

# *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 - Microsoft Access databases, E-mail Message

# Types of Computer Forensics Tools

- **Hardware forensic tools**
  - Range from single-purpose components to complete computer systems and servers
    - Write Blocker to Forensic workstation
- **Software forensic tools**
  - Specialized to perform one task to many different tasks
  - SafeBack, a command-line disk acquisition tool
  - Pro-Discover, forensics acquisition and analysis functions
  - Types
    - Command-line applications
    - GUI applications
  - Software tools are 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
  - The contents of a raw image file can be read with any hexadecimal editor



## Acquisition (continued)

- Creating smaller segmented files is a typical feature in vendor acquisition tools
- Make it easier to store acquired data on smaller media, such as CD-Rs or DVD-Rs.
- All computer forensics acquisition tools have a method for verification of the data-copying process
  - That compares the original drive with the image
  - MD5, SHA

# 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

# 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 the file 'ForensicData.doc.jpg' open. The file list on the left shows the file is 41.9 KB and was modified on 01/21/2009. The main window displays the file's content in hexadecimal and ASCII. An arrow points from the text 'Indicates a .jpeg file' to the 'JFIF' marker in the ASCII column at offset 00000000.

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 10:48:58	A	75275
EF7.txt	txt	59 B	01/22/2009 12:55:17	01/22/2009 12:15:20	01/24/2009 10:48:58	A	75277
desktop.ini	ini	0 B	01/21/2009 12:41:45	04/28/2009 12:22:51	01/21/2009 12:41:45	A	
Effel Turner Google.kmz	kmz	6.6 KB	01/21/2009 12:41:45	04/28/2009 12:05:50	01/22/2009 12:54:23	A	107372
ForensicData.doc.jpg	jpg	41.9 KB	01/21/2009 15:01:55	01/21/2009 15:01:55	01/21/2009 15:01:55	A	120250
Yahoo! Briefcase.inf	inf	206 B	01/21/2009 12:41:45	04/28/2009 12:05:50	01/24/2009 19:12:07	A	75271

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Hex	ASCII
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	01	60	FFD8FFE000104A46494600010101010160	JFIF
00000001	00	60	00	00	FF	DB	00	43	00	08	06	06	07	06	05	08	00600000FFDB00430008060607060508	...p0.C...
00000002	07	07	07	09	09	08	0A	0C	1A	0D	0C	0B	0B	0C	19	12	0707070909080A0C1A0D0C0B0B0C1912	.....s "
00000003	13	0F	14	1D	1A	1F	1E	1D	1A	1C	1C	20	24	2E	27	20	130F141D1A1F1E1D1A1C1C20242E2720	.....s "
00000004	22	2C	23	1C	1C	28	37	29	2C	30	31	34	34	34	1F	27	222C231C1C2837292C30313434341F27	"..#.(7).01444..
00000005	39	3D	38	32	3C	2E	33	34	32	FF	DB	00	43	01	09	09	393D38323C2E333432FFDB0043010909	9=82<.342y0.C...
00000006	09	0C	0B	0C	18	0D	0D	18	32	21	1C	21	32	32	32	32	090C0B0C180D0D1832211C2132323232	.....21.12222
00000007	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32323232323232323232323232323232	2222222222222222
00000008	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32323232323232323232323232323232	2222222222222222
00000009	32	32	32	32	32	32	32	32	32	32	32	32	32	32	FF	C0	32323232323232323232323232323232	2222222222222222yA
0000000A	00	11	08	02	58	03	80	03	01	22	00	02	11	01	03	11	00110802580380030122000211010311	...X.I..."
0000000B	01	FF	C4	00	1F	00	00	01	05	01	01	01	01	01	01	00	01FFC4001F0000010501010101010100	yA.....
0000000C	00	00	00	00	00	00	00	01	02	03	04	05	06	07	08	09	000000000000010203040506070809	.....
0000000D	0A	0B	FF	C4	00	B5	10	00	02	01	03	03	02	04	03	05	0A0BFFC400B510000201030302040305	..yA..p.....
0000000E	05	04	04	00	00	01	7D	01	02	03	00	04	11	05	12	21	0504040000017D010203000411051221	.....).....!
0000000F	31	41	06	13	51	61	07	22	71	14	32	81	91	A1	08	23	31410613516107227114328191A10823	1A..Qa."q.2.'i.#
00000010	42	B1	C1	15	52	D1	F0	24	33	62	72	82	09	0A	16	17	42B1C11552D1F02433627282090A1617	EtA..88063brI...
00000011	10	19	1A	25	26	27	28	29	2A	34	35	36	37	38	39	3A	10191A25262728292A3435363738393A	...%<'()=456789:
00000012	43	44	45	46	47	48	49	4A	53	54	55	56	57	58	59	5A	434445464748494A535455565758595A	CDEFGHIJSTUVWXYZ

Drive K: (Integrated)  
File system: NTFS  
Volume label: NTFS1

Default Edit Mode: original  
State: original  
Undo level: 0  
Undo reverses: n/a

Alloc. of visible drive space: 120250  
Cluster No.: 120250  
ForensicData.doc.jpg  
Documents and Settings\Chris\My Documents\

Snapshot taken: 0 min. ago

Physical sector No.: 570133  
Logical sector No.: 120250

Used space: 107 MB

Sector 120250 of 224846

Offset: 3AB7400 = 255 Back: n/a Size: n/a

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

# 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

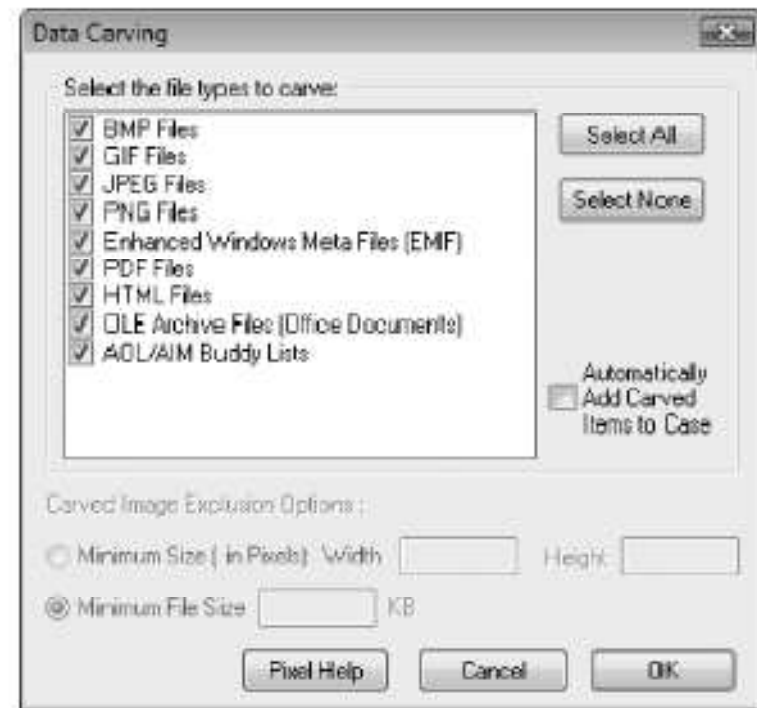


Figure 7-7 Data-carving options in FTK

## 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 (dd command, H/W & S/W tools)
  - 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
- Shadowing technique – Read from suspect drive and write to another drive (shadow drive)
  - Used to demonstrate in court how criminal activity was carried out

# Reporting

- To complete a forensics disk analysis and examination, you need to create a report
- Earlier - Manual examination, paper report
- Subfunctions
  - Log reports (tools records activities the investigator performed)
  - Report generator (EnCase, ProDiscovery,FTK)
- Use this information when producing a final report for your investigation

# 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