Guide to Computer Forensics and Investigations Sixth Edition

Chapter 6

Current Digital Forensics Tools

CENGAGE

Objectives

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

Evaluating Digital Forensics Tool Needs

- Consider open-source tools; the best value for as many features as possible
- Questions to ask when evaluating tools:
  - On which OS does the forensics tool run?
  - Is the tool versatile?
  - Can the tool analyze more than one file system?
  - Can a scripting language be used with the tool to automate repetitive functions and tasks?
  - Does it have automated features?
  - What is the vendor’s reputation for providing product support?

Types of Digital Forensics Tools

- Hardware forensic tools
  - Range from simple, 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 Digital Forensics Tools (1 of 20)

- Follow guidelines set up by NIST’s **Computer Forensics Tool Testing** (**CFTT**) program
- ISO standard 27037 states: Digital Evidence First Responders (DEFRs) should use validated tools
- Five major categories:
  - Acquisition
  - Validation and verification
  - Extraction
  - Reconstruction
  - Reporting

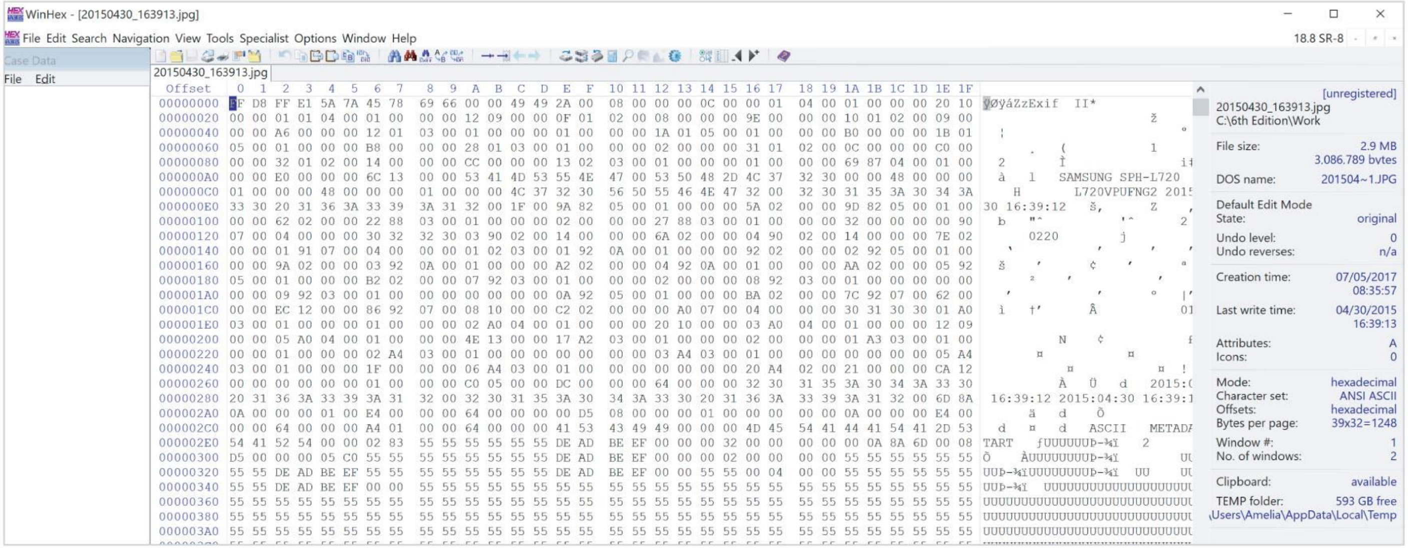
Tasks Performed by Digital Forensics Tools (2 of 20)

- **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, live, and memory acquisitions

Tasks Performed by Digital Forensics Tools (3 of 20)

- Acquisition (cont'd)
  - 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
  - You can view a raw image file's contents with any hexadecimal editor

Tasks Performed by Digital Forensics Tools (4 of 20)


WinHex - [20150430_163913.jpg]
File Edit Search Navigation View Tools Specialist Options Window Help
18.8 SR-8
Case Data
File Edit
20150430_163913.jpg

```
  Offset   0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F  10 11 12 13 14 15 16 17  18 19 1A 1B 1C 1D 1E 1F
00000000  FF D8 FF E1 5A 7A 45 78  69 66 00 00 49 49 2A 00  08 00 00 00 0C 00 00 01  04 00 01 00 00 00 20 10  ÿØÿáZzExif  II*
00000020  00 00 01 01 04 00 01 00  00 00 12 09 00 00 0F 01  02 00 08 00 00 00 9E 00  00 00 10 01 02 00 09 00                       ž
00000040  00 00 A6 00 00 00 12 01  03 00 01 00 00 00 01 00  00 00 1A 01 05 00 01 00  00 00 B0 00 00 00 1B 01    ¦                        °
00000060  05 00 01 00 00 00 B8 00  00 00 28 01 03 00 01 00  00 00 02 00 00 00 31 01  02 00 0C 00 00 00 C0 00        ¸   (           1
00000080  00 00 32 01 02 00 14 00  00 00 CC 00 00 00 13 02  03 00 01 00 00 00 01 00  00 00 69 87 04 00 01 00    2       Ì                i‡
000000A0  00 00 E0 00 00 00 6C 13  00 00 53 41 4D 53 55 4E  47 00 53 50 48 2D 4C 37  32 30 00 00 48 00 00 00    à   l   SAMSUNG SPH-L720
000000C0  01 00 00 00 48 00 00 00  01 00 00 00 4C 37 32 30  56 50 55 46 4E 47 32 00  32 30 31 35 3A 30 34 3A      H       L720VPUFNG2 2015
000000E0  33 30 20 31 36 3A 33 39  3A 31 32 00 1F 00 9A 82  05 00 01 00 00 00 5A 02  00 00 9D 82 05 00 01 00  30 16:39:12   š,      Z      ,
00000100  00 00 62 02 00 00 22 88  03 00 01 00 00 00 02 00  00 00 27 88 03 00 01 00  00 00 32 00 00 00 00 90    b   "^             '^      2
00000120  07 00 04 00 00 00 30 32  32 30 03 90 02 00 14 00  00 00 6A 02 00 00 04 90  02 00 14 00 00 00 7E 02        0220        j
00000140  00 00 01 91 07 00 04 00  00 00 01 02 03 00 01 92  0A 00 01 00 00 00 92 02  00 00 02 92 05 00 01 00     `              '       '    '
00000160  00 00 9A 02 00 00 03 92  0A 00 01 00 00 00 A2 02  00 00 04 92 0A 00 01 00  00 00 AA 02 00 00 05 92    š    '       ¢    '     ª
00000180  05 00 01 00 00 00 B2 02  00 00 07 92 03 00 01 00  00 00 02 00 00 00 08 92  03 00 01 00 00 00 00 00        ²     '             '
000001A0  00 00 09 92 03 00 01 00  00 00 00 00 00 00 0A 92  05 00 01 00 00 00 BA 02  00 00 7C 92 07 00 62 00     '             '       º  |'
000001C0  00 00 EC 12 00 00 86 92  07 00 08 10 00 00 C2 02  00 00 00 A0 07 00 04 00  00 00 30 31 30 30 01 A0    ì   †'       Â             01
000001E0  03 00 01 00 00 00 01 00  00 00 02 A0 04 00 01 00  00 00 20 10 00 00 03 A0  04 00 01 00 00 00 12 09
00000200  00 00 05 A0 04 00 01 00  00 00 4E 13 00 00 17 A2  03 00 01 00 00 00 02 00  00 00 01 A3 03 00 01 00            N    ¢            £
00000220  00 00 01 00 00 00 02 A4  03 00 01 00 00 00 00 00  00 00 03 A4 03 00 01 00  00 00 00 00 00 00 05 A4        ¤            ¤
00000240  03 00 01 00 00 00 1F 00  00 00 06 A4 03 00 01 00  00 00 00 00 00 00 20 A4  02 00 21 00 00 00 CA 12            ¤            ¤  !
00000260  00 00 00 00 00 00 01 00  00 00 C0 05 00 00 DC 00  00 00 64 00 00 00 32 30  31 35 3A 30 34 3A 33 30            À   Ü   d   2015:(
00000280  20 31 36 3A 33 39 3A 31  32 00 32 30 31 35 3A 30  34 3A 33 30 20 31 36 3A  33 39 3A 31 32 00 6D 8A   16:39:12 2015:04:30 16:39:1
000002A0  0A 00 00 00 01 00 E4 00  00 00 64 00 00 00 00 D5  08 00 00 00 01 00 00 00  00 00 0A 00 00 00 E4 00        ä   d   Õ
000002C0  00 00 64 00 00 00 A4 01  00 00 64 00 00 00 41 53  43 49 49 00 00 00 4D 45  54 41 44 41 54 41 2D 53    d   ¤   d   ASCII   METADA
000002E0  54 41 52 54 00 00 02 83  55 55 55 55 55 55 DE AD  BE EF 00 00 00 32 00 00  00 00 00 0A 8A 6D 00 08  TART   ƒUUUUUUÞ-¾ï   2
00000300  D5 00 00 00 05 C0 55 55  55 55 55 55 55 55 DE AD  BE EF 00 00 00 02 00 00  00 00 55 55 55 55 55 55  Õ     ÀUUUUUUUUÞ-¾ï        UU
00000320  55 55 DE AD BE EF 55 55  55 55 55 55 55 55 DE AD  BE EF 00 00 55 55 00 04  00 00 55 55 55 55 55 55  UUÞ-¾ïUUUUUUUUÞ-¾ï  UU    UU
00000340  55 55 DE AD BE EF 00 00  55 55 55 55 55 55 55 55  55 55 55 55 55 55 55 55  55 55 55 55 55 55 55 55  UUÞ-¾ï  UUUUUUUUUUUUUUUUUUUUUU
00000360  55 55 55 55 55 55 55 55  55 55 55 55 55 55 55 55  55 55 55 55 55 55 55 55  55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUUUUUUUUUUUUUUUU
00000380  55 55 55 55 55 55 55 55  55 55 55 55 55 55 55 55  55 55 55 55 55 55 55 55  55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUUUUUUUUUUUUUUUU
000003A0  55 55 55 55 55 55 55 55  55 55 55 55 55 55 55 55  55 55 55 55 55 55 55 55  55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUUUUUUUUUUUUUUUU
```

[unregistered]
20150430_163913.jpg
C:\6th Edition\Work

File size: 2.9 MB
3,086,789 bvtes

DOS name: 201504~1.JPG

Default Edit Mode
State: original

Undo level: 0
Undo reverses: n/a

Creation time: 07/05/2017 08:35:57

Last write time: 04/30/2015 16:39:13

Attributes: A
Icons: 0

Mode: hexadecimal
Character set: ANSI ASCII
Offsets: hexadecimal
Bytes per page: 39x32=1248

Window #: 1
No. of windows: 2

Clipboard: available

TEMP folder: 593 GB free
\Users\Amelia\AppData\Local\Temp

Figure 6-1 **Viewing data in WinHex**

Source: X-Ways AG, *www.x-ways.net*

Tasks Performed by Digital Forensics Tools (5 of 20)

- Acquisition (cont'd)
  - Creating smaller segmented files is a typical feature in vendor acquisition tools
  - Remote acquisition of files is common in larger organizations
    - Popular tools, such as AccessData and EnCase, can do remote acquisitions of forensics drive images on a network

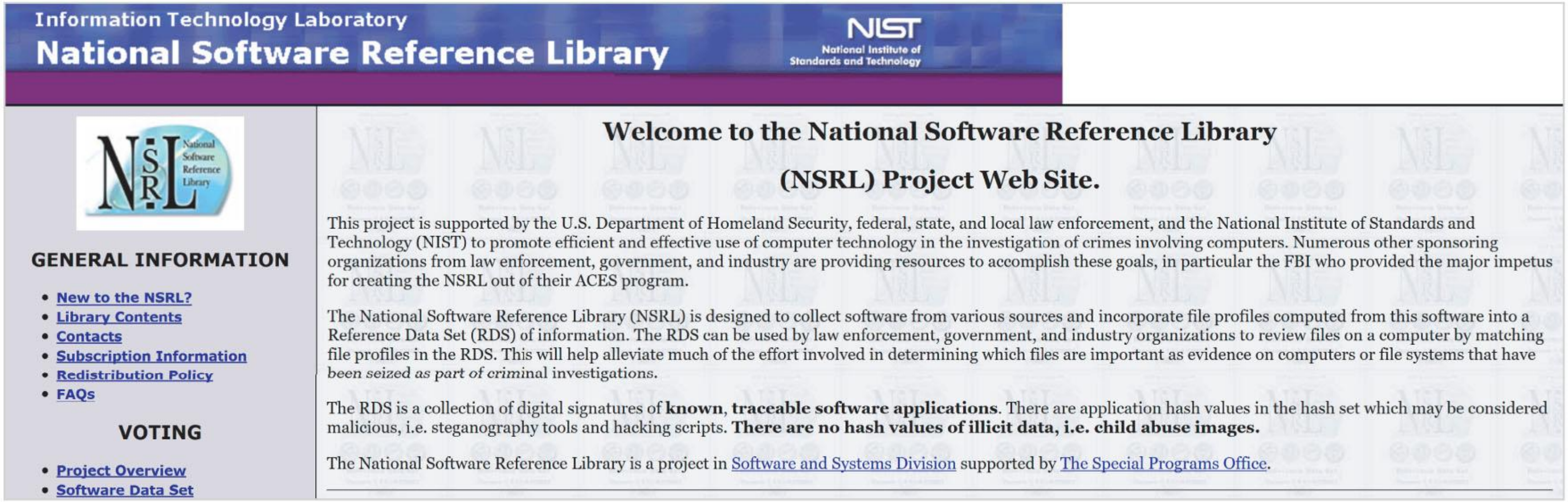
Tasks Performed by Digital Forensics Tools (6 of 20)

- Validation and Verification
  - **Validation**
    - A way to confirm that a tool is functioning as intended
  - **Verification**
    - Proves that two sets of data are identical by calculating hash values or using another similar method
    - A related process is filtering, which involves sorting and searching through investigation findings to separate good data and suspicious data

Tasks Performed by Digital Forensics Tools (7 of 20)

- Validation and verification (cont'd)
  - Subfunctions
    - Hashing
      - CRC-32, MD5, SHA-1 (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 Digital Forensics Tools (8 of 20)



Information Technology Laboratory
National Software Reference Library
NIST
National Institute of Standards and Technology
NSRL National Software Reference Library

GENERAL INFORMATION

- New to the NSRL?
- Library Contents
- Contacts
- Subscription Information
- Redistribution Policy
- FAQs

VOTING

- Project Overview
- Software Data Set

Welcome to the National Software Reference Library

(NSRL) Project Web Site.

This project is supported by the U.S. Department of Homeland Security, federal, state, and local law enforcement, and the National Institute of Standards and Technology (NIST) to promote efficient and effective use of computer technology in the investigation of crimes involving computers. Numerous other sponsoring organizations from law enforcement, government, and industry are providing resources to accomplish these goals, in particular the FBI who provided the major impetus for creating the NSRL out of their ACES program.

The National Software Reference Library (NSRL) is designed to collect software from various sources and incorporate file profiles computed from this software into a Reference Data Set (RDS) of information. The RDS can be used by law enforcement, government, and industry organizations to review files on a computer by matching file profiles in the RDS. This will help alleviate much of the effort involved in determining which files are important as evidence on computers or file systems that have been seized as part of criminal investigations.

The RDS is a collection of digital signatures of **known, traceable software applications**. There are application hash values in the hash set which may be considered malicious, i.e. steganography tools and hacking scripts. **There are no hash values of illicit data, i.e. child abuse images.**

The National Software Reference Library is a project in Software and Systems Division supported by The Special Programs Office.

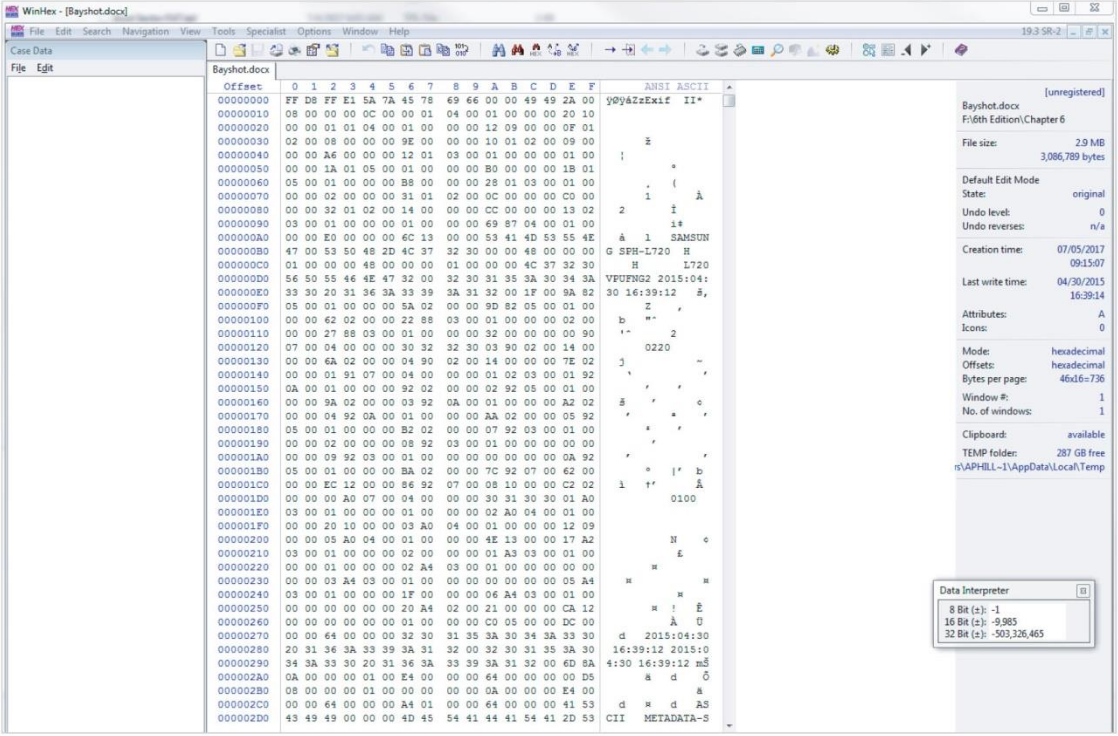
Figure 6-2 The home page of the National Software Reference Library

Source: *www.nsrl.nist.gov*

Tasks Performed by Digital Forensics Tools (9 of 20)

- Validation and discrimination (cont'd)
  - 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

Tasks Performed by Digital Forensics Tools (10 of 20)


WinHex - [Bayshot.docx]
File Edit Search Navigation View Tools Specialist Options Window Help
19.3 SR-2
Case Data
File Edit
Bayshot.docx

```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F     ANSI ASCII
00000000  FF D8 FF E1 5A 7A 45 78  69 66 00 00 49 49 2A 00  ÿØÿáZzExif  II*
00000010  08 00 00 00 0C 00 00 01  04 00 01 00 00 00 20 10
00000020  00 00 01 01 04 00 01 00  00 00 12 09 00 00 0F 01
00000030  02 00 08 00 00 00 9E 00  00 00 10 01 02 00 09 00        ž
00000040  00 00 A6 00 00 00 12 01  03 00 01 00 00 00 01 00    ¦
00000050  00 00 1A 01 05 00 01 00  00 00 B0 00 00 00 1B 01            °
00000060  05 00 01 00 00 00 B8 00  00 00 28 01 03 00 01 00        ¸   (
00000070  00 00 02 00 00 00 31 01  02 00 0C 00 00 00 C0 00        1       À
00000080  00 00 32 01 02 00 14 00  00 00 CC 00 00 00 13 02    2       Ì
00000090  03 00 01 00 00 00 01 00  00 00 69 87 04 00 01 00            i‡
000000A0  00 00 E0 00 00 00 6C 13  00 00 53 41 4D 53 55 4E    à   l   SAMSUN
000000B0  47 00 53 50 48 2D 4C 37  32 30 00 00 48 00 00 00  G SPH-L720  H
000000C0  01 00 00 00 48 00 00 00  01 00 00 00 4C 37 32 30      H       L720
000000D0  56 50 55 46 4E 47 32 00  32 30 31 35 3A 30 34 3A  VPUFNG2 2015:04:
000000E0  33 30 20 31 36 3A 33 39  3A 31 32 00 1F 00 9A 82  30 16:39:12   š‚
000000F0  05 00 01 00 00 00 5A 02  00 00 9D 82 05 00 01 00        Z    ‚
00000100  00 00 62 02 00 00 22 88  03 00 01 00 00 00 02 00    b   "ˆ
00000110  00 00 27 88 03 00 01 00  00 00 32 00 00 00 00 90    'ˆ      2
00000120  07 00 04 00 00 00 30 32  32 30 03 90 02 00 14 00        0220
00000130  00 00 6A 02 00 00 04 90  02 00 14 00 00 00 7E 02    j           ~
00000140  00 00 01 91 07 00 04 00  00 00 01 02 03 00 01 92     ‘           ’
00000150  0A 00 01 00 00 00 92 02  00 00 02 92 05 00 01 00        ’   ’
00000160  00 00 9A 02 00 00 03 92  0A 00 01 00 00 00 A2 02    š   ’       ¢
00000170  00 00 04 92 0A 00 01 00  00 00 AA 02 00 00 05 92     ’      ª    ’
00000180  05 00 01 00 00 00 B2 02  00 00 07 92 03 00 01 00        ²   ’
00000190  00 00 02 00 00 00 08 92  03 00 01 00 00 00 00 00         ’
000001A0  00 00 09 92 03 00 01 00  00 00 00 00 00 00 0A 92     ’           ’
000001B0  05 00 01 00 00 00 BA 02  00 00 7C 92 07 00 62 00        º   |’  b
000001C0  00 00 EC 12 00 00 86 92  07 00 08 10 00 00 C2 02    ì   †’      Â
000001D0  00 00 00 A0 07 00 04 00  00 00 30 31 30 30 01 A0              0100
000001E0  03 00 01 00 00 00 01 00  00 00 02 A0 04 00 01 00
000001F0  00 00 20 10 00 00 03 A0  04 00 01 00 00 00 12 09
00000200  00 00 05 A0 04 00 01 00  00 00 4E 13 00 00 17 A2            N   ¢
00000210  03 00 01 00 00 00 02 00  00 00 01 A3 03 00 01 00             £
00000220  00 00 01 00 00 00 02 A4  03 00 01 00 00 00 00 00         ¤
00000230  00 00 03 A4 03 00 01 00  00 00 00 00 00 00 05 A4     ¤           ¤
00000240  03 00 01 00 00 00 1F 00  00 00 06 A4 03 00 01 00             ¤
00000250  00 00 00 00 00 00 20 A4  02 00 21 00 00 00 CA 12         ¤ !   Ê
00000260  00 00 00 00 00 00 01 00  00 00 C0 05 00 00 DC 00            À   Ü
00000270  00 00 64 00 00 00 32 30  31 35 3A 30 34 3A 33 30    d   2015:04:30
00000280  20 31 36 3A 33 39 3A 31  32 00 32 30 31 35 3A 30   16:39:12 2015:0
00000290  34 3A 33 30 20 31 36 3A  33 39 3A 31 32 00 6D 8A  4:30 16:39:12 mŠ
000002A0  0A 00 00 00 01 00 E4 00  00 00 64 00 00 00 00 D5        ä   d   Õ
000002B0  08 00 00 00 01 00 00 00  00 00 0A 00 00 00 E4 00                ä
000002C0  00 00 64 00 00 00 A4 01  00 00 64 00 00 00 41 53    d   ¤   d   AS
000002D0  43 49 49 00 00 00 4D 45  54 41 44 41 54 41 2D 53  CII   METADATA-S
```

[unregistered]
Bayshot.docx
F:\6th Edition\Chapter 6

File size: 2.9 MB
3,086,789 bytes

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

Creation time: 07/05/2017 09:15:07

Last write time: 04/30/2015 16:39:14

Attributes: A
Icons: 0

Mode: hexadecimal
Offsets: hexadecimal
Bytes per page: 46x16=736
Window #: 1
No. of windows: 1

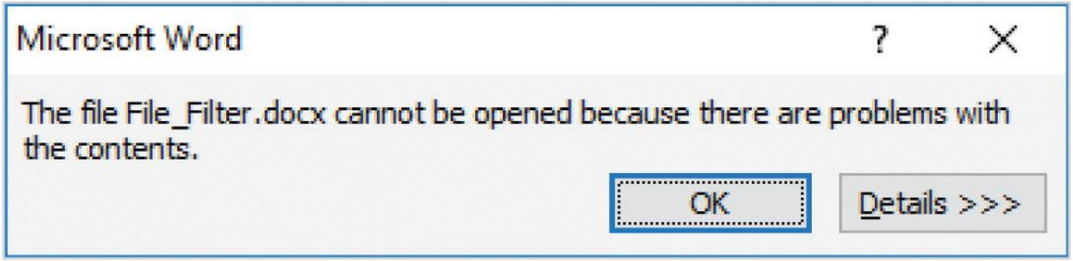
Clipboard: available
TEMP folder: 287 GB free
rs\APHILL~1\AppData\Local\Temp

Data Interpreter
8 Bit (±): -1
16 Bit (±): -9,985
32 Bit (±): -503,326,465

Figure 6-3 The file header indicates a `.jpeg` file

Source: X-Ways AG, *www.x-ways.net*

Tasks Performed by Digital Forensics Tools (11 of 20)



Microsoft Word

The file File_Filter.docx cannot be opened because there are problems with the contents.

Figure 6-4 Error message displayed when trying to open a `.jpeg` file in Word

Tasks Performed by Digital Forensics Tools (12 of 20)

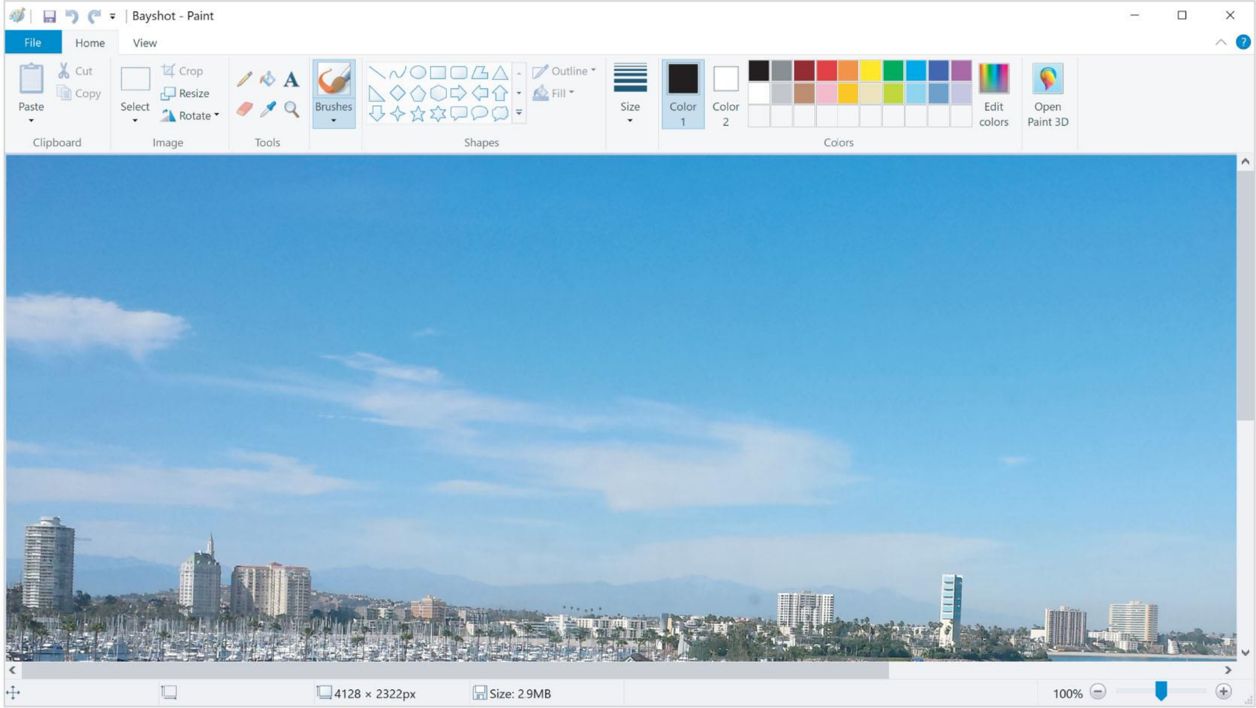


Figure 6-5 Bayshot.docx opened in Paint

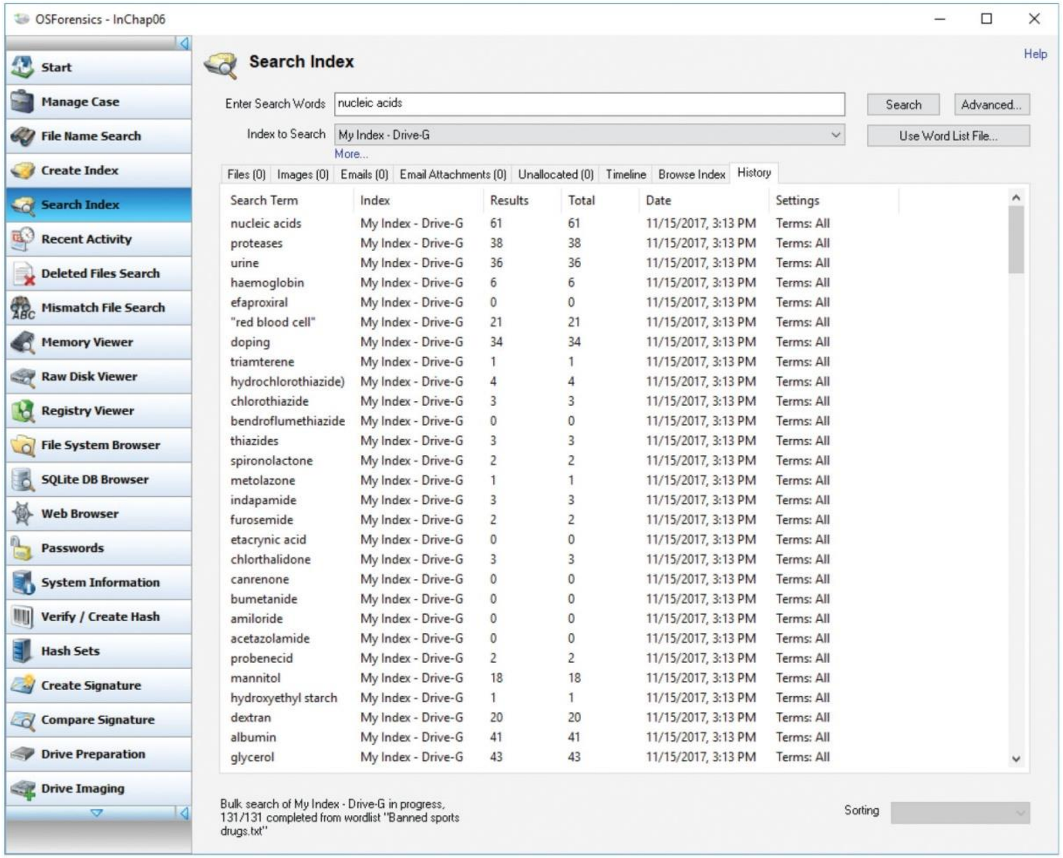
Tasks Performed by Digital Forensics Tools (13 of 20)

- **Extraction**
  - Recovery task in a digital investigation
  - Most challenging of all tasks to master
  - Recovering data is the first step in analyzing an investigation’s data

Tasks Performed by Digital Forensics Tools (14 of 20)

- Extraction (cont’d)
  - Subfunctions of extraction
    - Data viewing
    - Keyword searching
    - Decompressing or uncompressing
    - Carving
    - Decrypting
    - Bookmarking or tagging
  - **Keyword search** speeds up analysis for investigators

Tasks Performed by Digital Forensics Tools (15 of 20)



Search Index

Enter Search Words: nucleic acids

Index to Search: My Index - Drive-G

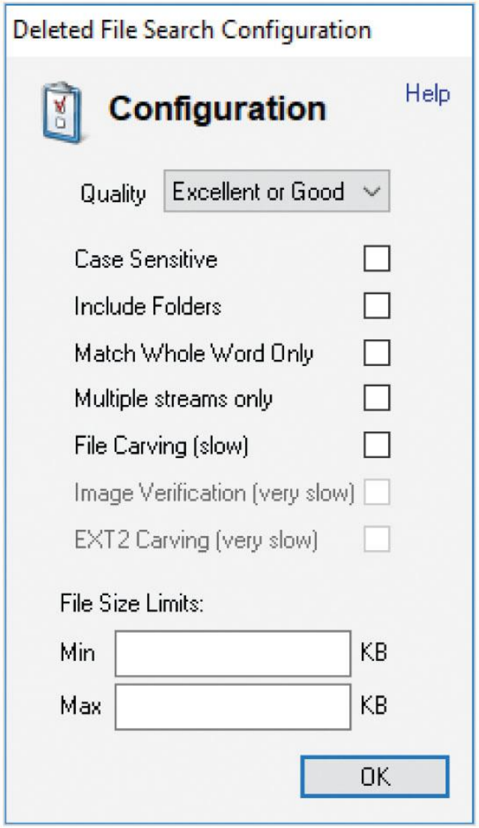
Search Term	Index	Results	Total	Date	Settings
nucleic acids	My Index - Drive-G	61	61	11/15/2017, 3:13 PM	Terms: All
proteases	My Index - Drive-G	38	38	11/15/2017, 3:13 PM	Terms: All
urine	My Index - Drive-G	36	36	11/15/2017, 3:13 PM	Terms: All
haemoglobin	My Index - Drive-G	6	6	11/15/2017, 3:13 PM	Terms: All
efaproxiral	My Index - Drive-G	0	0	11/15/2017, 3:13 PM	Terms: All
"red blood cell"	My Index - Drive-G	21	21	11/15/2017, 3:13 PM	Terms: All
doping	My Index - Drive-G	34	34	11/15/2017, 3:13 PM	Terms: All
triamterene	My Index - Drive-G	1	1	11/15/2017, 3:13 PM	Terms: All
hydrochlorothiazide)	My Index - Drive-G	4	4	11/15/2017, 3:13 PM	Terms: All
chlorothiazide	My Index - Drive-G	3	3	11/15/2017, 3:13 PM	Terms: All
bendroflumethiazide	My Index - Drive-G	0	0	11/15/2017, 3:13 PM	Terms: All
thiazides	My Index - Drive-G	3	3	11/15/2017, 3:13 PM	Terms: All
spironolactone	My Index - Drive-G	2	2	11/15/2017, 3:13 PM	Terms: All
metolazone	My Index - Drive-G	1	1	11/15/2017, 3:13 PM	Terms: All
indapamide	My Index - Drive-G	3	3	11/15/2017, 3:13 PM	Terms: All
furosemide	My Index - Drive-G	2	2	11/15/2017, 3:13 PM	Terms: All
etacrynic acid	My Index - Drive-G	0	0	11/15/2017, 3:13 PM	Terms: All
chlorthalidone	My Index - Drive-G	3	3	11/15/2017, 3:13 PM	Terms: All
canrenone	My Index - Drive-G	0	0	11/15/2017, 3:13 PM	Terms: All
bumetanide	My Index - Drive-G	0	0	11/15/2017, 3:13 PM	Terms: All
amiloride	My Index - Drive-G	0	0	11/15/2017, 3:13 PM	Terms: All
acetazolamide	My Index - Drive-G	0	0	11/15/2017, 3:13 PM	Terms: All
probenecid	My Index - Drive-G	2	2	11/15/2017, 3:13 PM	Terms: All
mannitol	My Index - Drive-G	18	18	11/15/2017, 3:13 PM	Terms: All
hydroxyethyl starch	My Index - Drive-G	1	1	11/15/2017, 3:13 PM	Terms: All
dextran	My Index - Drive-G	20	20	11/15/2017, 3:13 PM	Terms: All
albumin	My Index - Drive-G	41	41	11/15/2017, 3:13 PM	Terms: All
glycerol	My Index - Drive-G	43	43	11/15/2017, 3:13 PM	Terms: All

Bulk search of My Index - Drive-G in progress, 131/131 completed from wordlist "Banned sports drugs.txt"

Figure 6-6 Using a word list to search in OSForensics

Source: PassMark Software, *www.osforensics.com*

Tasks Performed by Digital Forensics Tools (16 of 20)



Deleted File Search Configuration

Configuration

Quality: Excellent or Good

Case Sensitive □

Include Folders □

Match Whole Word Only □

Multiple streams only □

File Carving (slow) □

Image Verification (very slow) □

EXT2 Carving (very slow) □

File Size Limits:

Min ____ KB

Max ____ KB

Figure 6-7 Data-carving options in OS Forensics

Source: PassMark Software, *www.osforensics.com*

Tasks Performed by Digital Forensics Tools (17 of 20)

- Extraction (cont’d)
  - 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 Digital Forensics Tools (18 of 20)

- **Reconstruction**
  - Re-create a suspect drive to show what happened during a crime or an incident
  - Methods of reconstruction
    - Disk-to-disk copy
    - Partition-to-partition copy
    - Image-to-disk copy
    - Image-to-partition copy
    - Disk-to-image copy
    - Rebuilding files from data runs and carving

Tasks Performed by Digital Forensics Tools (19 of 20)

- Reconstruction (cont’d)
  - To re-create an image of a suspect drive
    - Copy an image to another location, such as a partition, a physical disk, or a virtual machine
    - Simplest method is to use a tool that makes a direct disk-to-image copy
  - Examples of disk-to-image copy tools:
    - Linux dd command
    - ProDiscover
    - Voom Technologies Shadow Drive

Tasks Performed by Digital Forensics Tools (20 of 20)

- **Reporting**
  - To perform a forensics disk analysis and examination, you need to create a report
  - Subfunctions of reporting
    - Bookmarking or tagging
    - Log reports
    - Timelines
    - Report generator
  - Use this information when producing a final report for your investigation

Other Considerations for Tools

- Considerations
  - Flexibility
  - Reliability
  - Future expandability
- Create a software library containing older versions of forensics utilities, OSs, and other programs

Digital Forensics Software Tools

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

Command-line Forensics 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
- Command-line tools require few system resources
  - Designed to run in minimal configurations

Linux Forensics Tools (1 of 3)

- UNIX has been mostly replaced by Linux
  - You might still encounter systems running UNIX
- Linux platforms have become more popular with home and business end users
- 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

Linux Forensics Tools (2 of 3)

- Helix 3
  - One of the easiest suites to use
  - You can load it on a live Windows system
    - Loads as a bootable Linux OS from a cold boot
  - **Some international courts have not accepted live acquisitions as a valid forensics practice
- Kali Linux
  - Formerly known as BackTrack
  - Includes a variety of tools and has an easy-to-use KDE interface

Linux Forensics Tools (3 of 3)

- Autopsy and SleuthKit
  - Sleuth Kit is a Linux forensics tool
  - Autopsy was the browser interface used to access Sleuth Kit’s tools
  - Chapter 7 explains how to use these tools
- Forcepoint Threat Protection
  - Formerly known as Second Look
  - A Linux memory analysis tool
  - Could perform both onsite and remote memory acquisitions

Other GUI Forensics Tools (1 of 2)

- GUI forensics tools can simplify digital forensics investigations
- Have also simplified training for beginning examiners
- Most of them are put together as suites of tools
- Advantages
  - Ease of use
  - Multitasking
  - No need for learning older OSs

Other GUI Forensics Tools (2 of 2)

- Disadvantages
  - Excessive resource requirements
  - Produce inconsistent results
  - Create tool dependencies
    - Investigators’ may want to use only one tool
    - Should be familiar with more than one type of tool

Digital Forensics Hardware Tools

- Technology changes rapidly
- Hardware eventually fails
  - Schedule equipment replacements periodically
- When planning your budget consider:
  - Amount of time you expect the forensic workstation to be running
  - Failures
  - Consultant and vendor fees
  - Anticipate equipment replacement

Forensic Workstations (1 of 4)

- Carefully consider what you need
- Categories
  - Stationary workstation
  - Portable workstation
  - Lightweight workstation
- Balance what you need and what your system can handle
  - Remember that RAM and storage need updating as technology advances

Forensic Workstations (2 of 4)

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

Forensic Workstations (3 of 4)

- Building a forensic workstation is 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 (4 of 4)

- Some vendors offer workstations designed for digital forensics
- Examples
  - F.R.E.D. unit from Digital Intelligence
  - Hardware mounts from ForensicPC
- 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 (1 of 2)

- **Write-blocker**
  - Prevents data writes to a hard disk
- Software-enabled blockers
  - Typically run in a shell mode (Windows CLI)
  - 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 (2 of 2)

- You 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 and 3.0
  - SATA, PATA, and SCSI controllers

Recommendations for a Forensic Workstation (1 of 3)

- Determine where data acquisitions will take place
- With Firewire and USB write-blocking devices
  - You can acquire data easily with Digital Intelligence FireChief and a laptop computer
- If you want to reduce hardware to carry:
  - WiebeTech Forensic DriveDock with its regular DriveDock FireWire bridge or the Logicube Talon

Recommendations for a Forensic Workstation (2 of 3)

- Recommendations when choosing stationary or lightweight workstation:
  - Full tower to allow for expansion devices
  - As much memory and processor power as budget allows
  - Different sizes of hard drives
  - 400-watt or better power supply with battery backup
  - External FireWire and USB ports
  - Assortment of drive adapter bridges

Recommendations for a Forensic Workstation (3 of 3)

- Recommendations when choosing stationary or lightweight workstation (cont'd):
  - Ergonomic keyboard and mouse
  - A good video card with at least a 17-inch monitor
  - High-end video card and dual monitors
- If you have a limited budget, one option for outfitting your lab is to use high-end game PCs

Validating and Testing Forensic Software

- It is important to make sure the evidence you recover and analyze can be admitted in court
- You must test and validate your software to prevent damaging the evidence

Using National Institute of Standards and Technology Tools (1 of 3)

- NIST publishes articles, provides tools, and creates procedures for testing/validating forensics software
- Computer Forensics Tool Testing (CFTT) project
  - Manages research on forensics tools
- NIST has created criteria for testing forensics tools based on:
  - Standard testing methods
  - ISO 17025 criteria for testing items that have no current standards

Using National Institute of Standards and Technology Tools (2 of 3)

- Your lab must meet the following criteria
  - Establish categories for digital forensics tools
  - Identify forensics category requirements
  - Develop test assertions
  - Identify test cases
  - Establish a test method
  - Report test results
- ISO 5725 - specifies results must be repeatable and reproducible

Using National Institute of Standards and Technology Tools (3 of 3)

- NIST created the 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 (1 of 3)

- Always verify your results by performing the same tasks with other similar forensics tools
- Use at least two tools
  - Retrieving and examination
  - Verification
- Understand how forensics 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 (2 of 3)

- Disk editors do not have a flashy interface, however they:
  - Are reliable tools
  - Can access raw data
- Digital 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 (3 of 3)

- Digital 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 (1 of 3)

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

Summary (2 of 3)

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

Summary (3 of 3)

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