/21/2	009	12:54	10 IA		109978		
Ben2/f	12	1.4 KB	01/21	/2009	13:02	12 01	/21/2	2009	13:02:1	2.01	/21/2	9009	13:02	1214		87317		
Ben22/tf									13.04.4							87320		
BF1 214	14								18 02 4					59 A		75279		
BF1 2tst hidden	-								18:02.4					:59 (A)	151	41519		
In Grannan							-			-			-0			-		10
[unregistrient]	Offset	0	-	2	3 4	5	6	7	8	9	h.	В	C	DE			31	*
Drive K: 7% free	03CF7400				50 A1			E1						0 00			±	
File system: NTFS	03CF7410	0.0			00 00		00	00						TF 09			;þÿ	
/olume label: NTFS1	03CF7420			~ ~ ~	00 00	~~~		00	~~ ~					0 00				
	03CF7430	6E			00 00			αo						0 00				
Default Edit Mode	03CE7440				00 FE		FF	FF						0 00		b	777	
State: original	03CF7450				E PB		FF	F.F.						E FF	3.E	37779	7777777777 <u>7</u> 7	
0 Indo level	03CF7460	FF	58	FF F	7F F7	FF	FF	55	FF	FF	F7 8	F F	ΈF	77 FE	. FE	225522	*****	
Jindo revenas: n/a	03CF7470	FF			E FF			FF							YF	33333	*****	
prido revensos. Inva	03CF7480	FF			E FF		FF	55		FF I	FF I			T FF		77777	******	
Noc. of visible drive space:	03CE7490	FF			FF FF		FF	हह						T FE			<del>7777777777777</del>	
teoc. of visible drive space:	03CF74A0				F FF			FF						F FF		377777	777777777777	
Duster No.: 124858	03CF74B0	FF			E FF	FF	FF	FF						T FE		77777	******	
Ben_Franklin_22_2.doc	03CF74C0	FF			E FF		EE	FE			FF B			E FF	38	33333	****	
Documents and S\My Documents\	0 3CF74D0	FF	- FF	FF F	(F 62	$\mathbf{FF}$	FF	55	FF	FF I	F7 I	TF F		77 FE	75	333333	******	
Snapehottaken Omin. ago	03CF74E0	FF			E FE	FF	FF	탄문			FF 8			E FF		99999	****	
	0.0CF74F0	FF	25	FF F	7F F7	FF	FF	88	FF I	FF I	F7 I	F F	ΈF	7 FF	77	77777	******	
Physical sector No.: 574741	03CF7500	FF	. F.F.	FF F	F FF	FF	FF	<u>सिंह</u>	FF I	FF I	FF F			T FF	. FF	37797	<del>77777777777777</del>	_
logical sector No : 124858	03CF7510	FF	55	FF B	FF FF	FF	FF	55	FF I	FF I	FF 8	FF F	FF	TF FF	FF	777777	7777777777777	L
	03CF7520	FF	' FF	FF B	E FF	FF	FF	FF	FF I	FF I	FF I	EF E	ΈF	T FE	TF	37777	77777777777	
Jeed space: 102 MB	03CF7530	FF	FF	FF B	E FF	FF	FF	55	FF I	FF 1	FF B	F F	ΈF	W FF	35	77777	777777777777	
106,824,192 bytes	03CF7540	FF	58	FF F	F FF	$\mathbf{FF}$	EE	55	FF	FF I	F7 I	TF F	ΈF	77 FF	75	33333	******	
the space: 7.9 MB	03CF7550	FF	FF	FF F	E FF	FF	FF	FB		FF I	FF F	EF F	FF	F FF	75	999999	7777777777777	
8,296,960 bytes	03CF7560		78	FF F	(F 177	FF	FF	F7	FF I	FF I	FF 1	F F	FF	7 FF	77	77777	777777777777777777777777777777777777777	
	03CF7570	FF	FF	FF B	F FF	FF	FF	FF	FF I	FF I	FF B	EF B	FF	T FF	FF	77777	77777777777	
Total capacity: 110 MB	03CF7580	FF	FF	FF B	FF FF	$\mathbf{FF}$	FF	55	FF I	FF I	FF B	F F	ΈF F	W FF	FF	77777	777777777777	
115,121,152 bytes	03CF7590	FF	' FF	FF B	E FF	FF	FF	FF	FF I	FF 1	FF I	EF B	ΈĒ	T FE	FF	37599	******	
	03CF75A0	FF	FF	FF B	E FF	FF	FF	FF	FF I	FF I	FF 3	F F	Έ F	W FF	38	77777	77777777777	
lytes per cluster: 512	0.0CF75B0	FF	FF	FF 8	F FF	FF	FF	FF	FF I	EF 1	FF I	E B	ΈĘ	T FF	TE		37777777777	
free clusters: 16,205	03CF75C0	FF	वर	FF F	E FF	FF	FF	सम	FF	FF I	FF B	म म	F F	F FF	7F		77777777777	
Total clusters: 224,846	09CF75D0	FF	58	FF F	0F F7	FF	FF	88	FF I	FF 1	FF 1	F F	ΈF	7 FF	TE	33333	37777777777	
Evice per sector: 512	0 3CF75E0	FF	FF	FF B	F FF	FF	FF	FF	FF	FF I	77 8	FF F	ŦF	T FE	TE		77777777777777	
Sector count: 224,845	00CF75F0	FF	28	FF F	F FF			88	FF	FF I	77 1	FF	FF	T FF	78		*****	
ALT/010																		

Figure 7-1 Viewing data in a 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
      - 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

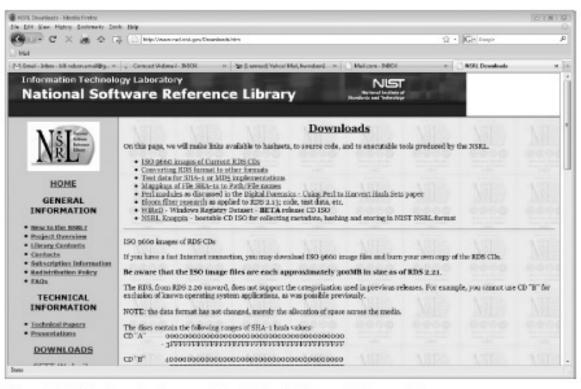


Figure 7-2 The download page of the National Software Reference Library

- 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

						Ir	ndica	tes	a.jp	eg	file	э						
WinHex - [Drive Ki]										1	5						152	- 142
Ge File Edit Search P	osition	View Tools	Special	et Or	tion	. W	indow	Hel	0	)								0
		1 13 In 12		10 2			1 -			+	1	e1 12	h d	3 n	. (	5 1	杀▲▶□圆	
Dive K:		1 M2 315	9.4	HER TH	0.00		1.000		1 4	*		1	0.4	-	- /	-	20 4 7 20 20	
													1					-
Documents and Settings/Chris	My Docu	7 1				0 m	n. 890			-	1		1	-	-		24 fie	15. Z
Name +		Et. Site		caled	_	_	Modif				00005		_	1	Ab		Tst sector	
BF6.bet		bé	56 B 01							_					×.		75275	
BF7.bd		bit	59 B 01	/22/20	09 12	255(1)	7 01/22	/2009	12:16	20 0	1/24/	2009	105	48.12	A B	. 7	75277	
] desktop ini		ini	080	/21/20	09 12	541.98	5 04/28	/2008	12:22	51.0	1/21	2003	125	41:42	5.A			
Effel Tower Google.kmz		kmz 0	6 KB 01	/21/20	19 12	641.48	6 04/28	/2008	12:09	50 0	1/22)	2009	12:	54.2	A.E	V	07372	
Forenec Data doc.jpg		pg 47	a KB DI	/28/20	19 19	131 31	01/23	/2003	15:31	550	1/28	2006	112	31 3	14		2350	
Yahool Biefcase url		url	206 B 01	/21/20	09 12	641.48	5 64/28	/2008	12:09	50.0	1/24/	2009	11:	125	7.A.	1	7523	
		Offeet	D	1 2	3	4	5 6	5 7	8	9	A	В	C	D	Ε	F	× 1461	
	gistriert] 7% free	D3AE7400	FF I	18 FF	χŋ	00	10.43	4.6	49	4.6	00	01	D1	01	0.0	60	Boya. JFIF	
Ale cystem:	NTES	D3AE7410		50 CO	DD	FF	DB 00		00	DB	06	06	07		05		WD.C	
	NTPS1	D3AE7420	07 0	17 07	D9	0.9	08 04	00	14	0D	0C	0B	DB	0C	19	12		
COLUMN TELEVIT.	anar	D3AE7430	13 (	F 14	1.D	1.4	1F 18	10	1.1.	10	10	20	24	2E	27	20	5.	
Default Edit Mode		D3AE7440	22 2	C 23	1C	10	28 37	29	ZC	30	31	34	34	34	1F	27	*.#. (71.01444	1
	orginal	D3AE7450	39 3	3D 38	32	3C	2E 33	3 3 4	3.2	FF	DB	00	43	01	0.9	09	9=82<.34200.C.	
		D3AE7460	09 0	C OB	DC	18	0D 00	18	32	21	10	21	32	32	3.2	32		22
Undo level:	0	D3AE7470	32 3	12 32	32	32	32 32	32	32	32	32	32	32	32	32	32	222222222222222222	22
Undo reverses:	n/a	D3AE7400	32 3	12 32	32	32	32 32	32	32	32	32	32	32	32	32	32	2222222222222222	22
		D3AE7490	32 3	32 32	32	32	32 32	32	32	32	32	32	32	32	FF	CD	222222222222222222	4k
Alloc. of visible drive space:		D3AE74A0	DD 3	1 08	D2	58	03 80	0 03	01	22	00	02	11	01	03	11		
Cluster No.:	120250	D3AE74E0	01 H	F C4	DD	1F	00 00	01	05	01	01	01	D1	01	01	00	.ÿĂ	
ForeneicData		D3AE74C0	00 0	00 00	DD	0.0	00.00	0 1	0.2	03	0.4	05	06	07	0.0	09		
Documents and S., Wy Docu		D3AE74D0	DA 0	B FF	C4	00	B5 10	0 00	0.2	01	03	63	D2	04	03	05		
		D3AE74E0	05 0	4 04	DD	0.0	01 71	01	0.2	03	0.0	0.4	11	05	12	21		.1
Snapshot taken 0 m	én, ago	03AE74F0	31 4	11 06	13	51	61 03	22	71	14	32	81	91	$^{h1}$	0.8	23	1AQs."q.2.'i	.1
Physical sector No.:	570133	D3AE7500	42.1	11 C1	15	52	Di FO	24	33	62	72	82	0.9	0Å	16	17	Etá. RÝð\$3br1.	
Logical sector No.:	120250	D3AE7510	18 1	19 1Å	25	26	27 28	29	24	34	35	36	37	38	39	36		19 :
		D3AE7520	43 4	4 45	4.6	47	48 49	4.4	53	54	55	56	57	58	59	54	CDEFGEIJSTUWW	
	IN2 MR																	
Sector 120250 of 224846		Offset:	348	7400				255	Bock:							n/a	Size	n

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

Microsof	t Word
	Microsoft Word needs a converter to display this file correctly. This feature is not currently installed. Would you like to install it now?
	<u>Y</u> es <u>N</u> o

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
    - Decrypting
    - Bookmarking

- Keyword search speeds up analysis for investigators

Overview	Explore	1	Graphics	E-Mail	Sea	rch	Bookmark				
indexed Search	Live Search	1			10 - 10 M	_					
Search Term			1	Add	port	Optiona	1				
Indexed Word	s Co	Search Ite	ims		Hits	Files					
		Ben w/1	ranklin		12	6					
		Son			300	6					
		*******									
		Cumulati	ve Results (us	ing AND)	16	3					
		Edit bem	Remove the	m Remove Al	View Item	Results »					
		Cumulative	operator: AN		Cumulation	e Resulta »					
*	- 1. 3	* 全型	10 C 16	Ð							
•											
•											
•											
		)   <b>Q</b> ==	Unfiltered	*		lolumns		• orz	2		>
		and the second se	Unfiltered	+			cleBi Đ	2	: ile Type	Category	+

Figure 7-6 The Indexed Search feature in FTK

Data Carving	×
Select the file types to carve: BMP Files GIF Files PNG Files PNG Files Files Finhanced Windows Meta Files (EMF) PDF Files HTML Files CLE Archive Files (Office Documents)	Select All Select None
<ul> <li>OLE Archive Files (Office Documents)</li> <li>AOL/AIM Buddy Lists</li> </ul>	Automatically Add Carved Items to Case
Carved Image Exclusion Options :	
O Minimum Size ( in Pixels): Width	Height
Minimum File Size     KB	
Pixel Help Cancel	ОК

Figure 7-7 Data-carving options in FTK

- 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

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

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

Table 7-1 Comparison of forensics tool functions

## 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

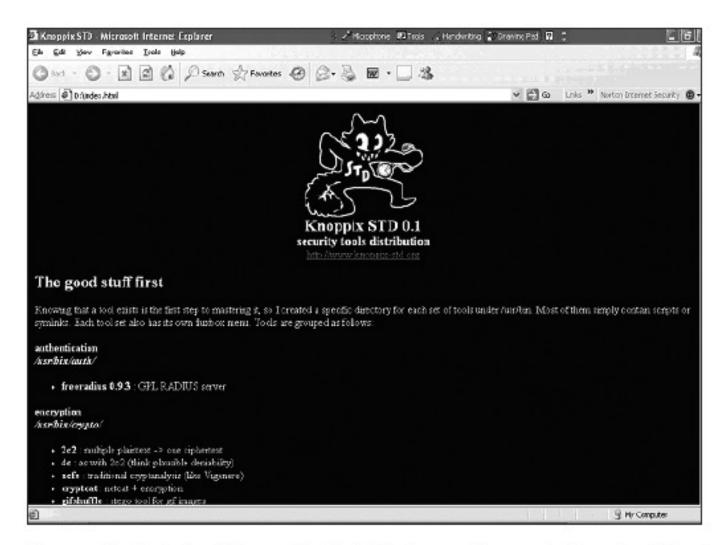


Figure 7-9 The Knoppix-STD information window in Windows

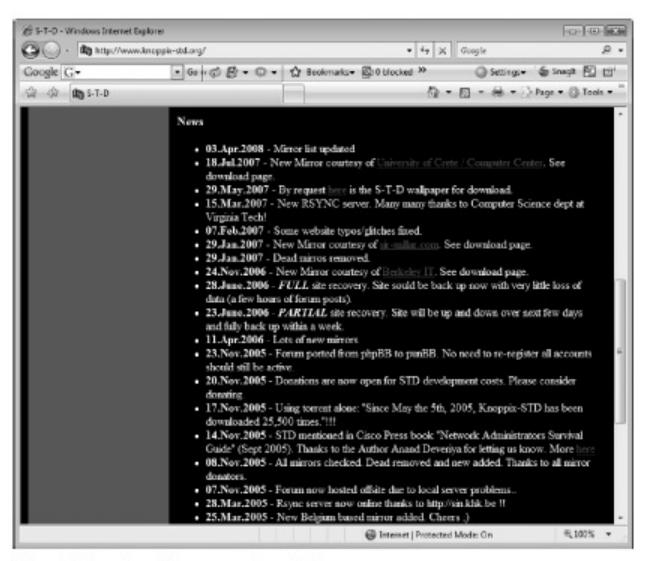


Figure 7-10 A list of forensics tools available in Knoppix-STD

# **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