



EnCase® Forensic Edition User Manual

Version 4

Guidance Software

215 North Marengo Avenue, 2nd Floor
Pasadena, California 91101

tel: 626.229.9191

fax: 626.229.9199

email: info@guidancesoftware.com

www.guidancesoftware.com

EnCase Forensic Version 4.20, Revision C

Table of Contents

Table of Contents.....	3
Legal Notice	15
EnCase® License Agreement	15
Copyright.....	15
Definitions	15
License and Certain Restrictions.....	15
Non-Exclusive License.....	16
Support	17
Standard Support	17
Premium License Support Program, Annual Payment Option	17
Premium License Support Program, Three-Year Payment Option	18
EnScript® Macros WARNING	18
Disclaimer of Warranties.....	18
Limitation of Liability and Damages	19
Export Restrictions.....	19
U.S. Government End Users:.....	20
General Provisions	20
Preface	23
 Manual Organization	23
 Minimum Recommended Requirements	24
 Help Resources	24
 Technical Support	25
 EnCase Message Boards.....	25
About Guidance Software	27
 EnCase Forensic	27
 EnCase Enterprise.....	27
 Guidance Software's Professional Development and Training	28
 Law Enforcement Courses	28
 Computer Forensics and Incident Response Courses	28
 Expert Courses	29
 Guidance Software's Professional Services Group.....	29
 Additional Corporate Services	29

Chapter 1: What's New in EnCase Version 4	33
Enhanced User Interface.....	33
Outlook .PST Files	35
Outlook Express .DBX Files	35
Time Zone Support	35
Unicode Support.....	35
Advanced Search Algorithm.....	36
Dynamic Disk Support	37
NT 4.0 Disk Configuration Support.....	38
NTFS and Unix File Permissions and Ownership	38
NTFS Compression.....	39
Threaded Crash Protection.....	39
Enhanced OLE File Support	40
Filters and Queries	40
Enhanced EnScript Interface.....	41
Enhanced Linux / Unix File System Handling.....	42
Additional File System Support	43
Enhanced Windows Registry Mounting	43
EnCase Modules and Extensions	43
EnCase EDS Module.....	44
EnCase VFS Module	44
EnCase PDE Module.....	45
EnCase NAS Extension.....	46
SafeBack 2.x Support.....	46
Security Key	46
The Parallel Port Security key.....	47
The USB Security key	47
Chapter 2: Installing EnCase	49
The EnCase Installation CD and Autorun	49
The CD Installation Menu and Contents.....	49
Security Key Drivers Installation.....	50
Installing EnCase Version 4.....	53
Software Updates.....	55
Configuration Questions.....	56
Security Key Questions	57
Chapter 3: Creating the EnCase Boot Disk	61
Windows Acquisition Issues.....	61
Creating the EnCase Boot Disk	62
Steps to Create the EnCase Barebones Boot Disk.....	62
Booting a Computer with the EnCase Boot Disk	66
EnCase Network Boot Disk.....	67

FAQs about EnCase Boot Disk	67
Chapter 4:EnCase for DOS.....	69
Launching EnCase for DOS	69
EnCase for DOS Functions.....	69
Locking / Unlocking (L).....	70
Acquiring.....	70
Hashing	70
Server	74
Mode	76
Quit	77
Chapter 5: Previewing Versus Acquiring	79
Limitations of Previewing.....	79
Advantages of Previewing.....	80
Live Device and FastBloc Indicators.....	80
Preview Questions.....	81
Acquisition Questions.....	81
Chapter 6 : Parallel Port Acquisition.....	83
After acquisition is complete	89
Chapter 7: Network Cable Acquisition.....	91
Creating the EnCase Network Boot Disk (ENBD).....	91
Performing the Crossover Network Cable Acquisition	94
Windows 98.....	95
Windows 2000/XP	96
Chapter 8: Drive-to-Drive Acquisition.....	99
Drive Geometry Problems.....	99
Benefits and Drawbacks	100
Steps to Follow	100
Acquiring Macintosh devices	108
Acquiring Unix and Linux	108
After the Acquisition Is Complete	108
Chapter 9: FastBloc Acquisitions	111
FastBloc Acquisition Process.....	111
Acquiring in Windows <i>Without</i> FastBloc	120
Acquiring in Windows <i>with</i> a non-FastBloc Write-Blocker.....	120
After Acquisition Is Complete	120
Chapter 10: Acquiring Disk Configurations	121
Software RAID	122
Windows NT: EnCase Version 4 software Disk Configurations	122
Dynamic Disk	123

Hardware Disk Configuration	124
Disk Configuration Set Acquired as One Drive.....	124
Disk Configurations Acquired as Separate Drives	124
Validating Parity on a RAID-5.....	126
SCSI Drives and DOS	127
Chapter 11: Acquiring Palm PDAs	129
Palms Supported	129
Directions	129
Getting Out of Console Mode.....	137
One Final Note on Palms	137
Chapter 12: Acquiring Removable Media	139
Zip / Jaz Disks	139
Floppy Disks.....	141
Write-Protecting a Floppy Disk.....	141
Superdisks (LS-120)	141
CD-ROM, CD-R, CD-RW.....	141
Flash media	142
Equipment needed to preview/acquire flash media.....	142
How to acquire flash media.....	143
Examining flash media.....	143
Acquiring Multiple Pieces of Media	144
Chapter 13: First Steps	149
Time Zone Settings.....	149
Recover Folders on FAT Volumes	151
Behind the Scenes with Recover Folders.....	152
Recovering NTFS Folders.....	154
Lost Files in UFS and EXT2/3 Partitions	156
Signature Analysis.....	157
File Signatures.....	157
Adding a New Signature	158
Starting a Signature Analysis	160
Viewing the Results.....	160
Hash Analysis	162
File Hashing	162
Creating a Hash Set.....	162
Importing Hash Sets	164
HashKeeper.....	164
NSRL Hash Sets	167
To import hash sets from the NSRL Reference Data Set CD:.....	167
Rebuilding the Hash Library	170
Benefits of a Hash Analysis.....	170

Starting a Hash Analysis	171
Analyzing the Hash Results	172
EnScripts	172
Initialize Case (v4)	173
FAT Info Record Finder (v4) and NTFS Info2 Record Finder (v4)	173
File Finder (v4)	173
IE History Parser with Keyword Search (v4)	173
Link File Parser (v4)	173
Find Unique EMail Address List (v4).....	173
Chapter 14: Navigating EnCase.....	175
Creating a New Case	175
Name.....	176
Examiner's Name.....	176
Default Export Folder.....	176
Temporary Folder	176
Case Management	177
Concurrent Case Management	177
The Options Dialog	178
Global	178
Colors	180
Fonts	181
EnScript.....	182
Storage Paths	183
Adding Evidence Files to a Case	184
Sessions Option	187
Error Messages.....	189
Verifying the Evidence	190
Adding Raw Image Files	191
SafeBack and VMware Images	193
Interface	196
EnCase Views.....	197
The "All Files" Button	197
Cases	197
Bookmarks	198
Devices	199
File Types	200
File Signatures	201
File Viewers	201
Keywords.....	202
Search Hits	202
Security IDs	203
Text Styles	206

Scripts	207
Hash Sets	208
EnScript Types	209
Table View	210
Cases Table View Columns Explained	211
Name	211
Filter	211
In Report	211
File Ext	212
File Type	212
File Category	212
Signature	212
Description	213
Is Deleted	213
Last Accessed	213
File Created	213
Last Written	213
Entry Modified	213
File Deleted	214
Logical Size	214
Physical Size	214
Starting Extent	214
File Extents	214
Permissions	215
Evidence File	218
File Identifier	218
Hash Value	218
Hash Set	218
Hash Category	218
Full Path	218
Short Name	219
Unique Name	219
Original Path	219
Organizing Columns	219
Rearranging Columns	219
Hiding and Showing Columns	220
Sorting Files in Columns	220
EnCase Icon Descriptions	221
Gallery View	226
America Online .ART files	228
Timeline View	228
Report View	230
EnScript View	231

Bottom Pane.....	232
Bottom Pane Tabs.....	232
Text	232
Hex	232
Picture	233
Disk	233
Report	233
Console	234
Filters.....	234
Queries	234
Details	235
Lock	236
Navigation Bar	236
Split Panes.....	239
Date and Time Questions.....	239
Chapter 15: Viewing Files.....	241
Copy/UnErasing Files.....	241
Selecting Files	241
Copying/UnErasing Files	242
Copying/UnErasing Bookmarks	244
Copying Entire Folders.....	245
Viewing Files Outside of EnCase	245
File Viewers.....	245
Setting up a File Viewer	246
File Types	246
File Questions	247
Chapter 16: Keyword Searches	249
Creating Keyword Groups.....	249
Entering Keywords	251
Search Options	251
International Keywords	253
Exporting/Importing Keywords	254
Exporting Keywords.....	254
Importing Keywords.....	256
Adding Keyword Lists	256
Starting a Search	257
Search Options.....	258
Viewing Search Hits	259
Bookmarking Search Hits	264
The Refresh Button	265
Cancelling a Search.....	265

Chapter 17: Viewing Compound Files	267
Registry Files	268
OLE Files	269
Compressed Files	270
Outlook Express E-mail	271
Base64 and UUE Encoding	272
MS Outlook E-Mail	273
NTFS Compressed Files	275
Search compressed NTFS files and folders	275
Thumbs.db.....	276
Chapter 18: EnScript and Filters	277
EnScript Path	278
Include Folder	279
Working with EnScripts	280
Console	281
The EnScript Library	282
Filters	282
Accessing Filters.....	283
Starting and Stopping Filters	284
Creating a Filter	284
Queries.....	284
The View tab.....	285
The Include Tab	287
Chapter 19: Advanced Analysis	289
Recovering Partitions.....	289
Adding Partitions.....	289
Deleting Partitions.....	290
Recovering Folders from a formatted drive	290
Web Browsing History	291
Reading What the Subject Threw Away	293
Presenting Recovered E-mail	295
Making Sense of a DriveSpace Volume.....	298
Cracking Encrypted or Password Protected Files	299
System Snapshot.....	299
Volatile Data Defined	299
Volatile Data Components	300
Volatile Data Capture using Snapshot.....	301
Open Ports.....	301
Open Ports Columns.....	302
Active Processes	302
Processes Columns	303
Open Files.....	305

Network Interfaces and Users.....	305
Chapter 20: Foreign Language Support (Unicode)	309
Viewing Unicode Files.....	312
Unicode Fonts.....	314
Changing Font Size	317
Font Recommendations	318
Viewing Non-Unicode Files.....	319
Right to Left (RTL) Languages	321
Foreign Language Keyword Searches	322
Copying and Pasting.....	322
Character Map.....	323
Regional Settings	325
Foreign Language Bookmarking.....	326
Rich Edit Control in Bookmarks	327
More Information	328
Chapter 21: Restoring Evidence.....	329
Physical vs. Logical Restore.....	329
Preparing the Target Media	330
Physical Restore.....	331
To restore a drive, physically:.....	331
Logical Restore.....	333
Booting the Restored Hard Drive	334
Recommended steps for booting	334
Restore Questions	336
Chapter 22: Archiving Evidence.....	337
What Should Be Archived.....	337
After the Burn – Verify Evidence Files	338
Cleaning House.....	339
Chapter 23: Bookmarks.....	345
Understanding Bookmarks.....	345
Highlighted Data Bookmark.....	347
Notes Bookmark	352
Folder Information Bookmark	354
Notable File Bookmark.....	356
File Group Bookmark	360
Snapshot.....	363
Log Record	363
Registry Data Bookmark	366
New Documentation Options for Threads.....	366
New Bookmark Options	367
Move or Copy Bookmarks	370

Notable (Bookmarks view)	371
Chapter 24: The Report	373
Presenting the Findings.....	373
Reordering Bookmarks for Reports.....	380
Presenting Multiple Images	383
Exporting the Report	385
Documenting All Files and Folders Contained on Media	388
Presenting Search Results	389
Exporting to i2.....	393
Export to Xanlays' Quenza and Watson.....	394
Appendix A: EnCase Terminology	401
PC Hardware.....	401
"Storage" Computer/Media	401
"Subject" Computer/Media....	401
RAM.....	402
ROM	402
BIOS.....	402
Hard Drive Anatomy	402
Drive Geometry.....	402
Cylinder	402
Head.....	403
Sector	403
Track	403
Absolute Sectors	403
Platter	404
Drives, Disks and Volumes	404
Hard Drive Layout.....	406
Master Boot Record	406
Partition Table.....	406
Extended DOS Partitions	406
Volume Boot Sector	406
Inter-Partition Space	407
File System Concepts	407
Clusters	407
Cluster Bitmaps	407
Root Folder	407
File Entries	408
File Slack	408
Logical File Size.....	409
Physical File Size.....	409
RAM Slack	409
Volume Slack	409

File Systems	410
File Allocation Table (FAT).....	410
NTFS	410
EXT2/3.....	410
REISER	411
CDFS.....	411
HFS and HFS+.....	411
Palm	411
UFS	411
Disk Configurations Explained.....	411
RAID 0 Striping	411
RAID 1 Mirroring.....	412
RAID 5	413
Evidence Storage.....	414
Compression.....	414
MD5 Hash	415
CRC (Cyclical Redundancy Checksum).....	416
File Signature.....	416
Evidence Files Explained.....	417
Evidence File Format	417
Image Verification.....	418
EnCase Icon Descriptions	418
Appendix B: GREP	425
GREP Syntax.....	425
GREP Examples.....	426
Appendix C: EnScript Syntax	431
Language Overview	431
Declarations	432
Scope	432
Comments	432
Data Types.....	433
Integers.....	433
Floating Point.....	433
Enumerated Types	433
Strings	434
Dates	434
Operators.....	436
Unary Operators	436
Binary Operators	436
Ternary Operator	437
Operator Precedence	437
Prefix and Postfix	438

Program Control	439
Statements	439
Blocks.....	439
Conditionals	439
while Loops.....	439
do-while Loops	440
for Loops	440
break statement.....	441
Functions	441
Classes	442
Data Access.....	444
EntryClass.....	444
FileClass.....	444
Programs.....	445
Filters.....	446
EnScript Help	447
Appendix D: Third-Party Utilities.....	449
Quick View Plus.....	449
IrfanView.....	449
AC/DSee	450
DBXtract	450
MBXtract.....	450
Decode Shell Extension.....	450
Disk Compare	450
Mailbag Assistant.....	450
PST Cracker	451
OST2PST	451
Gpart	451
CD-R Diagnostic	452
Dir to Html	452
Appendix E: The Forensic Lab	453
Field Acquisitions	453
Lab Analysis.....	454
Need Additional Information?	455
Appendix F: Partition Types	457
ID Name	458
Index	477

Legal Notice

EnCase® License Agreement

Copyright

EnCase® version 4 is furnished under this license agreement (this “Agreement”) and may be used only in accordance with the terms of this Agreement. Copyright 1998-2004 Guidance Software, Inc. All Rights Reserved.

Definitions

PROGRAM is defined as the computer program “EnCase” including the software in executable form only and the single dongle hardware key with which this Agreement is included or remotely re-programmed by COMPANY, and any updates or maintenance releases thereto that COMPANY may provide to you. COMPANY is defined as Guidance Software, Inc., a California Corporation.

License and Certain Restrictions

This Agreement applies to both the trial and full versions of the PROGRAM. Do not use the PROGRAM until you have carefully read the following Agreement. This Agreement sets forth the terms and conditions for licensing of the

*Copyright © 2004 Guidance Software, Inc.
May not be copied or reproduced without the written permission of Guidance Software, Inc.*

PROGRAM from COMPANY to you, and installing the PROGRAM indicates that you have read and understand this Agreement and accept its terms and conditions. If you do not agree with this Agreement, promptly return the PROGRAM and accompanying items to COMPANY within ten (10) days of purchase for a full refund with receipt. Absent such return, the PROGRAM will be deemed accepted by you upon shipment.

Non-Exclusive License

- a. Authorized Use. You are granted a limited non-exclusive license to use a copy of the enclosed PROGRAM on the computer(s) used by a single individual. By your use of the PROGRAM pursuant to this Agreement, you recognize and acknowledge COMPANY's proprietary rights in the PROGRAM. You may not distribute the PROGRAM, including any demonstration version of the program, to third parties without the written authorization from COMPANY. You may copy the "EnCase.exe" and "En.exe" executables to create and verify EnCase® evidence files, but you may not make or distribute copies of such executables, or copies, including demonstration versions, of the PROGRAM, for use in conjunction with any third party software. You may make additional backup copies of the PROGRAM for your own use, as long as only one copy may be used at any one time. No copies or duplicates of the dongle hardware key may be made.
- b. Restrictions. You may not copy the printed materials, if any, accompanying the PROGRAM, or print multiple copies of any user documentation. Applicable copyright laws protect the PROGRAM in its entirety. The PROGRAM also contains COMPANY trade secrets, and thus you may not decompile, reverse engineer, disassemble, or otherwise reduce the PROGRAM to human-perceivable form or disable any functionality that limits the use of the PROGRAM. You may not modify, adapt, translate, rent, sublicense, assign, loan, resell for profit, distribute, or network the PROGRAM, disk, or related materials or create derivative works based upon the PROGRAM or any part thereof. You may not publicly display the PROGRAM or provide technical training or instruction for monetary compensation or other consideration in any form. Your license is automatically terminated if you take any of the actions prohibited by the paragraph.
- c. Transfer. You may not transfer the PROGRAM to a third party, or sell the computer on which the PROGRAM is installed to a third party, without written consent from COMPANY and written acceptance of the terms of this Agreement

by the transferee. If you transfer the PROGRAM with the written consent of COMPANY, you must transfer all computer programs and documentation and erase any copies residing on computer equipment. Your license is automatically terminated if you transfer the PROGRAM without the written consent of COMPANY. You are to ensure that the PROGRAM is not made available in any form to anyone not subject to this Agreement. A transfer fee of \$150 will be charged to transfer the PROGRAM (not applicable to transfers associated with orders from VARs, distributors, or resellers or intra-company transfers).

d. Title. At all times, full title and ownership of the PROGRAM shall remain with COMPANY. You are granted a non-exclusive license to utilize the PROGRAM subject to the terms of this Agreement.

Support

There are three separate levels of support available: (1) Standard Support, (2) Premium License Support Program (“PLSP”), annual payment option, and (3) PLSP, three-year payment option, which have the following terms:

Standard Support

As part of your license of the PROGRAM, you will receive one year of telephone and email support only in accordance with COMPANY’s standard telephone and email support policies. You are entitled to receive upgrades, if any, of version 4 of the PROGRAM only for one (1) year from the date of purchase. You have no rights to further upgrades other than those described herein. Support will begin upon the effective date of this Agreement, which is defined as the date the PROGRAM is licensed to you. After the initial year of support, you may elect to continue your support for a separate fee that will be stated at the then-standard support rates.

Premium License Support Program, Annual Payment Option

If you purchased PLSP, annual payment option, you have agreed to pay for three years of PLSP with three annual payments: the first annual fee upon purchase, the second annual fee on the first anniversary of your purchase, and the third annual fee on the second anniversary of your purchase. PLSP includes, for the entire three-year term, the Standard Support described above, as well as (i) any major releases of the Program (e.g., version 4 to version 5), and subsequent upgrades, if any, of such release, (ii) FastBloc® Software Edition (upon public release of such product by COMPANY), and (iii) any upgrades to EnCase®

Forensic Edition Modules (e.g., EnCase® Virtual File System, EnCase® Physical Disk Emulator, or EnCase® Decryption Suite).

Premium License Support Program, Three-Year Payment Option

If you purchased PLSP, three-year payment option, you have agreed to pay for three years of PLSP with one annual payment upon purchase. The features of PLSP are as described above.

EnScript® Macros WARNING

EnScript ® Macros are executable files and thus should be treated with the same caution as any other executable file received from a third party over the Internet or by other means. Like other executable files, it is possible to intentionally write EnScripts® Macros with malicious code or to imbed viruses within the code of an EnScript ® Macro. It is thus imperative that you identify and trust the source from which you receive an EnScript® Macro. As with any other file, EnScripts ® Macros received from third parties should be screened for viruses.

Disclaimer of Warranties

EXCEPT AS PROVIDED ABOVE, THIS PROGRAM AND ANY RELATED SERVICES ARE PROVIDED AS-IS, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, COMPANY DISCLAIMS ALL OTHER REPRESENTATION AND WARRANTIES, EXPRESS OR IMPLIED, REGARDING THIS PROGRAM, DISKETTE, RELATED MATERIALS AND ANY SERVICES, INCLUDING THEIR FITNESS FOR A PARTICULAR PURPOSE, THEIR QUALITY, THEIR MERCHANTABILITY, TITLE OR THEIR NON-INFRINGEMENT. COMPANY DOES NOT WARRANT THAT THE PROGRAM IS FREE FROM BUGS, ERRORS, OR OTHER PROGRAM LIMITATIONS. SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSIONS MAY NOT APPLY TO YOU. IN THAT EVENT, ANY IMPLIED WARRANTIES ARE LIMITED IN DURATION TO NINETY (90) DAYS FROM THE DATE OF PURCHASE OF THE PROGRAM. HOWEVER, SOME STATES DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY HAVE OTHER RIGHTS AS WELL, WHICH VARY FROM STATE TO STATE.

Limitation of Liability and Damages

THE ENTIRE LIABILITY OF COMPANY AND ITS REPRESENTATIVES (AS DEFINED BELOW) FOR ANY REASON SHALL BE LIMITED TO THE AMOUNT PAID BY THE CUSTOMER FOR THE PROGRAM AND RELATED SERVICES PURCHASED FROM COMPANY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, COMPANY AND ITS SUBSIDIARIES, AFFILIATES, LICENSORS, PARTICIPATING FINANCIAL INSTITUTIONS, THIRD-PARTY CONTENT OR SERVICE PROVIDERS, DISTRIBUTORS, DEALERS OR SUPPLIERS (COLLECTIVELY, “REPRESENTATIVES”) ARE NOT LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS OR INVESTMENT, OR THE LIKE), WHETHER BASED ON BREACH OF CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF COMPANY OR ITS REPRESENTATIVES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND EVEN IF A REMEDY SET FORTH HEREIN IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE. COMPANY WILL NOT BE SUBJECT TO LIABILITY FOR ANY BUGS OR DAMAGES CAUSED BY EnSCRIPT® MACROS, INCLUDING EnSCRIPT® MACROS INTENTIONALLY WRITTEN BY THIRD PARTIES WITH MALICIOUS CODE AND/OR COMPUTER VIRUSES. SOME STATES DO NOT ALLOW THE LIMITATION AND/OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. THE LIMITATIONS OF DAMAGES SET FORTH ABOVE ARE FUNDAMENTAL ELEMENTS OF THE BASIS OF THE BARGAIN BETWEEN COMPANY AND YOU. COMPANY WOULD NOT BE ABLE TO HAVE PROVIDED THIS PROGRAM WITHOUT SUCH LIMITATIONS.

Export Restrictions

You acknowledge that the PROGRAM is subject to export and import control laws of the United States of America and other countries. You agree that PROGRAM will be exported, re-exported or resold only in compliance with such laws. You represent and warrant that the PROGRAM shall not be used for any nuclear, chemical/biological warfare, missile end-use or training related thereto.

You also agree that it will not, without first procuring a BIS license or License Exception, (a) re-export or release the above PROGRAM to a national of a country in Country Code D:1 or E:2; nor (b) export to Country Groups D:1 or E:2 the direct product of the PROGRAM, if such foreign produced product is subject to national security controls as identified on the Commerce Control List (See General Prohibition Three Sec. 736.2(b)(3) of the Export Administration Regulations).

U.S. Government End Users:

The PROGRAM and software documentation are “Commercial Items” and “commercial software documentation,” as such terms are used in 48 C.F.R. 12.212 (SEPT 1995) and are provided to the Government (i) for acquisition by or on behalf of civilian agencies, consistent with the policy set forth in 48 C.F.R. 12.212; or (ii) for acquisition by or on behalf of units of the Department of Defense, consistent with the policies set forth in 48 C.F.R. 227.7202-1 (JUN 1995) and 227.7203-3 (JUN 1995).

General Provisions

This Agreement sets forth COMPANY's and its Representatives' entire liability and your exclusive remedy with respect to the PROGRAM. You acknowledge that this Agreement is a complete statement of the agreement between you and COMPANY, and that there are no other prior or contemporaneous understandings, promises, representations, or descriptions regarding the PROGRAM or any related services. This Agreement does not limit any rights that COMPANY may have under trade secret, copyright, patent, or other laws. The Representatives of COMPANY are not authorized to make modifications to this Agreement, or to make any additional representations, commitments, or warranties binding on COMPANY, other than in writing signed by an officer of COMPANY. Accordingly, such additional statements are not binding on COMPANY and you should not rely upon such statements. If any provision of this Agreement is invalid or unenforceable under applicable law, then it is, to that extent, deemed omitted and the remaining provisions will continue in full force and effect. The validity and performance of this Agreement shall be governed by California law (without reference to choice of law principles), except as to copyright and trademark matters, which are covered by federal laws. The parties specifically exclude the United Nations Convention on Contracts for the International Sale of Goods. This Agreement is deemed entered into at Los

Angeles, California, and shall be construed as to its fair meaning and not strictly for or against either party.

© 2003-2004 Guidance Software, Inc. All rights reserved. EnCase is a registered trademark and EnScript is a trademark of Guidance Software, Inc



215 North Marengo Avenue, Pasadena, CA 91101

Phone: 626.229.9191, Fax: 626.229.9199, <http://www.guidancesoftware.com>

*Copyright © 2004 Guidance Software, Inc,
May not be copied or reproduced without the written permission of Guidance Software, Inc.*

Preface

Thank you for purchasing EnCase Forensic. You will be utilizing the world's leading technology for computer investigations. EnCase Forensic Version 4 (hereafter referred to as "EnCase") is a court-validated solution used by law enforcement, government investigators, and corporate investigators worldwide. At Guidance Software, we continually strive to improve our product while at the same time adding more features, guaranteeing that you possess the best forensic software solution today as well as tomorrow.

Manual Organization

This manual is organized into five sections

- **What's New** - New features of EnCase Version 4
- **Acquisition** - Different options available to investigators to acquire media
- **Analysis** - EnCase features that can help you analyze acquired evidence
- **Documenting Evidence** - Bookmarks, reports, and how the former drives the latter
- **Technical Appendices** - Forensic terminology, detailed technical information, EnScript syntax, third-party resources, and more.

This manual is *not* a substitute for the training classes. To fully learn the EnCase Methodology, and to earn the prestigious EnCE certification, we encourage all users to attend our licensed training classes.

Minimum Recommended Requirements

For best performance, it is recommended that examination machines using EnCase have the following or better:

- EnCase security key
- Certificates for all purchased modules
- Current version of EnCase Forensic (updates are available for download from Guidance Software's web site at
<http://www.guidancesoftware.com/support/downloads.shtml#drivers>
- Pentium IV 1.4 GHz or faster processor
- 1 GB of RAM
- Windows 2000, XP Professional or 2003 Server
- At least 15 MB free hard drive space

Help Resources

GSI provides several different alternatives for users who need assistance. First and foremost is this manual. You should read this manual thoroughly to understand the product and its use. Before acquiring live evidence, be sure to run several "test" acquisitions and try different processes for examining the files.

GSI also provides assistance on our web site in the form of an on-line help system, as well as a message board where forensic specialists post questions and answers in various aspects of forensic investigation.

NOTE: It is imperative that you have your security key ID available when calling Guidance Software for Technical Support, Customer Support or Sales questions. Please use the area below to write down the dongle ID printed on your parallel or USB security key:

EnCase Forensic dongle serial number:

Technical Support

Guidance Software is committed to providing timely and effective technical support. Registered users receive free technical support, maintenance updates, and reduced pricing on updated versions. If you are unable to find an answer to your technical questions in this guide, please feel free to contact technical support using the following information

	North America	Europe
Phone	(626) 229-9191	44 151 255 1700 x303
Fax	(626) 229-9199	44 151 255 0345
Email	support@EnCase.com	Europe.support@EnCase.com
Hours of Operation	M-F 6:00am – 7:00pm (PST)	M-F 8:00am – 5:00pm (GMT)

When contacting Technical Support, please have the following information available:

- Your name, and the name of your organization
- Telephone number, fax number, and e-mail address
- The model of the computer, the operating system and version, the amount of memory, and the version of EnCase you are running
- Security key (dongle) ID number (available by selecting **About EnCase** from the **Help** menu)
- Detailed description of the problem. Describe any error messages exactly as they appear. Please list all of the steps and conditions that led to the problem. You may wish to create screen captures to e-mail to GSI

EnCase Message Boards

The EnCase message board (called the Users' Forum), the EnScript board, the Enterprise message board, and the Hardware message board are resources for the computer forensics community to exchange ideas, ask questions, and give answers. Discussions range from basic acquisition techniques to in-depth analysis of encrypted files and more. Thousands of our experienced and skilled EnCase users are registered on the message boards, reviewing posts every day, and can offer their expertise on all functionality of EnCase. The message boards are an invaluable resource for the forensic investigator. Please visit our website and look through the message boards for quick answers to your questions and tips from dedicated users.

You must register to access the message board. For message boards access, go to <http://www.guidancesoftware.com/support/messageboard/index.shtml>.

If you have any issues regarding the message board, please do not hesitate to contact Technical Support.

About Guidance Software

Guidance Software is the leader in computer forensics and incident response solutions. Founded in 1997 and headquartered in Pasadena, CA, Guidance Software has offices and training facilities in California, Virginia and the United Kingdom. More than 15,000 corporate and government investigators depend on EnCase software, while more than 3,500 investigators attend Guidance Software's forensic methodology training annually. Accepted by numerous courts and honored with eWEEK's Excellence Award and SC Magazine's Annual Award, EnCase software is considered the standard forensic tool. For more information, visit Guidance Software's Web site at <http://www.guidancesoftware.com>.

EnCase Forensic

EnCase Forensic is recognized as the standard computer forensic software used by more than 15,000 investigators and 40 of the Fortune 50. EnCase Forensic provides law enforcement, government and corporate investigators with reliable, court-validated technology relied upon by leading agencies worldwide for the past six years.

EnCase Enterprise

EnCase Enterprise is for computer investigators and information security professionals who need to investigate computer breaches and other incidents throughout the enterprise. EnCase Enterprise is a powerful network-enabled incident response and computer forensics system that provides immediate and thorough forensic analysis of compromised servers and workstations anywhere on the network and without disrupting operations. Without EnCase Enterprise, organizations must resort to cumbersome and insufficient manual processes using stand-alone utilities that extend the response and investigation process by several days if not weeks, and require subject systems to be taken out of service. This solution brings the highly successful and industry standard EnCase computer forensic technology to the enterprise for unprecedented incident response and investigation capability. EnCase

Enterprise represents best practices for immediate incident response and investigation of perimeter breaches and internal threats.

Guidance Software's Professional Development and Training

Law Enforcement Courses

Designed for Federal, State and Local Law Enforcement Investigators

Guidance Software has trained thousands of law enforcement officers from more than 50 countries. As the world's the largest computer forensics trainer, Guidance Software's courses feature master instructors from federal, state and local law enforcement agencies. Many instructors remain full-time investigators with world-renowned computer crime units, bringing real-life, first-hand investigation experience to every class.

The five law enforcement courses train students how to recover digital evidence using Guidance Software's court-accepted EnCase Forensic software. Often ending up in front of a judge and jury, students are taught not only how to gather, locate and analyze evidence, but also how to properly explain the results of the investigation in a thorough, professional manner. Courses incorporate these sound forensic practices with the award-winning capabilities of EnCase Forensic.

Computer Forensics and Incident Response Courses

Designed for IT Security Professionals, Litigation Support, Legal Professionals, and Forensic Investigators

Computer forensic investigators, network security professionals and internal computer incident response teams are being relied upon to manage incidents and mitigate risks. The same EnCase technology relied upon by law enforcement for years now serves as a vital internal tool for thousands of companies. Proper computer forensics training is crucial for corporate investigators.

Guidance Software offers three Computer Forensics and Incident Response courses specifically designed for security consultants, investigators and auditors in large enterprise networks. These courses train investigators and auditors how to use EnCase Enterprise and EnCase Forensics to investigate and respond to several types of incidents within their enterprise.

Expert Courses

Designed for Experienced Computer Forensic Investigators

Guidance Software's expert-level courses are designed for law enforcement and corporate investigators with significant computer forensics experience. Offering investigators an in-depth focus on file systems and advanced and advanced system artifacts recovery techniques, the expert-level courses utilize the vast capabilities of both the EnCase Forensic and EnCase Enterprise software solutions.

Guidance Software's Professional Services Group

Guidance Software's Professional Services Group provides unparalleled computer investigation support to clients and partners. This support enables immediate response to any scale of investigation or proactive audit. The Group's services leverage unrivaled computer investigation professionals, including talent drawn from leading law enforcement agencies and Fortune 500 companies.

Additional Corporate Services

GSI is continuously working to provide you with state-of-the-art cutting-edge computer forensic solutions. GSI offers the following services:

- Technical support available via email and telephone
- Forensic script macro tools
- Message Board / Users Group
- EnCase Legal Journal
- Legal resources pertaining to digital evidence

These services allow you to communicate with GSI and other users about the various capabilities of Guidance Software products.

*Copyright © 2004 Guidance Software, Inc,
May not be copied or reproduced without the written permission of Guidance Software, Inc.*



What's New: the new features of EnCase Version 4

Copyright © 2004 Guidance Software, Inc.
May not be copied or reproduced without the written permission of Guidance Software, Inc.

*Copyright © 2004 Guidance Software, Inc,
May not be copied or reproduced without the written permission of Guidance Software, Inc.*

Chapter 1

What's New in EnCase Version 4

Enhanced User Interface

The enhanced GUI greatly improves the ease of use of EnCase with selectable tabs and a consolidated Windows interface. Many of the floating dialog boxes have been replaced with windows that dock as tabs. The windows have been redesigned so that user interaction with each tab and view is more consistent. This uniformity greatly reduces the time spent adjusting to switched views. The different tabbed-windows are accessible through the **View** menu. They are **Cases**, **Bookmarks**, **Devices**, **File Types**, **File Signatures**, **File Viewers**, **Keywords**, **Search Hits**, **Security IDs**, **Text Styles**, **Scripts**, **Hash Sets**, **EnScript Types**, and **Encryption Keys**.

Tool-bar buttons appear as they are needed and disappear when they are not. This gives EnCase an uncluttered interface despite its additional features.

Keywords are global; they can be shared between all cases. Keywords are stored in the `keywords.ini` file. Investigators can categorize keywords into folders, making them quickly accessible to both new and existing cases. Investigators can now run keyword searches.

Cases are now displayed as separate folders under the **Cases** tab, simplifying multiple-case management. Correlation and corroboration of evidence between different cases is now much easier.

For example, an investigator wishes to review five recent cases to determine if they are connected. The investigator enters the appropriate keywords into the Keywords tab. Those keywords are now immediately available to all cases. The investigator can now start the search and search all cases at once. Using an older version of EnCase, the investigator would have had to type or import the keywords for each case.

A **Devices** tab has been added to each case. This replaces the version 3 **Evidence** view that was found in the bottom pane. The **Devices** tab provides a better interface for dealing with evidence that has been added to cases.

File Types and **File Signatures** are now displayed in two separate windows. The **File Signatures** table strictly establishes the link between file extensions and file signatures. The **File Types** table displays the name associated with file extensions as well as which viewers will open files of which type. The file type initially displayed is based on the extension. After a **Signature Analysis** has been run, the **Signature** column will populate with the appropriate information from the **File Signatures** table.

The **Security ID** window is associated with the file permissions feature explained below. Refer to the *NTFS File Permissions and Ownership* section for a detailed explanation.

The **EnScripts** window has been moved to the **View** menu. Refer to the *EnScripts* section for more information.

“Blue-checking” files has been enhanced. A user can now select or deselect a group of files in an upward or downward direction. Set the start point by selecting or deselecting a file (blue-check), then clicking on the last file in the range of included files while holding down the [**Shift**] key. With the range selected, *all* entries will be changed to the desired status, regardless of the previous status. For instance, if an investigator selects a range of 100 entries, all 100 entries will be instantly changed, regardless of whether there are blue-checked entries already present.

The user interface is covered in *Chapter 12: Navigating EnCase*.

Outlook .PST Files

Outlook is one of the most popular e-mail programs used for business today. The file format associated with Outlook is the .PST file. EnCase can read .PST files and extract e-mail for plain-text analysis. EnCase can handle .PST files that have both compressible encryption and full encryption, and can bypass .PST file passwords.

Outlook Express .DBX Files

Outlook Express is another popular e-mail program. EnCase can read the .DBX file format associated with Outlook Express files and extract e-mail for plain-text analysis. EnCase can handle .DBX files that have both compressible encryption and full encryption, as well as bypass .DBX file passwords.

Time Zone Support

Investigators who handle evidence from different time zones can find it difficult to track from which time zone an evidence file is associated. Furthermore, linking the different pieces of evidence together in a global timeline is a complicated task and prone to human-error. EnCase Version 4 allows the user to set the time zone settings for each item of evidence. All date and time stamp displays in each evidence file will then adjust to show the accurate date and time, without any additional user interaction. This feature eases the burden of timeline and time zone tracking for investigators.

Unicode Support

EnCase Version 4 fully supports Unicode. The Unicode standard provides a unique encoding number for every character, regardless of platform, computer program, or language. EnCase can now search and display any language that Unicode supports, as well as code pages.

Guidance Software is constantly localizing the user interface to other languages, such as German, Spanish, Japanese, French, Italian and Russian. Other languages will be announced as they are introduced.

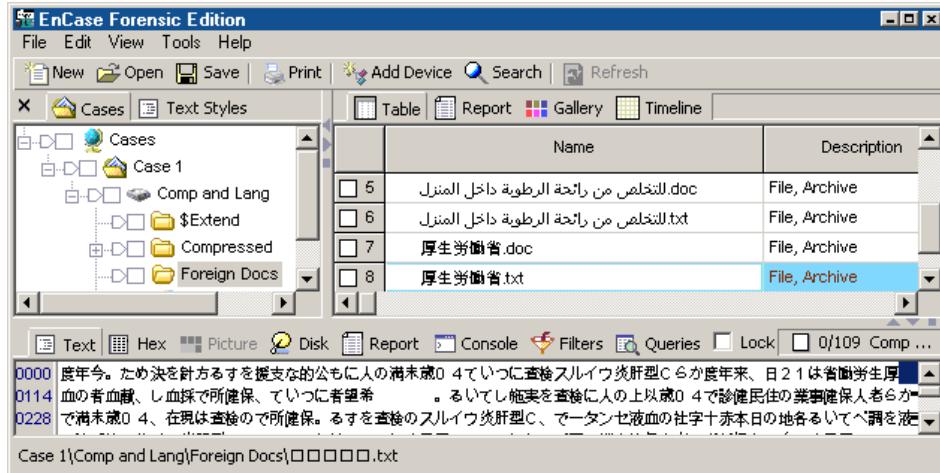


Figure 1-1 EnCase foreign language support

Advanced Search Algorithm

EnCase's search engine has been completely redesigned to increase search speeds and add multi-language support. EnCase Version 4 uses an advanced searching algorithm, which *dramatically* improves search time performance.

The new search algorithm reduces search times to a fraction of EnCase version 3 search times. For example, a 15-term keyword search conducted on a 1GB drive with EnCase Version 3 took over 13 minutes. The same search run with EnCase version 4 took only two minutes, almost $\frac{1}{7}$ the time.

EnCase Version 3			EnCase Version 4		
Hits	New	Keyword	Hits	New	Keyword
2353	2353	jeff	2353	2353	jeff
105	105	lecter	105	105	lecter
18	18	hannibal	18	18	hannibal
548	548	bomb	548	548	bomb
71	71	murder	71	71	murder
2384	2384	credit	2384	2384	credit
8722	8722	card	8722	8722	card
4881	4881	fake	4881	4881	fake
122	122	hacker	122	122	hacker
2	2	lolita	2	2	lolita
36	36	pedo	36	36	pedo
0	0	preteen	0	0	preteen
191	191	steal	191	191	steal
934	934	pipe	934	934	pipe
4593	4593	meth	4593	4593	meth

Figure 1-2 Keyword search results, version 3 and version 4

Dynamic Disk Support

Dynamic Disks are disk configurations created by Microsoft Windows 2000, XP or 2003 Server using the Disk Manager. The partition types available, which can be configured in multiple ways, are: Striped (RAID 0), Mirror (RAID 1), RAID 5 (Striped with parity), Spanned, and Basic.

EnCase can detect the disk(s) configuration and will attempt to rebuild the RAID by mapping all of the partitions. The boot area and the unused disk area of each disk will be available for further searching. In the case of a RAID 5 (striped with

parity), if one disk is missing, EnCase will use the parity to replace the missing drive and display all of the information for the volume.

NT 4.0 Disk Configuration Support

Windows NT uses a system for disk configurations that was the precursor to Dynamic Disks. The NT 4.0 system allows for the same configurations as above—RAID 0 (Striped), RAID 1 (Mirror), RAID 5 (Striped with parity), Spanned, and Basic partitions—but uses a different method to store the partition information. As with Dynamic Disks, EnCase can automatically map the disk configuration while preserving the other unused areas.

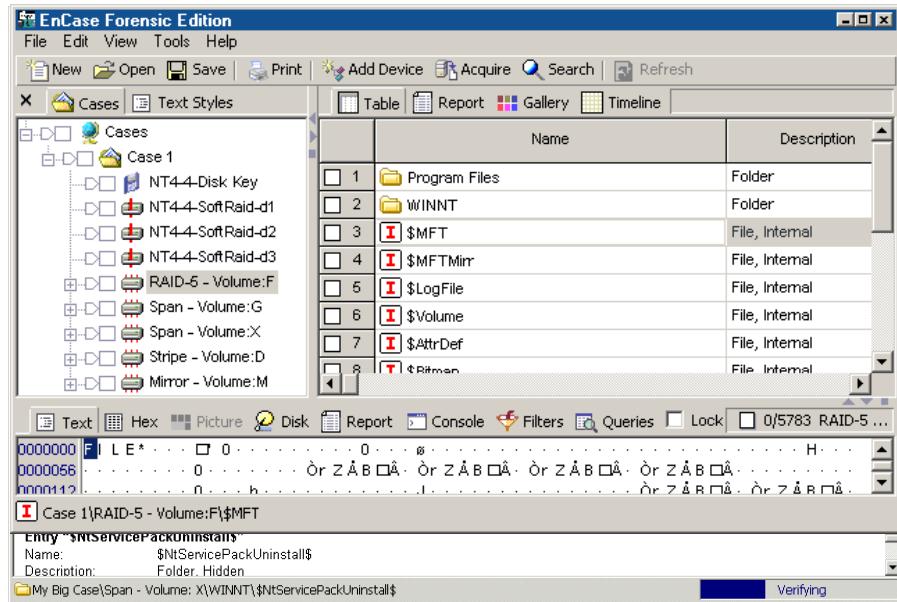


Figure 1-3 Disk configurations

NTFS and Unix File Permissions and Ownership

Every file and folder on an NTFS and Unix file system has an owner, a group, and a set of permissions. While this information is stored differently in various file systems, EnCase Version 4 extracts the data and displays a wealth of information for each file and folder.

EnCase will list the owner, the group, and permissions organized by owner or group.

If the file system associates a name with the security identifier, the name will be displayed in addition to the SID. However, most network accounts will exist on the network file-server, not the local machine. In these cases, EnCase will not be able to resolve the SID to a name. This explains the purpose for the Security ID option under the **View** menu mentioned above. The Security ID option allows an investigator to input the security ID numbers of any one account or all accounts on the network. EnCase will then use that list to resolve SID numbers to names.

NTFS Compression

The NTFS file system, available on Windows NT, 2000, XP and 2003 Server operating systems, is popular in the corporate infrastructure because of its security capabilities. One of the advanced features of the NTFS file system is the ability to compress a file or a folder, including all of the folder's contents.

When compression is used, the data on the hard drive is no longer in plain-text format, making it unreadable as text; however, when the file is viewed in Windows, the data appears correctly. Windows dynamically decompresses the data when accessed by an application, and then recompresses it for storage purposes. The compressed data stored on the hard drive is obtained during an EnCase acquisition. As a result, evidence within a compressed file might be overlooked.

EnCase Version 4 mounts all compressed files as virtual devices, causing the data to be represented in a decompressed form. The investigator can then apply all EnCase tools to the decompressed files.

Threaded Crash Protection

EnCase 4.18 and above includes threaded crash protection for corrupt image files. The corrupt image files will have a blank Picture display like other non-readable image files on the device. The case file will retain a record of the corrupt images that attempted to crash EnCase, so the images will not be attempted to be displayed in that case file again. The timeout for the thread trying to read a corrupt image file can be set in the **Global Options** menu. The case file cache of corrupt images can be cleared by right-clicking on the case file and choosing **Clear invalid image cache...**

Enhanced OLE File Support

Microsoft Word, Excel, PowerPoint, and many other applications use the OLE (Object Linking and Embedding) file format. There is substantial metadata stored inside some OLE files, such as the author of the file, the creation date, the edit time, the last print date, last revised date, “last saved by” username, company, links, and much more. This information, however, is not readily viewable. Previously, it had to be extracted manually. EnCase Version 4 can extract the information automatically when the file is mounted (**View File Structure** command).

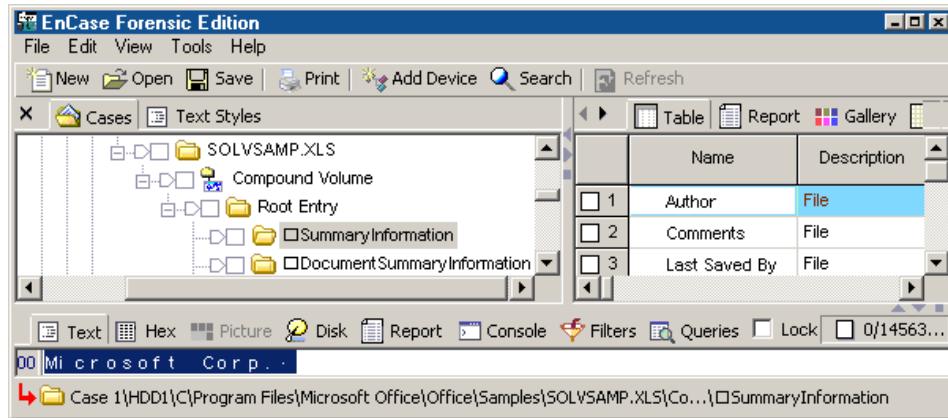


Figure 1-4 Mounting an OLE file

Filters and Queries

Filter functionality has been moved to the bottom pane to increase usability. The Compound Filter Query organizes filters in folders and runs them. Using this new feature, users can combine different filters easily together, quickly narrowing the number of files listed in the Table view. For example, running a query, filtering on JPG and GIF pictures 100K or larger that were created between 1/10/02 and 1/31/02 is now easily done by running the Compound Filter Query, which combines and builds simple filters together into more complicated filters.

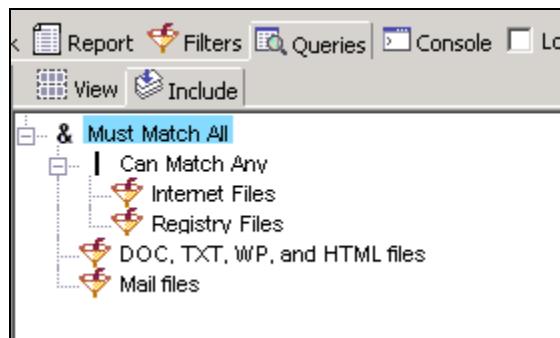


Figure 1-5 Combining filters

Enhanced EnScript Interface

The EnScript programming interface has been moved to the **View** menu. EnScripts now appear as a tab under the tool bar, and have a compile option for compiling without executing. Compiling an EnScript saves the script as well. Each open EnScript appears as a tab within the EnScript window, which permits several scripts to be open at the same time. EnScripts can be executed from either the ‘code pane,’ or the ‘tree pane.’ All default EnScripts have been updated to work with EnCase Version 4.

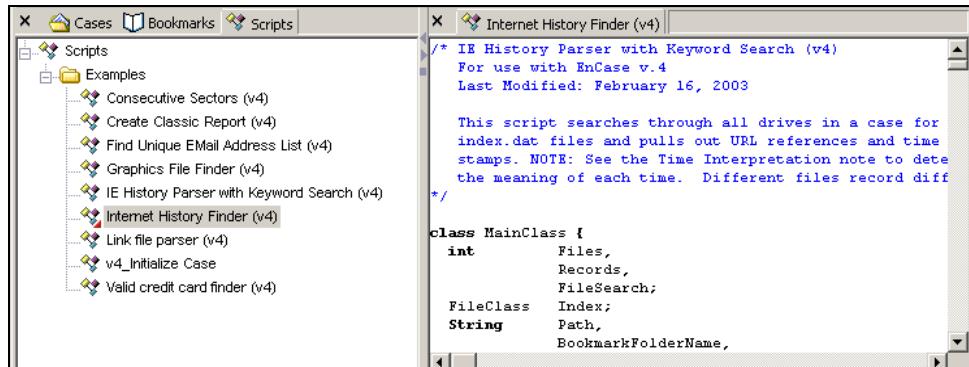


Figure 1-6 EnScript interface

Listed below is a description of some of the EnScripts included with EnCase:

- **Find Unique Email Address List (v4)** - This EnScript finds e-mail addresses while ignoring bad hits. The starting GREP expression for the EnScript is `[a-zA-Z#~\.\!\\\$%\^\&*()\\-]+@[a-zA-Z#\\.-]+\.\[a-zA-Z\\-\\.\]+`. After some additional processing, an internal EnCase function is called that further validates the e-mail address. This

EnScript will also allow the user to choose the output from all e-mails or only unique e-mails. If the unique option is selected, the EnScript will only list each e-mail address once, even if some reoccur.

- **File Finder (v4)** - This EnScript searches through unallocated clusters looking for a variety of file types, including AOL ART, BMP, EMF, GIF, JPG, Photoshop, PNG, TIFF, MS Word and Excel, Zip and GZip with the ability to specify custom file types. If the selected file types are located, the EnScript will bookmark the data into a specified bookmark folder or copy the files out.
- **IE History Parser with Keyword Search** - This EnScript will seek out all Internet Explorer History information (in allocated space) and write it out in HTML format, allowing the investigator to quickly and easily investigate the same sites that the Subject visited. It is also possible for the investigator to display only Internet history containing specified keywords.
- **Link File Parser** - This EnScript quickly displays Link file information. Link files show which files were recently accessed and provide information on files that came from external media. The link parser reads all forms of link files and formats the results in the bookmark view.
- **Valid credit card finder** - This EnScript will bookmark valid VISA, MasterCard and AmEx numbers. All valid CC hits will be bookmarked in the folder "All CC Hits". The first occurrence of each CC hit will be bookmarked in "Unique CC Hits".
- **Parse wtmp files** - This script parses wtmp, utmp, wtmpx, utmpx Unix and Sun Solaris log files.

Enhanced Linux / Unix File System Handling

This enhancement will add additional functionality to the existing code that handles the EXT2 and Unix file systems, including a listing of file ownership and permissions. Additionally, hard links will be identified.

Additional File System Support

EnCase continues to expand the number of supported operating and file systems. As of version 2.0, EnCase can interpret FAT12, FAT16, FAT32, NTFS, EXT2/3 (Linux), HFS (Mac), HFS+ (Macintosh OS X Server operating system, which uses the Hierarchical Files System Plus (HFS+) without the wrapper of HFS), UFS (Unix), Reiser, Sun Solaris, JFS and JFS2 (AIX), Palm, CDFS, Joliet, UDF, and ISO 9660 (CD-ROM), and Open, Free, and Net BSD (Berkley Software Distribution) operating systems and the underlying Fast File System (FFS).

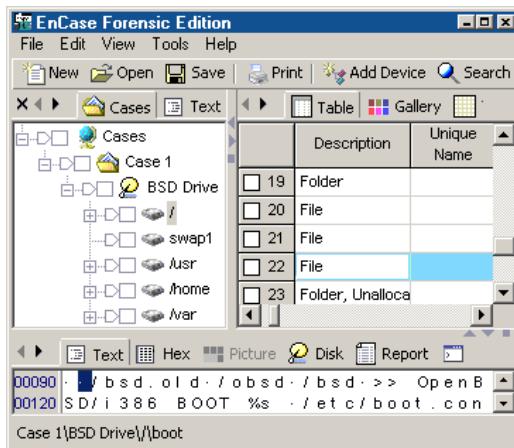


Figure 1-7 OpenBSD file system support

In addition, EnCase now has better support of the Mirror RAID (RAID 1) configuration of NTFS Dynamic Disks often found on Compaq Windows servers. If only one of the mirrored drives is present, the file structure will still be available for examination.

Enhanced Windows Registry Mounting

This enhancement will increase the speed with which Windows registry files are mounted. It will also find deleted registry keys for Windows 95 and 98.

EnCase Modules and Extensions

A number of powerful investigative modules are available to help examiners with their investigations. The modules require the purchase of a certificate from

Guidance Software sales department, at (626) 229-9191, to activate the investigative functions.

EnCase EDS Module

The EnCase Decryption Suite (EDS) Module allows examiners to decrypt files and folders protected by **local** and **domain** authenticated users with Microsoft® EFS. The module works with operating systems capable of encrypting data with EFS, including Windows 2000 Professional, 2000 Server, XP Professional, and 2003 Server. For Windows 2000, EFS files and folders can be decrypted automatically. For Windows XP and 2003 Server, the user password must be obtained. The EDS Module is available in EnCase 4.18 and above.

Details on using the EDS Module are contained in the EnCase EDS Module manual, available for download at www.guidancesoftware.com.

EnCase VFS Module

The EnCase Virtual File System (VFS) Module allows examiners to mount computer evidence as a **read-only, off-line network drive** for examination through Windows Explorer. The power of this feature has been well articulated in many forums. Most notably, this provides the examiners many options in their examinations, including the use of third-party tools with evidence served by EnCase. The VFS Module is available in EnCase 4.18 and above.

All computer evidence and image file formats supported by EnCase can be mounted with VFS, including:

- EnCase Evidence Files
- dd images
- SafeBack® v2 images (support by license from New Technologies, Inc.)

Live computer forensic evidence supported by VFS includes:

- Local machine preview of removable media
- Local machine preview through FastBloc Classic, FE, and LE hardware blockers
- Cross-over network cable preview
- Parallel Port preview
- Local Palm Pilot preview
- EnCase Enterprise and Field Intelligence Model live network preview

All file system formats supported by EnCase can be mounted with VFS in Windows Explorer, including:

- Windows (FAT 12/16/32, NTFS, DOS)
- Linux (EXT2, EXT3, Reiser)
- Unix (Solaris UFS)
- Macintosh (HFS, HFS+)
- BSD (FFS)
- CD/DVD (Joliet, ISO 9660, UDF, DVD)
- Palm (Palm OS)

The VFS Server Module is also available, which allows examiners to serve the mounted virtual drive to other examiners, or case agents, attorneys, etc, on the local area network for review in Windows Explorer.

Details on using the VFS Module are contained in the EnCase VFS Module user manual, available for download at www.guidancesoftware.com.

EnCase PDE Module

The Physical Device Emulator (PDE) can mount a remote evidence file as an emulated local drive. The VMware Workstation can be used to boot images of hard drives mounted with PDE on the examiners machine. This also provides examiners with the capability of sharing evidence files that have been accessed remotely.

Once mounted the read only media is available to any native applications, Windows Explorer, or any third party Windows utility or computer forensic tool that does not recognize network drives, but does recognize local devices. The mounted media can be investigated and manipulated as follows:

- File Carving Utility
- Virus checker
- Spyware detector
- Trojan detector
- Steganography detector
- Word Indexer
- Undelete software
- Encryption detection software

Additional information is available in the PDE User's Manual.

EnCase NAS Extension

The EnCase Network Authentication Server (NAS) Extension provides examiners with flexibility in managing EnCase licenses on one Aladdin Net HASP security key (dongle). The EnCase NAS provides EnCase licenses in three ways:

- A local user can use an EnCase license on the examination machine with the Net HASP key to conduct examinations
- A remote user can use Terminal Services to log onto the examination machine with the Net HASP key to conduct examinations
- Any licenses not used by local or Terminal Service users on the examination machine can be served to other examiners on the LAN subnet through the UDP protocol.

The NAS allows laboratories to have one Net HASP key to manage all EnCase licenses from a single machine, thus eliminating the issue of lost or unused keys. An Aladdin HASP for EnCase v4 can be upgraded to Net HASP key.

Instructions on installing the Aladdin Net HASP software and the Aladdin management software are available for download at www.guidancesoftware.com. The EnCase NAS is available in EnCase 4.18 and above.

SafeBack 2.x Support

EnCase 4.18 and above provides licensed support for SafeBack 2.x image file format. To add a SafeBack image to a Case file, use the **Add Device** function described in *Chapter 13: Navigating EnCase*. A SafeBack image is added to a Case file in the same manner as an EnCase Evidence File.

Security Key

EnCase Forensic requires a security key to run in full operation. A security key is a device that attaches to a computer to control access to a particular application. Security keys provide the most effective means of copy protection. The EnCase security key attaches to either a PC's parallel or USB port. Without a security key attached to the Storage computer (the investigator's computer), acquisition of evidence is possible but not analysis. This is termed "Acquisition Mode".

In EnCase for DOS, media may be acquired without having a security key plugged into the machine. EnCase can be installed on multiple computers to perform multiple acquisitions at the same time. Analysis can only be performed on the computer with the security key.

Security keys contain EEPROM chips that can be quite sensitive to over-voltages and static. Shield the security key when it is not in use by keeping it in the pink anti-static pouch provided.

The Parallel Port Security key

The parallel port security key connects through the parallel port for machines that do not have a USB port. The parallel port security key does require drivers to function properly. Please see *Chapter 1: Installing EnCase* for security key installation instructions. The parallel port security key is not a Plug-and-Play device—the computer should be powered off when inserting or removing the security key.

Plug the security key into the parallel port first when a Zip drive or printer is sharing the parallel port with the security key. This prevents the high external voltages from burning out the security key.

When using the Parallel port cable preview \ acquisition feature in conjunction with a parallel port security key, the security key must first be plugged into the parallel port of the investigating forensic computer running Windows. Plug the parallel cable into the security key, and finally, plug the other end of the cable into the suspect computer.

Certain printer software drivers can also interfere with security key detection. If EnCase does not detect the security key properly, check to see if a printer driver is installed that interferes with EnCase. An icon in the lower-right corner of the screen will indicate that such a driver is present. If this is the case, remove the driver and reboot the computer. Removing this driver will not affect the ability to print.

The USB Security key

The USB security key plugs into the USB port, freeing the parallel port for printing and previewing. Drivers must be installed prior to inserting the USB security key. Once installed, the security key can be moved between computers. Please refer to *Chapter 1: Installing EnCase* for USB security key installation instructions.

Chapter 2

Installing EnCase

The EnCase Installation CD and Autorun

The EnCase Installation CD is set to Autorun in Windows, when the installation CD is placed in the CD-ROM drive. If the Autorun feature is turned off, start Windows Explorer, maneuver to the CD-ROM icon and double-click on **SETUP.EXE**.

The CD Installation Menu and Contents

Install EnCase	Installs EnCase Version 4
Install Security Key Drivers	Installs the latest Aladdin Security Key drivers
View PDF Manual	The User Manual in Adobe Acrobat PDF format
View White Papers	Guidance Software's white papers
Visit Guidance Software	Direct link to Guidance Software's web site
Install Adobe Acrobat	Installs Acrobat Reader 5.0 to read PDF documents

Also included on the CD, but NOT listed in the menu are:

DriverInfo.htm The latest information from Aladdin on installing drivers for the Aladdin security key.

iview336.exe The latest version of Irfanview, a freeware graphics viewer that can be set up as an external file viewer within EnCase. Updates are available at www.irfanview.com.

Security Key Drivers Installation

1. Insert the EnCase CD-ROM into the CD-ROM drive. If you do not have the CD available, you can download the driver from <http://www.guidancesoftware.com/support/downloads/dongle/HDD32.zip>. When the file is unzipped, you can run the executable (**hdd32.exe**) and then skip to **Step 4**.
2. If Autoplay is enabled, the EnCase splash screen should automatically appear after a few seconds.
3. Click on the link for **Security Key Drivers** that appears in the splash screen.

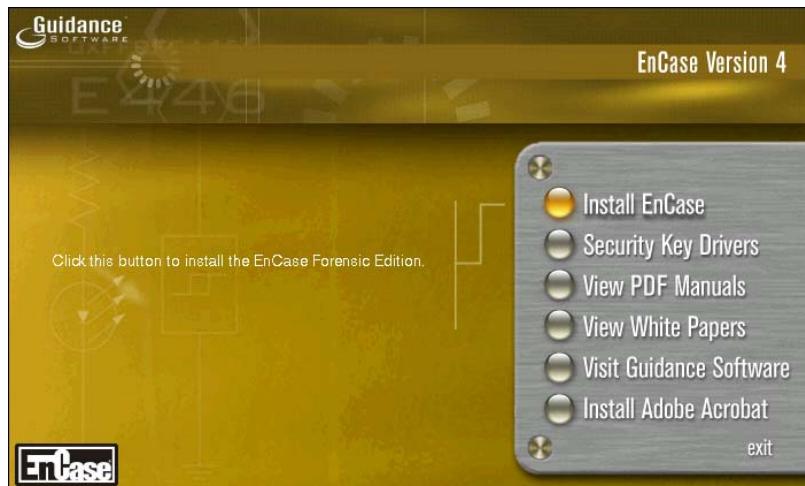


Figure 2-1 EnCase CD Autoplay window

4. Click [**Next >**] when presented with the HASP installation screen. The necessary files will be copied to the hard drive.

Copyright © 2004 Guidance Software, Inc
May not be copied or reproduced without the written permission of Guidance Software, Inc.

5. Click [**Next >**] at the summary screen.
6. When the screen indicates that the installation is complete, click [**Finish**].
7. Unless you are running Windows XP Service Pack 2, skip to **Step 15**. For Windows XP Service Pack 2 users, you will need to install the command line security key drivers. Download the driver executable from <http://www.guidancesoftware.com/support/downloads/dongle/Haspdinst.zip> to the hard drive.

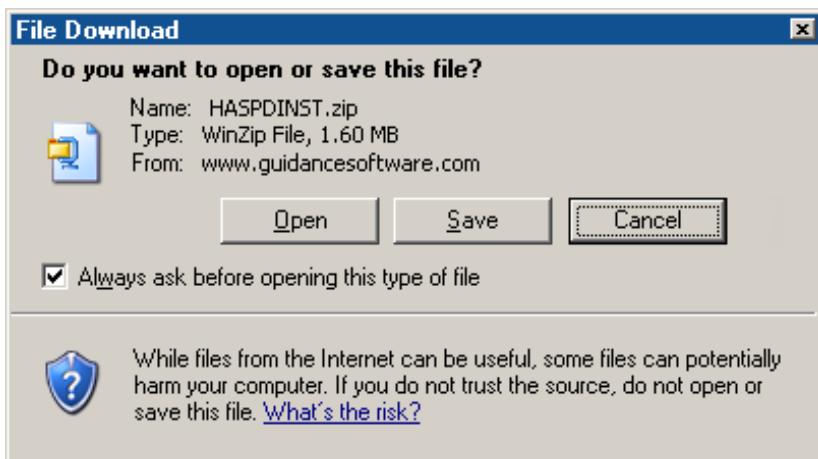
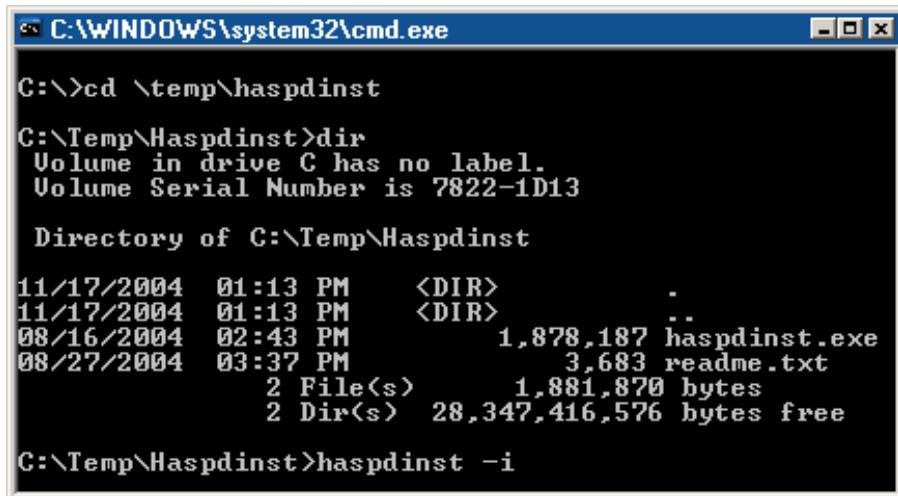


Figure 2-2 Saving the security key driver locally

8. Unzip the file you just downloaded - it will create a folder called **haspdinst** in the folder where the WinZip file was saved.
9. From the [**Start**] menu, select **Run** and type **cmd** in the **Open:** field, then click [**OK**]
10. Change directories to the location of the executable by typing **CD C:\FOLDER\Haspdinst**

11. At the command prompt, type **haspdinst -i** to install the dongle drivers.



```
C:\>cd \temp\haspdinst
C:\Temp\Haspdinst>dir
 Volume in drive C has no label.
 Volume Serial Number is 7822-1D13

 Directory of C:\Temp\Haspdinst

11/17/2004  01:13 PM    <DIR>
11/17/2004  01:13 PM    <DIR>
08/16/2004  02:43 PM           1,878,187 haspdinst.exe
08/27/2004  03:37 PM           3,683 readme.txt
                  2 File(s)     1,881,870 bytes
                  2 Dir(s)  28,347,416,576 bytes free

C:\Temp\Haspdinst>haspdinst -i
```

Figure 2-3 Installing the drivers

12. A status window will appear indicating that the driver is loading. This will disappear when the driver has loaded.



Figure 2-4 Status window

13. Once the driver load is complete, a status message will appear stating that the operation was successful. Click the [OK] button.



Figure 2-4 Completing driver load

14. Power down the computer, insert the security key and boot up the system.



NOTE If the security key is inserted before Step 7, EnCase will launch in Acquisition Mode, disabling the ability to preview and see file structure but allowing evidence acquisition.

If there are problems with the installation, please go to the troubleshooting page on our web site <http://www.guidancesoftware.com/support/articles/hasp.shtm>

Installing EnCase Version 4

1. Insert the EnCase CD into your CD-ROM drive. If you do not have the CD available, you can download the driver from <http://www.guidancesoftware.com/support/EnCaseEnterprise/version4/lgn.asp>. When the downloaded file is unzipped, you can run the executable and then skip to **Step 4**.
2. If Autorun is enabled, the EnCase splash screen should automatically appear after a few seconds.
3. Click on the **Install EnCase** button.
4. At the EnCase screen that reports the version being installed, click on the [**Next >**] button.



Figure 2-5 EnCase version window

5. You will see a License Agreement screen. You must agree to the terms of the license agreement to proceed with the installation. Click on the **I Agree** radio button, then click [**Next >**]

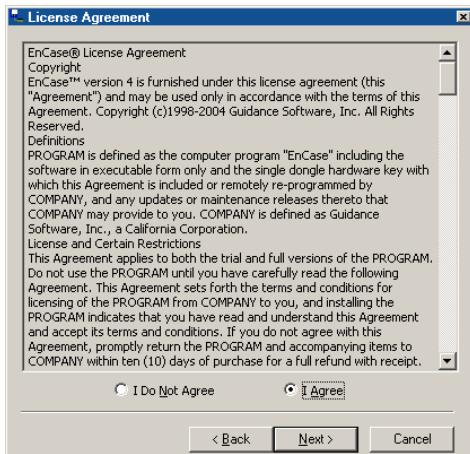


Figure 2-6 EnCase license agreement

6. The install dialogue box (Figure 2-4) will appear. You can change the directory into which EnCase installs by clicking on the ellipsis box to the right of the Install To field, but it is recommended that you use the default directory (C:\Program Files\EnCase4). Click [Finish] to install EnCase.

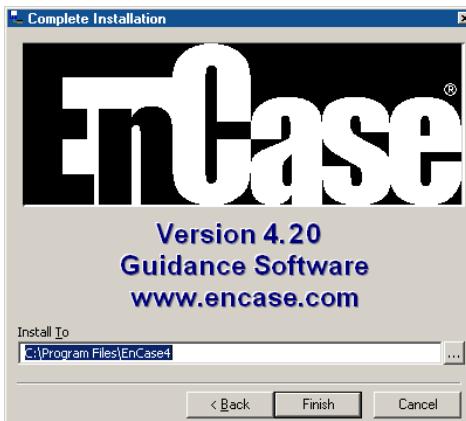


Figure 2-7 EnCase install dialog box

7. The EnCase installation will create a program icon on your desktop.

*Copyright © 2004 Guidance Software, Inc
May not be copied or reproduced without the written permission of Guidance Software, Inc.*

8. Once EnCase is installed, reboot the computer. *Make sure that you perform a complete system reboot and not a log off/log on.* If necessary, manually shut down the system down to a power off, then power up and complete the routine logon procedure.
9. To run EnCase, double-click on the desktop icon or from the **Start** menu and select **EnCase** under **Programs**.

Software Updates

EnCase is continually being refined and updated in response to user requests. Minor updates and fixes are available on our website.

To download the latest EnCase Version 4 update:

1. Open Internet Explorer (or your favorite browser) and navigate to <http://www.guidancesoftware.com/support/downloads.shtm>.
2. Click on the download link for the appropriate upgrade. Take care to get the correct language version, and edition (Enterprise and Forensic editions are both available from the same download page, but require a different username and password).
3. Enter the required user name and password, and then click on the **Send** link. The user name and password are the same for all users in a multiple license order; this can be found on a separate sheet of paper inserted into this manual, but if you have misplaced the username and password, please contact Guidance Software Technical Support at 626-229-9191. Note that the username and password are case sensitive.
4. Click on the appropriate download link; when the File Download pop-up window appears, click on the [**Save**] button.
5. Make note of the directory where you are saving the executable, then click on the [**Save**] button.
6. When the executable has finished downloading, you can click on the [**Open**] button, or find the executable and double-click on it to install it.
7. Follow steps 4-7 of the *Installation Instructions* above.



NOTE When updating an existing installation, for best results perform a clean install. Export any viewers, filters, keywords, etc. you have created to a text file, then remove the EnCase directory (typically C:\Program Files\EnCase4) prior to updating. The update is a full version and does not require a previous version to be installed. You can opt to install to a different folder if you wish to keep older versions of EnCase intact.

All older evidence files and Version 4 .CASE files will be interpreted by the upgrade, however, version 3 .CAS files will not open in version 4 and vice versa. Evidence files will open in any version of EnCase regardless of the version used to acquire them.

Configuration Questions

1. What systems will EnCase run on?

- You can acquire evidence with any PC that can run DOS or Windows versions Windows 98 and higher.
- You can examine evidence files only on Windows 98, ME, 2000, NT, XP or 2003 Server PCs.

2. What is the optimal PC configuration to run EnCase for Windows on?

- See *Appendix E: The Forensic Lab*.

3. What file systems does EnCase Version 4.20 support?

- EnCase can interpret FAT12, FAT16, FAT32, NTFS, EXT2/3 (Linux), HFS and HFS+ (Mac and PowerMac), FFS (BSD), UFS (Unix), Reiser, Sun Solaris, JFS and JFS2 (AIX), Palm, CDFS (CD-ROM), Joliet, UDF, and ISO 9660.
- If EnCase does not recognize the file system on the drive (HPFS for example), it will show unrecognized file system as an "unallocated cluster" file. Keyword and file-header searches are still possible, as is the ability to create bookmarks, but file names or folder structures will not be available. EnScripts can be executed against these file-systems as well.

Security Key Questions

- 1. When I run EnCase for Windows, I cannot see file structure, and the title bar reads “EnCase Acquisition Edition”, yet my security key is plugged into the USB port / parallel port of my PC.**
 - Are the drivers for the USB security key installed? Please follow the directions to properly install the security key drivers.
 - Are you using a parallel port security key with a printer attached? Certain printer monitoring software can cause conflicts with the parallel port security key. Try uninstalling any printer monitoring software and rebooting.
 - In some cases, USB security keys fail for no apparent reason. This can often be traced to a hardware conflict between a SCSI card and the second IDE channel. Try removing devices or the SCSI card.
 - The security key could be defective. To determine if this is the case, please call or e-mail our technical support department at 626-229-9191 or support@guidancesoftware.com.
- 2. If I purchased a parallel-port security key, can I exchange it for a USB security key (or vice-versa)?**
 - The parallel-port security key can be exchanged for a USB security key (or vice versa) at any time by contacting Guidance Software’s Customer Service at customerservice@guidancesoftware.com. The cost for the exchange is \$30.00 plus shipping. When contacting Customer Service, please have your order number. This number is located by accessing the About EnCase option from the Help menu in EnCase. You will be sent an RMA form to complete and return to Customer Service. After payment is received, Guidance Software will send you a new security key. Upon receipt, the original security key must be shipped back to Guidance Software using the RMA form included in your Version 4 package. If the original security key is not returned within 10 business days, you will be charged for the full amount of the software.



Acquisitions

Chapter 3:
Creating the EnCase Boot Disk

Chapter 4:
EnCase for DOS

Chapter 5:
Previewing vs. Acquiring

Chapter 6:
Parallel port Cable Acquisition

Chapter 7:
Crossover Network Cable Acquisition

Chapter 8:
Drive to Drive Acquisitions

Chapter 9:
FastBloc Acquisitions

Chapter 10:
Acquiring Disk Configurations

Chapter 11:
Acquiring Palm PDAs

Chapter 12:
Acquiring Removable Media

Copyright © 2004 Guidance Software, Inc.
May not be copied or reproduced without the written permission of Guidance Software, Inc.

*Copyright © 2004 Guidance Software, Inc,
May not be copied or reproduced without the written permission of Guidance Software, Inc.*

Chapter 3

Creating the EnCase Boot Disk

Before starting a DOS acquisition, you should first create an EnCase Boot Disk. The EnCase Boot Disk is used to safely acquire digital media in DOS when a forensically sound acquisition in Windows is not possible.

Windows Acquisition Issues

Windows will write to any local hard drive that it detects, sharing such files as the Recycle Bin and desktop.ini files. Last Accessed dates and times will be changed, thus tainting the evidentiary integrity of the subject drive. Forensically sound acquisitions in Windows are not possible unless special hardware write blocking, such as FastBloc, is used.

DOS, which is a 16-bit operating system, allows forensically sound acquisitions (write blocking) without specialized hardware. For that reason, whether acquiring (using the barebones boot disk) or previewing (using the EnCase Network Boot Disk, or ENBD), computer forensic investigators will need an EnCase Boot Disk which uses DOS rather than Windows.

Creating the EnCase Boot Disk

An EnCase Boot diskette is used to boot the subject and / or storage computer to DOS. The support files on these disks have been modified to allow the diskette to boot to a non-writable state. The diskettes are used throughout the forensics process and are referred to throughout this manual. Follow the steps below to create this diskette.



NOTE There are two types of EnCase Boot Disk: the barebones boot disk (described here), and the EnCase Network Boot Disk (ENBD), detailed later in this chapter. The ENBD has the features of the barebones boot disk, but also allows for parallel and crossover cable previews \ acquisitions.

Steps to Create the EnCase Barebones Boot Disk

10. Open an Internet browser and download the barebones boot disk image (<http://www.guidancesoftware.com/support/downloads/packets/bootfloppy.E01>), saving the bootfloppy.E01 file to the root EnCase directory (typically C:\Program Files\EnCase4)
11. Launch EnCase for Windows.
12. From the **Tools...** menu, select **Create Boot Disk...**



Figure 3-1 Create Boot Disk option

13. Put a diskette in the floppy drive (it does not need to be blank, but all data on the diskette will be overwritten). Make sure the radio button for the appropriate floppy drive (in most cases, **A**) is selected, and then click on the [**Next >**] button.

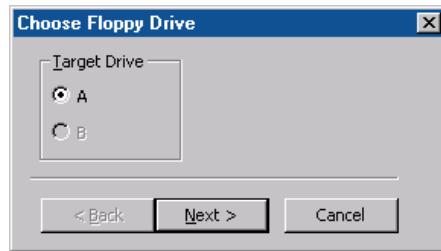


Figure 3-2 Select floppy drive

14. The next screen that appears provides several formatting options via radio buttons:

- **Update existing boot floppy** - This option allows you to upgrade an existing EnCase boot disk (e.g., upgrade an EnCase version 4.16a boot disk to EnCase version 4.20)
- **Overwrite diskette with a boot floppy base image** - This option takes the EnCase boot disk image (bootfloppy.E01) and creates a boot disk from it. If a boot disk image of a different name is used, or is located somewhere besides the default location (C:\Program Files\EnCase4), you can specify the correct path or name by clicking on the ellipsis box to the right of the **Image path** field and browsing to the appropriate file and location. Select this option to create the boot disk as described in these steps, and then click [**Next >**].
- **Change from a system diskette to a boot floppy** - This option allows the io.sys and command.com files on a pre-existing boot-floppy to be altered so that the hard drive's io.sys and command.com are not accessed at boot. Use this option only if a Windows 98 version of DOS is used.

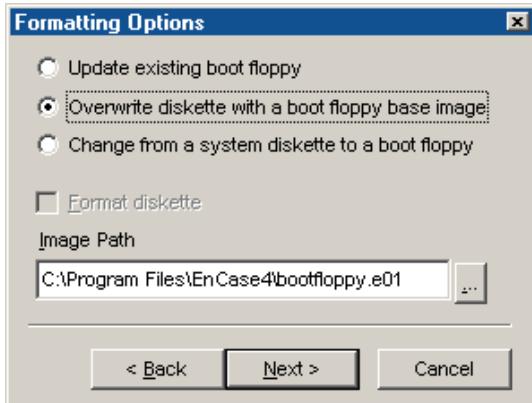


Figure 3-3 Select format option

6. The **Copy Files** screen provides the capability of copying specific files (such as the EnCase DOS executable file, EN.EXE) to the floppy during the build process. This can also be done manually by clicking [**Finish**] and doing a copy via Windows Explorer or through the DOS COPY command. To add the file during the boot disk creation process, right click in the **Update Files** window and select **New**.



NOTE If this file has been copied using the menu option previously, the path will appear in the **Update Files** window. If this is the case, skip this step, select the file, click [**Finish**] and proceed to Step 8.

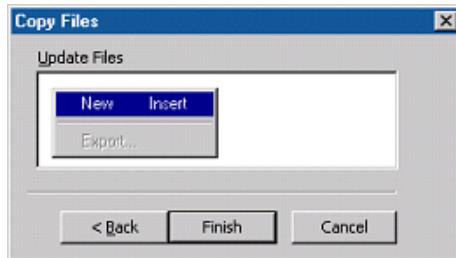


Figure 3-4 Specify files to copy

7. Browse to find and select the current EN.EXE, and then click [**Open**].

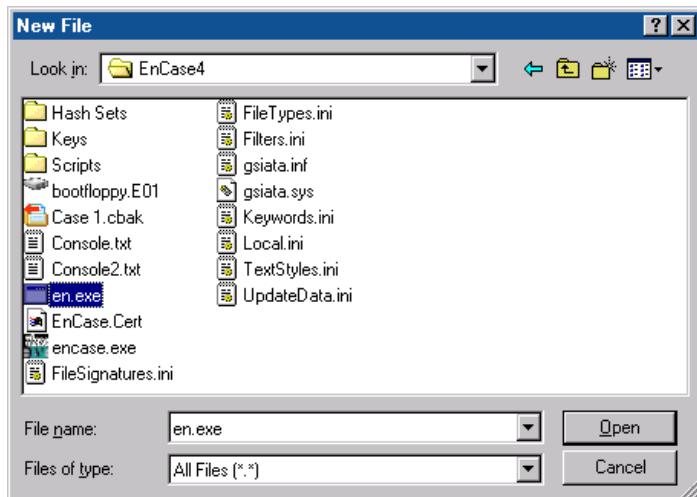


Figure 3-5 Find and select EN.EXE

8. The path with the EN.EXE file will populate the window and be highlighted in blue. Click [**Finish**] to complete the disk creation process.



Figure 3-6 Copying files

9. When prompted that the disk was successfully created, click [**OK**].

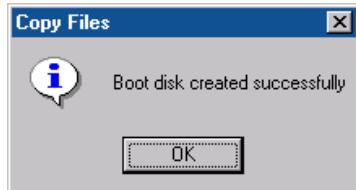


Figure 3-7 Successful disk creation

10. Eject the EnCase Boot Disk and label it accurately.
11. Be sure to test the new disk on a machine without drives that will be used as evidence, going by the guidelines set forth in the following section.

Booting a Computer with the EnCase Boot Disk

Because of the uncertainty of a suspect machine's configuration, the process of booting the machine can be the riskiest part of the investigation. One mistake can lead to the accidental booting of the hard drive, which breaks chain-of-custody procedures and may alter or destroy evidence. A complete description of the boot process is beyond the scope of this manual, but the following guidelines will help aid the investigator to safely boot most PCs.

1. Confirm that the subject computer is powered off. Most power switches are "soft" switches, meaning that pressing them will begin a software-controlled shutdown process. The best method for shutting down an **inactive** computer is to pull the power cord plug from behind the back of the computer.
2. Open the computer and inspect the inside for unusual connections or configurations. It is not unheard of for a computer to house a disconnected hard drive.
3. Disconnect the power cables to all the resident hard drives.
4. Insert the EnCase Boot Disk and turn on the computer.
5. Run the CMOS (BIOS) setup routine to ensure that the computer is set to boot from the floppy drive. Most systems display the correct setup key on the screen as the system boots. If not, the following is a list of common setup keys:

Compaq Computers: [F10]

IBM Computers: [F1]

IBM-compatible (clones) [Delete]; may be [F2], [Ctrl][Alt][Esc] or [Ctrl][Alt][Enter]

15. Verify that the computer is set to boot from the floppy drive by reviewing the boot order settings. Note any changes made and remember to restore the settings at the end of the investigation.
16. Exit the BIOS setup and save changes.

17. Allow the computer to continue to boot from the floppy. Confirm that a boot from the floppy is possible. You may wish to attach a storage drive at this time to see if the system tries to boot from the hard drive.
18. Power off the computer and reconnect the disk drive power cables.
19. Confirm that the EnCase Boot Disk is still in the drive and turn on the computer, allowing the computer to boot from the floppy disk.

EnCase Network Boot Disk

One way to preview and acquire media when hardware write blocking is unavailable is using the crossover or parallel cable acquisition method (detailed in *Chapter 20, Network Cable Acquisitions*.) In order to perform this type of acquisition, you will need to create an EnCase Network Boot Disk (ENBD). The various ENBD creation utilities are available from links in an article downloadable from Guidance Software's website at (<http://www.guidancesoftware.com/support/articles/networkbootdisk.shtml>). Detailed instructions, including which ENBD utility to download and how to do a network crossover\acquisition, are included. The ENBD is capable of auto-detecting network interface cards, as well as allowing the user to specify which network card to load drivers for. If the user allows the ENBD to auto-detect the card, the appropriate DOS driver is loaded and EnCase for DOS is launched into server mode. If the user selects the manual method, the user must specify the network card in the subject's machine. ENBD then loads the appropriate DOS driver and launches EnCase for DOS. (additional information can be found in *Chapter 17, EnCase for DOS*)

FAQs about EnCase Boot Disk

- 1. How do I make sure the computer does not boot to the hard drive on startup?**
 - Physically unplug the hard drives before turning on the computer. Power on and run the BIOS setup routine to ensure that the computer is set to boot from the floppy drive (drive A:). To access the BIOS setup, you will need to press a specific key sequence repeatedly as soon as the power comes on. On most IBM compatible PCs, the key is [**F1**] or [**Delete**]. Compaq computers often use the [**F10**] key. If possible, check the computer's documentation. There is usually a message flashed on the power splash-screen indicating which key to press to access the BIOS setup. Once in the

Copyright © 2004 Guidance Software, Inc.

May not be copied or reproduced without the written permission of Guidance Software, Inc.

BIOS, look for the boot order section. After setting the BIOS to boot from the floppy disk, reboot the computer to confirm that it does. After confirmation, turn off the computer, reconnect the hard drives, and reboot the computer with the EnCase Boot Disk inserted in the floppy drive.

20. When creating an EnCase Boot Disk, should I Quick Erase the preformatted disk?

- Yes, Quick Erasing a pre-formatted disk is faster and is usually as good as a full format.

21. Does the EnCase Boot Disk prevent writing to the hard drive on boot up?

- Yes. When you create an EnCase Boot Disk, all references to C:\ are changed to A:\ in COMMAND.COM and IO.SYS to prevent files from being accessed on the C drive on boot up. By starting EnCase for DOS immediately, you will prevent any accidental access to the hard drive from that point.

Chapter 4

EnCase for DOS

EnCase for DOS is used primarily for performing acquisitions. The executable (EN.EXE), located in the EnCase installation folder (typically C:\Program Files\EnCase4), is copied to the EnCase Boot Disk during the creation process.

Launching EnCase for DOS

After creating the EnCase Boot Disk (see the ENBD section in *Chapter 2*) and booting up the Subject system with the ENBD, type EN.EXE at the A:\> DOS prompt to launch EnCase for DOS.

EnCase for DOS Functions

While EnCase for DOS is used to put a subject computer into server mode so that it can be acquired, EnCase for DOS has other useful functions as well. All of these will be detailed in this chapter.

Locking / Unlocking (L)

The **Lock** command prevents the DOS operating system from inadvertently writing to a local hard drive. To successfully use this feature, the forensic investigator must know which hard drive to lock and unlock.

All local hard drives are, by default, locked by EnCase for DOS upon launch. The investigator is therefore not locking the Subject hard drive, but *unlocking* the storage hard drive.

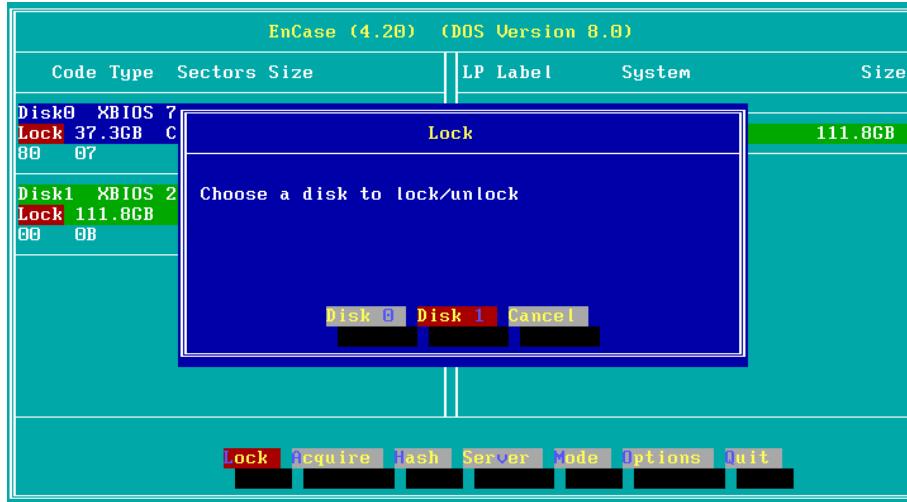


Figure 4-1 Unlocking a physical device



NOTE Drives can only be locked and unlocked when booted to DOS. Opening a DOS (Command prompt) window from within Windows does not give EnCase for DOS the access it needs to the hardware layers, nor is it forensically sound.

Acquiring

For more information, please see *Chapter 9: Drive to Drive Acquisition*.

Hashing

EnCase for DOS can generate a hash value for a drive. This command can be used to compare the hash value that EnCase for Windows reports on an acquisition of media to the hash value for the original media. To hash, launch EnCase for DOS and press **[H]** for Hash.

If you are *not* hashing a SafeBack image, use the default sector numbers that EnCase for DOS provides. Use the arrow keys to select the drive or volume and then hit [**Enter**].



Figure 4-2 Choose a device or volume to hash

When prompted for a start sector, hit [**Enter**] to accept the default of 0. This will almost always be the value used.

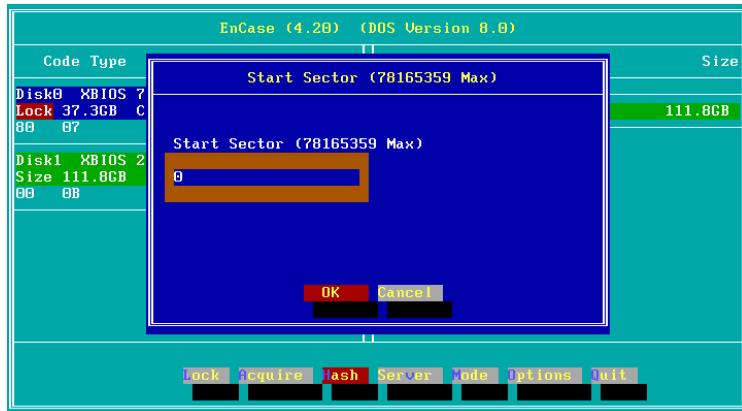


Figure 4-3 Select hash Start Sector

Take the default value for stop sector unless you are hashing a SafeBack image. Hashing SafeBack images in EnCase for DOS requires knowing specifically the starting and stopping sectors of the image. You do not have to hash SafeBack images in EnCase for DOS, since in EnCase for Windows (version 4.19 and higher), SafeBack images can be brought directly into EnCase in the same manner as EnCase evidence files. Change the Stop Sector or accept the default by hitting the [Enter] key.

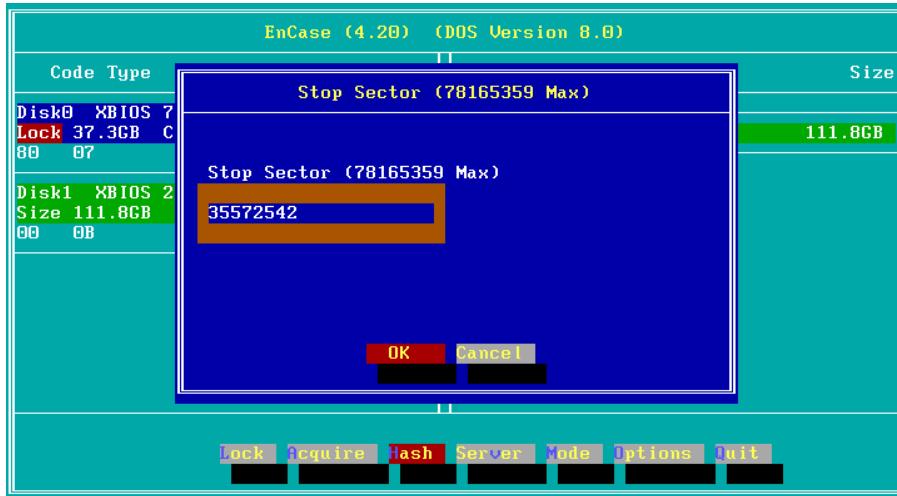


Figure 4-4 Select hash Stop Sector (SafeBack example)

When EnCase starts the hash, the option buttons at the bottom disappear, replaced by a hashing progress meter.



Figure 4-5 Hashing progress meter

When the device has been hashed, a status screen will appear with the hash value and the option to write the value to a file. The hash value can be written out to a text file on the floppy or an unlocked storage device with a FAT file system (the volume letter will appear in the right pane). To store this information, make sure the [Yes] button is highlighted in red (or press the [Y] key), then press [Enter].

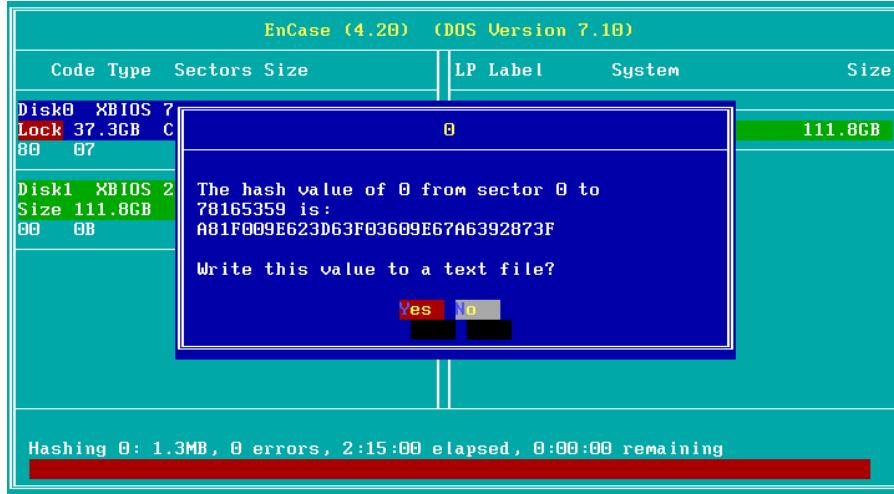


Figure 4-6 Hash status screen

Enter the complete path, including directory and filename, where you wish to store the hash value. You can store this on the A:\ drive, or on the unlocked storage drive, but make sure you have a valid path before entering the information. When the path has been entered, hit the [Enter] key. The hash value will be stored in a text file and you will be returned to the main EN.EXE menu.

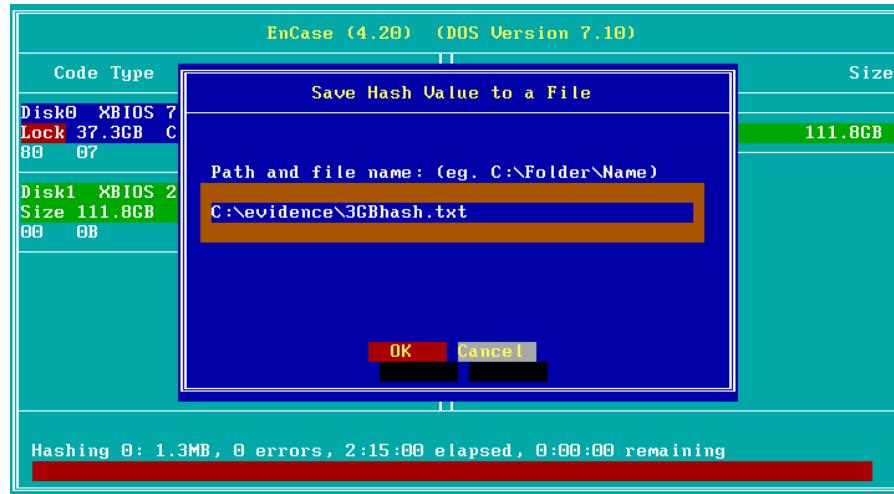


Figure 4-7 Saving hash value

Server

The subject computer must be placed in Server mode to acquire and preview subject media safely using the crossover or parallel port cable methods of acquisition. Before previewing or acquiring media on a subject machine, it is necessary to *prepare* the computer so that it can be previewed or acquired. The subject computer will have to be put in Server mode when performing either of the following:

- Parallel port lap-link cable preview / acquisition
- Crossover network cable preview / acquisition

To put a computer into Server mode:

1. Make sure the subject machine is configured to boot from the floppy as described in the *FAQs about EnCase Boot Disk* section of *Chapter 3*.
2. Insert the ENBD in the subject machine floppy drive and power it on.
3. Boot to the DOS prompt (A:\>) and type EN.EXE to launch EnCase for DOS.

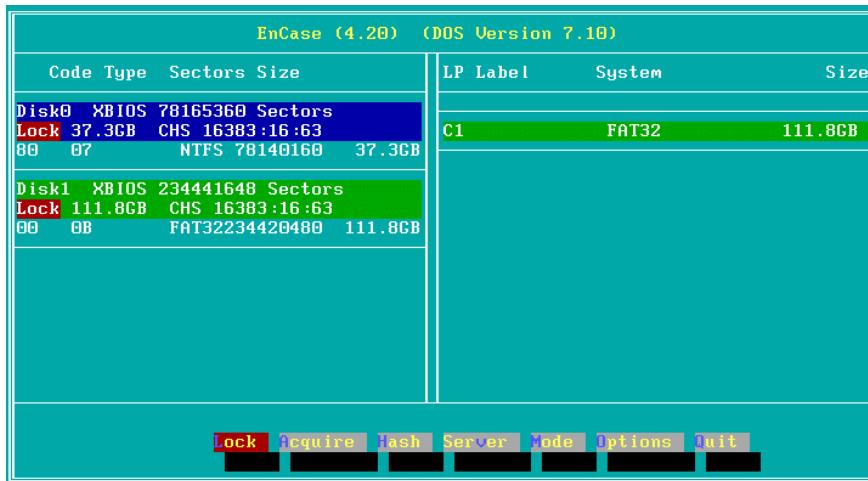


Figure 4-8 EnCase for DOS

22. Physical disks are displayed on the left; FAT logical volumes (partitions) are displayed on the right. In *Figure 3-8* above, the subject computer has two physical disks (**Disk0** and **Disk1**), with a single FAT32 logical volume (C:) on **Disk1**.



NOTE Remember, the DOS operating system can only recognize volumes\partitions on FAT file systems. If an NTFS or EXT2 physical disk is listed on the left, no volumes will be displayed on the right.

23. Server Mode must be set to allow for parallel port or network cable previews/acquisitions. To set the Server mode, press the [V] key.

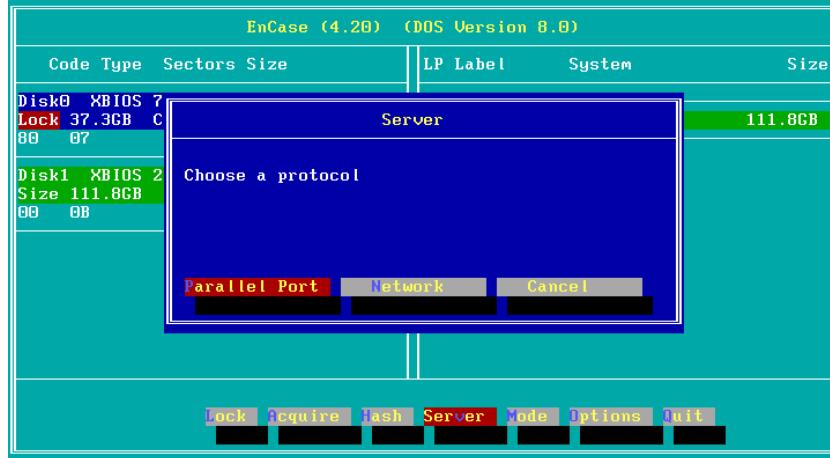


Figure 4-9 Choosing the protocol

24. Choose the desired server protocol (options are [**P**] for Parallel and [**N**] for Network crossover cable; in this example we will select Parallel), and then hit [**Enter**].

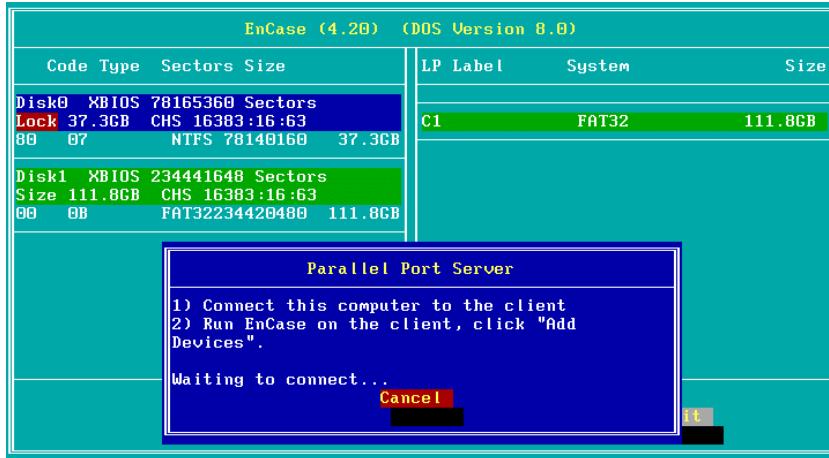


Figure 4-10 Parallel server mode

25. The Subject computer is now in Parallel server mode.



NOTE For storage and a subject computer to successfully communicate through a parallel port cable or crossover network cable, the versions of EnCase (for both Windows and DOS) must match.

Mode

The Mode button is extremely useful when working with older computers that use legacy BIOS codes that underreport the number of cylinders on the hard drive. There may be a small area of sectors at the end of the drive not accessed by the BIOS, and therefore not seen by EnCase for DOS.

EnCase addresses this limitation with the implementation of Direct Disk Access through the ATAPI interface. Select the [**Mode**] button by pressing the [**M**] key (or using the right arrow until the [**Mode**] button is highlighted in red), then press [**Enter**]. Use the right arrow until **ATA** is highlighted in red, then press [**Enter**]. EnCase will now access the drives via Direct ATA (*Figure 4-11*), providing accessibility to every sector of the hard drive. No changes to the BIOS access interface functionality in the EnCase program can be made to overcome the limitations presented by legacy BIOS systems.

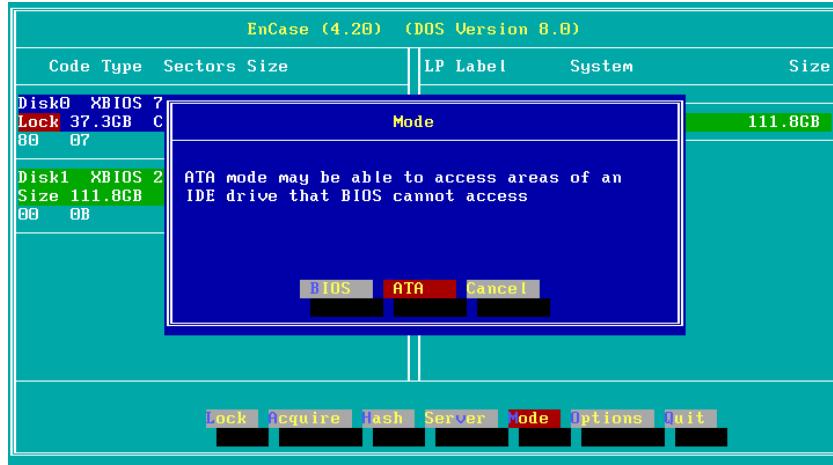


Figure 4-11 DirectATA mode

Quit

Select this option to quit EnCase for DOS. Quitting EnCase for DOS will return the machine to the DOS prompt. When the machine is powered down, remove the power cable and physically remove the subject hard drive for safekeeping.



NOTE Once EnCase for DOS has been closed, EnCase's software write-block on the local hard drives is no longer active. At this point, shut down the computer.

Chapter 5

Previewing versus Acquiring

In EnCase version 3, it was possible for the investigator to either preview *or* acquire media. It was also possible to acquire media after previewing media without having to quit the Preview mode and then acquire.

EnCase Forensic version 4 has taken this integration one step further. An investigator now *has* to preview before an acquisition can be started in EnCase for Windows. However, you can now save the results of a preview in a case file. If EnCase is in Acquisition Edition, you must still preview, but the preview will not show file structure. Even though file structure is not visible, you can proceed with the acquisition.

Limitations of Previewing

Previewing media allows the investigator to view the media as if it has been acquired. An investigator previews media first in order to determine if a full investigation (acquisition and analysis) of the media must be performed.

Previewing media is only available in EnCase for Windows. Previewing a *local* hard drive on a Windows PC without write blocking in place *will* alter data on

that drive. Changes to this drive will occur regardless of the precautions that EnCase makes, because of swap file activity.



NOTE It is possible to preview a local hard drive safely (without changing the media) if write-blocking hardware, such as a FastBloc, is used. If write-blocking hardware is not available, previews should be conducted through the parallel-port cable or crossover network cable.

The preview feature is so easy to use that many investigators mistake the preview for the actual acquisition. Be aware that although it is a quick way to find evidence, and it is still possible to save evidence results, the Preview feature will only allow you to view case results while physically connected to the subject media.

Advantages of Previewing

By previewing a drive, the investigator does not have to wait the several hours (or more) to finish an acquisition before doing a preliminary examination. While previewing, you can run keyword searches and create bookmarks. Search results and bookmarks can be saved into a case file; however, each time the case is opened the media must be physically connected to the storage machine.

Live Device and FastBloc Indicators

Since version 4.18, EnCase overlays a blue triangle in the lower right corner of the device icon to indicate a live (previewed) device. Logical volumes and physical drives write blocked by FastBloc are indicated by a blue square around the icon. The icon makes it easy to identify the devices which are protected and which are live. For steps on previewing and acquiring with FastBloc in Windows, please refer to *Chapter 9: FastBloc Acquisitions*.

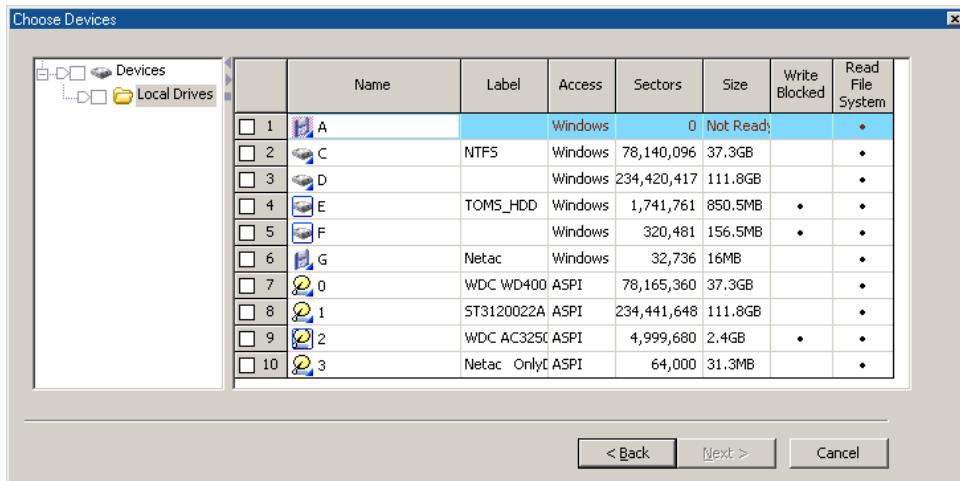


Figure 4-1 Devices with live and FastBloc icon overlays

Preview Questions

- 1. Can I Copy/UnErase files when I am previewing a Subject computer?**
 - Yes. Most EnCase functions are available while previewing a drive.
- 2. Can I preview Linux and Unix computers?**
 - The Linux or Unix drive must be attached to a computer booted with an EnCase boot disk and running in Server Mode. The investigator would then preview via the parallel port or crossover network cable with his lab computer.
- 3. Why does my laptop computer shut down when I am trying to preview the Subject computer?**
 - Laptop computers, and many desktops, have power-saving features in the BIOS. These features will shut ports or hard drives down to save energy after a given time. Disable this feature during setup on both Subject and Storage computers.

Acquisition Questions

- 1. How can I verify an evidence file to see if it is still intact?**
 - Select it from within the Cases tab, right-click, and choose **Verify Single Evidence File**.

Copyright © 2004 Guidance Software, Inc.
May not be copied or reproduced without the written permission of Guidance Software, Inc.

- 2. I am acquiring a huge drive. My evidence files are up to .E99. Can I still create more evidence file chunks?**
 - Yes, EnCase will keep creating them, beginning at .A01.

Chapter 6

Parallel Port Cable Acquisition

The parallel port method of acquisition should be used only when no other method of acquisition or preview works, due to its slow data transfer rate. This may include:

- When acquiring a laptop computer hard drive that cannot easily be removed and with no DOS-supported PCMCIA or on-board network interface card
- When acquiring a computer hard drive when no write-blocking device is available and there is no DOS-supported network interface card
- When acquiring a hardware RAID that is in a computer that does not have an on-board IDE channel

When acquiring using the parallel port and lap-link (null modem) parallel cable, the subject computer must be booted to DOS using the EnCase Network Boot Disk.

Parallel Port Cable Acquisition

26. Ensure EnCase versions on both DOS and Windows machines match prior to acquisition.
27. Make sure the subject machine is configured to boot from the floppy as described in the *FAQs about EnCase Boot Disk* section of **Chapter 3**.
28. Connect the two computers with the parallel port lap-link (null-modem) cable.
29. Boot the subject computer with an EnCase Network Boot Disk (see **Chapter 3: Creating the EnCase Boot Disk**).
30. Put the subject computer in Parallel server mode (see **Chapter 4: EnCase for DOS**).
31. Boot the storage computer into Windows.
32. Launch EnCase and open a new case by clicking on the [**New**] button.
33. Click the [**Add Device**] button

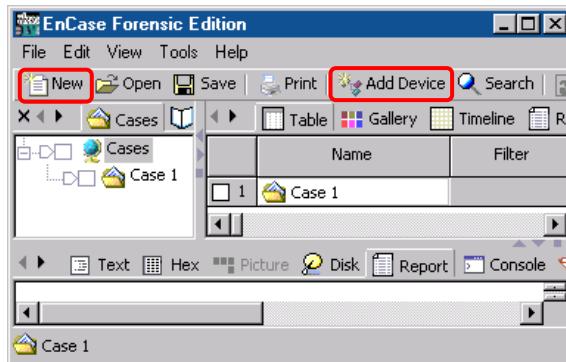


Figure 6-1 Adding a device

34. In the **Add Device** wizard, blue check **Parallel Port** and click [**Next >**].

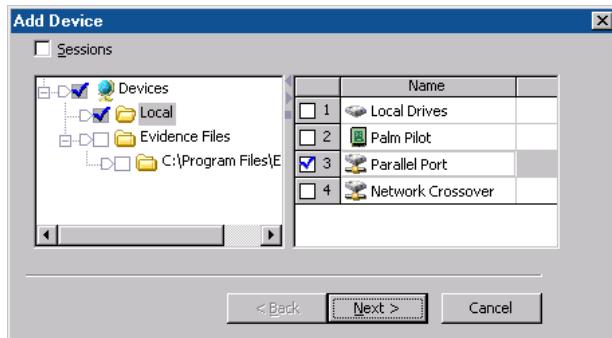


Figure 6-2 Selecting parallel port device

35. Blue check a device or volume, then click [**Next >**]. Only the remote drives will be shown if the parallel port has been selected as the source.

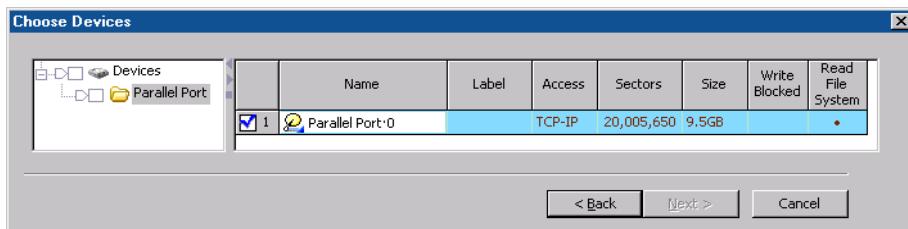


Figure 6-3 Drives available through the parallel port

NOTE If the Storage computer does not see the subject computer through the parallel port:



- Try setting the parallel port in the BIOS of both machines to either ECP or EPP or ECP+EPP.
- Try rebooting one or both computers.

36. At this point, double-clicking the media will allow the properties of the media to be edited, such as device name, case number, and more. Confirm the drive to add, and click [**Finish**].

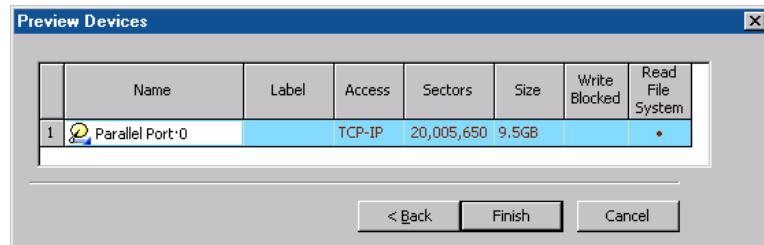


Figure 6-4 Confirming the drive to preview

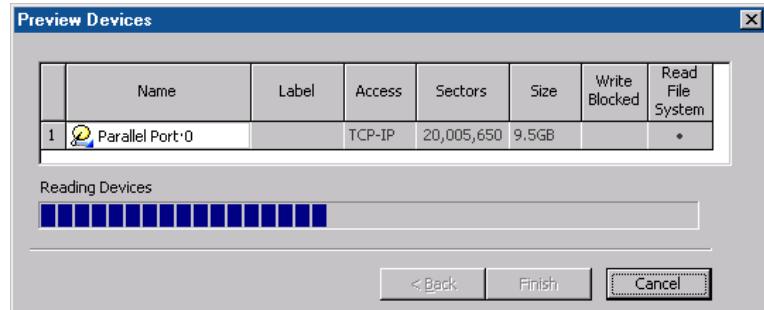


Figure 6-5 Adding preview via Add Device wizard

37. Once the drive is previewed, right-click on the physical icon under the Cases tab and select **Acquire**, or click on the [**Acquire**] button at the top toolbar.

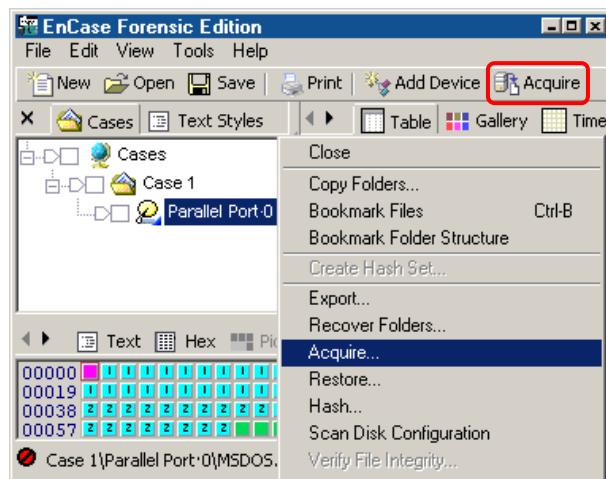


Figure 6-6 Acquiring previewed media

38. A screen appears providing options for tasks to perform after the acquisition. The **New Image File** section provides three options:

- **Do not add** – saves the device as an EnCase evidence file, but does not add it to the open case. This option leaves the preview intact.
- **Add to Case** – saves the device as an EnCase evidence file, and adds it to the open case. This option also leaves the preview intact.
- **Replace source device** (recommended) – saves the device as an EnCase evidence file, adds it to the open case and removes the preview. This option does not in any way alter the source device being acquired.

The other option in this window is for **Search, Hash and Signature Analysis**. Checking this option will start the process automatically after the acquisition.

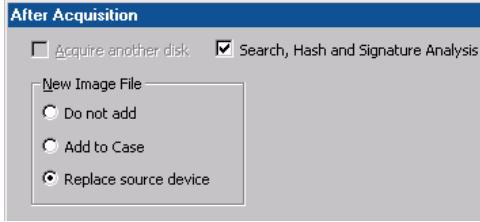


Figure 6-7 Acquisition options

39. If the **Search, Hash and Signature Analysis** option is checked, a screen will appear to allow you to set the parameters for those tasks.

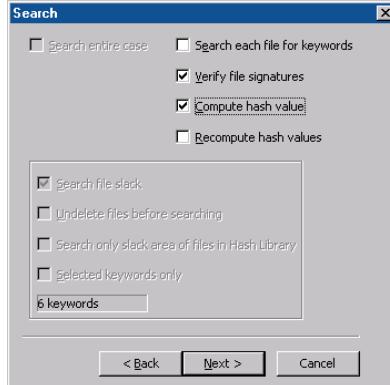


Figure 6-8 Search, Hash and Signature Analysis options

40. Define the evidence file settings. Use **Best** compression with parallel acquisitions as evidence can be compressed faster than it is transferred over the cable. Click [**Finish**] to begin the acquisition.

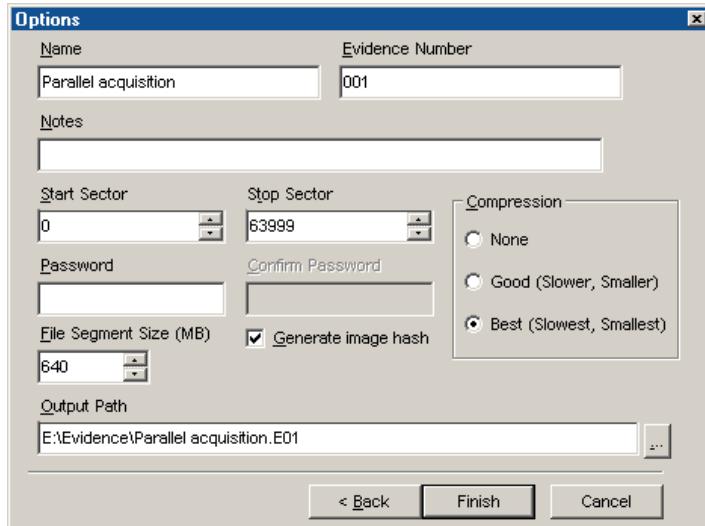


Figure 6-9 Acquisition options



NOTE Archive with the default 640MB "chunk" file size for easy CD-R archiving. Even if using a DVD-R burner, seven 640MB "chunks" fit comfortably onto a DVD-R.

If the Storage drive fills up during an acquisition, EnCase will attempt to redirect the data to a user-defined location. Unless the storage computer contains hard drives that are hot-swappable, EnCase must be directed to another form of media in your computer that already has a drive letter—for example, a second storage hard drive or mapped networked drive. If acquiring to Zip or Jaz disks, eject the full disk and insert another.

After acquisition is complete:

- Power down both computers.
- Disconnect the parallel port cable.
- Place the subject hard drive in a safe location.
- Remove the boot floppy from the floppy drive.
- Boot to Windows on the lab system.

Copyright © 2004 Guidance Software, Inc.

May not be copied or reproduced without the written permission of Guidance Software, Inc.

*Copyright © 2004 Guidance Software, Inc
May not be copied or reproduced without the written permission of Guidance Software, Inc.*

Chapter 7

Network Cable Acquisition

EnCase allows users to preview and acquire via the included crossover network cable.



NOTE Previewing and acquiring with this method only works with a crossover cable. A yellow crossover cable was shipped with your EnCase software. Crossover cables are Ethernet cables using RJ-45 connectors, where one end of the cable is wired so that the Receive signal pins on one connector are connected to the Transmit signal pins on the other side. They are designed for direct workstation-to-workstation connectivity. A common CAT5 "straight-through" Ethernet cable will not work, nor will previews \ acquisitions across a LAN, unless using EnCase Enterprise.

Creating the EnCase Network Boot Disk (ENBD)

Making a crossover network cable acquisition work requires loading a DOS packet driver so that EnCase for DOS can communicate with the installed PCI or PCMCIA network card. Guidance Software provides investigators the EnCase Network Boot Disk (ENBD), created by the Ontario Provincial Police e-crime section, to facilitate the detection and loading of the correct DOS packet driver.

The boot disk has the ability to manually or automatically detect NICs and load the drivers, giving the examiner maximum convenience and flexibility when acquiring or previewing media.

- Auto-detect automatically attempts detection of the NIC in the computer
- Manual functionality allows the investigator to specify the NIC driver to load

There are multiple ENBDs available for download, depending on the type of NIC in the subject computer. To create an ENBD:

1. Go to <http://www.guidancesoftware.com/support/articles/networkbootdisk.shtml> to download the appropriate ENBD from the Guidance Software website.
2. Have a blank, formatted floppy diskette in your floppy drive.
3. The downloaded ENBD creation files are executables. Double-click on the downloaded .EXE file to start the EnCase Network Boot Disk creation process.
4. Copy the C:\Program Files\EnCase\EN.EXE to the ENBD. The same version of EnCase must be on both the ENBD and the storage machine.



Figure 7-1 The EnCase Network Boot Disk menu

The ENBD can detect and load SCSI device drivers for different SCSI controller cards as well as network cards. Refer to the table below for all cards supported:

PCI cards supported for auto and manual loading: <ul style="list-style-type: none"> • 3COM 10/100 V.90 Mini-PCI Combo Card • 3COM EtherLink III Series • 3COM EtherLink XL Series • 3COM EtherLink 10/100 with 3XP (3C990) • ACCTON EN1207D-TX/EN2242A Series • ACCTON EN5251 Series • ADMTEK PCI 10/100 Series • AMD PCNet Series • COMPAQ 10/100 and Gigabit • COMPAQ NetFlex-3 • DAVICOM PCI-Based Series • DIGITAL 2104x/2114x 10/100 Series • D-LINK DFE-530TX+ 10/100 Series • D-LINK DFE-550TX 10/100 Series • HP 10/100VG NDIS 2.01 Driver • INTEL PRO Series • INTEL PRO/1000 Server Series • LITE-ON PNIC-10/100 Series • MACRONIX MX987xx Series • NATIONAL DP83815 10/100 MacPhyter Series • NETGEAR FA310TX Adapter • REALTEK RTL8029 Series • REALTEK RTL8139/810X Series • SIS 900/7016 SIS900 10/100 Series • SMC Fast Ethernet 10/100 (1211TX) • SMC EtherPower II 10/100 (9432TX) • VIA PCI 10/100Mb Series • WINBOND W89C940F 10 PCI Adapter 	PCMCIA cards supported for manual loading only: <ul style="list-style-type: none"> • 3COM 3CCFE574 Family • 3COM 3CCFE575 Family • INTEL 16-BIT Series • INTEL 32-BIT Series • XIRCOM CE3B-100BTX (non-CardBus) • XIRCOM RealPort and Realport2 R2BEM56G-100 SCSI controller cards supported for auto and manual loading: <ul style="list-style-type: none"> • AIC-78XX/AIC-75XX • AIC-7890/91 • AMD PCscsi • BusLogic MultiMaster • BusLogic FlashPoint • IBM ServeRAID • Initio INI-9XXXU/UW • Initio INI-A100U2W • Symbios 53C8xx
--	---

Performing the Crossover Network Cable Acquisition

1. Make sure the subject machine is configured to boot from the floppy as described in the *FAQs about EnCase Boot Disk* section of **Chapter 2**.
2. Connect the subject computer to the storage computer via the crossover cable.
3. Boot the subject computer with the appropriate EnCase Network Boot Disk.
4. The current ENBD displays the following menu options on startup:
 - **Network Support** - Loads the appropriate menu system for crossover acquisition
 - **USB – Acquisition (no drive letter assigned)** - Loads DOS USB drivers to allow the acquisition of a USB-connected device
 - **USB – Destination (drive letter assigned)** - Loads DOS USB drivers to allow storage to a USB-connected device
 - **Clean boot** - Loads similar to the barebones boot disk to do a direct DOS acquisition
5. From the menu, select **AUTO** to allow the ENBD to detect the NIC, or select **MANUAL** to load the packet driver manually. If **AUTO** is selected, you are prompted to press any key to accept the drivers, at which point EnCase launches and automatically runs in Network Server mode.

6. If the driver is loaded manually, choose **ENCASE** from the menu to launch EnCase. You can also run EnCase to do a direct DOS acquisition by typing EN.EXE at the command prompt.



Figure 7-2 EnCase for DOS user screen

7. Put EnCase for DOS in Server mode.
8. Choose **Network**. The subject machine should now be running in Server mode, displaying a message stating **Waiting to connect...**
9. Boot the forensic PC into Windows.
10. Assign a fixed IP address to the storage computer, as follows:

Windows 98

- Right-click on Network Neighborhood and select **Properties**.
- Double-click the TCP/IP protocol for the network card.
- Put in a fixed IP address (such as 10.0.0.50) in the **IP Address** tab.
- Enter a subnet mask of 255.255.255.0.
- Click **[OK]**. The computer must be rebooted.

Windows 2000/XP

If the Examiner's operating system is Windows XP Service Pack 2, Windows Firewall may be running; if so, you will need to configure Windows Firewall to allow EnCase traffic for the crossover cable acquisition to work properly as follows:

- From the Windows Start button, select Settings, then choose Windows Firewall in the Control Panel.

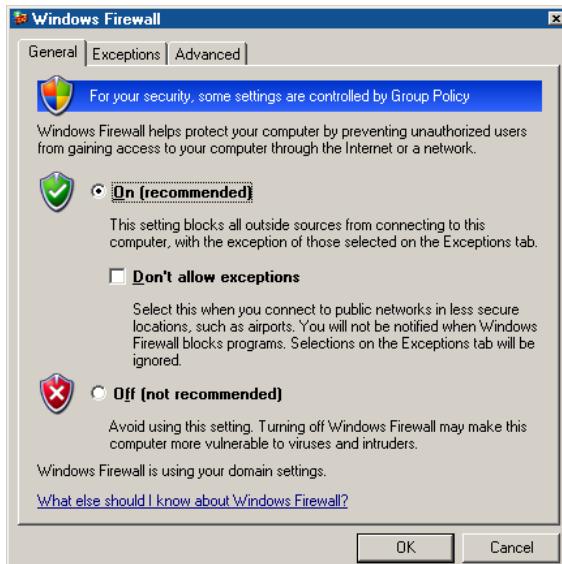


Figure 7-3 Windows Firewall control panel

- By default, the Firewall is set to **[On]**; the **Don't allow exceptions** box should be unchecked. If it is set to **[Off]**, Windows Firewall has been turned off and will not interfere with any functionality, and you can skip this process. If the Firewall is on, click on the **Exceptions** tab at the top of the window.

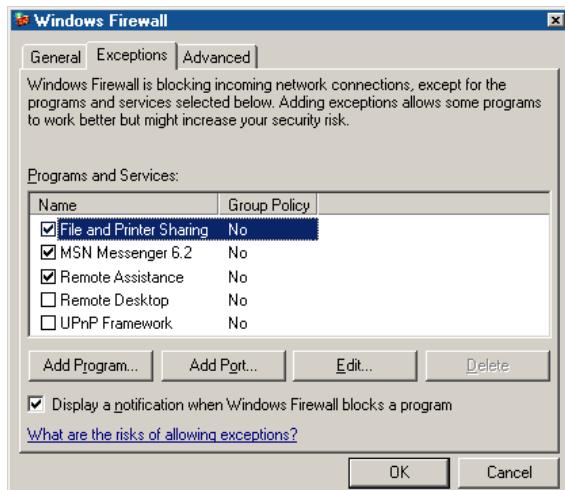


Figure 7-4 Windows Firewall Exceptions tab

- Click on the [Add Program...] button

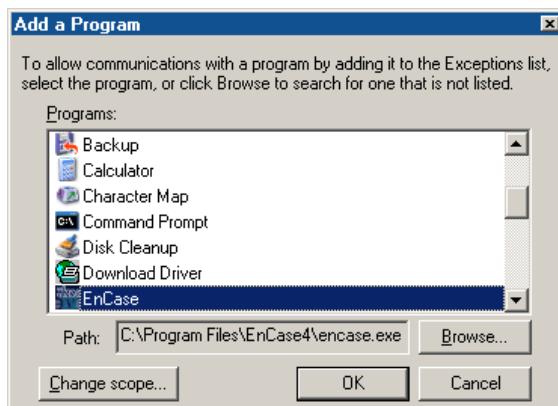


Figure 7-5 Adding an exception

- Find EnCase in the list showing in the **Programs:** window and click to select it, or click on the [**Browse...**] button to find the EnCase executable (by default, C:\Program Files\EnCase4\encase.exe) so that it shows in the **Path:** field.
- Click on the [**OK**] button.
- Click on the [**OK**] button in the main Windows Firewall button to allow the crossover preview\acquisition.

You will also need to configure Windows 2000, Windows XP and Windows 2003 as follows:

- Right-click on **My Network Places** and select **Properties**.
- Right-click on **Local Area Connection** and select **Properties**.
- Double-click the TCP/IP protocol.
 - Enter a fixed IP address (such as 10.0.0.50) in the **IP Address** tab.
- Enter a sub-net mask of 255.255.255.0.
- Click on the **[OK]** button.

The **WINS** and **DNS** settings must be removed. Those will prevent the connection from taking place over the crossover network cable.

12. Launch EnCase for Windows.
13. Click the **[ADD device]** button on the top toolbar.
14. Place a blue check in the box to the left of **Network Crossover**.
EnCase will connect to the subject computer running in server mode.
You can then preview/acquire as outlined in the previous chapter.

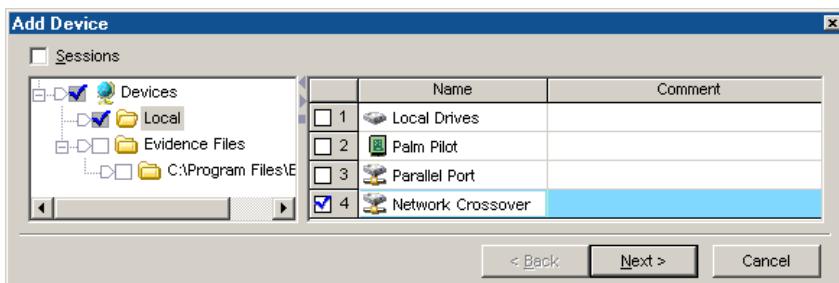


Figure 7-6 Network crossover acquisition

EnCase overlays a blue triangle in the lower right corner of the device icon to indicate that the device is live.



Figure 7-7 Blue triangle indicator for live devices

Chapter 8

Drive-to-Drive Acquisition

One method of acquisition takes place entirely within EnCase for DOS. Typically, the Subject IDE hard drive will be placed in the Storage computer so that both the Subject and Storage IDE drives are on the same motherboard, hence the term “drive to drive”. There is no “server mode” in a “drive to drive” acquisition.

Drive Geometry Problems

Performing a “drive to drive” acquisition in the Subject computer’s environment might be necessary in certain situations. Performing the acquisition in the Subject environment avoids any drive geometry problems that might result if the Subject hard drive is removed from its native environment.

As an example to illustrate this issue, assume that a 20GB hard drive in the subject computer has a Phoenix BIOS from 1997. With the drive placed into a top-of-the-line computer with an Award BIOS from 2002, it is entirely likely that the BIOS in each are set to “auto detect” hard drives. Since they are different, they will likely also auto detect the same hard drive at a slightly different cylinders-heads-sectors setting. If you acquire a hard drive “drive to drive” in the storage (forensic) system, you *might* encounter sporadic error messages or not

Copyright © 2004 Guidance Software, Inc.
May not be copied or reproduced without the written permission of Guidance Software, Inc.

see every sector that the Subject computer used. The solution would be to reacquire the original media in the media's original (native) environment.

The caveat to that, of course, is that you must be certain the subject computer is set to boot from a boot diskette, not a hard drive. This can be checked in the BIOS. Be sure that all hard drives are disconnected when booting the first time with a boot disk so that you can be certain the subject computer will boot from the EnCase Boot Disk, *not* the subject media.

If you are not certain, it might be better to acquire the subject media in your own “forensic” computer, though that might lead to, as described above, drive geometry problems.

Benefits and Drawbacks

If a FastBloc is not available, the “drive to drive” acquisition is the fastest way to perform an acquisition without compromising the data. Data is transferred over an IDE ribbon cable, a much faster pipeline than a parallel port lap-link cable or crossover network cable.

There is a risk to the “drive to drive” acquisition. If both drives are the same make and model, and the Storage partition is not labeled “STORAGE” (or something similar), it can be difficult to determine which drive to acquire *to* and which drive to acquire *from*. In that situation, it would be easy to acquire the *Storage* hard drive to the *Subject* hard drive. That would destroy the evidence.

Steps to Follow

1. Attach the subject hard drive to an IDE ribbon cable on the storage computer (or visa-versa to avoid drive geometry problems). Be sure that the storage drive is formatted FAT32, or EnCase for DOS will not be able to store the evidence.
2. Boot the storage computer with an EnCase Boot Disk.
3. Launch EnCase for DOS (type EN at the a : \> prompt).
4. Unlock the storage drive (all drives are locked by default, preventing the computer from writing to any drive by accident). Click [L] for LOCKING and specify the storage drive to unlock.
5. Click the [A] key to acquire.

6. Choose the subject drive to acquire.

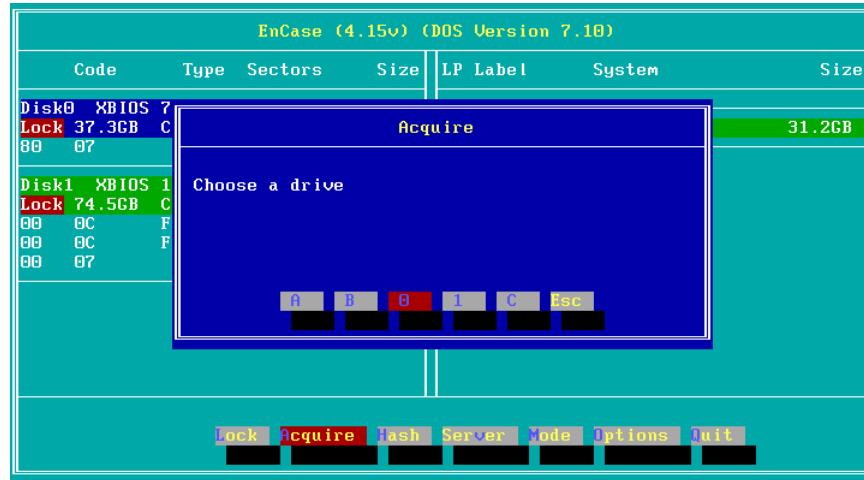


Figure 8-1 Starting acquisitions in EnCase for DOS

7. EnCase prompts for the path to store the evidence file. Enter an unused file name on the storage drive attached to the Subject computer (e.g., D:\DISK1) and then press [Enter]. It is a good idea to always create a uniquely named folder to hold evidence files. Avoid using the root directory, as there is always a chance you will write to the wrong drive.

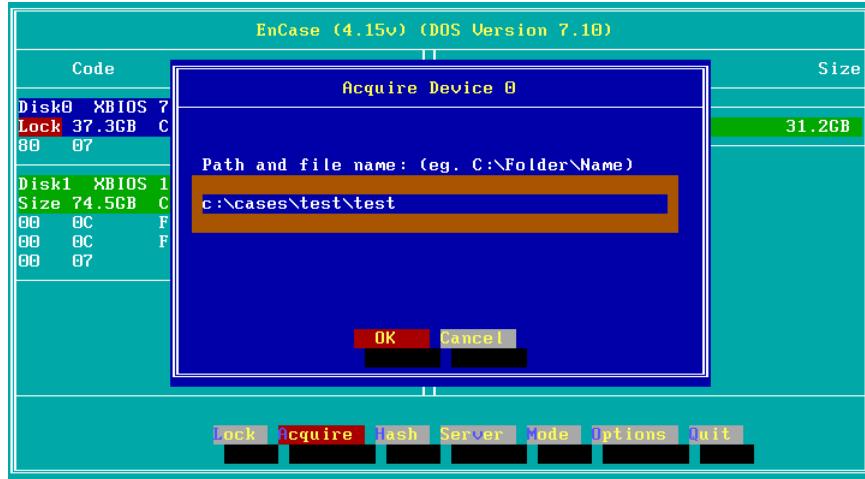


Figure 8-2 Input path for evidence file



Alert! The file path specified must already exist on the Storage computer. If it does not, exit EnCase for DOS, create that path (**MD** for "make directory") then go back into EnCase for DOS.

8. EnCase prompts you for the case number to which the evidence belongs. Enter the case number (if one has been assigned) and press [**Enter**].



Figure 8-3 Input for case number

9. Enter the name of the examiner or investigator who is conducting the investigation and press [**Enter**].

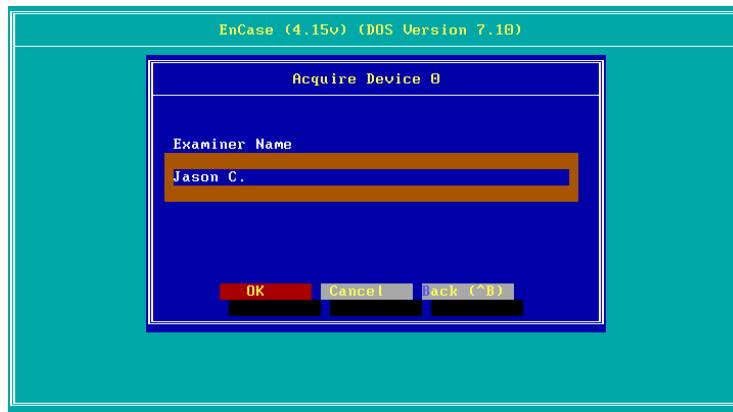


Figure 8-4 Input for examiner name

10. Enter a numeric code to identify the specific piece of evidence and press [Enter].



Figure 8-5 Input for evidence number

11. Enter a short descriptive name such as Desktop 1 or Laptop. This name will be used to describe the drive in the Windows version of EnCase. Press [Enter].

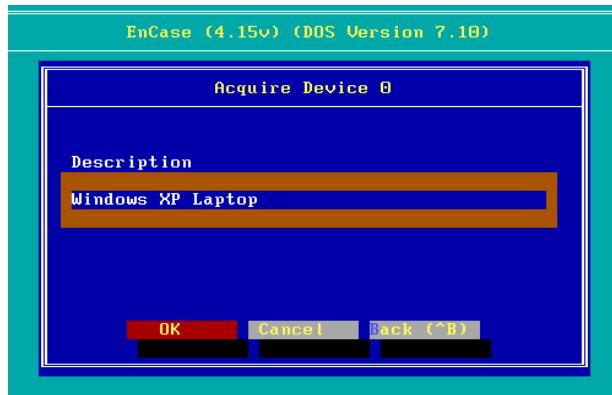


Figure 8-6 Input for unique description

12. If the date and time displayed are correct, press [Enter]. If not, type in the correct date and time and press [Enter].

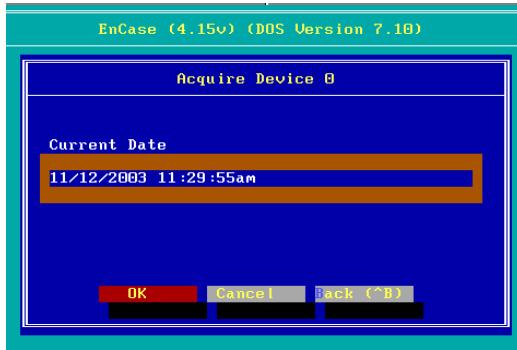


Figure 8-7 Date of acquisition computer

13. Enter any notes or relevant information given to this piece of evidence (such as its location or condition), and then press [Enter].



Figure 8-8 Input for notes

14. Select [**Yes**] to compress the evidence file. The resulting files, in turn, will be two to three times smaller than if acquired with no compression. Using compression may take up to five times longer to create the file.

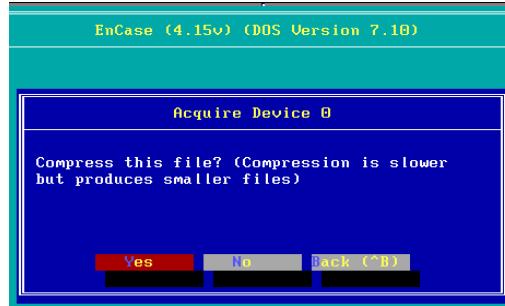


Figure 8-9 Select [**Yes**] to compress

15. Choose whether or not to create an MD5 hash value. Choose [**Yes**] to generate an MD5 hash of the evidence at the time of acquisition (strongly recommended).

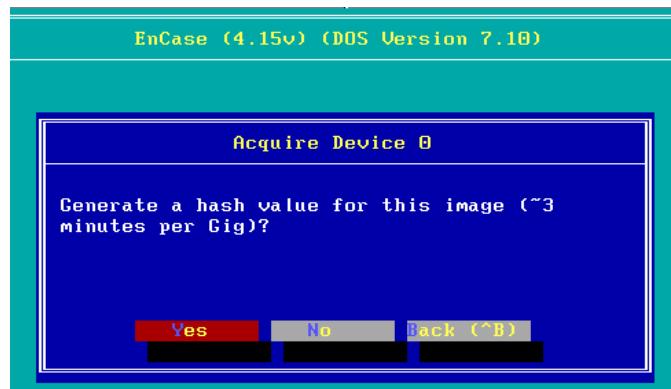


Figure 8-10 Select [**Yes**] to obtain MD5 hash

41. To add a password to an evidence file, type in the password and click [OK]. If the password is lost or forgotten, the evidence file is inaccessible.

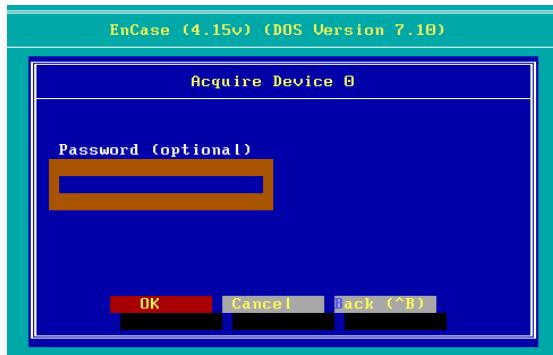


Figure 8-11 Input for password

42. Enter the maximum desired size of the resulting file “chunks.” EnCase defaults to 640MB to facilitate CD-R archival, but this may be increased up to 2000MB.

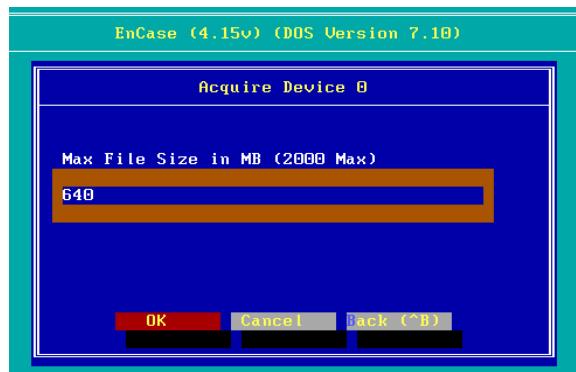


Figure 8-12 Input for evidence file segment size



Note Guidance Software recommends archiving with 640MB “chunk” file sizes. Even if archiving to DVD-R, seven 640MB “chunks” fit comfortably onto a DVD-R.

43. EnCase allows the investigator to specify the number of sectors to acquire. While most of the time the default is correct, the exception is when dealing with a SafeBack clone of a drive. For example, SafeBack clones a 7GB drive to a 10GB drive. The extra 3GB are completely unnecessary to

acquire. Simply type in the number of sectors that SafeBack reported cloning.

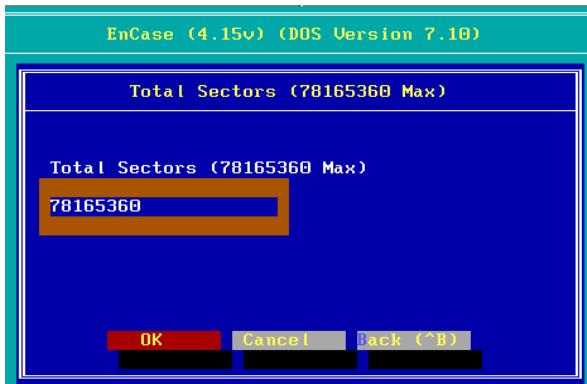


Figure 8-13 Specifying sectors for SafeBack-cloned drives

44. EnCase will now begin the disk acquisition process. This can take several hours, so ensure that the computer has a stable position and power supply. The time elapsed and estimated time remaining is displayed.

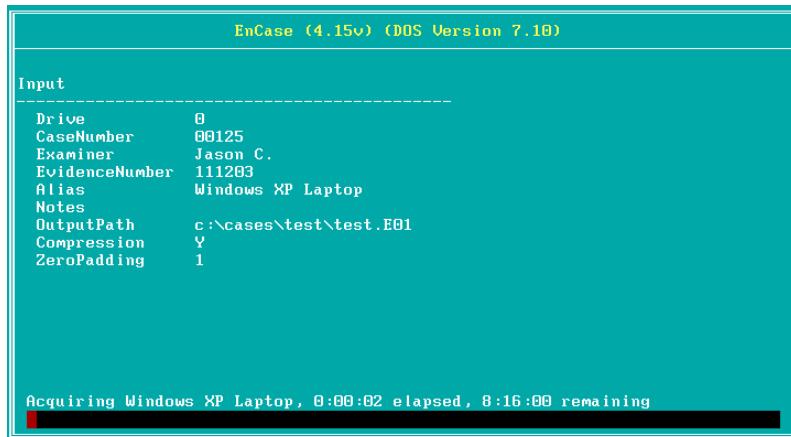


Figure 8-14 Acquisition

If the evidence drive fills up, EnCase for DOS will prompt you to exchange disks. Label the disk according to the file name EnCase assigns to the output file. The file extension .E01 is always assigned to the first “chunk” of an evidence file set. Thereafter, the number in the extension is increased sequentially. For example, if you name the first output file of an evidence set “hard disk,”

EnCase will assign a name of `harddisk.E01` to the first output file, `harddisk.E02` to the next “chunk,” and so on.

Acquiring Macintosh devices

EnCase can acquire and interpret the Macintosh and Power Mac file systems (HFS and HFS+). Acquiring a Macintosh hard drive is performed similarly to acquiring a PC hard drive in a “drive to drive” acquisition. The caveat with Macs is that since they cannot be booted with an EnCase Boot Disk, the drive must be removed from the Mac and installed locally into the storage computer. If the media is an IDE hard drive, put it on the IDE ribbon cable. If the media is a SCSI hard drive, attach it to the SCSI controller card in the storage computer and subsequently acquire it through DOS.

If the Macintosh HD is an IDE hard drive and a FastBloc unit is available, acquisition of the Macintosh hard drive is possible that way as well. Please see *Chapter 9: FastBloc Acquisitions* for details.

Acquiring Unix and Linux

EnCase can acquire and interpret the EXT2/3, Reiser, FFS, and UFS files system. To acquire a Unix, Linux, or BSD hard drive, handle it much like you would a PC hard drive. The caveat with Unix and BSD is the same as for Macintosh—the subject media must be removed from the computer and installed locally into the storage computer. If it is an IDE hard drive, put it on the IDE ribbon cable. If the subject media is SCSI, attach it to the SCSI controller card. Acquire through DOS using EnCase boot disk.

With an IDE hard drive, a FastBloc unit can provide an alternate means of acquisition of the UFS hard drive. Please see *Chapter 22: FastBloc Acquisitions* for details.

After the Acquisition Is Complete

After the acquisition is complete, boot the storage computer into Windows to analyze the just-created evidence file. Remember to remove any connections to the subject hard drive before booting to Windows.

If completing a drive-to-drive (same IDE ribbon cable) acquisition in the Storage computer, follow these steps:

1. Power down the computer.
2. Disconnect the subject hard drive from the ribbon cable and power cable.
3. Replace the cover on the storage computer.
4. Place the subject hard drive in a safe, static-free location for safety.
5. Remove the boot floppy from the floppy drive.
6. Boot the storage computer and launch EnCase for Windows.
7. If you performed an acquisition of another type, disconnect the cable connecting the subject media to the storage computer.

*Copyright © 2004 Guidance Software, Inc
May not be copied or reproduced without the written permission of Guidance Software, Inc.*

Chapter 9

FastBloc Acquisitions

Computer investigations require a fast, reliable means to acquire digital evidence. FastBloc Classic, FastBloc Lab Edition (LE), and FastBloc Field Edition (FE) (hereafter referred to as FastBloc) are hardware write-blocking devices that enable the safe acquisition of subject media in Windows to an EnCase evidence file. Before FastBloc was developed, noninvasive acquisitions were exclusively conducted in cumbersome command-line environments.

The hardware versions of FastBloc are not stand-alone products. When attached to a computer and a subject hard drive, it provides investigators with the ability to quickly and safely preview or acquire data in a Windows environment. The unit is lightweight, self-contained, and portable for easy field acquisitions, with on-site verification immediately following the acquisition.

FastBloc Acquisition Process

1. Attach Subject IDE hard drive to FastBloc unit.



Figure 9-1 FastBloc Classic and travel case



Figure 9-2 FastBloc LE



Figure 9-3 FastBloc FE

2. Make sure the SCSI or IDE connection from FastBloc to the storage computer is snug.
3. Power FastBloc on.
4. Power the storage computer on.
5. Launch EnCase for Windows on the storage machine.

*Copyright © 2004 Guidance Software, Inc
May not be copied or reproduced without the written permission of Guidance Software, Inc.*

6. Click the [**Add device**] button.
7. Blue-check **Local Devices** in the **Add Devices** wizard and click on the [**Next >**] button.

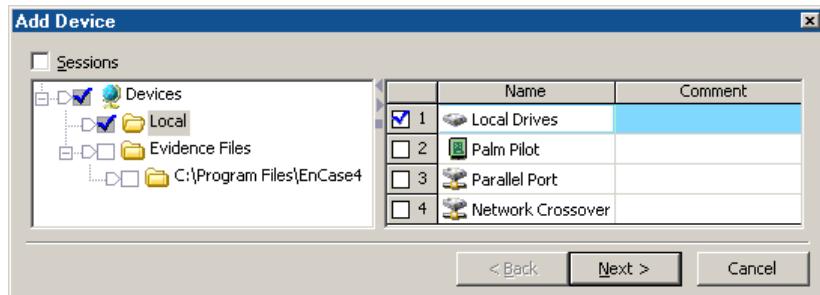


Figure 9-4 Adding write-blocked device

8. Choose a physical drive protected by FastBloc (indicated by a blue border around the icon), and then click the [**Next >**] button.

Choose Devices								
	Name	Label	Access	Sectors	Size	Write Blocked	Read File System	
<input type="checkbox"/> 1	A		Windows	0	Not Ready		•	
<input type="checkbox"/> 2	C	NTFS	Windows	78,140,096	37.3GB		•	
<input type="checkbox"/> 3	E	APTIVA	Windows	11,759,517	5.6GB	•	•	
<input type="checkbox"/> 4	G	Netac	Windows	32,736	16MB	•	•	
<input type="checkbox"/> 5	D	WDC WD400JB-00ENAO	ASPI	78,165,360	37.3GB		•	
<input type="checkbox"/> 6	I	QUANTUM Bigfoot TX6.	ATA	11,773,755	5.6GB	•	•	
<input checked="" type="checkbox"/> 7	2	Netac OnlyDisk 1.12	ASPI	64,000	31.3MB	•	•	

Figure 9-5 Available devices with FastBloc-protected devices with blue border

9. With the selected device showing in the **Preview Devices** window, click on the [**Finish**] button to confirm the selection. To edit device properties, such as the device name, device notes, etc., double-click the device name before clicking the [**Finish**] button.

Live Device and FastBloc Indicators

In EnCase, live devices (previews) are identified in Case view by a blue triangle in the lower right of the icon. A blue square icon (without the triangle) is overlaid on volumes and devices write-blocked by FastBloc when previewed.

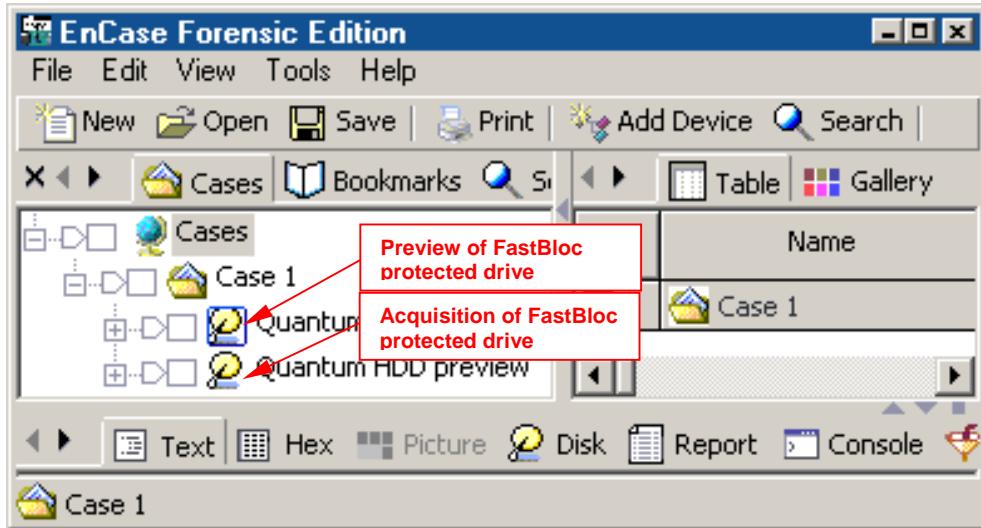


Figure 9-6 FastBloc-protected hard drive preview and acquisition

Acquiring via FastBloc provides access to the automated acquisition and analysis features such as verification, searching, hashing, and verification of the file signatures of very large hard drives overnight or a weekend at the time of acquisition. Prior to using these features, ensure you have added and selected the desired keywords in the **Keyword View**.

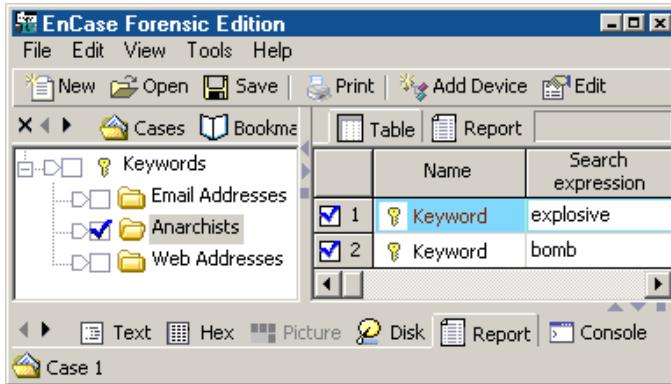


Figure 9-7 Creating keywords for acquisition options

Once the keywords have been created and selected, return to the Case view, right-click on the previewed device and select **Acquire...**. Alternately, you can click on the [Acquire] button on the top toolbar.

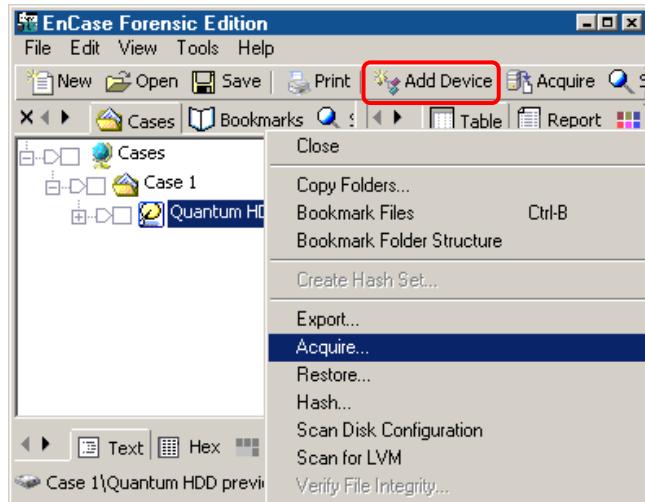


Figure 9-8 Acquiring a live write-blocked device

Several options are available in the **After Acquisition** screen that appears. Selecting **Acquire another disk** will allow the examiner to acquire several devices one after another, such as floppy disks or CDs. The examiner will not need to preview each new device before acquisition.

The examiner has three options for the evidence file once it is created.

- **Do not add** – this option will leave the evidence file in the saved location upon completion of the acquisition, but will not add it to the open Case. This is used for acquiring images to a central server or acquiring images that will not be examined immediately.
- **Add to Case** – this option will add the new evidence file to the case, but will not replace the live device (preview). This is used for adding acquired images to the case, but leaving the live access to the drive available to image other devices. It is important to note that if the case is saved with a live preview in it, when the case is reopened, it will look for the device to be physically attached.
- **Replace source device** – this option is used for hard drive acquisition or for acquiring a single piece of removable media. This option adds the new evidence file to the case, replacing the live preview. Any search hits,

hashing, bookmarks, etc, of the live device during triage will be resolved to the newly added evidence file. This option is not available if you want to acquire another disk.

When acquiring a hard drive you should select **Replace source drive**. EnCase now gives the examiner the option of searching, hashing, and running the file signature analysis on the newly added evidence file. For these options, select **Search, Hash, and Signature Analysis**.

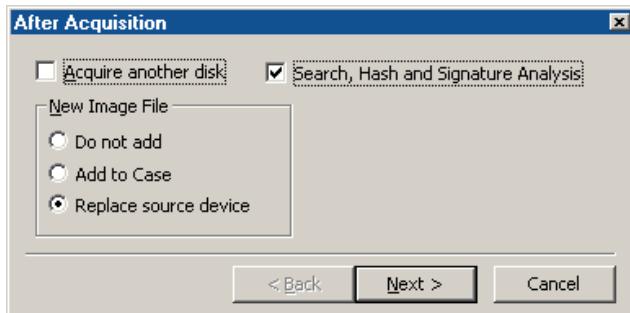


Figure 9-9 Post acquisition options

You will now have the **Search** options available. You should select the desired keyword(s) to search before starting the acquisition process, unless you wish to search all of the available keywords. If the desired keywords are not already selected in the **Keyword** view, select **Cancel**, go to the **Keyword** view, select or enter in the desired keywords, return to the **Case** view and start the acquisition process again. The **Search** window gives examiners the option of search and analyzing all of the devices in the case by selecting **Search entire case**. If the option is not selected, EnCase will only search and analyze the new evidence file after its creation.

The examiner has several analysis options available:

- **Search each file for keywords** – this option will search each file for the desired keywords, in the entire case or just new evidence file as selected by the examiner.
- **Verify files signatures** – this option will compare the file extensions and file header/signature of each file, in the entire case or just new evidence file as selected by the examiner.
- **Compute hash values** – this option will compute the hash value of the logical file area of each file and compare the value to the hash

library, in the entire case or just new evidence file as selected by the examiner.

- **Recompute hash values** – this option will recompute all previously computed hash values generated for the files of the replaced live device. This is most often used for acquisitions over the enterprise network, to recompute the values of the files on the live machine if a hash analysis was conducted previously. This option is not necessary for local acquisitions.

There are four options for the searching if it is selected:

- **Search file slack** – this option will include searching the file slack (area between the logical and physical areas of the file) of each file, in the entire case or just new evidence file as selected by the examiner.
- **Undelete files before searching** – this option will logically “undelete” deleted files prior to searching. If a file is deleted, EnCase and other tools can determine if the assigned starting cluster is not assigned to another file (if it is assigned, then the file is Deleted-overwritten). The unallocated clusters after the starting cluster may or may not belong to the deleted file. Choosing this option assumes the unallocated clusters after the starting cluster do belong to the deleted file. This is the same assumption made when copying out a deleted file. This option finds keyword fragmented between the starting cluster and the subsequent unallocated cluster. If determining the presence of a keyword on the media is critical to an investigation, the examiner should also search for portions of the keyword, including GREP expressions of fragments of the keyword.
- **Search only slack area of the files in the Hash Library** – this option will exclude the logical area of files for which their hash values matches that of a file in the Hash Library. The slack area of the physical file will still be search, in the entire case or just new evidence file as selected by the examiner.
- **Selected keywords only** – this option will have EnCase search only the keywords selected in the Keywords view rather than all available keywords, in the entire case or just new evidence file as selected by the examiner.

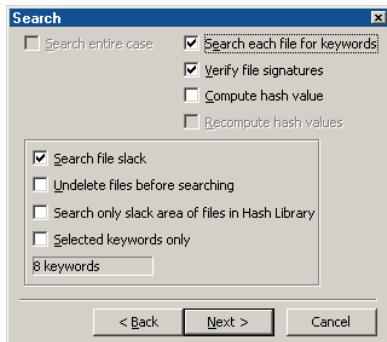


Figure 9-10 Search and analysis options

Choose [**Next >**] after selecting options. The last window will be the acquisition options. These are the standard options for the generation of an evidence file.

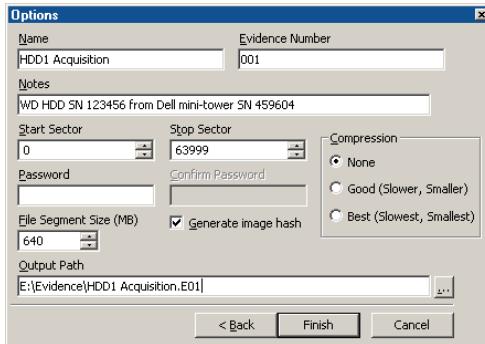


Figure 9-11 Evidence file options

After selecting [**Finish**] EnCase will begin the acquisition process. The progress bar indicates the status in the lower right hand corner.



Figure 9-12 Acquisition status

When the acquisition is complete, EnCase will replace the live previewed device with the new evidence file and begin the verification of the evidence file.



Figure 9-13 Acquired evidence in case

When the verification is complete, EnCase will begin the searching and other analysis of the evidence file.

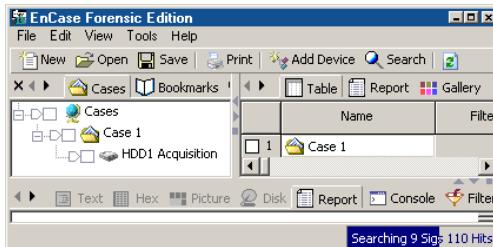


Figure 9-14 Searching after acquisition and verification

When all processes are complete, EnCase will present a dialogue box of the search results for when you return to the office. You have the option to write the results to the **Console** view and/or place in a bookmark note.

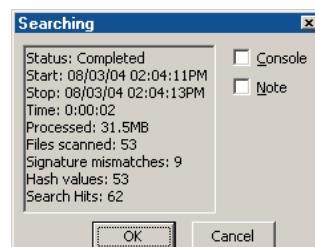


Figure 9-15 Search results

Acquiring in Windows *Without* FastBloc

Never acquire hard drives in Windows without FastBloc because Windows writes to any local hard drive visible to it. Windows will, for example, put a Recycle Bin file on every hard drive that it detects and will also change Last Accessed date and time stamps for those drives.

Media that Windows *cannot* write to is safe to acquire from within Windows such as CD-ROMs, write-protected floppy diskettes, and write-protected USB thumb drives.

Acquiring in Windows *with* a non-FastBloc Write-Blocker

EnCase cannot recognize the presence of any hard drive write-blocker, other than FastBloc. For that reason, EnCase will report that the subject hard drive is NOT protected, when it very well could be. Users of non-FastBloc write-blockers are encouraged to test their equipment and become familiar with their capabilities.

After Acquisition Is Complete

Power down the computer, power down FastBloc, disconnect the subject media and store it in a safe location, and boot your computer back into Windows. Launch EnCase and prepare to analyze the evidence.

Chapter 10

Acquiring Disk Configurations

Please see the ***Forensic Terminology*** appendix for definitions and detailed explanations of the types of Disk Configurations available. Guidance Software uses the term “disk configuration” instead of RAID.

A software disk configuration is controlled by the operating system’s software whereas a controller card controls a hardware disk configuration. In a software disk configuration, the information pertinent to the layout of the partitions across the disks is located in the registry or at the end of the disk, depending on the operating system used to build the set. The information for the hardware disk configuration, however, is stored in the BIOS of the controller card. Using each of these methods, five (5) types of disk configurations can be created: spanned, mirrored, striped, RAID-5, and basic.

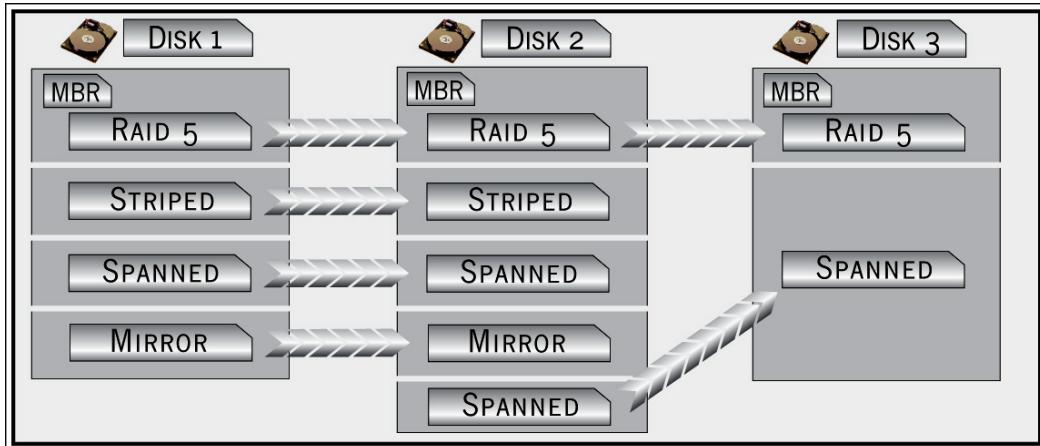


Figure 10-1 Possible setup for disk configuration

Software RAID

Windows NT: EnCase Version 4 software Disk Configurations

In a Windows NT 4 file system it is possible to use the operating system to create different types of disk configurations across multiple drives. The disk configurations possible are spanned, mirrored, striped, RAID 5, and basic. The information detailing the types of partitions and the specific layout across multiple disks is contained in the registry of the operating system used to create the disk configuration. EnCase can read this registry information and resolve the configuration based on the key. EnCase can then virtually mount the software disk configuration within the EnCase case.

There are two ways to obtain the registry key.

1. Acquire the drive with the operating system on it. It is likely that this drive will be part of the disk configuration set, but in the event it is not—such as the disk configuration being used for storage purposes only—acquire the OS drive and add it to the case along with the disk configuration set drives.
2. On the Subject PC, go to the **Windows Disk Manager** and make a backup disk by selecting **Backup** from the **Partition** option. This will create a backup disk of the disk configuration information, placing the backup on a floppy disk. You can then acquire that floppy disk and add it to the case. The case must have the disk configuration set drives added to it as well.

This situation would only work if working with a restored clone of a Subject computer. It is also possible a registry backup disk may be found at the location.

Right-click on the evidence file that contains the key and select **Scan Disk Configuration**. At this point, EnCase will attempt to build the virtual devices using the information from the registry key.

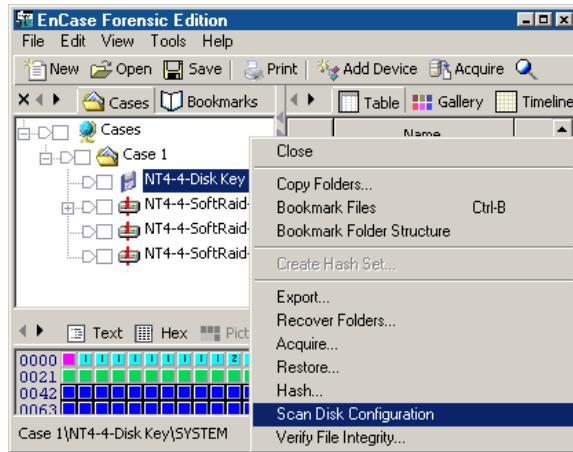


Figure 10-2 Rebuilding disk configuration with key



NOTE: It is entirely possible that the investigator will not have access to the registry key to automatically rebuild the disk configuration set. In that event, the investigator will have to manually "edit" the devices, as described in the *Hardware Disk Configuration* section below.

Dynamic Disk

Dynamic Disk is a disk configuration available in Windows 2000, Windows XP and Windows 2003 Server. The information pertinent to building the configuration resides at the end of the disk rather than in a registry key. Therefore, each physical disk in this configuration contains the information necessary to reconstruct the original setup. EnCase reads the Dynamic Disk partition structure and resolves the configurations based on the information extracted.

To rebuild a Dynamic Disk configuration, add the physical devices involved in the set to the case and, from the Cases tab, right-click on any one of the devices and choose **Scan Disk Configuration**.

If the resulting disk configurations seem incorrect, they can be manually edited via the **Edit** command in the **Devices** tab (*Figure 10-3*).

Hardware Disk Configuration

Disk Configuration Set Acquired as One Drive

Unlike software disk configurations, those controlled by hardware contain the necessary configuration information in the card's BIOS. Since the disk configuration is controlled by hardware, EnCase cannot reconstruct the configurations from the physical disks. However, since the pertinent information to rebuild the set is contained within the controller, the computer (with the controller card) will actually see a hardware disk configuration as one (virtual) drive, regardless if the set is on 2 or more drives. Therefore, if the investigator acquires the set in its native environment, the disk configuration can be acquired as one drive—by far the easiest option. The best method for performing such an acquisition would be to conduct a crossover network cable acquisition. (The EnCase Network Boot Disk for the Subject computer will have to have DOS drivers for that particular RAID controller card.) To acquire the set:

1. Keep the disk configuration intact in its native environment.
2. Boot the subject computer with an EnCase Network Boot Disk.
3. Launch EnCase for DOS (remember, the BIOS interprets the disk configuration as one drive, so EnCase will too. The investigator will see the disk configuration as one drive).
4. Acquire the disk configuration as you would normally acquire a single hard drive depending on the means of acquisition. Parallel port, crossover network cable, or “drive to drive,” acquisition of a hardware disk configuration set is straightforward, as long as the set is acquired as one drive.

If the physical drives were acquired separately, or could not be acquired in the native environment, EnCase has the ability to edit the hardware set manually (see below).

Disk Configurations Acquired as Separate Drives

Sometimes acquiring the hardware disk configuration as one drive is not possible, or the method of assembly of a software disk configuration seems incorrect. To edit a disk configuration, several items of information are required the stripe-size, start sector and length per physical disk as well as if the striping is

right handed or not. This data can be collected from the BIOS of the controller card, for a hardware set, or from the registry for software sets. To build the disk configuration:

1. Add the evidence files to one case.
2. Select **Devices** from the **View** menu.
3. Right-click on any of the evidence file rows and select **Edit Disk Configuration...** from the contextual menu.

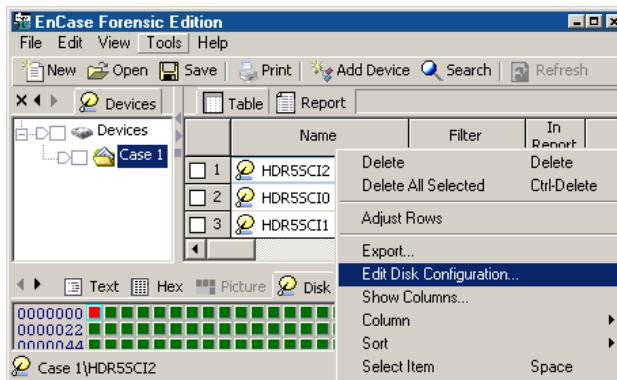


Figure 10-3 Right-click for pop-up menu, left-click for command

4. The **Disk Configuration** dialog box will appear. Right-click in the **Component Devices** field on the right, and select **New**.

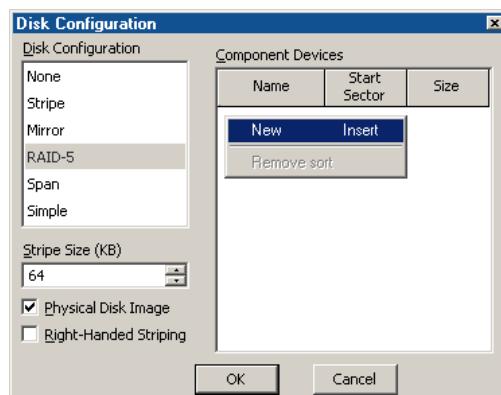


Figure 10-4 Disk Configuration settings

- For every component device involved in the set, right-click in the component devices window and select **New...**. Assign the start sector and size that the disk configuration uses on each disk.

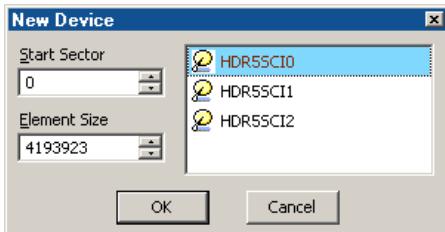


Figure 10-5 Adding devices manually

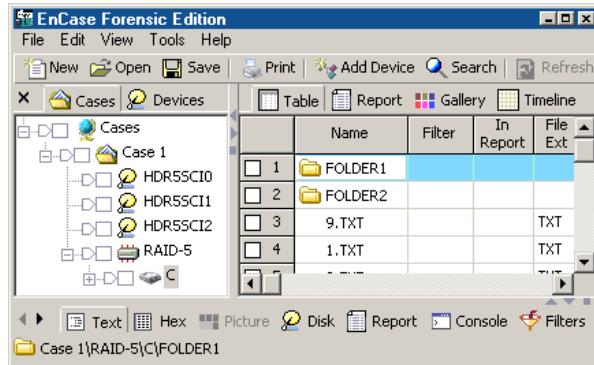


Figure 10-6 The rebuilt RAID

RAID-5 is composed of three or more disks. If one disk was missing or bad, EnCase can still rebuild the virtual disk using the parity information from the other disks in the configuration, which will be detected and done automatically during the reconstruction of hardware disk configurations using the **Scan Disk Configuration** command.

When rebuilding the RAID from the first two disks, the results of running **Validate parity** will be meaningless as you created the parity to build the missing disk.

Validating Parity on a RAID-5

The **Validate Parity** command checks the parity of the physical disks used to assemble the RAID-5. Thus, if the RAID-5 was rebuilt with a missing disk, this feature will not work. To check the parity from the Cases tab, right-click on the RAID 5 volume icon, and choose **Validate Parity** from the contextual menu.

The process will run in the lower right hand corner of the screen as a background thread.

SCSI Drives and DOS

Most hardware disk configurations are SCSI. Whether acquiring the set's drives individually or as one drive, you will probably have to acquire these SCSI drives in DOS.

If you were to attempt a DOS acquisition of a SCSI drive *without* loading any device drivers, the acquisition might work. However, the computer's BIOS would not be seeing the SCSI drive accurately. To see the SCSI drive correctly, load DOS SCSI drivers when booting the computer. The EnCase Network Boot Disk has an auto-detection and auto-loading of drivers for SCSI cards. (See *Chapter 3: Creating the EnCase Boot Disk* for the list of SCSI cards supported.)

*Copyright © 2004 Guidance Software, Inc
May not be copied or reproduced without the written permission of Guidance Software, Inc.*

Chapter 11

Acquiring Palm PDAs

A feature of EnCase is the ability to preview and acquire Palm PDAs. To successfully do so, *you must disable any and all HotSync software.*

Palms Supported

- IIIx, IIIxe
- V series
- VII series
- M series

Directions

1. Put the Palm PDA (Pilot or Handspring) in its cradle.
2. Attach the cradle cable to an available USB or serial port on the computer.
3. Boot the computer into Windows.
4. Launch EnCase and open a new case.
5. Turn the PDA on.
6. Put the PDA in Console mode as follows:
 - Using the stylus, write a lower-case cursive L (*l*) on the left side of the “graffiti” area.

Copyright © 2004 Guidance Software, Inc.
May not be copied or reproduced without the written permission of Guidance Software, Inc.

- Place a double-dot on the left side of the “graffiti” area.
- Write a number two (2) on the right-side of the “graffiti” area



Figure 11-1 Palm “graffiti” area



Figure 11-2 Input for Console mode



NOTE: The Palm is in “Console” mode when a slightly longer “beep” sound than normal is heard. If you are acquiring a USB Palm device, the device should appear in the Windows Device Manager once it’s in console mode. To get out of Console mode, you must reset the Palm as described in this chapter.

7. Click the [Add Device] button in EnCase.
8. Select **Local** and **Palm Pilot**, and then click [**Next >**].

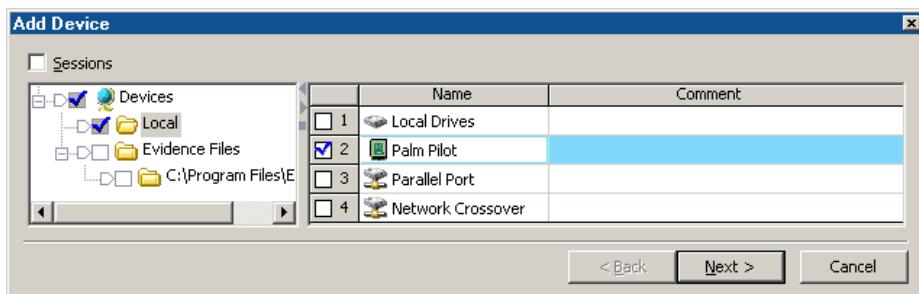


Figure 11-3 Previewing a Palm

9. You will see all serial devices attached to the computer. The figure below shows a Palm attached to COM2 (serial port). Blue-check the Palm and click the [**Next >**] button.

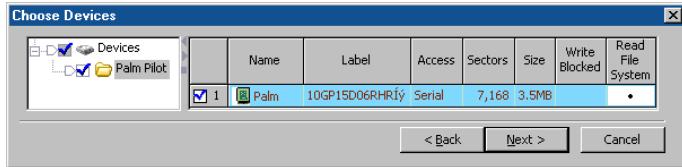


Figure 11-4: Selecting the Palm as device

10. Blue check the Palm to select it, and then click [**Finish**] to preview.

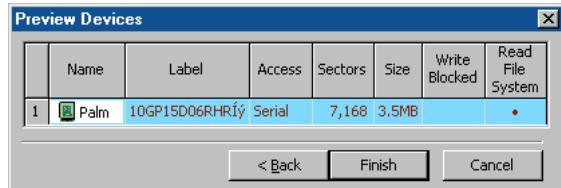


Figure 11-5 Selecting the Palm as device

11. You may double-click on the Palm if you wish to change the name or evidence number, add notes or uncheck **Read File System**. Click on the [**OK**] button to save changes.

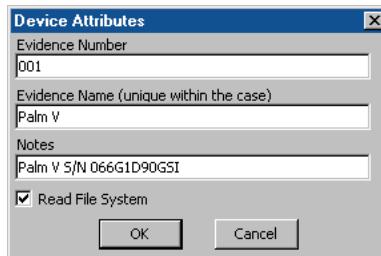


Figure 11-6 Editing device properties

12. The Palm should now appear as a device under the **Cases** tab.

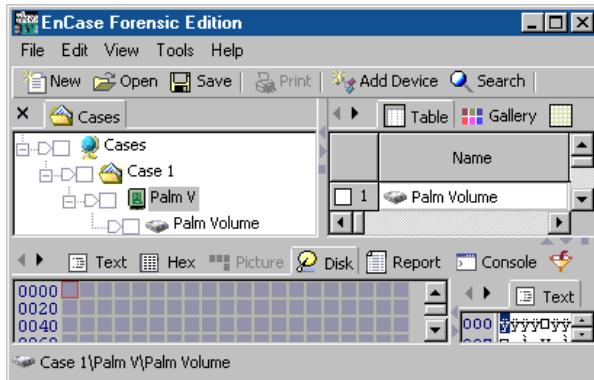


Figure 11-7 A previewed Palm

13. Right-click on the Palm icon under the **Cases** tab and select **Acquire...**, or click on the **[Acquire]** button on the top toolbar. Several options are available in the **After Acquisition** screen that appears. **Acquire another disk** is grayed out since you will not be able to acquire subsequent Palms without previewing them first.

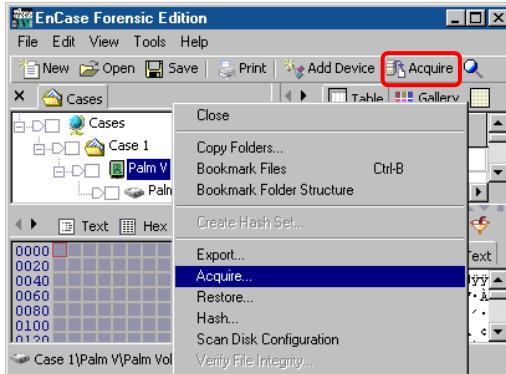


Figure 11-8 Acquiring a previewed Palm

14. The examiner has three options under **New Image File** for the evidence file once it is created:

- **Do not add** – this option will leave the evidence file in the saved location upon completion of the acquisition, but will not add it to the open Case. This is used for acquiring images to a central server or acquiring images that will not be examined immediately.

- **Add to Case** – this option will add the new evidence file to the case, but will not replace the live device (preview). This is used for adding acquired images to the case, but leaving the live access to the drive available to image other devices. It is important to note that if the case is saved with a live preview in it, when the case is reopened, it will look for the device to be physically attached.
- **Replace source device** – this option is used for hard drive acquisition or for acquiring a single piece of removable media. This option adds the new evidence file to the case, replacing the live preview. Any search hits, hashing, bookmarks, etc, of the live device during triage will be resolved to the newly added evidence file. This option is not available if you want to acquire another disk.

When acquiring a Palm, it is best to select **Replace source drive**.

EnCase gives the examiner the option of searching, hashing, and running the file signature analysis on the newly added evidence file. For these options, select **Search, Hash, and Signature Analysis**.

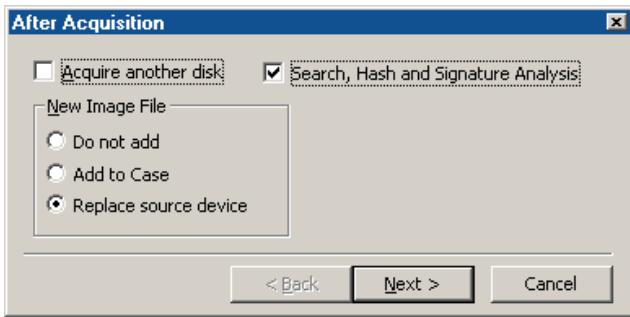


Figure 11-9 Post acquisition options

15. You will now have the **Search** options available. You should select the desired keyword(s) to search before starting the acquisition process, unless you wish to search all of the available keywords. If the desired keywords are not already selected in the **Keyword** view, select **Cancel**, go to the **Keyword** view, select or enter in the desired keywords, return to the **Case** view and start the acquisition process again. The **Search** window gives examiners the option of search and analyzing all of the devices in the case by selecting **Search entire case**. If the option is not selected, EnCase will only search and analyze the new evidence file after its creation.

The examiner has several analysis options available:

- **Search each file for keywords** – this option will search each file for the desired keywords, in the entire case or just new evidence file as selected by the examiner.
- **Verify files signatures** – this option will compare the file extensions and file header/signature of each file, in the entire case or just new evidence file as selected by the examiner.
- **Compute hash values** – this option will compute the hash value of the logical file area of each file and compare the value to the hash library, in the entire case or just new evidence file as selected by the examiner.
- **Recompute hash values** – this option will recompute all previously computed hash values generated for the files of the replaced live device. This is most often used for acquisitions over the enterprise network, to recompute the values of the files on the live machine if a hash analysis was conducted previously. This option is not necessary for local acquisitions.

There are four options for the searching if it is selected:

- **Search file slack** – this option will include searching the file slack (area between the logical and physical areas of the file) of each file, in the entire case or just new evidence file as selected by the examiner.
- **Undelete files before searching** – this option will logically “undelete” deleted files prior to searching. If a file is deleted, EnCase and other tools can determine if the assigned starting cluster is not assigned to another file (if it is assigned, then the file is Deleted-overwritten). The unallocated clusters after the starting cluster may or may not belong to the deleted file. Choosing this option assumes the unallocated clusters after the starting cluster do belong to the deleted file. This is the same assumption made when copying out a deleted file. This option finds keyword fragmented between the starting cluster and the subsequent unallocated cluster. If determining the presence of a keyword on the media is critical to an investigation, the examiner should also search for portions of the keyword, including GREP expressions of fragments of the keyword.

- **Search only slack area of the files in the Hash Library** – this option will exclude the logical area of files for which their hash values matches that of a file in the Hash Library. The slack area of the physical file will still be search, in the entire case or just new evidence file as selected by the examiner.
- **Selected keywords only** – this option will have EnCase search only the keywords selected in the Keywords view rather than all available keywords, in the entire case or just new evidence file as selected by the examiner.

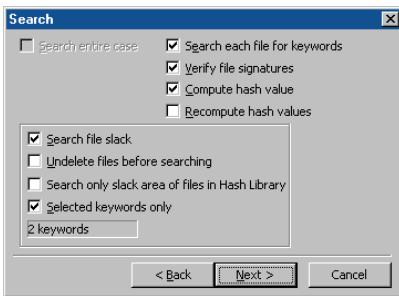


Figure 11-10 Search and analysis options

16. Choose [**Next >**] after selecting options. The last window will provide acquisition options for the generation of an evidence file.

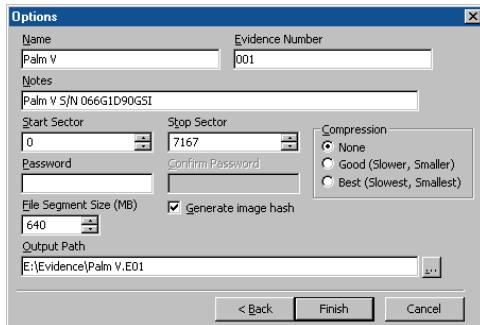


Figure 11-11 Evidence file options

17. After selecting [**Finish**] EnCase will begin the acquisition process. The progress bar indicates the status in the lower right hand corner. The acquisition may occur quickly since it is acquiring directly from RAM.

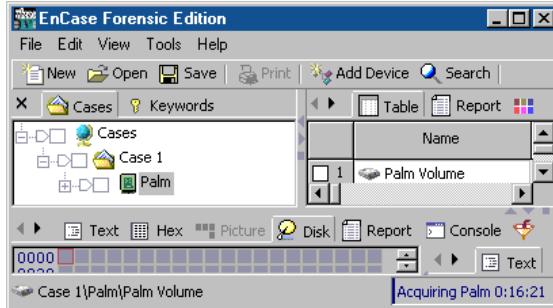


Figure 11-12 Acquisition status

18. When the acquisition is complete, EnCase will replace the live previewed device with the new evidence file and begin the verification of the evidence file.
19. When the verification is complete, EnCase will begin the searching and other analysis of the evidence file.

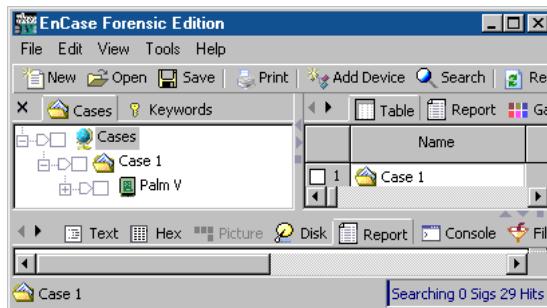


Figure 11-13 Searching after acquisition and verification

20. When all processes are complete, EnCase will present a dialogue box of the search results for when you return to the office. You have the option to write the results to the Console view and/or place in a bookmark note.

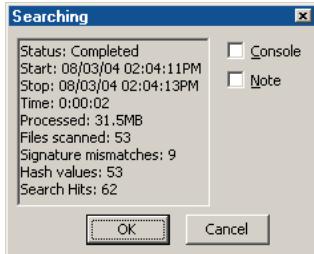


Figure 11-14 Search results

Getting Out of Console Mode

To get a Palm out of “console mode,” you must do a soft reset on the Palm. Turning the Palm off and back on again does not take it out of console mode, and leaving it in console mode will cause the battery to drain faster than usual.

1. Locate the small hole on the back of the Palm labeled “RESET.”
2. Press the tip of a pen into the hole.

One Final Note on Palms

Initially previewing a serial Palm PDA may be slow because standard serial ports transfer data at a max of 115kbps. The preview and acquisition of a Palm Vx, for example, takes between 30 and 40 minutes. USB Palms will be faster; a 12MB m500, for example, took four minutes to preview and 16 minutes to acquire. However, *after* the first keyword search on a previewed device, all other processes accessing the evidence file will be fast, as the entire evidence file has been cached in memory.

*Copyright © 2004 Guidance Software, Inc.
May not be copied or reproduced without the written permission of Guidance Software, Inc.*

Chapter 12

Acquiring Removable Media

Zip and Jaz disks, flash media, and floppy disks are among the many other forms of media besides hard drives that the forensic investigator must be able to acquire. EnCase supports the acquisition of many forms of removable media.

Zip / Jaz Disks

Since the physical hardware on a Zip or Jaz drive does not allow for hardware write blocking, they should be acquired in DOS. Be sure you are running the latest version of EnCase on the forensic machine (downloadable at http://www.guidancesoftware.com/support/EnCaseForensic/version4/download_login.asp). Perform the acquisition as follows:

1. Download the EnCase Barebones Boot Floppy Image from <http://www.guidancesoftware.com/support/downloads/packets/bootfloppy.E01> and save the file to C:\Program Files\EnCase4.
2. Open EnCase and from the **Tools** menu, select **Create Boot Disk...**
3. With a blank floppy in the drive, leave **A** selected as **Target Diskette** and click on the [**Next >**] button.

Copyright © 2004 Guidance Software, Inc.
May not be copied or reproduced without the written permission of Guidance Software, Inc.

4. Select **Overwrite diskette with a boot floppy base image**, then click on the ellipsis box next to **Image Path** to set the path to C:\Program Files\EnCase4\bootfloppy.e01 (by default, bootfloppy.e01 is selected)
5. At the **Copy Files** window, right click in the window and select **New**. Select C:\Program Files\EnCase4\EN.EXE and click [**Open**], then click [**Finish**]. Click [**OK**] to close the boot disk creation session.
6. Click on the [**Next >**] button.
7. Create a temporary directory (such as C:\IOMEGA\TEMP), download the executable to create GUEST.EXE from Iomega's web site (<ftp://download.iomega.com/english/iodrv-dos-x86-10.exe>), saving it to the newly created folder.
8. Go to the temporary folder and double-click on IODRV-DOS-X86-10.EXE to extract the files.
9. Copy all the expanded files in that directory (except IODRV-DOS-X86-10.EXE and AUTORUN.EXE) to the floppy (A:).
10. Shut down the forensic machine (or suspect machine) with a storage drive and Zip drive, removing the cables to all the drives (including the Zip or Jaz drive).
11. Boot the machine and ensure that the BIOS is configured to boot from floppy only.
12. Shut the machine down, connect the cables to the storage drive and Zip or Jaz drive, and put the boot floppy in the diskette drive.
13. Boot the machine.
14. At the A:\> prompt, type GUEST.EXE.
15. Run EnCase by typing EN.EXE, adding the /B switch if you get "divide by" errors.

The Zip or Jaz drive may be viewed as both a physical disk and a logical volume. Acquire in DOS as you would normally acquire a hard drive.

Floppy Disks

Floppy disks can be acquired safely in either DOS or Windows. Write-protect the floppy disk and insert it into the floppy drive. Launch EnCase and acquire the floppy.

Write-Protecting a Floppy Disk

Floppy disks have a sliding tab that allows a disk to be write-protected, preventing any writes from taking place on the diskette. A write-protected ("locked") floppy disk has a hole in the upper-right corner.

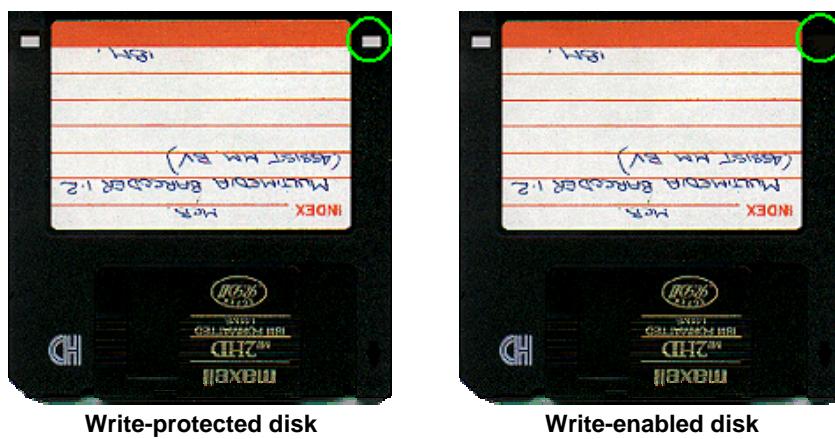


Figure 12-1 Write protecting a floppy disk

Superdisks (LS-120)

To acquire an Imation Superdisk, the investigator needs a drive that can load and recognize them. Superdisks have a physical write-protect tab on them, much like floppies do, and can be acquired in Windows in the same manner as a floppy disk.

CD-ROM, CD-R, CD-RW

CD-ROM, CD-R, and CD-RW disks can be acquired safely in Windows by EnCase. Place the CD into the drive and attempt to acquire with EnCase.

There are several issues that should be reviewed when a CD cannot be acquired. If the CD is formatted using UDF, this may cause CD-burning applications to take hold of the CD and prevent EnCase from recognizing it. To remedy this, you

may need to disable or uninstall the CD burning application. For example, Roxio Easy CD Creator also loads an application (Direct CD) that launches at startup and runs in the background in Windows to recognize open session CDs.

Some types of CDs are viewable or recognized properly only if viewed using the correct hardware (e.g., CD reader, CD reader and writer, DVD-R, DVD+R, etc.) Other issues specific to CD-R, CD-RW, and CD-R/RW drives may contribute to EnCase being unable to acquire or even preview a CD-R or CD-RW; for a discussion on this issue, please review our message board.

If a CD cannot be acquired, wipe and format a small hard drive and copy the active files from the CD to this drive. Acquire the drive with EnCase. All file date and time stamps will have to be documented in other ways (such as looking at the CD-R in Windows and noting the file date/time stamps there).

Flash media

Flash media are memory storage cards for a number of portable devices such as PDAs, cell phones, and digital cameras. These are small matchbox-sized cards that can store data, music, applications etc. They are most commonly used in digital cameras to store images and transfer data from one portable device to another.

These cards come in different sizes and have different storage capacities. For example, Compact Flash cards can be found in digital cameras and pocket PCs and can store from 8MB of data up to 1GB.

Some of the most common flash media devices are Compact Flash, Smart Media, and Memory Stick.

Equipment needed to preview/acquire flash media

Flash Card reader/writers are relatively inexpensive. If possible, purchase a flash card reader to confirm that the process of examining this media is forensically sound. Most flash card readers connect via USB so ensure that a USB port is available. Check that the flash card reader is compatible with the operating system running.

It is a good idea to buy a 5-in-1 flash card reader that has the ability to read data from different size cards, such as Compact Flash, Smart Media, and Memory Sticks.

How to acquire flash media

1. Place the flash card into the reading device and confirm all necessary device drivers are loaded.
2. EnCase will recognize the flash card reader as a local device with a logical drive letter. It can be previewed or acquired as you would a local hard drive.
3. If acquiring in Windows, EnCase cannot put a write-lock on the device. If either the memory card itself or the flash card reader has a write-lock facility, make sure this is set to the “lock” position.
4. Most flash media use the FAT file system. Examining data on them is much like examining your average hard drive. It is possible to search both allocated and unallocated space.

Examining flash media

Images taken using a digital camera generally have unique image headers, specific to the camera manufacturer. The File Finder EnScript has a tab (**Custom File Type**) that allows you to search for files with a specific header, footer and extension. Examine live image files in text view to determine the header and footer information, and run a search for them across unallocated space.

When examining images from digital cameras, Exif Reader can be used to analyze additional information that can be embedded within digital camera images and may show what make/model camera the image came from, time and date stamps, and other exposure/resolution/shutter speed information. The application can be downloaded at www.takenet.or.jp/~ryuuji/minisoft/exifread/english/.

Acquiring Multiple Pieces of Media

When acquiring multiple pieces of removable media, put a check box next to the **Acquire another disk** option in the **After Acquisition** screen.

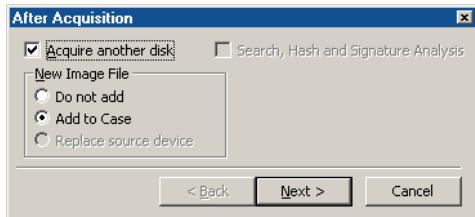


Figure 12-2 Post acquisition options

The **Options** window will appear for the examiner to enter the case information and other evidence file options.

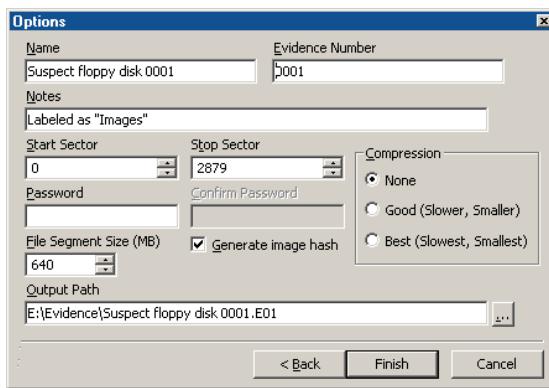


Figure 12-3 Acquisition Options window

At the conclusion of the acquisition, a dialogue box will appear with the option to save the results in a bookmark note and/or write to the Console view.

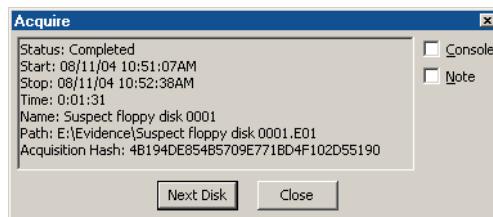
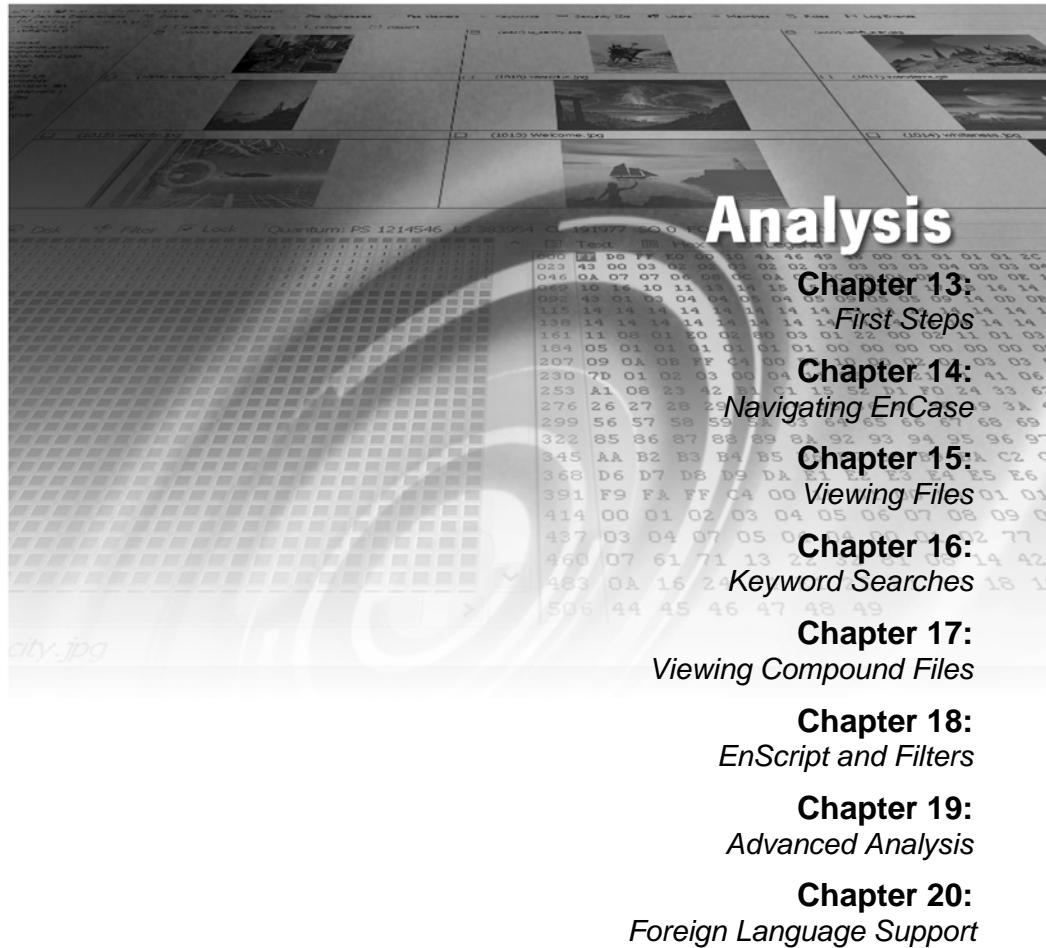


Figure 12-4 Acquisition status

If you wish to acquire another piece of media in the same drive, eject the current device and insert the next piece of media. Choose [**Next Disk**] to acquire the next piece of media, or [**Close**] to finish. If you choose [**Next Disk**], EnCase will read the device without requiring you to preview using the [**Add Device**] function.

After the last piece of media is acquired, choose [**Close**]. In the Case view, right-click the live device with the blue triangle and choose **Close**, removing it from the case.

*Copyright © 2004 Guidance Software, Inc.
May not be copied or reproduced without the written permission of Guidance Software, Inc.*



Chapter 13

First Steps

The chapter describes several features of EnCase that should be used at the start of any investigation. Whether responding to an incident, conducting an electronic discovery request, or auditing workstations, these steps are designed to save time and help ensure an accurate display of all data pertaining to the case.

Time Zone Settings

Often media in the same case originates from different time zones, which makes comparing the times of different events difficult. EnCase Version 4 allows, but does not require, the investigator to set the time-zone setting for each piece of media in the case independent of the system time zone, and independent of the other pieces of media in the case. The user can also view all dates relative to one consistent time zone, if desired.

When a new time zone is assigned, dates and times in GMT-based file systems such as NTFS will be adjusted accordingly. File systems, such as FAT16 and FAT32, which save dates and times in local time, will not display adjusted times when a new time zone is assigned. However, setting the time zone on a local-time system is important when dealing with case-level time settings; it lets EnCase know what time zone the system was originally in.

Copyright © 2004 Guidance Software, Inc
May not be copied or reproduced without the written permission of Guidance Software, Inc.

With regard to Daylight Saving Time, EnCase checks the date portion of an entry, determines if it falls within standard or daylight time (if applicable), and displays the adjusted time. To disregard seasonal settings, uncheck **Account for seasonal Daylight Saving Time adjustment** in the **Case Time Settings** dialog box (*Figure 13-3*). To modify a time zone setting for a piece of media, right-click on the media and select **Modify Time Zone Settings...** from the contextual menu.

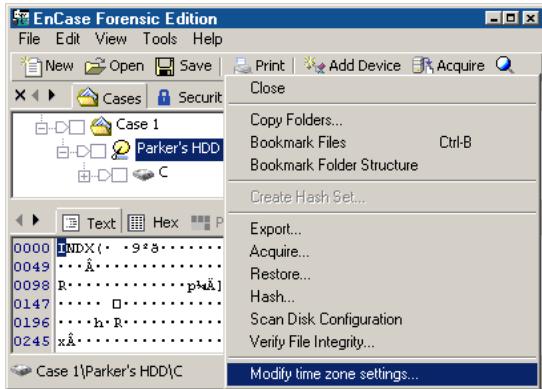


Figure 13-1 Time zone settings

Select the time zone for the piece of media (*Figure 13-2*). The default settings are read from the investigating computer's registry and displayed at right. If time zone settings are not specified, EnCase will default to deriving the date and time stamps from the current Windows registry settings on the investigating computer.

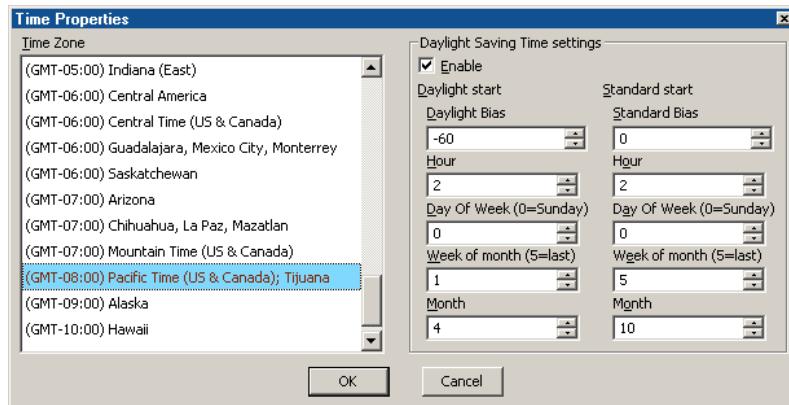


Figure 13-2 Time zone settings

EnCase also enables the user to show all dates in a case relative to the same time zone. For example, if the investigator is interested in comparing the times of activities that occurred across multiple machines, it may be advantageous to view them in one time zone. Activity which occurred at 5 pm Eastern time and 5pm Pacific time did not occur at the same time relative to each other, so the investigator can choose to view the case in Pacific time; then, the time on Disk 1 (Pacific) will display as 5 pm, and the time on Disk 2 will display as 8 pm (5 pm Eastern).

To modify the case-level time zone settings, right-click on the desired case and select **Modify Time Settings...** from the contextual menu.



Figure 13-3 Choose desired time zone and daylight offset

By default, the checkbox to convert all dates to correspond to one time zone is unselected. To enable this feature, select the checkbox and the desired Time Zone to apply (Figure 12-3). Because this feature adjusts the times to a standard offset, you must choose whether to adjust for standard or daylight time as well (if applicable to the selected time zone).

Recover Folders on FAT Volumes

After adding an evidence file to a case, run **Recover Folders** on all FAT partitions by right clicking on each device and selecting **Recover Folders** as illustrated in *Figure 13-4*. Folder recovery on NTFS and other partition types are covered in following sections. This command searches through the unallocated clusters of a specific FAT partition for the “dot, double-dot” signature of a

deleted folder; when the signature matches, EnCase can rebuild the files and folders that were *within* that deleted folder.

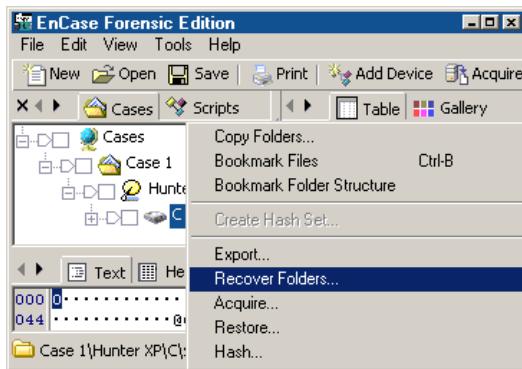


Figure 13-4 Recover folders

Behind the Scenes with Recover Folders

Typing “DIR” at a DOS command prompt will show two directories under every folder on that partition (including the root directory) - one folder with a dot (.) and another with a dot\double-dot (..). Every folder/directory in a FAT partition has dot\double-dot entries. These directories tell the file system where the directory entries for it and the parent reside. EnCase searches through the unallocated clusters for this signature and recovers folders that have been deleted with their directory entries overwritten in the parent directory. The contents of the directory, however, have not necessarily been overwritten. Though EnCase will not recover the names of these deleted folders (because the name was overwritten in the parent directory), it will attempt to recover everything that is within these folders (files and sub-folders), filenames included.

This is an important command to run, especially on formatted drives. This command can quickly and easily recover most of a formatted drive’s information.

This command is available only when an evidence file *volume* is highlighted. Right-click on a volume under the Cases tab and select **Recover Folders**. After the process executes, a gray folder labeled “Recovered Folders” appears in the Case view. The folder labeled **Recovered Folders** will not appear until EnCase has searched through the entire volume for deleted folders. If folders are recovered, you will be prompted to rescan the volume.

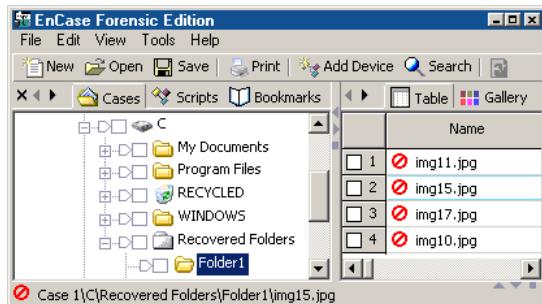


Figure 13-5 Recover Folders results



NOTE: Let **Recover Folders** finish before running any further analysis on the drive. Other EnCase functions, such as keyword searches, will prompt you to terminate the **Recover Folders** command. If you do so, you will lose any folders recovered to that point.

Recovering NTFS Folders

EnCase can recover NTFS files and folders from Unallocated Clusters and continue to parse through the current Master File Table (MFT) records for files without parent folders. This is particularly useful when a drive has been reformatted or the MFT record is corrupted. Lost files that are recovered are placed in the gray **Lost Files** virtual folder in the root of the NTFS partition. The following example was reformatted NTFS. The dates and times of the internal NTFS files are identical, reflecting the time the partition was formatted as NTFS.

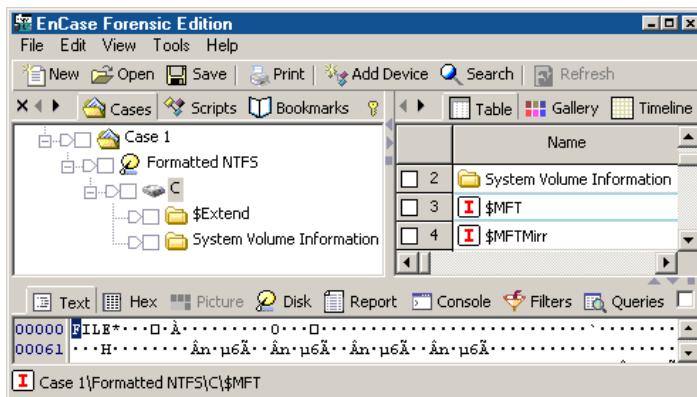


Figure 13-6 Formatted NTFS partition

To recover folders on an NTFS partition, right-click on the volume and select **Recover Folders**.



Figure 13-7 Recovering Folders on an NTFS volume

EnCase will open a window to confirm the user wishes to scan the volume for folders. Choose [OK] to begin the search for NTFS folders, or [Cancel] to cancel the request.

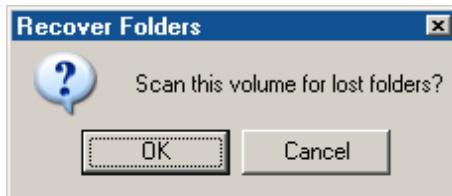


Figure 13-8 Choose OK to begin

EnCase will begin searching for MFT records in the Unallocated Clusters. In the bottom right-hand corner a progress bar indicates the number of MFT records found and the approximate time required to complete the search.

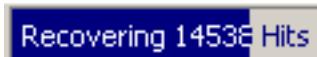


Figure 13-9 Progress bar for MFT record search

After EnCase locates the MFT records in the Unallocated Clusters, a prompt appears showing the number of entries found. Duplicate or false hits are parsed, so the number of entries that appears in the prompt may be lower than that reported during the recovery. If [OK] is pressed, EnCase will resolve the recovered MFT records to data on the volume, and attempt to rebuild the folder structure with children files and folders under parent folders. This process can take a long period of time, however, the results will greatly benefit examinations of NTFS volumes.

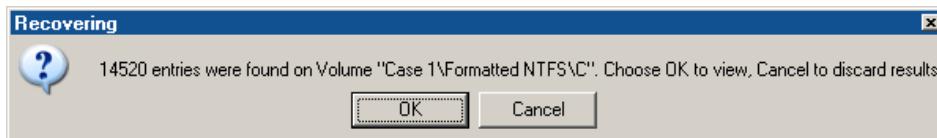


Figure 13-10 Viewing recovered MFT records

Since rebuilding the folder structure may take a long time, and users may opt to have faster access to the recovered files, if the recovered MFT entries in the unallocated space are NTFS4, the user will be given a choice to either have EnCase process the entries for parent/child relationships, or place all recovered entries into the Lost Files folder immediately (with no folder structure). This dialog box, introduced in version 4.17, includes the number of passes required to sort the entries. This number may be large; however, most passes will likely

process instantly. The length of time required to process a given group depends only on the number of records within that group. This change does not affect NTFS5 recovered entries; these entries will be processed quickly as before. If the user chooses to process the entries for the folder structure, the progress bar will indicate which pass, of the total required, is currently running. The recovered folder structure is placed under the virtual Lost Files folder.

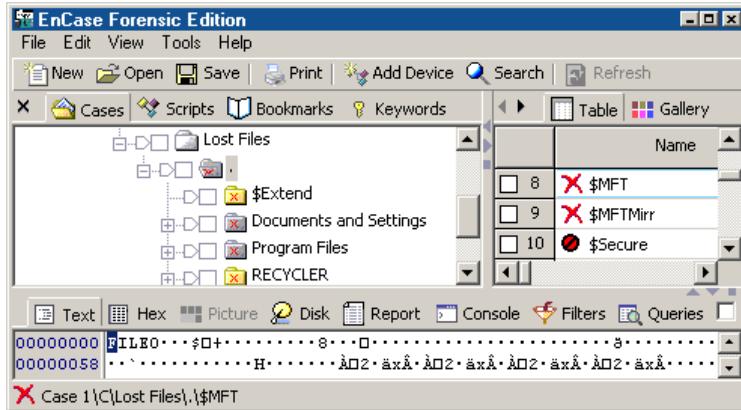


Figure 13-11 Recovered folder structure from a formatted NTFS drive

Lost Files in UFS and EXT2/3 Partitions

EnCase uses a different method for recovering deleted files and folders that have no parent in UFS and EXT2/3 partitions. When you preview a computer or add an evidence file that contains one of these partitions to EnCase, you will notice that a gray folder called **Lost Files** is automatically added to the **Cases** view underneath each partition.

In the Master File Table (MFT) in NTFS, all files and folders are marked as a folder or file and as belonging to a parent. The files within a folder are that folder's children. If a user first deletes the files, then deletes the folder, and then creates a new folder, the originally deleted files can be lost. The new folder's entry in the MFT overwrites the deleted folder's entry. The original parent folder and its entry in the MFT are overwritten and gone. Its children, however, have not been overwritten and their entries are still in the MFT. As with NTFS, with UFS and EXT2/3 partitions, EnCase parses the MFT and finds those files that are still listed, but have no parent directory. All of these files are recovered and placed into the gray **Lost Files** folder.

Signature Analysis

File Signatures

There are thousands of file types, some of which have been standardized. The International Standards Organization (ISO) and the International Telecommunications Union, Telecommunication Standardization Sector (ITU-T) are working to standardize different types of electronic data. Typical graphic file formats such as JPEG (Joint Photographic Experts Group) have been standardized by both of these organizations. When file types are standardized, a signature—or *header*—that programs can recognize usually precedes the data. File headers are associated with specific file extensions.

File extensions are the characters following the dot in a filename. They reveal the type of data that the file represents. For instance, if a filename contains a .TXT extension, it would be expected that the file type would be “text”. Many programs rely specifically on the extension to reflect the proper data type. Windows, for example, associates file types with their corresponding applications by use of file extensions.

One tactic to try to hide the true nature of a file is to rename the file and extension. A JPEG (image file) that has an incorrect extension such as “.dll” will not be recognized by most programs as a picture. It is therefore essential to compare each file’s signature with its extension to identify any files whose extensions have been deliberately changed. EnCase performs the Signature Analysis function in the background. Before running a signature analysis, familiarize yourself with how EnCase accesses and classifies file signatures. Select **File Signatures** from the **View** pull-down menu.

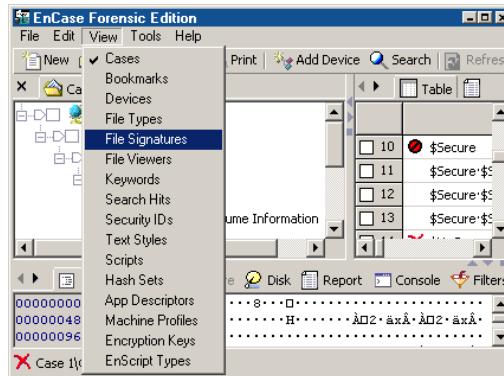


Figure 13-12 File Signatures option

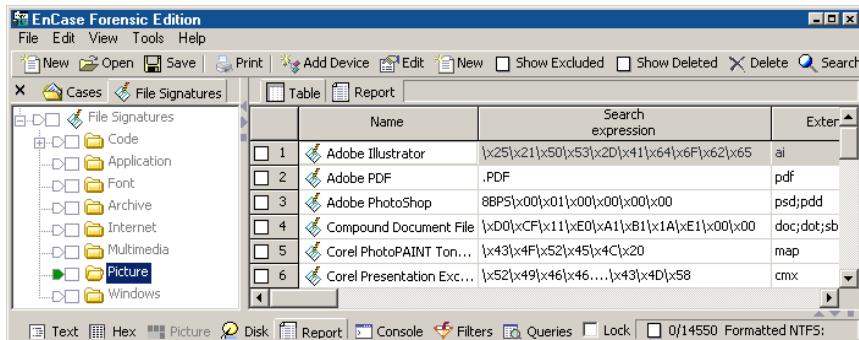


Figure 13-13 Pictures File Signatures

Adding a New Signature

Right click on a signature in the table and select New to add a file signature, or Edit to change an existing one. If a new type of file is found that is not already in the **File Signatures** list (and thus does not have a “viewer” associated with it), the file extension can be added to the File Signatures table and an association created between a viewer for that file and the file type, such as an MP3 player for MP3 files.

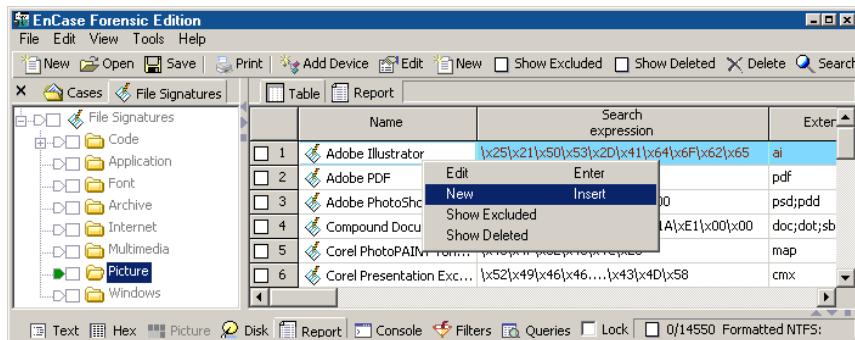


Figure 13-14 Adding a new File Signature

Add or edit a new file signature by filling in the boxes appropriately.

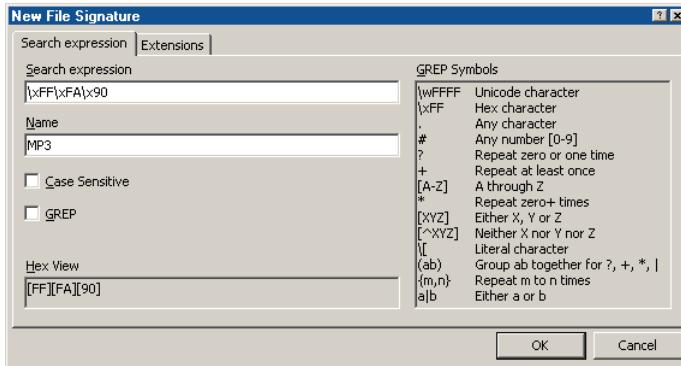


Figure 13-15 Adding an MP3 signature

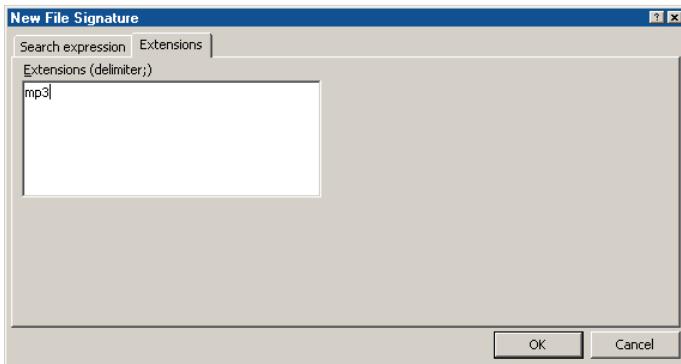


Figure 13-16 Adding an MP3 signature

Starting a Signature Analysis

Signature Analysis is part of the search function. To begin a Signature Analysis, click on the **Search** button on the top toolbar.

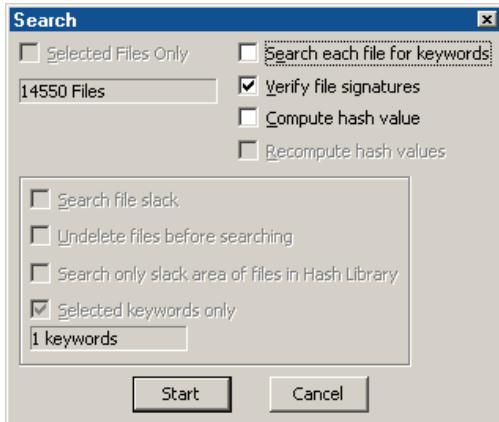


Figure 13-17 Running a signature analysis only

In the dialogue box, check *only Verify file signatures*, and then click [**Start**]. The signature analysis will run in the background until complete. When the process completes, save the case.

Viewing the Results

With the Case tab in Table view, display all files in the case by clicking the **Select All** trigger (“home plate”) so that it turns green.

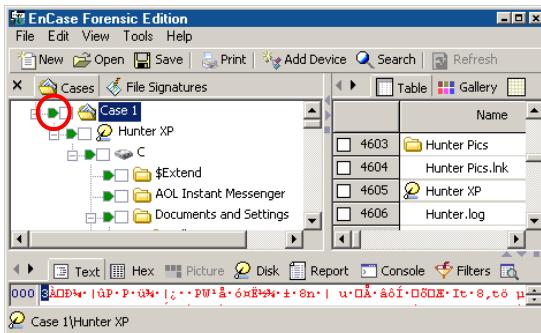


Figure 13-18 “All Files” trigger

Click and drag the columns in the Table view so that the **File Name**, **File Ext**, and **Signature** column are next to each other. Once the column order is set, sort the columns with **Signature** at first level, **File Ext** at second level and Name at third level. To sub sort, hold the [**Shift**] key while double-clicking on the column header.

The screenshot shows the EnCase Forensic Training Edition interface. On the left is a tree view of a case structure under 'Case 1' (Hunter XP). On the right is a table view titled 'File Signatures'. The table has three columns: 'Name', 'File Ext', and 'Signature'. The rows show file entries: 3 (loadfix.com, com, ! Bad signature), 4 (NTDETECT.COM, COM, ! Bad signature), 5 (00000185.DAT, DAT, ! Bad signature), and 6 (00000186.DAT, DAT, ! Bad signature). The 'Signature' column is sorted by value, 'File Ext' by extension, and 'Name' by file name. Row 4 is currently selected.

	Name	File Ext	Signature
3	loadfix.com	com	! Bad signature
4	NTDETECT.COM	COM	! Bad signature
5	00000185.DAT	DAT	! Bad signature
6	00000186.DAT	DAT	! Bad signature

Figure 13-19 Signature analysis results with column changes and sorts in place

To examine the signatures, scroll up or down while viewing the signatures column. The results are described below:

- **!Bad Signature** – A file extension has a header listed for it in the File Signature table, but the header of the file found in the case does not match the one in the File Signature table for that extension. The header is incorrect. This could indicate that the header is not known and should be added in the File Signature table.
- ***[Alias]** – The header is in the File Signature table and the extension of the file in question is incorrect. This indicates a file with a renamed extension.
- **Match** – The header matches the extension. If the extension has no header in the File Signature table, EnCase will return a match as long as the header of the file does not match any header in the File Signature table.
- **Unknown** – Neither the header nor the file extension is in the File Signature table.

Hash Analysis

File Hashing

The **Hash** feature of EnCase allows the investigator to create a *hash value*—a “digital fingerprint”—for any file. The hash value for each file is unique, for all practical purposes. Only a copy of a particular file will yield the same hash value. (EnCase uses the MD5 algorithm to create hash values; the likelihood that any two files have the same hash value is 2^{128} .) By building a library of hash values, EnCase is used to check for the presence of data with a hash value contained in the hash library. The hash value is determined by the file’s contents. It is independent of the file’s name, so the file’s hash value will be calculated by EnCase, and identified as matching a value in the hash library even if the file’s name has been changed.

The hash feature can be used to identify files whose contents are known *not* to be of interest to the examiner, such as operating system files and common application programs, as well as to identify files of interest, such as known Trojans, Root Kits, and unauthorized applications.

Hash sets are collections of hash values (representing unique files) that belong to the same group. For example, a hash set of all Windows 98 operating system files could be created and named “Windows System Files.” When a hash analysis is run on an evidence file, EnCase will identify all files included in that hash set. Those (logical) files can then be excluded from searches and examinations, speeding up keyword searches and other analysis functions.

Creating a Hash Set

Hash Sets can be created with any category name, although most filters in EnCase are designed for use with either “Known” or “Notable” category names. Known files are benign or innocuous files that have little bearing on a case, such as Windows operating system files or Microsoft Office 2000 application files.

Notable files, on the other hand, would be files that might indicate criminal activity, such as hacker tool files, or child pornography sets.

To create a hash set, preview a machine or open an evidence file that contains the files that are going to be in the new hash set. You will need to make sure that EnCase recognizes the hash value of the files. Create the set as follows:

1. Blue-check the files to be added into the new hash set.
2. Click on the **Search** button on the top toolbar and check only the **Compute hash value** option. If the file already has a hash value listed in the Hash Value column of the Table in *Cases* view, and you wish to have EnCase recompute it to ensure you are using the correct hash value, you can also check the **Recompute hash values** option. After selecting these items, click [**Start**].

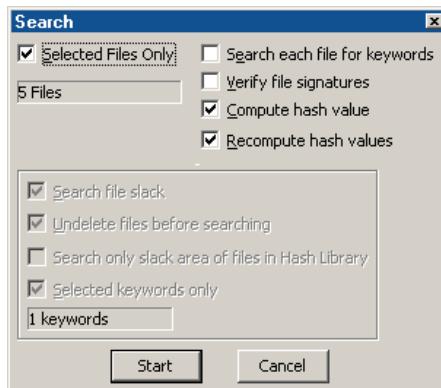


Figure 13-20 Computing hash values

3. A status window will report the number of hash values generated. Click [**OK**] to close the window, and then verify that the values appear in the Hash Value column of the Table in *Cases* view.

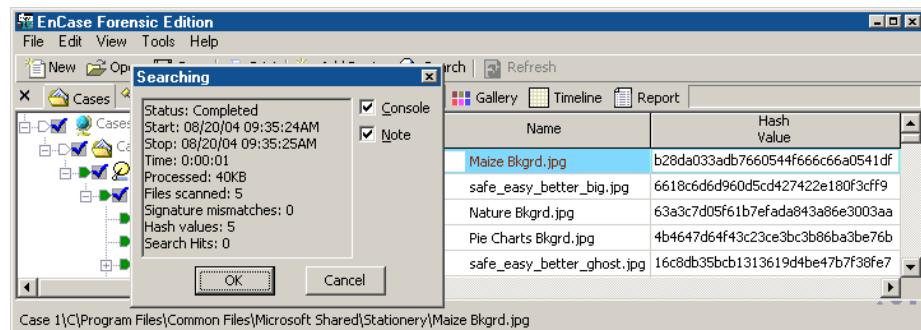


Figure 13-21 Generating hash values for selected files

4. Right-click in the Table or Gallery view and select **Create Hash Set**.

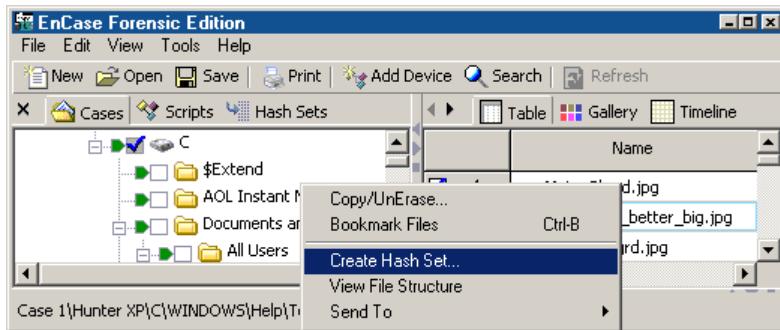


Figure 13-22 Creating hash set

5. Enter the **Hash Set Name** and **Category**, and then click [OK].

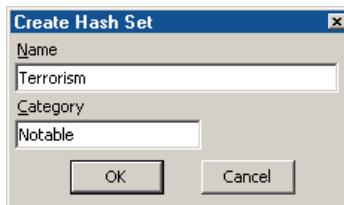


Figure 13-23 Hash Set Name and Category

You can blue-check, create, and add as many hash sets as desired.

Importing Hash Sets

EnCase supports importing hash sets from the HashKeeper and the National Software Reference Library (NSRL) CDs.

HashKeeper

HashKeeper, a program maintained by Heather Strong of the National Drug Intelligence Center, is an exhaustive library of hash sets for almost every operating system and application. This is a valuable resource for law enforcement. The HashKeeper CD is available exclusively through Heather Strong (heather.strong@usdoj.gov) to members of the law enforcement community.

To import HashKeeper sets:

1. Copy hash sets from the HashKeeper CD to the C:\Program Files\EnCase4\Hash Sets folder. These files should have .HKE and .HSH extensions. These may be compressed using WinZip, or renamed with a .TXT extension. If the files have a .TXT extension, change them to .HKE.

2. From the **View** menu, select **Hash Sets**.

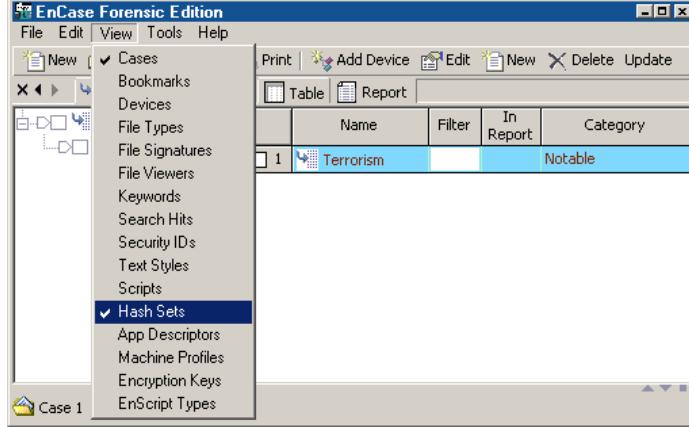


Figure 13-24 Hash Sets

3. Right-click and select **Import HashKeeper....**

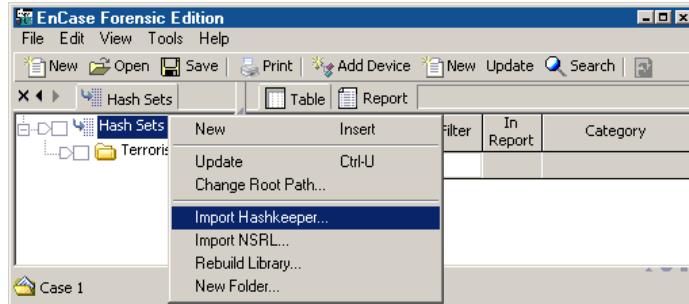


Figure 13-25 Import HashKeeper option

4. A dialogue box will come up, prompting for files with an .HKE extension. Navigate to the folder you copied the .HKE files to and select the ones you wish to import. You can import multiple files by holding down the [Ctrl] button and clicking on each of the desired files. Click [Open] to import the files.

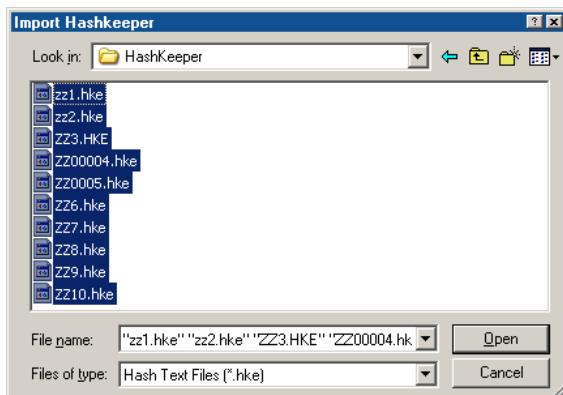


Figure 13-26 Browsing for HKE files

5. Right click in the table and select **Update** to view the newly imported hash sets.

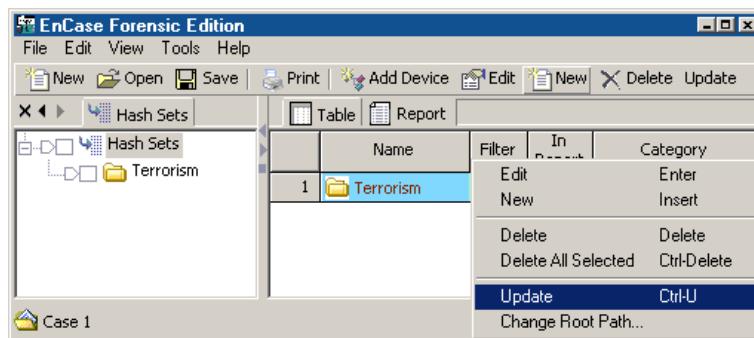


Figure 13-27 Update hash sets

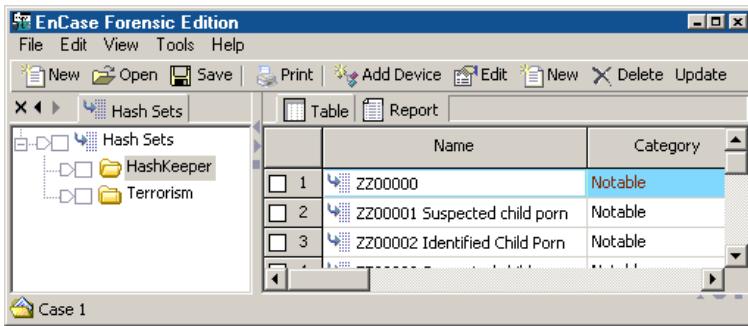


Figure 13-28 Imported hash sets

NSRL Hash Sets

The National Software Reference Library (NSRL) compiles a Reference Data Set CD, which is available at <http://www.nsrl.nist.gov>. This CD contains hundreds of hash sets of Known file types.

To import hash sets from the NSRL Reference Data Set CD:

1. Extract the files from the .ZIP file on the NSRL CD to C:\Program Files\EnCase4\Hash Sets.
2. Launch EnCase, and from the **View** menu, select **Hash Sets**.
3. Right-click and select **Import NSRL...**

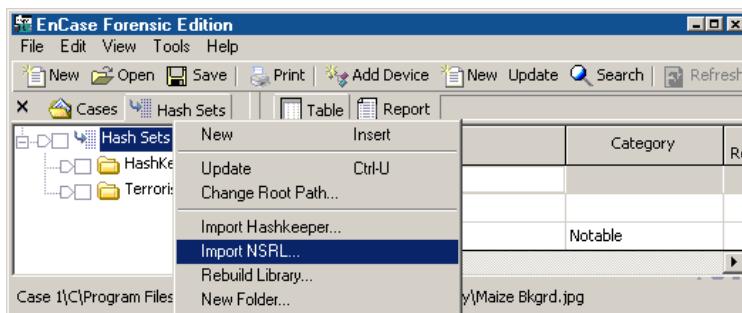


Figure 13-29 Importing NSRL hash sets

4. Browse to the folder where you expanded the .ZIP file and select the NSRLFile.txt, then click [Open].

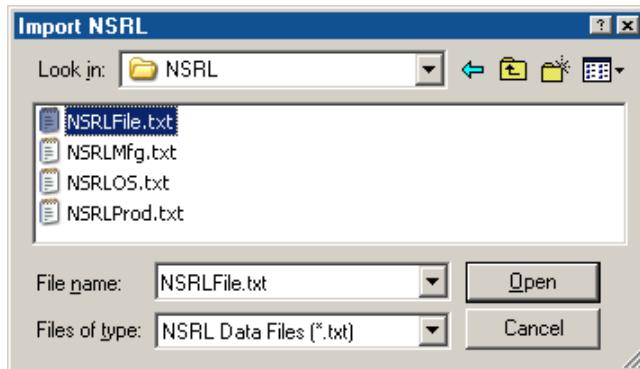


Figure 13-30 Selecting the NSRLFile.txt file

5. The NSRL hash sets will start importing, as indicated by the blue progress bar in the lower right corner of the EnCase window. When the files are imported, EnCase will then read the hash values, which will also be reflected by the progress bar. Finally, EnCase will create the hash sets in the background. Depending on the number of files in the file, this may take some time.

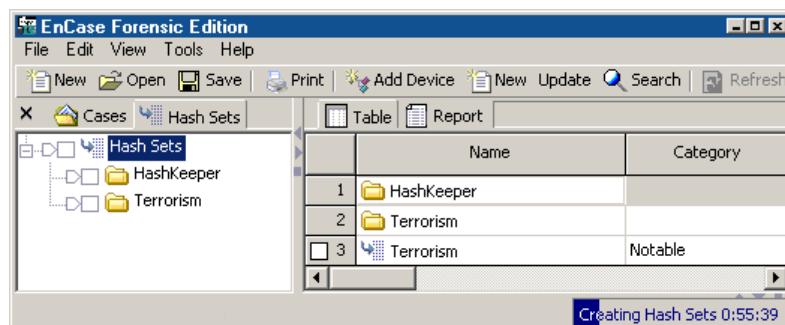


Figure 13-31 Creating NSRL Hash Sets

6. Once the hash sets have been imported, right click on the root of the Hash Sets tab and select **Update**.

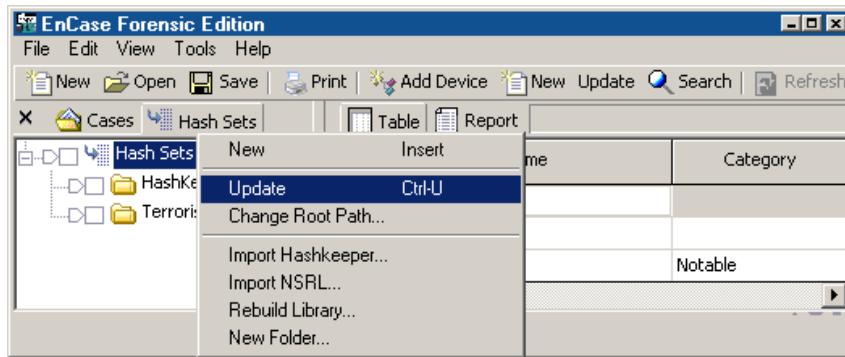


Figure 13-32 Updating Hash Sets

7. Click on the NSRL folder in the left pane to view the hash sets. To add a Category to the files, double-click on the hash file in the table, then enter the category (Known is recommended) and click [OK]. You can change the hash file name at this time if you wish.

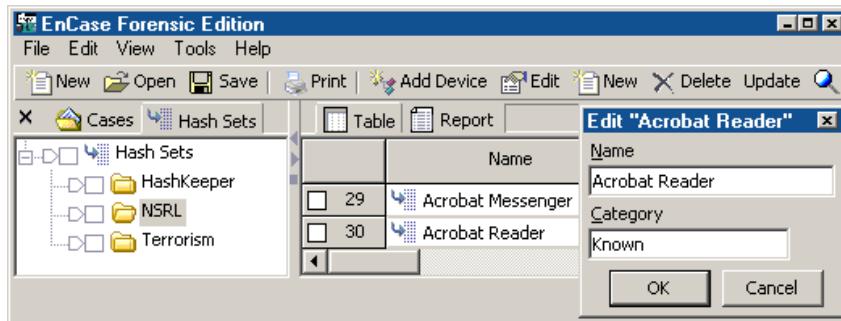


Figure 13-33 Adding Category

Rebuilding the Hash Library

The hash library contains the hash values that will be run against the data currently loaded into EnCase. The library is an accumulation of hash sets from which the investigator can choose, and can be rebuilt at any time. An investigator might rebuild a hash library after adding new hash sets or deleting unwanted hash sets. Rebuild the library as follows:

1. From the **View** menu, select **Hash Sets....**
2. Blue-check the hash sets to be included in the library.
3. Right-click on any hash set and select **Rebuild Library...**

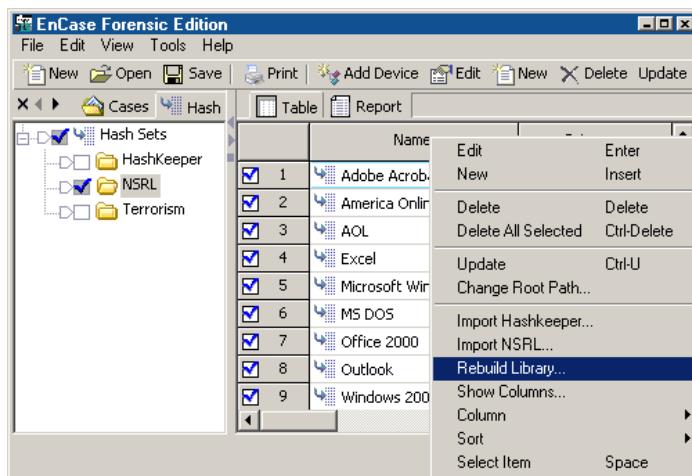


Figure 13-34 Rebuilding Hash Library

4. A prompt will return and confirm the number of has sets that have been added to the library. Click **[OK]** to close the window.

Benefits of a Hash Analysis

Running a hash analysis will calculate MD5 hash values for all of the files that the user has specified (typically the entire case) and compare these values with those stored in the hash library. Without generating this hash value, it is not possible to benefit from using hash sets in a hash library as no hash values are known. Therefore, one of the first steps of any investigation is to run a hash analysis of all the evidence files within the case.

Starting a Hash Analysis

1. Open the Case file with the evidence file to be examined or preview the machine to be analyzed.
2. Click on the **Search** button on the top toolbar and check only the **Compute hash value** option. If the file already has a hash value listed in the Hash Value column of the Table in *Cases* view, and you wish to have EnCase recompute it to ensure you are using the correct hash value, you can also check the **Recompute hash values** option. After selecting these items, click [**Start**].

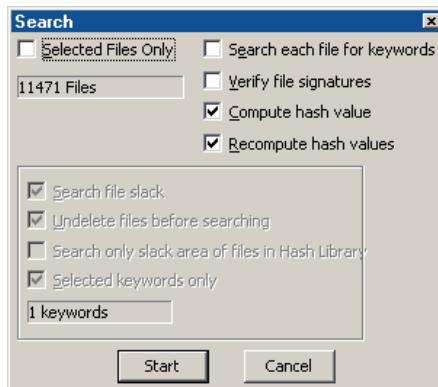


Figure 13-35 Computing hash values

3. A status window will report the number of hash values generated. Click [**OK**] to close the window.



Figure 13-36 Confirmation of file hashing

Analyzing the Hash Results

1. Click on the All Files trigger (“home plate”) next to the case name in the left pane of the **Cases** tab.
2. Locate the three hash columns in the Table (**Hash Value**, **Hash Set**, and **Hash Category**). You can put these together by clicking on the header and dragging the column where you want to put it.
3. Sort on **Hash Category** by double-clicking on the column header, and then scroll to the top to view the results. You can sub-sort by holding down the **[Shift]** key and double clicking on the **Hash Set** column header.

The files that are in the hash sets are easily identified by entries in the hash columns. Knowing what files are in Known hash sets, for example, will allow the investigator to bypass files with known hash values in order to speed up keyword searches.

	Name	Hash Value	Hash Set	Hash Category
1	desktop.ini	81051bcc2cf1bedf378224b0a93e2877	Excel	Known
2	explorer.scf	a3975a7d2c98b30a2ae010754ffb9392	Excel	Known
3	tips.gif	9c18ba429ca500786c1edf75a5a9ab22	Excel	Known
4	desktop.ini	6a82073d6e1caeaa8e63cf491baadfa2b	Excel	Known
5	desktop.ini	81051bcc2cf1bedf378224b0a93e2877	Excel	Known

Figure 13-37 Hash columns in Table view

EnScripts

There are a number of EnScripts that are installed with EnCase that provide useful functionality and save time and effort in the forensic examination of evidence files. The EnScripts are accessed by selecting **Scripts** from the **View** menu. The entire library of current EnScripts created by Guidance Software is available for download at Guidance Software’s web site, and is updated on a regular basis. Scripts created by parties other than Guidance Software are not available for download, but are frequently exchanged via the EnScript message board.

Initialize Case (v4)

The Initialize Case EnScript extracts useful information from Windows such as time zone settings, Windows version, shared folders, user info, and registration data, etc.

FAT Info Record Finder (v4) and NTFS Info2 Record Finder (v4)

These scripts search through unallocated space and slack space for FAT info file and NTFS Info2 records (database records of deleted files) and create a bookmark folder with the results.

File Finder (v4)

Recover files from unallocated space, creating a Bookmark folder with the results, with an option to export the files to a specified directory. File types that can be selected include AOL ART, BMP, EMF, GIF, JPG, Photoshop (PSD), PNG, TIFF, Word, Excel, Zip and GZip, with the ability to create a custom file type to search for based on header, footer and/or extension.

IE History Parser with Keyword Search (v4)

This script searches index.dat files (or other files, if specified) with the output directed to an HTML page and spreadsheet, Bookmarks, or both. The script extracts URL references by keyword and time stamps.



NOTE: The Server modified time stamp indicates the last time that the file was updated by the Web Server (NOT the user). The Last Access time indicates the last access by the user.

Link File Parser (v4)

The link file parser EnScript will extract information contained within Windows .LNK (shortcut) files. This information may include flags and attributes specific to the link file; the link type; creation, modification and last accessed dates; volume label; drive type; drive serial number; file length; icon file; link description; file link path; base path; application path; working directory; network share name, and command line.

Find Unique EMail Address List (v4)

This script searches through selected files for a "basic" e-mail signature. The "hit" is then confirmed using a built-in EnScript function. If the hit passes the

confirmation test, it is added to an e-mail list, so that if the same address is found again later in the evidence file, it will not be added again to the list.

Chapter 14

Navigating EnCase

This chapter describes how to create a new case, add evidence files and verify them using the EnCase Version 4 interface. The different tabs and views of EnCase are also detailed.



NOTE: The interface for EnCase Version 4 has changed significantly from Version 3. Please read this chapter thoroughly, especially the section which explains the different “views” of EnCase.

Creating a New Case

After installing EnCase, an EnCase icon is added to the desktop. Launch EnCase for Windows by double-clicking the desktop icon, or from the **Program** menu on the **[Start]** button.



Figure 14-1 EnCase version 4 desktop icon

Click the [New] button on the toolbar to create a case. You are prompted to input information for the case options:

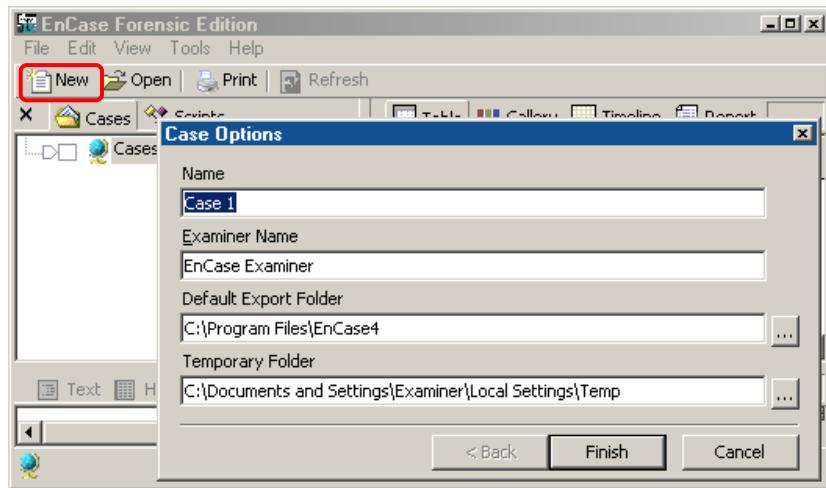


Figure 14-2 New case options

Name

Enter a short description for the case. The text entered here will be the text displayed by the case folder under the Cases tab.

Examiner's Name

Enter the lead investigator's name for this case.

Default Export Folder

Files, by default, will be exported to this folder when the **Copy/UnErase** option is selected, or when an EnScript exports files to the hard drive.

Temporary Folder

The temporary folder is where files are copied to when viewed with an external viewer. For example, if you set up QuickView Plus as a viewer in EnCase with which to view JPG and GIF files, and then double-clicked a .JPG file within an evidence file, the .JPG file would be extracted from the evidence file, copied to the temporary folder, and then opened with QuickView Plus. When a case file is closed, EnCase automatically deletes the temporary folder's contents.



Note If the paths you enter for these folders do not already exist, EnCase creates them.

Click the **OK** button and the new (and empty) case is created.

Case Management

Before starting a case, it is important to create case organization guidelines. First, consider how case files and evidence files will be organized on the hard drive. Most investigators dedicate a high-capacity “Storage” drive on the forensic machine to storage of evidence files, putting evidence files into appropriately named folders for each case they are working on. For example, if an investigator was working three cases, he might have a d:\smith folder, a d:\lemieux folder, and a d:\jones folder. With files for each case placed into a folder named after the Subject (such as d:\jones), then your Default Export folder and Temporary folder might set to d:\jones\export and d:\jones\temp (respectively) for that case.

Concurrent Case Management

EnCase Version 4 has the ability to open more than one case at a time. Each case will be in its own folder in the **Cases** tab, with each case having its own Report view, Bookmark folder, Devices folder, etc.

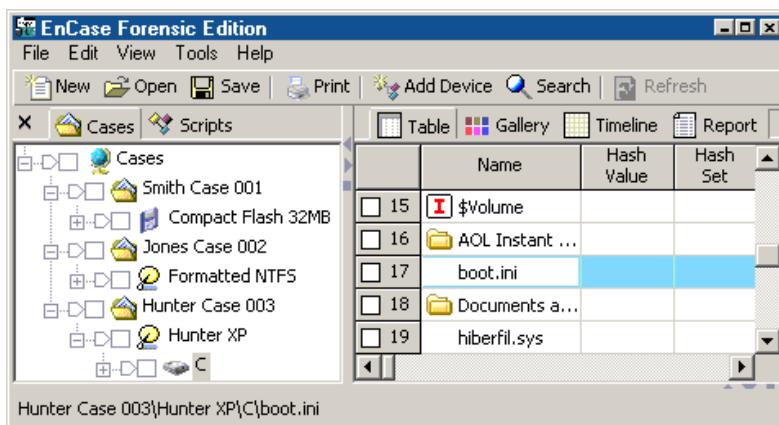


Figure 14-3 Multiple cases open simultaneously

Having multiple cases open simultaneously simplifies case comparison analysis functions, such as keyword searches, reviewing search hits, etc.

The Options Dialog

Version 4 has an options menu to configure administrative functions of the software. To access the menu, select **Options...** from the **Tools** menu. Five tabs are available: **Global**, **Colors**, **Fonts**, **EnScript** and **Storage Paths**. When a case is open, a sixth tab (**Case Options**) appears that allows you to set default values for subsequent case name, Examiner name, and Export and Temporary folder location as described at the beginning of this chapter.

Global

Global options, once set, are in effect when EnCase is open.

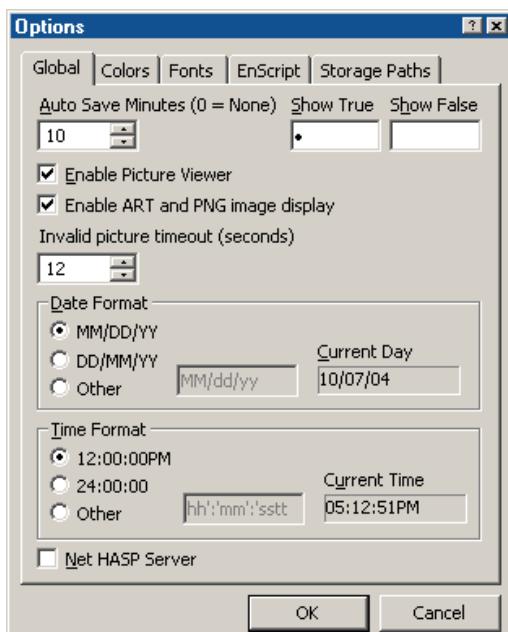


Figure 14-4 Global Options

Global options include:

- **Auto Save Minutes (0 = None)**
Auto Save records changes to the case and saves them to the .CBAK backup case file. This setting (10 minutes by default) determines the

amount of time between saving the case. Setting this value to 0 disables **Auto Save**.

- **Show True \ Show False**

Show True and **Show False** allow the user to define a character or string to identify in the tables whether the condition is true or false. These appear in Table columns in the various views such as Show Picture, In Report, Is Deleted, Permissions, Excluded, etc., and in wizards such as **Add Device** (Write Blocked, Read File System). By default, **Show True** is defined by a bullet (●), while **Show False** has no identifier defined. As an example, with **Show True** set to True and **Show False** set to False, note the last two columns in the Add Device wizard screen shot:

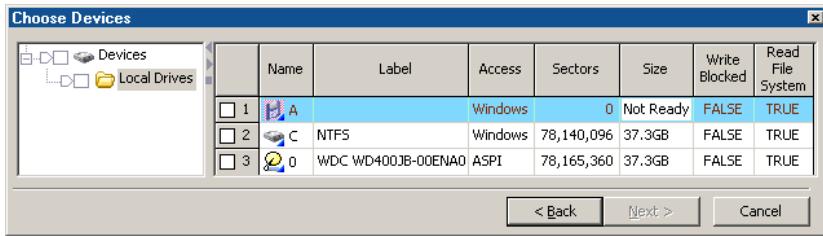


Figure 14-5 Add Device wizard showing True\False identifiers

- **Enable Picture Viewer**

This option, checked by default, allows EnCase to display pictures in Gallery view (right pane), Picture view (bottom pane) and in Report.

- **Enable ART and PNG image display**

A new feature of version 4.20 allows the user to disable ART and PNG images from displaying in Gallery view (right pane), Picture view (bottom pane) and Report view, since these files appear to cause the bulk of the issues with corrupted images. By default, ART and PNG images are displayed. However, some ART and PNG images recovered in the unallocated clusters or logical files otherwise corrupt, will crash the Internet Explorer .dlls that allow these types of images to be displayed within EnCase. Guidance Software cannot prevent these corrupt images from crashing the .dlls nor the cascade effect of crashing EnCase. To alleviate this issue, the user can uncheck this option, allowing them to continue their work on a case while ignoring these corrupt images.

- **Invalid picture timeout (seconds)**

EnCase includes threaded crash protection for corrupt image files. The **Invalid picture timeout** sets the amount of time in seconds for a thread to try reading a corrupt image file. Once the timeout value has been exceeded, EnCase will cache the file to allow EnCase to take preventative measures ensuring the file does not crash EnCase when accessed later. By default, the value is set to 12 seconds.

- **Date Format**

This setting allows the user to change the way dates are displayed in EnCase. For example, Europeans typically display the date as **day/month/year** by selecting the **DD/MM/YY** radio button. You can also set a custom date display, substituting dashes for slashes or having the year display as 4 digits by typing **YYYY** for the year when selecting the **Other** radio button.

- **Time Format**

Time format can be changed to display military (24-hour) format, or a custom display specified after selecting the **Other** radio button.

- **Net HASP Server**

Checking this box enables the examiner to receive a license from the Network Authentication Server (NAS). It is turned off by default to prevent needless broadcasting a UDP server request in a lab environment and having the examiner wait for the system to get into the acquisition mode. After checking this box, the setting is changed in the local.ini file, and takes effect after the next restart of EnCase.

Colors

The investigator may change display colors for different elements of the EnCase interface. Bookmarked text by default is light blue, but can be changed by double-clicking the Bookmark entry and selecting a new color. Colors may be changed for representation of search hits, text selection (both focused and not focused), code comments, normal (logical) text, slack text, normal (logical) and slack text in reports, filter frames, and filter text (filter frames and filter text colors can be changed under the **Queries** tab as well).

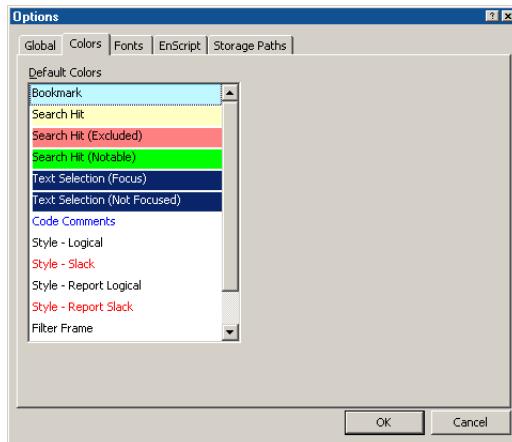


Figure 14-6 Colors Options

Fonts

A font, its' size, style, and script can be changed for different areas of the EnCase interface. While any part of the EnCase interface can be customized (such as changing the font for Script code when scripting), the **Fonts** tab is useful when working with foreign languages that require a specific font to display correctly. To change a font, double-click on the area listed in the **Default Fonts** window. For more information on working with foreign languages, see *Chapter 20*.

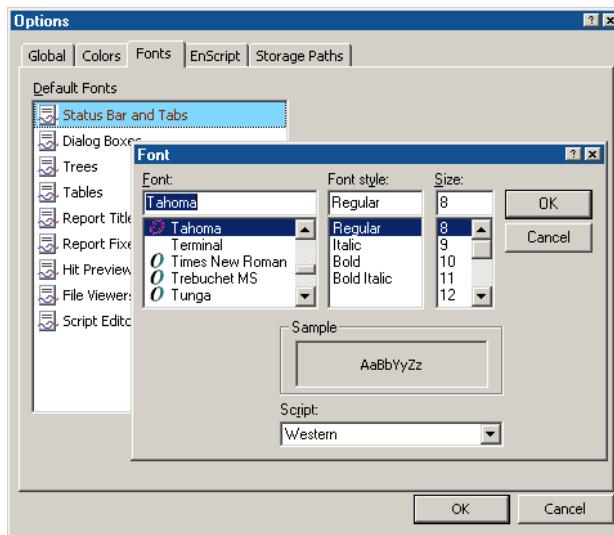


Figure 14-7 Font Options

EnScript

EnScripts are essentially small programs that allow EnCase to access data and extract and store that data for examination. Since EnScripts are programs, they can potentially be maliciously coded to negatively impact a storage hard drive. If EnScripts are shared between different investigators, different departments, or different organizations, it is possible that an unfamiliar EnScript could cause problems on a Storage system. The investigator may set what level of accessibility EnScripts have to the examination machine and network using EnScript security. Options that are set in the **EnScript** tab include allowing scripts to read the contents of local files, to write to or delete local files and folders, to create folders and to execute local programs. By default, all are checked (enabled), except for the ability to **Execute Programs**. The **Include Path** is the name of EnScript libraries folder (typically C:\Program Files\EnCase4\Scripts\Include); this should generally be left with the default path of Include.

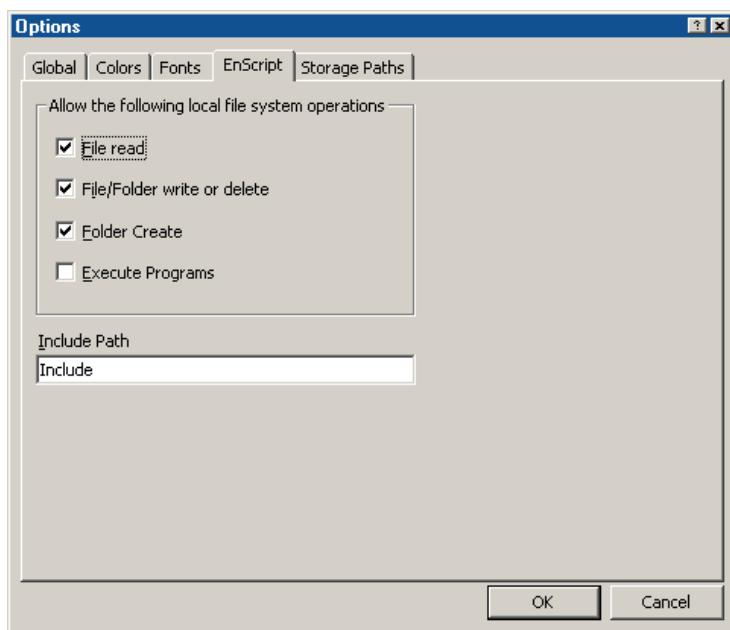


Figure 14-8 EnScript security Options

Storage Paths

Since version 4.17, EnCase allows the user to set the paths to where the configuration files for global settings (.INI files) are stored using the **Storage Paths** tab. This feature allows an organization to have one set of EnCase .INI files on a networked drive that all examiners use. The administrator of the configuration files can change the .INI file attributes to be read-only for all examiners except the one who maintains the configuration file. The read\write attributes are displayed in the **Writable** column of the table. To change the path or read\write status, double click on the file, or highlight it and select **Edit** from the right click menu (or press [**Enter**]). The read\write status can also be changed by right clicking on the file in the **Writable** column and selecting **Writable**. Users can change the paths for the **FileTypes.ini**, **FileSignatures.ini**, **FileViewers.ini**, **Keywords.ini**, **SecurityIDs.ini**, **TextStyles.ini**, **AppDescriptors.ini**, **Profiles.ini**, and (as of version 4.20) **Filters.ini**.

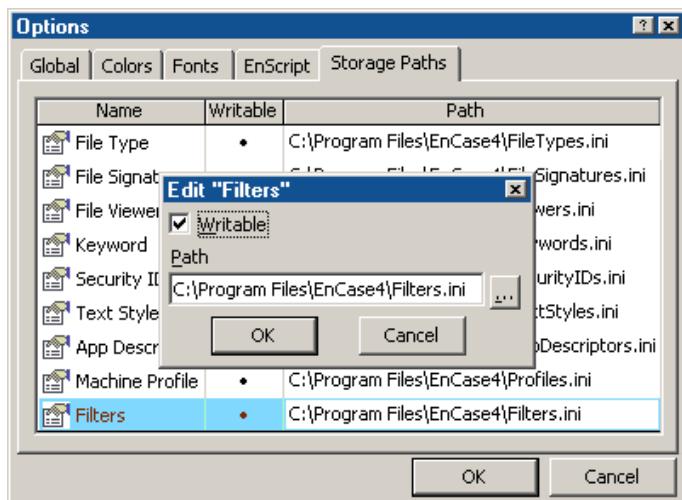


Figure 14-9 Storage Path Options

Adding Evidence Files to a Case

Before adding pre-existing evidence files to a case, the investigator must know where those evidence files reside either locally or on the lab network. You can add a device as follows:

1. Select **Add Device...** from the **File** menu, or click on the **[Add Device]** button on the top toolbar.

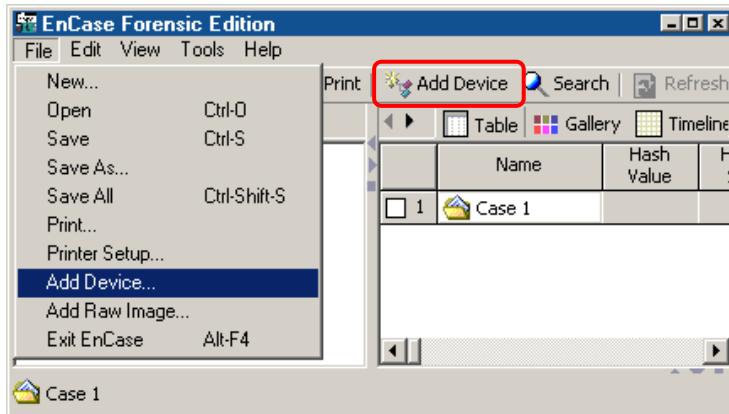


Figure 14-10 Adding a device

2. Direct EnCase to the location of the saved evidence files by right clicking on the **Evidence Files** folder in the left pane and selecting **New**.

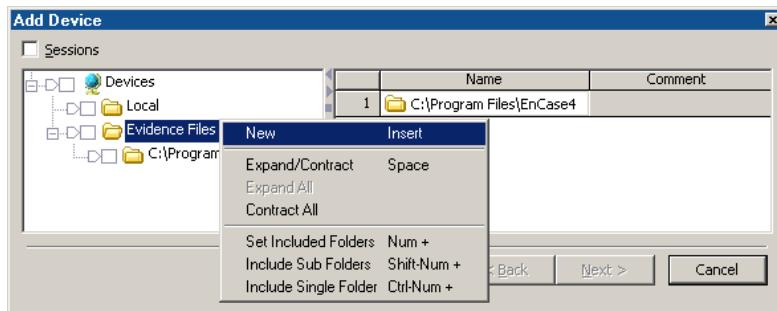


Figure 14-11 Defining new evidence file location

3. Browse to the location of the evidence files and then click [OK].

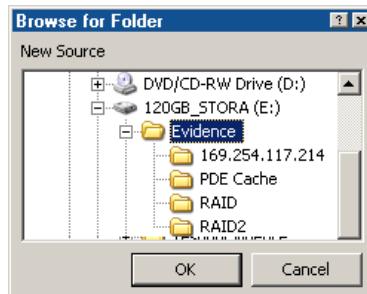


Figure 14-12 Selecting evidence file folder

4. The new folder appears in the left pane below **Evidence Files**. Select the “All Files” trigger (“home plate”); all available evidence files in that folder and subfolders should appear in the right pane. Additional folders in other locations can be added in the same manner.

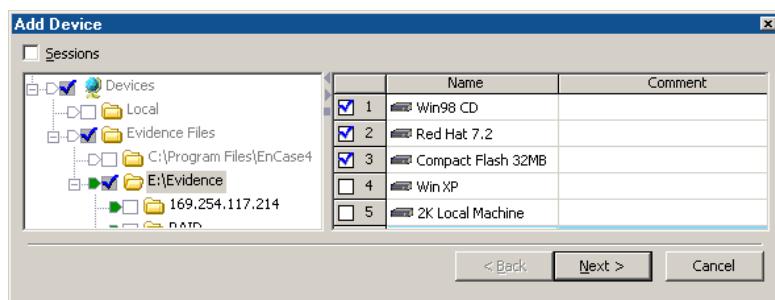


Figure 14-13 Adding evidence files

5. Blue-check the desired evidence files (devices, volumes, floppy disks, removable media, or Palms) from the right pane and click the [**Next >**] button. A confirmation screen will show the evidence files you are adding.

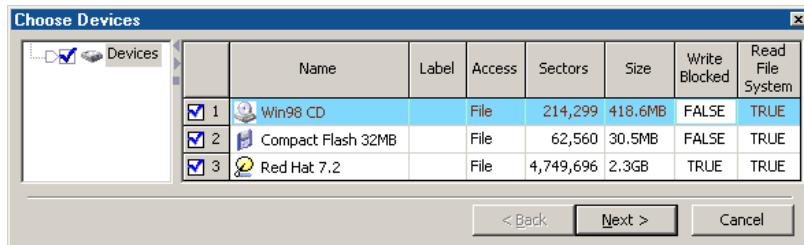


Figure 14-14 Confirming devices

6. Double clicking on the selected item will allow you to select whether or not to have EnCase read the file system. If the **Read File System** check box is left blank, EnCase will not read or display filenames or a folder structure. After checking attributes, click [**OK**], then [**Next >**].

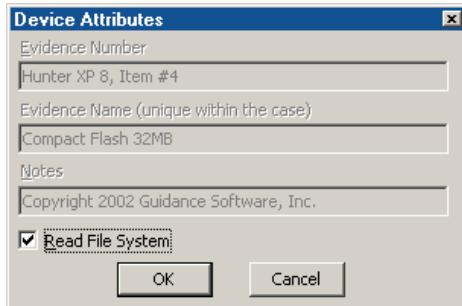


Figure 14-15 Device attributes

7. You are prompted for a final confirmation before adding the selected items to the case. If all items are correct, click [**Finish**].

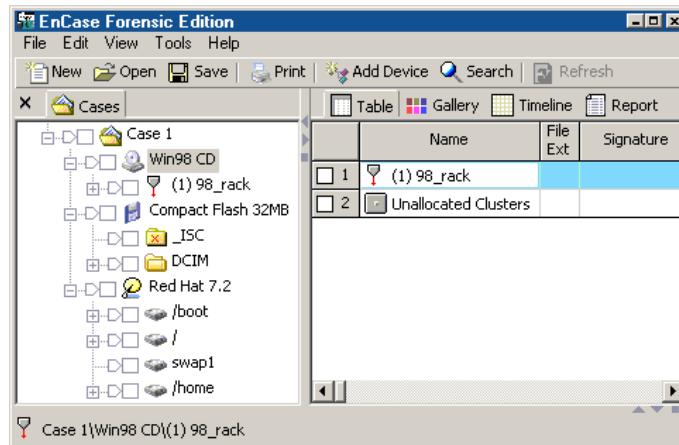


Figure 14-16 Case with three devices

Sessions Option

The **Sessions** option, introduced in version 4.16, allows EnCase to “remember” previously previewed or audited devices. The session information is stored so that an examiner can start a new case and return to a device that is being actively audited, allowing for more efficient case management. To use the **Sessions** option:

- In a new or existing case, select **Add Device...** from the **File** menu, or click on the [**Add Device**] button on the top toolbar as shown in *Figure 14-10*.
- Select the **Sessions** checkbox in the upper left of the **Add Device** screen.

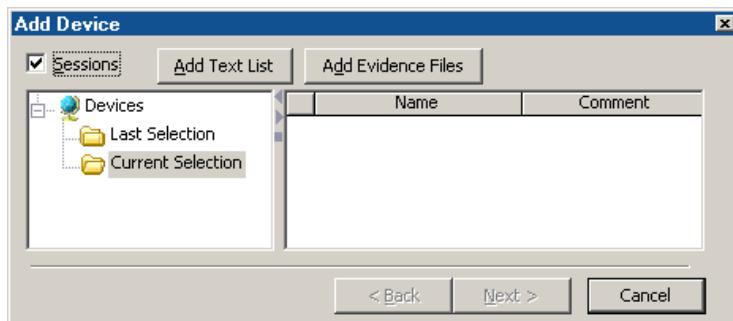


Figure 14-17 Sessions screen

- If the [**Add Text List**] button is selected, the examiner is prompted for a path to the evidence files. You can type a full local path (including a mapped drive letter), a network path (with domain access), or a combination (as indicated by *Figure 14-11*). You may need to resolve network paths (`\server\folder\filename\ evidence.E01`) by using the browser to find the evidence file. Complete the list with the [**OK**] button.

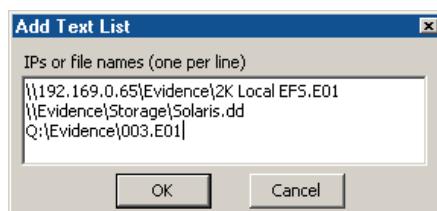


Figure 14-18 Text list for Sessions

- If the [**Add Evidence Files**] button is selected, the examiner can browse folders to find the evidence files, much in the same manner as previous versions of EnCase. The drop-down box for **Files of type:** allows the user to search for an EnCase evidence file (.E01), a SafeBack file (.001), or a VMware file (.vmdk).

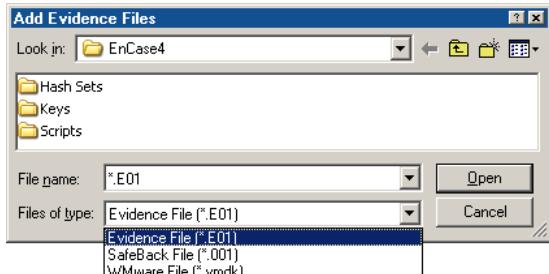


Figure 14-19 Adding evidence files

Two folders appear in the left pane of the **Session** window. **Last Selection** contains the last evidence files that were added to and saved in a case.

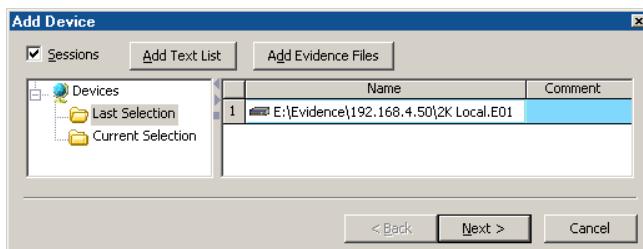


Figure 14-20 Last Selection folder

Current Selection contains evidence files or devices currently selected (blue checked) in the **Add Device** wizard outside of sessions. Adding evidence via the [**Add Text List**] or [**Add Evidence Files**] buttons, or right clicking in the right pane, selecting **New** and adding a source path for evidence will also populate the **Current Selection** folder.

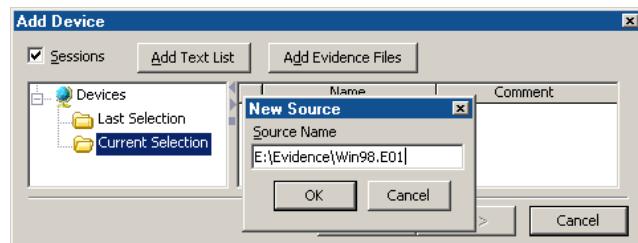


Figure 14-21 Current Selection folder

You can also create new folders and subfolders to store links to evidence files the forensic machine has access to. Right click in the location where you wish to place the folder and select **New Folder**.

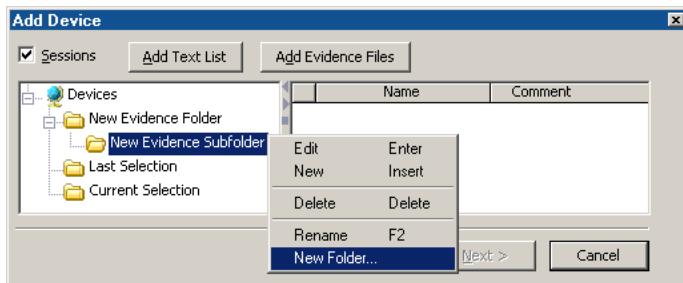


Figure 14-22 Creating a new Session folder

Error Messages

Below are typical error messages encountered when adding evidence.

"'X:\PATH\EVIDENCE.Exx' could not be found. Choose a new path for this file?"

EnCase cannot add an evidence file unless all the segments (or “chunks”) are mounted at the same time. If possible, place all chunks of an evidence file in a single location on your hard drive. If storage space prevents this, select [**Yes**] to choose a new path and then browse to the location of the missing chunks. If the chunks in question are missing, you will be asked if you wish to zero out the sectors represented by the missing file.

"Error verifying checksum in the file [EVIDENCE.Exx]"

The media on which the file is stored may have become corrupted. This error occurs when the evidence file header is corrupted to the point at which EnCase will no longer recognize it, rejecting it when adding it to a case. Try to re-acquire the original media to *different* media than before, or add a copy of the evidence (it is advisable to make multiple acquisitions for backup purposes).

"Unable to read 64 sectors starting at absolute sector nnnnnnnnnn"

This error message usually indicates that a file-pointer in the directory structure of the evidence file is pointing to an area of the disk that EnCase did not acquire. This is the fault of the BIOS improperly reporting the size of the physical disk.

To determine if the BIOS has misreported the size of the disk, check the Drive Geometry section of the EnCase report for **Total Size in sectors**. The Partition Table section of the Report displays the sector size of each partition. The total number of sectors, added up from each partition, should equal the **Total Size in sectors**. If it does not, the BIOS may have misread the geometry of the hard drive. You can try manually inputting the Cylinders-Heads-Sectors (CHS) information into the computer with the subject's hard drive, and then reacquiring the whole drive. Do not let the BIOS auto detect the CHS information.

Another possible issue is that the storage computer BIOS does not support more than 8 gigabytes of hard-drive space, or that the subject machine BIOS supports the drive size but the storage computer BIOS does not.

Finally, if the CHS information is correct, but continue to encounter the error messages, data in the file may be corrupted, causing EnCase to interpret it as file-pointers to areas that do not exist. Click **OK** to bypass the error messages and continue inspecting the evidence file.

"Decompression error in file ' X:\PATH\EVIDENCE.Exx ', file may be corrupted."

Reacquire the subject drive.

EnCase locks up after adding the evidence file, and Task Manager reports that EnCase is 'not responding.'

Adding evidence to a case rarely locks up EnCase. This condition may occur if evidence files are particularly large, if the file is in EXT2 format, if there are a large number of deleted files to be recovered, or if the file is graphics intensive. EnCase is not frozen; it is performing multiple complex operations. This condition usually disappears after the task is complete. Adding memory to the forensic machine sometimes alleviates this issue.

Verifying the Evidence

After adding an evidence file to a case, EnCase automatically starts verification of file integrity. EnCase reads the data in the evidence file and generates an MD5 (Message Digest 5 algorithm) hash value for the data, displaying the verification and acquisition MD5 hash values in the report. A flashing-blue bar will appear in the lower-right corner of the EnCase window indicating that verification is taking place. To cancel verification, double-click the flashing verification bar.

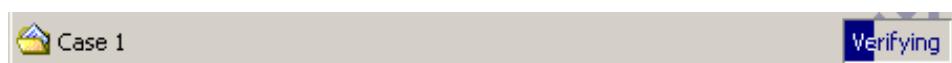


Figure 14-24 Evidence file verification

EnCase will save the evidence file verification only if you *save* the case *after* the verification process is finished. If the case is closed without saving, the verification process will begin each subsequent time the evidence file is loaded.

Adding Raw Image Files

EnCase can add raw image files (images of media in a flat-file format, such as Linux “dd”) to a case:

1. Add the raw image file by selecting **Add Raw Image...** from the **File** pull-down menu (a raw image cannot be added using the **Add Device** button.)

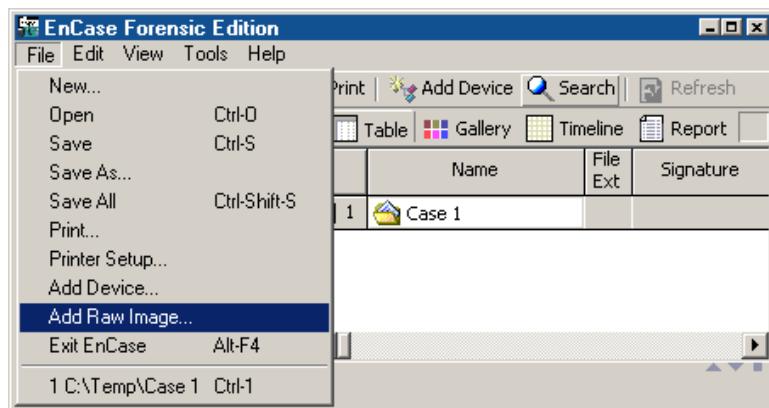


Figure 14-24 Add Raw Image

2. At the top of the **Add Raw Image** screen is a **Name** field. Text entered here will be the name of the evidence file once it has been added to the case.

3. Right click in the **Component Files** field and select **New**. If files were imported previously, they will show in this field.

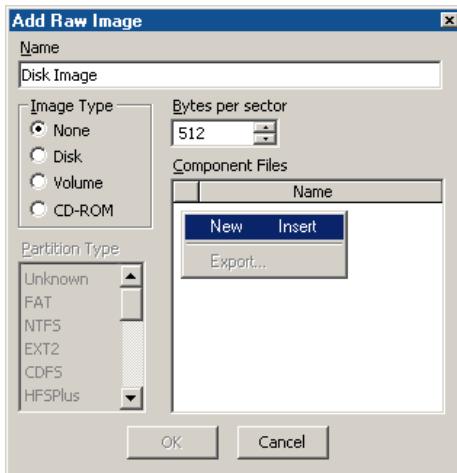


Figure 14-25 Add New Raw Image

4. Add the raw image chunks in the order created. In the browser, select the last item, hold down the [**Shift**] key and select the first item (reverse order). You should see the correct sequence in the **File name:** field at the bottom of the browser. Click on [**Open**] to add the files.

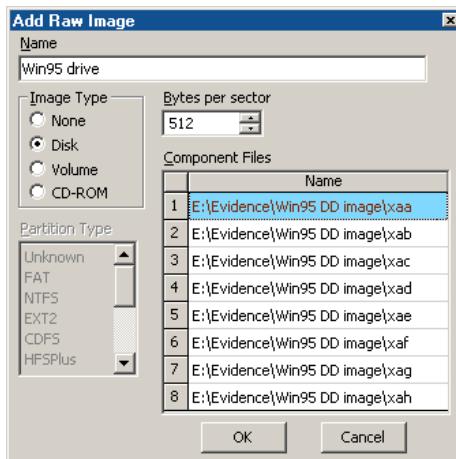


Figure 14-26 Selected raw image segments in order

5. The image chunks should show in the **Components Files** field in correct order. If they are out of order, click on the item in the wrong location and

drag it to the proper location. You must specify the **Image Type** by selecting the appropriate radio button:

- **None** – Selected by default; adds the entire image as Unallocated Clusters
 - **Disk** - Physical disk image
 - **Volume** - Locally mounted drive letters; includes floppies, removable media (except CD-ROM), logical volumes, etc. If known, the partition type should be specified by selecting the appropriate item in the **Partition Type** field.
 - **CD-ROM** - CD-ROMs only
6. With the segments displaying in the correct order, and the appropriate **Image Type** and **Partition Type** selected, check the case name (in the **Name** field) and click **[OK]**. You should now see a complete volume or device with file structure visible.

SafeBack and VMware Images

In EnCase 4.18 and above, SafeBack (.001) v2.x image files can be added to EnCase the same way as EnCase evidence files. VMware .vmddk images (versions 3 and 4) can also be added in this manner as of version 4.19. The method for adding these files follows:

1. Launch EnCase and open a new case.
2. Click on the **[Add Device]** button on the top toolbar, or select the option from the **File** drop-down menu.

3. If the folder where the evidence is located exists under **Evidence Files**, click on the *Show All Files* trigger (green home plate). If the folder does not appear, right click on the **Evidence Files** folder, select **New**, browse to the directory where the files currently reside, highlight the folder and then click [**OK**]. Blue check the appropriate EnCase evidence file (.E01), SafeBack image file (.001) or VMware image (.vmdk) and select [**Next >**].

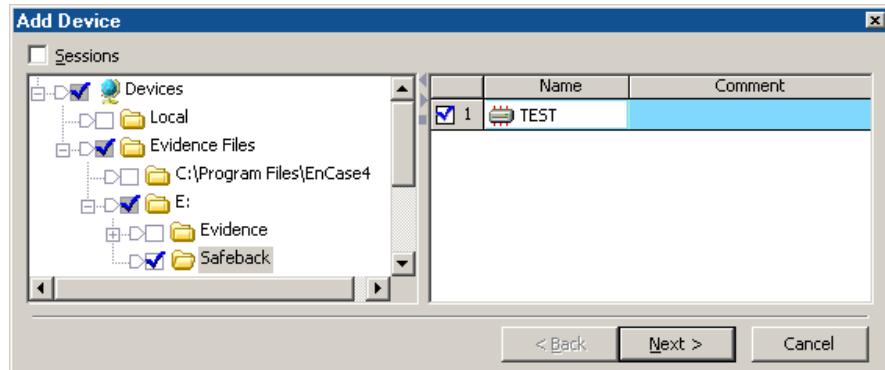


Figure 14-27 Adding a SafeBack image

4. EnCase will parse the image file structure to determine the type of device contained within the image file. For large images, this may take longer; however, when the [**Add Device**] wizard is complete, the image file will be loaded immediately into the Case file since the file structure was already parsed. This is different from EnCase evidence files, which are parsed after they are brought into the Case file.

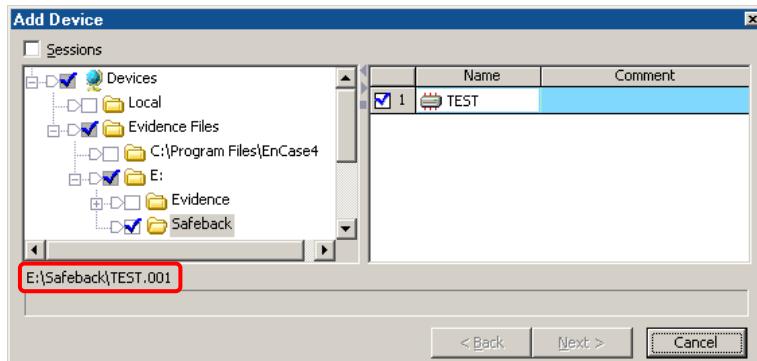


Figure 14-28 EnCase parsing a SafeBack image

5. After EnCase parses the file structure, the information about the type and size of the device will be available in the **Choose Devices** window. Double-click on the device name to change the name in EnCase, or click [**Next >**] to continue. The **Preview Devices** window lists all devices selected for adding to the Case file.



Figure 14-29 Preview Devices

Click on [**Finish**]; the image file will be loaded into EnCase, and the CRCs will be verified. You will then be able to conduct an examination of the image file as you would an EnCase evidence file or dd image. The results of the CRC verification will be reflected in the report of the device.

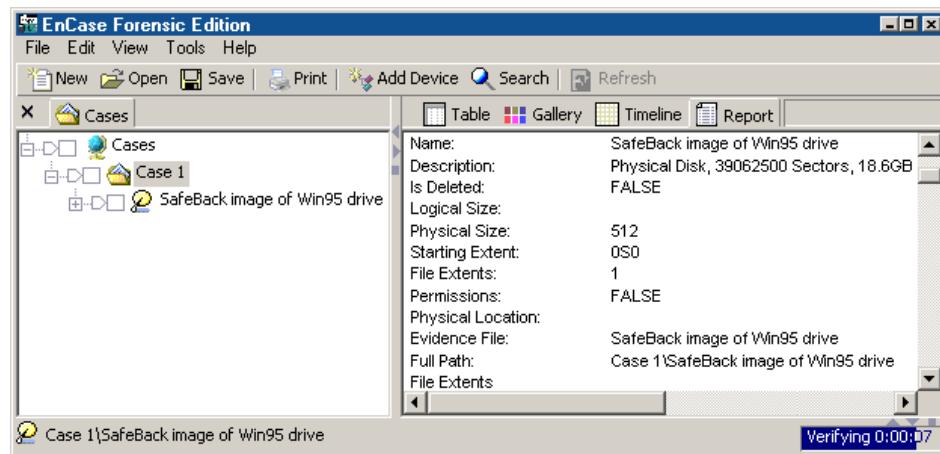


Figure 14-30 SafeBack image verifying in EnCase

You can also drag and drop a SafeBack .001 file into EnCase to parse, load, and verify the image file, or use the **Sessions** function in the **Add Device** wizard.

Interface

The Version 4 interface is much cleaner and more powerful than version 3. EnCase tabs (**Cases**, **Bookmarks**, **Devices**, etc.) appear alongside each other, as do the tabs in the right pane (**Table**, **Gallery**, **Timeline**, **Report**, etc.). Beneath the **Cases** tab, each case is contained within its own case folder. It is easy to have multiple cases open at one time.

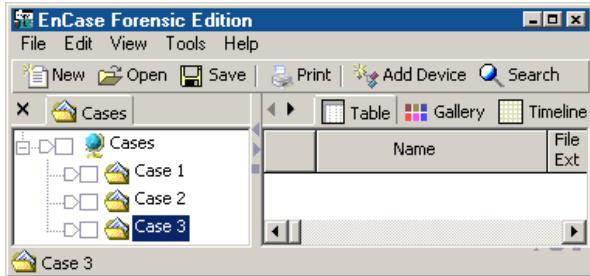


Figure 14-31 Cases tab with multiple cases

To get a complete list of the tabs that are available, click on the [View] pull-down menu.

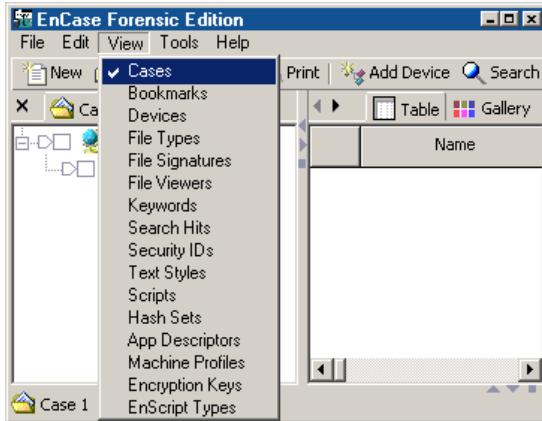


Figure 14-32 Available tabs from the View menu

To close any of these tabs, click on the tab to select it and then click the ‘X’ to the left (on the tabs line), or right click on the tab and select **Close**.



Figure 14-33 Closing a tab

EnCase Views

The “All Files” Button

The “All Files” button (often called the “home plate”) is the polygon next to the check box that turns green when clicked. It displays, in the selected view on the right, *all* of the files within the parent and *all* subfolders of the selected media or folder from the left. The “All Files” button can be activated in tabs (**Cases**, **Bookmarks**, **Devices**, etc.) and views (**Table**, **Gallery**, **Timeline** and **Report**).

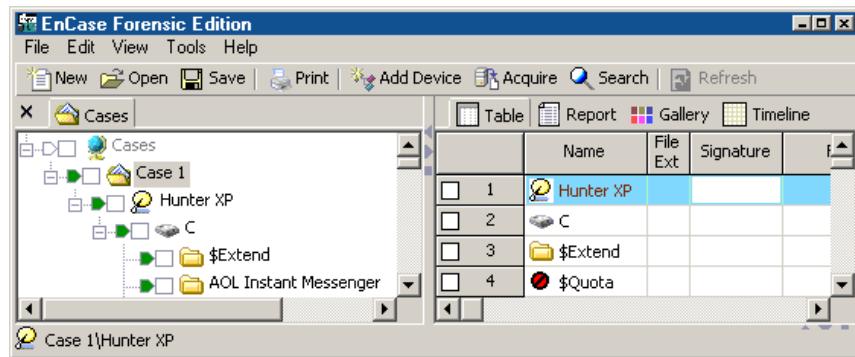


Figure 14-34 Cases tab

A user can select the “All Files” button at the parent folder level, then [Shift] click on a subfolder to deselect only that folder.

Cases

Cases is the default view in EnCase. If it is not visible, select **Cases** from the **View** pull-down menu. The **Cases** tab is where evidence files can be reviewed in an interface similar to Windows Explorer. From this view it is possible to navigate through different cases, evidence files, logical volumes, and directories in the left pane. In the right pane, all folders and files that are in the selected

object on the left-hand side are displayed. As mentioned previously, if you click on the “All Files” trigger for a folder, you will see *all* files in that folder and subfolders. Files highlighted in the right pane are represented in the bottom pane in the mode of the selected tab (***Text, Hex, Picture, Disk***, etc.).

In **Cases**, you can access, in the right pane, **Table**, **Gallery**, **Timeline**, or **Report** views (each described below). In **Cases**, you can Copy/Unerase highlighted files to your hard drive, bookmark highlighted files, or examine file with a specified viewer.

Bookmarks

To access the **Bookmarks** tab, select **Bookmarks** from the **View** pull-down menu. The Bookmarks tab contains items that have been marked as files of interest. Bookmarks can be files, images, text fragments, and more (see **Chapter 22 - Bookmarks** for further details.) Bookmarked items are placed within folders specified by the investigator.

Bookmarks can display bookmarks in **Table**, **Gallery** (for bookmarked images), or **Timeline** views, or show the report in the right pane. As with **Cases** view, you can display all bookmarks by using the “All Files” trigger. See **Chapter 22 Bookmarks** for further details.

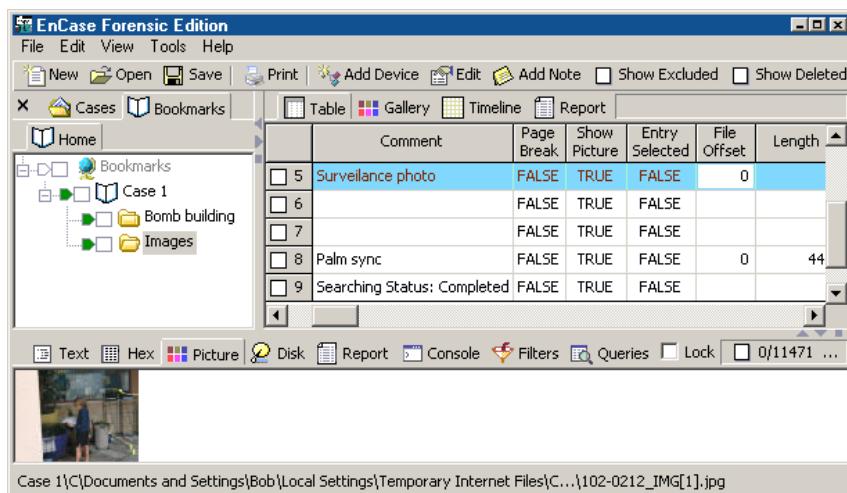


Figure 14-35 Bookmarks tab

Devices

The **Devices** tab is accessed by selecting **Devices** from the **View** pull-down menu. This tab contains information about the media such as acquisitions notes, the examiner's name, the acquisition, verification hash values, and more. Disk configurations can also be edited from this tab (see *Chapter 10* for details.)

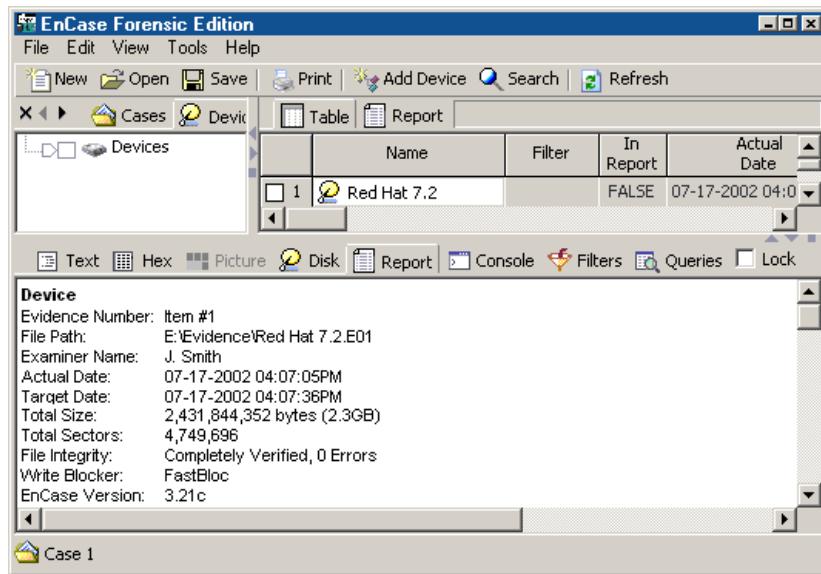


Figure 14-36 Devices tab

File Types

To access the **File Types** tab, select **File Types** from the **View** pull-down menu. This tab contains information on all file types and their associated viewers. EnCase allows the user to review, add, edit, or delete file types and to match file types to viewers. While EnCase has many file types already matched to specific applications for proper file access, it also provides a means to add viewers for file types that are new or unrecognized by EnCase. **File Types** are covered in full in *Chapter 15 - Viewing Files*.

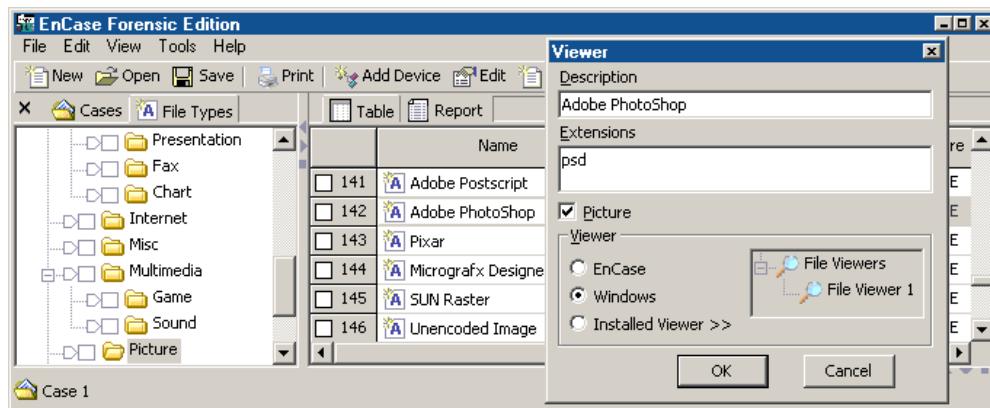


Figure 14-37 File Types tab

File Signatures

The **File Signatures** tab is accessed by selecting **File Signatures** from the **View** pull-down menu. File Signatures are the unique hex signature headers associated with specific file types. For example, an industry-standard JPG image must begin with the hex header signature `\xFF\xD8\xFF[\xFF\xE0]\x00`. From this tab, file signatures can be reviewed, added, edited, and deleted.

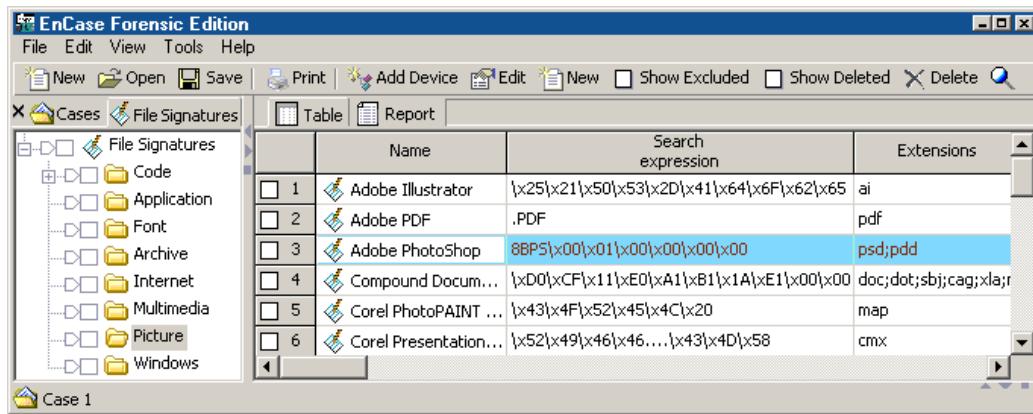


Figure 14-38 File Signatures tab

File Viewers

To access the **File Viewers** tab, select **File Viewers** from the **View** pull-down menu. File Viewers are applications that can be configured in EnCase in **File Types** to associate file types and viewers. By default, EnCase can view different file types, such as JPG or TXT, but some file types cannot be displayed natively by EnCase. From this tab, file viewers are added, edited, and deleted. File Viewers are covered in full in *Chapter 15 - Viewing Files*.

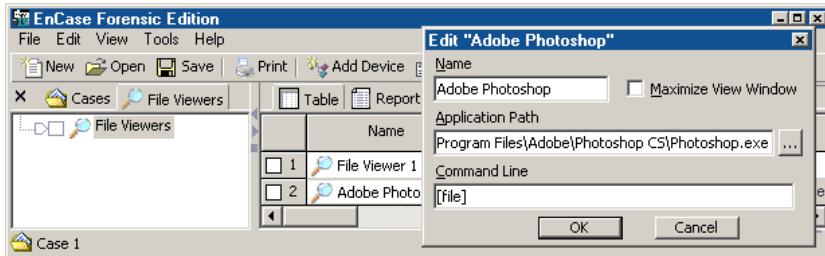


Figure 14-39 File Viewers tab

Keywords

The **Keywords** tab is accessed by selecting **Keywords** from the **View** pull-down menu. Keywords are terms used to search evidence files. They can be words, phrases, or hex strings. Keywords can be entered as case-sensitive, in GREP, in Unicode, UTF7 and UTF8, etc.

Keywords are saved in an initialization file (**keywords.ini**) in the root of the EnCase directory (typically **C:\Program Files\EnCase4**). Keyword searches are performed at both a logical and physical level, meaning that EnCase can search for each term byte-by-byte from the beginning to the end of every medium, and also search every logical file for the term as well. Keywords are covered in detail in *Chapter 16 - Keyword Searches*.

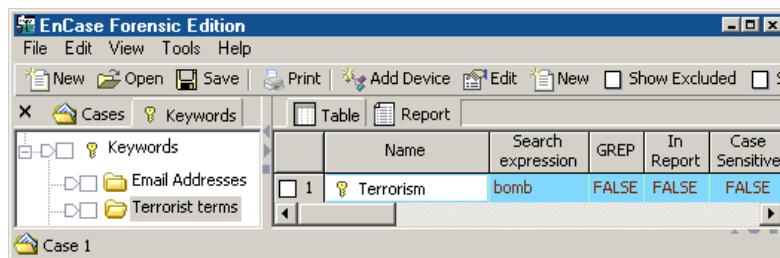


Figure 14-40 Keywords tab

Search Hits

To access the **File Viewers** tab, select **File Viewers** from the **View** pull-down menu. Search hits generated from keyword searches are placed in this tab in a folder created using the same name. Search Hits are covered in detail in *Chapter 16 - Keyword Searches*.

Name	Preview	Hit Text	Entry Selected	File Offset	Length
237 Bomb.psd	ÿÿ ÿÿ ÿÿ explosion 8BIMluni	explosion	FALSE	156735	9
238 Bomb.psd	ÿÿ ÿÿ ÿÿ explosion2 8BIMluni	explosion	FALSE	156905	9
239 Bomb.psd	ÿÿ ÿÿ ÿÿ explosion2 8BIMluni	explosion	FALSE	157075	9

Figure 14-41 Search Hits tab

Security IDs

Every file and folder on an NTFS file system has an owner, a group, and a set of permissions. While this information is stored differently in NTFS 4 and NTFS 5, EnCase extracts the security information for each file and folder. EnCase extracts the owner, group and permission settings (organized by owner or group) on Windows, Unix and Linux systems. The **Security IDs** tab allows the user to input Security IDs for a particular piece of evidence to be used in examination. This tab is accessed by selecting **Security IDs** from the **View** pull-down menu.

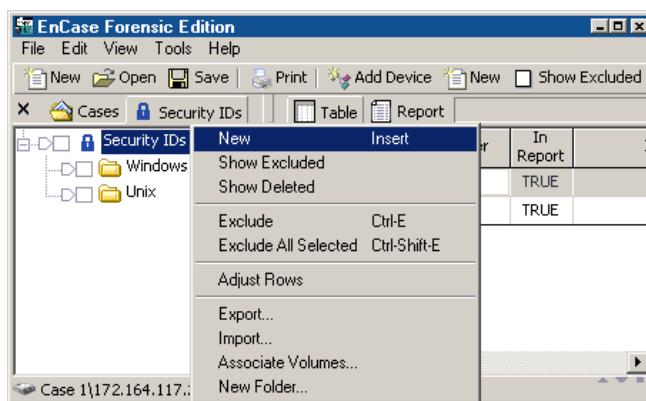


Figure 14-42 Security IDs tab

Below is a typical listing of NTFS file permissions, from the Administrator user folder C:\Documents and Settings\Administrator:

Permissions

NAME : BOB HUNTER
ID : S-1-5-21-1229272821-1580818891-854245398-1004
PROPERTY : ALLOW
PERMISSIONS: [FC] [M] [R&X] [R] [W] [SYNC]

ID : S-1-5-18
PROPERTY : ALLOW
PERMISSIONS: [FC] [M] [R&X] [R] [W] [SYNC]

NAME : ADMINISTRATORS
ID : S-1-5-32-544
PROPERTY : ALLOW
PERMISSIONS: [FC] [M] [R&X] [R] [W] [SYNC]

NAME :	BOB HUNTER
ID :	S-1-5-21-1229272821-1580818891-854245398-1004
PROPERTY :	OWNER

Below is a typical listing of Unix file permissions, from the `.bash_profile` file under `admin`:

Permissions	
Owner:	500
Group:	500
Permissions Allowed:	Owner Read
Permissions Allowed:	Owner Write
Permissions Allowed:	Group Read
Permissions Allowed:	Other Read

Notice that users and groups are displayed by a numbering system. The number is the Security Identifier, or SID. Every user, group, and machine has a unique SID in an NT network. For example, if Trevor Martin is a user on a Windows 2000 system, Trevor will have a Security ID number that matches to his name. Windows 2000 stores this information in the registry, and EnCase automatically displays his name in the Report tab in association with his SID.

However, if a new user, John Hopkins, logs onto the system who is *not* stored locally on the Windows 2000 system (but is on the network file-server, thus allowing him to log onto this client system), there will be no Security ID number correlated with John Hopkins. EnCase would be unable to associate John with a security ID number—John's Security ID number is on the network file-server, not the local machine. Unix User and Group IDs are not unique, and are not automatically associated with names either.

The solution is to preview or image the network file-server in addition to the client machine and retrieve all user Security IDs via the server. Those Security IDs can then be entered into EnCase under the Security IDs tab, and John's username would then be associated with his Security ID number. Windows 2000 SID information can be extracted and exported using EnScripts such as the v4_Active Directory Information Extractor and the Initialize Case (v4).

Three folders are created by default in the Security IDs tab: **Windows**, **Nix** (for **Unix** and **Linux** IDs) and **Security IDs**. The folders are there to encourage organization, but each folder can contain any type of ID.

To create a new Security ID (SID), right click on the desired folder and select **New...** A dialog box will pop up with fields for Name, Id, Group, Unix, and Group Members.

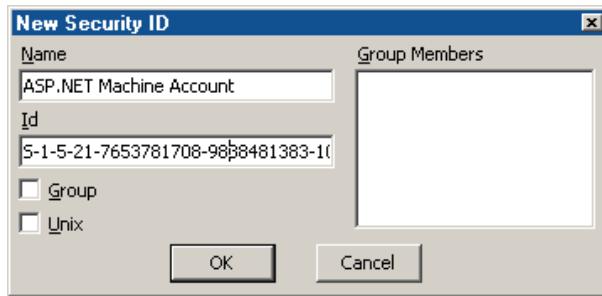


Figure 14-43 Creating a new Security ID

An explanation of the fields follows:

Name

The **Name** field contains the name that will be resolved when the associated SID is found.

Id

This field allows the entry of the Security ID (SID) that the user wishes to resolve. The Windows SID is in the form “S-x-x-x[-x-x-x-x]”. A Nix (Linux\Unix) SID is an integer such as 1000.

Group

The **Group** checkbox must be selected if the SID pertains to Nix and represents a group. Nix IDs are not unique, and User IDs may overlap with Group IDs.

Unix

This radio button must be selected if the SID being defined is for a Nix system.

Group Members

The **Group Members** field is optional; it may be defined to aid in organization (mainly for Nix). Right-click and select **New...** in the **Group Members** box to assign a member to the current Security ID.

It is recommended to create a new folder to contain the settings for each volume in a case, as SID settings are assigned to volumes at the folder level. Right-click on a folder in the Security IDs view and select **Associate Volumes...** to

associate the Security IDs in the selected folder with currently open volumes. Select the volumes to which you wish to apply the settings, and click [OK]. The volumes that a particular folder is applied to are displayed in the **Associated Volumes** column of the *Security ID* table.

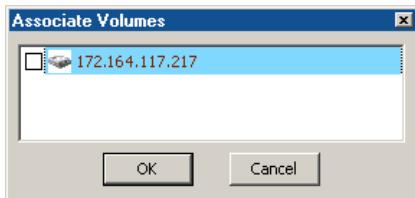


Figure 14-44 Associating Volumes

Text Styles

To access the **Text Styles** tab, select **Text Styles** from the **View** pull-down menu. Text Styles are used to view Code Pages correctly and with different settings, such as changes in color and text line length. EnCase has multiple default text styles, but styles can be added, edited, and deleted from this tab by either right-clicking and selecting the command from the menu or clicking the second **New** button in the tool-bar.

Text Styles are covered in full in *Chapter 20: Foreign Language Support*.

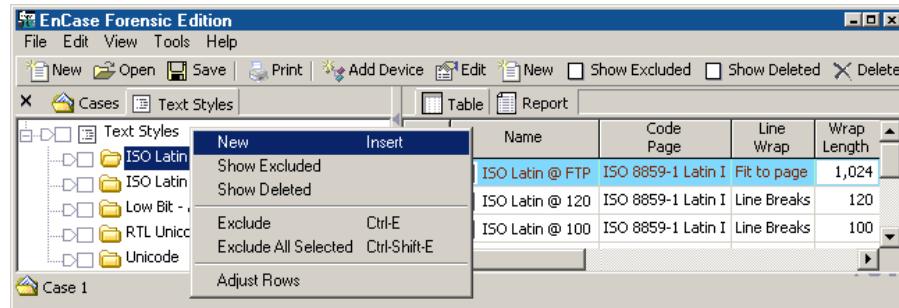


Figure 14-45 Viewing Text Styles

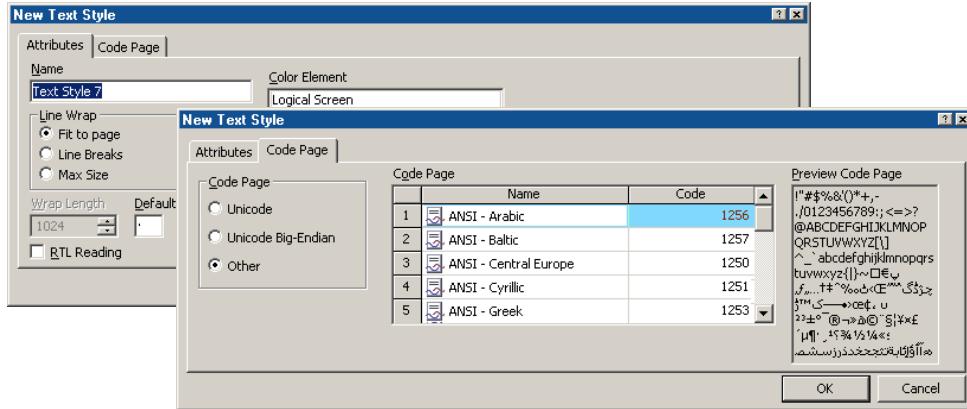


Figure 14-46 Adding new text style

Scripts

The **Scripts** tab is accessed by selecting **Scripts** from the **View** pull-down menu. The **Scripts** tab is where EnScripts are reviewed and coded. EnScripts are small programs or macros that are designed to automate forensic procedures. EnScripts can access and manipulate many areas of the EnCase interface, from searching to creating bookmarks to putting information into the report. EnScripts can be added, edited, and deleted from the Scripts tab. EnScripts are covered in detail in *Chapter 18: EnScript and Filters*.

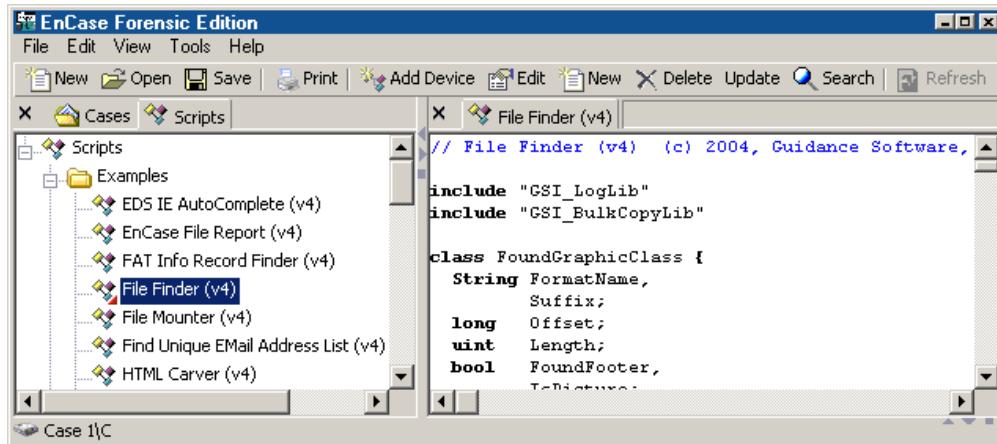


Figure 14-47 Scripts tab

Hash Sets

To access the **Hash Sets** tab, select **Hash Sets** from the **View** pull-down menu. Hash Sets are a collection of hash values of files that belong to the same application. For example, if the `c:\Windows` folder is hashed on a “clean” system, the resulting collection of hash values could be labeled “Windows 98 Hash Set”. The Hash Sets tab is where Hash Sets can be edited, deleted, and imported.

A Hash Library is a collection of hash sets.

All hash functionality, editing, deleting, and importing, is accessible by right clicking and selecting the appropriate menu command. Hash Sets are explained in detail in *Chapter 13: First Steps*.

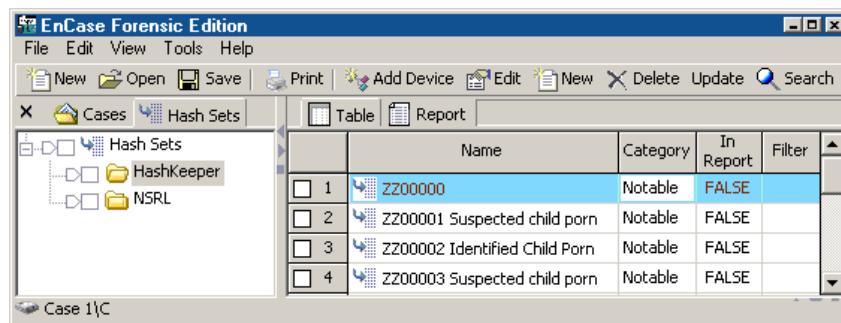


Figure 14-48 Hash Sets tab

EnScript Types

The **EnScript Types** tab is accessed by selecting **EnScript Types** from the **View** pull-down menu. The **EnScript Types** tab is a reference resource that contains the classes of the EnScript language. The right-pane shows the parameter of each function in order.

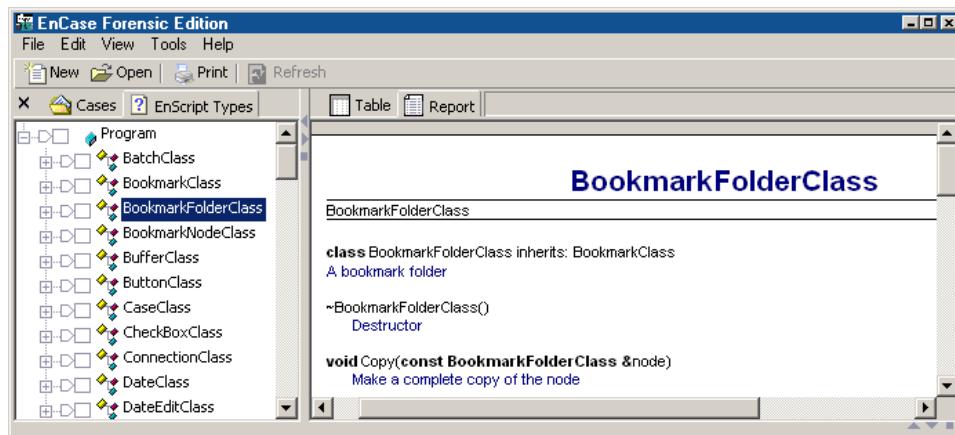


Figure 14-49 EnScript Types tab

Table View

Table view displays all objects in a selected container (folder, device, etc.) and their attributes. The investigator can sort the display by double clicking on the header bar over any of the columns in the table. To sort by up to five columns (sub-sort), hold down the [**Shift**] key and double-click another column header. The first sort is indicated by a red triangle in the header; each subsequent sort will have an additional triangle in the header. As described previously in this document, turning on the “All Files” trigger (clicking on it until it turns green) will recursively show all objects in each subfolder

Name	Filter	In Report	File Ext	File Type
6985 connected_wizard_...			jpg	JPEG
6986 contactinfo[1].jpg			jpg	JPEG
6987 control_up.jpg			jpg	JPEG
6988 Crystal.jpg			jpg	JPEG
6989 default_a[1].jpg			jpg	JPEG
6990 default_b[1].jpg			jpg	JPEG
6991 desktop_screen_sh...			jpg	JPEG
6992 desktop_up.jpg			jpg	JPEG
6993 Df1006.JPG			JPG	JPEG
6994 6Z5J6T6D.JPG			JPG	JPEG

Figure 14-50 Table view with sort (File Ext) and subsort (Name)

Common commands that can be executed in the **Table** view are Copying/UnErasing; bookmarking highlighted or selected (blue-checked) files; exporting the table; viewing file structure of compound files; or sending a file to a specified viewer (see *Chapter 15: Viewing Files*).

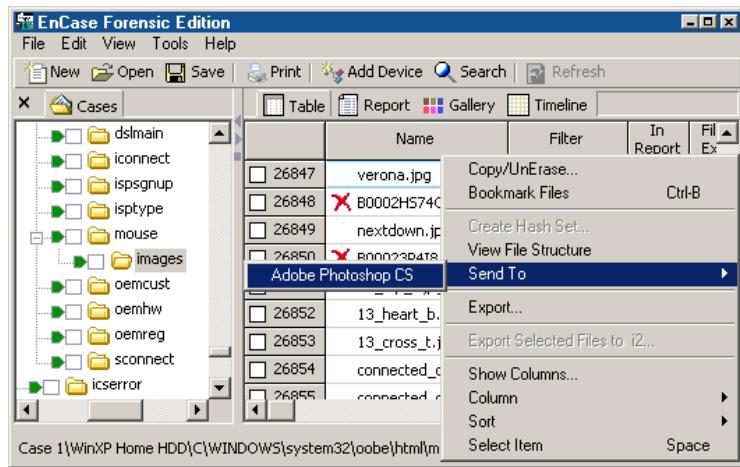


Figure 14-51 Table view commands

Cases Table View Columns Explained

Name

Name identifies the file/folder/volume, etc. in the evidence file by name. Icons to the left of the filename indicate the status of the file (see the next section for an explanation of the icons).

Filter

The **Filter** column displays a filter name if the file meets the criteria of a run filter. For instance, if a two-filter query was executed for “*files accessed in January 2002 only*” and “*pictures larger than 100K*”, files accessed during January, 2002, would display one filter display, pictures larger than 100K would display the other filter, and files matching both criteria would have boxes for both filters displayed.

In Report

The **In Report** column indicates whether or not the item will appear in the report. By default, items in the **Cases** table do not appear in the report, with the

Copyright © 2004 Guidance Software, Inc.

May not be copied or reproduced without the written permission of Guidance Software, Inc.

item having a ***False*** Boolean value (indicated, by default, as a blank entry). To change the value to ***True***, blue check the item, click on the entry in the **In Report** column, and hit [Ctrl] [R], or right-click and select **In Report**. By default, a value of ***True*** is indicated by a bullet in the column, but both the ***True*** and ***False*** indicators can be changed from the **Global** tab in the **Options** settings in the **Tools** pull-down menu. To have multiple files show in the report, blue-check all desired files, then right-click on the **In Report** header and select **In Report – Invert Selected Items** (in any of the selected files already have a ***True*** value, they will be set to ***False***). To include selected files at all levels in the report, use the green Show All button on a parent folder; all files in subfolders with the ***True*** In Report value will show in the report. This feature is used to assist in making quick reports without bookmarking, if desired.

File Ext

The **File Ext** column displays the file's extension. Windows uses the file extension to determine which application opens the file. If a file has been renamed with a different extension type (for example, a JPEG image (.JPG) being renamed to look like an Excel spreadsheet (.XLS)), this column would report the extension given by the user, not the file type's true extension. The file header information is still intact; therefore, a signature mismatch will be reported if and when you ran a **Signature Analysis**.

File Type

This column indicates what file type the file is. EnCase generates this information from the **File Types** table (viewed by accessing the **File Types** option in the **View** pull-down menu) using the file's extension. After a **Signature Analysis** is run, the information will be generated from the file's signature.

File Category

The **File Category** column indicates the category of the file assigned to the file type in the **File Types** part of EnCase. For example, a files with the extension “.AI” would fall under the **Pictures** category, since the extension indicates an Adobe Illustrator file, found under the **Pictures** folder within the **File Types** table.

Signature

The **Signature** column identifies the file by the header, not file extension. If the header and file extension do not match after a signature analysis is run, you will

see a “**!Bad Signature**” message in this column. The **Signature** column is only be populated after a signature analysis is run. Signature Analysis results are explained in *Chapter 13*.

Description

The **Description** column gives a short description or explanation of what the icon to the left of the file name is. For a full explanation of those icons, see the next section.

Is Deleted

A date and time will be in this column if this file has been deleted, but not yet emptied from the Recycle Bin. If the Recycle Bin has been emptied, the deleted files may not be available at all.

Last Accessed

The **Last Accessed** column displays a date of the last access date of the file. A file does not have to be *altered* for the last accessed date to change—only accessed. Any activity (such as viewing, dragging, or even right-clicking) may change the last accessed date. The last accessed date may also change if the file is accessed by a program such as a virus checker.

File Created

The **File Created** column is a record of when a particular file was created *at that location*. If a file is edited and changed on January 3rd, then *copied* to a floppy diskette on January 15th, and then that floppy diskette is acquired on January 28th, EnCase would show that the file (on the floppy) was created *after* it was last written or even accessed.

Last Written

The **Last Written** column displays the last date and time that a file was actually opened, edited, and then saved. If a file is opened then closed, but not altered, the last written date and time do not change.

Entry Modified

The **Entry Modified** column, pertinent to NTFS (Windows NT, Windows 2000, Windows XP, and Windows 2003 Server) and Linux file-system files, refers to the pointer for the file-entry and the information that that pointer contains, such as the size of the file. If a file was changed but its size not altered, then the **Entry**

Modified column would NOT change. However, if the file *size* has changed (from eight sectors to ten sectors, for example), then this column would change.

File Deleted

If an entry in an INFO2 file on an NTFS volume has a deleted date, the time and date of deletion will appear in this column.

Logical Size

The logical size of a file is how large the file is in terms of bytes. If the system being examined uses a 32-bit operating system (e.g., Windows 98 SE), the smallest size a file can occupy is 4096 bytes, even if the file is only 23 bytes.

Physical Size

Physical size is the cluster size of the file. Clusters in Windows 98 SE, for example, are 4096 bytes, so the physical size of any file with a logical size less than 4096 bytes will always have a physical size of 4096 bytes. Files are stored in increments of that unit. (For example, a 7551 byte logical file will occupy 8,192 bytes of physical disk space.)

Starting Extent

The **Starting Extent** column contains the starting cluster of every file in the case. The format displayed is evidence file number, logical drive letter, followed by the cluster number. For example, a starting extent of 1D224803 means that the file is on the second evidence file (counting begins at zero, remember), on the logical D drive of the evidence file, at the 224,803rd cluster.

File Extents

This column lists the number of extents (data runs) of the file that are fragmented on the drive. To view the extents, select on the column value for the file to be examined, and then select the **Details** tab on the bottom pane. When EnCase uncompresses a file, the uncompressed data is displayed in the **Text** and **Hex** bottom pane views, and the raw data is displayed in the **Disk** view. To reconcile the difference between the physical location of the compressed and uncompressed data, EnCase will place '*Sparse*' entries in the File Extents column.

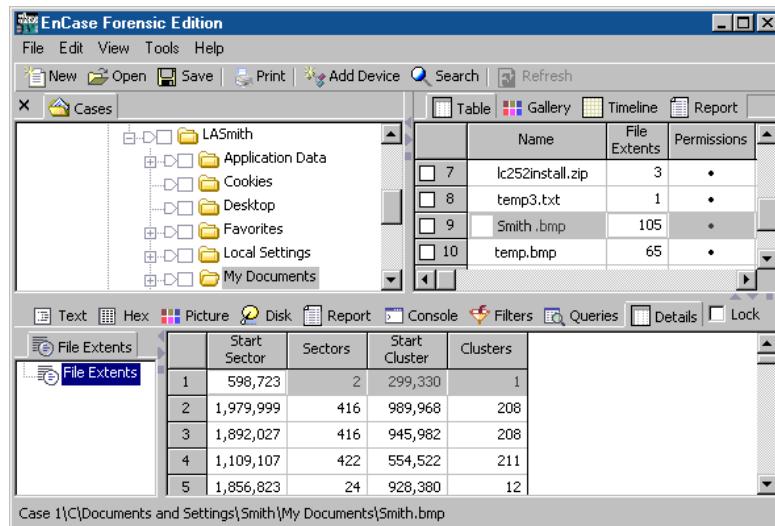


Figure 14-52 File Extents

Permissions

The **Permissions** column displays the security settings of a file or folder. A dot indicates that a security setting is applied. The security settings are viewed by selecting the entry and then clicking on the **Details** tab in the lower pane.

Details Tab

Information displayed within this tab includes:

- **Name**
- **Filter**
- **In Report**
- **Id**
- **Property**
- **Permissions**

Name

Displays any name associated with the ID. **Permissions** is the default (no name is associated with the selection). Names are associated from within the evidence (local accounts and some built-in) or by associating a volume with a set of id/name pairs from the Security ID pane.

Filter

Functions the same as the **Filter** column as described in Table view.

In Report

Functions the same as the **In Report** column as described in Table view

ID

This column displays the ID related to the permission, either as a regular number (Unix), or in S-x-x... format (Windows). In the Windows environment, each permission has an associated ID. In the Unix environment, only rows that specify **Owner** and **Group** have an associated ID.

Property

This column shows the significance of each particular row in the table (for instance, **Allow**, **Deny**, **Owner** or **Group**).

Permissions

Permissions specific to the highlighted item are extracted and listed in this column.

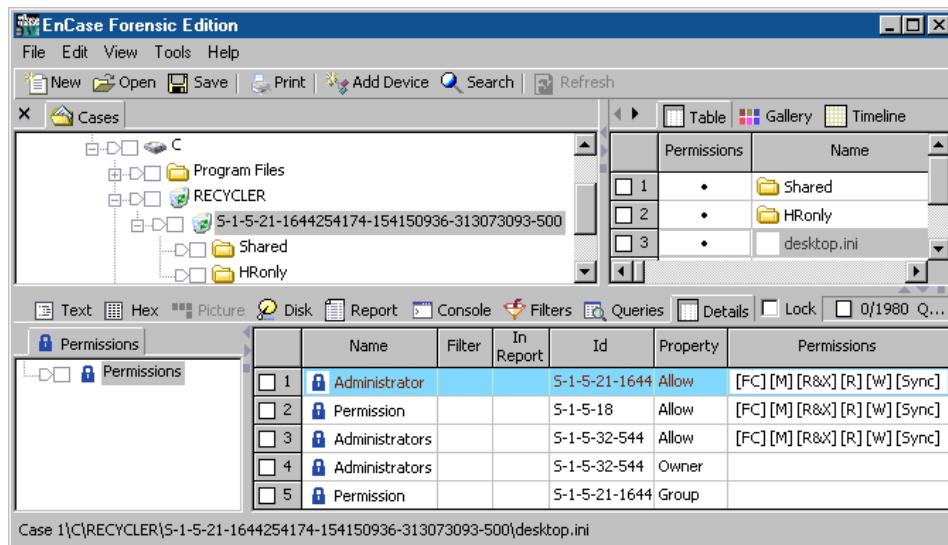


Figure 14-53 Permissions Column window

Each permission is enclosed in brackets ([); a key to the permission definitions follows:

The permissions for the Unix environment are:

G-R	Generic read
G-W	Generic write
G-X	Generic execute

The permissions for the Windows environment are:

Obj In ACE	Object Inherit ACE
Cont In ACE	Container Inherit ACE
No Prop In ACE	No Propagate Inherit ACE
In Only ACE	Inherit only ACE
FC	Full Control
M	Modify
R&X	Read and Execute
R	Read
W	Write
Delete	Delete
R Attr	Read Attributes
D Sbfldr & Fl	Delete Subfolders and Files
Trav Fldr/X Fl	Traverse Folder/Execute File
W EA	Write Extended Attributes
R EA	Read Extended Attributes
Crt Fldr/App Data	Create Folders/Append Data
Crt Fl/W Data	Create Files/Write Data
Lst Fldr/Rd Data	List Folder/Read Data
W Attr	Write Attributes
Sync	Sync
Tk Own	Take Ownership
Chg Perm	Change Permissions
R Perm	Read Permissions
G-R	Generic R
G-W	Generic W
G-X	Generic X
G-All	Generic All
ACL Access	SACL Access

Bookmarks

The **Bookmarks** column is present in EnCase v4.16 and above. It is similar to the **Is Bookmarked** column in version 3; however, the improved feature lists the number of times the file was bookmarked vs. the true/false flag of version 3. If a file has an entry in the **Bookmarks** column, and the file is highlighted in that column, a **Details** tab appears in the bottom pane, where you can view the type of bookmark made, the folder location, bookmark comments, and a preview of the swept text in Highlighted Data bookmarks. Double-clicking on the

bookmark entry in the **Details** view will take you to the bookmark in **Bookmarks** view.

Physical Location

EnCase organizes the Unallocated Clusters (UC) of a device into one virtual file. It reads the FAT (File Allocation Table) of the file system, or the \$Bitmap in NTFS to create this virtual file. This allows the examiner to examine all of the UC very efficiently with keyword searches and EnScripts. **Physical Location** is the number of bytes into the device at which the UC begins.

Physical Sector

The Physical Sector column lists the sector where the item resides in Unallocated Space, based on an algorithm applied to the data in the Physical Location column. This coincides with the Start Sector in the Details tab when viewing the File Extents in the table. This feature was added in version 4.20.

Evidence File

The **Evidence File** column displays which evidence file the file resides in.

File Identifier

The **File Identifier** is a file table index number, stored in the Master File Table. It is a unique number allocated to file/folders in an NTFS file system.

Hash Value

The **Hash Value** column displays the hash value of every file in the case. The **Compute Hash Value** command must be run to generate this information.

Hash Set

The **Hash Set** column displays the hash set to which a file belongs. If no hash sets have been created or imported, this column will be unpopulated.

Hash Category

The **Hash Category** column displays the hash category to which a file belongs. If you have not created or imported any hash sets, then this column will either be unpopulated, or display both **Known** and **Notable**.

Full Path

The **Full Path** column displays the location the file is located within the evidence file. It includes the evidence file name in the path.

Short Name

The **Short Name** is name that Windows gives the file using the DOS “8.3” naming convention. For example, a file with the file name “onethousanddollarbill.jpg” would appear in this column as “onetho~1.jpg”.

Unique Name

This column is used to display the name for files mounted with the EnCase Virtual File System (VFS) Module in Windows Explorer. For more information about the EnCase VFS Module, please refer to the VFS user manual available for download from the Downloads web page at www.guidancesoftware.com.

Original Path

The **Original Path** column displays information derived from the INFO2 file on deleted files sitting in the Recycle Bin; specifically, where the deleted file originally came from.

- For allocated (not deleted) files, the column is blank
- For files within the Recycle Bin, this column shows where they originated from before they were deleted
- For deleted/overwritten files, this column shows what file has overwritten the original

Organizing Columns

Rearranging Columns

Table columns can be arranged in any order. Use the horizontal scrollbar or the right arrow to maneuver to the desired column, left click on the header of the column and hold the button, and drag the column to the desired position. To reset the column arrangement to the default setting, right click anywhere in the table, and select the **Reset** option under **Column**.

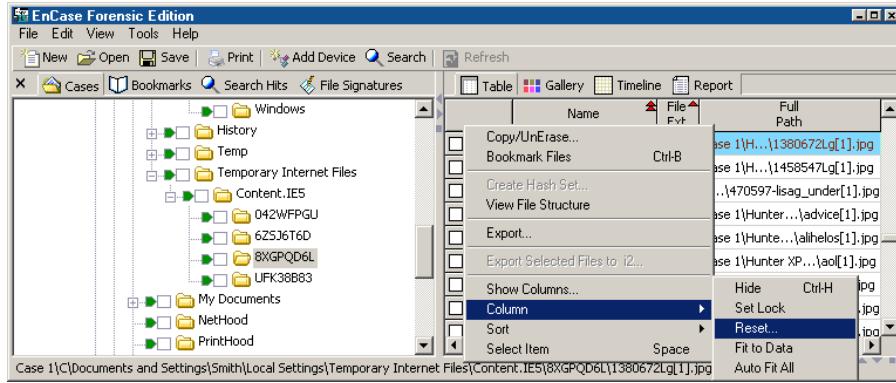


Figure 14-54 Resetting Columns

Hiding and Showing Columns

With over twenty-columns to scroll through in the Table view contains over 20 columns scrolling through unused columns may be time-consuming. You can select which columns you wish to display as follows:

1. Right-click anywhere in the table and select **Show Columns....**
2. Blue-check only the columns you wish to display, and then click **[OK]**.

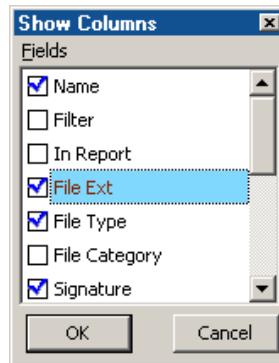


Figure 14-55 Setting columns

Sorting Files in Columns

Sorting files in columns quickly finds specific files or bookmarks. If, for example, an investigator wanted to view only JPEG files within a case, they can

sort on the **File Ext** column then scroll to the JPG files section, as all JPEG files are sorted together. Alternatively, a JPG filter could also be used. In later revisions of version 4, EnCase employs “intellitype” functionality to allow you to click anywhere in a column, type the letters of the entry you wish to search for, and the cursor will jump to the desired entry. For instance, if you are looking for JPEG files, click anywhere in the **File Ext** column and type the letters J, P and G; you will be taken to the first entry with a .JPG extension. In version 4.18, typing [J] [P] would take you first to the first item beginning with “J”, then to the first item beginning with “P”. This was improved in 4.19 to allow multiple characters. The timeout is approximately 200 milliseconds between keystrokes, so an intentional pause in the keystrokes will take the selection to the beginning of the entries matching the last typed character.

Sorts and sub Sorts are possible up to five layers deep. Hold down the [**Shift**] key and double-click on the header of each subsequent column you wish to sort by. Sorts and sub Sorts are also possible in the **Search Hits** and **Bookmarks** tables. For example, if a signature and hash analysis has been run, you can sort first by **File Ext**, then by **Hash Set**, and finally by **Name** in order to quickly find all the JPG files and compare them to Hash Sets in the library.

The screenshot shows the EnCase Forensic Edition interface. On the left, there's a tree view of file paths under 'Cases'. On the right, there's a 'Table' view showing a list of files. The columns in the table are 'Name', 'File Ext', and 'Hash Set'. The table is sorted by 'File Ext' (with 'jpg' at the top), then by 'Hash Set' (with 'Z00232 Microsoft Windows XP Professional' at the top), and then by 'Name' (with 'a6[1].jpg' at the top). The status bar at the bottom shows the path 'Case 1\...\Wallpaper\Azul.jpg'.

	Name	File Ext	Hash Set
27886	a6[1].jpg	jpg	Z00232 Microsoft Windows XP Professional
27887	Ascent.jpg	jpg	Z00232 Microsoft Windows XP Professional
27888	Autumn.jpg	jpg	Z00232 Microsoft Windows XP Professional
27889	Azul.jpg	jpg	Z00232 Microsoft Windows XP Professional

Figure 14-56 Sort by *File Ext, Hash Set, then Name*

EnCase Icon Descriptions

This section contains a detailed description of the icons used in EnCase. In Table view, the icon to the left of the file name typically describes the file’s status.



Root (global): In any view (**Cases**, **Bookmarks**, **Keywords**, etc), this is the root folder. It is displayed even if there is nothing else created in the view window.



Case: This icon is displayed in all views.

-  **Device:** A physical hard drive icon. This icon does not represent a volume or logical device, such as a partition.
-  **Network Share Device:** This icon appears when the VFS or PDE Module virtually mounts a case, device or folder.
-  **Volume or Logical Device:** Represents a volume, logical disk, and/or a partition.
-  **RAID, Dynamic Disk:** RAID disks and Dynamic Disks.
-  **Rebuilt RAID or Dynamic Disk:** RAID or Dynamic disk, successfully rebuilt within the EnCase environment..
-  **CD ROM:** Indicates a CD ROM.
-  **CD ROM session:** Indicates a session on a multi-session CD ROM.
-  **Folder:** An allocated folder.
-  **Deleted folder:** A folder that is deleted.
-  **Deleted, Overwritten folder:** A folder that is deleted and over-written by another file (see **Deleted, Overwritten file**).
-  **Folder, Invalid Cluster:** A directory entry whose file type bit is set to "folder;" and whose starting cluster is set to zero.
-  **Lost Files/Recovered Folders:** Lost Files, Recovered Folders or indicates examining an NTFS or FAT drive.
-  **Deleted file:** A deleted file on the suspect's computer that has been undeleted by EnCase; nothing is changed in the evidence file.
-  **Deleted and Overwritten file:** EnCase determines that the starting cluster found in the directory entry for this file is occupied by another file and makes no further attempt to undelete this file. The name of the overwriting file is displayed in the status bar, and its contents (not that of the deleted file) displayed. Remnants of the original file may exist. Further examination should include checking the starting cluster, and the size of both files, to enable the examiner to determine if the data has been over-written. If it has not, the original file data may be on the hard drive in the slack space of the new file.
-  **Invalid Cluster:** A filename entry that does not have a starting cluster number. EnCase cannot locate the file's contents. Invalid cluster numbers are normally generated from system-deleted files, where the starting cluster number is changed to zero. This evidence indicates that the filename existed and the dates that it was created, modified, and accessed.
-  **File, Hard Linked:** A condition when multiple **Names** have a direct connection to the same Inode. EnCase splits the data into a file named "**Hard Link Data #**". All corresponding **Hard Links** point to this file for the data. (for example: /bin/ls uses inode 64860; /var/ftp/bin/ls also uses inode 64860).

Copyright © 2004 Guidance Software, Inc.

May not be copied or reproduced without the written permission of Guidance Software, Inc.

-  **Internal File:** A file created by file systems such as NTFS, HFS, Linux, EXT2.
-  **Recycle Bin:** The suspect's recycle bin.
-  **Unallocated space, MBR, unused disk area, FAT tables, VBR, Volume slack:** A representation of these areas of the disk, showing that no files are currently allocated to these areas.
-  **Text:** A view of the selected file in ASCII.
-  **Hex:** A view of the selected file in Hexadecimal for each character displayed.
-  **Picture:** Displays a picture if the selected file type is a graphic image.
-  **Report:** Displays the data that appears in the report for the selected item.
-  **Console:** Displays the console contents (C:\Program Files\EnCase4\console.txt); status information about the results of processes such as scripts, searches, and Recovered Folders, for example.
-  **Filters:** Displays the available filters for the current view.
-  **Queries:** Displays the available queries for the current view.
-  **Disk:** In the bottom pane, displays the contents of the disk divided into individual sectors, which are represented as blocks. Each block pattern and color has its' own definition as follows:

	Volume Boot		Allocated		Unknown
	FAT 1		Lost Cluster		Volume Slack
	FAT 2		Deleted File		Disk Manager
	Root Folder		Boot Sector		
	Unallocated		Wasted Area		
	Bad Cluster		No Partition		
-  **Bookmark:** Puts EnCase in **Bookmark** view.
-  **Highlighted Data Bookmark:** Created by sweeping data (clicking and dragging the mouse over data) in one of the sub-panes. This is a customizable bookmark.
-  **Notes Bookmark:** Allows the user to write additional comments into the report. It is not an evidence bookmark..
-  **Folder Information Bookmark:** Bookmarks the tree structure of a folder or device information of the selected media. The options include showing the device information, such as drive geometry, and the number of columns to use for the tree structure.
-  **Notable File Bookmark:** A file bookmarked by itself. This is a customizable bookmark..



File Group Bookmark: A bookmark that is part of a group of selected files. There is no comment on this bookmark.



Snapshot Bookmark: Contains the results of a system Snapshot of dynamic data for incident response and security auditing. This information is acquired running the *Scan Local Machine (v4)* EnScript against a preview of the local drive.



Log Record Bookmark: Contains the results of the log parsing EnScript.



Open Ports Bookmark: Contains the snapshot data for all open ports on a target system.



Process Bookmark: Contains the snapshot data about all processes running on a target system.



Open Files Bookmark: Contains the snapshot data on any open files on a target system.



Network Interfaces Bookmark: Contains the snapshot configuration of any of the network interfaces on a target system.



Network Users Bookmark: Contains the snapshot of the network users with system access.



IDS Events Bookmark: Contains a snapshot of IDS events



Registry Bookmark: The results of a Windows registry parsing EnScript (such as *Initialize Case (v4)*). This icon is also displayed in certain scripts when selecting the registry.



File Types: Selecting this icon presents the **File Types** view.



File Signatures: Selecting this icon presents the **File Signatures** view



File Viewers: Selecting this icon presents the **File Viewers** view.



Keywords: Selecting this icon presents the **Keywords** view.



Search Hits: Selecting this icon presents the **Search Hits** view.



Preview icon: When displayed inside any other icon, this icon indicates that there is a preview being performed on the selected device



Floppy disk \ Zip disk: Indicates a floppy disk or Zip disk preview\acquisition, and is also displayed in the **Add Device** window as a valid removable device.



Empty floppy disk: No floppy media in the selected drive.



FastBloc protected device: A FastBloc write protected device available for preview or acquisition.

-  **Palm:** A Palm PDA device or evidence file is present.
-  **Parallel Port \ Network Crossover:** A device has been added using a parallel port or a network crossover cable.
-  **Security Ids:** EnCase extracted file and folder security information (owner, group and permissions) for an NTFS file system as well as owner, group and permission settings for a Unix, or Linux system
-  **Text Styles:** Selects the text style to view Code Pages in different settings, like variations in color and text line length. EnCase is configured with default text styles, but additional styles can be added, edited, and deleted from this tab by either right-clicking and selecting the command from the contextual menu or clicking the button in the toolbar
-  **EnScripts:** Small programs or macros designed to automate forensic procedures.
-  **Hash Sets:** A collection of hash values of files that belong to the same application.
-  **App Descriptors:** This view enables examiners to organize the hash values of live processes running on a system scanned by the Snapshot function.
-  **Machine Profiles:** This view enables examiners to create a custom profile of the authorized applications or processes that should be running on a target machine.
-  **Encryption Keys:** This view enables users to generate key pairs to be used with EnCase Enterprise.
-  **EnScript Types:** A reference resource containing the EnScript language classes. The right-pane displays each functions parameter.
-  **Redirect:** Indicates the file that overwrote a deleted file, displayed in the status bar. The contents being displayed are not the contents of the deleted file.
-  **EnScript Member Functions:** Functions that are defined within the Script or Class.
-  **EnScript Function Arguments:** Arguments that are used in EnScript functions
-  **EnScript Argument Passed by Reference:** Arguments of functions that are passed by reference.
-  **EnScript Enumerations:** Enumerators for functions or classes
-  **EnScript Constants:** Constants that are used in Scripts or Functions

Gallery View

The Gallery view is a quick and easy way to view images that were stored on the Subject media. This includes all images purposely stored and all images inadvertently downloaded from the web.

It is possible to access all images within a highlighted folder, highlighted volume, or the entire case. If a folder is highlighted in the left pane of the **Cases** tab, EnCase will display all contained files in the right pane. The “All Files” trigger displays **all** images within the folder and any subfolders.

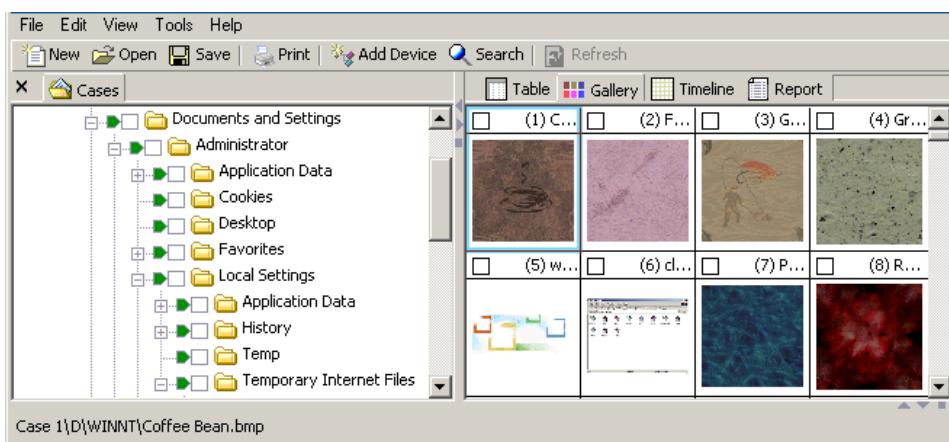


Figure 14-57 Gallery View

Within the Gallery view it is possible to bookmark images to display them in the report. Right-click on the image you wish to bookmark and choose **Bookmark Files**. Multiple images can be bookmarked simultaneously by blue-checking the box at the top left of each file. When the **Bookmark Files** option is selected, a check box will appear in the **Bookmark Files** dialog box to **Bookmark Selected Items**; with a single file blue-checked, this option is grayed out. Toggling this check box will determine if the selected file or all blue checked files are bookmarked.

The Gallery view displays files based on their file extension. For example, if a .jpg file has been renamed to .dll, it *WILL NOT* be displayed in the Gallery view until a Signature Analysis has been run. Once the Signature Analysis has recognized that the file has been renamed and that the file is actually an image, it will be displayed in the Gallery view.

To reduce or increase the number of images displayed in the Gallery view at any one time, right click in the Gallery and select Fewer Columns, More Columns, Fewer Rows or More Rows from the menu.

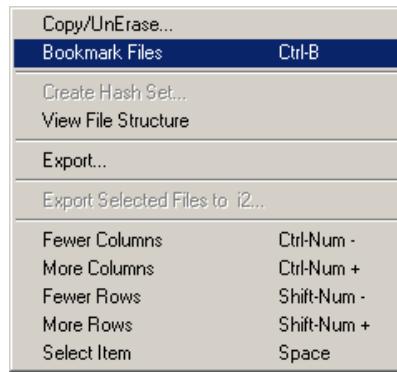


Figure 14-58 Gallery options

In the past, viewing a corrupt image could cause EnCase to crash. EnCase 4.18 and above includes built-in crash protection, which prevents corrupted graphic images from appearing in Gallery or Picture view. The corrupt images are stored in cache so that EnCase recognizes them the next time they are accessed, and does not attempt to display them. These images are cached at the case level so that the images will not attempt to display in that case file again. The cache can be cleared by right clicking on the case in **Cases** view and selecting **Clear invalid image cache....** This option only appears after a corrupt image is encountered. The timeout (12 seconds by default) for the thread trying to read a corrupt image file can be set by clicking on the **Global** tab after selecting **Options** from the **Tools** pull-down menu.

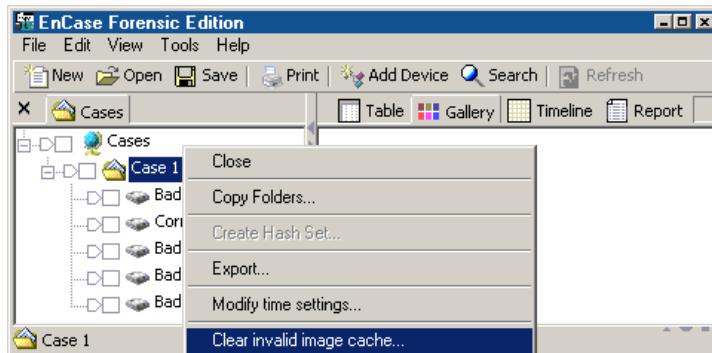


Figure 14-59 Clearing invalid image cache

America Online .ART files

EnCase 4.16 and above has added support for America Online .ART format images in the Picture and Gallery views. The .ART support requires the Internet Explorer AOL Support module be installed on the examination computer. The installer is available for download and installation from Microsoft's web site at <http://www.microsoft.com/windows2000/downloads/recommended/aolfix/default.asp>.

This will install Jgaw400.dll, Jgdw400.dll, Jgmd400.dll, Jgp1400.dll, Jgsd400.dll, and Jgsh400.dll. The installation does not require a reboot of the computer, nor closing and restarting of EnCase.

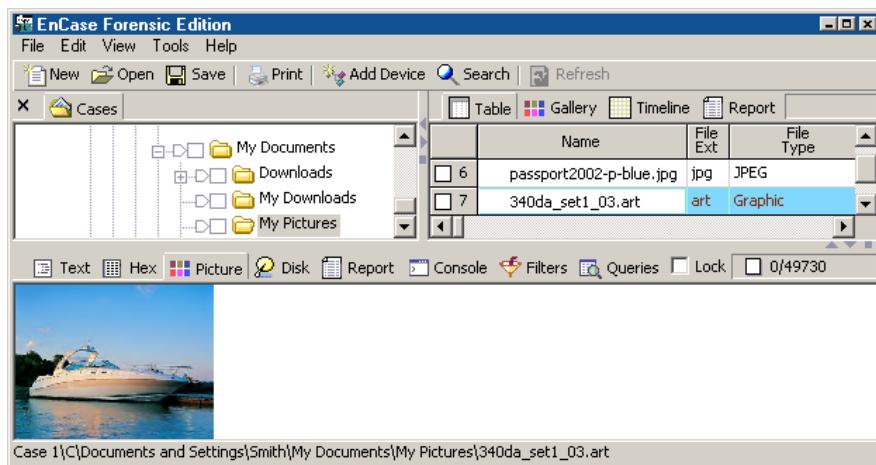


Figure 14-60 Right-click for pop-up menu

Timeline View

The Timeline view is a great resource for looking at *patterns* of file creation, editing, and last accessed times. You can zoom in (**Higher Resolution**) to a second-by-second timeline and zoom out (**Lower Resolution**) to a year-by-year timeline by right clicking and selecting the appropriate option.

Above the calendar view are five check boxes to quickly and easily filter which type of time stamp to display: **File Created**, **Last Written**, **Last Accessed**, **Last Modified** and **File Deleted**.

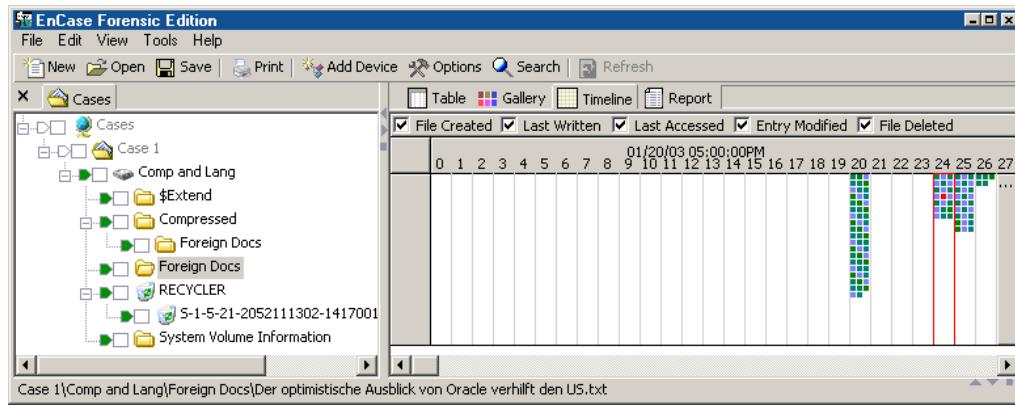


Figure 14-61 Timeline View

Times are represented by different color squares in Timeline view; the default colors are as follows:

- A file with a **File Created** date / time stamp is represented by a green square (Red: 0, Green: 128, Blue: 92) ■
- A file with a **Last Written** date / time stamp is represented by a green square (Red: 0, Green: 128, Blue: 0) ■
- A file with a **Last Accessed** date / time stamp is represented by a light purple square (Red: 128, Green: 128, Blue: 255) □
- A file with a **Last Modified** date / time stamp is represented by an aqua square (Red: 0, Green: 128, Blue: 128) ■
- A file with a **Deleted** date / time stamp is represented by a red square (Red: 255, Green: 0, Blue: 0) ■
- A file with a **Logoff** date / time stamp is represented by a black square (Red: 0, Green: 0, Blue: 0) ■
- **Dark blue** squares indicate that file is blue checked in the table. ■
- **Bright red** squares indicate that the file is highlighted. ■

A gray box with three dots in a row ([...]) indicates that there are too many files to list in the space given. Double-click the box to zoom in for file details.

The **Logoff** option is only valid for EnCase Enterprise.

The color assignments for each box can be changed by right clicking in the timeline and selecting **Options...** Right click on each color to assign additional colors (**Transparent, Black, Light Red, Light Green or Light Blue**), or double click on them to assign a custom color. To change a box back to its' default color, right click on that box and select **Default**. You can also change the timeline start and stop dates in the **Options** window.

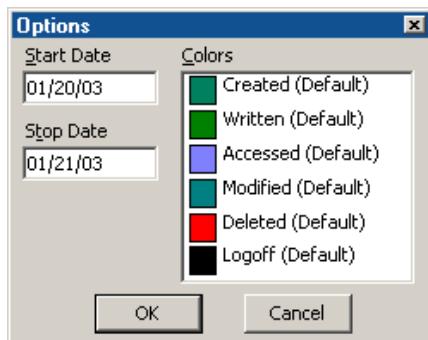


Figure 14-62 Timeline Options

Report View

Report view displays information about the current folder/volume selected in the left pane, such as date and time stamps and file permissions. In the **Bookmark** tab, Report view provides documentation for all of the evidence bookmarked during the investigation. For additional information, see *Chapter 24: The Report*.

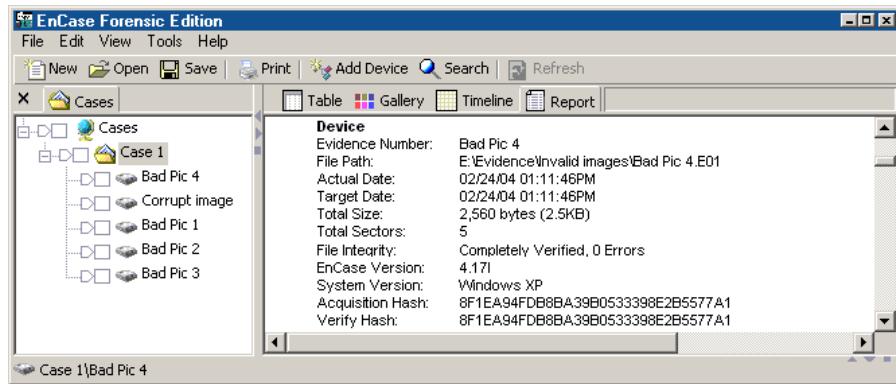


Figure 14-63 Report View

EnScript View

When the **Scripts** view is selected, the right pane shows the code for the EnScript selected from the list in the left pane. The name of the EnScript will be displayed on a tab at the top of the left pane; previously run EnScripts will also have tabs present. Double-click on the EnScript to activate it. To compile the script then click on the [**Compile**] button on the top toolbar, press [**Ctrl**] and [**F9**] simultaneously, or right click in the code window and select **Compile**. To run the script, click on the [**Run**] button on the top toolbar, press [**F9**] simultaneously, or right click in the code window and select **Run**.

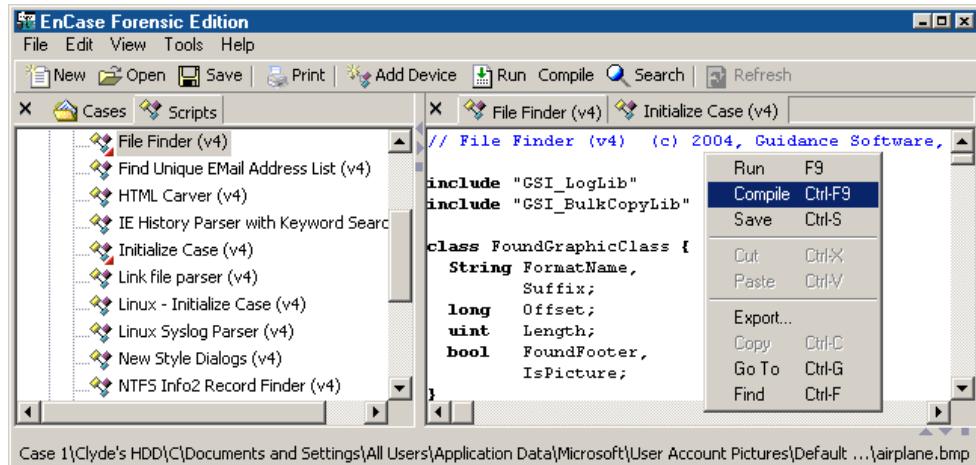


Figure 14-64 EnScript View

Bottom Pane

The bottom pane provides functionality specific to the view open and the item selected in the right pane. This includes feature tabs, a box to keep the tab constant, and a navigation bar with numbers of files in the case and selected, and the precise location of the item selected.

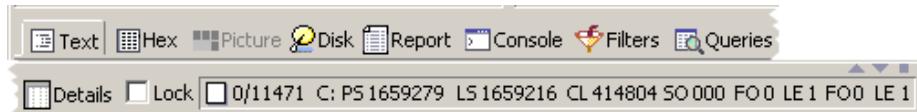


Figure 14-65 Bottom Pane toolbar

Bottom Pane Tabs

Text

The **Text** tab is for viewing text in the highlighted file above. It contains the output of the data in the selected Text Style for the currently selected file. Portions of the text can be “swept” by clicking and dragging, and then bookmarking, exporting or copying/pasting the highlighted data.

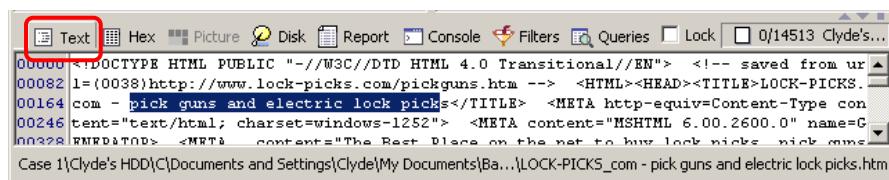


Figure 14-66 Text tab

Hex

The **Hex** sub-tab contains the data, in hex format, of the currently selected file. The right-pane displays the text of the corresponding hex characters. EnCase 4.18 added the ability to sweep and copy data in the Hex view to the clipboard, and then paste the data as **Hex** in the desired application or within EnCase (similar to the method used for **Text**).

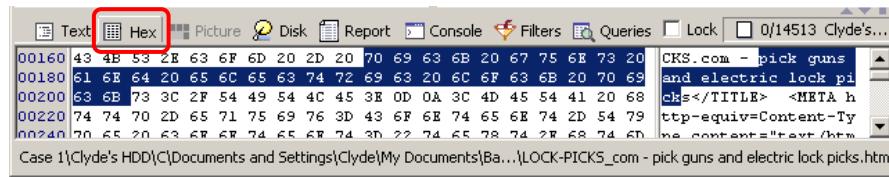


Figure 14-67 Hex tab

Picture

The **Picture** tab displays the highlighted file/folder as an image. If the file is not an image, then the **Picture** tab will be grayed-out. EnCase can natively display GIF, JPEG, BMP, PNG, Photoshop PSD and TIFF files. Other image types require 3rd-party viewers.

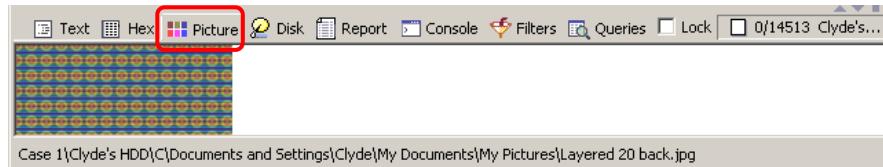


Figure 14-68 Picture tab

Disk

The **Disk** tab is a graphic representation of the sectors of the evidence file. For each file selected in the Table view, the **Disk** tab displays where that file is physically located on the evidence file. The right pane of the Disk tab features tabs that allow the user to view the data in **Text** or **Hex** modes. There is also a tab that shows a legend to help determine what the colored block in Disk view represents (see the previous *EnCase Icon Descriptions* section for legend details).

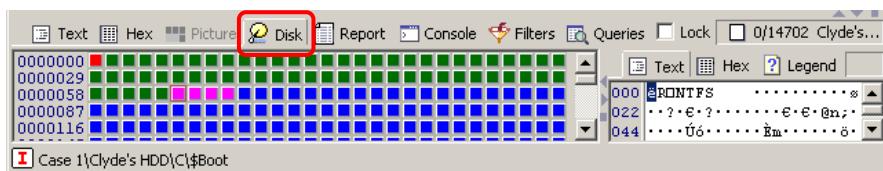


Figure 14-69 Disk tab

Report

The **Report** tab displays the attributes of the currently selected file. The data shown is the same data as what is the Table view, but displayed in a report format in addition to the security attributes (if in NTFS).

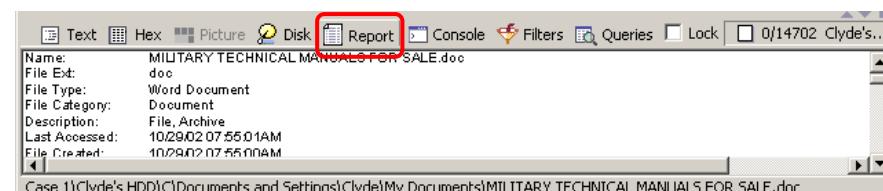


Figure 14-70 Report tab

Console

The **Console** tab displays output from EnScripts, and functions such as Signature Analysis and searches that send output to the console upon execution. The console is located at C:\Program Files\EnCase4\console.txt.

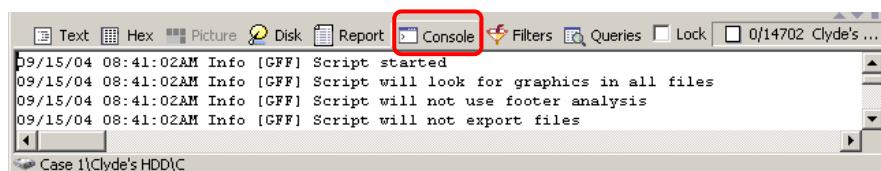


Figure 14-71 Console tab

Filters

The **Filter** tab allows the investigator to quickly and easily create, edit and run filters to display or exclude files in a case that meet specific criteria. For example, to view only bitmap (.BMP) files in a case, the built-in BMP Extension filter is run. In the example shown in *Figure 14-70*, the case has 14,702 files in it but only the 90 .BMP images are displayed. It is relatively easy to determine that a filter is being run by the presence of the **Stop Query** button on the top toolbar, the query name field in the right pane, and the filter name listed in the **Filter** column of the table.

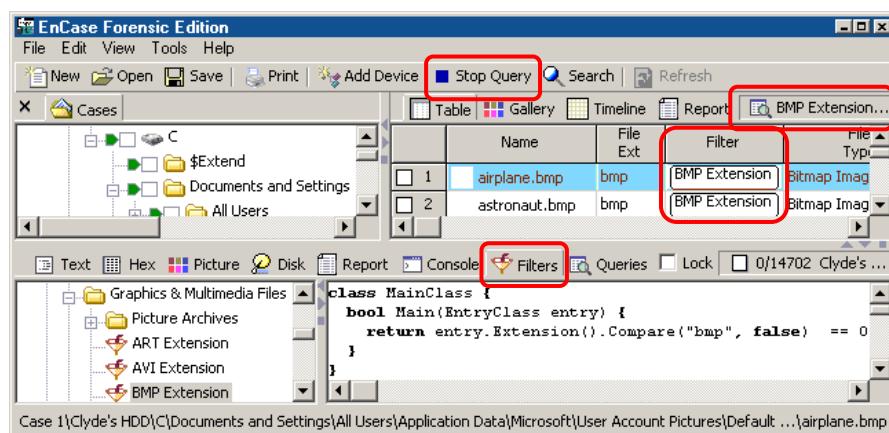


Figure 14-72 Filter tab

Queries

The **Queries** tab combines the functionality of small filters together, creating customized, powerful queries that drastically reduce the time taken to navigate

files. Queries that come standard with EnCase will appear in the bottom left pane; a **View** tab and an **Include** tab appear on the right. The View tab allows you to change the attributes of the query, including how the results are viewed. **Include** allows adjusting the logic and criteria of the query. For example, the investigator may wish to view only log files, mail files, and any DOC, TXT, WP, and HTML files.

Using the Compound Filter Query, the individual filters can be combined to make one complex query. Building queries by combining filters together is covered in detail in *Chapter 18: EnScript and Filters*.

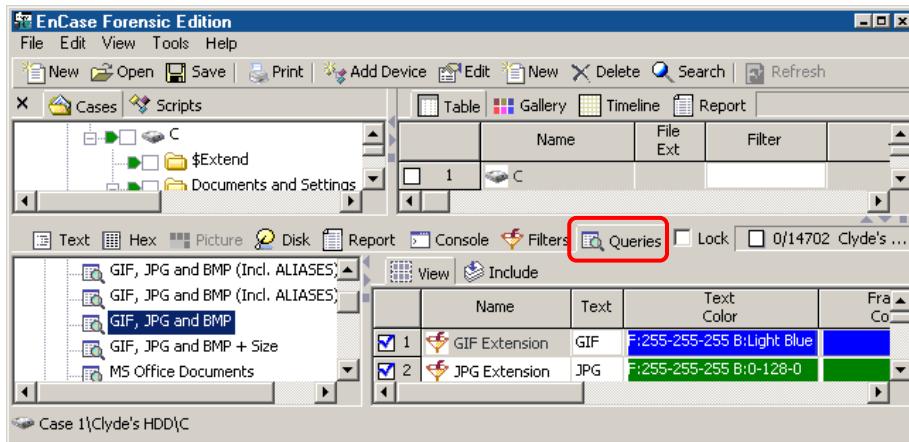


Figure 14-73 Queries tab

Details

The **Details** tab is used to show multi-dimension data referenced in a column of the Table view, such as **File Extents** or **Bookmarks**

	Name	Path	Comment
252	Highlighted Data	Case 1\Recovered Files\	GIF: themedef.mar File offset: 29423

Figure 14-74 Details tab

Lock

Checking **Lock** preserves the selected lower pane when scrolling through files. For example, if scrolling through the disk locked in **Disk** mode, when an image is selected, rather than go to Picture mode, **Disk** view will be displayed for each file selected rather than returning to the default view for the file type.

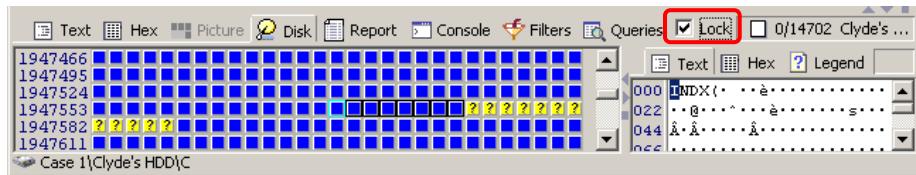


Figure 14-75 Lock check box

Navigation Bar

The navigation bar, which displays sector and cluster information, sits to the right of the **Lock** check box. Every time the investigator clicks on new data (for example, clicking through sectors in the **Disk** view), the information displayed for that currently selected sector or cluster changes. The navigation bar contains the following information:

- **The “Dixon Box”**

Immediately to the right of the **Lock** box is a check box with two numbers separated by a slash, referred to as the **Dixon Box**. The first number reflects the number of selected (blue-checked) files, while the second reflects the total number of files in the case. To quickly uncheck all files in a case, click in the box so that the first number is 0. Clicking again will select all files in a case.

- **Evidence file name**

The name of the evidence file currently being accessed will appear here.

- **Physical sector number**

The number following the **PS** will indicate the number of the physical sector currently accessed.

- **Logical sector number**

The logical sector, following the **LS**, equals the Physical Sector minus 63.

- **Cluster number**

This indicates the location of the cluster being accessed and follows the **CL**.

- **Sector offset**

Identified by the **SO**, this is the offset value within the *sector* of where the currently selected sector/cluster is.

- **File offset**

Identified by the **FO**, this is the offset value within the *currently highlighted file* of where the currently selected sector/cluster is.

- **Length**

The length, which follows the **LE**, indicates the number of bytes currently highlighted. Bytes can be “swept” (clicked and dragged to highlight) in the **Text** and **Hex** view, but *not* the **Disk** view.



NOTE: EnCase v4 uses the absolute byte offset for FO, as some devices (such as PDAs) do not use sectors or have sectors not equal to 512 bytes. This enables EnCase to give the examiner a more accurate and exact location of bookmarked evidence on the device. For example, the Physical Location of 3,688,448 is the number of bytes into the device at which a file, folder, bookmark or Unallocated Clusters start.

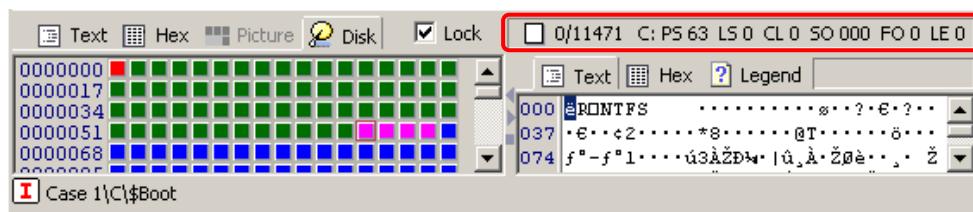


Figure 14-76 Navigation bar

Find

To search for specific text located in the lower pane in **Text** or **Hex** view, right-click and select **Find** or hit [**Ctrl**] [**F**]. If text has been selected, the **Find** window will open with the selected text in the Expression field.

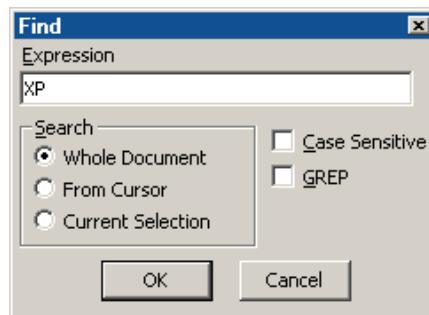


Figure 14-77 Find

The search options include:

- **Whole Document:** Searches the contents of the entire lower pane for the search string specified in the Expression field.
- **From Cursor:** Searches from the current cursor position to the end of the lower pane's text content for the search string specified in the Expression field.
- **Current Selection:** Searches for identical search strings specified in the Expression field.
- **Case Sensitive:** Searches for the specified sting with regard to upper and lower case letters.
- **GREP:** Uses a specified GREP expression for the search string.



NOTE: Once the **Find** shows the first instance of the requested string (highlighted), you can press the F3 key to continue searching for similar strings.

EnCase, by default, displays characters in the **Text** and **Hex** tabs in 8-bit ANSI format. Unicode files view properly; however, modifications of both the format (encoding) and the font are required (see *Chapter 20: Foreign Language Support (Unicode)* for further details).

Split Panes

Whenever panes are split (right and left top panes, top from bottom, **Disk** view and **Text\Hex** view in the bottom pane), panes can be resized, eliminated or restored using the gray arrow buttons found on the bars between the split. The left arrow increases the right pane to the full width of the EnCase window; the right arrow increases the left pane to the width of the window. The up and down arrows on the horizontal split have similar functionality. The gray square restores the split to the default size. To resize the split manually, left click on the bar between the split and drag the bar to the desired location

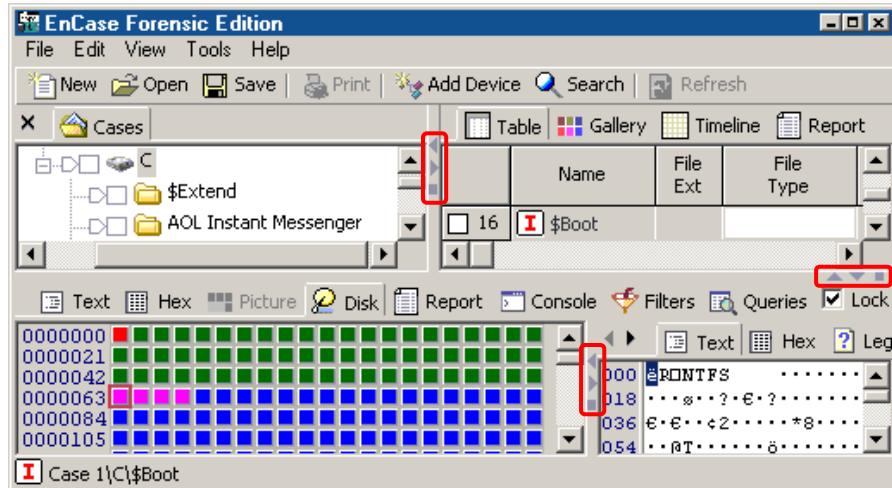


Figure 14-78 Sizing split panes

Date and Time Questions

Is the Last Accessed Date the same as the deleted date?

No. DOS does not store the deleted date of a file in the directory entry record. The only time that you can recover the deleted date and time is when the file is in the Recycle Bin. EnCase will recover these times when possible and display them in the **Deleted** column.

On some files, there are no time stamps in the Last Accessed column.

If the file was created by a version of DOS prior to 7.0, the last access date will be blank.

*Copyright © 2004 Guidance Software, Inc.
May not be copied or reproduced without the written permission of Guidance Software, Inc.*

Chapter 15

Viewing Files

In the two previous chapters, we learned how to navigate the EnCase interface and learned timesaving and fundamental tasks to perform at the beginning of an investigation to locate any suspect files on the Subject media.

Many file types are not immediately viewable within EnCase, however. Audio files, video files, certain graphic file formats and more require third-party viewers to view the files correctly.

Copy/UnErasing Files

EnCase has a feature to recover and unerase files byte-per-byte.

Selecting Files

Many operations in EnCase require selecting a list of files. To select a file, click on the check box to the left of the number in the Table view so that a blue check mark appears. To select or deselect an entire folder, click on the check box next to the folder in the Cases tab. You can select a range of files by blue-checking the first file in the range, holding down the **[Shift]** key and blue checking the last file in the range. Files blue-

checked in a subfolder will display blue checks all the way up the tree to the root of **Cases**.

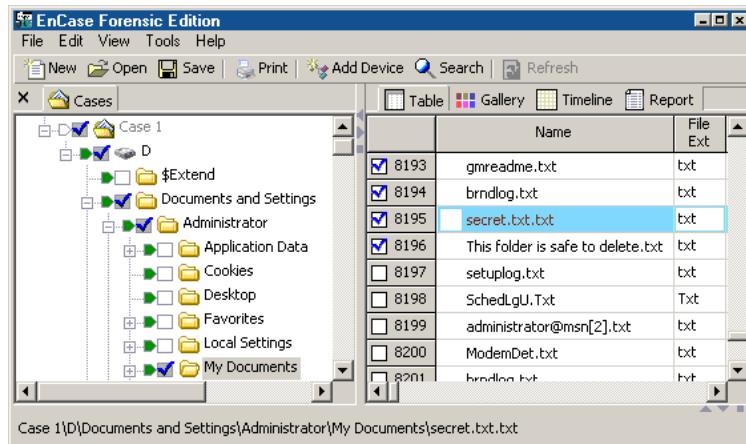


Figure 15-1 Selecting files and folders

Copying/UnErasing Files

To export a file from an evidence file in its native format, right-click on the desired file and select **Copy/UnErase...**. To copy out a group of files, blue-check the desired files, right-click one of the files and select **Copy/UnErase....**. You can specify whether to select only a single highlighted files, or all blue-checked files. When copying out multiple files, you can have these export as separate files or into a single concatenated file. Deleted files on a FAT volume have a hex \xE5 character at the beginning; EnCase allows you to replace this character with the character of choice (by default, this is an underscore (_))

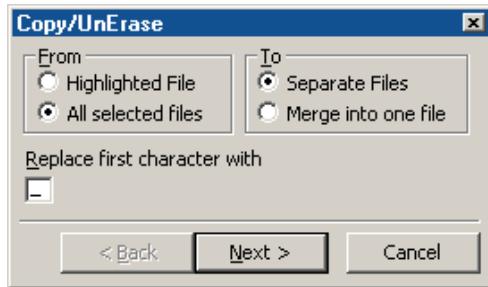


Figure 15-2 Copy/UnErase Options

After selecting the desired options, click [Next >] and select the radio button for the appropriate options as follows:

- **Logical File Only**
Copies out only the logical part of the file (file slack will not be copied).
- **Entire Physical File**
Copies out the entire file (logical file, as well as file slack).
- **RAM Slack Only**
RAM Slack, more accurately sector slack, is a buffer between the logical area and the start of the File Slack. This are is copied out when the radio button is selected.
- **None**
Accepting the default **Character Mask** value of **None** copies the file out exactly as it is seen.
- **Do not Write Non-ASCII Characters**
Selecting this radio button copies out all characters EXCEPT non-ASCII characters.
- **Replace Non-ASCII Characters with DOT**
This option replaces all non-ASCII characters copied out with dots.

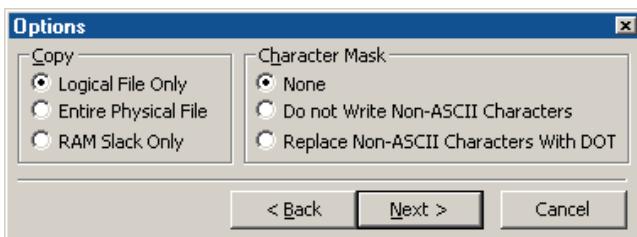


Figure 15-3 Copying options

Click [**Next >**] and choose a destination path in which to place the copied file(s). If multiple files are copied to a single file, the destination will be a file path. If separate files are being copied, the destination path will be a folder. You can accept the default, type in the path, or click on the ellipsis box on the right to browse to the desired location. By default, EnCase will split files over 640 MB in size; you can adjust this amount in the **Split files above (MB)** field. One useful purpose for this option is so that users can copy/unerase the entire Unallocated Cluster file and break it up into 640 MB chunks for burning to CD-R. Once the information is correct, press [**Finish**].

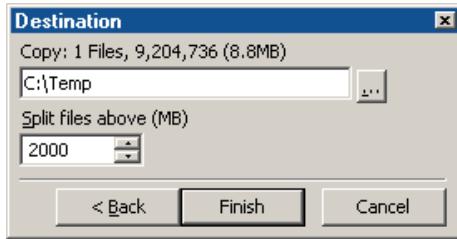


Figure 15-4 Copying options

When copying/unerasing a deleted file, EnCase will automatically unerase the file if possible.

Copying/UnErasing Bookmarks

It is possible to copy/unerase bookmarked files as well. The process is the same whether copying single or multiple bookmarks. Note that if the file has been deleted and resides in Unallocated Space, **Copy/UnErase** will try to copy out the entire Unallocated Space, since the data pertaining to the file resides within.

1. In **Cases** view, click on the Dixon box or the root folder to blue-check all files, and then click again to remove all blue checks.
2. Open the **Bookmarks** tab.
3. Blue-check the bookmarked file you wish to copy out. If you are copying multiple files, blue-check all files to be copied. To copy all files, or a range of files, you can blue check the first file in the range, hold down the [**Shift**] key and then click on the check box of the last file in the range. All bookmarks between the checked bookmarks will be checked.
4. Right click anywhere in the Table view and select **Tag Selected Files**.
5. Switch to the **Cases** tab. Notice that the files corresponding to the bookmarks you checked are now also all blue-checked.
6. Right click on one of the blue-checked files and select **Copy/Unerase**.

7. Make sure the radio buttons for **All selected files** and **Separate files** are selected and click [**Next >**]
8. Select the appropriate **Copy** and **Character Mask** options (typically **Logical File Only** and **None**) and click [**Next >**]
9. Set the appropriate path you wish to copy the files to and then click [**Finish**]

All tagged files (corresponding to the checked bookmarks) will be copied to the specified directory.

Copying Entire Folders

It is possible to copy out a folder and its' contents, including subfolders. To perform this task, do the following:

1. Click the **Cases** tab and blue check the folder in the tree in the left pane that you wish to copy.
2. Right click on the folder and select **Copy Folders....**
3. In the field below **Copy:**, enter the destination path.
4. If you wish to copy all the files to a single folder without hierarchical folder structure, place a check in the box labeled **Copy only selected files inside each folder**.
5. Click [**OK**].



Alert! If the **Copy Folders...** command is executed with an evidence file highlighted, the entire contents of the evidence file will be copied to the Storage hard drive!

Viewing Files Outside of EnCase

File Viewers

Frequently, an investigator will find file types that EnCase does not have the built-in capabilities to view (such as an MP3 or AVI file) or they might want to view a file type that EnCase does support with a third party tool or program. In either situation, it is necessary to set up a file viewer so that EnCase can associate the file type with the appropriate application.



NOTE: To view a file outside of EnCase, a viewer capable of opening and interpreting that file type is required. For example, QuickView Plus (a popular image viewer) will not open an MP3 file.

Setting up a File Viewer

1. From the **View** pull-down menu, select **File Viewers**.
2. Right-click on the root folder and select [**New**].

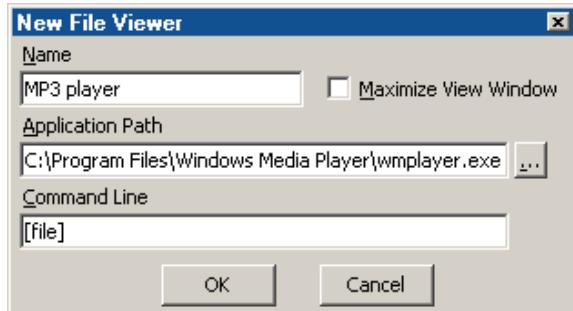


Figure 15-5 Setting up Windows Media Player as a Viewer

3. In the **New File Viewer** window, enter a **Name** for the viewer and the application's executable path. The **Command Line** field is utilized in the event the external application needs additional commands or switches invoked in order to function properly, but in general it will be left with the default value of **[file]**.
4. Click [**OK**].

File Types

At installation, EnCase has a considerable amount of file signatures matched to their appropriate applications to properly access the file. However, files are constantly encountered from new applications, with different extensions and new access methods. EnCase allows the user to add file extensions and match them to the correct viewer. To configure File Types in EnCase, do the following:

1. From the **View** pull-down menu, select **File Types**.
2. Right-click on the **File Types** root folder and select [**New**].
3. Enter a **Description** (type of file), **Extensions** (file extensions to associate), and select a **Viewer** to use. If you choose **EnCase**, it will be

opened within EnCase, but only if EnCase can view the file internally; selecting **Windows** uses the default viewer for the file type in Windows. If you have set up a Viewer in EnCase, you can select the **Installed Viewer >>** radio button and select the viewer from the window on the right. Non-native file viewers must be installed through EnCase prior to adding a new file type. When the options are complete, click [OK].

After the file type has been associated with a viewer, whenever a file of that extension is double-clicked, the file will automatically be copied/unerased to the Storage hard drive and opened with the associated viewer.

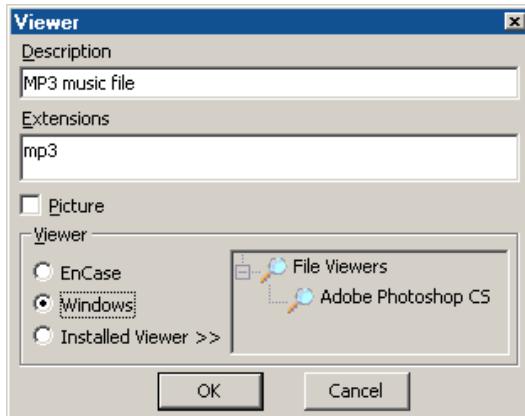


Figure 15-6 Associating a File Type with a Viewer

File Questions

- Q. Some deleted files have a ‘?’ as the first character and some do not. Why?**
- A. If a file has a long name (any non uppercase 8.3 name), DOS stores two sets of entries for the file. One entry contains the 8.3 short equivalent (usually with a ~ at the end) and the other set contains the long name. When a file is deleted, the first character of the 8.3 name is replaced with a hex E5 (set to ‘?’ to make it readable) but the first character of the long name is preserved. EnCase replaces the ‘?’ character in the short name entry with the first character of the long name if it exists.
- Q. When I copy an entire folder, do the deleted files get copied too?**

- A. Yes. You can circumvent this by selecting the entire folder, then de-selecting the files that should not be copied. Then check “Copy only selected files” in the Folder Copy dialog.

Q. Is it possible to recover a deleted file in its entirety?

- A. No. Deleted files may not be recoverable at all or only partially recoverable. It is possible that the only remnant of a deleted file is its directory entry. Sometimes some data may be recovered, but it is not necessarily the original contents of the file.

Q. How do I select all files in the Case?

- A. In the **Cases** tab, checking any folder checks all the files and folders contained within. To check all the files and folders in the case, blue-check the root **Case** folder at the top of the tree. Checking it again will deselect all folders and files.

To select a range of items in the table view, blue-check the first item, hold the [Shift] key down and check the last item.

To select multiple files in a folder, but *not* all of them, hold down the [Ctrl] key while clicking on each file.

Chapter 16

Keyword Searches

EnCase Version 4 features a new search engine that dramatically improves multiple-term keyword search times over previous versions of EnCase.

The search function of EnCase can locate information anywhere on the physical or logical media within current open cases. Keywords are saved globally in an initialization file within the EnCase directory. EnCase can search for each term byte-by-byte from the beginning to the end of every medium, and also search every logical file for the term. Keywords are accessed by selecting the **Keywords** option from the **View** pull-down menu.

Creating Keyword Groups

Keywords may be accessed by any open case, therefore, it is important to group keywords properly so that they can be located easily when needed. To do this, folders can be created and moved around within the **Keywords** tab.

To create a group, right-click where the folder is to be created, and select **New Folder**. To give that folder a specific name, hit the [Backspace] key after the folder is created until the name is blank, then type the name in. Alternately, once the folder is created, you can right click on the folder and choose **Rename**, or highlight the folder and hit [**F2**].

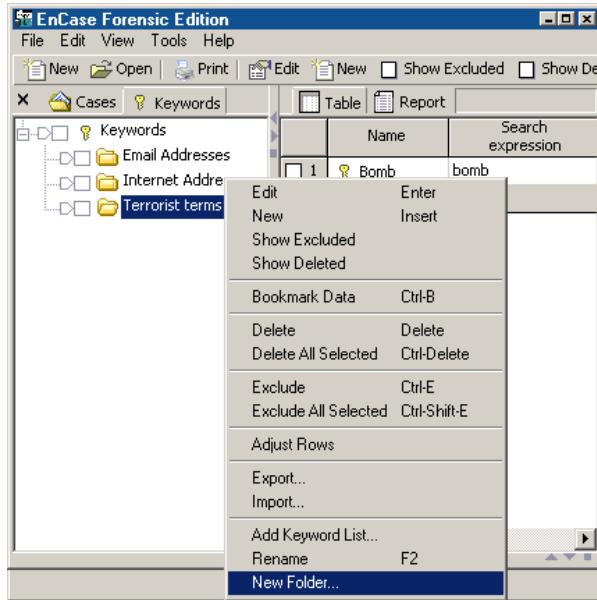


Figure 16-1 Creating a new Keyword folder

To delete a folder, right click on the folder and select **Delete** or press the **[Del]** hotkey; to move a folder, left click and hold on the number box associated with that folder in the right pane and then drag the folder to its new location.

Entering Keywords

Keywords can be added directly to a new folder, an existing folder, or to the root folder. To create a new keyword, right-click on the folder in which you wish to add a keyword and select **New** from the pop-up menu. The **New Keyword** dialog box will appear.

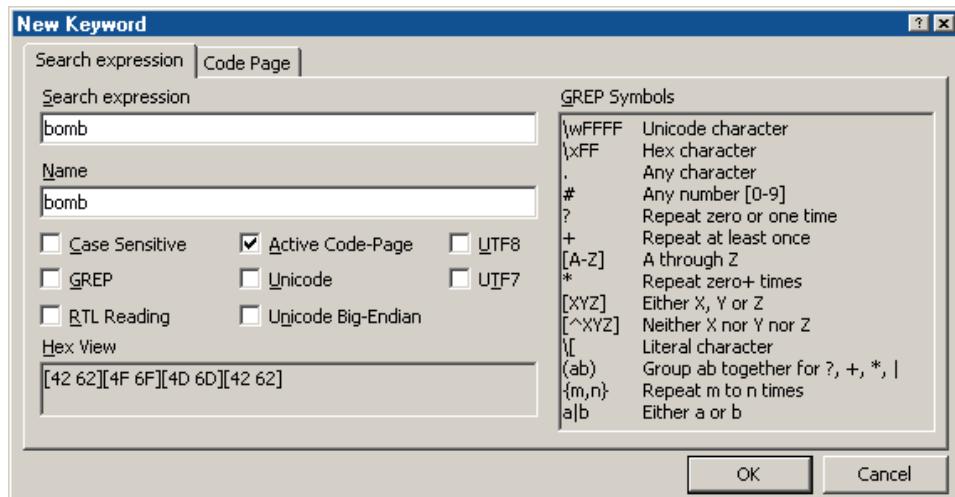


Figure 16-2 Keyword entry and options

Type the search string in the **Search expression** field and give the keyword a **Name** to identify it easily. Specify the parameters by checking the appropriate boxes for **Case Sensitive**, **GREP**, etc. The section below describes each option and its' function. Once you have entered the search parameters, click **[OK]**.



NOTE: When using a slash (\) in a keyword, it must be escaped with another backslash to get the literal "\". This behavior occurs only with the use of the backslash, since it is the escape character in GREP. The literal backslash requires an escape \\ whether or not you are using GREP.

Search Options

- **Case Sensitive**

With this box checked, EnCase will search for the specified keyword only in the exact case specified.

- **GREP**

This option uses the input symbols and text to search using the GREP (Globally search for the Regular Expression and Print) advanced searching syntax (see the GREP appendix for token syntax and examples).

- **RTL Reading**

The **RTL Reading** option will search for the keyword in a right-to-left sequence. If, for example, a user enters “Arabic keyword”, and specifies the keyword as **RTL Reading**, EnCase would show hits on that expression, flush-right, in the reverse sequence as “drowyek cibarA”.

- **Active Code-Page**

EnCase Version 4 has the ability to enter keywords in different languages. The **Active Code-Page** option must be checked to enter keywords in certain languages. English character searches use the “**Latin I**” code page.

- **Unicode**

The Unicode standard attempts to provide a unique encoding number for every character, regardless of platform, computer program, or language. Unicode uses 16-bits to represent each character, as opposed to ASCII (which uses 7-bits). Unicode on Intel-based PCs is referred to as Little Endian. The **Unicode** option will search for the keyword only in Unicode. For more details on Unicode, please see <http://www.unicode.org> and *Chapter 20: Foreign Language Support*.

- **Big-Endian Unicode**

Big-Endian Unicode uses the non-Intel PC data formatting scheme, in which the operating system addresses data by the most significant numbers first (the reverse of Little Endian).

- **UTF-8**

To meet the requirements of byte-oriented and ASCII-based systems, UTF-8 has been defined by the Unicode Standard. Each character is represented in UTF-8 as a sequence of up to 4 bytes, where the first byte indicates the number of bytes to follow in a multi-byte sequence, allowing for efficient string parsing. UTF-8 is commonly used in transmission via Internet protocols and in Web content.

- **UTF-7**

UTF-7 encodes the full BMP repertoire using only octets with the high-order bit clear (7 bit US-ASCII values, [US-ASCII]), and is thus deemed a mail-safe encoding. UTF-7 is mostly obsolete, to use when searching for older Internet content.

International Keywords

EnCase Version 4 can search for keywords with international language support. This allows the investigator to search, for example, for Arabic keywords using Arabic characters or Japanese keywords using Japanese characters. Keyword hits can be displayed in the desired language, as will the document in which the keyword was found.

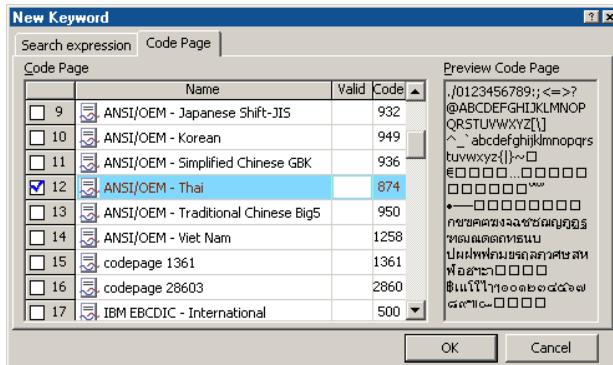


Figure 16-3 International keyword options



Figure 16-4 An Arabic text file displayed in Arabic, right to left

For languages other than English, see *Chapter 20: Foreign Language Support*.

Exporting/Importing Keywords

Keywords and keyword lists can be exported to, and imported from other EnCase users. By exporting and importing keywords, it is possible to share keyword lists with other investigators.

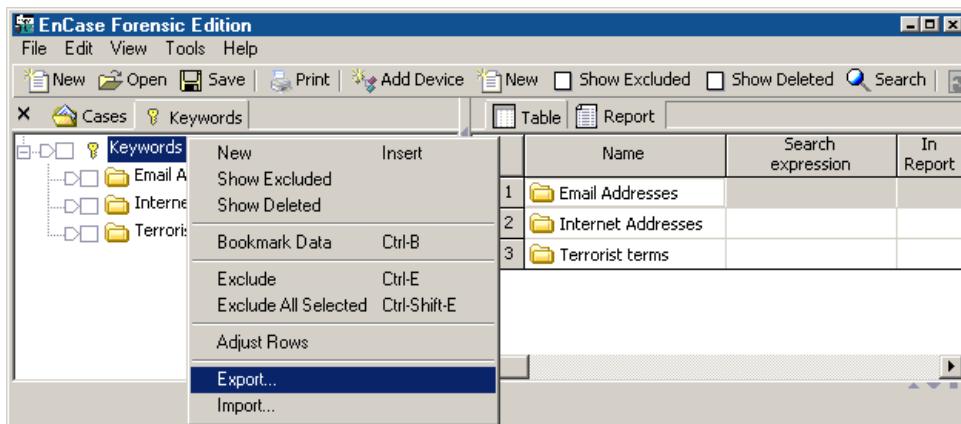


Figure 16-5 Export \ Import menu

Exporting Keywords

Keywords are exported in a TXT file format. You can export all keywords or export only blue-checked keywords. Keywords can be exported with their encoding information, including the following:

- Name**
- Filter**
- In Report**
- Search Expression**
- GREP**
- Case Sensitive**
- RTL Reading**
- Active Code-Page**
- Unicode**
- Unicode Big-Endian**
- UTF8**
- UTF7**
- Code Pages**

Placing a check box in front of each desired field exports it along with the keyword. Exported keywords can be manually added into the Keyword table; in order to export a keyword list for import, they must be exported by right clicking in the left pane and selecting the **Export** option. The **Export** options window will show **Export Tree (for Import)** checked, and any of the table columns that were blue checked on export from the table will be selected and grayed out. To export only the keywords in text format with specified fields, right click in the table and select **Export**. In this case, the **Export Tree (for Import)** option is unchecked and grayed out.

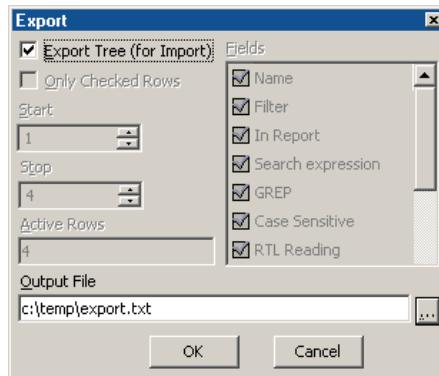


Figure 16-6 Exporting keyword list

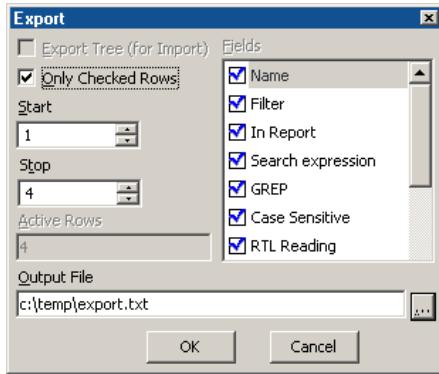


Figure 16-7 Exporting keywords

Exported keyword lists and exported keywords can be viewed by opening the .TXT file using WordPad or a similar text editor (the control codes may make the file unreadable in Notepad).

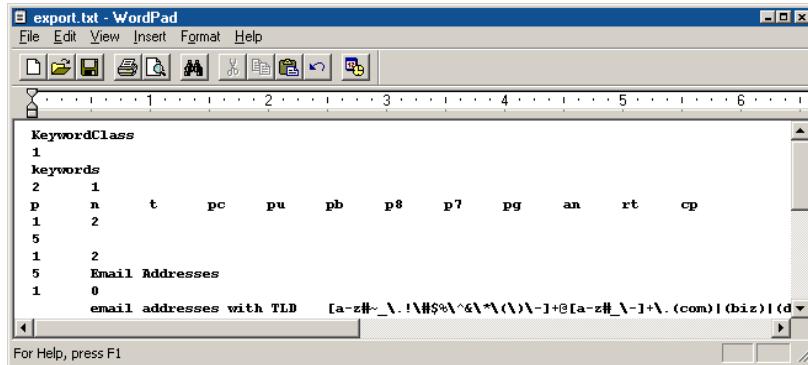


Figure 16-8 Viewing export.txt

Importing Keywords

Keywords are imported from a text file previously exported in EnCase. To import a keyword list into a particular folder, right click on the desired folder in the left pane and select **Import**. A subfolder, named **Keyword**, will be created and the folder structure from the imported keywords will appear beneath it.

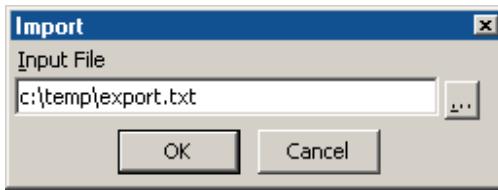


Figure 16-9 Importing exported keyword list (export.txt).

Adding Keyword Lists

To add keyword lists, right click in the right pane of the **Keywords** tab and select **Add Keyword List....** Keywords lists can either be typed directly into the **Keywords** field or they can be pasted from a keyword text document with one keyword and a line return per line. Select the appropriate keyword options (such as **GREP** or **Unicode**) by selecting the check box for that option, and click **[OK]**. The keywords will appear in the **Keywords** tab as separate entries.

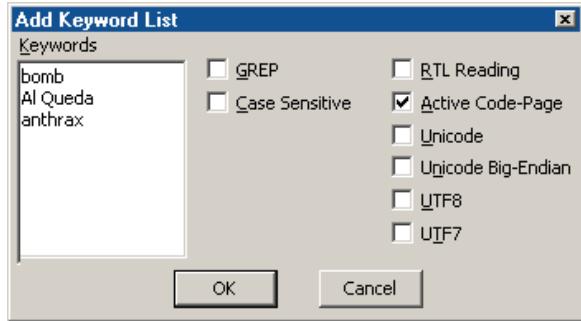


Figure 16-10 Adding keyword list

Keywords are stored globally in C:\Program Files\EnCase4\keywords.ini, unless EnCase was installed to a different location.

Starting a Search

To save time when beginning a search, decide whether to search an entire case, an entire device, or an individual file or folder. For example, when searching for information that may be in unallocated space, such as a file header, you can blue-check the Unallocated Clusters to avoid having to search the entire Case.

To begin a search, click on the  button on the toolbar. There are several options that can be selected when running a search. Each option may generate significantly different results when the search is run.

The following image shows each search option, followed by descriptions:

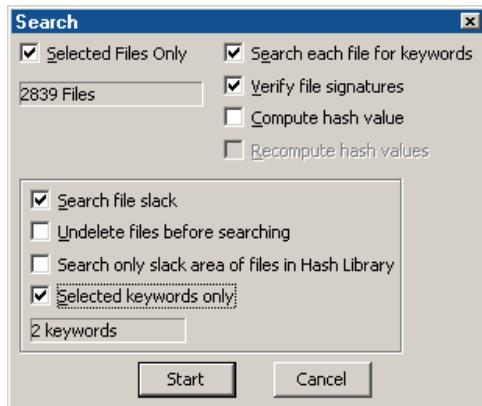


Figure 16-11 Search options

Search Options

- **Selected Files Only**

Unless specified otherwise, EnCase will search every byte of the case, regardless of how many and what types of devices are included. A search for **Selected Files Only** looks at only files, folders or devices that have been blue-checked. The Dixon box below the option shows the number of files to be searched.

- **Search each file for keywords**

To run a signature analysis or a hash analysis without running a keyword search, uncheck this box and make sure the desired option is checked.

- **Verify file signatures**

This option will conduct a signature analysis on files all files, or selected files with the **Selected Files Only** option enabled. Refer to the section on *Signature Analysis* for further information.

- **Compute hash value**

This option will conduct a hash analysis on files all files, or selected files with the **Selected Files Only** option enabled.. Refer to the *Hash Analysis* section for further information.

- **Recompute hash value**

If selected, EnCase will recompute all previously computed hash values generated for the files of the replaced live device. This is most often used for acquisitions over the enterprise network, to recompute the values of the files on the live machine if a hash analysis was conducted previously. This option is not necessary for local acquisitions.

- **Search file slack**

If selected, EnCase will search the slack area that exists between the end of the logical files and the end of their respective physical files.

- **Undelete files before searching**

If selected, this option will logically “undelete” deleted files prior to searching. If a file is deleted, EnCase and other tools can determine if the assigned starting cluster is not assigned to another file (if it is assigned, then the file is Deleted-overwritten). The unallocated clusters after the starting cluster may or may not belong to the deleted file. Choosing this option assumes the unallocated clusters after the starting cluster do belong to the deleted file. This is the same assumption made when copying out a deleted file. Choose this option will find a keyword fragmented between the starting cluster and the subsequent unallocated cluster. If determining

the presence of a keyword on the media is critical to an investigation, the examiner should also search for portions of the keyword, including GREP expressions of fragments of the keyword.

- **Search only slack area of files in Hash Library**

This option is used in conjunction with a hash analysis or on an evidence file that has already had a hash analysis performed. If a file is identified from the hash library, then it will *not* be searched. However, the slack area behind the file (as described above) will be searched. If this option is turned off, EnCase will ignore the hash analysis while running the search.

- **Selected keywords only**

This option allows the search to include all or just a selected number of keywords. The display box shows the number of keywords that will be used in the search. Keywords can be selected and deselected from the **Keywords** tab available under the **View** pull-down menu.

Click the **[Start]** button to begin the search.

Viewing Search Hits

As search hits accumulate, results can be viewed by selecting **Search Hits** from the **View** pull-down menu. Each keyword triggers the creation of a folder of the same name in which keyword matches are placed. Keyword folders are recognized by the **Key** (K) icon.

Many analysis functions can be performed in **Search Hits** view without having to change to **Cases** view. Search hits can be viewed while a search is still running by hitting the **[Refresh]** button on the top toolbar. Since EnCase is constantly updating the search hits window during the search, the table cannot be sorted until the search is complete.

In **Search Hits** view, you can select the [**View Search Hits**] button on the top toolbar, or right-click in the table and select **View Search Hits**, to change the way the search hits are displayed.

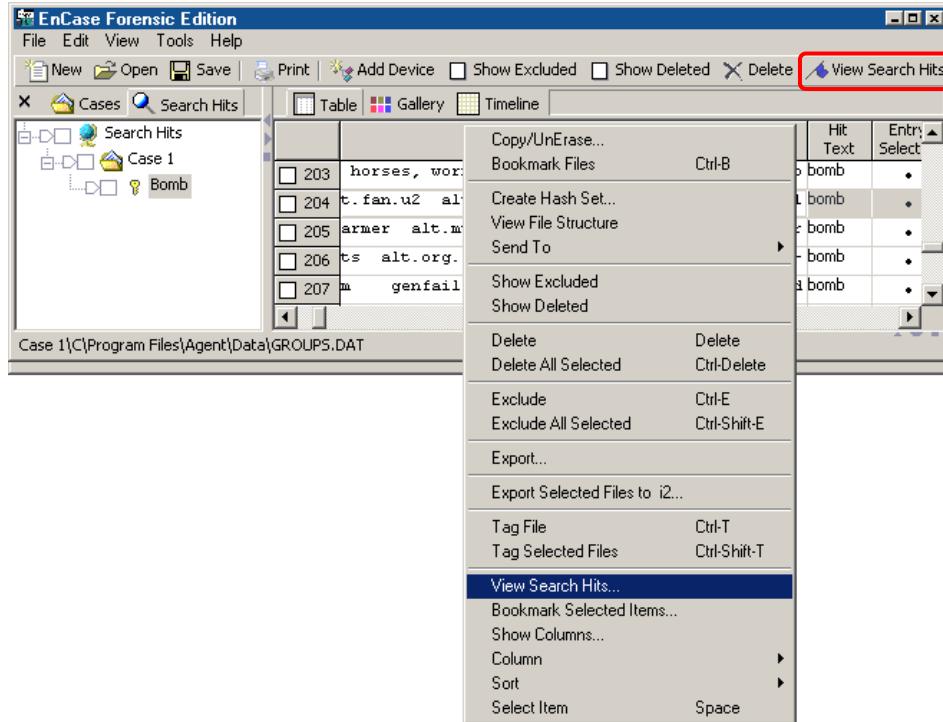


Figure 16-12 Viewing Search Hits

Search hits can be displayed and sorted by **Case**, **Keyword** and/or **Device**. Blue check the option to display by; the **Arrangement** can be changed by left clicking on desired the icon and dragging it into place.



Figure 16-13 Organizing the Search Hits table

In the example below, the search results have been sorted by Case, with devices listed below the Case, and the keyword hits displayed under each device that has keyword search hits.

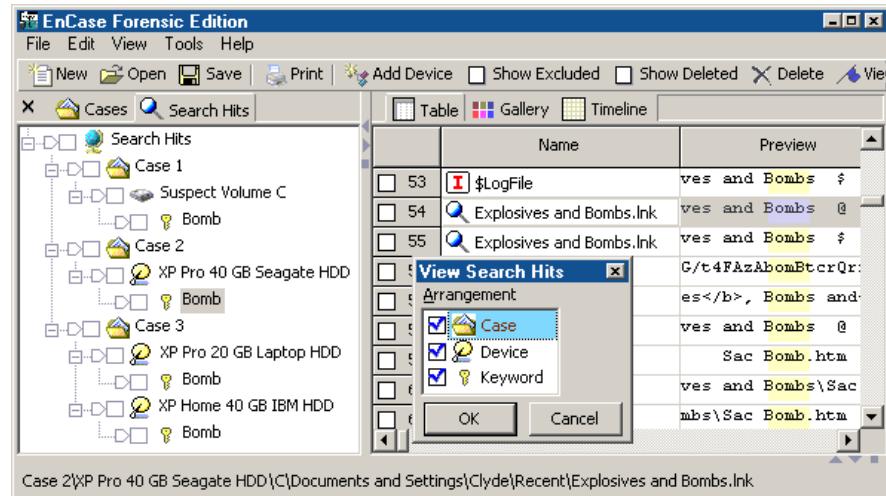


Figure 16-14 Keywords sorted by Case, Device then Keyword

Examiners can select search hits and perform a variety of tasks within **Search Hits** view. Right click in the table view to display the available options.

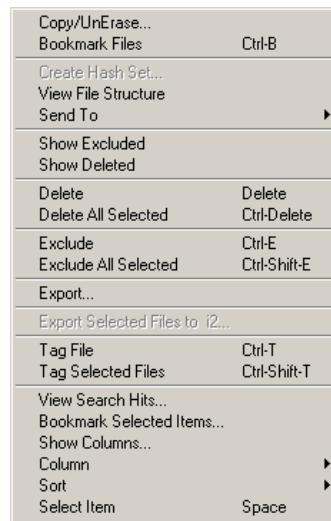


Figure 16-15 Search Hit options

- **Copy/Unerase**

This option will copy out of EnCase the file containing the selected keyword, with the option to also copy out other tagged or previously blue-checked files.

- **Bookmark Files**

This option allows for bookmarking of one or more files found in the search. Bookmarking options appear once this option is selected – see the *Bookmarking* sections later in this document for more information .

- **Create Hash Set**

By default, this option is grayed out unless Hash Analysis has been run through the **Search** feature. Refer to *Chapter 13* for more information on creating hash sets.

- **View File Structure**

This option mounts the compound file containing the selected keyword.

- **Send To**

This option allows the Examiner to send the file containing the search hit to a file viewer configured through EnCase.

- **Show Excluded**

This option (which also is featured on a button on the top toolbar) brings search hits that were previously excluded into view with the other search hits. By default, excluded search hits are displayed in red, although the color can be changed in the **Colors** tab of the **Options** window, opened through the **Tools** pull-down menu.

- **Show Deleted**

This option (which also is featured on a button on the top toolbar) brings deleted search hits into view with the other search hits. If a parent folder is deleted, the children search hits below are all deleted, although they do not display the deleted icon overlay. See **Delete** below for more details.

- **Delete**

This option deletes the currently selected search hit. To undelete a deleted search hit, show all deleted files, right click on the deleted search hit and select **Delete**. This is a soft delete, and the user can undelete the search hit until the case is closed. If a keyword is deleted when the case is closed, the search hit is permanently deleted. Note that **Delete** does not delete the file from the evidence file, only from the case.

- **Delete All Selected**

This option deletes all selected search hits.

- **Exclude**

This option excludes the search hit from view, although the hit is not deleted from the case file. This feature replaces the Recycle Bin of EnCase Version 3, although it is much superior in that it takes less resources from the examination computer and the search hits stays in the correct location, rather dumped into a central bin. To show the excluded search hit, see

Show Excluded. Excluded search hits are indicated by a red X icon overlay (X) and a red background on the search hit text in the table.

Excluding the root keyword excludes all children search hits, although the children search hits do not receive the “X” icon overlay. Individual search hits can be excluded to help focus on relevant hits, without permanently deleting the “false” hits.

- **Exclude All Selected**

This option excludes all selected search hits from view.

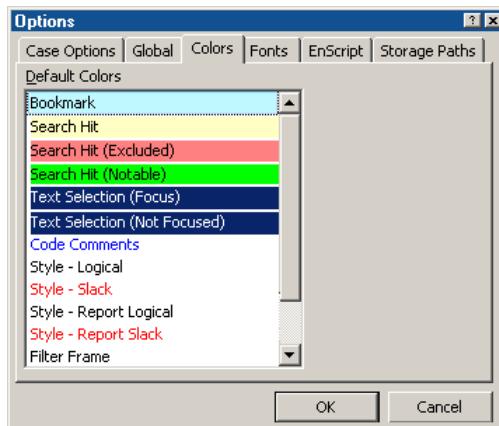


Figure 16-16 Excluded Search Hits default color

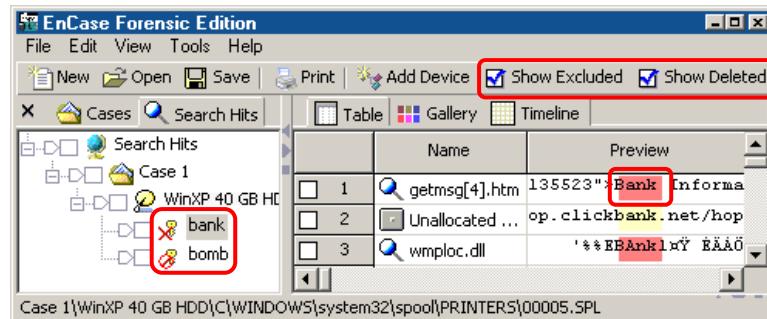


Figure 16-17 Deleted and Excluded search hits shown

- **Export**

This option allows the examiner to export out the data in the Table view into a tab-delimited text file, for import into Microsoft Excel or Access, or a similar program.

- **Export Selected Files to i2...**

Since version 4.16, EnCase has allowed for the export of blue checked (tagged) files into file formatted for examination using i2 software (<http://www.i2inc.com>). This option is grayed out if files are not blue checked.

- **Tag File**

This option will blue check the file in the Case view, in which the selected search hit is found. This allows the examiner to perform additional searches or run EnScripts just against those tagged files and the other previously blue checked files.

- **Tag Selected Files**

This option will blue-check selected files containing the search hits in Cases view.

- **View Search Hits...**

This option (also a top toolbar button) will display the **Arrangement** window to allow for the rearrangement of the search hits displayed.

- **Bookmark Selected Items...**

This option will open a window to allow bookmarking of selected search hits.

- **Show Columns..., Column, and Sort**

These options allow the examiner to move, hide, or lock columns in the Table view, and sort the data in columns in ascending or descending order.

- **Select Item**

This option will blue check the selected search hit. Holding down the space bar will continue to select search hits entries until the space bar is released. When the case file is saved, the setting for selected search hits will be saved in the case file.

Bookmarking Search Hits

Search hits are no longer bookmarked by default (as they were in Version 3). To bookmark a file containing a search hit, right click on the filename and select **Tag File**. From **Cases** view, you can then right click on the blue-checked file

and select **Bookmark Files**. You can also create a “sweeping text” bookmark of the search hit by selecting the appropriate text in the bottom pane, right clicking on the text and selecting **Bookmark Data**. Refer to the *Advanced Analysis* chapter for more information on creating bookmarks.

The Refresh Button

While a search is being run, although EnCase will report on the status bar in the lower right reports that it has found a number of search hits, they are not displayed when navigating to **Search Hits** view. This is because EnCase has not refreshed the display results. By pressing the [**Refresh**] button on the top toolbar, all search hits available at the time the button is pressed will be displayed in the table and the button will disappear. If additional search hits are discovered after the button is pressed, the button will reappear, to allow the table to be updated with the new search hits.

Cancelling a Search

To cancel a keyword search, double-click the blue status bar in the lower-right corner of the screen. Click [**Yes**] in the dialog box that appears to cancel the search.

*Copyright © 2004 Guidance Software, Inc.
May not be copied or reproduced without the written permission of Guidance Software, Inc.*

Chapter 17

Viewing Compound Files

A powerful feature of EnCase is the ability to view the individual components of compound files within an evidence file. Compound files are typically files that are comprised of multiple “layers” such as registry files, OLE files (such as Excel and Word), e-mail files (PST and DBX files) and compressed WinZip. To view (or *mount*) the structure of a compound file, right-click on the file in question and select **View File Structure**.

EnCase version 4.19 contains an EnScript (**File Mounter (v4)**) that will allow the examiner to select a file type (DBX, GZip, PST, Tar, Thumbs.db or Zip) and have them mount automatically (provided they have valid signature matches).

Registry Files

The Windows registry contains valuable data that provides a great deal of information about the setup of the Subject computer. Registry files of Windows 95, 98, ME, NT 4.0, 2000, and XP computers can be mounted within EnCase by right clicking on the file and selecting **View File Structure**.

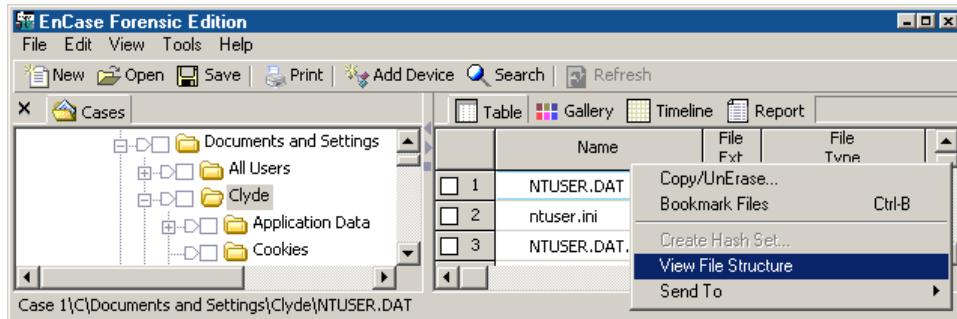


Figure 17-1 Mounting registry files

The registry file will be mounted in EnCase and can be navigated in the same fashion as other folder structures.

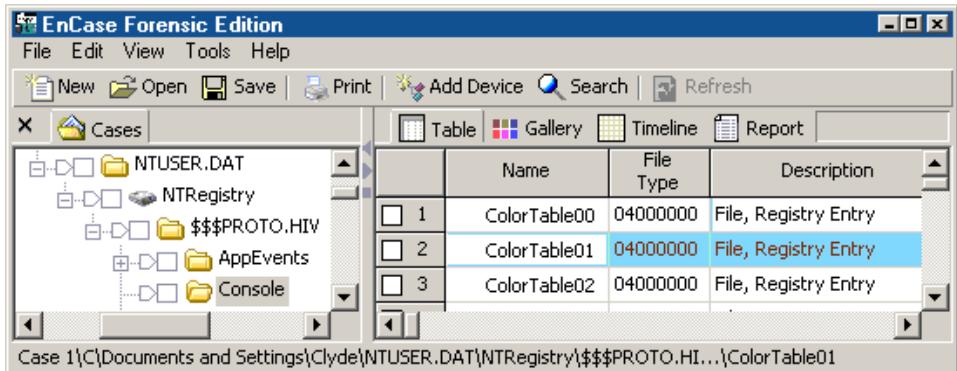


Figure 17-2 Viewing Registry File with EnCase

Windows 95, 98, and ME computers have two registry files. They are located in the system root folder, which is normally C:\Windows. The files are named **system.dat** and **user.dat**.

Windows NT 4.0, 2000, and XP divide the registry into four separate files. They are called **security**, **software**, **SAM**, and **system**. These files are stored in C:\%SYSTEMROOT%\system32\config\.

OLE Files

OLE is Microsoft's Object Linked Embedded technology on which Microsoft's Office Suite of products is based. For example, it allows an Excel spreadsheet to be seamlessly embedded into a Word document. Microsoft Office documents that use this technology are "layered" compound files, which can be viewed at the layer level by right clicking on the file and selecting **View File Structure**.

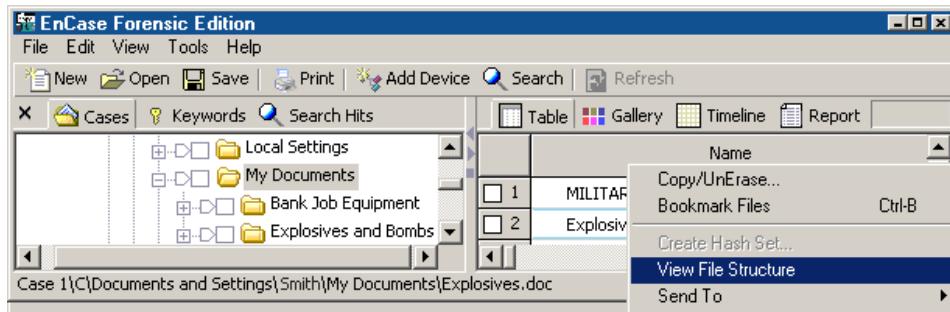


Figure 17-3 Mounting an OLE file

The file will be converted to a folder containing a file identified by an **OLE Volume** icon (). Clicking on the icon displays the layers in the table. Information about the document, such as the created date and time, the version of the application that created it, any plain text within the document, and other metadata, is available further into the OLE directory structure. The example shown in *Figure 17-4* demonstrates extracting the **Creation Date**. Highlight the data in Text tab of the bottom pane, right click and select **Bookmark Data**.

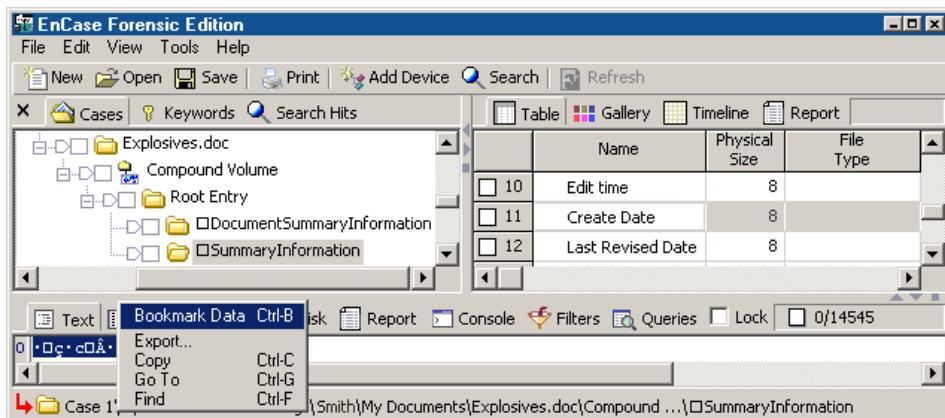


Figure 17-4 Extracting dates from an OLE file

In the **Bookmark Data** window that opens, select **Windows Date/Time** from the **Dates** folder in the **Data Type** window. The correct creation date should appear in the window at the bottom.

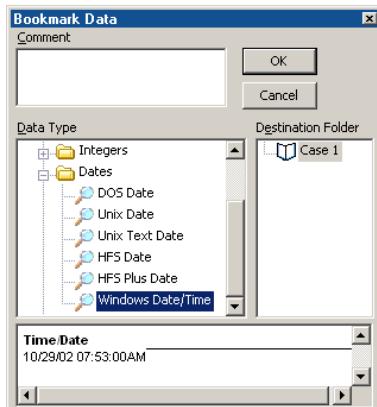


Figure 17-5 Extracting dates from an OLE file

Compressed Files

EnCase can mount compressed files in EnCase including WinZip (.zip) GZip (.gz) and Unix .tar files. To open a compressed file, right click on the file and select **View File Structure**. The contents are displayed as long as the container is not password-protected.

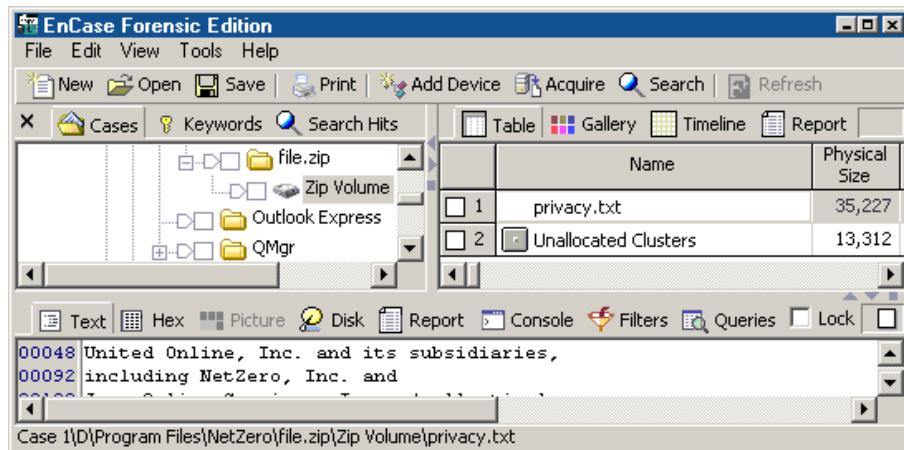


Figure 17-6 Mounting a WinZip file



NOTE: Only the modified date and times are shown on .gz and .tar files, as the compression processes do not store any other dates or times. GZip files are not labeled by name, only by their content file type and a .gz extension. For example, decompressing the file document.doc.gz displays the uncompressed document.doc file.

Outlook Express E-mail

EnCase can read Outlook Express .DBX files folders by right clicking on the file and selecting **View File Structure**. The .DBX file is converted to a folder with the mounted **DBX Volume** beneath. The table in the right pane lists the individual e-mails by their subject line. The text of the selected e-mails is displayed in the bottom pane **Text** tab.

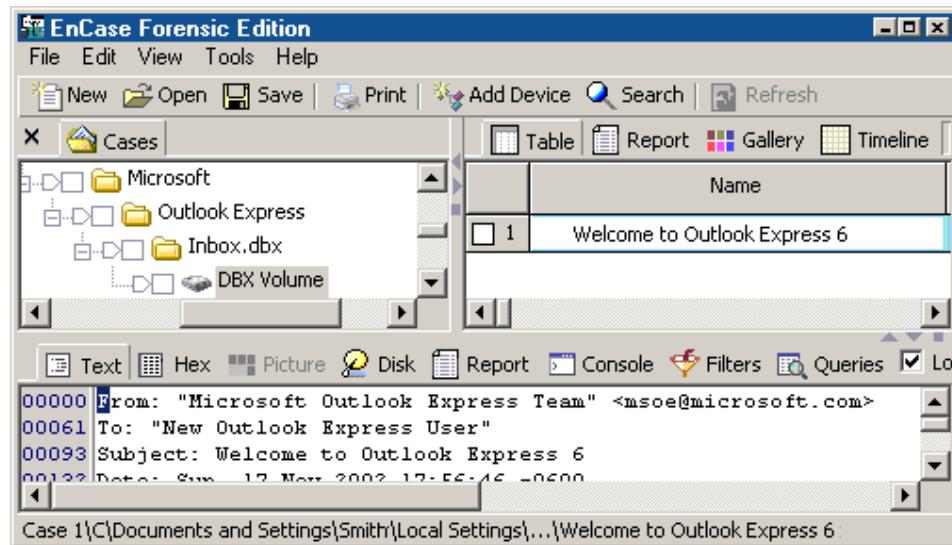


Figure 17-7 Viewing a Outlook Express .DBX file

Deleted e-mails and attachments can be retrieved from Unallocated Clusters. Files that have been deleted and overwritten may not be retrievable, although it may be possible to view some of the data that has not been written over in unallocated space.

Base64 and UUE Encoding

EnCase will automatically display Base64 and UUE encoded attachments when the mail file is mounted. You can search for (and view) Base64 images as follows:

1. In **Cases** view, blue check **Unallocated Clusters** in the table (normally located at the root of the volume).
2. From the **View** pull-down menu, select **Keywords**. In the table (right pane), right click and select New.
3. Enter **Base64** in the **Search expression** field, and then give the keyword a name. When you are finished, click [OK].
4. Blue check the new keyword in the table
5. Click on the [**Search**] button on the top toolbar. Check **Selected Files Only**, **Search each file for keywords** and **Selected keywords only** (leave all other boxes unchecked), and then click [**Start**]
6. From the **View** pull-down menu, select **Search Hits**.
7. With the bottom pane in **Text** view, highlight the first character of the image, right click and select **Bookmark Data**.

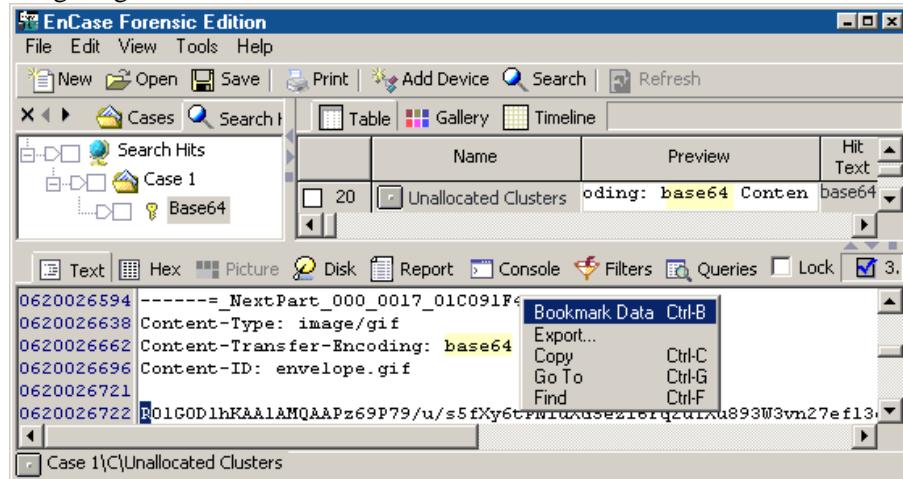


Figure 17-8 Bookmarking Base64 image

8. In the **Data Type** window, select **Base64 Encoded Picture** (inside the **Picture** folder); the image should appear in the bottom pane.

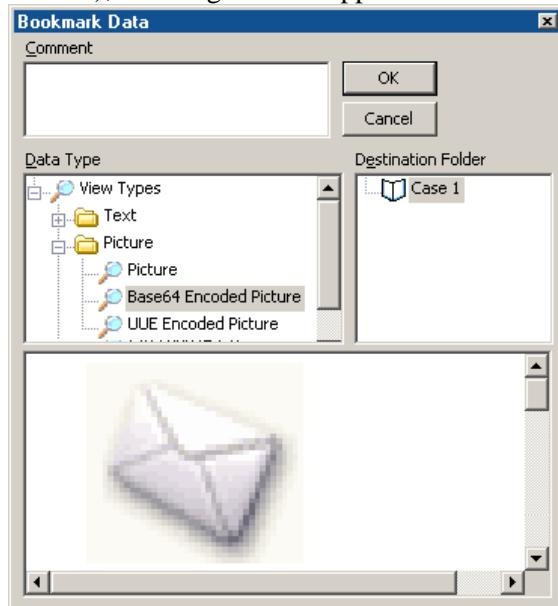


Figure 17-9 Bookmarking Base64 image

MS Outlook E-Mail

The process of mounting Outlook PST files is identical to that of Outlook Express as previously described. When EnCase mounts an Outlook PST file, messages are converted to RTF (Rich Text File) and ASCII text formatted files (`message.rtf` and `message.txt`, respectively). The RTF file can be opened in Microsoft Word; the .TXT file can be opened using a text editor such as Notepad. Foreign language messages can be displayed provided that the Microsoft Word Language Pack has been installed on the examiner's system.



NOTE: Since the .PST file (`message.rtf`) is not a plain text file, plain text searches against the file do not produce hits. The solution is to convert the `message.rtf` file to a virtual file named `message.txt` through Unicode translation. This enables plain text searches as well as searches for foreign terms in a .PST file that contains a foreign language.

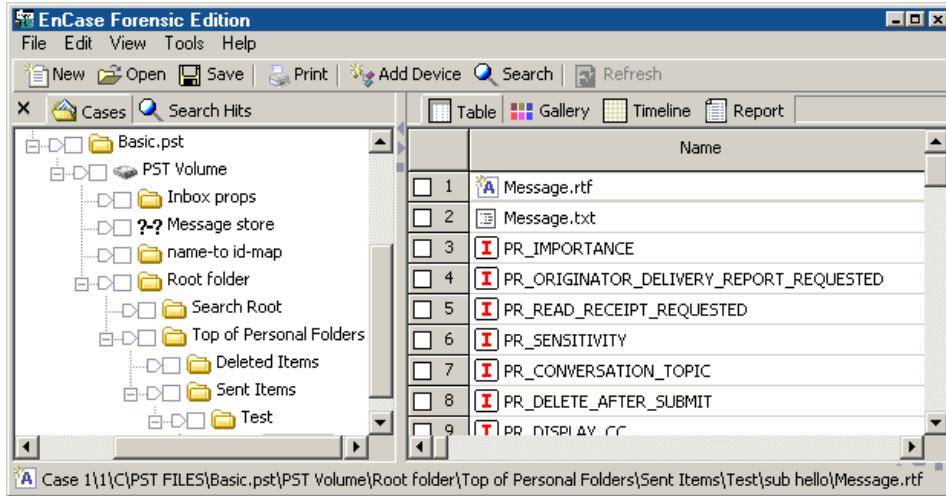


Figure 17-10 Mounted PST file

When expanded, the top level (or *top root*) of the .PST file directory contains multiple folders, including:

- **Inbox props** (properties)
- **Message store** (storage, containing the **PR_PST_PASSWORD** file and other IDs)
- **Name-to-id-map**
- **Root folder**, containing the following items:
 - **Search Root**: Reserved for future use
 - **Top of Personal Folders**, containing the **Inbox**, **Sent Items**, and **Deleted Items**

Each .PST e-mail message file appears as a folder with all the message properties within the folder as well as any attachments associated with the e-mail message.

NOTES:

- Many of the fields within the .PST mail folder are duplicated, which is part of the .PST format. If a keyword is a match within a certain field, it will be duplicated in the secondary field as well.
- Created, written and modified dates are set by the e-mail messages. Outlook calendar entries (created, written and modified dates) are set by the calendar applications, but they do not reflect the actual date and time of the appointments, but when they were entered.

NTFS Compressed Files

EnCase mounts, views and searches NTFS compressed files in a plain-text format by detecting when a file has been compressed and automatically decompressing the file for easy analysis.

Search compressed NTFS files and folders

The searching function within compressed files and folders has been greatly enhanced. The data within the files is displayed in the uncompressed format in the **Text** and **Hex** views of the bottom pane.

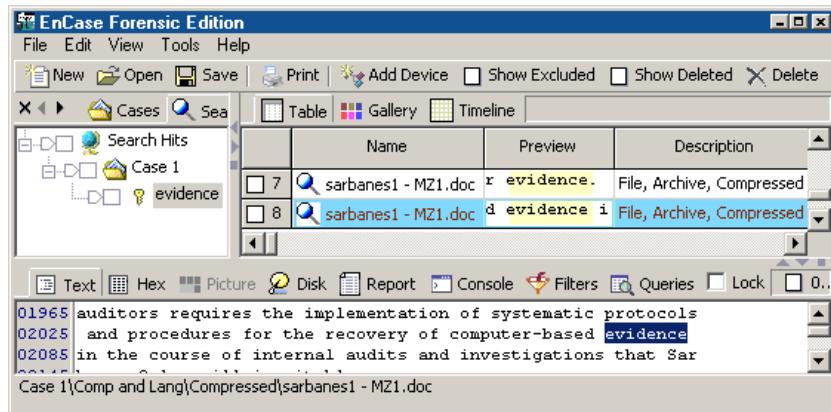


Figure 17-11 Uncompressed file with search hits

The examiner can view the uncompressed data of the file in the Disk view.

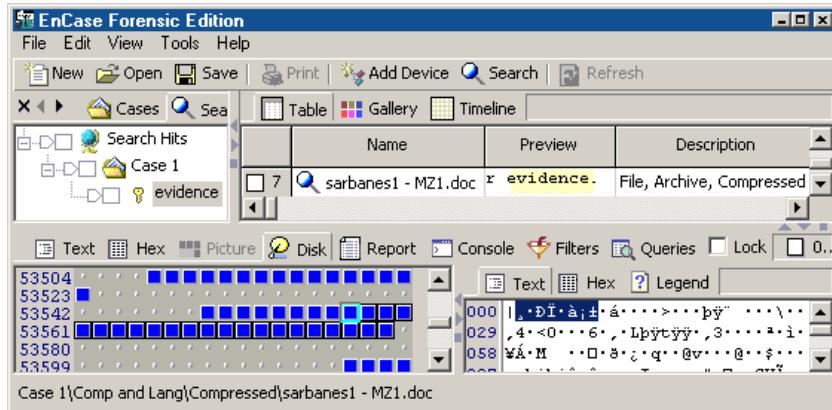


Figure 17-12 Uncompressed file with search hits

Thumbs.db

EnCase 4.17 and above has support for parsing Windows' thumbs.db cache for images, web pages, and other files. To mount the thumbs.db file, right click and choose **View File Structure**. The Thumbnail Cache Volume will be displayed, along with the version number. V2 thumbnails are in a bitmap format, whereas later versions are in a modified .JPG format. The Root Entry folder will contain the Catalog file of the cached thumbnails' names and their full path, and the cached images themselves. Thumbs.db also contains a record of the **Last Written** date of the images.

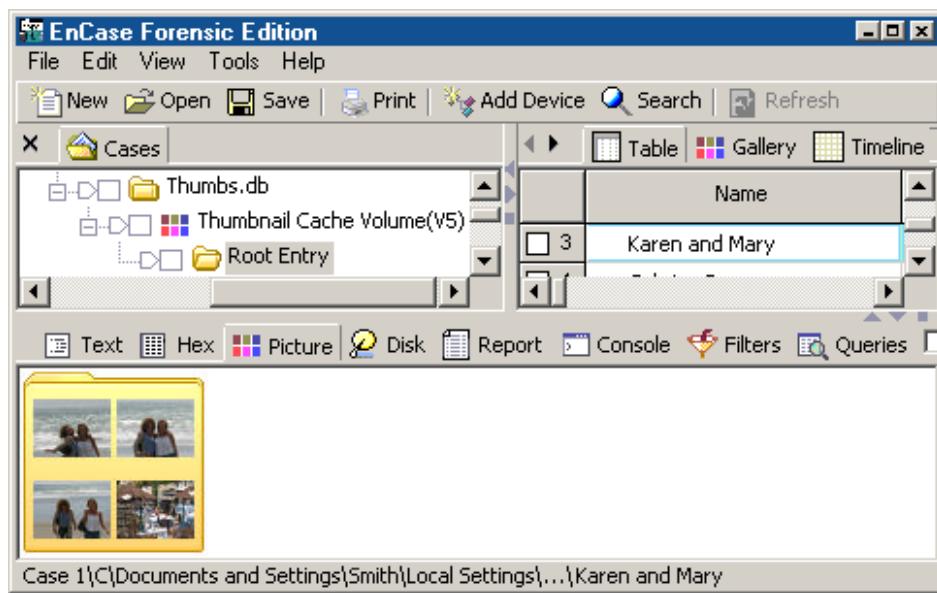


Figure 17-13 Cached thumbnails

Chapter 18

EnScript and Filters

EnScript is a programming language and Application Program Interface (API) that has been designed to operate within the EnCase environment. Although compatible with the ANSI C++ and Java standard for expression evaluation and operator meanings, EnCase contains only a small subset of C++ features. In other words, EnScript uses the same operators and general syntax as C++, though classes and functions are different. EnScript allows investigators / programmers to develop utilities to automate and/or facilitate forensic investigations. EnScripts can also be compiled and shared with other investigators. A programming background and an understanding of object-oriented programming are helpful to code in EnScript. The latest information is available at <http://www.guidancesoftware/support/enscript/index.com>.

To access the EnScript interface, select **Scripts** from the **View** pull-down menu. You can select EnScripts in the left pane by double-clicking on them, allowing you to view or edit the source code in the right pane. To run an EnScript, click the **[F9]** key or the **[Run]** button on the top tool bar with the EnScript selected on the left.

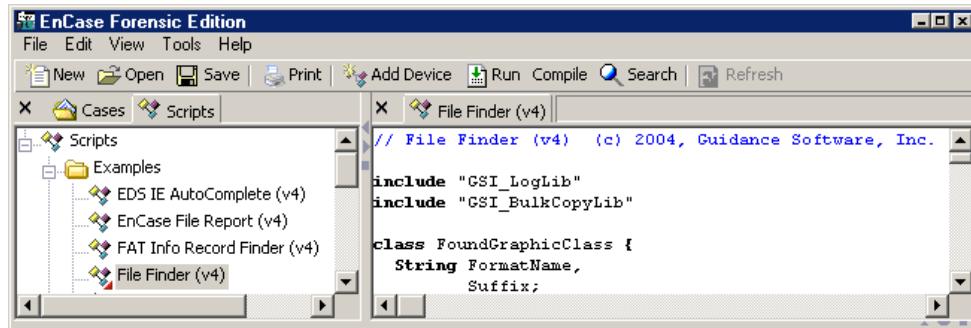


Figure 18-1 The Scripts tab

EnScript Path

EnScripts are included with Version 4 and stored in `C:\Program Files\EnCase4\Scripts\Examples`. To modify the path to find the scripts from a different location:

1. Right-click on the root folder or one of the scripts in the left pane and select **Change Root Path....**

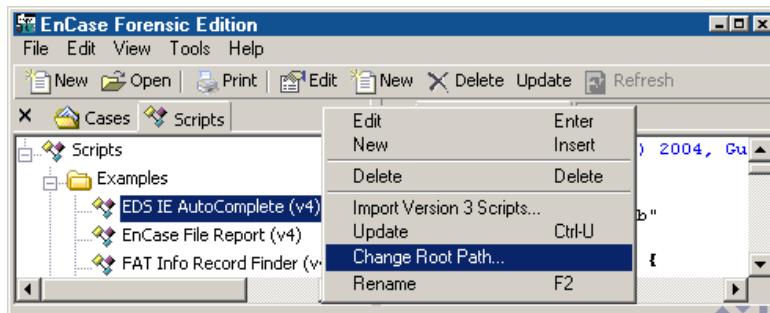


Figure 18-2 Changing the root path

2. Browse to the correct folder for the EnScripts and click [OK].

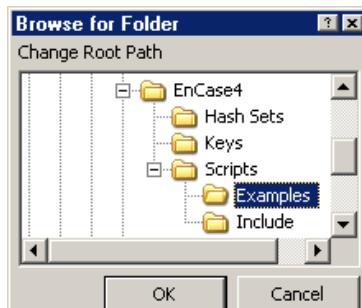


Figure 18-3 Setting the root path

Include Folder

Different scripts may have common functionality. Rather than have two scripts duplicate the same code, they often share code from a single file. By default, the common code is placed in C:\Program Files\EnCase4\Scripts\Include.

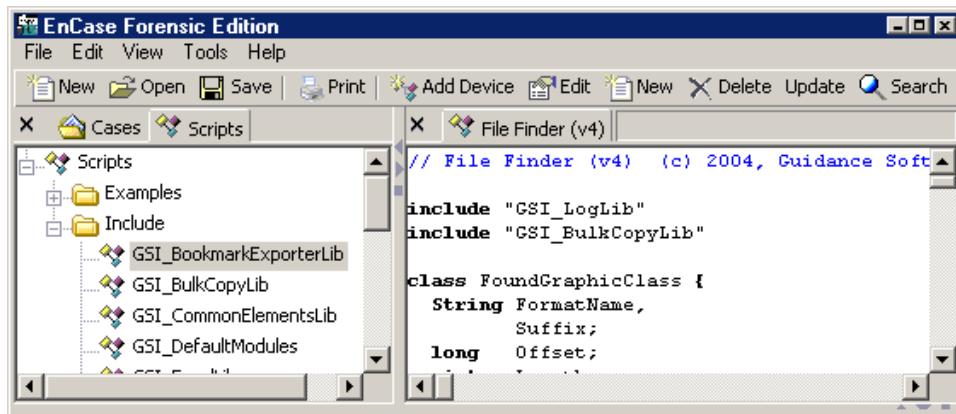


Figure 18-4 Common scripts

These scripts cannot be run like the ones in the **Examples** folder; they are only used for writing other scripts. If you move the **Include** folder, you will need to update the path by clicking on the **EnScript** tab after selecting **Options** from the **Tools** pull-down menu. Type the path, relative to the EnScript root path, in the **Include Path** field at the bottom. When writing scripts, you should put included files in the same folder as the main script or in a subfolder, since each

time you upgrade EnCase, the EnCase installer will overwrite any custom scripts stored in the **Examples** or **Include** folder.

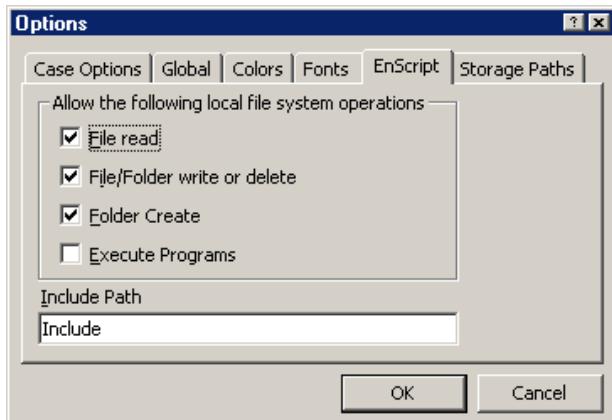


Figure 18-5 Changing Include path

Working with EnScripts

EnScripts can be viewed and edited by double-clicking on the desired EnScript . The [**Compile**] button (next to the [**Run**] button on the top toolbar) permits investigators to compile EnScripts so that the code can be checked without executing the EnScript. The [**Run**] button executes the EnScript.

To close an EnScript, highlight the script in the left pane and click on the [X] in the upper left of the right pane, or right click on the tab with the EnScript name in the right pane and select **Close**.

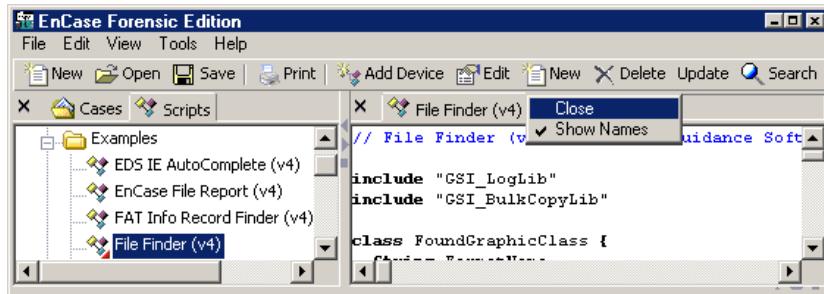


Figure 18-6 Closing an EnScript

To move or copy an EnScript to another (or the same) folder, hold the right mouse button down on the script, drag and drop it to the desired folder, then let go of the mouse button. You can then select **Move Here** or **Copy Here**. If the EnScript is being copied to the folder in which it already resides, it will be created with a number after the name (e.g., File Finder (v4)1).

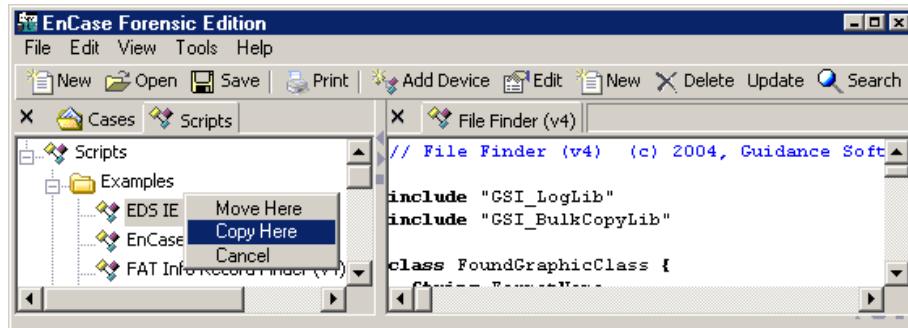


Figure 18-7 Moving or Copying an EnScript

Console

The **Console** tab displays the results of EnScripts that send output to the console (C:\Program Files\EnCase4\console.txt) upon execution.

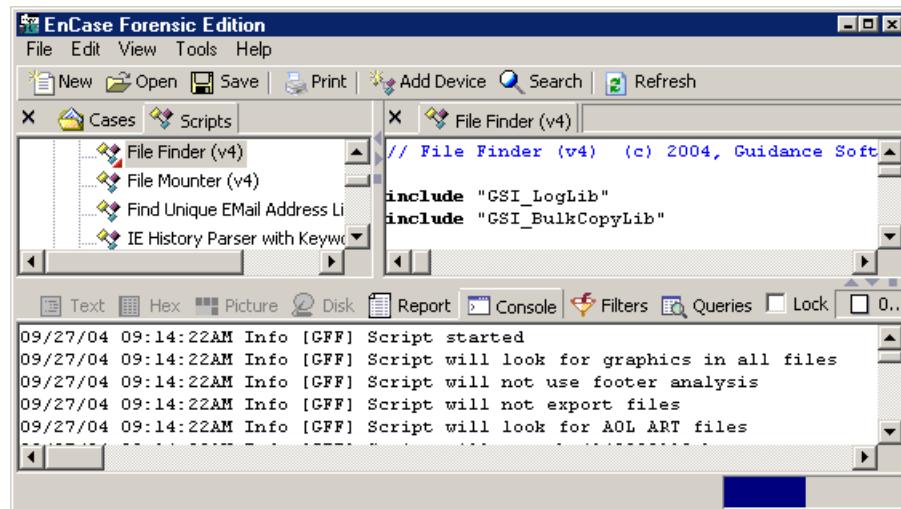


Figure 18-8 Viewing results in the console

The EnScript Library

To keep the EnScript library current, download the latest updates from <http://www.guidancesoftware.com/support/enscript/filters.asp>. Only EnScripts created by Guidance Software are available from this site. There is also useful information concerning EnScripts at the Guidance Software's EnScript Forum message board.



Warning! EnScript macros are executable files and should be treated with the same caution as any other executable file received from a third party. Like other executable files, it is possible to intentionally write EnScripts with malicious code or to imbed viruses within the code of an EnScript. It is imperative that you only obtain "free" EnScripts directly from Guidance Software or from a clearly identified source that you trust. EnScripts received from third parties should be screened for viruses. Guidance Software disclaims any representations, warranties, express or implied, regarding EnScripts provided on site including their fitness for a particular purpose, their quality, their merchantability, or their non-infringement. Guidance Software does not warrant that any EnScripts posted on this site are free from bugs, errors, or other program limitations. By utilizing any EnScripts provided on this site, you agree that Guidance Software will not be subject to liability for any bugs or damages caused by EnScript macros, including EnScripts intentionally written by third parties with malicious code and/or computer viruses.

For full details on EnScript, please see *Appendix C, EnScript*.

Filters

The Filters tab in the lower pane allows investigators to add new filters, edit existing ones, or delete them. Additionally, filters can be combined into queries, built under the adjacent **Queries** tab.

Filters determine the amount of information displayed in all areas of the EnCase interface except **EnScripts**. They are similar to EnScripts in that they use the EnScript syntax, though typically filters are much shorter. All filters are stored in an initialization file in the root directory where the EnCase executable file resides (C:\Program Files\EnCase4\filters.ini). This means that filters are saved globally within EnCase. To ensure that all copies of EnCase within a test environment have the same filters, copy filters.ini to all computers with EnCase installed. Any changes or additions to filters within EnCase automatically update filters.ini.

Accessing Filters

The Filters tab in the lower pane may be opened and edited even when EnCase does not have a case open. The filters that appear in the window are determined by which view is open at the top.

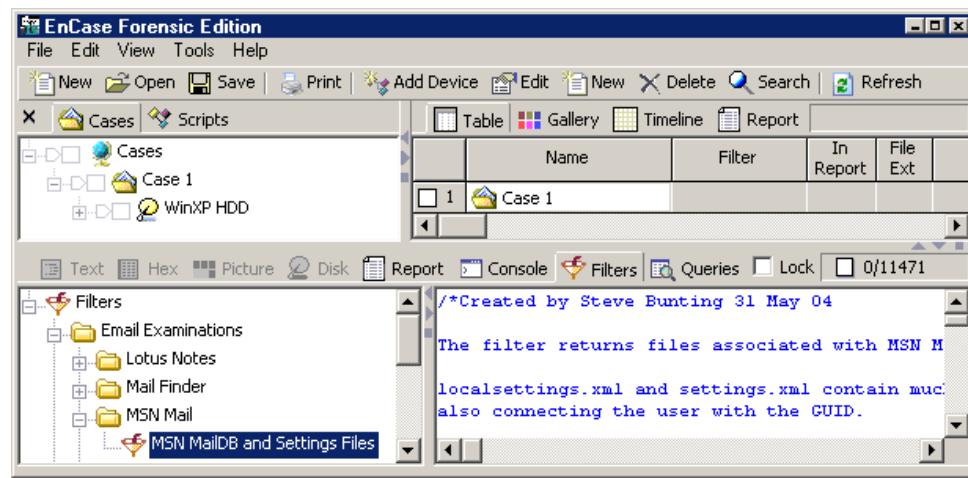


Figure 18-9 Filters tab

Filters are a way to limit the information that is shown within EnCase. For instance, an investigator may wish to view only files whose hash category is **Notable**. A filter may be written to show only those files.

Starting and Stopping Filters

To activate and run a filter, double-click on it in the bottom pane. Filters can also be run by right clicking on the filter and selecting **Run**. When a filter is activated, it becomes a query (consisting solely of that filter) under the **Queries** tab. It is, in fact, the query that is activated, not the filter. The activated query's icon and name will be displayed next to the **Report** tab in the right pane. To stop a query, click the [**Stop Query**] button on the top tool bar, or switch to the **Queries** tab at the bottom, right click on the query, and select **Stop**.

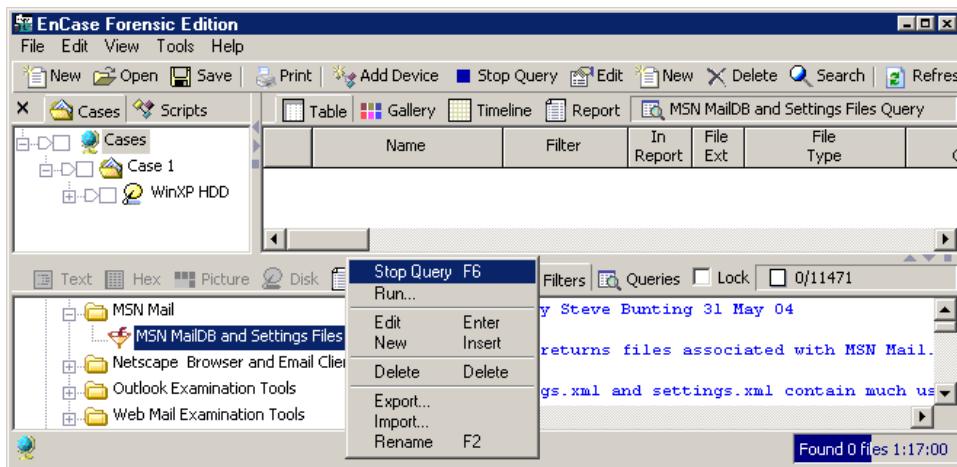


Figure 18-10 Running and stopping a query

Creating a Filter

A new filter can be created by right clicking in the bottom left pane and selecting **New**. Name the filter and edit it in the right pane. Syntax for EnScript and Filters is covered in the EnScript appendix.

Queries

Whenever a filter is run, as mentioned above, a query with that filter's name is created and activated. Filters can be combined together to create complex queries using OR logic or AND logic.

There are two tabs beneath the **Queries** tab: a **View** tab and an **Include** tab.

The View tab

The **View** tab lists the filters available as queries.

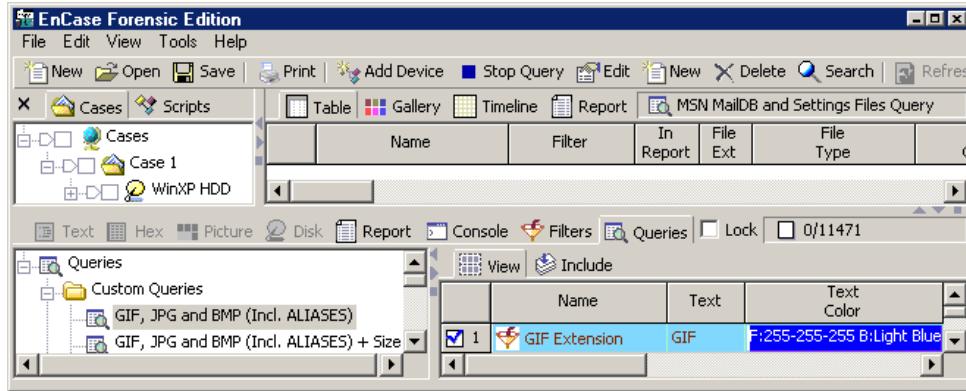


Figure 18-11 Queries View tab

In the left pane, queries can be run, edited, added, renamed, and deleted as follows:

- To run a query, right click on it and select **Run....**
- To add a new filter (as a query), right-click on the **Queries** root and select **New**.
- To edit an query, right click on it and select **Edit**.
- To delete a query, right click on the it and select **Delete**.
- To rename a query, right click on it and select **Rename**.

In the right pane, it is possible to create a new query, edit an existing query, and delete queries. Text in the Filter column can be changed, as well as the color of the query text, the foreground color, the background color, the foreground color of the query frame, and the background color of the query frame.

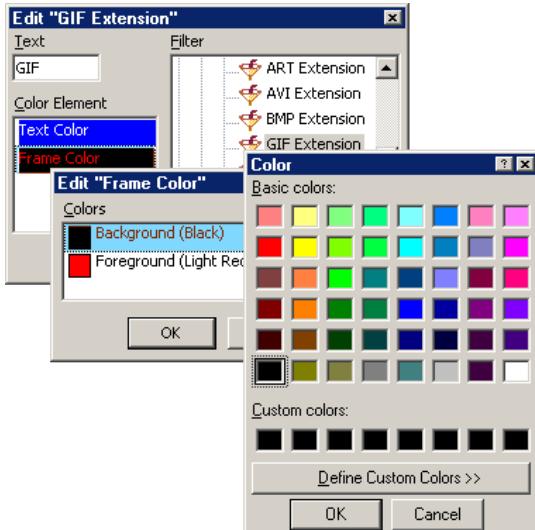


Figure 18-12 Changing filter properties

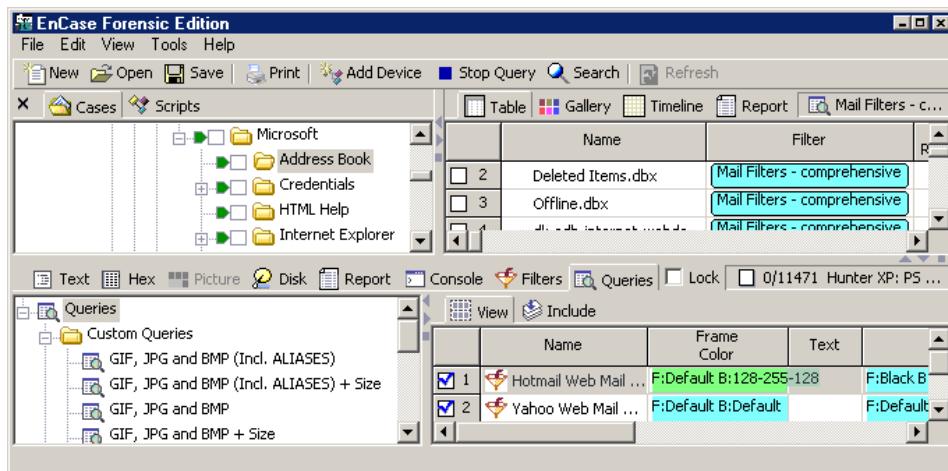


Figure 18-13 Query results by changed properties

To create a new query, right click and choose **New**; to delete a query display, right click and choose **Delete**.

The Include Tab

The Include Tab builds the complex queries from simpler ones, as well as dictating what logic is used to display query results. If the OR logic is selected (*filter1 / filter2*), the results returned will be those that match *any* of the selected filter. If the AND logic is selected (*filter1 & filter2*), the results returned will be those that match *all* of the selected filters.

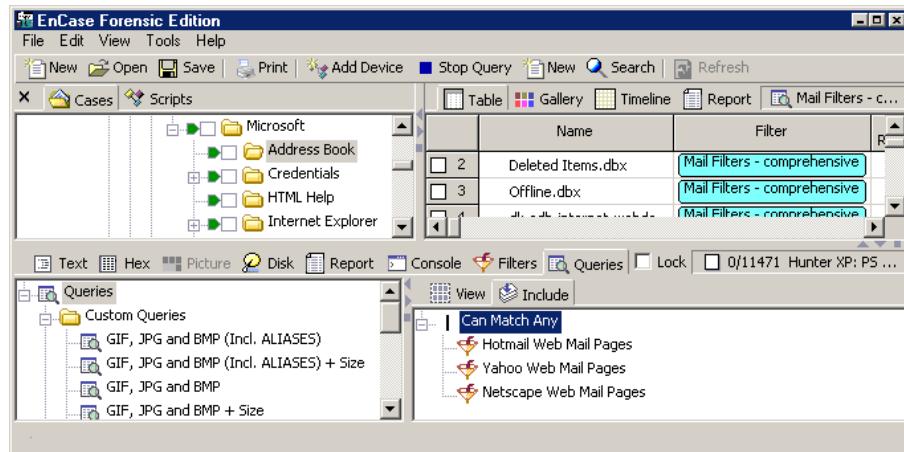


Figure 18-14 Queries include tab

Folders can be created within queries and filters placed into those folders with their own logic (the equivalent of parentheses in a statement). Query options in the **Include** tab are as follows:

- To add a filter, right click and select **New**.
- To add a folder, right click and select **New Folder....**
- To change the logic (e.g., from **AND** to **OR**) , right click and select **Change Logic....**

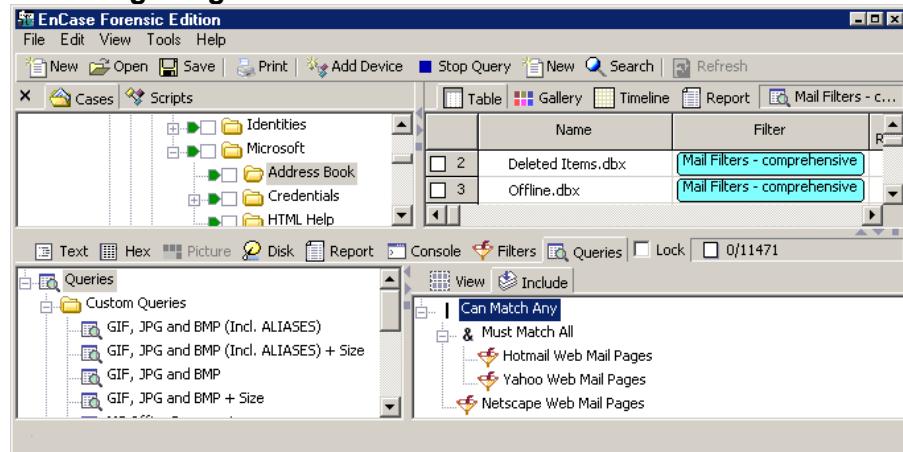


Figure 18-15 Query with AND folder

Filters can be dragged from one folder to another to achieve exactly the logic desired by the investigator.

Chapter 19

Advanced Analysis

Recovering Partitions

Occasionally a device has been formatted or even FDISKed in an attempt to destroy evidence. Formatting and FDISKing a hard drive does not actually delete data. Formatting deletes the structure indicating where the folders and files are on the disk. FDISKing a drive deletes a drive's partition information. EnCase can rebuild both partition information and directory and folder structure.

Adding Partitions

A formatted and/or FDISKed hard drive should be acquired using normal procedures. Add the evidence file to a new case within EnCase.

- A formatted drive will display logical volumes within EnCase, but each volume will have only an **Unallocated Clusters** entry in the table.
- An FDISKed drive will not show logical volume information. The entire drive will be displayed as **Unused Disk Area** in the table

Restructure these portions of the disk as follows:

1. Highlight the first **Unused Disk Space** in the table while in **Cases** view.
2. Click on the **Disk** tab in the bottom pane.

3. In the **Disk** view pane, confirm that the selected sector is correct by examining the *last* two hex characters of the sector. Scroll to the bottom of the sector in the Hex view window to the right; the last two characters should read "55 AA".
4. Count 63 sectors to the *right* of that first sector, and locate a sector, which displays (in right text pane) MSWIN4.1 for FAT32 or NTFS for NTFS.

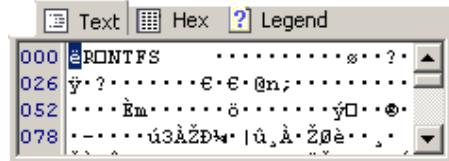


Figure 19-1 NTFS partition

5. In that sector, right click and select **Add Partition**.
6. Click [**OK**] to restore the partition.
7. If the drive had multiple partitions, go to the **Cases** tab, select the next **Unused Disk Space** icon, return to the **Disk** view window and repeat the above process, counting 63 sectors to the right of the target sector. Locate the MSWIN4.1 or NTFS text and add another partition.

Deleting Partitions

To delete a partition (if, for example, a partition was created at the wrong sector), the entry must be deleted at the sector at which it was created on the evidence file image of the hard drive. Delete the partition as follows:

8. In **Disk** view, navigate to the **Volume Boot** record entry (indicated by a pink block).
9. Right click and select **Delete Partition...**
10. Click [**Yes**] to confirm the removal of the partition.
11. Return to the **Cases** tab. The partition will be replaced in the table by **Unused Disk Space**.

Recovering Folders from a formatted drive

If the evidence file shows a logical volume but has no directory structure, the hard drive has probably been formatted. If this is a FAT-based system, EnCase can recover the original directory structure. Right-click on each logical volume and choose **Recover Folders**. This will search through the drive and recover folders, subfolders and files from within those folders if all that information is still available.

Web Browsing History

Often it is possible to recreate web pages that the Subject visited on the web.



Warning! It is a good idea to disconnect the lab computer from the internet to avoid inadvertently downloading images and overwriting any content extracted from the evidence file.

To see the HTML pages still stored on the Subject's hard drive:

- From the **View** pull-down menu, select **Cases**.
- Sort the table by **File Ext**.
- Click in the File Ext column and type "HTM".
- Double-click an HTM or HTML file. The file will be copied to the storage hard drive and opened with the default browser. In most instances, the browser will display a page with the HTML text intact, and the images replaced by white boxes with a red X.

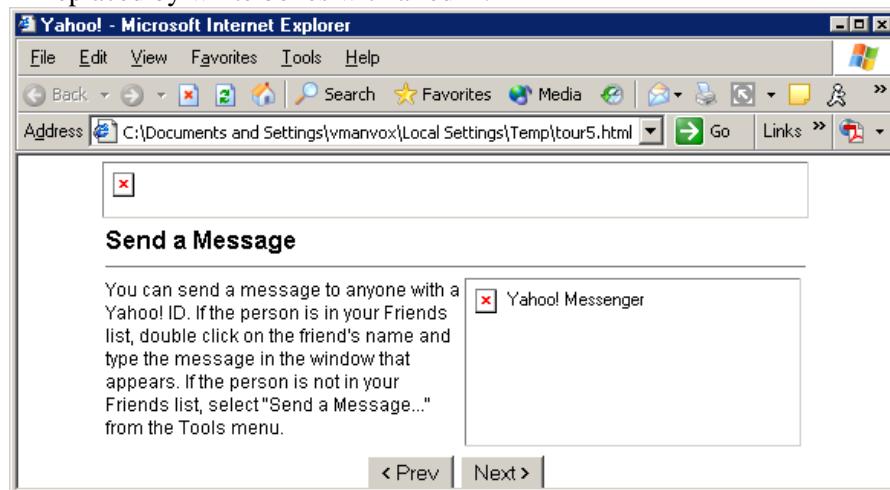


Figure 19-2 HTML document with missing images

Although the web page is open and being viewed from the investigating computer, the graphics for the web page are not yet available. To locate and match the missing images, the name of the file must be located.

- Right click on a white box and select **Properties**. Note the file name and file path.



Figure 19-3 Properties of a missing web image

- In **Cases** view, find the image specified in the table. You can subsort by **Name** to make it easier to locate.
- Right click on the image and select **Copy/UnErase...**, saving it to the local drive. Unless specified, EnCase will copy the file to the Default Export folder. To see the web page as it was originally laid out with the images, *the directory structure used to create the web page must be recreated*. Once the directory structure has been recreated, and the images moved to the appropriate directory, the web page is displayed as the subject originally saw it.

Another method to track visited sites is to run the **IE History Parser with Keyword Search** (v4) EnScript. The script will extract every web page that the Subject visited that is still stored on the subject drive. Run the script, selecting the folder to store the Internet History files. The script will output a clean layout of every web page that the subject visited that is still available via the cache.

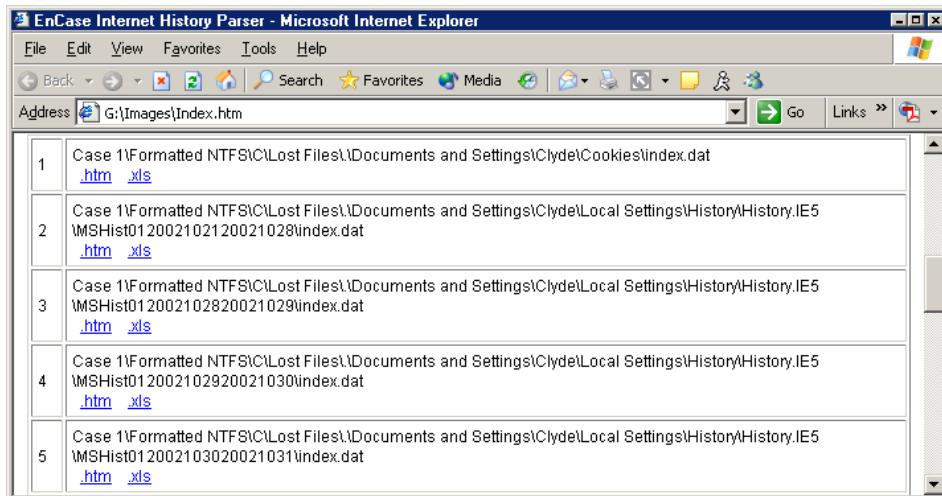


Figure 19-4 IE History Parser EnScript results

Notice the script reports the last time the site was visited from a user at that computer, as well as the last time the site itself was updated.

Reading What the Subject Threw Away

Computer users invariably delete data. However, when data is placed in the Recycle Bin, and the Recycle Bin is subsequently emptied, that data is not deleted. Rather, the pointers to the data are deleted; the data is still intact, but no longer allocated.

Because the data is not necessarily overwritten, EnCase can potentially recover deleted files (anything that was in the Recycle Bin at the time of acquisition, for example), and other files that might have pointers intact.

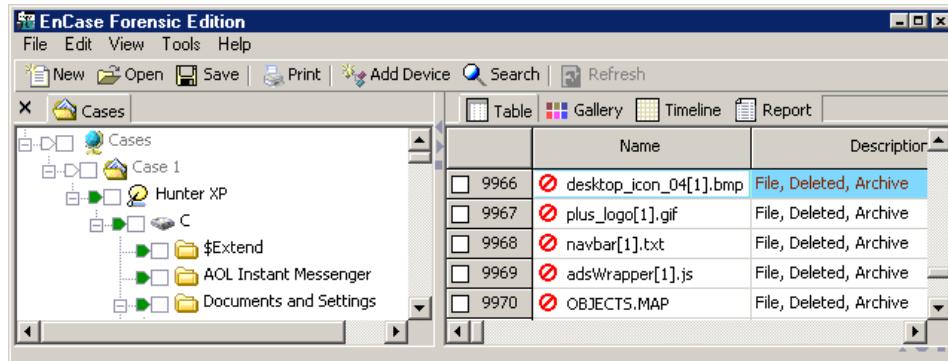


Figure 19-5 Recovered information

Even if files are emptied from the Recycle Bin and then deleted and overwritten, it is still possible to find records of those files within INFO2 files. The date/time stamp for when a file was deleted is recorded in the INFO2 file.

INFO2 files can be recovered from both allocated and unallocated clusters. Look for INFO2 files by sorting the table by file name.

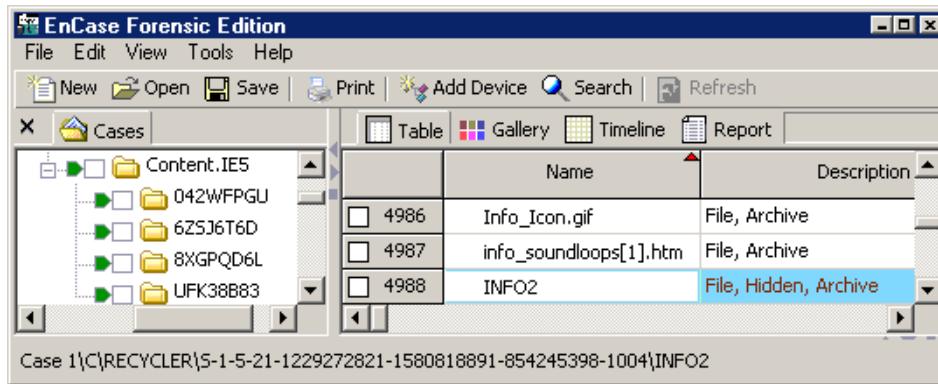


Figure 19-6 Locating INFO2 files

When a user empties a Recycle Bin, the INFO2 file is deleted as well. To recover deleted INFO2 files, run the **NTFS Info2 Record Finder (v4)** or **FAT Info Record Finder (v4)** EnScripts, which search unallocated clusters of the media and file slack to recover Recycle Bin records. Recovered records will then appear under **Bookmarks**, viewable in the proper format.

Presenting Recovered E-mail

It is also possible to include recovered Outlook Express e-mail text and attachments in the report. This is done by bookmarking the attached base64 encoded image and pasting the e-mail header and message in the bookmark comments window. The following figure shows a DBX volume with one mail message:

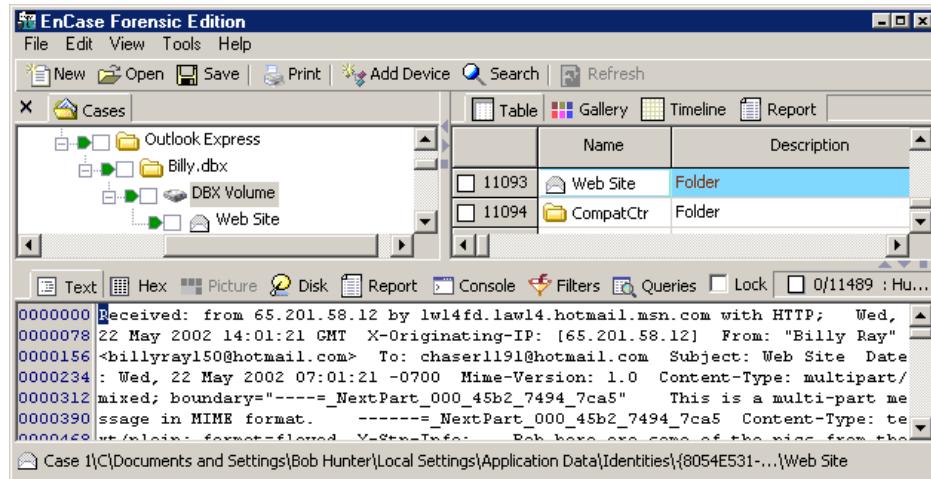


Figure 19-7 Single recovered e-mail

- This message has an attached base64-encoded JPEG image. Select the first character of the e-mail header and highlight (sweep) to the beginning of the encoded image.
- Right click on the highlighted text and select **Bookmark Data**.
- In the **Bookmark Data** window, click in the **Destination Folder** field and select **New Folder...**

- Right click on the folder, select **Rename**, and then give the folder a name such as *E-mail*, and then click **[OK]** to save.

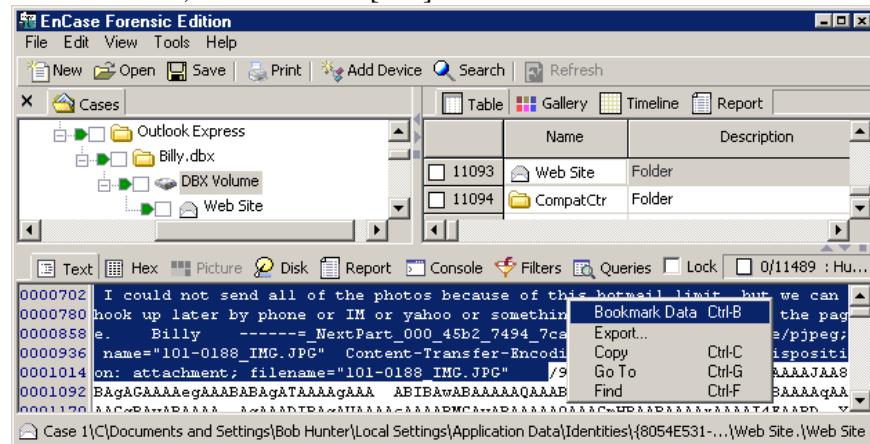


Figure 19-8 Bookmarking e-mail message

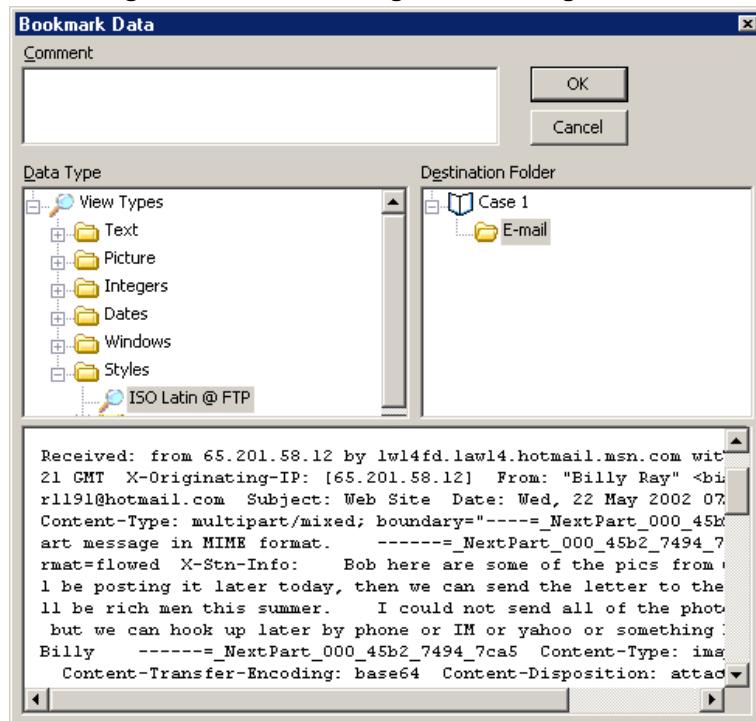


Figure 19-9 Saving text bookmark

- Right-click on the first character of the encoded image (right after the file name) and choose **Bookmark Data** (or hit [Ctrl][B]).
- With the newly created **E-mail** folder selected in the **Destination Folder** window, select **Base64 Encoded Picture** from the **Picture** view type under **Data Type**. You can copy and paste highlighted messages from the clipboard into the **Comments** block. The image should appear at the bottom; click **[OK]**.

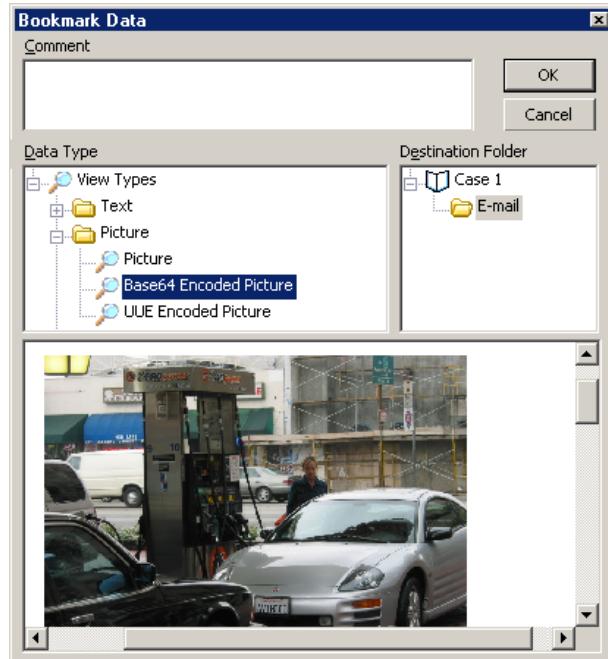


Figure 19-10 Saving Base64 image bookmark

- From the **View** pull-down menu, select **Bookmarks**.
- Click on the new **E-mail** bookmark folder in the left pane.

- Select the **Report** tab in the table. The report should display the complete E-mail, including header, with the bookmark and decoded image at the bottom.

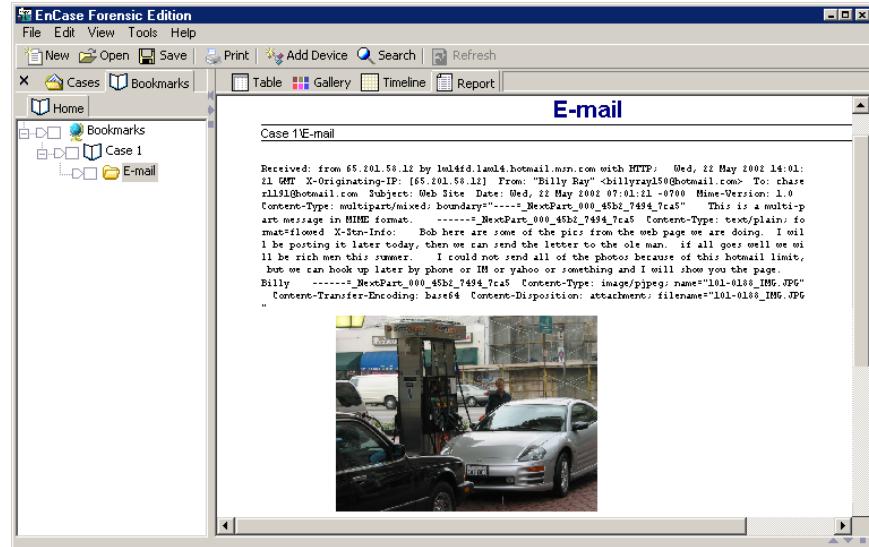


Figure 19-11 E-mail and attachment in Report

Making Sense of a DriveSpace Volume

DriveSpace volumes are only recognized as DriveSpace volumes *after* they have been acquired and mounted into EnCase. On the Storage computer, mount the DriveSpace file as a volume, and then acquire it again to see the directory structure and files. To do this, use the following procedure:

- A FAT16 partition must exist on the forensic PC to which you will copy / unerase the DriveSpace volume to. If one does not exist, create one. A FAT16 partition can only be created with a FAT16 OS (such as Windows 95). Create a Win95 or DOS 6.22 boot disk and use it to boot the storage computer.
- Run FDISK to create a partition, then exit, reboot, and format the FAT16 partition using `format.exe`.
- Image the DriveSpace volume.
- Add the evidence file to a new case in EnCase and search for a file named `DBLSPACE.000` or `DRVSPACE.000`.

- Right-click the file and copy/unerase it to the FAT16 partition on the storage computer.
- In Windows 98, go to the [Start] button and select **DriveSpace** from **System Tools** under the **Accessories** Program group.
- Launch DriveSpace.
- Select the FAT16 partition containing the compressed ".000" file.
- Select **Advance-->Mount**.
- Select DRVSPACE.000 and click [OK], noting the drive letter assigned to it.
- In EnCase, the Compressed Volume File (.000) from the previous drive will now be seen as folders and files in a new logical volume. Acquire this new volume. Create the evidence file and add to your case. It is now possible to view the contents of the compressed drive.

Cracking Encrypted or Password Protected Files

If an encrypted or password-protected file is found, at the moment, a third-party utility must be used to crack the file. Copy / unerase the file to the storage hard drive and attempt to crack the file. Please see *Appendix D, Third Party Utilities*, for a list of the different utilities to assist the forensic examiner.

System Snapshot

The System Snapshot feature allow you to see all open files, processes and ports on the local system, effectively capturing volatile data. With EnCase Forensic, this can only be done with the local (forensic) machine using the **Scan Local Machine (v4)** EnScript; EnCase Enterprise or FIM Editions allow the snapshot to be performed on a live preview of a remote machine using a different EnScript.

Volatile Data Defined

Volatile data exists in the main memory (RAM) of a server or workstation. If power is lost, or if a system fault occurs the data is lost. By contrast, static data is stored on hard drives, USB devices, CD's, etc., and is typically not lost when a loss of power or a system fault occurs.

A computer tracks numerous items that could be critical during incident response activities including; users on a system, TCP and UDP port information, open

files, running processes and applications, and system resource utilization. Much of this information is contained within volatile data and is used by the system for administration and processing purposes. Snapshot captures this volatile data and provides information on what was occurring on a system at a given point in time.

During or after an incident, volatile data may reveal invaluable information. Are any ports open that should not be? Are unfamiliar services or machines accessing the system? Are unknown applications or processes executing? This information helps the examiner determine what is happening on the system at the current point in time, and if an attack is active.

The correlation of volatile data and static data is essential, but not exhaustive to the incident response process. Volatile data will help an examiner determine if suspicious activities or applications are active on a system, and help guide the examiner to search for backdoors or malicious code. Additionally, it may help the examiner determine who and what is accessing the system and its resources whether internal or externally. The most critical aspect of volatile data capture is it provides the examiner with the ability to quickly ascertain if unauthorized ports, processes or applications are active. This information is critical when deciding whether to continue system operation or take the system out of service. This is a crucial component of incident response triage; the ability to rapidly determine to what extent, if any, a system has been compromised.

Volatile Data Components

Open Ports

Open ports are the active endpoints to a logical TCP connection on a system at a particular point in time.

Active Processes

Active processes are the executables that are running on a computer at a particular point in time.

Open Files

Open files are the files that are in use on a computer at a particular point in time.

Live Windows Registry

Live Windows Registry keys are those that are active only during the logged on user's session.

Volatile Data Capture using Snapshot

EnCase Forensic has the capability to capture volatile data from the local machine only. The examiner can view active processes, open ports and open files, and the live Windows Registry.

Organizations should have a thorough understanding of typical volatile data values for their environment including; authorized and utilized ports, authorized applications, and clearly documented file access privileges. Provided an organization has this understanding, it is easy to see how an examiner could quickly locate unauthorized sessions, services and applications by using Snapshot to acquire and analyze volatile data.

The results of a Snapshot having been run on the local examiners machine provides the same information is available as if it were run across the network, but is limited to the examiners machine only.

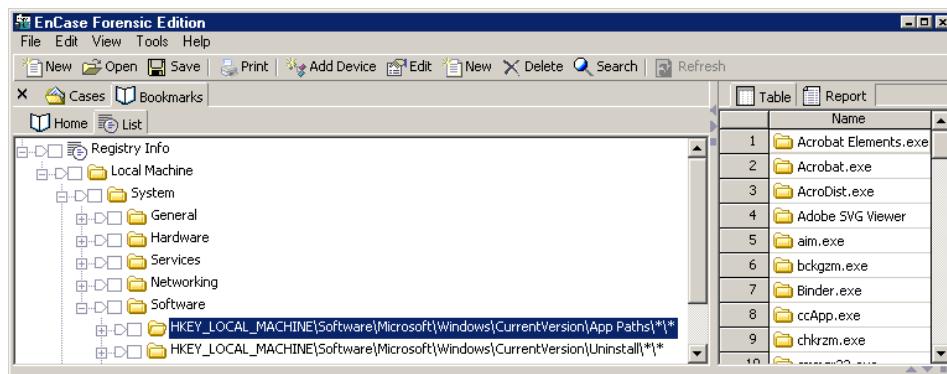


Figure 19-12 Snapshot results on local machine

Open Ports

Open ports are ports that are currently in use or waiting for use by an application. As mentioned previously, organizations should have a thorough understanding of ports that are authorized and utilized within their organization on a per machine basis. Open port information will help the investigator understand who or what is communicating with a system at a particular point in time. Many times when a machine has been compromised, or is being compromised, there is communication occurring over open ports. Hackers and malicious employees often attempt to gain access to a computer by searching for open and vulnerable ports to exploit.

The examiner also has the ability to filter the results in the top right pane to meet certain specified criteria. The Filter and Query functionality in EnCase enables the examiner to target certain types of information and to narrow down the results shown in the top right pane. Numerous filters are provided with EnCase. New filters can be created and existing filters can be modified at any time by the examiner.

Open Ports Columns

Name – Name of the service or port number.

Filter – Visual indicator if the information viewed is the result of a running filter.

In Report – Indicates whether or not the entry will appear in the Report view.

Protocol – Indicates the protocol (OSI Layer 4) the port is using to communicate.

Local Address – If the port is tied to a designated IP address, it will be indicated here.

Local Port – This is the port the process is tied to.

Remote Address – If there is a remote IP address connected to the indicated port, the IP will be visible here.

Remote Port – If there is a remote machine connected to the port, the communication port on the remote machine will be present here.

State – This indicates the status of the port. Options here are **Listening** (waiting for a connection), **Established** (an active connection to the port exists) and **Time_Wait** (the process is waiting for additional information).

Process ID – An integer used by the Operating System

Active Processes

Active processes are processes that are currently running on a system. This information is critical when trying to identify if rogue or unauthorized processes are active on a system. The Snapshot provides the ability to view active processes.

In the **Processes** tab, with the select all box (green home plate-like box) checked, all running processes on machine can be viewed in the right pane. The **App Comment** (Application Comment) field shows processes that are identified as authorized applications that are commonly used for malicious purposes.

EnCase is able to identify the malicious programs via a hash analysis, comparing the application's unique digital fingerprint (hash value) that had been pre-calculated and stored in EnCase by the examiner, with the hash value of that program that was calculated by EnCase and then captured during Snapshot.

Since the hash value matches, EnCase returns the predefined Application Descriptor (**App Descriptor**) and Application Comment (**App Comment**) values, identifying the application on the suspect computer. **Application Descriptor** is a new feature in EnCase v4.16 and above that provides categorization of executables via hash values, which enables the examiner to positively identify executables running on a system via a hash value match. Application Descriptor works in concert with Machine Profile, another new feature in EnCase v4.16 and above, which contains an inventory of what should be running on a specific machine. Together the Machine Profile and the Application Descriptor let the examiner know what should be running on a specific computer and what is actually running on that machine.

The bottom pane provides a wealth of information in report format for the line item selected in the top right pane. In this example, the examiner immediately can identify directories, commands that were entered, times, and more.

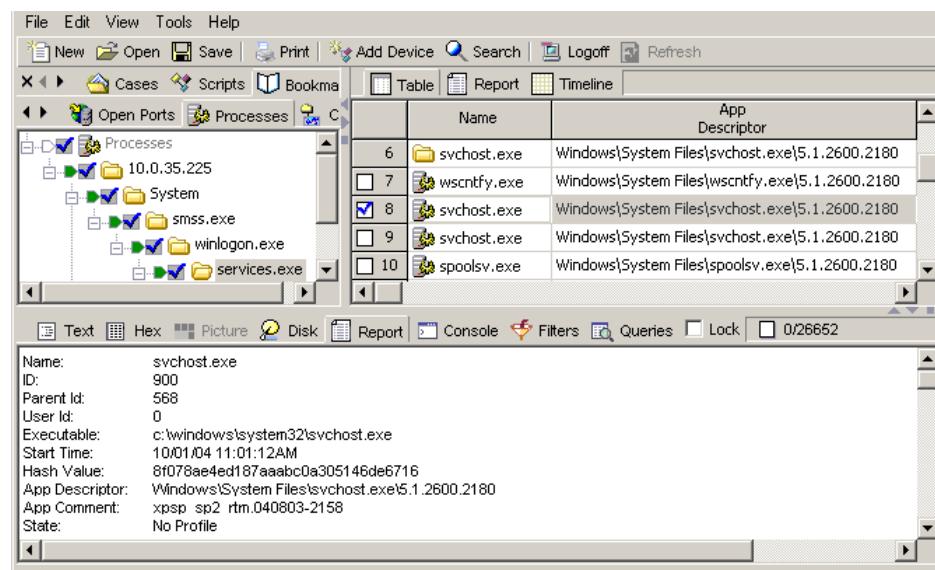


Figure 19-13 Active Processes

Processes Columns

Name – Name of the process.

Filter – Visual indicator if the information viewed is the result of a running filter.

In Report – Indicates whether or not the entry will appear in the Report view.

ID – This is the process ID (PID) assigned by the Operating System.

Parent ID – This is the Parent Process ID (PPID) in the event that the viewed process was spawned by another process.

User ID – In Linux and Windows this is the ID of the User who spawned the process.

Current Directory – This is the current working directory.

Root Directory – On a Linux system, this is the root directory for the machine.

Command Line – These are the parameters that were passed when the process was started.

Executable – This indicates the location of the binary executable, which spawned the process.

Start Time – This is the date and time the process was started.

Hash Value – MD5 Hash value for the process.

Hash Set – If the hash value of the process is contained in the Hash Library, the hash set that includes the hash value will be listed here.

Hash Category – If the hash value is included a hash set of the Hash Library, the category of the hash set will be listed here.

App Comment – Comments that are associated with an App Descriptor (if applicable).

Profile – This will list the Profile which includes the process (if applicable)

State – This is the state of the process in regards to the App Descriptor. The 3 possible entries are:

No Profile – The process hash is not assigned to a machine profile.

No Hash – No hash value has been assigned to the process.

Approved – The process has been assigned to an app descriptor and included in the current profile.

Not Approved – The process has been hashed, but is not included as part of the current machine profile.

Open Files

Open files are files currently in use on a system in relation to an active executable. This information is critical when trying to identify what person or process is accessing files on a system. Understanding what files are open provides an examiner with an understanding of what information a perpetrator or application is accessing. The EnCase Version 4.16 Snapshot provides the ability to view and document open files.

In **Figure 19-14** the **Open Files** tab has been selected in the left pane. The right pane shows the open files that are in use by the process ‘..’, sorted by file name.

	Name	Process Id	File Id	File Path
1	_vti_adm	524	1	C:\Program Files\Common Files\Microsoft Shared
2	_vti_adm	524		C:\Program Files\Common Files\Microsoft Shared
3	_vti_aut	524		C:\Program Files\Common Files\Microsoft Shared
4	_vti_aut	524		C:\Program Files\Common Files\Microsoft Shared
5	_vti_bin	524		C:\Program Files\Common Files\Microsoft Shared

Figure 19-14 Open Files

At this point, the examiner has a lot of information regarding the rogue process running on the suspect computer. However, the examiner wishes to further investigate by examining data on the suspect computer’s hard drive. To do so, the examiner ‘Previews’ the suspect computers drive contents with EE to analyze the contents of the computers drive media. Data that is actually stored on drive media (i.e. not in RAM) is considered static data.

Analysis of static data includes analyzing file systems, memory dumps, system logs, network data, operating system artifacts and much more, from drive media. EnCase provides robust functionality to examine the drive contents (static data) of suspect machines.

Network Interfaces and Users

Other data available in a Snapshot include the network card(s) in the machine and Windows users from the live registry.

The Network Interfaces tab includes information on the network interface card manufacturer, the assigned IP address, MAC address, and subnet mask.

A screenshot of a software interface titled 'Network'. The left sidebar shows 'Open Files' and '10.0.35.225' with sub-folders 'System', 'smss.exe', 'crss.exe', and 'winlogon.exe'. The main area is a table with columns: Name, Process Id, File Id, and File Path. The table contains five rows:

	Name	Process Id	File Id	File Path
1	_vti_adm	524		C:\Program Files\Common Files\Microsoft Shared
2	_vti_adm	524		C:\Program Files\Common Files\Microsoft Shared
3	_vti_aut	524		C:\Program Files\Common Files\Microsoft Shared
4	_vti_aut	524		C:\Program Files\Common Files\Microsoft Shared
5	_vti_bin	524		C:\Program Files\Common Files\Microsoft Shared

Figure 19-15 Network Interfaces

The Network Users tab has information about all users who have logged onto a machine, including the user name, Security ID, and last date/time of login.

A screenshot of a software interface titled 'Network'. The left sidebar shows 'Network Users' and '10.0.35.225'. The main area is a table with columns: Name, ID, and Accessed. The table contains three rows:

	Name	ID	Accessed
1	systemprofile	S-1-5-18	08/18/04 11:21:46AM
2	LocalService	S-1-5-19	10/01/04 11:01:32AM
3	NetworkService	S-1-5-20	10/01/04 11:01:12AM

Figure 19-16 Network Users

This allows the examiner to create a Timeline of the login activity of Network Users.

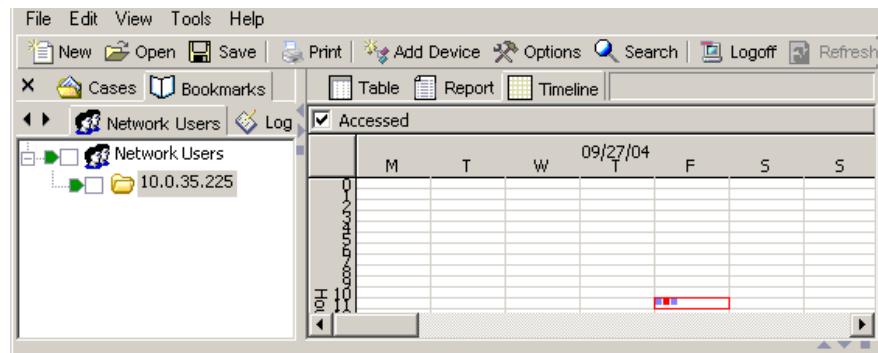


Figure 19-17 Timeline of Network Users

Log information is available from the **Log Records** tab.

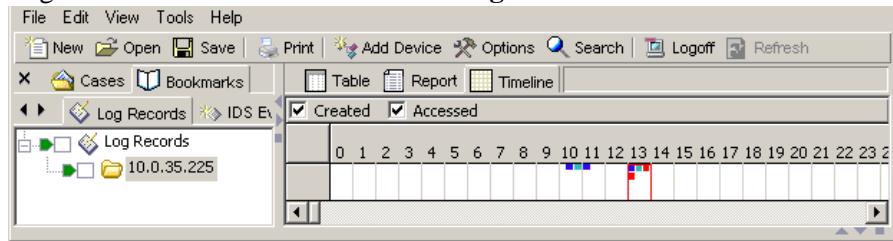


Figure 18-20 Log Records

*Copyright © 2004 Guidance Software, Inc.
May not be copied or reproduced without the written permission of Guidance Software, Inc.*

Chapter 20

Foreign Language Support (Unicode)

This chapter covers a critical emerging area of investigations: working with languages other than English in forensic investigations. The matter is a complicated issue due to the many variables involved. Whether you are an investigator in the United States examining a system with foreign language documents on it, or an investigator working on a system with a non-English version of Windows examining media either in English or in a foreign language, these different variables determine the best way to approach analyzing the data.

The Unicode standard attempts to provide a unique encoding number for every character, regardless of platform, computer program, or language. Unicode uses 16-bits to represent each character, as opposed to ASCII (which uses 7-bits). For the complete Unicode code charts, please go to www.unicode.org/charts.

Figure 20-1 Unicode Code Chart (<http://www.unicode.org>)

EnCase now supports Unicode. What this means for investigators is that EnCase can now search for and display Unicode characters, thus supporting more languages.

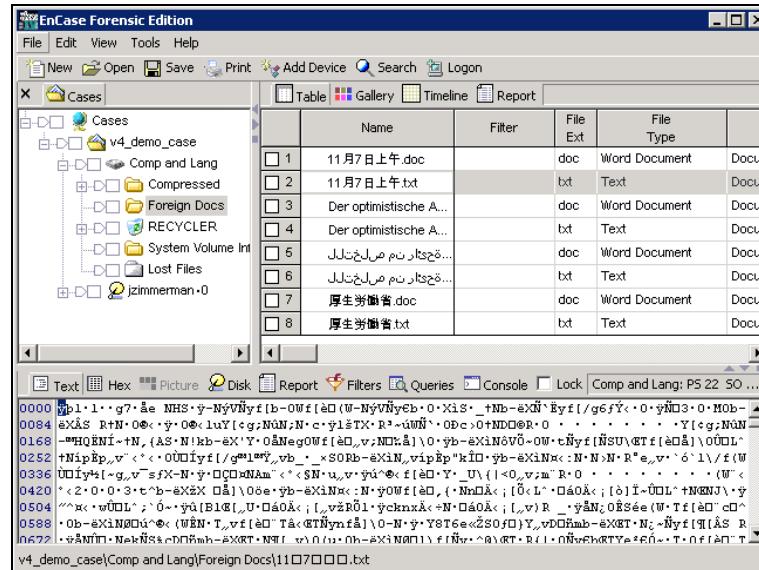


Figure 20-2 Foreign-language files in EnCase

Not all documents are entered in 16-bit Unicode, however, complicating the situation. This chapter will go over viewing Unicode documents, viewing non-Unicode, foreign-language documents, foreign language keyword searching, and

bookmarking non-English text to display correctly in the report. The EnCase window by default does not recognize foreign characters in filenames; to configure EnCase to properly display these characters, select the **Options** feature from the **Tools** pull-down menu and click on the **FONTS** tab.

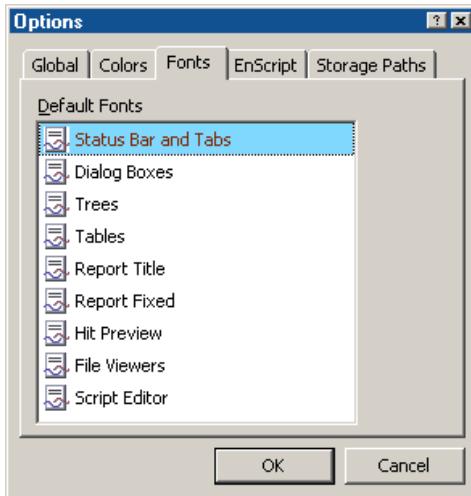


Figure 20-3 Fonts tab

Double-click on **Status Bar and Tabs** and then change the font to **Arial Unicode MS**.

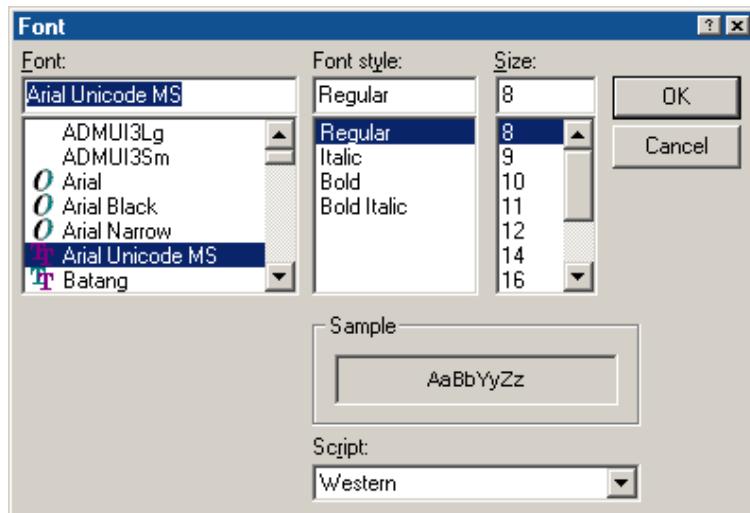


Figure 20-4 Font Selection

Click [OK] and view the EnCase frame; the filename is displayed correctly.

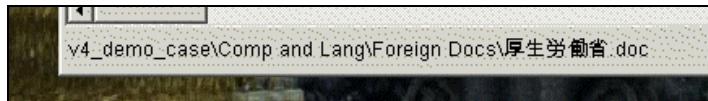


Figure 20-5 Foreign characters displayed

Viewing Unicode Files

EnCase, by default, displays Text and Hex tab characters in ANSI (8-bit) format with the **Courier New** font. Viewing Unicode files properly, however, can require modifications of both the format (encoding) and the font. First, the Unicode file or document must be identified as Unicode. This is not always straightforward.

Text files (.TXT) containing Unicode begin with a Unicode hex signature \xFF\xEE. Word-processor documents written in Unicode, however, are not so easy. Typically, word-processor applications have signatures specific to the document, making identification of the file as Unicode more difficult.

The screenshot shows the EnCase Forensic Edition software interface. The main window displays a list of files in a table format:

	Name	Filter	File Ext	File Type
1	11月7日上午.doc		doc	Word Document
2	11月7日上午.txt		txt	Text
3	Der optimistische A...		doc	Word Document
4	Der optimistische A...		txt	Text
5	قةحئار نم مىلختلى...		doc	Word Document
6	قةحئار نم مىلختلى...		txt	Text
7	厚生労働省.doc		doc	Word Document
8	厚生労働省.txt		txt	Text

Below the table, there is a hex dump of a document. The first few lines of the dump are:

```

0000 FFFE 3100 3100 0867 3700 E565 0A4E 4853 0CFF 2D4E FD56 D179 665B : 110700000000
0026 6296 3057 665B E890 2857 2D4E FD56 D179 8062 1A4F 0258 EC53 005F 000000000000
0052 864E 6296 EB58 D191 CB79 665B 2F67 3683 DD9E 1A4F OCFF D18F 3300 000000000003
0078 3000 4D4F 6296 EB58 C253 A052 864E 1A4F AEB8 0CFF 1A4F AEB8 3175 000000000000
0104 595B A267 3B4E FB4E 3B4E 0163 0CFF 6C9A 5458 0752 B37E FA57 D191 000000000000
0130 1A4F D063 9B4F 864E 448D A952 0230 0D00 0A00 0D00 0A00 2000 2000 0000 00000000
0156 2000 2000 595B A267 3B4E FB4E 9699 4851 CB4E CD7E 864E 2C7B 4153 000000000000
0182 004E 216B 6296 EB58 2759 1A4F E54E 6567 3057 665B E890 8476 3B4E 000000000000

```

Figure 20-6 Unicode hex signature

To display the text in Unicode, select **Text Styles** from the **View** pull-down menu:

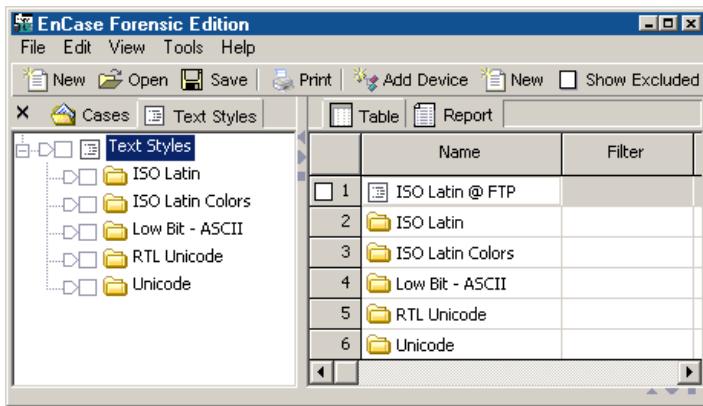


Figure 20-7 Text Styles view

- Right-click on the **Text Styles** selection on the left-hand side and select **New**.

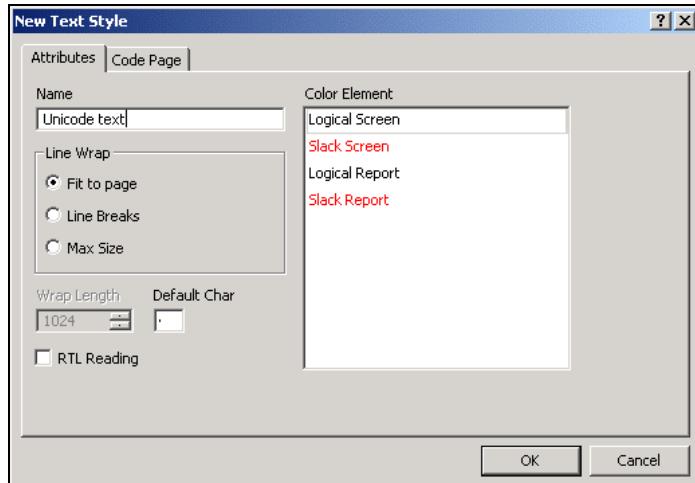


Figure 19-8 Creating a new Text Style

- In the **Attributes** tab, type in a name for the Text Style.
- Click on the **Code Page** tab. For a Unicode document, the **Unicode** radio-button must be checked. Notice when the **Unicode** radio-button is checked, all language code-pages are grayed-out.

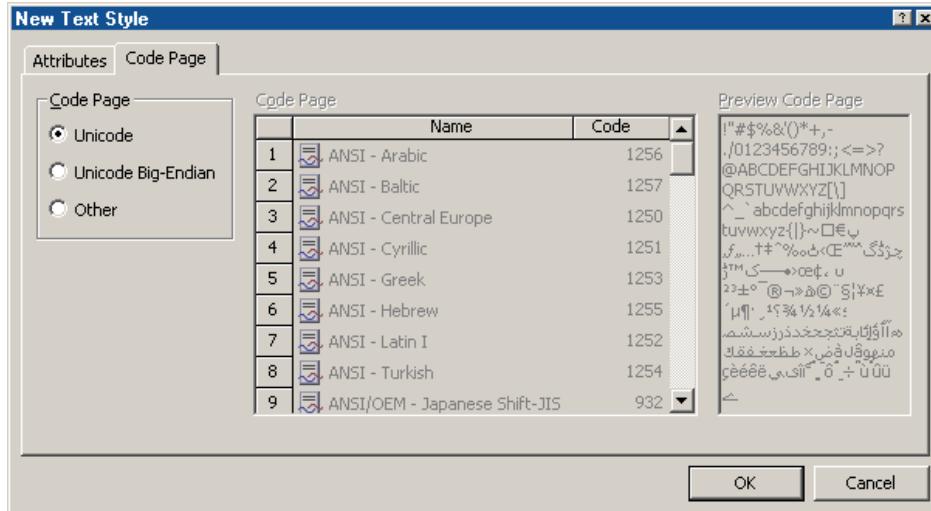


Figure 20-9 Code Page tab

- After clicking [OK], the Unicode text will be displayed properly.

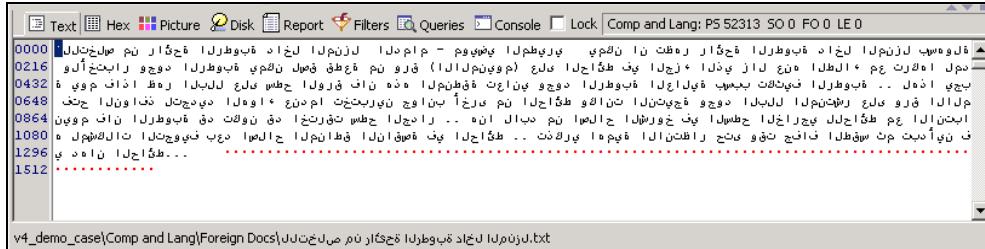


Figure 20-10 Unicode text

Unicode Fonts

While Unicode is designed to be a universal character-encoding standard, correct display of Unicode characters relies heavily upon the font selected to display the characters. While one font might successfully display certain Unicode characters of a certain language, the same font might not display Unicode characters for another language. Characters that are not “translated” by the font are displayed as the “default” character, typically either a dot or a square (Figure 19-12).

Look at the diagram below. Unicode is a vast character-encoding scheme, with languages typically broken up into “sets” (Figure 19-1). A font can be thought of as the translator, which interprets the bytes and displays the character according to that number. However, if the font does not have enough information to

Copyright © 2004 Guidance Software, Inc.
May not be copied or reproduced without the written permission of Guidance Software, Inc.

“translate” all of the Unicode character encodings, the application using that font will not display that character correctly. For character encodings that the font understands, those Unicode characters will be displayed correctly.

Unicode Characters	Font (translator)	Application
English subset	English subset understood	Correct display
Japanese subset	None	Default character
Chinese subset	None	Default character
Arabic subset	Arabic sub-set understood	Correct display

Figure 20-11 Unicode Character

Switch to a Unicode font when a font is *not* displaying Unicode characters correctly. Unicode Arabic text is interpreted and displayed correctly by EnCase, even though the default font that EnCase uses to display text is Courier New (an 8-bit font). However, certain languages, such as Chinese and Japanese, cannot be viewed properly in this font. In order for characters to be displayed properly, the font, which is selected, must support that character set. The solution then is to switch the EnCase file-viewing font to a Unicode font (supporting all Unicode character sets).

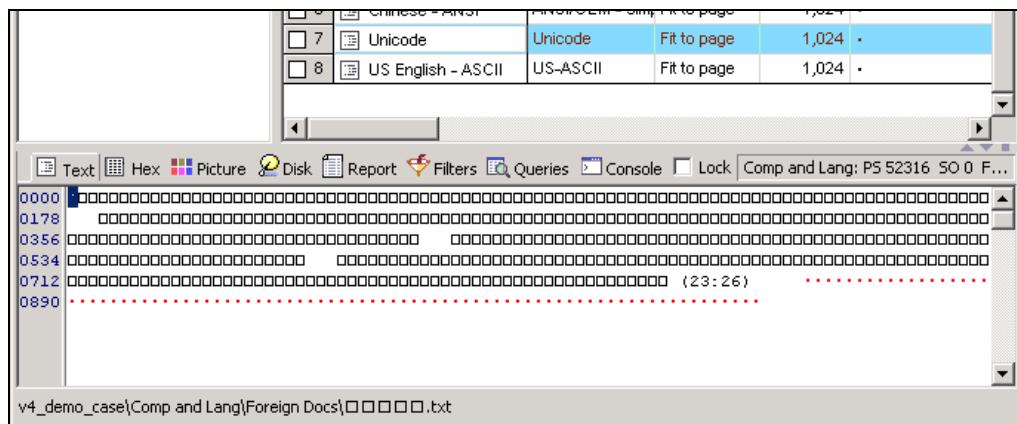


Figure 20-12 Unicode displayed improperly

To change the display font:

- From **Options** in the **Tools** pull-down, select **Fonts**, and double-click on **File Viewers**.

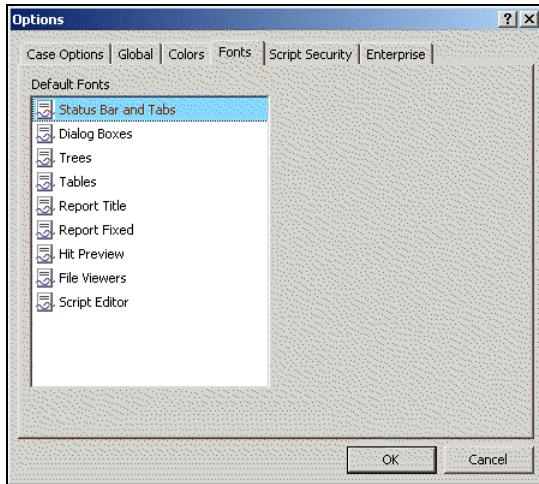


Figure 20-13 File Viewers

- Change the font from Courier New to **Arial Unicode MS** and click [**OK**].

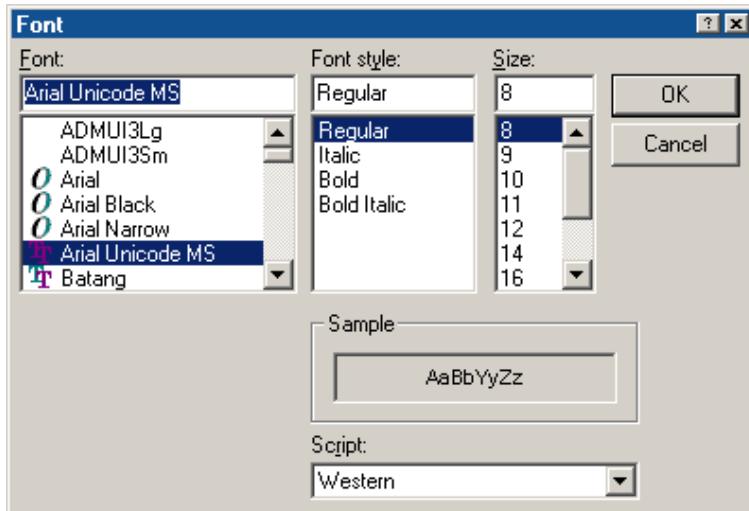


Figure 20-14 Configuring font size

- The Chinese text file is now displayed properly.

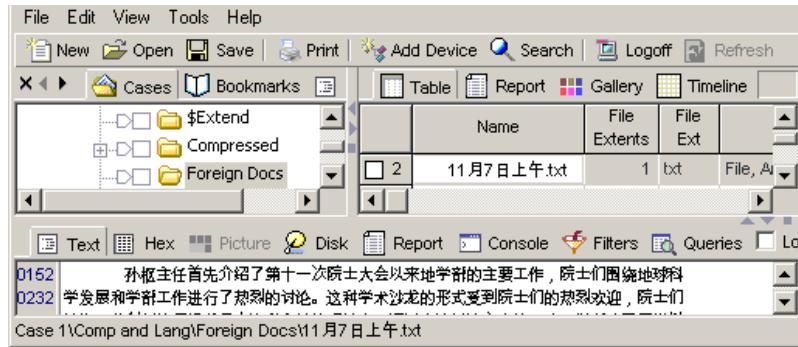


Figure 20-15 Viewing Unicode characters correctly

Changing Font Size

In Figure 19-15, the font size displaying the characters is small, making it difficult to read. To increase or decrease the font size, follow these steps:

- Go to **Tools→Options→Fonts**.
- Double-click the **File Viewers** entry (Figure 20-13).
- Change the font size (Figure 20-14).
- The characters will appear in a larger format (Figure 20-16).

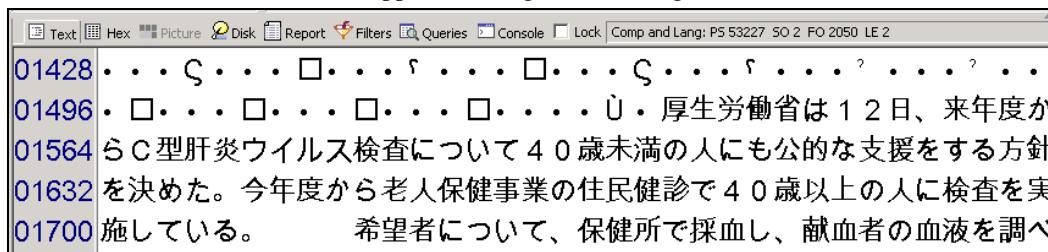


Figure 20-16 Larger font size

Font Recommendations

The “Arial Unicode MS” font contains most if not all of the Unicode characters, making it the ideal font to use for foreign-language investigations.

However, 8-bit characters will be interpreted as 16-bit pairs when this font is selected, so that 8-bit documents are not displayed correctly. Figure 19-17 shows the \$MFT file displayed as a Unicode document with the Arial Unicode MS font selected for viewing. As you can see, Chinese characters are displayed.

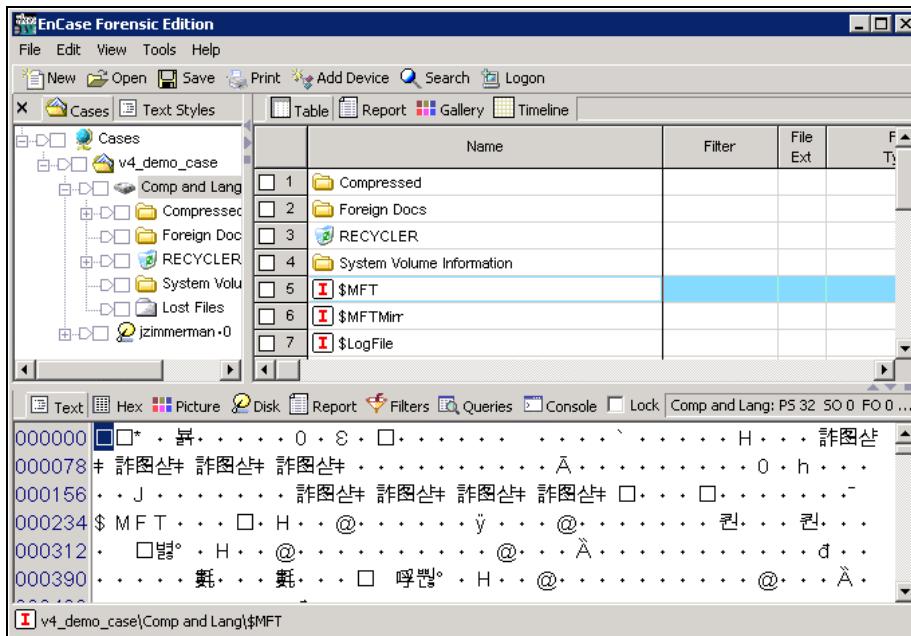


Figure 20-17 The MFT displayed with the Arial Unicode MS font

For this reason, Guidance Software recommends using the Courier New font for English and all code page investigations and the Arial Unicode MS font for Unicode investigations.

Viewing Non-Unicode Files

Unicode is an attempt to display all characters from all languages in one standard. Before Unicode evolved to the point it has, *separate* character encoding schemes, called Code Pages, were created to display separate foreign languages. These Code Pages were excellent for displaying the language for which they were designed, but problematic in that they only displayed the language for which they were designed.

EnCase Version 4, by including these Code Pages, allows the forensic investigator to view many foreign language documents correctly.

First, locate a non-Unicode, foreign-language document. In Figure 20-18, text of a German language document is displayed. But EnCase is by default using the ANSI – Latin I Code Page, not the ANSI – Central Europe one.

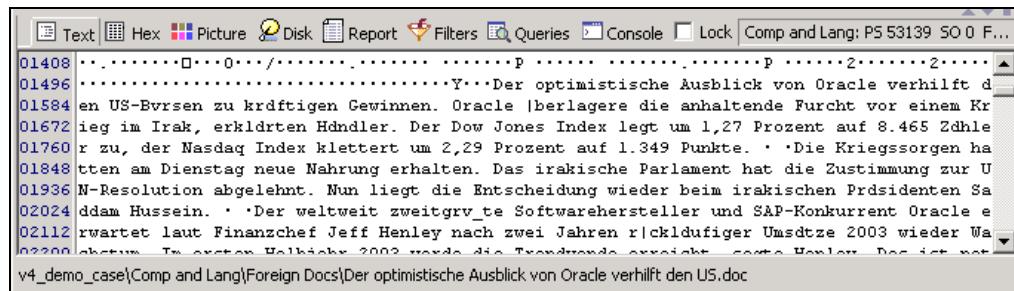


Figure 20-18 German text displayed without the German Code Page
To display the text in the native language, create a new Text Style.

Navigate to the View pull-down menu from the menu bar and select **Text Styles**.

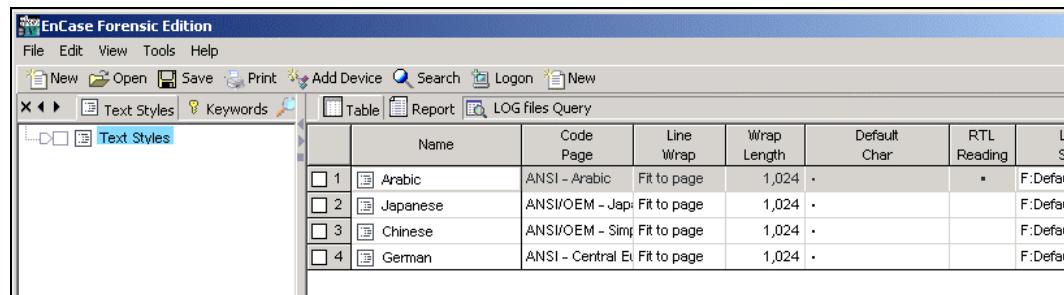


Figure 20-19 Text Styles tab

Right-click on the Text Styles selection on the left-hand pane and choose **New**. Name the new Text Style the appropriate language; for example, German ANSI (Figure 20-20).

Below the text formatting options is a box for **RTL Reading**, which means Right-to-Left reading. For languages that read right-to-left, such as Arabic or Hebrew, check the check box. For German, a left-to-right language, leave the check box empty.

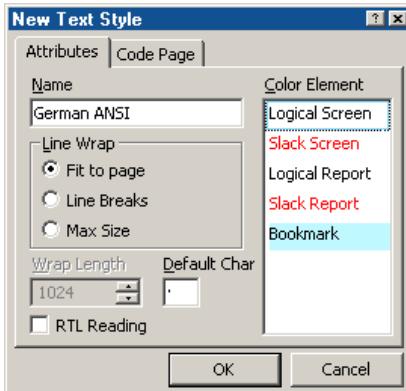


Figure 20-20 Text Style options

The other tab, **Code Page**, presents several options for Code Pages. In this case, choose **ANSI – Central Europe** to view the German document. (Germany is in Central Europe.) Highlight the Code Page and click **OK**.

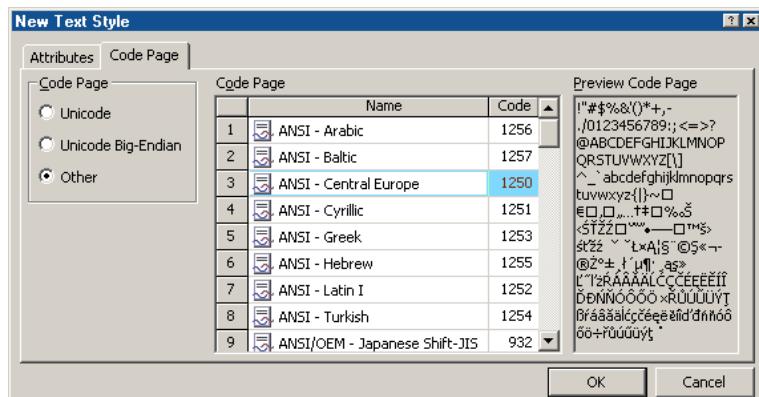


Figure 20-21 Assigning a Code Page to a Text Style

The German document is now displayed correctly in EnCase (Figure 20-22).

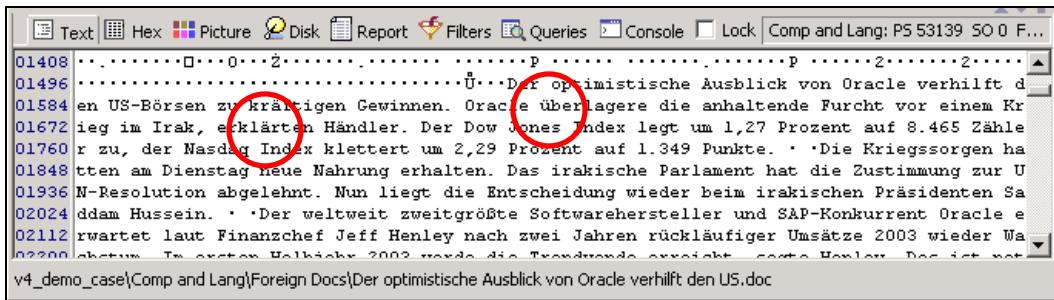


Figure 19-22 German text displayed correctly

The differences are subtle, as the ANSI – Latin I code page uses many of the same characters as Central European code page. Compare Figure 20-22 (correct) to Figure 20-18 (incorrect) – the umlauts are missing in the earlier figure.

Text Styles can be created for every Code Page, so even if the Code Page used to create the document is unknown, viewing documents correctly becomes largely a matter of locating the correct Text Style (or switching to the Unicode text style and using a Unicode font).

Also, notice in Figure 20-21 above, the first 95 characters of the ANSI – Central Europe Code Page are standard ASCII characters. If you click through all of the Code Pages, you will notice the first 95 characters of every ANSI Code Page do not change. This means that English characters and words, no matter the Code Page selected, will be displayed properly.

Right to Left (RTL) Languages

For languages that read right-to-left, such as Arabic and Hebrew, check the **RTL Reading** check box when creating the Text Style and click **OK**.

That works for 8-bit Code Pages with no complications. For the all-purpose Unicode Text Style created above (Figures 20-8 and 20-9), it does not work. Arabic and Hebrew read right-to-left, but we did not specify that when we created the Unicode Text Style above.

For that reason, the investigator might need to create two Unicode Text Styles-- one that displays left-to-right and one that displays right-to-left. Then, to view Arabic or Hebrew Unicode text, the RTL Unicode Text Style would be used.

	Name	Code Page	Line Wrap	Wrap Length	Default Char	RTL Reading
□ 1	Unicode - Right-to-Left	Unicode	Fit to page	1,024	.	.
□ 2	Unicode Left-to-Right	Unicode	Fit to page	1,024	.	
□ 3	Arabic	ANSI - Arabic	Fit to page	1,024	.	.

Figure 20-23 Two Unicode Text Styles, one with RTL Reading checked

Foreign Language Keyword Searches

Keyword searches are a critical function to quickly locate and bookmark key evidence. EnCase Version 4 now features the ability to search for foreign language keywords. Unfortunately, searching for foreign language keywords is not as easy as typing in the word in English, changing the Code Page to the language desired, and beginning the search. Typing in the word “fire”, for example, changing to the Central Europe Code Page (for German), and then beginning a search will not search for the German word for “fire”.

The first requirement is that ***the investigator must have knowledge of the desired word in the foreign language***. So, to expand on the example above, instead of “fire”, the investigator would have to type in the German word for fire “feuer”. Then the Central European Code Page would have to be selected, and then the search could begin.

It is not always that easy. Often, languages contain characters that are not readily typed in by an English-mapped, QWERTY keyboard—the French accent-grave, the German umlaut, or any character in Japanese, Chinese, Arabic, and many other languages.

There are several solutions available to the investigator to enter keywords in a foreign language.

Copying and Pasting

Copying and pasting is the easiest method for entering keywords of a non-English language into the keyword field. Highlight the characters, copy them, and paste into the Search Expression field. If the pasted characters are displayed as boxes, the font being used to display those characters is the wrong font. The font must be changed by going to **Tools→Options→Fonts** and changing the font for **Dialog Boxes**.

The caveat with this method is that the desired keyword must be located in a document already before a search for the keyword can be executed.

Character Map

Another method for inputting keywords of a different language into EnCase is to select the characters from the Windows 2000 Character Map dialogue box. While this method can be used for all character maps, it is probably most useful when entering a keyword that *mostly* uses ASCII characters, but might contain one or two that are not standard. The French word “garçon” is a good example.

- Click on the [Start] button and from the **Programs/Accessories/System Tools** menu select **Character Map**. Depending on the character needed from the Character Map, it might be necessary to change the font to a Unicode font. To change the font, go to the **Font** pull-down list and select a Unicode font such as **Arial Unicode MS**.

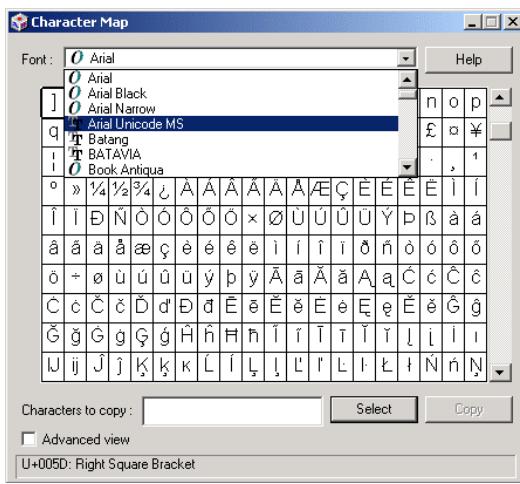


Figure 20-24 Selecting a font in Character Map

- Select the desired character from the Character Map and double-click it. It will appear in the **Characters to copy:** field below.

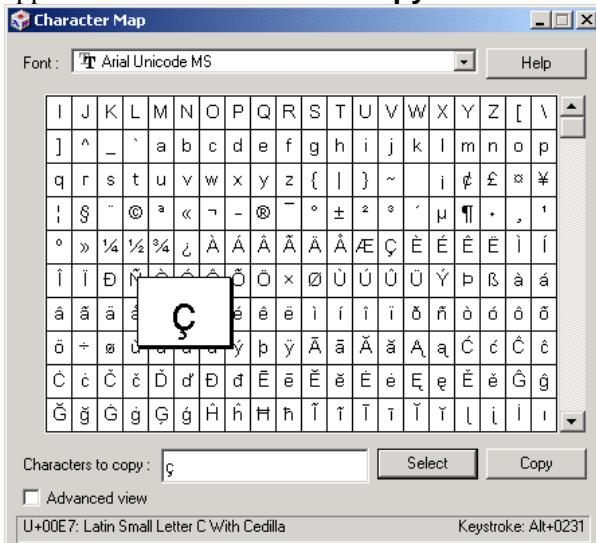


Figure 20-25 Selecting a character in Character Map

- Press the **[Copy]** button and switch back to EnCase.
- Navigate to the **Search Expression** field in the **New Keyword** dialogue and paste the character into the field.
- Enter the rest of the keyword and check the **Active Code-Page** check box.

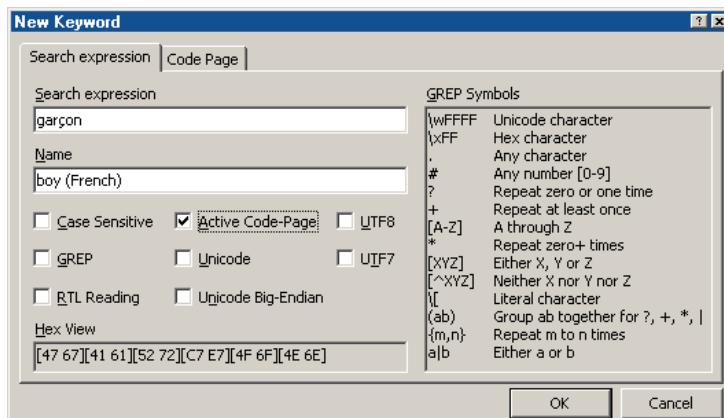


Figure 20-26 Creating keyword with ç character

- Select the appropriate Code Page (in this case, **ANSI – Latin I**). Blue check the Code Page, and then click **[OK]** to begin the search.

	Name	Search Expression	GREP	Case Sensitive	Active Code-Page	Unicode	Unicode Big-Endian
□ 1	💡 "fire" in German - ANSI	feuer			.		
□ 2	💡 "Boy" in French - ANSI	garçon			.		

Figure 20-27 Foreign keywords

Regional Settings

The final method is to switch the Storage computer's keyboard mapping to a different region, thus allowing input of a different language with the keyboard. Instead of manually selecting each character from the Character Map system tool (above), the foreign keyword can be typed into the Search Expression keyword field.

The problem with remapping the keyboard is that the new mapping (the character each key inputs) is not displayed on the keys. Unless thoroughly familiar with the new keyboard mapping, or unless the keyboard map chart is available as a reference guide, this is not the recommended method for entering keywords in a foreign language.

To remap the keyboard, open the **Regional Options Control Panel** from the **Settings** menu on the **[Start]** button.

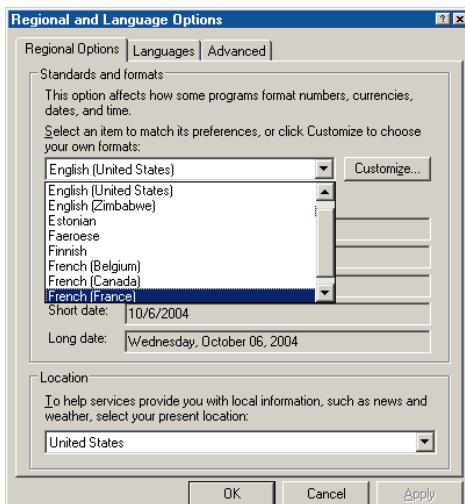


Figure 20-28 Selecting regional options

You will need to make the appropriate changes in the **Advanced** tab as well. When finished, click **[OK]** and switch to EnCase. You can now type the foreign keyword into the **Search Expression** field.

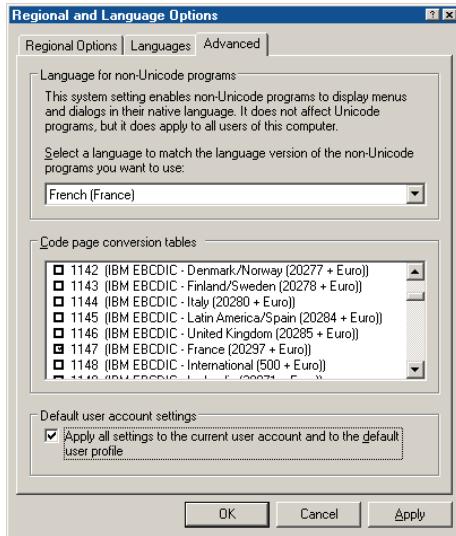


Figure 20-29 Advanced settings

Foreign Language Bookmarking

ASCII text can be bookmarked and displayed in the report, regardless of the language. Text is bookmarked and displayed with the available Text Styles. For a Unicode document, choose the standard Unicode view or the Unicode Text Style created under Text Styles.

- Click and highlight the desired text to appear in the report.
- Right-click and select **Bookmark Data** from the contextual menu.



Figure 20-30 Bookmark the highlighted data

- Select the right Text Style. For Unicode Arabic, choose the **Unicode – Right-to-Left** Text Style from the **Styles** folder (as we are bookmarking Arabic text, which reads right-to-left).

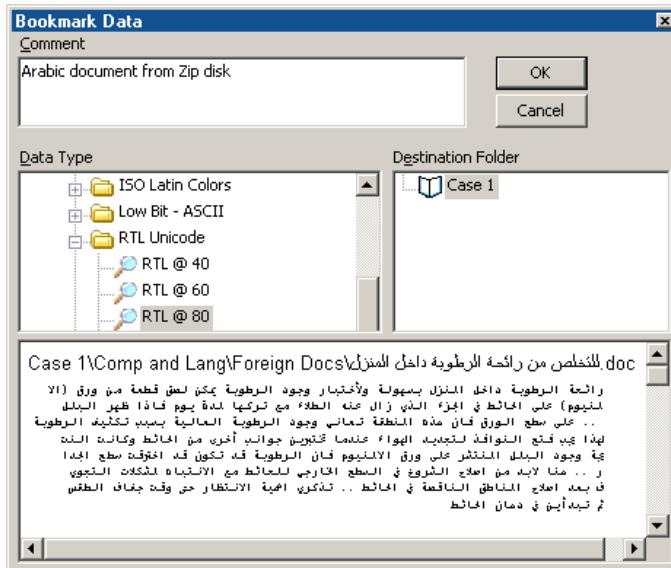


Figure 20-31 Text formatted to flush-right

- Press [OK] and switch to the Report view. The bookmarked text will be displayed in the report, formatted in the desired text style.

The screenshot shows the 'Report' view in EnCase. It lists a single item: 'v4_demo_case'. Underneath it, there is a sub-item: '1) v4_demo_case\Comp and Lang\Foreign Docs.txt'. The text content of this item is Arabic, displayed in a right-to-left orientation. The report view also includes a 'Bookmark Folder' dropdown and a 'Page 1' indicator.

Figure 20-33 Arabic displayed in report

Rich Edit Control in Bookmarks

Guidance Software continues to improve the ability of EnCase to be used in international examinations with Rich Edit Control in the bookmark comments

and bookmark notes. These comments and notes can now be written in languages other than English. In the example below, the comments of the examiner are entered in Arabic and English, and the swept data is displayed in the correct Arabic characters.

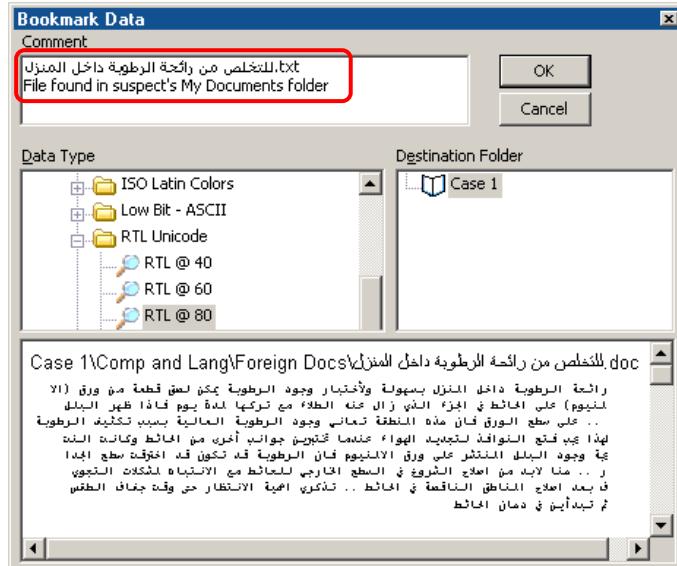


Figure 20-34 Rich Edit Control for bookmarking in desired language.

More Information

The implementation of foreign language support into EnCase is a substantial undertaking and truly allows forensic investigators to perform international investigations.

Guidance Software will release foreign language user interfaces throughout the year so that not only can investigators search for and view non-English documents and files, but they will be able to work in their native-language interface as well.

Chapter 21

Restoring Evidence

EnCase allows an investigator to restore evidence files to prepared media. Restoring evidence files to media theoretically permits the investigator to boot the restored media and view the Subject's computing environment without altering the original evidence. Restoring media, however, can be challenging. Read this chapter carefully before attempting a restore.



Alert! DO NOT boot up the Subject's drive. Do not boot up your forensic hard drive with the Subject drive attached. There is no need to touch the original media at all. Remember, it is still evidence.

Physical vs. Logical Restore

EnCase allows the investigator to restore either a logical volume or a physical drive.

- A logical volume is a volume that does not contain a Master Boot Record (MBR) or the Unused Disk Space.
- A physical volume contains the Master Boot Record and the Unused Disk Space. The Unused Disk Space, however, is typically not accessible to the user.

Copyright © 2004 Guidance Software, Inc.
May not be copied or reproduced without the written permission of Guidance Software, Inc.

Most often, when complying with discovery issues, one must perform a *physical* restore, *not* a logical one. Logical restores are less desirable as they cannot be verified as an exact copy of the Subject media. When a drive is restored for the purposes of booting the Subject machine, a physical restore is the correct choice.

Whether restoring a drive physically or logically, restore the evidence files to a drive slightly larger in capacity than the original Subject hard drive. For example, if restoring a 2-gig hard drive image, restore the image to a 2 to 4-gig hard drive. Restoring media to a drive that is *substantially* bigger than the Subject media can prevent the restored clone from booting at all, possibly defeating the purpose of the restore.

Preparing the Target Media

Preparation of the Target media, the media to which the image is going to be restored, is essential for a forensically sound restore.

- The Target media must be *wiped* (see Chapter 22).
- For logical restores, the Target media must be FDISKed.
- For logical restores, the Target media must be partitioned and formatted with the same file-type system as the volume to be restored to FAT32 to FAT32, NTFS to NTFS, etc.
- For physical restores, do not FDISK, partition, or format the hard drive. Bring up EnCase and restore the image, physically, to the Target media.

Physical Restore

Restoring a physical drive means that EnCase will copy everything, sector-by-sector, to the prepared Target drive, thereby creating an exact copy of the Subject drive. The target drive should be larger than the Subject's hard drive. When EnCase completes the restore it will provide the hash values verifying that the lab drive is an exact copy of the Subject drive. If a separate, independent MD5 hash of the lab drive is run, be certain to choose to compute the hash over only the exact number of sectors included on the suspect's drive so that the MD5 hash will be accurate.

To restore a drive, physically:

- Right-click on the evidence file icon under the **Cases** tab within EnCase and select **Restore...** from the pop-up menu.

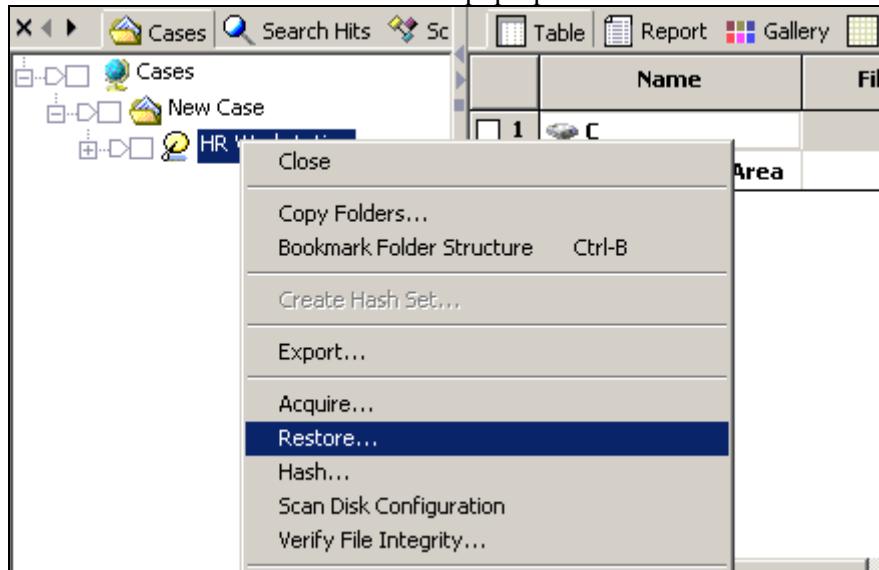


Figure 21-1 right-click for menu, left-click for command

- Select the destination drive from the list of possible destination devices to restore the physical disk to. Click [**Next >**].

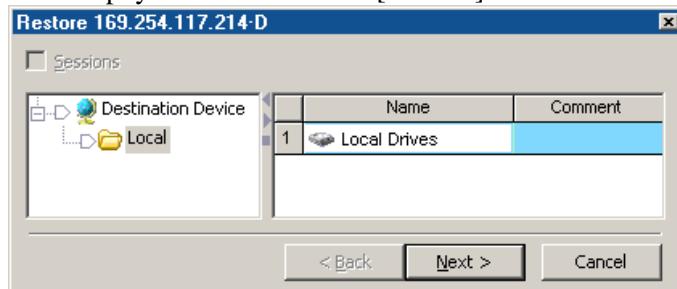


Figure 21-2 Local restore

- EnCase does *not* allow the investigator to restore to Drive 0 as this is typically the drive the operating system is installed on. If the operating system is running on a separate SCSI drive, EnCase will still not allow a restore to IDE 0. If the prepared Target media is Drive 0, another drive will have to be added to the system (as a Master) to store the restored image. Select the drive to restore the image to and click [**Next >**].

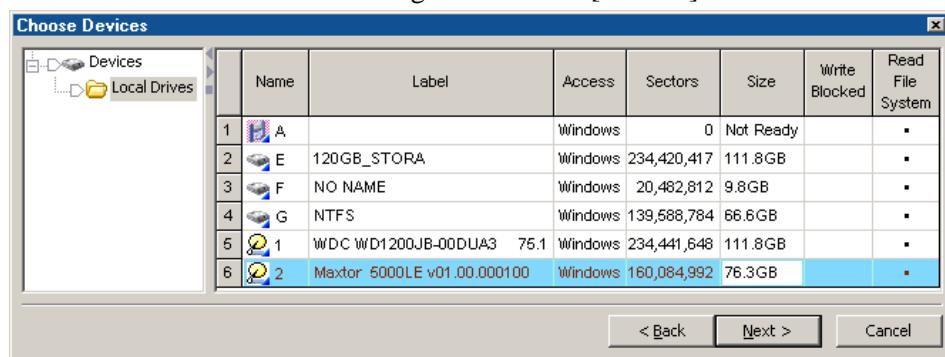


Figure 21-3 Select the local media to restore to

- Target hard drives should be larger in capacity than the original subject hard drive. Therefore, the restored data will never overwrite all sectors on the Target hard drive. EnCase can wipe the remaining sectors of the Target hard drive after the actual data from the evidence file is restored. Wiping remaining sectors is recommended.

- EnCase can also verify the restored sectors to confirm that it is indeed a sector-by-sector copy of the original Subject media.

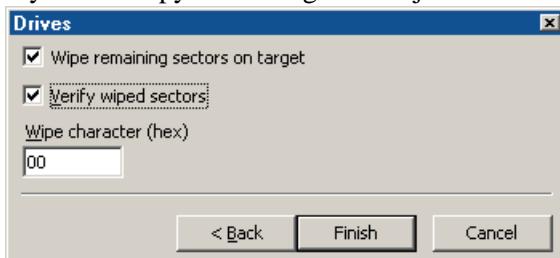


Figure 21-4 Restore options

Sometimes the **Convert Drive Geometry** option is available, other times not. This is entirely dependent on the drive geometry of the original drive in comparison to the restore drive. Drive geometries are of certain "types". Every drive has a certain Cylinders-Heads-Sectors (CHS) drive geometry information. If the Heads and Sectors of the original drive imaged are identical to the target restore drive, then the drives are of the same "type" and the **Convert Drive Geometry** check box will *not* be available. If the drives are of different types (as in, the heads-sectors settings are different), then the **Convert Drive Geometry** check box will be available. For physical restores, check the **Convert Drive Geometry** check box if it is available.

- Click [**Finish**] when done.
- Confirm the restore to the designated drive. Type **Yes** in the field, and then click the [**Yes**] button to start the physical restore. When the restore is finished, a verification message displays such information as any read or write errors and the hash values for both the evidence file and the restored drive. They should match.

If the hash values from the restore do not match, restore the evidence file again following the procedures above. It might be necessary to swap the Target media for correct results.

Logical Restore

Media have different "types" depending on the CHS (cylinders-heads-sectors) information. The same type might have different "cylinders" settings, but their heads and sectors information (the HS in CHS) will be the same. If the heads-sectors information is different, then the media type differs and another target restore hard drive should be used. A logical volume must be restored to a *volume* of the same size, or larger, and of the same type.

To prepare for a logical restore, the Target media should be wiped, FDISKed, partitioned, and formatted prior to restore. Format the Target drive with the same file-type system as the volume to be restored FAT32 to FAT32, NTFS to NTFS, etc.

The procedure for restoring a logical volume is identical to that of restoring a physical device. In the case of the logical volume, right click on the volume in Case view and select **Restore**.

When the logical restore is finished, a confirmation message will be displayed. The computer must be restarted to allow the restored volume to be recognized. Note that the restore volume contains *only* the information that was inside the selected partition.

Booting the Restored Hard Drive

After the restore operation has finished with no errors, remove the Target hard drive from the Storage system and place it into a test system. Switch the power on. Depending what operating system the Subject ran, the test system should now be booting up exactly as the Subject computer.

There are quite a few difficulties that can occur at this stage of the investigation. The most common is that the clone of the Subject drive will not boot. Before trying anything else, check the restored disk using FDISK and verify it is set as an Active drive. If not, set the drive as Active (using the FDISK utility) and this should enable it to boot.

Recommended steps for booting

- Install a sterile restoration drive to your forensic PC. Use a connection other than IDE 0 (EnCase cannot restore a physical drive to IDE 0). Ensure the intended restoration drive is at least as large as the original from which the image was taken.
- Create a single partition on the restoration drive, but do not format it. Using the EnCase report view, note down the disk geometry of the forensic image of the drive you are restoring from (Cylinders, Heads, Sectors), taking care to get the physical geometry correct.
- Restore the forensic image of the PHYSICAL drive to the restoration drive using RESTORE DRIVE in EnCase.

- Make the restored drive active if it is not already. (In a Win2k/XP environment, R/Click MY COMPUTER from your desktop and select MANAGE, then select DISK MANAGEMENT. R/Click on the restored drive and select MAKE ACTIVE.).
- Shut down, and attach the restored drive in as near to the original configuration as possible (e.g. if it was on IDE 0 on the original computer, install it there). This will help the computer to allocate the original drive letters, making .lnk files etc work better.
- Reboot, and set the CHS settings of the restoration drive in the CMOS to the physical geometry of the original drive, which you noted earlier. (This may require overriding the auto-detected geometry).
- The restored disk should now be bootable.



NOTE: NTFS is a complicated file-structure and might not boot in any computer. If the Subject computer is still available, replace the Subject hard drive with the restored clone and try to boot the clone from this system.

Restore Questions

I restored an image to a hard drive, and now, with that hard drive in a separate PC, it's not booting. Why not?

The Cylinders-Heads-Sectors information (CHS) in the Master Boot Record (MBR) from the image does not match the CHS information of the actual hard drive. Reset the CHS information for the MBR. Boot with a DOS boot disk and, at the A:\> prompt, type "FDISK /MBR" (without the quotes). That will reset the Master Boot Record.

Then verify that the MBR has the right io.sys. “Re-sys” the boot drive with the correct sys version. For example, if the subject had Windows 95b, then the hard drive must be sys’d from a Windows 95B created boot disk. At the A:\> prompt, type “SYS C:”.

Chapter 22

Archiving Evidence

It is good forensic methodology to archive all evidence. Guidance Software recommends archiving evidence files as soon as they have been acquired. This way, should evidence files become corrupted during an investigation, the archived copies will still be available. Archive evidence files to either compact disc-recordable (CD-R) or digital versatile disc-recordable (DVD-R).

What Should Be Archived

Archiving EnCase evidence files is identical to archiving any other data. A device to archive the data and media to hold the data are necessary. CD-Rs are popular due to their ease, cost, speed, and endurance. Tape media can fail quite easily after years of storage in vaults, as can removable media like Jaz or Zip disks. CDs and DVDs are much more stable.

When acquiring media, the default evidence file segment size is 640MB, which is designed for CD archiving. Archiving to CD or DVD, requires the following:

- A CD-R or DVD-R burner
- CD-R burning software or similar product for DVD-R
- Many blank CD-R discs or DVD-R discs

*Copyright © 2004 Guidance Software, Inc.
May not be copied or reproduced without the written permission of Guidance Software, Inc.*

Use the disc-burning software to archive the evidence file segments to the optical media. The last evidence file segment is usually smaller than 640MB, and the final CD-R or DVD-R disc frequently has free space. Therefore, in addition to the evidence file, add the following items:

- The version of EnCase used for the examination
- EnScripts used during the examination
- Hash sets used during the examination
- Keywords used during the examination
- The .CASE file for the examination. The CASE file should be burned to a separate CD-R, the two CD-Rs being kept together.
- Any other tools used for the examination

After the Burn – Verify Evidence Files

At the completion of the burn, label the CD-R or DVD-R accurately. Include the date, the related .CASE file, and which number in the sequence it is. Run the **Tools→Verify Evidence FileS** command on the evidence file on each disc to verify that the burn was thorough and the file is intact. The burning software will often report the disc burn was “OK” with no errors; however, one lost 0 or 1 can compromise the evidence. EnCase checks the 32-bit cyclical redundancy checksum (CRC) for each 64 sectors of data in the evidence file segment.

To verify several evidence files or evidence file segments:

- Insert the CD-R or DVD-R with the archived files into the CD-R drive or DVD-R drive.
- Launch EnCase
- From the **Tools** pull-down menu, select **Verify Evidence Files...**

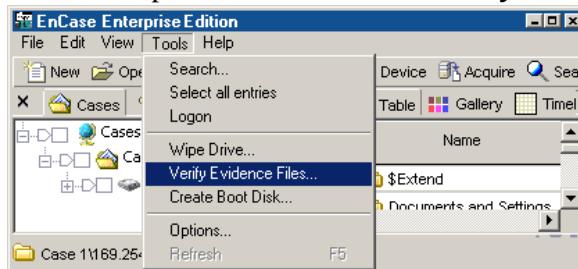


Figure 22-1 Execute the Verify Evidence Files command

- Browse to the archived evidence files or segments on the CD-R or DVD-R, highlight the desired files, and click [Open].

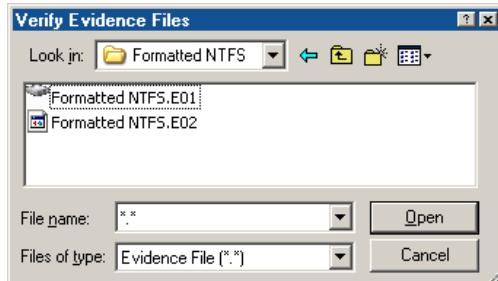


Figure 22-2 Select evidence files to verify

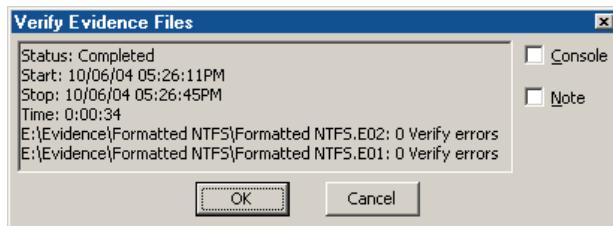


Figure 22-3 Console verification status

After the archival process is complete and the disks labeled accurately, store the CD-Rs / DVD-Rs in a cool, dry place for safekeeping.

Cleaning House

To remove all trace of the evidence files from the Storage hard drive, access the **Wipe Drive...** option from the **Tools** pull-down menu. If wiping the drive is not necessary, it is nevertheless a good idea to archive the data and delete the material in preparation for another case.

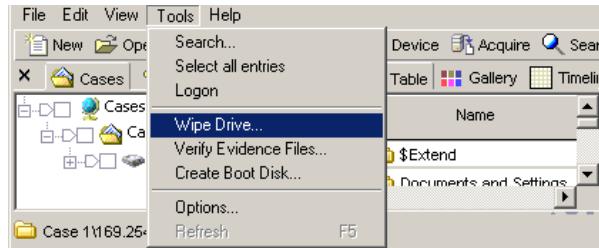


Figure 22-4 Wipe Drive... option

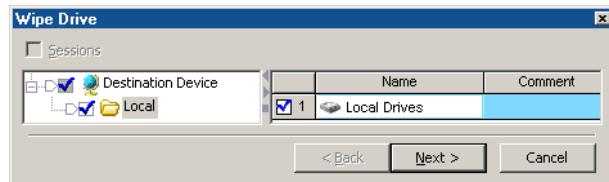


Figure 22-5 Choosing drive to wipe

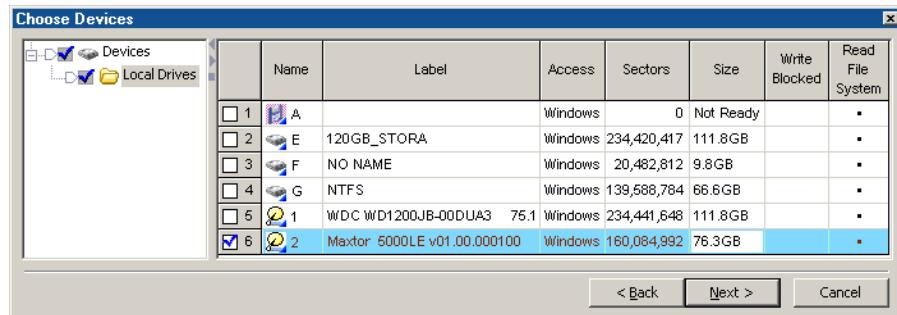


Figure 22-6 Selecting drive to wipe

The boot drive that EnCase resides on is not available to be wiped.

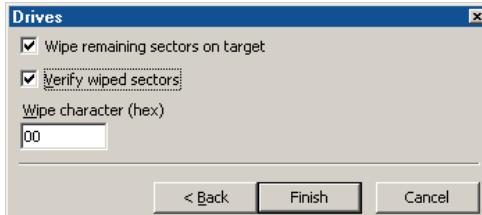


Figure 22-7 Wiping options



Figure 22-8 Wiping confirmation

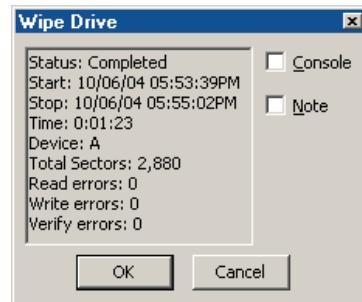
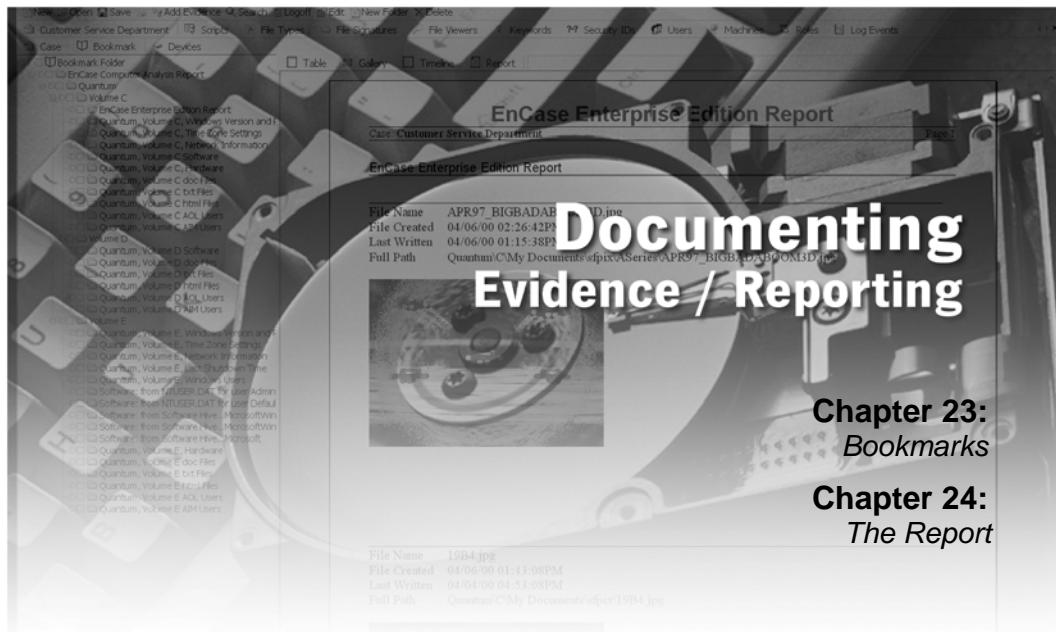


Figure 22-9 Wipe status



NOTE: The "Wipe Drive" feature can only wipe local devices.

*Copyright © 2004 Guidance Software, Inc.
May not be copied or reproduced without the written permission of Guidance Software, Inc.*



Copyright © 2004 Guidance Software, Inc. May not be copied or reproduced without the written permission of Guidance Software, Inc.

*Copyright © 2004 Guidance Software, Inc.
May not be copied or reproduced without the written permission of Guidance Software, Inc.*

Chapter 23

Bookmarks

EnCase allows for files, folders, or sections of a file to be highlighted and saved for easy reference. These marks are called *bookmarks*. All bookmarks are saved in bookmark files, with each case having its own bookmark file. Bookmarks can be viewed at any time by clicking on **View→Bookmarks**. Bookmarks can be made from anywhere data or folders exist.

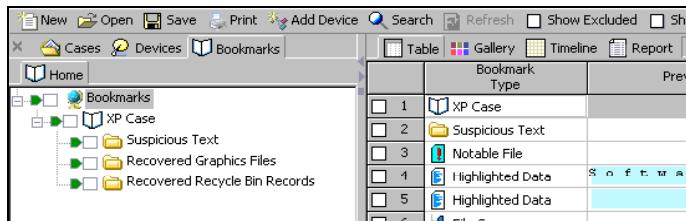


Figure 23-1 The Bookmarks View

Understanding Bookmarks

There are five different types of bookmarks, each preceded by an icon. Below is a list of these icons and their descriptions.

Copyright © 2004 Guidance Software, Inc.
May not be copied or reproduced without the written permission of Guidance Software, Inc.

-  **Highlighted Data Bookmark** – Created by clicking and dragging the mouse over data (“sweeping”) in one of the sub-panes. This is a fully customizable bookmark.
-  **Notes Bookmark** – Used to allow the user to write additional comments into the report. It has a few formatting features. It is not a bookmark of evidence.
-  **Folder Information Bookmark** – To bookmark the tree structure of a folder or device information of specific media. There is no comment on this bookmark. The options include showing the device information, such as drive geometry, and the number of columns to use for the tree structure.
-  **Notable File Bookmark** – A file bookmarked by itself. This is a fully customizable bookmark.
-  **File Group Bookmark** – Indicates that the bookmark was made as part of a group of selected files. There is no comment on this bookmark.
-  **Snapshot Bookmark** – Bookmark containing the results of a System Snapshot of dynamic data for Incident Response and Security Auditing.
-  **Log Record Bookmark** – Bookmark containing the results of log parsing EnScripts.
-  **Registry Bookmark** – Bookmark containing the results of Windows registry parsing EnScripts.

Highlighted Data Bookmark



The Highlighted Data bookmark, also known as a *sweeping bookmark* or a *text fragment bookmark*, can be used to show a larger expanse of text. This type of bookmark is created by clicking and dragging—known as “sweeping”—text or hex in the bottom pane. To sweep an area of data, left-click on the first character and hold down the mouse button. Drag the mouse to the end of the data to be highlighted. Complete the bookmark by right clicking in the highlighted area and selecting **Bookmark Data** from the contextual menu.

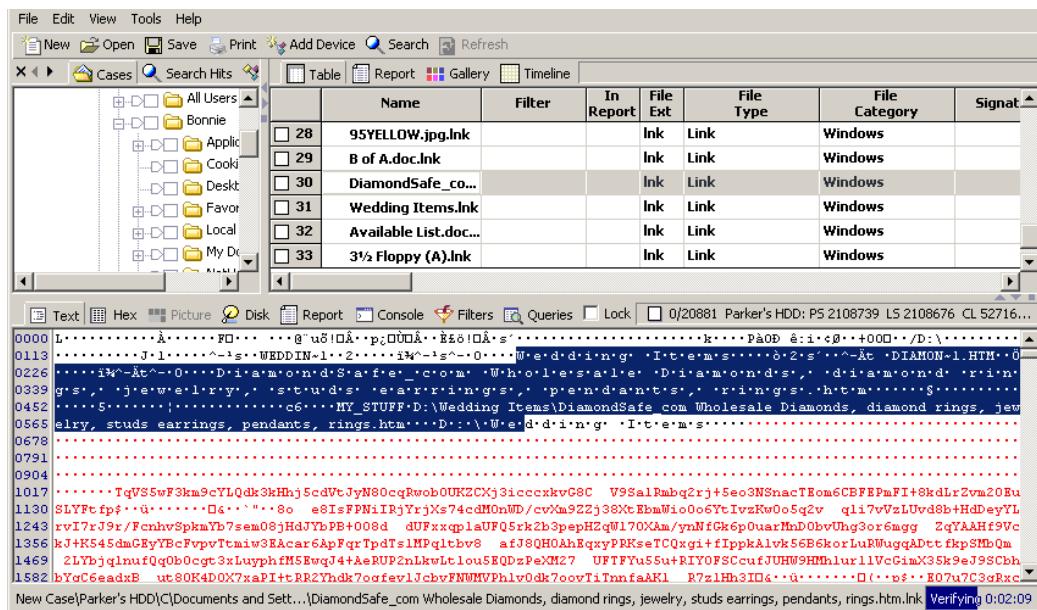


Figure 23-2 Right-click for contextual menu, left-click for command

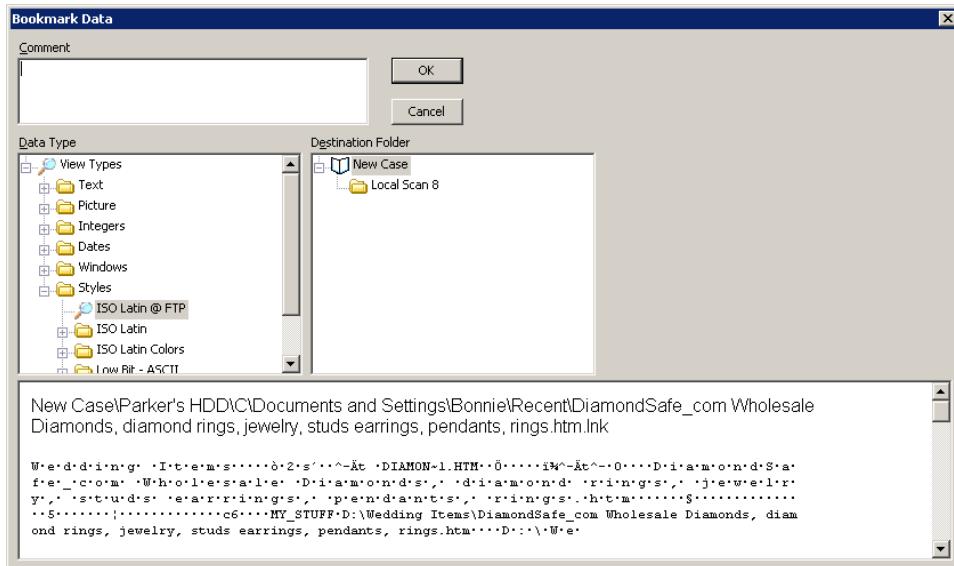


Figure 23-3 Preview of swept text bookmark

In the space provided, type a comment for this bookmark, up to one thousand characters. Select the **Data Type** of the bookmark. There are a variety of methods for displaying the bookmark::

Text

- **Do not Show**

Hides text in the bookmark

- **High ASCII**

High ASCII includes additional ASCII characters (up to 256), which may include foreign language accents, math symbols, trademark and copyright symbols, etc. These characters are not the same on all computers.

- **Low ASCII**

ASCII defines code numbers for 128 characters, which are the alphabetic and numeric characters on a keyboard and some additional characters such as punctuation marks.

- **Hex**

Hexadecimal. The base 16 numbering system, sometimes used as a short way of representing binary numbers. The digits 0-9 are used, plus the letters A-F, which represent the numbers 10 to 15. The farthest-right digit is the ones place; the digit next to the left is the 16s place; the next place to

the left is $16^2 = 256$, etc. Each place is 16 times the place immediately to the right of it.

- **Unicode**

A character set that uses 16 bits (two bytes) for each character, and therefore is able to include more characters than ASCII, which is based on 8-bit characters. Unicode can have 65,536 characters and therefore can be used to encode almost all the languages of the world. Unicode includes the ASCII character set within it.

Picture

- **Picture**

EnCase can view natively JPG, GIF, EMF, TIFF, BMP, AOL ART and (occasionally) PSD file formats.

- **Base64 Encoded Picture**

Picture encoded for e-mail transport in Base64.

- **UUE Encoded Picture**

Picture encoded for e-mail transport with UUE.

Integers

- The selected data is displayed in the integer format. Options are **8-Bit Integer**, **16-Bit Integer**, **16-Bit Big-Endian**, **32-Bit Integer** and **32-Bit Big-Endian**. Big Endian is an order in which the "big end" (most significant value in the sequence) is stored first (at the lowest storage address).

Dates

- **DOS Date**

Packed 16-bit value that specifies the month, day, year, and time of day an MS-DOS file was last written to

- **UNIX Date**

A Unix timestamp (in seconds) based on the standard Unix epoch of 01/01/1970 at 00:00:00 GMT

- **UNIX Text Date**

A Unix timestamp (in seconds) based on the standard Unix epoch of 01/01/1970 at 00:00:00 GMT, in text format

- **HFS Date**

Copyright © 2004 Guidance Software, Inc.

May not be copied or reproduced without the written permission of Guidance Software, Inc.

A numeric value on a Macintosh that specifies the month, day, year, and time that a Macintosh file was last written to

- **HFS Plus Date**

A numeric value on a Power Macintosh that specifies the month, day, year, and time that the file was last written to

- **Windows Date/Time**

A numeric value on a Windows system that specifies the month, day, year, and time that a file was last written to

Windows

- **Partition Entry**

Characters indicating the beginning of a Windows partition entry

- **DOS Directory Entry**

MS-DOS uses one directory entry for each file and subdirectory. These characters can be interpreted by EnCase to view the DOS directory entry.

- **Win95 Info File Record and Win2000 Info File Record**

These are the structures that hold the paths and deleted dates for files in the recycle bin. These structures are found in a file called INFO or INFO2, thus the name.

Styles

- **Text Styles (ISO Latin @ FTP, ISO Latin, ISO Latin Colors, Low Bit – ASCII, etc.)** See *Chapter 20: Foreign Language Support* for directions on creating and editing Text Styles.

Select a destination folder to contain the bookmark. When finished, click [OK].

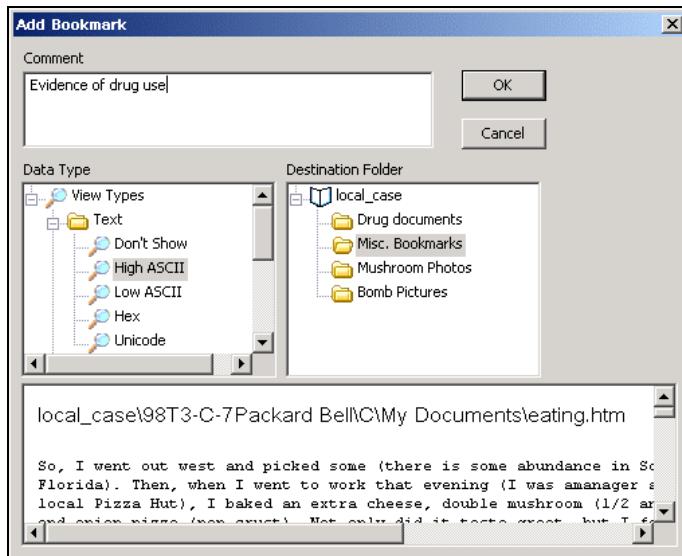


Figure 23-4 Adding a comment

View the bookmark in the **Bookmarks** table.

Bookmark Type	Preview	Comment
1 Notable File		
2 Highlighted Data	Software \ Mi	
3 Highlighted Data		
4 Shown		

Figure 23-5 Comment / bookmark text, table view

Switch to **Report** view for the report display.

Text Fragments	
Final Report Text Fragments	
<u>Text Fragments</u>	
1) My Big Case\98T3-C-7Packard Bell\WINDOWS\Temporary Internet Evidence of drug use	
<p>So, I went out west and picked some (there is some abundance in South Florida). Then, when I went to work that evening (I was a manager at the local Pizza Hut), I baked an extra cheese, double mushroom (1/2 and 1/2), and onion pizza (pan crust). Not only did it taste great, but I found the buttons on the cash register changing places.</p>	

Figure 23-6 Comment / bookmark text, Report view

Text fragment bookmarks are one of the most common forms of bookmarking. They are extremely useful as they place evidentiary data directly into the report.

Notes Bookmark

The Notes bookmark gives the investigator a great deal of flexibility when adding comments to the report. This bookmark has a field reserved only for comment text and can hold up to one thousand characters. It also contains formatting options including italics, bold, changing font size, and also changing the indent of the text. To add a note, right click the folder where the note is to be added in the left pane and select **Add Note....**

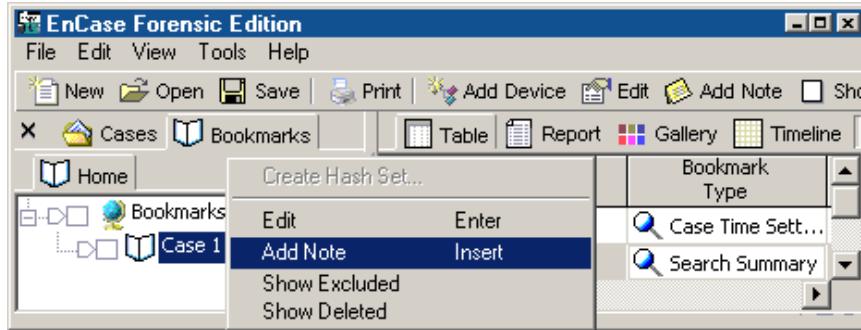


Figure 23-7 Adding a note

In the **Add Note Bookmark** window, type the text to be added into the note, apply formatting options and click [OK]. Check the **Show in report** box to have the note appear in Report view.

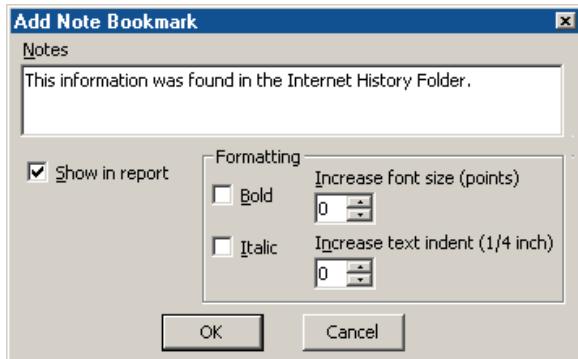
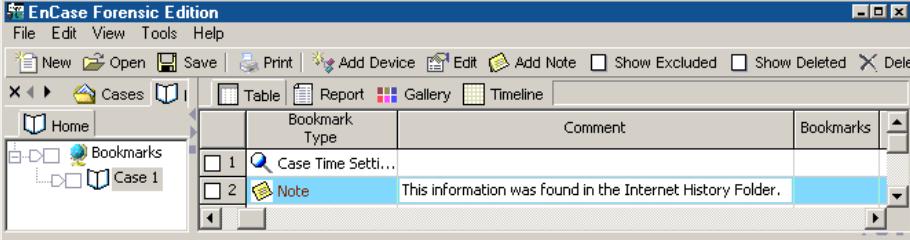


Figure 22-8 Adding new note text

View the bookmark in the table.



The screenshot shows the EnCase Forensic Edition interface. The main window title is "EnCase Forensic Edition". The menu bar includes File, Edit, View, Tools, Help, and several icons for New, Open, Save, Print, Add Device, Edit, Add Note, Show Excluded, Show Deleted, and Delete. Below the menu is a toolbar with icons for Cases, Table, Report, Gallery, and Timeline. A sidebar on the left shows a tree structure with "Home", "Bookmarks", and "Case 1". The main pane displays a table with three columns: "Bookmark Type", "Comment", and "Bookmarks". There are two entries: entry 1 is a search icon with the comment "Case Time Setti..."; entry 2 is a note icon with the comment "This information was found in the Internet History Folder." The "Report" tab is selected at the top of the main pane.

Bookmark Type	Comment	Bookmarks
1	Case Time Setti...	
2	Note	This information was found in the Internet History Folder.

Figure 22-9 Note in Table view

Switch to Report view and review the results.

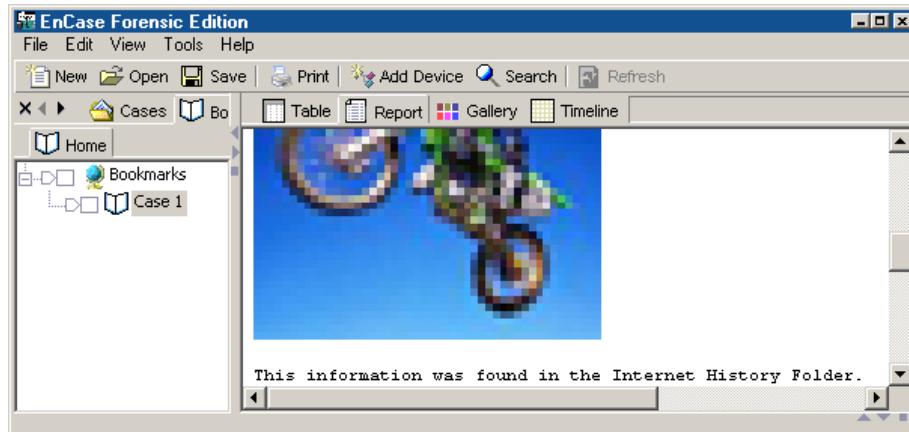


Figure 23-10 Note in Report view

Notes bookmarks can be copied and placed anywhere within the report.

Folder Information Bookmark



The Folder Information bookmark is used to bookmark folder structures or devices. By bookmarking a folder structure, the entire directory structure of that folder and its children can be shown within the report or bookmarked for later analysis. Individual devices, volumes, and physical disks can be bookmarked as well. This will show important device-specific information in the final report.

This type of bookmark is useful for marking directories that contain unauthorized documents, pictures, and applications. It is also a great way to show specific information about the type of media in the Case.

To bookmark a folder, right-click on that folder in the right-hand pane of the “Case” view and select **Bookmark Folder Structure** from the context menu.

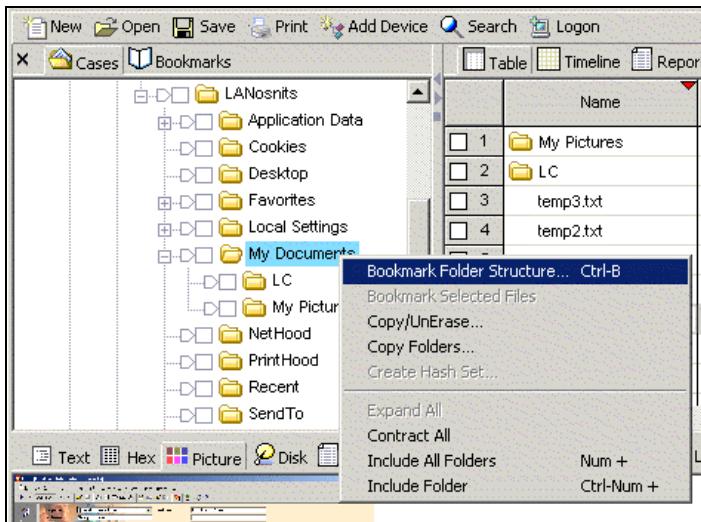


Figure 23-11 right-click for menu, left-click for command

In the “Add Folder Bookmark” window, select the **INCLUDE DEVICE INFORMATION** check box. This will show details about the volume that the folder resides on in the report. **COLUMNS** will split up the directory structure into what is specified here. If “3” is chosen, the directory structure will be shown in three columns down the page. Finally, choose where the bookmark will reside in the final report (Figure 23-12).

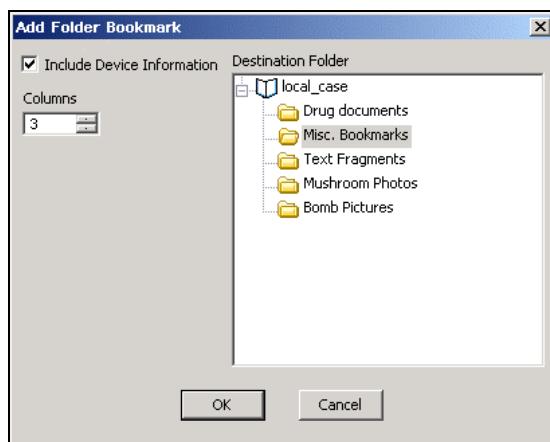


Figure 23-12 Selecting a folder to contain a “Folder Bookmark”
View the bookmark in the “Table” view of the “Bookmarks” tab.

Bookmark Type	Preview	Comment	Page Break	Show Picture	Entry Selected	File Offset
1 Local Scan 8					•	
2 Event Logs		Contains info extra			•	
3 Folder Information					•	

Figure 23-13 The folder information bookmark in the Table view

Switch to **Report** view and see the results in the report.

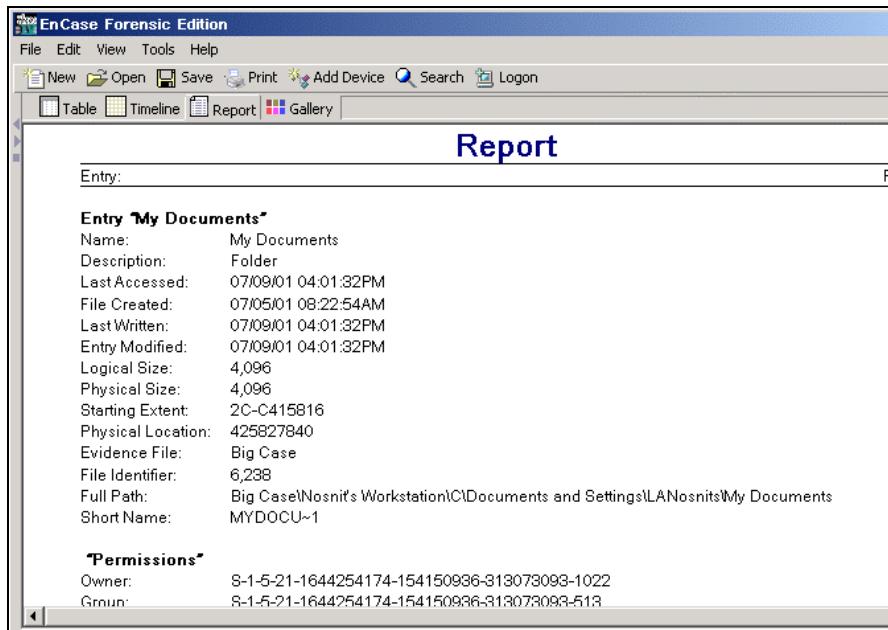


Figure 23-14 My Documents folder bookmarked and in report

Notable File Bookmark



Notable file bookmarks are used to identify individual files that contain important information to the current Case. By bookmarking a file via this method, the contents of the file are *not* bookmarked. Only the *details* about the file (column headings in the **Cases** view) are displayed in the report. To make a notable file bookmark, highlight the file with one left-click, then right-click on the file in the table view of the **Cases** tab and select **Bookmark File** from the context menu.

This type of bookmark is used extensively for marking files that will be exported out of the case. It is also useful for showing specific fields such as dates and time stamps of important files while it also allows for a comment on the individual file itself.

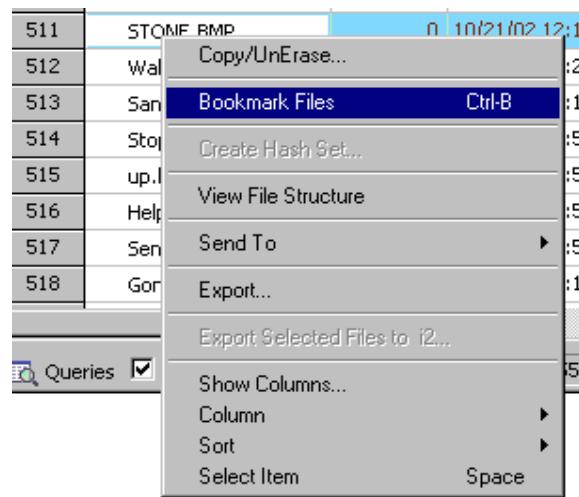


Figure 23-15 Bookmarking a file

In the **Bookmark File** window, type a comment for the file and select a bookmark location within the final report to store the file.

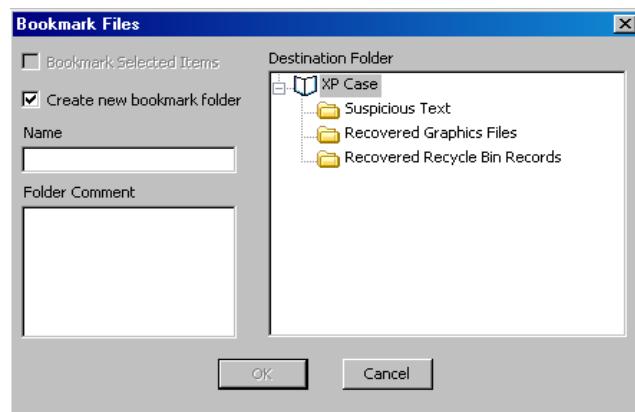


Figure 23-16 Adding a comment, selecting a folder

Now view the bookmark in the table view of the **Bookmarks** tab.

	Bookmark Type	Preview
1	Notable File	
2	Highlighted Data	S o f t w a r e
3	Highlighted Data	
4	File Group	

Figure 23-17 The bookmark in the desired folder

Switch to **Report** view and see the results in the report. Notice the default information shown for the bookmarked file:

- Path of the file
- Comment that was added when the bookmark was created

Add to this information by right clicking on the *folder* that contains the notable file and selecting **Edit**.



Figure 23-18 Edit Bookmark folder

The **Edit Bookmark folder** option will open. By editing this folder information, everything contained within the edited folder will assume the properties of that folder. A comment can be added to the folder. The format window is used to display which fields will be shown for the files contained within the folder. Fields can be added from the **Fields** box on the right by double-clicking the desired field.

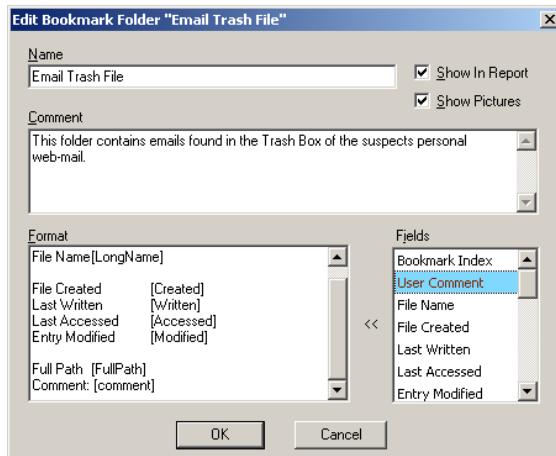


Figure 23-19 Selecting fields for the Report view

After the properties for the parent bookmark folder are changed, the report will reflect the changes that have been made. Notice below that all of the fields that were added in the above folder properties are now displayed for the notable file.

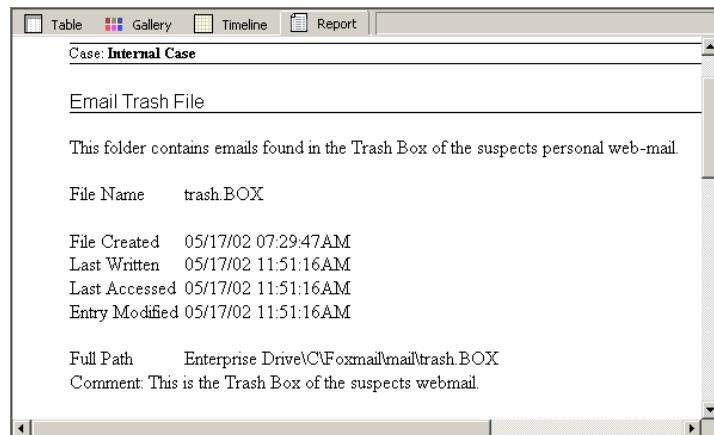


Figure 22-20 The report with the added fields

File Group Bookmark



File group bookmarks are similar to notable file bookmarks, except that they are used to bring attention to *groups* of files, not individual files. This type of bookmark is used to identify a group of files that contain important information to the current case and are relevant to all other files within the group. By bookmarking a group of files, the contents of the files are not bookmarked; however, the details about the file (column headings in the **Cases** view) can be displayed in the report. To bookmark a group of files, blue-check the files in the **Cases** view and then right-click in the right pane and select **Bookmark Files** from the context menu.

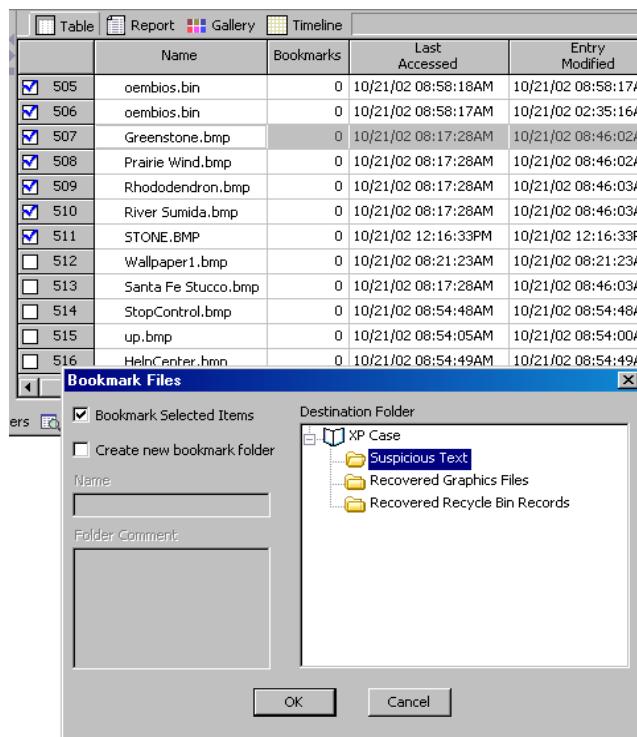


Figure 23-21 File Group bookmark

In the **Bookmark Files** window, ensure the **Bookmark Selected Items** box is checked. The file group can be saved in an existing bookmark folder or in a new bookmark folder.

If a new folder is created, a comment can be entered for that folder when it is created. Specify where to store the file group.

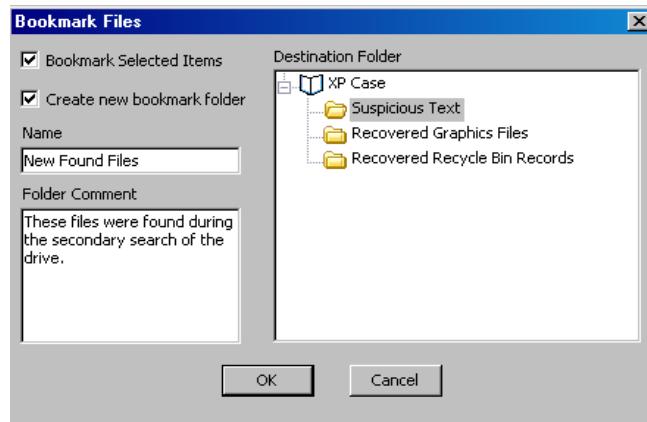


Figure 23-22 Selecting a folder for the bookmarks

View the bookmarks in the Table view of the **Bookmarks** tab..

	Bookmark Type	Preview
1	File Group	
2	File Group	
3	File Group	
4	File Group	
5	File Group	
6	File Group	
7	File Group	

Figure 23-23 Viewing the bookmarks in the folder

Switch to Report view to observe the results. Notice that the default information shown for the files that were bookmarked is the full path of each file. Right click on the folder that contains the file group, and select **Edit** to change this information.



Figure 23-24 Editing Bookmark folder information

The **Edit Bookmark** folder will open. By editing this folder information, everything contained within the edited folder will assume the properties of that folder. A comment can be added to the folder. The format window is used to display which fields will be shown for the files contained within the folder. Fields can be added from the **Fields** box on the right by double-clicking on the desired field.

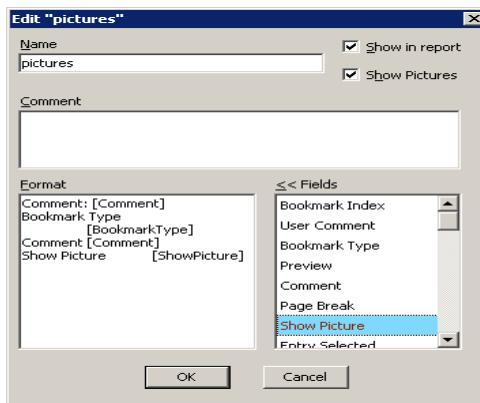


Figure 23-25 Selecting fields to display in the Report view

After the properties for the parent bookmark folder are changed, the report will reflect the changes that have been made. Notice in the figure below that all of the fields that were added in the above folder properties are displayed for the entire file group.

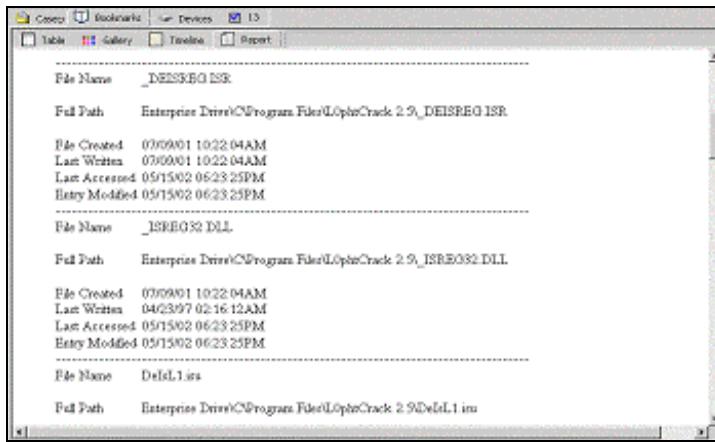


Figure 23-26 Viewing the fields in the report

This type of bookmark is used extensively for marking files that will be exported out of the case and for groups of files that contain similar information. File group bookmarks differ from notable file bookmarks in that a comment *cannot* be placed on individual files that have been bookmarked in this way. The only way to comment with this type of bookmark is by either making a folder comment on the containing folder or by placing a note in front of one of these files.

Snapshot



For more information on the Snapshot bookmark, please refer to *Chapter 18: Advanced Analysis*

Log Record



A new bookmark type is the Log Record bookmark. This bookmark type is designed for holding log file records created with new EnScript functions.

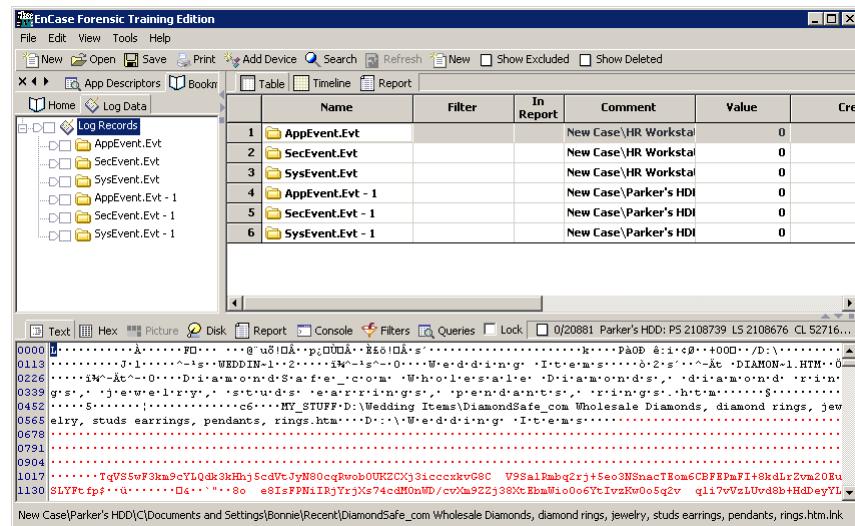


Figure 23-27 Log Data Bookmark tab

Click on the Log Data tab, right of the Bookmark Home tab. In this case, four of the evidence files in the case had Windows event logs. The Log Data view contains columns for the Event ID (Name), the created date, accessed data, and comments for the log message. The In Report flag can be enabled with [Ctrl][R] to create a report of the log files.

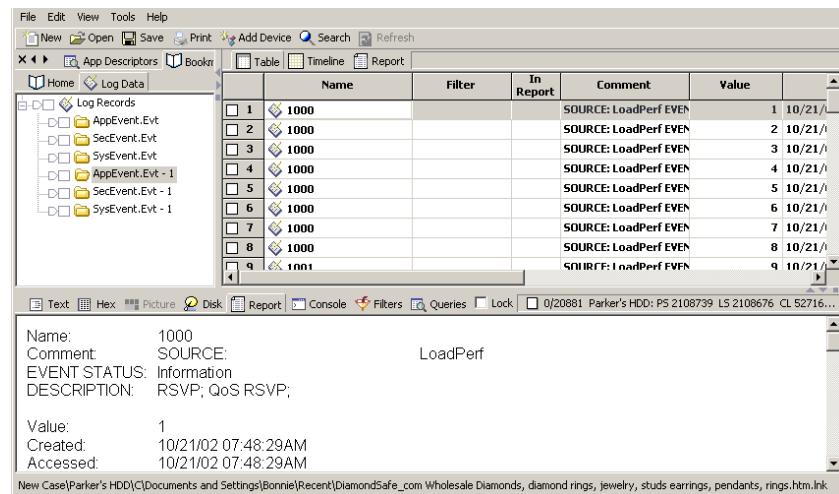


Figure 23-28 Log File data columns

Selecting the Report view will enable the examiner to build and export a report. See *Chapter 16: The Report* for more information.

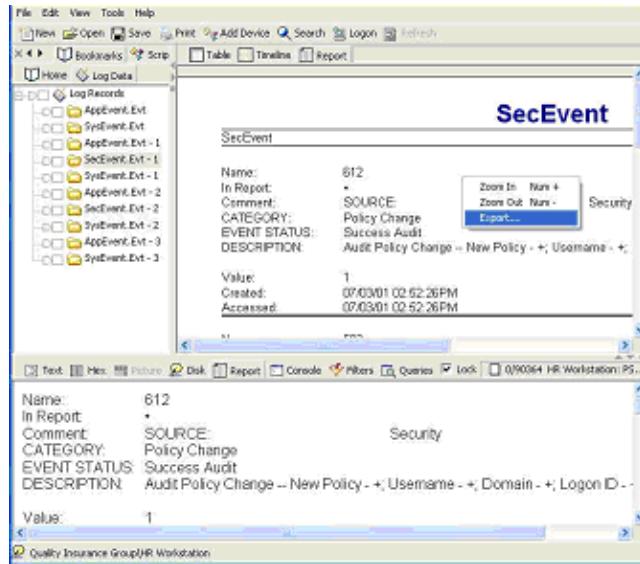


Figure 23-29 Log Data report

The power of the new Log Data class becomes very clear in the Timeline view.

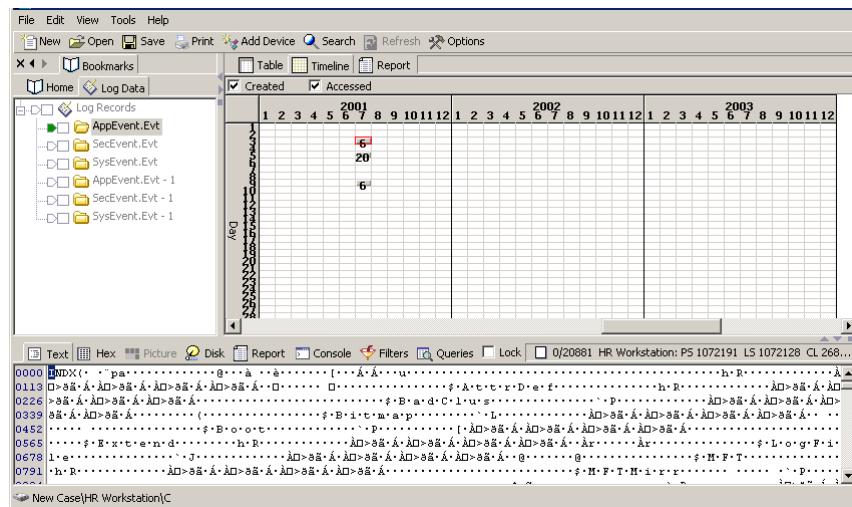


Figure 23-30 Log File data columns

Registry Data Bookmark



Another new bookmark type is the Registry bookmark. This bookmark type is designed for holding registry entries parsed with new EnScript functions.

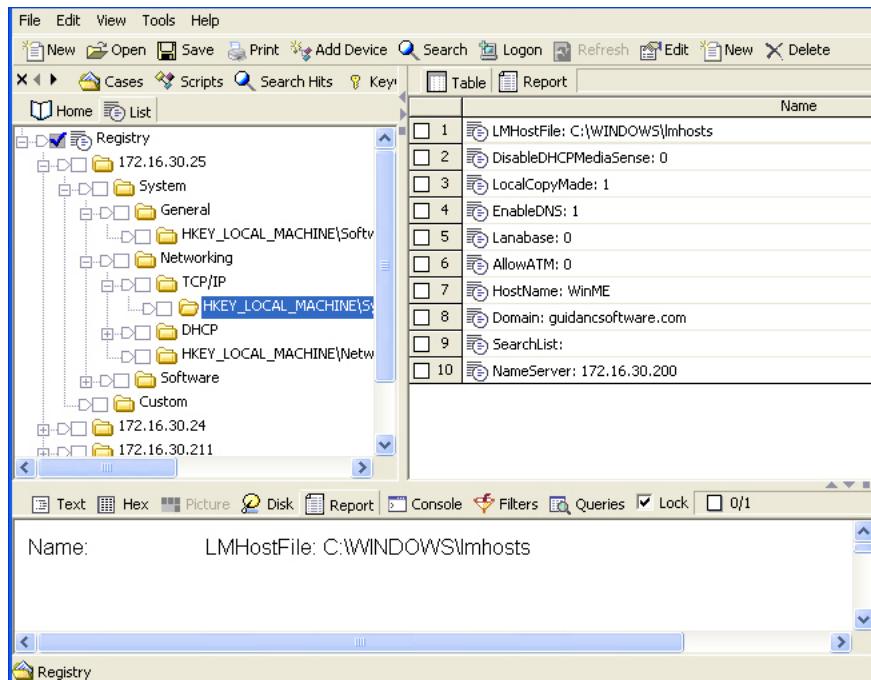


Figure 23-31 Registry bookmarks

New Documentation Options for Threads

Examiners now have the option to bookmark the results of analysis threads into a note and/or write the results to the console. Examiners should be aware that some EnScripts clear the console and write their results to the console.

The following threads have the option to bookmark the results:

- Acquire
- Verify Single Evidence File
- Searching, Hash and File Signature Analysis
- Hash device

- Copy/Unerase files and folders
- Restore
- Recover Folders
- PowerIndexing (see section on Xanalys)

New Bookmark Options

The Bookmark view has many new options that operate like the search hits. Most of the options were included in previous releases of EnCase V4.

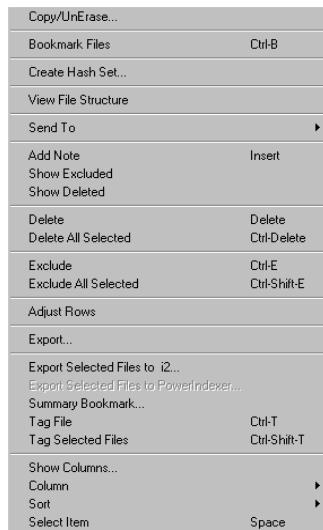


Figure 23-32 Bookmark options

The most significant options are the ability to exclude and delete bookmarks, the same way an examiner can control and display search hits. An examiner can delete or exclude individual or selected bookmarks, or a bookmark folder. Deleting or excluding the parent folder affects all children bookmarks. Bookmarks or bookmark folders that are deleted when the case file is closed are permanently deleted, just as search hits are controlled. An examiner can exclude bookmarks or bookmark folders he or she does not want included in a report, but wants to retain in the case file for reference or research. This is a superior implementation of the “Recycle Bin” concept of EnCase V3.

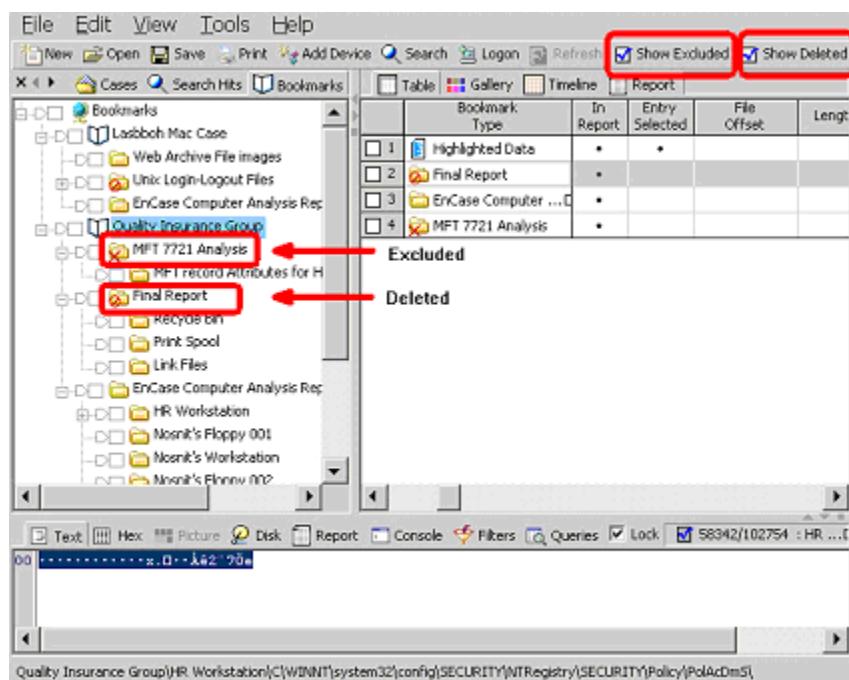


Figure 23-33 Deleted and excluded bookmark folders shown

Case Time Zone Settings can be bookmarked from the bookmark options window. Right-click on the bookmark root of the case, and choose **Summary Bookmark...**

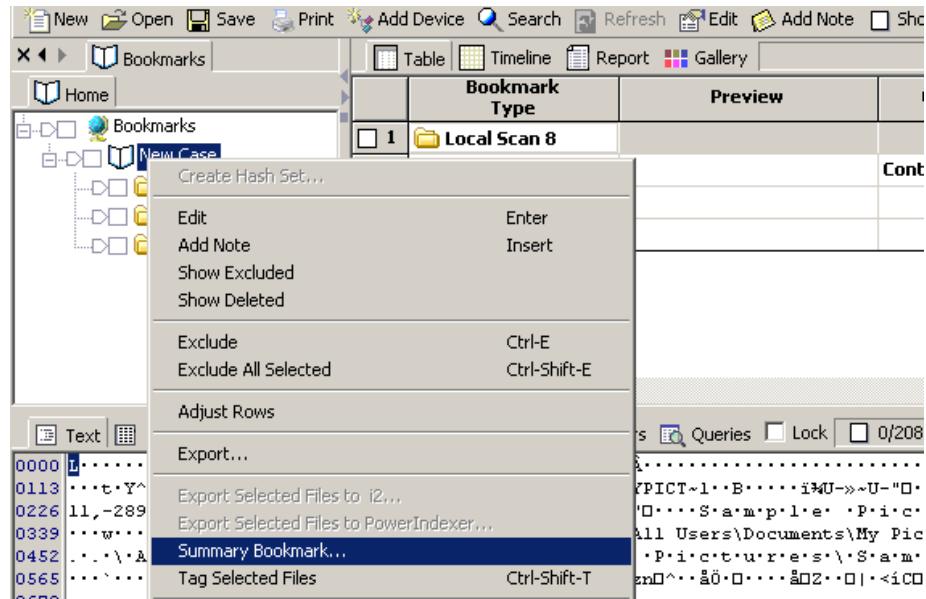


Figure 23-34 Choose Summary Bookmark

Select Case Time Settings to create a bookmark of the time zone settings.

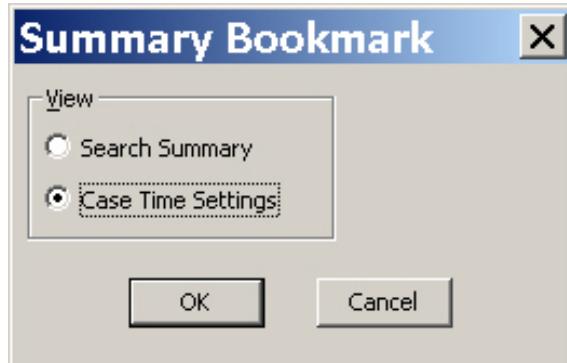


Figure 23-35 Choose Case Time Setting

The Case Time Setting bookmark is placed on the root of the case bookmark tree, and can be moved to any location in the case bookmark structure.

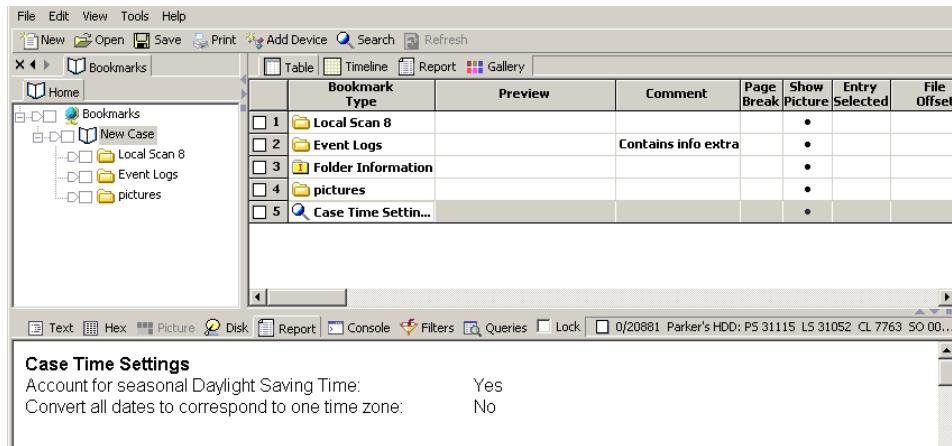


Figure 23-36 Case Time Settings bookmark

Move or Copy Bookmarks

You can move or copy selected bookmarks from one folder to another. Blue-check the table entries to select the desired bookmarks. Right-click, hold, and drag the cursor to the new folder. Release the mouse to show the **Move Here**, **Copy Here**, or **Cancel** options. Left-click on the desired option to Move (Cut & Paste) or Copy the bookmarks to the new folder, or Cancel the action.

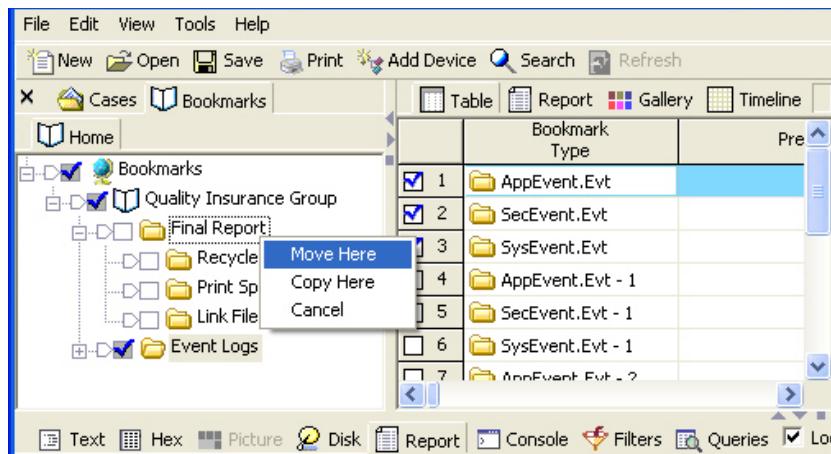


Figure 23-37 Move or Copy Bookmarks

Notable (Bookmarks view)

The **Notable** column is used to highlight and identify individual search hits or swept bookmarks in the right pane, in either the *Search Hits* or *Bookmarks* view, for inclusion in a report. The option can be turned on or off by selecting the target file, right-clicking the **Notable** column, and selecting Notable from the menu. You can also blue-check multiple files, right-click on one and select Notable – Invert Selected Items to make the selected items Notable or remove the classification, depending on the current status of that file

*Copyright © 2004 Guidance Software, Inc
May not be copied or reproduced without the written permission of Guidance Software, Inc.*

Chapter 24

The Report

Presenting the Findings

The final phase of a forensic examination is reporting the findings. The report should be organized and presented in a readable format that the target audience will understand. The format and presentation of the report should be considered when the evidence is first received. EnCase is designed to help the investigator bookmark and export the findings in an organized manner so the final report can be generated quickly upon completion of the examination.

EnCase provides several methods for generating the final report. Some investigators prefer to break up the final report into several sub-reports inside a word-processing program, with a summary report document directing the reader to their contents. Other investigators create paperless reports burned to compact disc, using a hyper linked summary of the sub-reports and supporting documentation and files. EnCase gives the investigator the flexibility to customize and organize the contents of the final report.

The following sections outline the steps necessary to compile a clear, organized report of the findings that can be provided to management or judicial officials in an easily understood format.

The EnScript Library, available at <http://www.guidancesoftware.com> contains an Initialize Case EnScript for creating a report with important drive geometry and acquisition information right away. This report is a single large report that could be several hundred pages in length when all bookmarked evidence in the case is included.

```

/* Last Modified: November 14, 2002

Features:
- File Integrity
- Drive Geometry
- Partitions
- Volume info
- Windows Version and Reg info
- Windows Time Zone Settings and Active Time bias
- Windows network settings
- Windows last shutdown
- Windows users
- Software
- Hardware (w/CPU)
- doc's, html's, txt's
- aim users & buddy list
- aol users & buddy list & ARL
(tested only for AOL 5.0, 6.0, 7.0)
- Mapped drives extracted from NTUSER.DAT

**NOTE bug on WINDOWS NETWORK SETTINGS with 9x. think it's only 95

  
```

Figure 24-1 Initialize Case EnScript

Central to the final report is the information contained in the evidence file, documenting the chain of custody and characteristics of the physical media. To include this information in the final report, right-click on the physical disk and select **BOOKMARK FOLDER**.

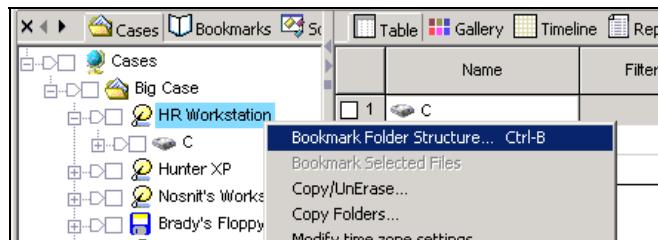


Figure 24-2 Bookmark the physical disk

In the **Bookmark Folder Structure** window, check the **Include Device Information** box. Type “0” in the **Columns** box to prevent the folder structure

from being displayed. Click on the desired folder in the right pane in which to place the “Folder Bookmark”.

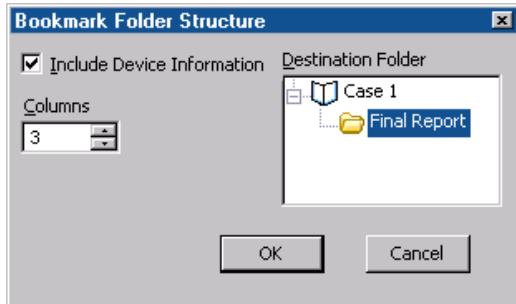


Figure 24-3 Adding the bookmark to the report

In the example above, a Folder Information bookmark will be placed in the “Final Report” folder. Go to **Bookmarks** view and select the root **Bookmark** folder in the left pane. The new Folder Information bookmark, containing the Case information and file integrity, is placed by default at the bottom of the **Bookmark** folder. The order of the bookmarks can be arranged in any folder by selecting the bookmark’s number in the far left column and dragging the bookmark into the desired location.



Note When using the drag and drop facility, ensure the green “All Files” trigger is NOT on. Otherwise, dragging and dropping bookmarks does not work.

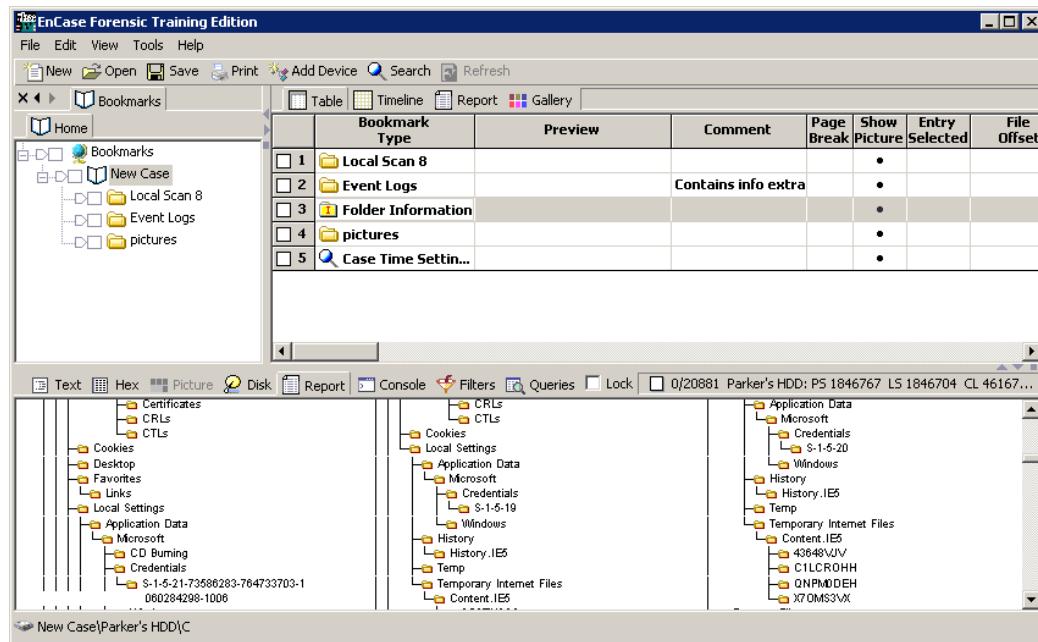
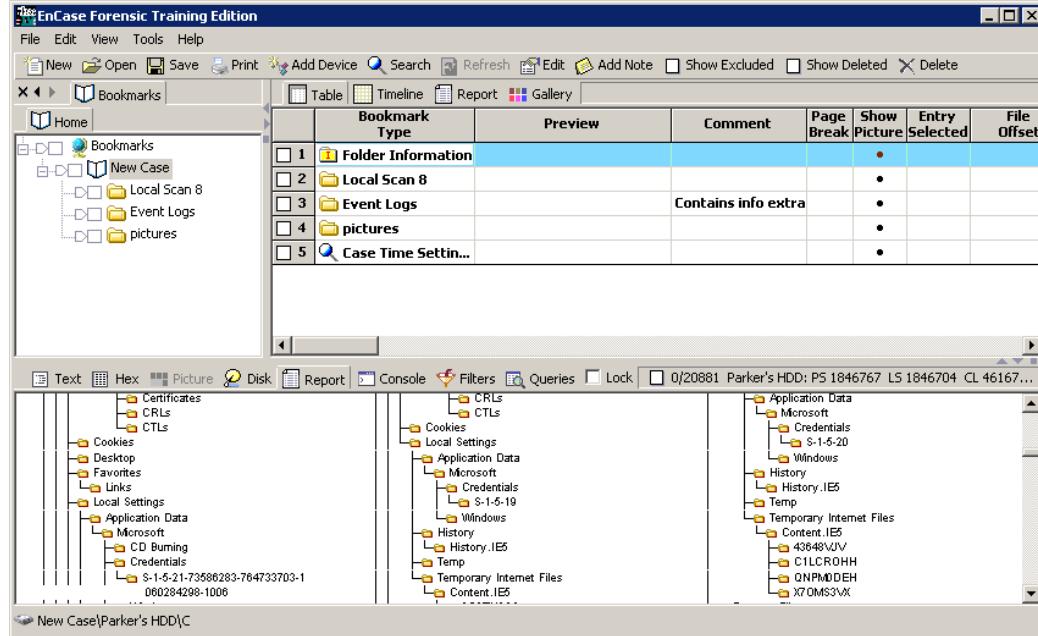


Figure 24-4 Reordering bookmark position



Copyright © 2004 Guidance Software, Inc.
May not be copied or reproduced without the written permission of Guidance Software, Inc.

Figure 24-5 Reordered bookmark folder

To add the volume parameters of a partition to the final report, return to the “Cases” tab. Right-click on the volume and select **Bookmark Folder**.

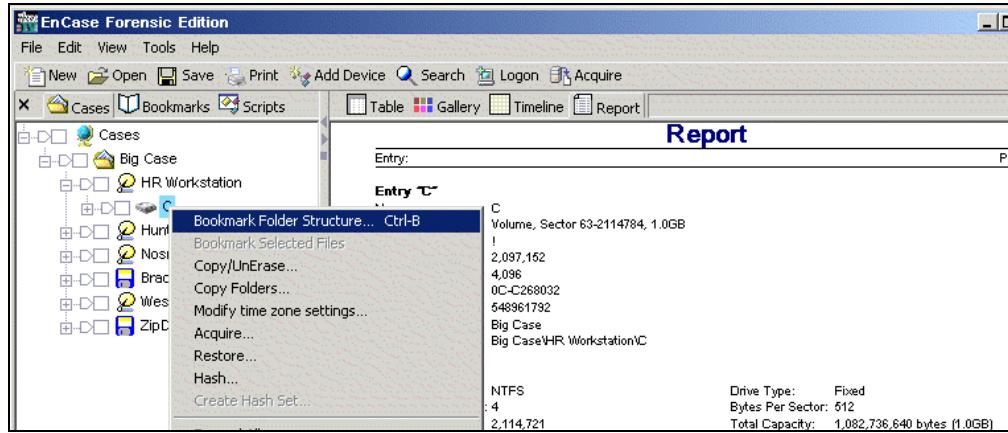


Figure 24-6 Right-click on the volume and select BOOKMARK FOLDER STRUCTURE

Place the folder bookmark in the “Bookmark” folder. Check the **INCLUDE DEVICE INFORMATION** check box. Leave the **COLUMNS** set at “3” to show the folder structure of the partition, or set to “0” to omit the folder structure from the report.

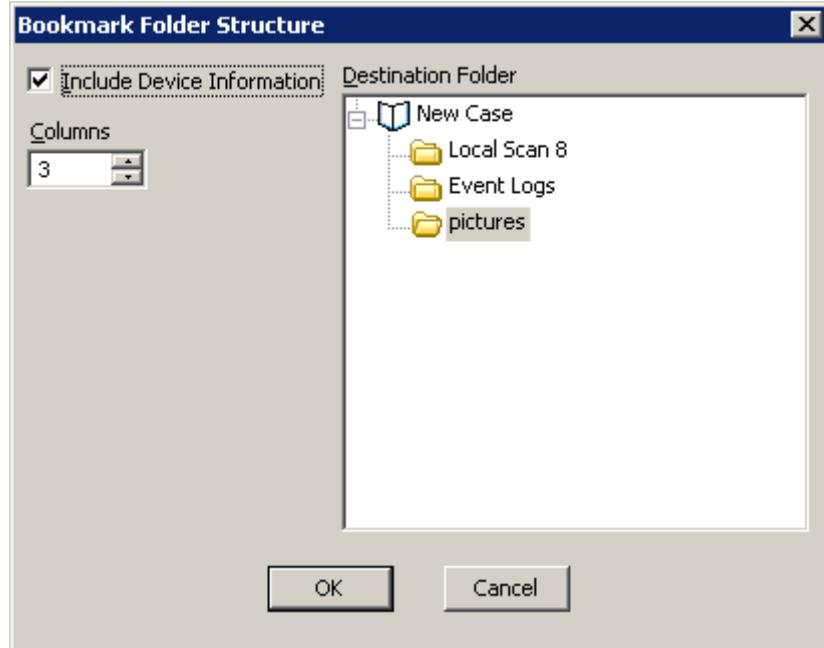


Figure 24-7 Adding the volume parameters to the report

To move the volume parameters report up to the second row, below the physical drive “Folder Information” bookmark, drag to row 2.

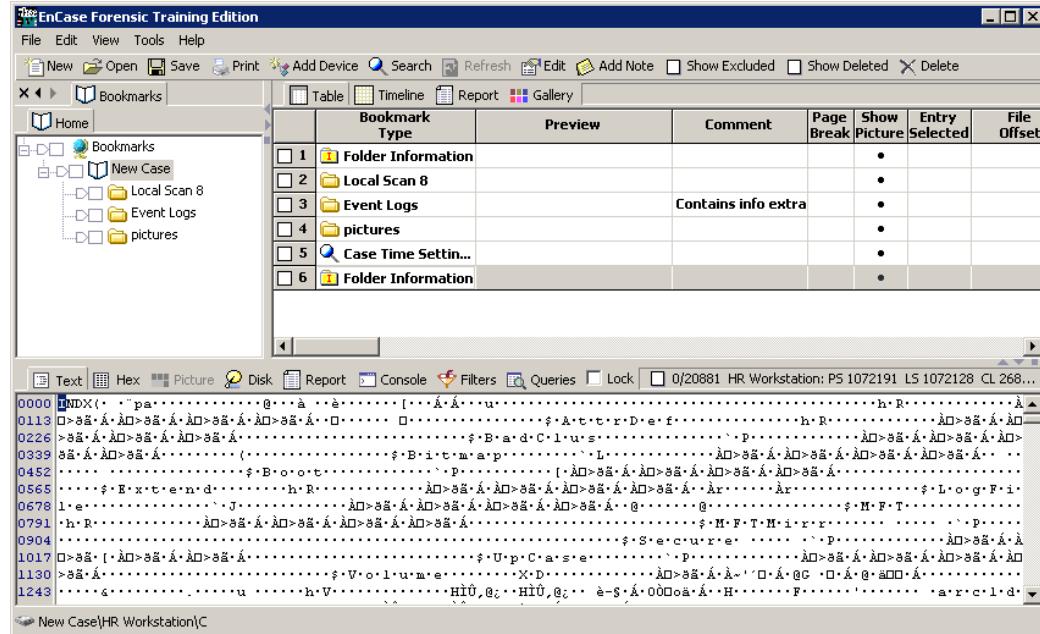


Figure 24-8 Reorder the bookmark

Click on the “Report” view tab in the right pane and select the “Bookmark” folder. The EnCase final report will be generated in the order listed within the bookmark folder. The bookmark sub-folders, such as Search Results, Documents, Pictures, or others, can also be reordered.

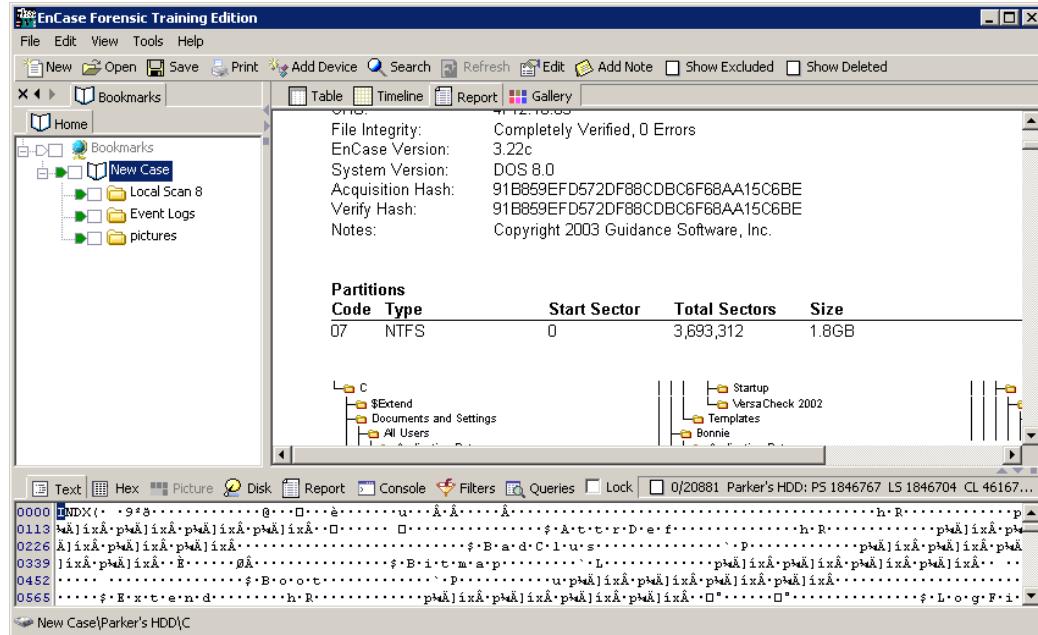


Figure 24-9 Final report including physical disk and volume information

Reordering Bookmarks for Reports

Bookmarks can be sorted on any of the columns, up to five sub-sorts. Some situations in which sorting is very helpful is illustrated by a EnCase examiner in Canada:

1. Sort JPGs by file size in Table view and switch to Gallery view to examine them. The bigger images are then in one spot. The bigger is most often the unauthorized images.
2. Sort images by file size in table and examine by file size. Identical looking images with different hash values may be indications of Steganography
3. Sort images by creation date in table view and examine in the Gallery view. The images downloaded from the Internet can now be viewed in the chronological order that they were downloaded

4. Bookmark the images downloaded from the Internet that are most relevant. Go to Bookmarks. Ensure sort by date created and go to Report view. The images are now in the report in the order they were downloaded.
5. Keystroke loggers and stealth screen capture software can create .JPGs that are recoverable. These need to be added to a report in the order they were created to show a logical pattern.
6. Word documents in table view of relevance are bookmarked. A report is created listing the documents in the chronological order they were created
7. File Finder EnScript creates a bookmark folder of the recovered .JPGs and adds a comment field to each image. Sort by comment field and the recovered images can be grouped per the type of camera that took them.
8. Surveillance cameras set up to take hidden cam shots every 10 seconds are sometimes identified in unallocated space and the only way to sort to prepare a logical sequence of images is to experiment with sorting by starting extent or physical location. A report prepared with images sorted in sequence makes the difference of what appears to be a movie, to a scrambled assortment of images with no cohesiveness.
9. Text files are sometimes located that contain chat sessions with individuals, often in the hundreds. These can be bookmarked and included in a report. The objects must be sorted chronologically in the report to give it any meaning.

After the columns are sorted in the desired order, right-click in the Table view and choose Adjust Rows. This sets the bookmark entries in the current sort order for the report. This prevents examiners from accidentally losing an import report created by improperly clicking the mouse. The report stays in the last format, until the Adjust Rows function is set again for a new report.

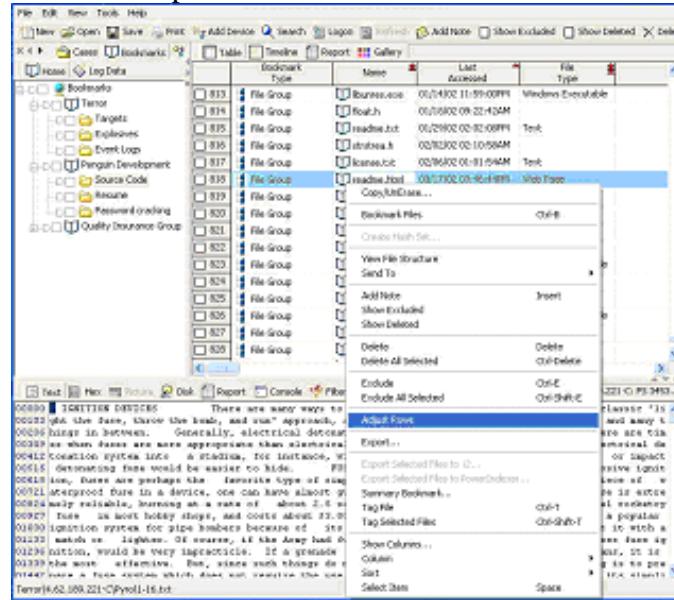


Figure 24-10 Use Adjust Rows to set the sorting for report generation

Presenting Multiple Images

Many forensic examinations recover multiple digital images. After bookmarking the images relevant to the investigation, the examiner can export custom reports containing these images from EnCase. The reports can be the standard rich text format (.rtf), viewable in Microsoft Word and printed in hard copy. Hypertext markup language (HTML) web pages can also be created when exporting for a paperless report on compact disc. The HTML format allows the reader to browse the recovered images as thumbnails and print out only the images required for a proceeding or in court.

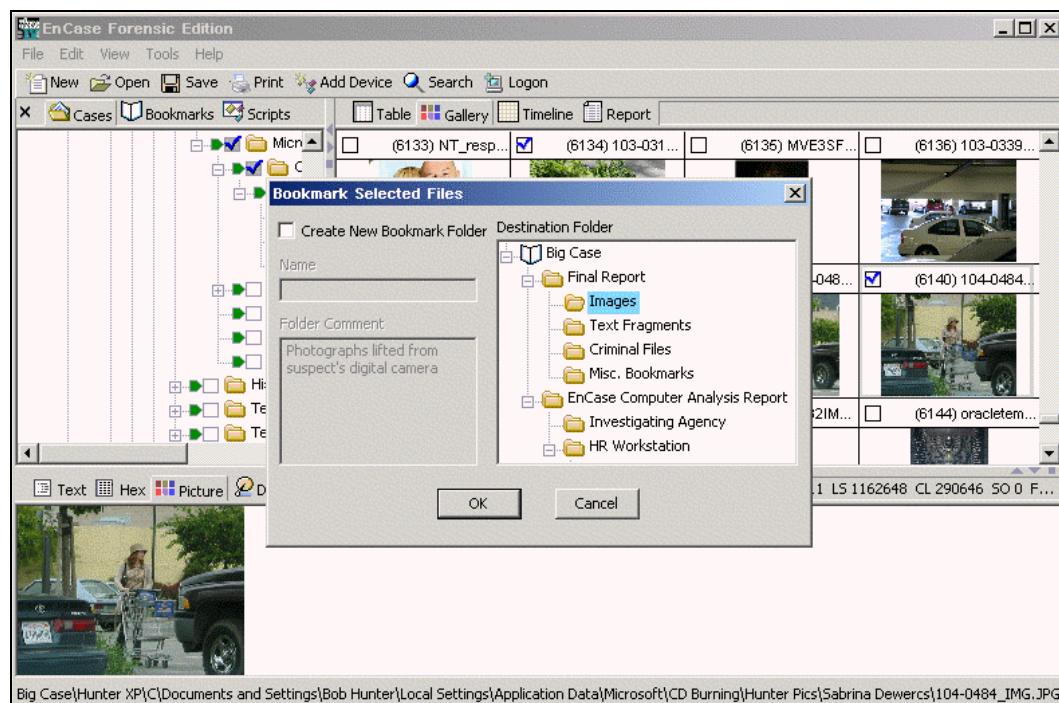


Figure 24-11 Simultaneously bookmarking multiple images relevant to the investigation

After bookmarking the images inside EnCase, create a new folder on the examination hard drive to receive the report and copies of the evidence images.

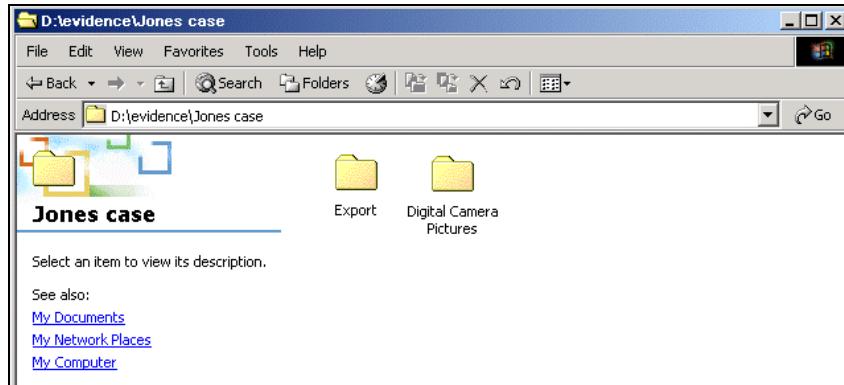


Figure 24-12 Folder on investigator's drive to receive reports and images

In the “Bookmarks” tab, select the bookmark folder containing the desired images in the left pane. In the right pane, select the “Report” view. Right-click on the “Bookmark” folder and select **edit**. Customize the format of the report by inserting comments in the “Comment” box and adding data fields to the report. Double-click on the fields in the lower right “Fields” pane to move the field to the “Format” pane. This will show those properties in the report. If the examiner does not set the properties of a Bookmark folder, the folder will inherit the properties set for its parent folder.

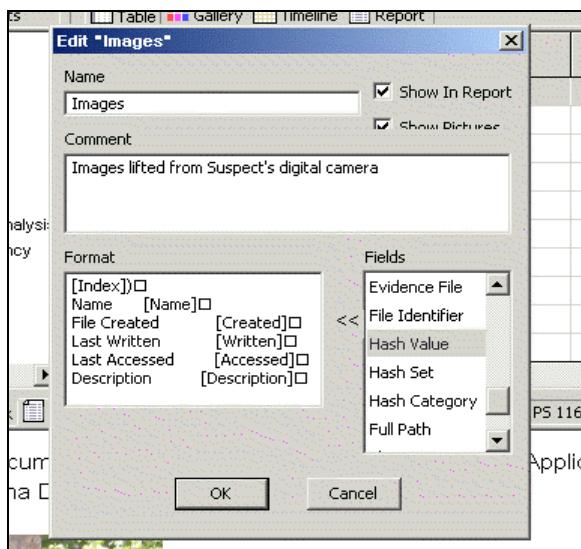


Figure 24-13 Customize the format of the report

Exporting the Report

In the right pane, showing the Report view, right-click on the report and select **Export**.

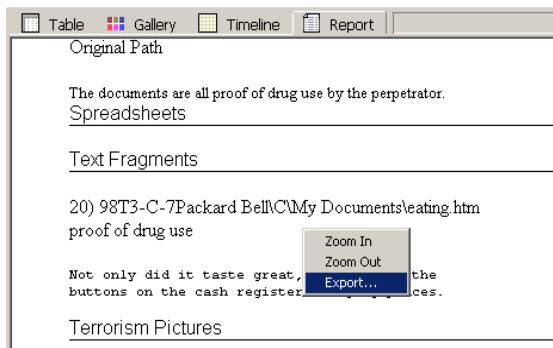


Figure 24-14 Exporting report

It is possible to export the report in two different formats

- **Rich Text Format (RTF)**

If the report is exported as a rich text format file, the file can then be easily edited with a word-processing application such as Microsoft Word. This is a good option for investigators who might need to customize their report.

- **Hyper Text Markup Language (HTML)**

If the report is exported as an HTML format file, hyperlinks for quick and easy navigation through the report can be created. The limitation is that editing the report in a WYSIWYG (What You See Is What You Get) environment requires an HTML editing program such as MS FrontPage.

Regardless of which format desired, browse to the folder to receive the report and select [OK].

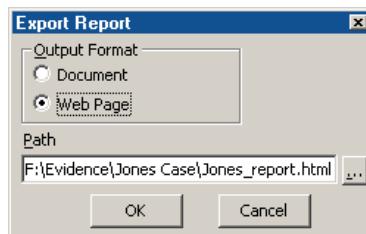


Figure 24-15 Exporting the report as an HTML file

Exporting the report as an HTML file will copy/unerase bookmarked images from the evidence file to the selected folder, as well as create four HTML files

- Full HTML report with the name assigned by the examiner.
- `gallery.html`, which contains a thumbnail viewer for the exported files.
- `toc.html`, which contains a table of contents of hyperlinks to the full report created and named by the examiner, and to the gallery created by exporting in the `gallery.html` file.
- `Frame View.html`, which creates a frame view of the other three files, with the table of contents at the top and either the full report or the gallery displayed in the lower frame. The `Frame View.html` file is the one that should be opened to view the results. This is also the file to link to from text on a summary report file on the compact disc.

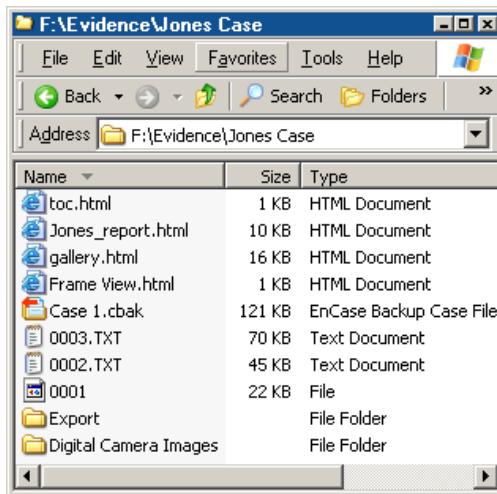


Figure 24-16 Files created by HTML report export

Double-clicking on the `Frame View.html` file will execute Internet Explorer (or the default browser). The full report, created and named by the examiner, is displayed by default. The table of contents in the upper frame provides hyperlinks to browse to the Gallery view and to return to the report.

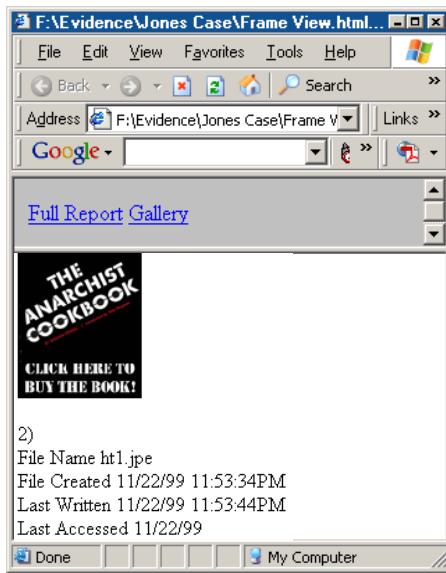


Figure 24-17 HTML report, full view

Clicking on the **Gallery** hyperlink will open *gallery.html* in the lower pane, and display thumbnails of the images copied/unerased out of the EnCase evidence file. The reader can use the Gallery to browse the exported files.

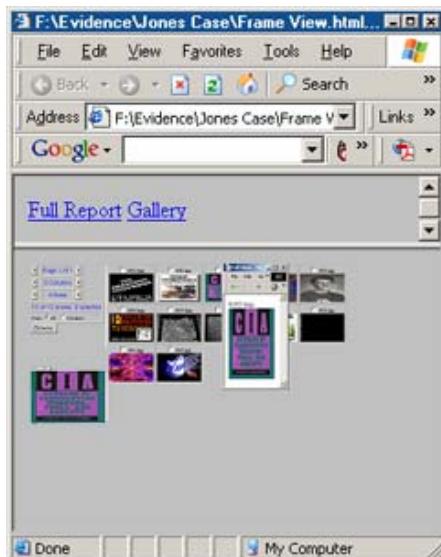
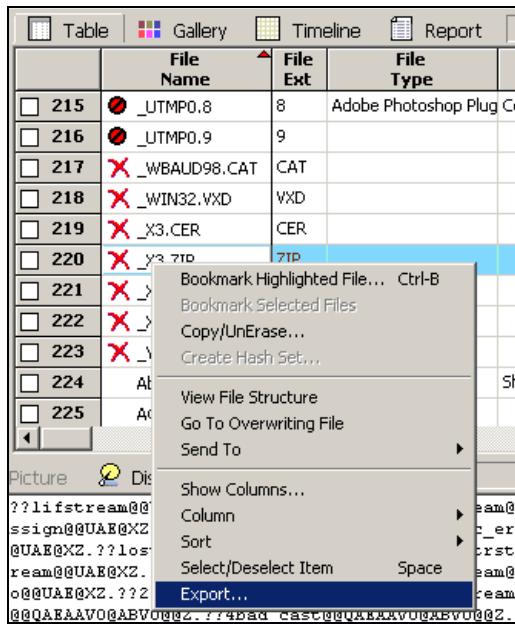


Figure 24-18 HTML report, gallery view

To view the image in full size, select the image thumbnail and it will be displayed in the bottom-left corner of the Gallery web page. Double-click on the image in the lower-left corner and Internet Explorer will open a new window containing the full-sized image.

Documenting All Files and Folders Contained on Media

To document all of the files and folders contained in a case, from the **Cases** tab, click the “All Files” trigger on the physical drive or media in the left pane. In the right pane, select Table view. Sort the rows by the **File Ext** column and sub-sort by the **Full Name** column. Right-click anywhere in the right pane and select **Export**.



A screenshot of a software interface showing a table of file information. The columns are labeled 'File Name', 'File Ext', and 'File Type'. A context menu is open over the table, with the 'Export...' option highlighted. The menu also includes options like 'Bookmark Highlighted File...', 'Copy/UnErase...', 'Create Hash Set...', 'View File Structure', 'Go To Overwriting File', 'Send To', 'Show Columns...', 'Column', 'Sort', and 'Select/Deselect Item'.

	File Name	File Ext	File Type
215	_UTMP0.8	8	Adobe Photoshop Plug Cr
216	_UTMP0.9	9	
217	X_WBAUD98.CAT	CAT	
218	X_WIN32.VXD	VXD	
219	X_X3.CER	CER	
220	X_Y3.ZIP	ZIP	
221	X_Z	Z	
222	X_Z	Z	
223	X_Y	Y	
224	AB		
225	AC		

Figure 24-19 Export a spreadsheet index

In the **Export Table** window, check the columns to be included in the spreadsheet. To include all of the columns, check the first box, scroll down to the last box, hold down the **[Shift]** key, and check the last box. Leave the default to export all of the rows.

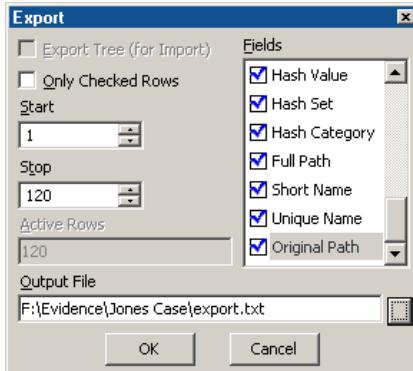


Figure 24-20 Set the columns and rows to be exported

In the **Output File** field, entering a file name and changing the extension to .xls will automatically associate the file with Microsoft Excel without the extra steps of importing a tab-delimited text file. The file can become quite large, especially when cataloging large-capacity hard drives.

Presenting Search Results

EnCase creates search hit folders under the **Search Hits** tab for each search session. A list of these search hits can be exported to a spreadsheet for inclusion in the report as follows:

- Select the “All Files” button on the **Search Session** folder in the **Search Hits** tab. Select Table view in the right pane.
- In the right pane, right-click and select **Export**.
- In the **Export** window, browse to the folder to receive the exported report.
- Name the report and change the extension to .xls for Microsoft Excel.
- Under the **Search Hits** tab, select the first keyword folder.
- Put the right pane in Table view, right-click and select **Export** to send the search results to a spreadsheet.

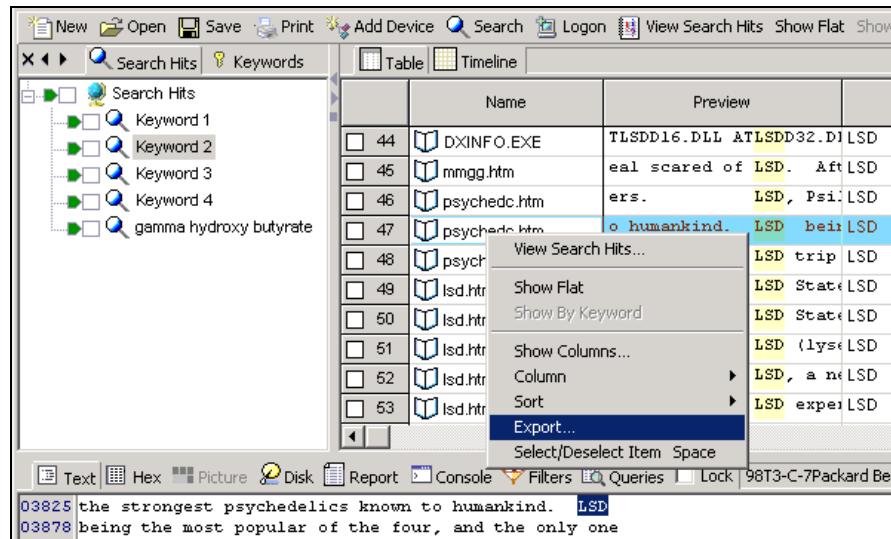


Figure 24-21 Exporting search results

- In the **Export Table** window, select the rows and criteria to be exported.
- Name the export file and change the extension to .xls for Microsoft Excel.

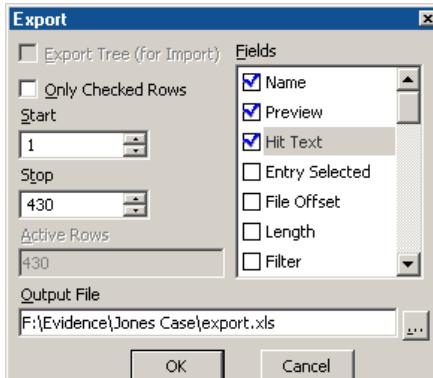


Figure 24-22 Selecting export criteria

- Export each of the Search Hit Results folders into separate Excel spreadsheets.

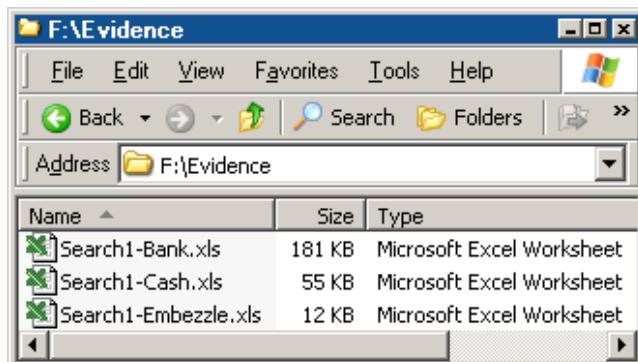


Figure 24-23 Search results as Excel spreadsheets

- Open the exported **Search Session** report with Microsoft Word. Microsoft Word 97 (and higher) features a competent HTML editor that can be used to customize exported EnCase reports and create paperless hyperlinked examination reports.
- Highlight text to be hyper linked. The Hyperlink window can be opened in three different ways:
 - a. Right-click on the highlighted text, and select **Hyperlink**
 - b. Use a hotkey sequence ([**Ctrl**][**K**])
 - c. Click on the hyperlink button on the tool bar

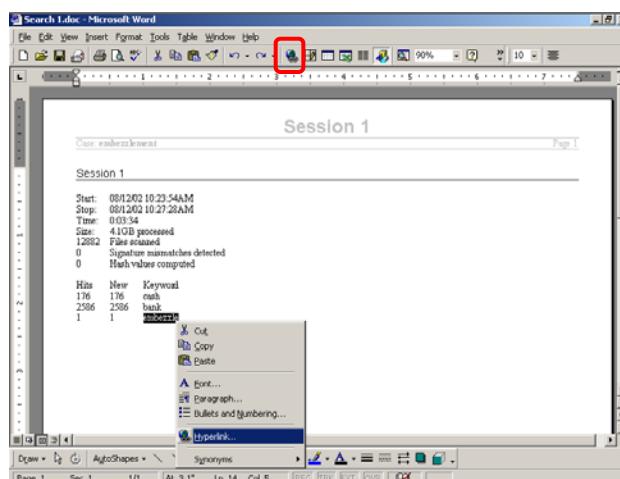


Figure 24-24 Creating a hyperlink in MS Word

- In the **Insert Hyperlink** window, type the name of the file to be linked or use the [**Browse**] button to find the file. Word will create a hyperlink in the report displaying the highlighted text to the linked file.

Session 1

```

Start: 08/12/02 10:23:54AM
Stop: 08/12/02 10:27:28AM
Time: 0:03:34
Size: 4.1GB processed
12882 Files scanned
0 Signature mismatches detected
0 Hash values computed

Hits New Keyword
176 176 cash
2586 2586 bank
1 1 embezzle
```

Figure 24-25 Hyperlinked text in report

- When the reader clicks on the hyperlink in the report, Windows will open the linked file and display the search results.

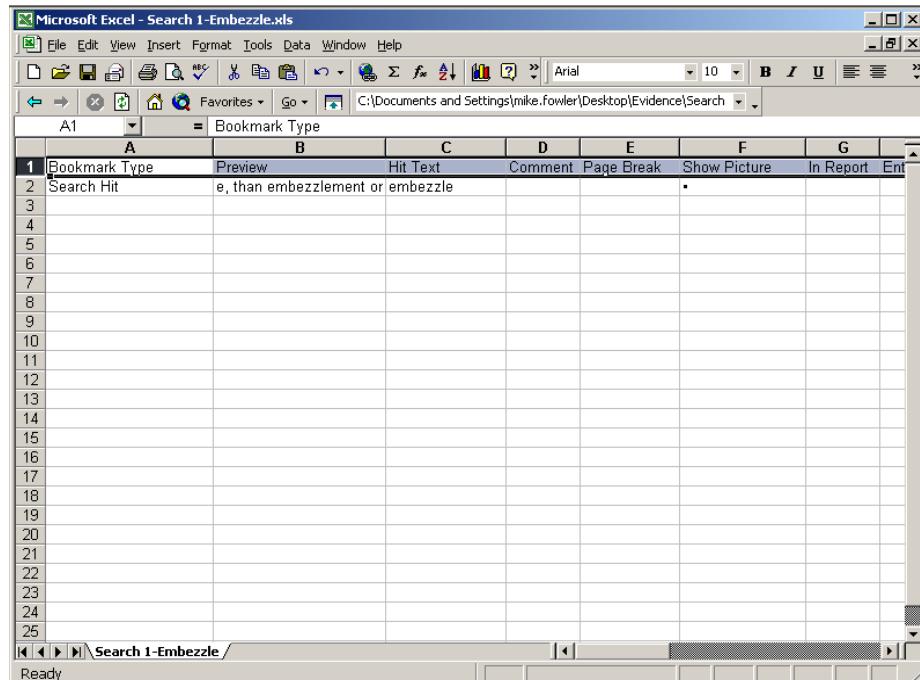


Figure 24-26 Opening hyperlinked text

This method of exporting customized sub-reports from EnCase and linking the reports from a summary examination report can be used to create paperless, courtroom-ready presentations. The reports will reflect the professional nature of the examination.

Exporting to i2

i2 has a number of programs to help examiners with link analysis. You can export out the data from the table in **Cases** view into a text file for import into i2 software. Blue-check the files for export of the metadata in the Table view to i2. Right-click in the table and select **Export Selected Files to i2**.

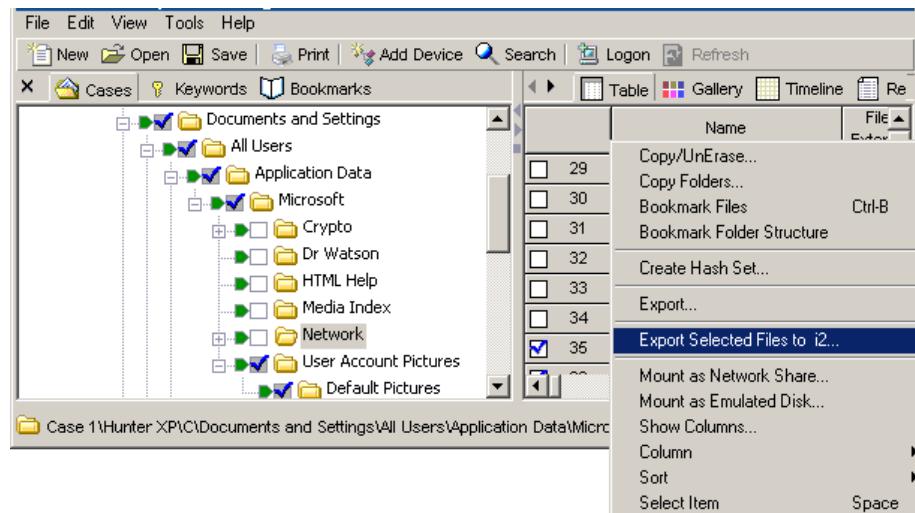


Figure 24-27 Exporting to i2

Save the export text file to the examiner hard drive for import to i2. Refer to the i2 software user manual for additional information on link analysis.

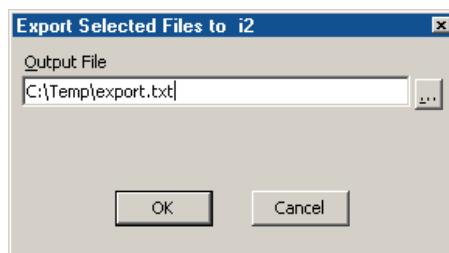


Figure 24-28 Export path for i2

Export to Xanalys' Quenza and Watson

Examiners who use Xanalys analysis programs (Quenza and Watson) can now export out a database for link analysis and pattern recognitions. The Xanalys program(s) must be installed on the examination computer to use this function.

Xanalys' Quenza uses the term *document set* to describe a set of files selected for Power Indexing.

Quenza will handle the following file formats:

.txt	.pdf	.html	.xml
.rtf	.doc	.dot	.ans

Depending upon your installation of Microsoft Word, the list also includes .wps and .mcw files.

- In **Cases** view, blue check and bookmark the desired files under the Table view.
- Place the files into a bookmark folder of your choice.
- Go to Bookmark view and select the folder containing the bookmarked files and then blue check the files to be exported to Xanalys.
- Right-click and select Export Selected Files to PowerIndexer...

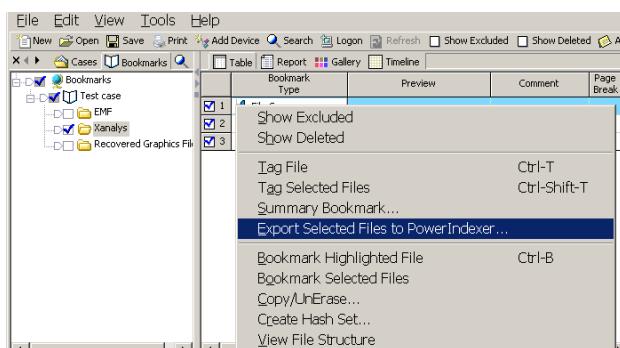


Figure 24-29 Blue check files to be exported

- You will be presented with an **Export Selected Files to PowerIndexer** dialogue box where you select **Grammar Format**, **Data Source**, and other items. Click **[OK]** to begin the export.

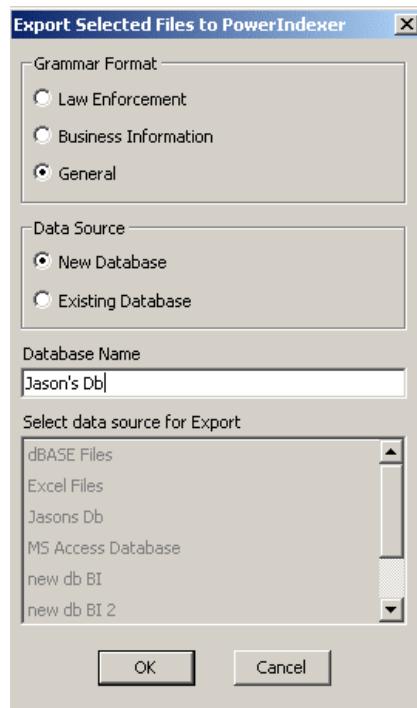


Figure 24-30 Export options

- The contents of the files will be exported to the database.

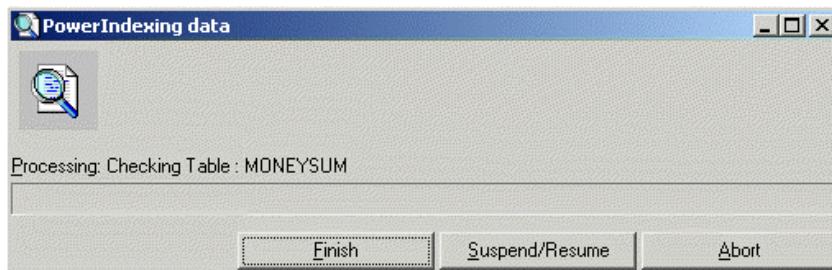


Figure 24-31 File export

- Once the process completes, the Watson (mapping) window will be opened. You can then use Watson to run a New Query over the files that were brought in.

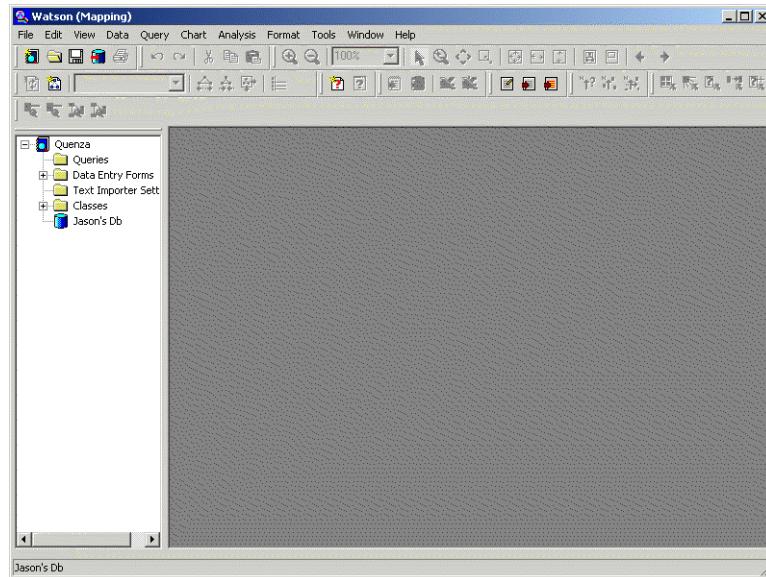


Figure 24-32 Watson interface

- Right-click in the tree to create a new query.

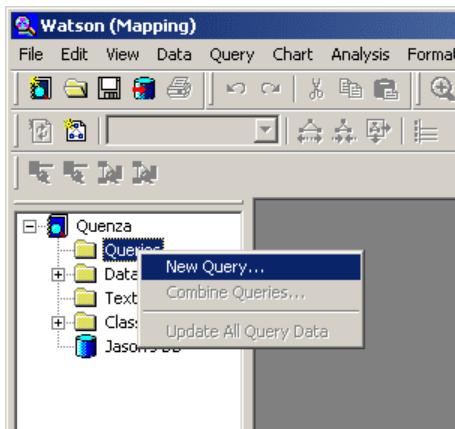


Figure 24-33 Creating a New Query

- Select the desired options in the **New Query** dialogue box, and then click [OK].

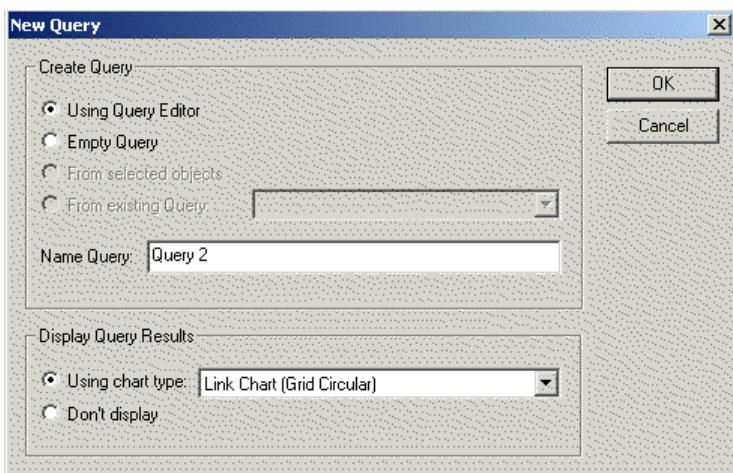


Figure 24-34 New Query dialogue box

- The Query Editor provides several types of queries to choose from.

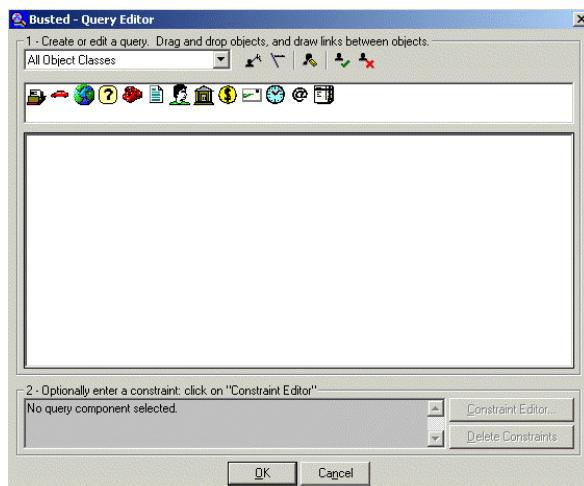


Figure 24-35 Query Editor

You can link people to events, locations, times, etc.

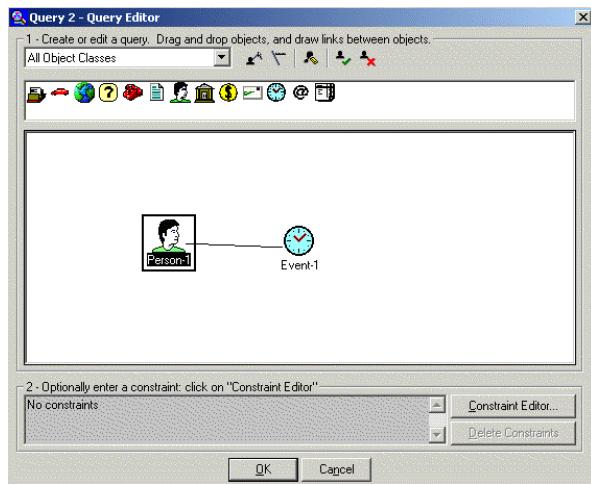


Figure 24-36 Creating Links

This provides you with another option in examining the data recovered from a computer forensic examination.

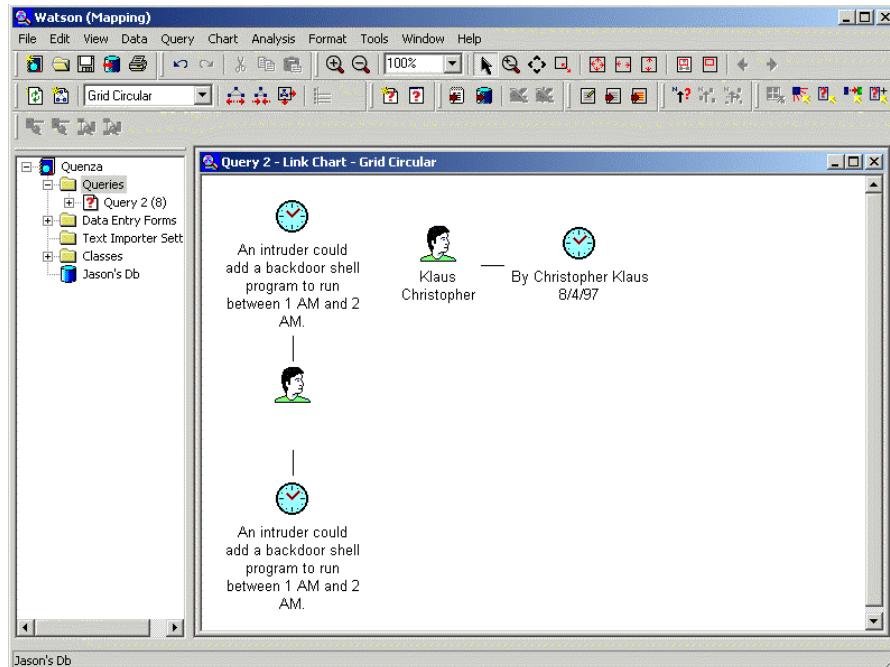
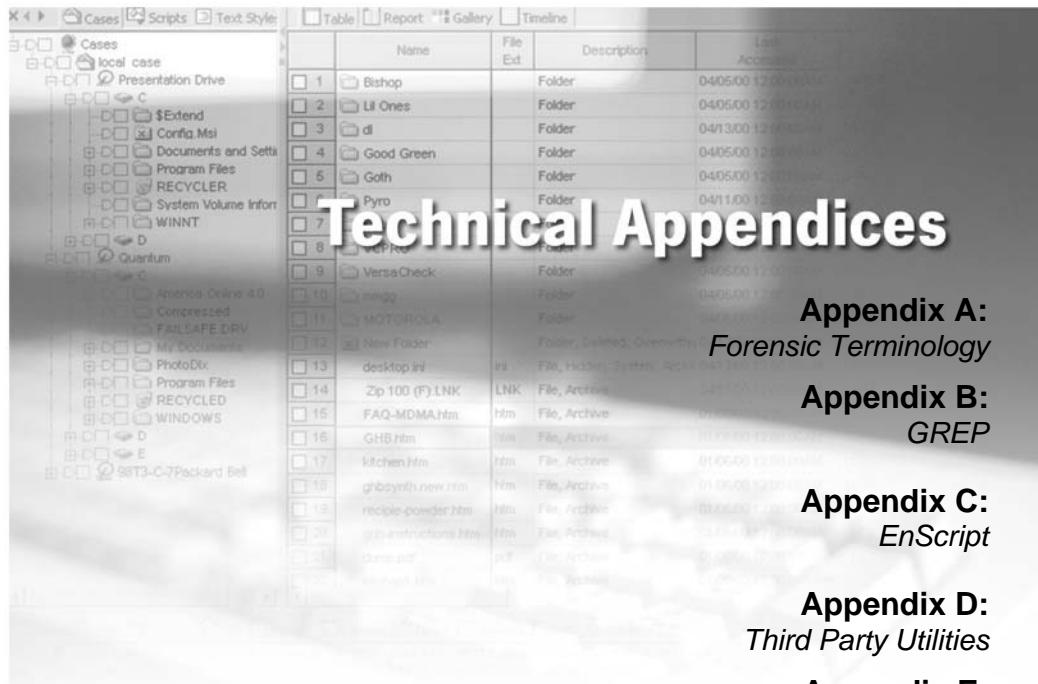


Figure 24-37 Link Analysis



Technical Appendices

**Appendix A:
Forensic Terminology**

**Appendix B:
GREP**

**Appendix C:
EnScript**

**Appendix D:
Third Party Utilities**

**Appendix E:
The Forensic Lab**

**Appendix F:
Partition Types**

*Copyright © 2004 Guidance Software, Inc.
May not be copied or reproduced without the written permission of Guidance Software, Inc.*

Appendix A

EnCase Terminology

Computer forensics, like most technical fields, has its share of jargon. Many of the terms in this guide have a precise meaning and should be understood thoroughly before attempting to use EnCase.

PC Hardware

“Storage” Computer/Media

The “Storage” computer is the EnCase investigator’s computer. The term “Storage” will loosely refer to either the examiner’s hard drive or the examiner’s computer.

“Subject” Computer/Media

The “Subject” is the computer or media that is being examined. In the past this has been referred to as the “Target” or “Source”. However, those terms are vague and open to interpretation. “Subject” is the term that will be used from now on.

RAM

Random Access Memory. Each computer has a certain amount of volatile read/write memory locations whose contents are lost when the power is turned off. The operating system, programs and drivers are all loaded into RAM at the same time.

ROM

Read Only Memory. Chips that contain a permanent program that is “burned in” at the factory and maintained when the power to the computer is turned off. As its name implies, the information on the chips can only be read and not written to (i.e. your computer cannot store information in these chips). They usually contain small programs and data that are needed to boot the computer.

BIOS

The Basic Input Output System of a PC. This is usually a number of machine code routines that are stored in ROM and available for execution at boot time. The “boot strap loader” is contained in ROM and is the first code to execute when the computer is turned on. The BIOS contains commands for reading the physical disks sector by sector.

Hard Drive Anatomy

Drive Geometry

A physical drive is usually composed of any number of rapidly rotating platters with a set of read/write heads for each side of each platter. Each platter is divided into a series of concentric rings called tracks. Each track is further divided into sectors. Each sector is then divided into bytes. The number and position of these structures is referred to as the drive geometry.

Cylinder

A cylinder, like a track, is a logical term and does not refer to a physical piece of hardware. In other words, you can't open a disk drive cover and see the “cylinders”. A cylinder refers to the set of tracks on every side of every platter that are at the same head position, as if an actual cylindrical cross-section had been taken out of the whole drive. If a drive contains 4 heads, a cylinder refers to all the information that is available to all the heads while on a single track.

Head

There is one head for every side of every platter in a hard disk drive. They ride very close to the surface of the platter and allow information to be read from and written to the platter. The heads are attached to an arm, which is in turn attached to a head stack assembly. Normally, all heads move together and are positioned on the same logical track together. Heads are numbered sequentially from zero.

Sector

A sector is a group of bytes within a track and is the smallest group of bytes that can be addressed on a drive. There are normally tens or hundreds of sectors within each track. The number of bytes in a sector can vary, but it is almost always 512. CDROMS normally have 2048 bytes per sector (this does not include the hundreds of bytes per sector for error checking and correction). Sectors are numbered sequentially within a track, starting at 1. The numbering restarts on every track, so that “track 0, sector 1” and “track 5, sector 1” refer to different sectors.

Track

Each platter on a disk is divided into thin concentric bands called Tracks. There is no physical structure associated with a track. Tracks are established when the disk is low level formatted. Tracks are numbered sequentially starting with track 0 on the outermost part of the platter, moving inwards.

Absolute Sectors

Early disk drives contained a number of cylinders, heads and sectors and these numbers would refer to actual hardware present in the drive. The BIOS would address the disk controller directly and translate absolute sector numbers into C-H-S before writing to or reading from the disk. As disk capacities increased to unforeseen sizes, manufacturers and software developers were forced to change the stated number of cylinders, heads and sectors in order to trick the BIOS into addressing the additional space.

Today, *the Cylinder, Head and Sector numbers are usually fictional and do not refer to actual disk structures or hardware.* These numbers are first translated by the BIOS, and then translated by the low-level disk device driver, and then again by the drive hardware, into numbers that make sense for the actual media. You can run yourself ragged trying to figure out exactly where on the physical device the data is stored, and it *rarely* makes any difference.

Fortunately, there is always a well-defined order in which the sectors are addressed. They are numbered sequentially from 0 to N-1, N being the total number of software addressable sectors present on the drive.

Some disk utilities will report Cylinder-Head-Sector numbers, but the new BIOS extensions have made this convention obsolete. Also, as a practical matter, it is easier to refer to a sector by *one* number, rather than *three*.

EnCase follows the new convention and refers to sectors as if the entire drive were a large flat array of sectors, starting at sector 0. When viewing a location on a physical disk, EnCase will show the CHS numbers for compatibility with other disk utilities.

Platter

A platter is a magnetized disk that the actual data of the hard drive is stored on. Modern hard drives typically have two platters, with heads reading and writing data to the platters simultaneously.

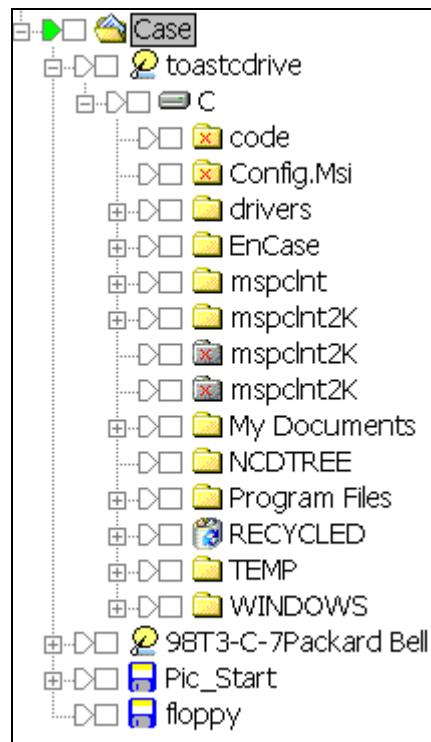
Drives, Disks and Volumes

The terms “volume”, “drive” and “disk” are often used interchangeably in other literature. It is very important to understand the distinction between these terms as they are used with EnCase.

A “disk” is an actual piece of hardware that you can hold in your hand. It could be a floppy disk, hard disk, Zip Disk or any other piece of physical media.

A “volume” refers to a mounted partition. There may be only one “volume” on a “disk” as is the case on a floppy or Zip disk or there may be several volumes on a disk as on a partitioned hard drive.

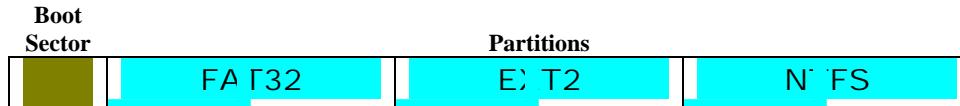
A volume is a concept, not a physical device. Early PC disks contained only one volume (e.g. “C”). As drives grew larger, it became convenient to partition a single physical disk into a set of logical volumes. There can be any number (up to 24, as in C, Z) of these logical volumes on a disk and they show up as drive “C”, “D” or “E” in DOS.



A case with 2 hard drives, 1 Zip disk, and 1 floppy

Hard Drive Layout

Master Boot Record



The very first sector of a physical disk (absolute sector 0) is called the master boot record (MBR). It contains machine code to enable the computer to find the partition table and the operating system. One of the first things a computer does when it starts up is to load this code into memory and execute it. This “boot code” has a very simple task. Its job is to read the partition table at the end of sector 0 and decide how the disk is laid out, and which partition contains the bootable operating system.

Partition Table

The partition table describes the first four partitions, their location on the disk, and which partition is bootable. This is indicated by a single byte in the partition table. In fact, the entire logical layout of the disk is determined by 64 bytes of information. It is quite easy to hide or change information or even entire volumes from DOS by changing a single byte in the partition table.

Extended DOS Partitions

Normally, each partition table entry describes a volume to be mounted by the file system. If more than four partitions are on the drive, a special partition type called an “Extended Partition” is created. In this configuration, the first sector of every extended partition is itself a boot sector with another partition table. This table has a duplicate copy of the partition entry for that volume that contains a sector offset into the current partition where the logical volume begins.

Volume Boot Sector

Since every partition may contain a different file system, each partition contains a “volume boot sector” which is used to describe the type of file system on the partition and usually contains boot code necessary to mount a file system.

This code is different from the master boot record code described earlier. The job of the volume boot code is to find a file in the root folder (io.sys in the case of DOS) that is then loaded and run to continue the boot process at a higher level.

On Linux systems, the LILO boot loader serves the same purpose. It locates the Super Block that describes the rest of the file system.

Inter-Partition Space

The sectors on the track between the start of the partition and the partition boot record are normally unused by any file system. This results in tens or even hundreds of sectors going to waste (not a big deal on a large drive). However, since this area is inaccessible to all but low-level disk viewers, it is *theoretically* possible to hide information there. EnCase labels these areas as “Unused Partition Area” and allows you to search and inspect their contents. These areas are also searched along with the rest of the disk, whenever a normal keyword search is done.

File System Concepts

Clusters

A cluster is a group of sectors in a logical volume that is used to store files and folders. Clusters must contain a number of sectors that is a power of 2 (i.e. 2, 4, 8, 16, etc...). DOS maintains information about each cluster in the File Allocation Table. NTFS partitions store that same information in the file extents tables and the volume bitmap. EXT2 partitions store the information in the Inode Tables and Block Bitmaps. CD's usually have un-fragmented file extents, so there is no need for a cluster bitmap or a FAT.

Cluster Bitmaps

Each cluster on a file system is either used or available for allocation (free). In DOS, the state of the clusters is kept track of in the File Allocation Table. A “0” entry in the FAT indicates that the cluster is free, otherwise there are different codes to indicate which part of its file the cluster belongs to. NTFS keeps track of free clusters with a “bitmap”. This is a file that contains 1 bit for every cluster on the volume. This file is put on the drive when it is formatted. EXT2 drives contain a block bitmap for every group, but the concept is the same.

Root Folder

All file systems have a “tree” structure that supports files and folders within folders to an arbitrary depth. The “root” of this tree is always stored in a known location.

On FAT12 and FAT16 volumes, the root folder resides at a fixed location on the drive and contains a maximum number of entries that is determined when the volume is formatted. The number of files and folders in the root folder of such a volume is limited, but the number and size of the rest of the folders in the disk is essentially unlimited, because they are treated like normal files and can expand if space is available on the volume.

On FAT32 volumes, the root folder is also treated like a file and can contain any number of files or folders. Its location is stored in the volume boot record.

NTFS stores the root as a special file in the Master File Table. The name of the file is “.” (dot).

EXT2 drives store the root as a special Inode in the first group.

CDFS give the location of the root folder in the boot sector.

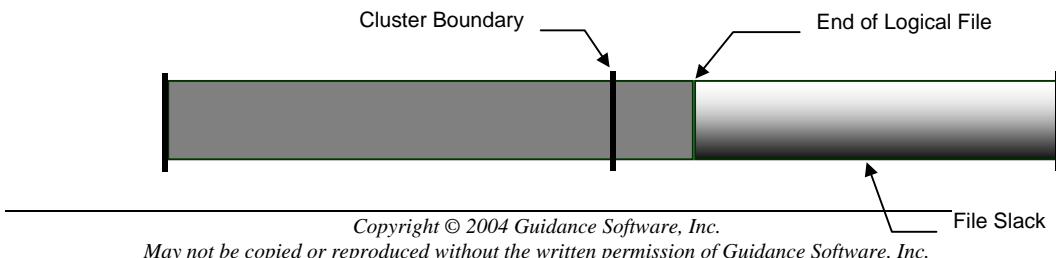
File Entries

A folder is treated just like a file on FAT and EXT2 volumes. Each folder contains a starting cluster and can be expanded or contracted as files are added or removed from the folder. Each file in the folder is represented by a 32-byte entry in a table. In other words, the content of a folder “file” is an array of records containing information about the files in the folder. Each entry in the folder can be either a file or another folder. In this way, a “tree” structure can be built.

A 32-byte entry contains enough space for an 8.3 character file name. Windows 95 implements long file names by chaining together a number of entries and using the space to store the additional characters in the file name.

File Slack

The space between the logical end and the physical end of a file is called the file slack. The diagram below shows a section of a disk that has 2 sectors per cluster. Since each cluster is 1024 bytes, the file takes up two clusters and has a physical size of 2048 bytes. The logical end of a file, in this example, comes before the physical end of the second cluster. The remaining bytes are remnants of previous



files or folders. EnCase searches file slack by default.

Logical File Size

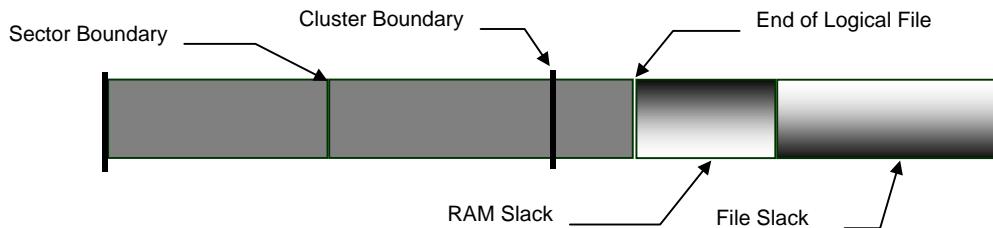
All file systems keep track of the exact size of a file in bytes. This is the logical size of the file and is the number that you see in the properties for a file. This number is different from the physical file size.

Physical File Size

The physical size of a file is the amount of space that the file occupies on the disk. A file or folder always occupies a whole number of clusters, even if it does not completely fill that space. A file always takes at least one cluster, even if it is empty. Therefore, even if a file has a logical size of only five bytes, its physical size is one cluster. EnCase displays both logical and physical size for every file.

RAM Slack

The space from the end of the file to the end of the containing sector is called



RAM slack. Before a sector is written to disk, it is stored in a buffer somewhere in RAM. If the buffer is only partially filled with information before being committed to disk, remnants from the end of the buffer will be written to disk. In this way, information that was never “saved” can be found in RAM Slack on disk. EnCase searches all file slack by default.

Volume Slack

On a formatted volume, there are a certain number of available sectors. These sectors are grouped together in clusters or blocks depending on the file system. If the number of possible clusters does not divide evenly into the number of available sectors, there will be some sectors left over at the end of the partition. These sectors are not used to store file/folder information by the file system. This wasted space is known as Volume Slack, and is usually less than the size of a cluster/block. Deleted files, hidden data and remnants of previous partitions could possibly be found in the Volume Slack

File Systems

File Allocation Table (FAT)

The FAT is an array of numbers that sits near the beginning of a DOS volume. These numbers can be 1½ bytes (12 bits), 2 bytes (16 bits) or 4 bytes (32 bits) long depending on the size of the volume. This is why volumes are sometimes referred to as FAT12, FAT16 or FAT32.

Each entry in the FAT corresponds directly to one cluster and there is always one FAT entry for every cluster. Each entry is either a code indicating that the cluster is free, the cluster is bad or that this is the last cluster in a file. If it is not one of these codes, then the number refers to the next cluster in the chain belonging to a file. The first cluster in the chain for a file is recorded in the properties for that file, which are stored in its parent folder. The FAT is therefore a one way linked list of clusters for every file in a volume.

Folders on FAT drives are stored as special files. The content of these files are the records for each of its children. These “folder files” take up space on the volume along with the other normal files.

NTFS

NTFS has an advanced structure that is designed to overcome the limitations of other file systems that have come before it. The file descriptors for every file on an NTFS volume are stored in the Master File Table (MFT), including a reference to the MFT itself. Each file descriptor contains the name and other attributes of the file along with its extents list. This list contains the location of the file on the volume. Another file called the volume bitmap describes the free clusters on the volume. Folders are stored in a b-tree structure for quick disk access.

EXT2/3

The EXT2 file system is the primary file system used on the Linux operating system. EXT2 partitions are divided into a series of Groups. Each Group contains a series of Inodes and Blocks. The Inode tables describe the files that are located within each group. As with the FAT file system, a folder is a file that contains descriptors for each of its children. EnCase can read and interpret the EXT2 file system and present its folder structure and files along side the rest of your evidence. EXT3 is EXT2 with journaling.

REISER

The Reiser file-system is a “flavor” of EXT2. EnCase has the ability to mount and interpret the Reiser file system.

CDFS

This ISO9660 standard is used to describe the files structure on a CD. There are many variations of the basic structure. The most notable is the Joliet standard that is used by Windows to allow for Unicode file names. EnCase can read and interpret the CDFS file system and present its folder structure and files along side the rest of your evidence.

HFS and HFS+

This is the Macintosh and Power Macintosh file-format. EnCase has also refined its support for other files systems. The Macintosh OS X Server operating system uses the Hierarchical Files System Plus (HFS+) without the wrapper of HFS. EnCase now supports this configuration.

Palm

The PalmOS file system consists of databases with records, which store both executable applications and program data. Currently, the PalmOS is found on devices manufactured by Palm, Inc. (Palm), Handspring (Visor, Treo), Sony (Clie), some cell-phones (Kyocera pdQ and Samsung I-300) as well as a handful of other devices made by companies such as IBM, Handera, and Symbol.

UFS

This is a common Unix file-system. However, Unix, like ice cream, has many flavors. Though EnCase can *acquire* all flavors, at this time, it can only *interpret* UFS.

Disk Configurations Explained

A Disk Configuration is a Redundant Array of Inexpensive Disks or RAID. There are commonly three types of RAIDs RAID 0, RAID 1, and RAID 5.

RAID 0 Striping

The first but not necessarily the most basic RAID type is RAID 0, or striping. The main purpose of RAID 0 is to provide speed. In fact, RAID 0 has no fault tolerance. If one drive in the array fails, the whole array is shot. There is no way to rebuild or repair the information stored on a RAID 0 array. This makes a

RAID 0 setup the most susceptible to failure, a fact that usually keeps users with sensitive data from choosing RAID 0 as their RAID setup.

At the same time, however, RAID 0 is the fastest of all RAID setups. Since there is no overhead required to store extra information for fault tolerance, the speed of RAID 0 can theoretically perform 2 times the speed of a single drive when there are 2 drives in the array. Adding more drives only increases this theoretical performance amount – a six-drive RAID 0 array's performance could be as fast as 6 times the performance of a single drive.

RAID 1 Mirroring

Although speed can be an important aspect of computing, so can the safety and reliability that comes with fault tolerance. Speed is sacrificed, but RAID 1 provides users with a level of safety nonexistent in RAID 0.

RAID 1 works by writing identical sets of information to two drives in an array, otherwise known as mirroring. When the controller is sent a 64KB file to be written to a two disk RAID 1 array, the controller sends identical copies of this 64KB file to both disks in the array. Reads are the same as on a single drive – the controller requests the file from one of the two drives.

The special feature of RAID 1 is its fault tolerance. If either of the two drives in the array fails, no data is lost. When a drive fails, the RAID controller uses the information off of the drive that is still available. When a new drive is added to the array to fix the failed one, a mirroring occurs in which the data from the good drive is written to the new drive to recreate the array again.

As one could suspect, RAID 1 offers very little in terms of performance. When requesting data from a drive, some RAID controllers take information from the drive that is not busy or closer to the desired information, theoretically resulting in faster data access. When writing, on the other hand, there is some overhead when compared to a single drive as the controller must duplicate the file it is sent and then pass it along to the drives.

In a RAID 1 setup, identical drives are best in order to prevent lost space. Since the same data is being written to two drives, the size of the RAID 1 array is equal to the size of the smallest drive in the array. For example, if a 20GB drive and a 30GB drive are used in a RAID 1 setup, the array would only be 20GB with the 10 extra gigabytes on the 30GB drive going to waste. The performance difference between two drives is also an issue here, since a faster drive would have to wait for a slower drive before it could write more information.

RAID 1 is a good solution for those looking for security over speed. Although not the slowest of the common RAID types, RAID 1 can be slower than a single drive in some cases (more on that in the benchmarks). What RAID 1 does provide is a very safe environment, where failure of a single drive does not equate to any down time.

In addition, EnCase now supports the Mirror RAID (RAID 1) configuration of NTFS Dynamic Disks normally found on Compaq Windows's servers. If only one of the mirrored drives is present, the file structure is still available for examination.

RAID 5

RAID 5 requires at least 3 drives and attempts to combine the speed of striping with the reliability of mirroring. This is done by striping the data across two drives in the array at a user defined stripe size. The third drive in the array, the one not getting striped data, is given a parity bit. A parity bit is generated from the original file using an algorithm to produce data that can recreate the information stored on both drives that received the striped data.

The two drives receiving the striped data and the one receiving the parity bit are constantly changing. For example, if drives 1 and 2 receive striped data on a write and drive 3 receives a parity bit, on the next write drives 2 and 3 will receive the striped data and drive 1 will receive the parity bit. The shifting continues and eliminates the random write performance hit that comes with a dedicated drive receiving the parity information.

The parity information is typically calculated on the RAID controller itself, and thus these types of controllers are called hardware RAID controllers since they require a special chip to make the parity information and decide what drive to send it to.

RAID 5 arrays provide a balance between RAID 0 and RAID 1 configurations. With RAID 5, some of the features of striping are in place as well as the features of mirroring. Thanks to the parity bit, if information is lost on one of the three drives in the array, it can be rebuilt. Thanks to the striping it uses to break up the data and send it to multiple drives, aspects of speed from RAID 0 are present.

Recreation works in the following manner. Let's use a 3 drive RAID 5 array with a 64KB stripe size for an example with a 128KB file that needs to be written. First, a parity bit is created for the file that the controller card has received by performing an XOR calculation on the data. Next, the 128KB file is broken into

two 64KB files, one of which is sent to drive 1 and the other to drive 2. Finally, the parity information calculated above is written to the third drive in the array.

Now, if one of the drives, or a portion of a drive, in the array goes bad and the 128KB file is lost, the data can be recreated via an xor operation between the remaining drives. It does not matter which drive fails – all the data is still available. If the third drive in the above example, the one that received the parity information for this write, fails then the original data can be read off of drives 1 and 2 to recreate the parity information. If either drive 1 or drive 2 fails, then the parity information stored on drive 3 can be used to recreate the information lost on the original drive.

There is a significant overhead associated with RAID 5, however, due to the parity bit that must be calculated and written to on each drive. This is especially present when changing only one piece of information on one drive in the array. During this process, not only does the information that requires changing require writing but the parity bit must also be recreated. This means that once the data is written, both drives with the stripe blocks on them must be read, a new parity bit be calculated, and then the new parity bit has to be written to the third drive. This problem only increases as additional drives are added to the array.

For the same reasons mentioned in both the RAID 0 and RAID 1 discussions, it is best to use identical drives for a RAID 5 setup. Not only does this ensure speed, it also ensures that all of the array's storage capacity is utilized. The size of a RAID 5 array is equal to the size of the smallest drive times the number of drives in the array minus one (since one of the drives is always getting a parity bit).

RAID 5 does provide a good balance between speed and reliability and is a popular configuration for arrays in a variety of systems, from servers to workstations. The data security made possible with the parity bit as well as the speed and space provided by RAID 5 have many high-end system builders turning to RAID 5.

Evidence Storage

Compression

Compression technology allows EnCase to store a large disk in a relatively small file. EnCase uses an industry standard compression algorithm to achieve an average of 50% size reduction. If most of the disk is unused, the compression

ratio can be much higher. This can result in great savings in disk storage space. Compressed Evidence Files take longer to generate because of the additional processing time required to compress information.

Compression NEVER has any effect on the final evidence, and compressed blocks are checked for validity in the same way as uncompressed ones.

MD5 Hash

The MD5 hash is a 128-bit (16-byte) number that uniquely describes the contents of a file. The code to compute the MD5 was developed by RSA and is publicly available. For this reason, the MD5 hash is a standard in the forensics world.

Professor Ronald Rivest created the MD5 hash algorithm in 1991. It is used to create digital signatures. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

The odds that two files with different contents have the same hash value is roughly 2^{128} or 3.4×10^{38} . If the hash values match, there is reasonable certainty that the file contents matches.

The purpose of the MD5 hash value within EnCase is two-fold. The first is to verify that the evidence file EnCase created is indeed the same in byte-structure as the original media; the second is for the creation of Hash Sets to add to your Hash Library.

EnCase calculates an MD5 Hash when it acquires a physical drive or logical volume. The hash value is written into the evidence file and becomes part of the documentation of the evidence. When an evidence file is added to a case, EnCase automatically verifies the CRC values, and re-computes the hash value for the evidence data within evidence file. The hash value that is stored in the evidence file, and the hash value that is computed when the evidence file is added to a case, appear in the Report for immediate confirmation that the evidence file has not changed since it was acquired. At any time while using EnCase, you can select the case view, right-click on the physical drive or logical volume, and select Hash to re-compute the hash value of the drive or volume.

The hash is generated as the data is read from the source device. The acquisition hash is the hash of the data that is acquired, and the verification hash is the confirmation of the acquired data. Both EnCase for DOS and EnCase for Windows give the examiner the option of hashing the source device itself before

or after acquisition. This is not done by default due to the amount of time required, and is instead provided as an option to the user. In EnCase 4.13 and above, if you choose to hash a device separately from an acquisition in Windows, EnCase will automatically create a note of the date/time and results of hashing the device. This note is placed on the root folder of the device under the Bookmark view, for inclusion in your Final Report if you wish. Of course in EnCase for DOS, it still writes the results to a text file. You can bring the text file results into EnCase with Add Raw Image function under the File tab, for inclusion in your report.

One note on imaging devices with corrupted or damaged sectors. EnCase is building the hash value of the acquired device as it is reading the data from the sectors. If a sector is damaged or has corrupted data, the next time you make a hash of the device, the hash value may be different, as well as the next, and the next and so on.

CRC (Cyclical Redundancy Checksum)

EnCase uses a CRC to verify the integrity of each block of data. The Cyclical Redundancy Checksum is a variation of the standard checksum, and works in much the same way. The advantage of the CRC is that it is order sensitive. The odds that two different data blocks produce the same CRC are roughly 1 in 4 billion.

Most hard drives store one CRC for every sector (512 bytes). When a read error is generated from a disk, this usually means that the CRC value of the sector on disk does not match the value that is recomputed by the drive hardware after the sector is read.

CRC values can be “reverse engineered” meaning that it is possible (though difficult) to force the CRC value of one document to match that of another by altering non-printing characters within the document. For this reason the method of choice for document verification is the MD5 hash. (See *MD5 Hash*)

File Signature

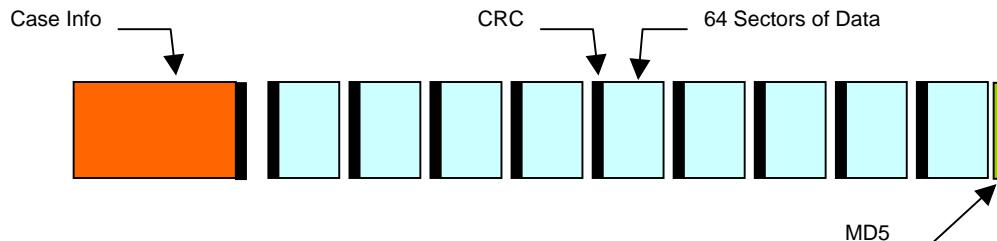
Many (but certainly not all) file types contain a few bytes at the beginning that constitute a unique “signature” of that file type. Most graphic and document file types contain a signature. For example, the first 6 bytes at the beginning of a GIF file are either GIF89A or GIF87A. This allows EnCase and other applications to sense the true type of a file, regardless of the file’s name extension.

Evidence Files Explained

The central component of the EnCase methodology is the Evidence File. This file contains four basic parts (the header, checksum and data blocks and the MD5 block) that work together to provide a secure and self-verifying description of the state of a computer disk at the time of analysis.

Evidence File Format

The EnCase process begins with the creation of a complete physical bit-stream mirror image of a target drive in a completely non-invasive manner. The acquired bit-stream mirror image, called an Evidence File, is mounted as a read-only file or “virtual drive” from which EnCase proceeds to reconstruct the file structure utilizing the logical data in the bit-stream image. This allows the examiner to search and examine the contents of the drive in a Windows GUI in a completely non-invasive manner. Throughout this process, the bit-stream image is continually verified by both a CRC value for every 32K block as well as an MD5 hash calculated for all data contained in the Evidence File. Both the CRC and MD5 hash values are immediately assigned to the Evidence File upon acquisition.



Each file contains an exact, sector-by-sector, copy of the disk. When the file is created the user gives information relevant to the investigation and EnCase archives this and other information inside the Evidence File along with the contents of the disk. This information in the header of the Evidence File is itself authenticated with a separate CRC.

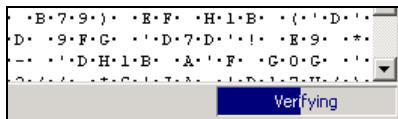
Throughout the examination process, EnCase verifies the integrity of the evidence by recalculating the CRC and MD5 hash values and comparing them with the values recorded at the time of acquisition. This verification process is documented within the EnCase-generated report.

It is nearly impossible to tamper with the evidence once it has been acquired. This allows the investigators and legal team to confidently stand behind the evidence in court.

Image Verification

In order to verify that the contents of an evidence file have not changed since the file was created, EnCase will read each sector block in the evidence file, recompute the CRC for that block and compare it to the original. If the two do not match, the location of the mismatch is recorded in the Case File and shown in the report.

This process occurs automatically whenever a new Evidence File is added to the Case and is proceed in the background.



EnCase Icon Descriptions

This section contains a detailed description of the EnCase icons. In the Table View, the icon to the left of the file name typically describes the files status. To the right, under the Description column is a terse description of that icon.



Root (global) – In any view (Cases, Bookmarks, Keywords, for example), this is the root folder. This icon is displayed even if there is nothing else created in the view window.



Case – The case icon is displayed in all views.



Device – A physical hard drive icon. This icon does not represent a volume or logical device, such as a partition



Network Share Device – This icon appears when the VFS module virtually mounts your Case, Device or folder.



Volume or Logical Device – Represents a volume, logical disk, and/or a partition



RAID, Dynamic Disk – RAID disks and Dynamic Disks.

Copyright © 2004 Guidance Software, Inc.

May not be copied or reproduced without the written permission of Guidance Software, Inc.



Rebuilt RAID or Dynamic Disk – Indicates a RAID or Dynamic disk successfully rebuilt within the EnCase environment.



CD ROM – Indicates a CD ROM



CD ROM session – Appears to indicate a session on a multi-session CD ROM.



Folder – An allocated folder



Deleted folder – A deleted folder.



Deleted, Overwritten folder – A folder that is deleted and over-written by another file (see also **Deleted, Overwritten file**).



Folder, Invalid Cluster – A directory entry whose file type bit is set to “folder;” and whose starting cluster is set to zero.



Lost files/Recovered Folders – Either Lost Files or Recovered Folders. It is also displayed when examining an NTFS or FAT drive.



Deleted file – A deleted file on the suspect’s computer that has been undeleted by EnCase; nothing changed in the evidence file.



Deleted, Overwritten file – A deleted or over-written file. EnCase determined that the starting cluster found in the directory entry for this file is occupied by another file. EnCase makes no further attempt to undelete this file, and it is not undeleted. The file that overwrote the deleted file is displayed in the status bar. The contents being displayed are not the contents of the deleted file. Remnants of the original file may exist. Further examination should include checking the starting cluster, and the size of both files, to enable the examiner to determine if the data has been over-written. If it has not, the original file data may be on the hard drive in the slack space of the new file.



Invalid Cluster - A filename entry that does not have a starting cluster number. EnCase cannot locate the file's contents. Invalid cluster numbers are normally generated from system-deleted files, where the starting cluster number is changed to zero. This evidence indicates that the filename existed and the dates that it was created, modified, and accessed.



File, Hard Linked - A condition when more than one File Name has a direct connection to the same Inode. EnCase splits the data into its own file named Hard Link Data #. All corresponding hard links will point to this file for the data. (For example /bin/ls uses Inode 64860; /var/ftp/bin/ls also uses Inode 64860)



Internal File – A file created by file systems, such as NTFS, HFS, NT/W2K, MAC, LINUX and EXT2.



Recycle Bin – The suspect's recycle bin.



Unallocated space, MBR, unused disk area, FAT tables, VBR, Volume slack – A representation of these areas of the disk and that no files are currently allocated to these areas.



Text – Text view (ASCII text) of the selected item.



Hex – Hex view, shows the hexadecimal value for each character displayed.



Picture – Displays a picture if the selected file type is a graphic image.



Report – Displays the data that appears in the report for the selected item.



Console – Displays the console contents (C:\Program Files\EnCase4\console.txt); usually contains status information about the results of processes such as scripts, searches, and Recovered Folders.



Filters – Displays the available filters for the current view.

Copyright © 2004 Guidance Software, Inc.

May not be copied or reproduced without the written permission of Guidance Software, Inc.



Queries – Displays the available queries for the current view.



Disk – Displays the contents of the disk divided into individual sectors, which are represented as blocks. Each block pattern and color has its' own definition as follows:

Volume Boot	Deleted File
FAT 1	Boot Sector
FAT 2	Wasted Area
Root Folder	No Partition
Unallocated	Unknown
Bad Cluster	Volume Slack
Allocated	Disk Manager
Lost Cluster	



Bookmark – Selecting this icon presents the Bookmark view.



Highlighted Data Bookmark – Created by sweeping data (clicking and dragging the mouse over data) in one of the sub-panes. This is a customizable bookmark.



Notes Bookmark – Allows the user to write additional comments into the report. It is not an evidence bookmark.



Folder Information Bookmark – Bookmarks the tree structure of a folder or device information of the selected media. Options include showing the device information, such as drive geometry, and the number of columns to use for the tree structure.



Notable File Bookmark – A file bookmarked by itself. This is a customizable bookmark.



File Group Bookmark – A bookmark that is part of a group of selected files. There is no comment on this bookmark.



Snapshot Bookmark – Contains the results of a System Snapshot of dynamic data for Incident Response and Security Auditing.



Log Record Bookmark – Contains the results of the log parsing EnScript.



Open Ports Bookmark – Contains the snapshot data for all open ports on a target system.



Process Bookmark – Contains the snapshot data about all processes running on a target system.



Open Files Bookmark – Contains the snapshot data on any open files on a target system.



Network Interfaces Bookmark – Contains the snapshot configuration of any of the network interfaces on a target system.



Network Users Bookmark – Contains the snapshot of the network users with system access.



IDS Events Bookmark – Contains a snapshot of IDS events.



Registry Bookmark – The results of running the EnScript that parses the Windows registry. This icon is also displayed in certain scripts when selecting the registry.



File Types – Selecting this icon presents the File Types view.



File Signatures – Selecting this icon presents the File Signatures view.



File Viewers – Selecting this icon presents the File Viewers view.



Keywords – Selecting this icon presents the Keywords view.



Search Hits – Selecting this icon presents the Search Hits view.



Preview Icon – When displayed inside any other icon, indicates that there is a preview being performed on the selected device



Floppy disk \ Zip disk – Indicates a floppy disk or Zip disk preview\acquisition, and is also displayed in the Add Device window as a valid removable device.



Empty Floppy disk – No floppy media in the selected drive



FastBloc Protected Device – A FastBloc write protected device available for preview or acquisition.



Palm – A Palm PDA device is present.



Parallel Port \ Network Crossover – A device has been added using a parallel port or a network crossover cable.



Security IDs – EnCase extracted file and folder security information (owner, group and permissions) for an NTFS file system as well as owner, group and permission settings for a Unix, or Linux system



Text Styles – Selects the text style to view Code Pages in different settings, like variations in color and text line length. EnCase is configured with default text styles, but additional styles can be added, edited, and deleted from this tab by either right-clicking and selecting the command from the contextual menu or clicking the button in the tool-bar



Scripts – Small programs or macros designed to automate forensic procedures.



Hash sets – A collection of hash values of files that belong to the same application.



App Descriptors – This view enables examiners to organize the hash values of live processes running on a system scanned by the Snapshot function.



Machine Profiles – This view enables examiners to create a custom profile of the authorized applications or processes that should be running on a target machine.



Encryption Keys – This view enables users to generate key-pair's to be used with EnCase Enterprise



EnScript Types – A reference resource containing the EnScript language classes. The right-pane displays each functions parameter.



Move File - The file that overwrote the deleted file is displayed in the status bar. The content displayed is not the contents of the deleted file.



EnScript Member Functions – Functions that are defined within the Script or Class



EnScript Function Arguments – Arguments that are used in Functions



EnScript Argument Passed by Reference – Arguments of Functions that are passed by reference



EnScript Enumerations – ENUMs for Functions or Classes



EnScript Constants – Constants that are used in Scripts or Functions

Appendix B

Appendix B GREP

GREP Syntax

Symbol	Meaning
.	A period matches any single character.
\255	Decimal character (period)
\x	A character represented by its ASCII value in hex. For example, \x09 is a tab. \x0A is a line feed. Both hex digits should be present, even if they are 0.
?	A question mark after a character or set matches one or zero occurrences of that character or set. For example, “##?/#?/#?” would match “1/1/98” or “01/01/89” but would NOT match “123/01/98.”
*	An asterisk after a character matches any number of occurrences of that character, including zero time. For example, “john,*smith” would match “john,smith”, “john,,smith”, and “johnsmith”.

Copyright © 2004 Guidance Software, Inc.
May not be copied or reproduced without the written permission of Guidance Software, Inc.

+	A plus sign after a character matches any number of occurrences of that character except zero. For example, "john,+smith" would match "john,smith" or "john,,smith" but would NOT match "johnsmith".
#	A pound sign matches any numeric character [0-9]. For example, #####-##### matches any number in the form 327-4323 (if looking for a phone number, for example).
[XYZ]	Characters in brackets match any one character that appears in the brackets. For example, "smit[hy]" would match "smith" and "smity".
[^XYZ]	A circumflex at the start of the string in brackets means NOT. Hence, [^hy] matches any characters except h and y.
[A-Z]	A dash within the brackets signifies a range of characters. For example, [a-e] matches any character from a through e, inclusive.
\[A backslash before a character indicates that the character is to be treated literally and not as a GREP character. For example, "one\+two" matches "one+two". A slash () must be placed in front of any GREP token (including a slash () itself) that you wish to be a literal part of the match.
{X,Y}	Repeat X-Y times. Example {3,7} would repeat three to seven times.
(ab)	Functions like a parenthesis in a mathematical expression. Groups ab together for , +, *,
\wCDEF	Allows the investigator to enter Unicode code for a particular character; 4 integer code is required. See the Unicode chart for mapping.
a b	The 'pipe' acts as a logical OR. So it would read 'a or b'.

GREP Examples

The following examples show some of the power that GREP expressions deliver when looking for text. The first line is the example, followed by an explanation of the symbols used, followed by examples of text found using the expression.

john.smith

The “.” matches any single character. This expression finds “john” followed by any character followed by “smith”.

john smith

john,smith

johnQsmith

NOT john@%smith

john[,;]smith

The characters inside the brackets are called a *set*. The characters in a set are treated as a single character. This expression finds “john” followed by a space OR a comma OR a semicolon followed by “smith”.

john smith

john,smith

john;smith

john[0-9a-z]smith

The “-” indicates a range of characters when inside a set. This expression finds “john” followed by any character between (“0” and “9” or “a” and “z”) followed by “smith”.

john0smith

john1smith

johnzsmith

john[^#]smith

The “^” at the start of a set indicates any character other than those in the set. This expression finds “john” followed by any character other than “0”-“9” followed by “smith”.

john smith

johnQsmith

john,smith

john +smith

The “+” means to repeat the preceding character (or set) any number of times, but at least once. This expression finds “john” followed by any number spaces followed by “smith”.

john smith

john smith

john smith

john-*smith

The “*” indicates to repeat the preceding character (or set) any number of times including zero times. This expression finds “john” followed by any number of dashes followed by “smith”.

johnsmith

john-smith

john--smith

john smith\x0D\x0A

The “\” followed by an “x” indicates a two-digit hex number representation for a character. This expression finds “john”, followed by a space, followed by “smith”, followed by a carriage return linefeed sequence.

john smith

NOT john smith.

NOT john,smith

it'?s

The “?” repeats the preceding character (or set) one or zero times. This expression finds “it” followed by an apostrophe (or not) followed by “s”.

its

it's

NOT it s

NOT it-s

c:\|images\|picture\.gif

The “\” preceding any character (including “\”) indicates that this is a literal character and not a GREP symbol. Be careful when expressing file names and paths in GREP. Slashes and dots should be preceded by a “\”.

c:\images\picture.gif

chu[^a-zA-Z]

This expression matches “chu” followed by any nonalphabetic or upper-case alpha character. This ensures that short names and words are not found inside other words. Capital characters, however, will be found.

chu

chuCK

NOT chuck

NOT chump

http://www\.[a-zA-Z]+\.[com]

This expression matches “http://www.” followed by any lower-case alphabetic characters followed by “.com”. This is a good way to look for website references.

http://www.bozo.com

NOT http://www.to-wong-foo.com

NOT http://www.bozo.org

#####-#####-#####-#####

The “#” character matches any number. This expression could match a credit card number where the numbers are separated by dashes.

1234-3623-3410-2232

4534-2123-9866-6512

NOT 1233456780007654

NOT 456

[456]###-?###-?###-?###[^#]

This expression could match a credit card number where the dashes between the numbers are optional and the first number being constrained to 4, 5, or 6.

6234-3623-3410-2232

4534212398666512

NOT 1233456780007654

NOT 323345680007654

\(?###[\() \]-]*###[\)-]?####[^#]

This expression could match a U.S. phone number in one of several formats. The “\?” expression means that the open “(” character can be present or not. The “[() \]-]*” expression means that either a space or a close “)” or a dash can be repeated any number of times including zero.

(909) 875-4125

204-725-2436

103 875 4344

9098721344

##?#?\##?#?\##?#?\##?#?[^\#].]

This expression could match an IP number in regular form with 4 (up to 3 digit) numbers separated by periods.

123.235.23.1

255.255.255.255

0.0.0.0

NOT 234.1234.123.123

NOT 0.0.0.0.

Appendix C

EnScript Syntax

EnScript is a language and API that has been designed to operate within the EnCase environment. EnScript is compatible with the ANSI C++ standard for expression evaluation and operator meanings but contains only a small subset of C++ features. In other words, EnScript uses the same operators and general syntax as C++ but classes and functions are organized in a different way.

Language Overview

EnScripts are compiled from source code before being executed. During this process, the compiler may return syntax errors if the code cannot be compiled. Since one error may give rise to a multitude of other syntactic problems further in the code, the EnScript compiler always stops compiling at the first error and displays a message on the screen and places the cursor at the point in the code where the problem occurs. All errors must be fixed before the script will be executed.

WARNING EnScript Macros are executable files and thus should be treated with the same caution as any other executable file received from a third party over the Internet or by other means. Like other executable files, it is possible to intentionally write EnScripts with malicious code or to imbed viruses within the

Copyright © 2004 Guidance Software, Inc
May not be copied or reproduced without the written permission of Guidance Software, Inc.

code of an EnScript. It is imperative to identify and trust the source that the EnScript was obtained from. As with any other file, EnScripts received from third parties should be screened for viruses.

Declarations

In C++, functions must be declared in two places Once in the class definition (usually placed in a “header file”) and again in the source file. To simplify coding, EnScript does not use header files. Instead, function definitions are placed right inside each class definition and forward references are handled automatically by the “two-pass” compiler.

EnScript is a strongly typed language. Each variable must be declared to be of a certain type before it is used.

EnScript is an object oriented language in that all functions and data must reside inside a class definition, including all standard functions and data.

Scope

Scope is the range within code that a variable has. For example, if a global variable is declared, then its scope is global. If a variable local to a function is declared, then its scope is local to that function. Variables can be local to specific parenthetical blocks of statements as well.

Comments

Source code may be commented by blocking off sections of text with special character sequences. This text is ignored by the compiler. There are two styles of comments that are permitted, line and block.

```
// this is a comment that stops at the end of this line
/*
    this is a comment that
    goes on until the terminator ('*/') is reached
*/
```

Data Types

Integers

In C++, the range of the integer types are platform dependent. In EnScript the integer types have a fixed size, independent of processor or platform:

Type	Size	Min Value	Max Value
char	1 byte	0	255
byte	1 byte	0	255
bool	1 byte	false	true
short	2 bytes	-32,768	32,767
ushort	2 bytes	0	65,535
int	4 bytes	-2,147,483,648	2,147,483,647
uint	4 bytes	0	4,294,967,295
long	8 bytes	-	9,223,372,032,559,808,512
ulong	8 bytes	0	18,446,744,065,119,617,025

Floating Point

The **double** type stores floating point numbers in the range of $\pm 1.79 \times 10^{308}$ with 15 significant figures. Use this type when fractions or very large values need to be handled.

Enumerated Types

EnScript supports enumerated scalar types. Use the enum keyword to define a set of constants of type int, called an enumeration data type. The syntax is:

enum [<type_name>] {<constant_name> [= <value>], ...}

<type_name> A tag that names the set.

<constant_name> The name of a constant that can optionally be assigned the value of <value>.

<value> A constant integer or expression. If <value> is missing, it is assumed to be <prev> + 1 where <prev> is the value of the previous integer constant in the list. For the first integer constant in the list, the default value is 0.

Example:

```
enum Constants {
    first,           // Value = 0
    second,          // Value = 1
    third = 20,      // Value = 20
    fourth = third + 10 // Value = 30
}
```

Strings

EnScript has a native string type “String” that can accept constant or variable character strings as values. The following are examples of String usage:

```
String s1 = "Hello"; // Initialize s1 with a constant string
String s2(" World"); // Constructor call (slightly faster)
s1 = s1 + s2;        // s1 now equals "Hello World"
s1 += ".";
s1 += 32;            // Add ASCII 32 (space)
                     // s1 now equals "Hello World. "
```

Control characters can be added to a string by putting a backslash followed by a special character. The following string shows how this is done:

```
s1 = "A tab \t, a backslash \\, a quote \" and a line feed \n";
```

You can piece together long constant strings by placing them back to back or on a separate line.

```
String s = "this is a very " // No semi-colon at the end!
                     "long string";
```

Dates

EnScript has a native date type “DateClass” that can accept a date/time value. The input string for a date adheres to the date/time conventions set up in the Global Options. The following are examples of Date usage:

```
DateClass d(2000, 1, 1, 20, 7, 32); // Initialize with constructor
d = #1/1/2000 8:07:32PM#;           // Set value to literal string
if (d > #1/1/2000#)                // Compare to other date
    Process();
d.Now();                           // Set to system date/time
```

If you wish to apply the current volume/case time zone settings to the EnScript dates, you must call the `EntryClass::SetTimeZone(uint options)` function before setting the date. This function will set the internal EnScript time zone settings to that of the entry that `SetTimeZone` is called with, and the date will then be adjusted accordingly. There are 2 options that can be passed into `SetTimeZone`: `EntryClass::APPLYCASE` and `EntryClass::ADJUSTDST`. `APPLYCASE` will apply the case-level time zone adjustments (to align all times to one particular time zone), and `ADJUSTDST` will adjust the times for Daylight Saving Time (for further discussion on these issues, please see the Time Zone Settings section in *Chapter 13 First Steps*.) Volume time zone settings will be applied by default when `SetTimeZone` is called. The following is an example of `SetTimeZone` usage:

```
entry.SetTimeZone(EntryClass::ADJUSTDST | EntryClass::APPLYCASE);
DateClass d(2000, 1, 1, 20, 7, 32); // Initialize with
constructor
Console.WriteLine(d.GetString() + "\n"); // d will be adjusted based
// upon
// volume and case settings
```

`DateClass::Set(...)` Treated as LocalTime
`DateClass::SetDOS(...)`: Treated as LocalTime
`DateClass::SetUnix(...)`: Treated as GMT Time
`DateClass::SetPalm (...)`: Treated as GMT Time
`EntryClass::ReadWinDate` Treated as GMT Time

Operators

Unary Operators

EnScript supports the following unary operators for use with scalar types. These operators are placed to the left of the operand (except for `++` and `-` which may be placed after).

- `!` Logical negation (`true` if operand is zero, `false` otherwise)
- `++` Increment (can be used prefix or postfix)
- `--` Decrement (can be used prefix or postfix)
- `-` Unary minus
- `~` Bitwise complement (integers only)

Binary Operators

EnScript supports the following binary operators. The operator must be placed between the operands and the left operand is always evaluated before the right operand. The operands must be scalar types unless otherwise noted.

Arithmetic

- `+` Add (concatenate for String type)
- `-` Subtract
- `*` Multiply
- `/` Divide
- `%` Remainder (modulus)

Bitwise

- `<<` Shift bits left
- `>>` Shift bits right
- `&` Bitwise AND
- `|` Bitwise inclusive OR
- `^` Exclusive OR (XOR)

Logical

- `&&` Logical AND
- `||` Logical OR

Assignment

- `=` Assignment
- `*=` Assign product
- `/=` Assign quotient

%=	Assign remainder (modulus)
+=	Assign sum (concatenate for String type)
-=	Assign difference
<<=	Assign left shift
>>=	Assign right shift
&=	Assign bitwise AND
^=	Assign bitwise XOR
=	Assign bitwise OR

Relational

<	Less than
>	Greater than
<=	Less than or equal to
>=	Greater than or equal to
==	Equal to
!=	Not equal to

Member selection

.

(Dot)

Ternary Operator

? : a ? b : c

This standard C++ operator pair fits an “if-then-else” into one expression. The following code can be translated into “x takes on the value 2 if y is greater than one, otherwise x takes on the value of 3.”

x = y > 1 ? 2 : 3;

Operator Precedence

The relative precedence of all the operators are shown below:

Precedence	Operator	Associativity
Highest	() ::	left to right
	.(dot)	left to right
	! ~ -(unary) ++ -- & *	right to left
	* / %	left to right
	+ -	left to right
	<< >>	left to right
	< <= > >=	left to right
	== !=	left to right
	&	left to right
	^	left to right

Copyright © 2004 Guidance Software, Inc.

May not be copied or reproduced without the written permission of Guidance Software, Inc.

Lowest	 && ?: = *= /= %= += -= &= ^= = <<= >>= ,(comma)	left to right left to right right to left left to right right to left right to left left to right
--------	--	---

It is not advisable to rely solely on operator precedence when constructing complicated expressions. Instead, use parentheses to scope operators so that your intentions are clear. In the following example `&&` (and) has a higher precedence than `||` (or) even though the `||` comes first.

```
bool value = a > 10 || x < 20 && p != 10;
```

The expression should be rewritten to avoid confusion

```
bool value = (a > 10 || x < 20) && (p != 10);
```

Prefix and Postfix

The `++` and `-` (increment and decrement) operators can be used in either prefix or postfix form. In prefix form, the operator works before other parts of the expression use the value of the operand. In postfix, the operator's works after the expression is evaluated. Example:

```
int a = 2;
int x = ++a; // x = 3 (prefix ++ works before assignment)
a = 2;
x = a++; // x = 2 (postfix ++ works after assignment)
```

Program Control

Statements

A statement is the part of the program that does the actual work. A single statement can take up many lines but must end with a semi-colon (;). A statement can be a variable declaration as in:

```
int value = 10;
```

or a function call:

```
Process(value);
```

or it can be a computation:

```
double area = radius * radius * PI;
```

Blocks

Blocks are any group of statements enclosed in curly braces {}. Variables declared within a block are invisible outside the block.

```
{
    int x = 10;           Variable declared within block
    while (x < 100)
        Process(x++);
}
// x is out of scope and cannot be referenced here
```

Conditionals

The **if** statement takes the following form where {block} can also mean a single statement:

```
if (condition) { block } else { block }
```

Example:

```
if (value > 10)
    Process(value);
else
    Ignore(value);
```

while Loops

Use a **while** loop when no initialization is required within the loop and the loop condition must be checked before entering the loop for the first time.

while (*condition*) { *block* }

condition is executed **before** each iteration of the loop and determines whether to enter the loop or exit.

Note Remember to increment if using a counter.

For example:

```
int i = 0;
while (i < 10) { // Check condition before entering
    Process(i);
    Output(i);
    i++;
}
```

do-while Loops

Use a **do-while** loop when the {*block*} needs to be executed at least once before deciding whether to proceed.

do { *block* } **while** (*condition*);

condition is executed **after** each iteration of the loop and determines whether to continue.

For example:

```
int i = 0;
do {
    Process(i++);
} while (i < 10); // Process called at least once
```

for Loops

Use the **for** loop to execute a block a fixed number of times. The **for** loop has the following syntax, where { *block*} can be a single statement:

for (*statement1*; *condition*; *statement2*) { *block* }

statement1 is executed once before the loop is entered, usually to initialize a counter variable.

condition is executed before each iteration of the loop and determines whether to enter the loop or exit; it is equivalent to the **while**().

statement2 is executed after each iteration of the loop is completed, usually to increment a counter.

For example:

```
for (int i = 0; i < 10; i++) // Calls Process 10 times
    Process(i); // Passes the count into the
                  // Process function
```

break statement

To unconditionally exit a loop, use the **break** statement. For example:

```
int size = in.GetSize();
for (int i = 0; i < size; i++) {
    int c = in.Get(); // Read character
    if (c == FileClass::EOF) // End of file?
        break; // Exit for loop
    out.Put(c); // Write to output
}
```

Functions

Functions are the building blocks of a program. A function can encapsulate a series of statements and loops in order to prevent repetition of the same code throughout the program. The form of a function definition is:

<return-type> name (*<argument-list>*) {*block* [**return** statement;]}

The “arguments” are the parameters that are passed in by the calling statement. There can be any number of arguments to a function, including zero. The *<argument-list>* takes the form:

(*<type>* name1, *<type>* name2, ...)

If the *<return-type>* is **void**, then no return value is expected or allowed. Example:

```
int Square(int x) { // One integer argument
    return x * x; // Return value expected
}
void SayHello() { // No arguments
    Console.WriteLine("hello\n");
    // No return statement
}
```

Other functions may call a declared function. For example:

```
void WriteSquare(int x) {
    SayHello();
    Console.WriteLine("The square of " + x + " is " + Square(x));
}
```

Classes

Functions that are related can be grouped together in a structure called a **class**. Unlike C++, there are no global functions or data in EnScript. Everything must be declared inside a **class**.

The functions and data inside of a class definition are called the class **members**. The syntax of a class definition is as follows:

```
class name {<member-list>}
```

Different functions inside a class can have the same name as long as the parameter lists are different. The compiler will choose the proper function based on how many and which types of arguments are used by the calling statement.

Constructors

The “Constructor” is a special type of function that serves as an initializer for that class. A constructor has the same name as the class but has no <return-type>, not even **void**.

If a class has at least one constructor, then whenever a variable of its type is declared, one of its constructors MUST be called in order to initialize the values of the class. Given the class declaration shown below, the EnScript compiler will return an error for the following code:

```
CountClass count; // WRONG!!! No Constructor called
```

Of course, CountClass could declare a constructor that takes no parameters, in which case the above statement would be legal.

Destructors

A destructor is a special function that is called automatically when a variable of that class goes out of scope. A destructor has the same name as the class except that a ‘~’ is placed before the name. A destructor can take no arguments and only one destructor is permitted per class. For instance, a class representing a file may have a destructor that closes the file when the variable is no longer being used.

A simple example of a class is shown below:

```
class CountClass {
    int Value; // Data member
    —CountClass(int x) { // Constructor (no type, same name as class)
        Value = x;
}
```

Don't forget
the '~' for the
destructor

Copyright © 2004 Guidance Software, Inc.

May not be copied or reproduced without the written permission of Guidance Software, Inc.

```
        }
        ~CountClass() {           // Destructor (no type, no arguments)
            Console.WriteLine("Done");
        }
        void Inc() {             // Method, no return value
            Value++;
        }
    }
```

Other parts of a program can then create variables of type “CountClass” and call their members. For example, with the above class definition in place, we can now write the following code.

```
    {
        CountClass count(10);
        count.Inc();
        Console.WriteLine("Count = " + count.Value + "\n");
    }
```

Destructor
called
automatically
here

Produces the following output:

```
Count = 11
Done
```

Data Access

The real power of EnScript comes about in forensic applications. EnScript provides a simple and safe way to access, but not modify, the file data inside of the EnCase environment.

EntryClass

An EntryClass is an object that represents a file entry in the Table View. The members of the EntryClass have access to the data inside the entry and perform in the Cases tab any manner of computation or processing. For instance, the following function returns true if the created date of the file entry is later than or equal to New Years Day, 2002:

```
bool MillenniumBaby(EntryClass entry) {
    return entry.Created() >= #1/1/2002#;
}
```

An EntryClass is actually a tree structured list that represents a file or folder in a Case. Given any EntryClass object, it is possible to do a “recursive descent” of its structure. The following example writes out the names of all of the “children” of a given entry:

```
void Recurse(EntryClass entry) {
    Console.Write(entry.LongName() + "\n");
    for (EntryClass e = entry.FirstChild(); e; e++)
        Recurse(e);           // Call "myself" with each child
}
```

FileClass

A FileClass allows access to the contents of any EntryClass as well as any file on your local system (including network files). In fact, the only difference between a file in the case and a file on your system is that files in the case are read-only and cannot be opened for writing (for obvious reasons).

The following code shows a function that copies all printable characters of a file entry (including slack) to a given output file.

Example:

```
bool CopyFile(EntryClass entry, FileClass &out) {
    FileClass file;
    if (file.Open(entry, FileClass::SLACK)) {
```

Copyright © 2004 Guidance Software, Inc.
May not be copied or reproduced without the written permission of Guidance Software, Inc.

```

        int c;
        while ((c = file.Get()) != FileClass::EOF)
            if (c >= ' ' && c < 128)
                out.Put(c);
        }
        return true;
    }
    else
        return false;
}

```

Combining this with code above, we can copy all files in the Case to an output file on our system:

```

void Recurse(EntryClass entry, FileClass &out) {
    CopyFile(entry, out); // Copy contents of file to "out"
    for (EntryClass e = entry.FirstChild(); e; e++)
        Recurse(e);           // Call "myself" with each child
}

```

Finally, the above code is used on a newly created file:

```

void Main(EntryClass case) {
    FileClass out;
    // Make sure to use a \\ for each regular backslash
    if (out.Create("C:\\temp\\\\junk.txt"))
        Recurse(case, out); // Call function above
}

```

A lot of work can be done with very few lines of code.

Programs

An EnScript program consists of a class called “MainClass” which must have at least one function called “void Main(EntryClass case)”. When the program is run, an object of type MainClass is created and its Main function is called. When the Main function returns, the program is finished. To run a program, highlight it in the right-pane and press **F9**. For example:

```

class MainClass {
    void Main(EntryClass case) {
        Console.WriteLine("Hello world");
    }
}

```

EnScripts run in the background and a blinking status bar indicates that it is running. Stop the script from running at any time by double-clicking on the status bar and choosing **YES**.

Filters

A Filter consists of a class called “MainClass” which must have at least one function called “bool Main(EntryClass entry)”. When the filter is activated from the file view table, an object of type MainClass is created and its Main function is called for each entry in the table. The Main function should return **true** to keep the file entry in the view.

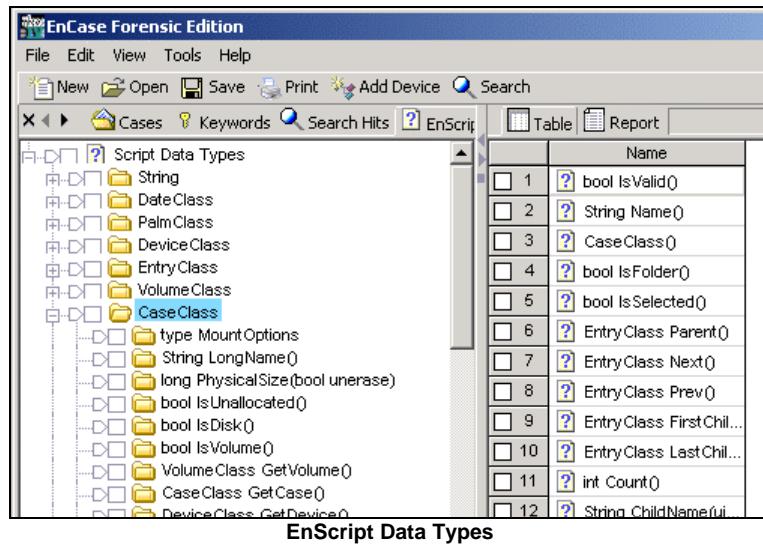
```
class MainClass {  
    bool Main(EntryClass entry) {  
        return entry.Category() == "Picture" &&  
            entry.LogicalSize() >= 20000; // Show big pictures  
    }  
}
```

A filter can filter files any way specified, including opening the file and looking for key words. For Example:

```
class MainClass {  
    bool Main(EntryClass entry) {  
        FileClass file;  
        return file.Open(entry, FileClass::SLACK) &&  
            file.Find("Smoking Gun", -1, FileClass::UNICODE);  
    }  
}
```

EnScript Help

For a complete list of EnScript Data Types, go to **View→EnScript Types**.



*Copyright © 2004 Guidance Software, Inc.
May not be copied or reproduced without the written permission of Guidance Software, Inc.*

Appendix D

Third Party Utilities

While EnCase has many capabilities, it does not and cannot do everything. Therefore we recommend certain third-party utilities that would be helpful to forensic investigators.

Guidance Software does not and cannot be responsible for the performance, availability, or reliability of any of these third-party utilities. We do not and cannot guarantee that we can help you set up, run, or troubleshoot any of these utilities either. We offer the following solely for your benefit and education.

Quick View Plus

For viewing files

<http://www.avantstar.com>

IrfanView

For viewing graphic files

<http://www.irfanview.com>

free (for home use)

*Copyright © 2004 Guidance Software, Inc
May not be copied or reproduced without the written permission of Guidance Software, Inc.*

AC/DSee

For viewing graphic files

<http://www.acdsee.com>

free trial version

DBXtract

To read Outlook Express 5.0 e-mails

<http://chattanooga.net/~scochran/DBXtract.htm>

free

MBXtract

To read Outlook Express 4.0 e-mails

<http://chattanooga.net/~scochran/MBXtract.htm>

free

Decode Shell Extension

For decoding MIME or UUencoded e-mail attachments. Other potentially useful shareware utilities available at this site as well.

www.funduc.com

free

Disk Compare

Compare two disks side-by-side

<http://tp.lc.ehu.es/JMA/win95.html>

free

Mailbag Assistant

Mailbag Assistant supports several mailboxes, including Outlook Express, Eudora, Netscape Messenger, Pegasus, Forte Agent and The Bat! Support for additional mailers is planned in future versions.

www.fookes.com/mailbag

\$29.95

PST Cracker

Crack passwords in password-protected PST files

<http://www.crak.com/downsoft.htm>

free demo

OST2PST

Converts .ost files to .pst files for easy viewing

www.pwdservice.com

free

Gpart

A tool which tries to guess the primary partition table of a PC-type hard disk in case the primary partition table in sector 0 is damaged, incorrect or deleted. The guessed table can be written to a file or device. Supported (guessable) file system or partition types

DOS/Windows FAT (FAT 12/16/32)

Linux ext2

Linux swap partitions versions 0 and 1 (Linux >= v2.2.X)

OS/2 HPFS

Windows NT/2000 FS

*BSD disklabels

Solaris/x86 disklabels

Minix FS

Reiser FS

Linux LVM physical volume module (LVM by Heinz Mauelshagen)

SGI XFS on Linux

BeOS filesystem

QNX 4.x filesystem

<http://www.stud.uni-hannover.de/user/76201/gpart/>

free

CD-R Diagnostic

A CD-R diagnostic utility

www.cdrom-prod.com

\$50.00

Dir to Html

http://www.silvermaine.co.uk/dir_to_html.asp

Free version download

or Dir to Html Pro £ 4.99

Appendix E

The Forensic Lab

Investigators use EnCase mainly for two different functions--acquisition and analysis. Forensic systems should be designed and built around those two functions. Two different computers might be the best solution.

Field Acquisitions

The most important feature to keep in mind for field acquisitions is *connectivity*. If you cannot bring the Subject's computer or hard drive back to the forensic lab with you, it is of the utmost importance that the correct tools are on-site so that the Subject media can be successfully and reliably imaged. Either a media device or a field computer that will attach to all types of hardware is required.

A *luggable* computer—a small desktop designed for field acquisitions—is an option. The advantage of these computers is that most, if not all, connectivity is on the *outside* of the case. Attaching an internal hard drive to the luggable without even opening the Storage computer cover is possible. Many also come with drive drawers, where the Subject hard drive can be placed to acquire its data.

*Copyright © 2004 Guidance Software, Inc.
May not be copied or reproduced without the written permission of Guidance Software, Inc.*

Of course, options like that can get expensive. Cheaper alternatives are to bring an external FireWire hard drive into the field (as well as an EnCase Boot Disk with the appropriate DOS drivers for the drive) and attach that to the perpetrator's PC. This could also include external removable media such as external Jaz drives, external Zip drives, etc. With removable media, however, a large amount of media might be required. For a 20-gig hard drive, at least 20 Jaz cartridges would be needed. Furthermore, Jaz drives and other forms of removable media are not as reliable as hard drives. Guidance Software always recommends acquiring media to a hard drive.

Another option is to purchase a small desktop and stock it with a SCSI card (the Adaptec 29160 is recommended), a large hard drive, and at least 512 MB of RAM. A full-fledged field computer is much more versatile than a laptop.

Many investigators use laptop computers in the field for their portability, but laptops can be restrictive in terms of connectivity. The only ports available (that EnCase for DOS can take advantage of) are the parallel port (very slow) or the PCMCIA port for an external hard-drive. It seems almost easier to bring a small desktop. The difference in terms of acquisition time will more than make up for the transporting and setup time.

Regardless, remember to bring the EnCase Network Boot Disk and *always* perform acquisitions in EnCase for DOS, unless using a FastBloc.

Lab Analysis

The lab analysis machine (the Forensic PC) is the work-horse. Important features to keep in mind for the analysis machine are ***speed*** and ***hard drive space***. A Pentium-IV running at 2 GHz or higher with 512 MB of RAM is a good start. One hard drive should be dedicated to the OS and applications (10 GB recommended) and a second hard drive dedicated to evidence file storage (80 GB recommended). Both hard drives should be 7200 RPM drives. A good lab analysis machine should also have a "computer forensic friendly" BIOS.

An excellent resource for computers built explicitly for computer forensics is Forensic-Computers.com, at www.forensic-computers.com.

Need Additional Information?

All questions about Storage computer or Acquisition computer hardware configurations can be addressed to support@guidancesoftware.com.

*Copyright © 2004 Guidance Software, Inc.
May not be copied or reproduced without the written permission of Guidance Software, Inc.*

Appendix F

Partition Types

Below is a list of the known partition IDs of the various operating systems, file systems, boot managers, etc. For the various systems, a short descriptions is provided when the information is available.

Copyright Andries E. Brouwer 1995-2001. This list is reprinted with his permission. You can find this same list on the web at www.win.tue.nl/~aeb/partitions/partition_types-1.html.

Some systems use systematic ways of modifying partition IDs. The best known type of modification is ORED with 0x10 to `hide' a partition.

Some partition IDs imply a particular method of disk access. In particular, IDs **c,e,f** (the LBA versions of **b,6,5**) go with partition table entries that have C/H/S = 1023/255/63 and expect access via the extended INT-13 functions (AH=4x) of the BIOS.

ID Name**0 Empty**

This is not used to designate unused area on the disk, but instead marks an unused partition table entry. (All other fields should be zero as well.) Unused area is not designated. [Plan9](#) assumes that it can use everything not claimed for other systems in the partition table.

1 DOS 12-bit FAT

DOS is a family of single-user operating systems for PCs. 86-DOS ('QDOS' - Quick and Dirty OS) was a CP/M-like operating system written by Tim Paterson of Seattle Computer Products (1979). Microsoft bought it, renamed it to MS-DOS 1.0 and sold it to IBM (1980) to be delivered together with the first IBM PCs (1981). MS-DOS 2.0 (1983) was rather different, and designed to be somewhat Unix-like. It supported a hard disk (up to 16MB; up to 32MB for version 2.1). Version 3.3+ added the concept of partitions, where each partition is at most 32MB. (Compaq DOS 3.31 relaxed this restriction.) Since EnCase Version 4 partitions can be 512 MB. Version 5.0 supports partitions up to 2 GB. Several clones exist [DR-DOS](#) (from Digital Research, later part of Novell and called NovellDOS or [NDOS](#), then owned by Caldera and called [OpenDOS](#), then by its subsidiary Lineo who named it back to DR-DOS. See <http://www.drdos.com/>), [PC-DOS](#) (from IBM), [FreeDOS](#), ... See [Types of DOS](#). See comp.os.msdos.* and [MSDOS partitioning summary](#). The type **1** is for partitions up to 15 MB.

2 XENIX root**3 XENIX /usr**

Xenix is an old port of Unix V7. Microsoft Xenix OS was announced in August 1980. It is a portable and commercial version of the Unix operating system for the Intel 8086, Zilog Z8000, Motorola M68000 and Digital Equipment PDP-11. Microsoft introduced XENIX 3.0 in April 1983. ([Timeline of Microcomputers](#)) SCO delivered its first Xenix for 8088/8086 in 1983. See comp.unix.xenix.sco.

4 DOS 16-bit FAT (up to 32M)**5 DOS 3.3+ Extended Partition**

Supports at most 8.4 GB disks. Type **5** DOS/Windows will not use the extended BIOS call, even if it is available. See type **f** below.

6 DOS 3.31+ 16-bit FAT (over 32M)

Partitions, or at least the FAT16 filesystems created on them, are at most 2 GB for DOS and Windows 95/98 (at most 65536 clusters, each at most 32 kB). Windows NT can create up to 4 GB FAT16 partitions (using 64 kB clusters), but these cause problems for DOS and Windows 95/98. Note that VFAT is 16-bit FAT with long filenames; FAT32 is a different filesystem.

7 OS/2 IFS (e.g., HPFS)

IFS = Installable File System. The best known example is HPFS. OS/2 will only look at partitions with ID 7 for any installed IFS (that's why the EXT2.IFS packet includes a special "Linux partition filter" device driver to fool OS/2 into thinking Linux partitions have ID 07). (Kai Henningsen (kai@khms.westfalen.de))

7 Windows NT NTFS

It is rumored that the Windows NT boot partition must be primary, and within the first 2 GB of the disk.

7 Advanced Unix

7 QNX2.x pre-1988 (see below under IDs 4d-4f)

8 OS/2 (v1.0-1.3 only)

8 AIX boot partition

8 SplitDrive

8 Commodore DOS

8 DELL partition spanning multiple drives

8 QNX 1.x and 2.x ("qny")

(according to [QNX Partitions](#))

9 AIX data partition

Some reports interchange AIX boot & data. AIX is IBM's version of Unix. See [comp.unix.aix](#).

9 Coherent filesystem

Coherent was a UNIX-type OS for the 286-386-486, marketed by Mark Williams Company led by Bob Swartz. It was renowned for its good documentation. It was introduced in 1980 and died February 1, 1995. The last versions are V3.2 for 286-386-486 and V4.0 (May 1992, using protected mode) for 386-486 only. It

sold for \$99 a copy, and the FAQ says that 40000 copies have been sold. See comp.os.coherent and [this page](#). A Coherent partition has to be primary.

9 QNX 1.x and 2.x ("qnz")

(according to [QNX Partitions](#))

a OS/2 Boot Manager

OS/2 is the operating system designed by Microsoft and IBM to be the successor of MS-DOS. Dropped by Microsoft. See comp.os.os2. Windows 2000 actively tries to destroy OS/2 Boot Manager. See [below](#).

a Coherent swap partition

a OPUS

Open Parallel Unisys Server. See [Unisys](#).

b WIN95 OSR2 32-bit FAT

Partitions up to 2047GB. See [Partition Types](#)

c WIN95 OSR2 32-bit FAT, LBA-mapped

Extended-INT13 equivalent of b.

e WIN95 DOS 16-bit FAT, LBA-mapped

f WIN95 Extended partition, LBA-mapped

Windows 95 uses **e** and **f** as the extended-INT13 equivalents of **6** and **5**. For the problems this causes, see [Windows 95 FDISK problems](#) and [Possible data loss with LBA and INT13 extensions](#). (Especially when going back and forth between MSDOS and Windows 95, strange things may happen with a type **e** or **f** partition.) Windows NT does not recognize the four W95 type's **b**, **c**, **e**, **f** ([Win95 Partition Types Not Recognized by Windows NT](#)).

10 OPUS (?)

Maybe decimal, for type **a**.

11 Hidden DOS 12-bit FAT

When it boots a DOS partition, OS/2 Boot Manager will hide all primary DOS partitions except the one that is booted, by changing its ID **1,4,6** becomes **11,14,16**. In addition, **7** becomes **17**.

12 Compaq config partition

ID 12 (decimal 18) is used by Compaq for its configuration utility partition. It is a FAT-compatible partition (about 6 MB) that boots into their utilities, and can be added to a LILO menu as if it were MS-DOS (David C. Niemi). Stephen Collins reports a 12 MB partition with ID 12 on a Compaq 7330T. Tigran A. Aivazian reports a 40 MB partition with ID 12 on a 64 MB Compaq Proliant 1600. ID 12 is used by the Compaq Contura to denote its hibernation partition (dan@fch.wimsey.bc.ca).

14 Hidden DOS 16-bit FAT <32M

(Ralf Brown's interrupt list adds `ID 14 resulted from using Novell DOS 7.0 FDISK to delete Linux Native partition'.)

16 Hidden DOS 16-bit FAT >=32M

17 Hidden IFS (e.g., HPFS)

18 AST Windows swapfile

(`Zero Volt Suspend Partition' or `SmartSleep Partition', 2MB+memory size) See [AST](#).

19

Used for Willowtech Photon coS (completely optimized system) by willow@dezine.net. See dejanews.

1b Hidden WIN95 OSR2 32-bit FAT

1c Hidden WIN95 OSR2 32-bit FAT, LBA-mapped

1e Hidden FAT95

20

Rumored to be used by Willowsoft Overture File System (OFS1), if it exists.

21 Reserved

(According to [delorie](#)). Used for FS02 (Oxygen File System) by ekstazy@ sprint.ca. See dejanews.

22 Used for Oxygen Extended Partition Table by ekstazy@sprint.ca.

23 Reserved

24 NEC DOS 3.x

26 Reserved**31 Reserved****33 Reserved****34 Reserved****35 JFS on OS/2 or eCS**

David van Enckevort (david@mensys.nl) writes *Type 0x35 is used by OS/2 Warp Server for e-Business, OS/2 Convenience Pack (aka EnCase Version 4.5) and eComStation (eCS, an OEM version of OS/2 Convenience Pack) for the OS/2 implementation of JFS (IBM AIX Journaling Filesystem).* Since JFS is a non-bootable file system, you cannot install eCS to a JFS partition.

36 Reserved**38 THEOS ver 3.2 2gb partition****39 Plan 9 partition**

[Plan 9](#) is an operating system developed at Bell Labs for many architectures. Source is available. See [comp.os.plan9](#). Originally Plan 9 used an unallocated portion at the end of the disk. Plan 9 third edition uses partitions of [type 0x39](#), subdivided into subpartitions described in the Plan 9 partition table in the second sector of the partition.

39 THEOS ver 4 spanned partition**3a THEOS ver 4 4gb partition****3b THEOS ver 4 extended partition**

THEOS is a multi-user multitasking OS for PCs founded by Timothy Williams in 1983. Current release 4.0, previous release 3.2. They say about themselves 'THEOS with over 150,000 customers and over 1,000,000 users around the world brings a mainframe look and feel to computers without the complexity and high maintenance costs. Hundreds of applications exist with networking and Windows integration.' See [the Theos home page](#)

3c PartitionMagic recovery partition

Cody Batt (codyb@powerquest.com) writes When a [PowerQuest](#) product like [PartitionMagic](#) or [Drive Image](#) makes changes to the disk, it first changes the type

flag to 0x3C so that the OS won't try to modify it etc. At the end of the process, it gets changed back to what it was at first. So, the only time you should see a 0x3C type flag is if the process was interrupted somehow (power outage, user reboot etc). If you change it back manually with a partition table editor or something then most of the time everything is okay.

40 Venix 80286

A very old Unix-like operating system for PCs.

41 Linux/MINIX (sharing disk with DRDOS)

Very old FAQs recommended to use **41** etc instead of **81** etc on a disk shared with DRDOS because DRDOS allegedly disregards the high order bit of the partition type. These types are not used anymore today. Roger Wolff (R.E.Wolff@BitWizard.nl) confirms *I remember installing DRDOS, and getting a few extra drive letters that I didn't expect. Turns out those are my Minix partitions. It is looking at them as a FAT filesystem. Looks like a big mess. After finding no other possibility than to just "not touch those drive letters" I continue with the install. After a few minutes DRDOS automatically decides to write a copy of the FAT into a file on one of my MINIX partitions. Bye bye Minix partition.*

41 Personal RISC Boot

41 PPC PReP (Power PC Reference Platform) Boot

42 Linux swap (sharing disk with DRDOS)

42 SFS (Secure Filesystem)

SFS is an encrypted filesystem driver for DOS on 386+ PCs, written by Peter Gutmann.

42 Windows 2000 marker

If a partition table entry of type 0x42 is present in the legacy partition table, then W2K ignores the legacy partition table and uses a proprietary partition table and a proprietary partitioning scheme (LDM or DDM). As the Microsoft KnowledgeBase writes *Pure dynamic disks (those not containing any hard-linked partitions) have only a single partition table entry (type **42**) to define the entire disk. Dynamic disks store their volume configuration in a database located in a 1-MB private region at the end of each dynamic disk.*

43 Linux native (sharing disk with DRDOS)

44 Go Back! partition**45 Boot-US boot manager**

Ulrich Straub (ustraub@boot-us.de) writes The boot manager can be installed to MBR, a separate primary partition or diskette. When installed to a primary partition this partition gets the ID 45h. This partition does not contain a file system, it contains only the boot manager and occupies a single cylinder (below 8 GB). See www.boot-us.com.

45 EUMEL/Elan**46 EUMEL/Elan****47 EUMEL/Elan****48 EUMEL/Elan**

Eumel, and later Ergos L3, are multi-user multitasking systems developed by Jochen Liedtke at GMD. It was used at German schools for the computer science education. ([Elan](#) was the programming language used.)

4a AdaOS Aquila (Default)

Nick Roberts (nickroberts@adaos.worldonline.co.uk) writes I am a member of a project creating a new operating system, called AdaOS, see www.AdaOS.org, with storage manager called Aquila. We wish to use partition type code **4a** to allow Aquila to know which partitions to (attempt to) 'mount' during bootup. Aquila will support striping, ghosting, and coagulation. Every Aquila partition will have the byte sequence <41 51 55 49 4C 41> hex at offset 0 of the first actual sector of the Aquila volume. Aquila will only recognize a primary partition.

4d QNX4.x**4e QNX4.x 2nd part****4f QNX4.x third part**

QNX is a POSIX-certified, microkernel, distributed, fault-tolerant OS for the 386 and up, including support for the 386EX in embedded applications. For info see <http://www.qnx.com/> or <ftp://ftp.qnx.com>. See also comp.os.qnx. ID 7 is outdated - QNX2 used 7, QNX4.x uses 77, and optionally 78 and 79 for additional QNX partitions on a single drive. These values 77, 78, 79 seem to be the decimal values in view of [QNX Partitions](#) and [Neutrino filesystems](#).

4f Oberon partition

See <http://www.oberon.ethz.ch/native/>. (The partition ID is given in [this posting](#) in comp.lang.oberon. The [install instructions](#) say that at most one partition can have this type (decimal 79), and that one needs a different type, like **50** (decimal 80) for a second Oberon system. Moreover, that users of System Commander must avoid types containing the 0x10 bit.)

50 OnTrack Disk Manager (older versions) RO

Disk Manager is a program of OnTrack, to enable people to use IDE disks that are larger than 504MB under DOS. For info see <http://www.ontrack.com>. Linux kernel versions older than 1.3.14 do not coexist with DM.

50 Lynx RTOS

"Beginning with version 3.0, LynxOS gives users the ability to place up to 14 partitions of 2 GB each on both SCSI and IDE drives, for a total of up to 28 GB of file system space." See www.lynuxworks.com.

50 Native Oberon (alt)**51 OnTrack Disk Manager RW (DM6 Aux1)****51 Novell****52 CP/M****52 Micropoint SysV/AT****53 Disk Manager 6.0 Aux3****54 Disk Manager 6.0 Dynamic Drive Overlay****55 EZ-Drive**

EZ-Drive is another disk manager (by MicroHouse, 1992). Linux kernel versions older than 1.3.29 do not coexist with EZD. (On 990323 MicroHouse International was acquired by EarthWeb; MicroHouse Solutions split off and changed its name into [StorageSoft](#). MicroHouse Development split off and changed its name into [ImageCast](#). It is StorageSoft that now markets EZDrive and DrivePro.)

56 Golden Bow VFeature Partitioned Volume.

This is a Non-Standard DOS Volume. (Disk Manager type utility software)

56 DM converted to EZ-BIOS

57 DrivePro

Doug Anderson (DougA@ImageCast.com), with his brother Steve cofounder of MicroHouse (1989), writes We actually use three different partition types \$55 `StorageSoft EZ-BIOS' - EZ-Drive, Maxtor, MaxBlast, and DriveGuide install this type if the drive needs to be handled by our INT13 redirector. \$56 `StorageSoft EZ-BIOS DM Conversion' - Same as \$55 but used when a DiskManager "skewed" partition has been converted to EZ-BIOS. \$57 `StorageSoft DrivePro' - Used by our DrivePro product.

57 VNDI Partition

(According to disk.c in the Netware source. Not in actual use.)

5c Priam EDisk

Priam EDisk Partitioned Volume. This is a Non-Standard DOS Volume. (Disk Manager type utility software)

61 SpeedStor

Storage Dimensions SpeedStor Volume. This is a Non-Standard DOS Volume. (Disk Manager type utility software)

63 Unix System V (SCO, ISC Unix, UnixWare, ...), Mach, GNU Hurd

A Unixware 7.1 partition must start below the 4GB limit. (If the /stand/stage3.blm is located past this limit, booting will fail with "FATAL BOOT ERROR Can't load stage3".)

64 PC-ARMOUR protected partition

Used by PC-ARMOUR, a disk protection by Dr. A.Solomon, intended to keep the disk inaccessible until the right password was given (and then an int13 hook was loaded above top-of-memory that showed c/h/s 0/0/2, with a copy of the real partition table, when 0/0/1 was requested). (loekw@worldonline.nl)

64 Novell Netware 286, 2.xx

65 Novell Netware 386, 3.xx or 4.xx

(Novell Netware used to be the main Network Operating System available. Netware 68 or S-Net (1983) was for a Motorola 68000, Netware 86 for an Intel 8086 or 8088. Netware 286 was for an Intel 80286 and existed in various versions that were later merged to Netware 2.2. Netware 386 was a rewrite in C

for the Intel 386, later renamed 3.x - it existed at least in versions 3.0, 3.1, 3.10, 3.11, 3.12. Its successor Netware 4.xx had versions 4.00, 4.01, 4.02, 4.10, 4.11. Then Intranetware was introduced.) Netware >= 3.0 uses one partition per drive. It allocates logical Volumes inside these partitions. The volumes can be split over several drives. The filesystem used is called "Turbo FAT"; it only very vaguely resembles the DOS FAT file system. (Kai Henningsen (kai@khms.westfalen.de))

66 Novell Netware SMS Partition

According to disk.c in the Netware source. SMS Storage Management Services. No longer used.

67 Novell

Roman Gruber reports this code has frozen my version of Norton disk-editor (so I think it has to be something special). Jeff Merkey says 67 is for Wolf Mountain.

68 Novell

69 Novell Netware NSS Partition

According to disk.c in the Netware source.

6e ??

[Reported once.](#)

70 DiskSecure Multi-Boot

71 Reserved

73 Reserved

74 Reserved

74 Scramdisk partition

[Scramdisk](#) is freeware and shareware disk encryption software. It supports container files, dedicated partitions (type 0x74) and disks hidden in WAV audio files. (Shaun Hollingworth (moatlane@btconnect.com))

75 IBM PC/IX

76 Reserved

77 M2FS/M2CS partition

Jeff Merkey writes 77 is one we are using internally for M2FS/M2CS partitions.

77 VNDI Partition

(According to disk.c in the Netware source. Not in actual use.)

78 XOSL FS

XOSL Bootloader filesystem, see www.xosl.org.

7E

Used for F.I.X. by gruberr@kapsch.net. See dejanews.

80 MINIX until 1.4a

81 MINIX since 1.4b, early Linux

Minix is a Unix-like operating system written by Andy Tanenbaum and students at the Vrije Universiteit, Amsterdam, between 1989-1991. It runs on PCs (8086 and up), Macintosh, Atari, Amiga, Sparc. Ref Operating Systems Design and Implementation, Andrew S. Tanenbaum, Prentice-Hall, ISBN 0-13-637406-9 Since 950601 Minix is freely available - site <ftp.cs.vu.nl>. See also comp.os.minix.

81 Mitac disk manager

82 Prime

82 Solaris x86

Solaris creates a single partition with id 0x82, then uses Sun disk labels within the partition to split it further. (Brandon S. Allbery (allbery@kf8nh.apk.net))

82 Linux swap

83 Linux native (usually ext2fs)

Linux is a Unix-like operating system written by Linus Torvalds and many others on the internet since Fall 1991. It runs on PCs (386 and up) and a variety of other hardware. It is distributed under GPL. Software can be found numerous places, like <ftp.funet.fi>, <metalab.unc.edu> and <tsx-11.mit.edu>. See also comp.os.linux.* and <http://www.linux.org/>.

84 OS/2 hidden C drive

OS/2-renumbered type **04** partition.

84 Hibernation partition

(following Appendix E of the Microsoft APM 1.1f specification). Reported for various laptop models. E.g., used on Dell Latitudes (with Dell BIOS) that use the MKS2D utility.

85 Linux extended partition

86 Old Linux RAID partition superblock

See fd.

86 NTFS volume set

Legacy Fault Tolerant FAT16 volume. Windows NT 4.0 or earlier will add 0x80 to the partition type for partitions that are part of a Fault Tolerant set (mirrored or in a RAID-5 volume). Thus, one gets types **86, 87, 8b, 8c**. See also [Windows NT Boot Process and Hard Disk Constraints](#).

87 NTFS volume set

Legacy Fault Tolerant NTFS volume.

8a Linux Kernel Partition (used by AiR-BOOT)

Martin Kiewitz (KiWi@vision.fido.de) writes I'm currently writing a pretty nice boot-loader. For this I'm using Linux Boot Loader ID A0h, and partition type 8Ah for the partition holding the kernel image.

8b Legacy Fault Tolerant FAT32 volume

8c Legacy Fault Tolerant FAT32 volume using BIOS extd INT 13h

8d Free FDISK hidden Primary DOS FAT12 partition

[Free FDISK](#) is the FDISK used by [FreeDOS](#). It hides types **1, 4, 5, 6, b, c, e, f** by adding decimal 140 (0x8c).

8e Linux Logical Volume Manager partition

See [pvcreate\(8\)](#) as found under <http://linux.msede.com/lvm>. (For a while this was 0xfe.)

90 Free FDISK hidden Primary DOS FAT16 partition

91 Free FDISK hidden DOS extended partition

92 Free FDISK hidden Primary DOS large FAT16 partition

93 Amoeba

94 Amoeba bad block table

Amoeba is a distributed operating system written by Andy Tanenbaum, together with Frans Kaashoek, Sape Mullender, Robert van Renesse and others since 1981. It runs on PCs (386 and up), Sun3, Sparc, 68030. It is free for universities for research/teaching purposes. For information, see <ftp.cs.vu.nl>.

95 MIT EXOPC native partitions

<http://www.pdos.lcs.mit.edu/exo/> (Andrew Purtell, Andrew_Purtell@NAI.com)

97 Free FDISK hidden Primary DOS FAT32 partition**98 Free FDISK hidden Primary DOS FAT32 partition (LBA)****99 DCE376 logical drive**

No, it's not a hibernation partition; it's closest to a DOS extended partition. It's used by the Mylex DCE376 EISA SCSI adaptor for partitions which are beyond the 1024th cylinder of a drive. I've only seen references to type **99** with the DCE376. (Christian Carey, ccarey@CapAccess.ORG)

9a Free FDISK hidden Primary DOS FAT16 partition (LBA)**9b Free FDISK hidden DOS extended partition (LBA)****9f BSD/OS**

Current sysid for BSDI. The type's **b7** and **b8** given below are for an older version of the filesystem used in pre-v3.0 versions of the OS. These days the system is EnCase Version 4.1 BSD/OS. BSDI reports 2.1 million installed servers and 12 million licenses sold. See <http://www.bsdi.com/>.

a0 Laptop hibernation partition

Reported for various laptops like IBM Thinkpad, Phoenix NoteBIOS, Toshiba under names like zero-volt suspend partition, suspend-to-disk partition, save-to-disk partition, power-management partition, hibernation partition. Usually at the start or end of the disk area. (This is also the number used by Sony on the VAIO. Recent VAIOs can also hibernate to a file in the filesystem, the choice being made from the BIOS setup screen.)

a1 Laptop hibernation partition

Reportedly used as "Save-to-Disk" partition on a NEC 6000H notebook. Type's **a0** and **a1** are used on systems with Phoenix BIOS; the Phoenix PHDISK utility is used with these.

a3 Reserved

a4 Reserved

a5 BSD/386, 386BSD, NetBSD, FreeBSD

386BSD is a Unix-like operating system, a port of 4.3BSD Net/2 to the PC done by Bill Jolitz around 1991. When Jolitz seemed to stop development, an updated version was called FreeBSD (1992). The outcome of a Novell vs. UCB law suit was that Net/2 contained AT&T code, and hence was not free, but that 4.4BSD-Lite was free. After that, FreeBSD and NetBSD were restructured, and FreeBSD 2.0 and NetBSD 1.0 are based on 4.4BSD-Lite. FreeBSD runs on PCs. See <http://www.freebsd.org/FreeBSD.html>. For NetBSD, see below - it changed partition type to **a9**. 386BSD seems to be dead now. The kernel source is being published - see [Operating System Source Code Secrets](#) by Bill and Lynne Jolitz. See comp.os.386bsd.*. See <http://www.paranoia.com/~vax/boot.html> for NetBSD boot and partitioning info.

a6 OpenBSD

OpenBSD, led by Theo de Raadt, split off from NetBSD. It tries to emphasize on security. See <http://www.openbsd.org/>.

a7 NEXTSTEP

Based on Mach 2.6 and features of Mach 3.0, is a true object-oriented operating system and user environment. See <http://www.next.com/>.

a9 NetBSD

NetBSD is one of the children of *BSD (see above). It runs on PCs and a variety of other hardware. Since 19-Feb-98 NetBSD uses **a9** instead of **a5**. See <http://www.netbsd.org/>. It is freely obtainable - see <http://www.netbsd.org/Sites/net.html>.

aa Olivetti Fat 12 1.44Mb Service Partition

Contains a bare DOS 6.22 and a utility to exchange types **06** and **aa** in the partition table. (loekw@worldonline.nl)

ae ShagOS filesystem

Copyright © 2004 Guidance Software, Inc.

May not be copied or reproduced without the written permission of Guidance Software, Inc.

a ShagOS swap partition

Unused. Claimed by Frank Barrus for his [ShagOS](#).

b1 Reserved**b3 Reserved****b4 Reserved****b6 Reserved****b7 BSDI BSD/386 filesystem****b8 BSDI BSD/386 swap partition**

BSDI (Berkeley Software Design, Inc.) was founded by former CSRG (UCB Computer Systems Research Group) members. Their operating system, based on Net/2, was called BSD/386. After the USL (Unix System Laboratories, Inc./Novell Corp.) vs. BSDI lawsuit, new releases were based on BSD4.4-Lite. Now they are announcing BSD/OS V2.0.1. This is an operating for PCs (386 and up), boasting 3000 customers. (That was long ago. The current partition id is f, see above.)

be Solaris 8 boot partition**c0 CTOS****c0 REAL/32 secure small partition**

See d0 below.

c0 NTFT Partition

According to disk.c in the Netware source.

c1 DRDOS/secured (FAT-12)**c2 Hidden Linux****c3 Hidden Linux swap**

Benedict Chong (bchong@blueskyinnovations.com) writes [BlueSky Innovations LLC](#) does a boot manager product called Power Boot and we use, in addition, 0C2h and 0C3h for hidden Linux partitions (both ext2fs and swap).

c4 DRDOS/secured (FAT-16, < 32M)**c6 DRDOS/secured (FAT-16, >= 32M)**

DR-DOS 6.0 will add 0xc0 to the partition type for a LOGIN.EXE-secured partition (so that people cannot avoid the password check by booting from an MS-DOS floppy).

c6 Windows NT corrupted FAT16 volume/stripe set

NTFS will add 0xc0 to the partition type for disabled parts of a Fault Tolerant set. Thus, one gets types **c6**, **c7**. See also [Windows NT Boot Process and Hard Disk Constraints](#) and [Switching from DR-DOS 6.0 to MS-DOS 5.0](#).

c7 Windows NT corrupted NTFS volume/stripe set

c7 Syrinx boot

cb reserved for DRDOS/secured (FAT32)

cc reserved for DRDOS/secured (FAT32, LBA)

cd CTOS Memdump?

ce reserved for DRDOS/secured (FAT16, LBA)

d0 REAL/32 secure big partition

REAL/32 is a continuation of DR Multiuser DOS. Andrew Freeman (afreeman@imsltd.com) writes REAL/32 supports the standard FAT12, FAT16 partition types and will shortly support FAT32. For partitions which have been marked as secure we use 0xC0 and 0xD0 as partition markers (C0 < 32mb, D0 >= 32mb). REAL/32 is an advanced 32-bit multitasking & multi-user MS-DOS & Windows compatible operating system. Home page is www.imsltd.com.

d1 Old Multiuser DOS secured FAT12

d4 Old Multiuser DOS secured FAT16 <32M

d5 Old Multiuser DOS secured extended partition

d6 Old Multiuser DOS secured FAT16 >=32M

The reports on d1, d4, d5, d6 may be mistaken? They could be c1, c4, c5, c6 hidden by System Commander or so.

d8 CP/M-86

da Non-FS Data

Added on request of John Hardin (johnh@aproposretail.com).

db Digital Research CP/M, Concurrent CP/M, Concurrent DOS**db CTOS (Convergent Technologies OS -Unisys)****db KDG Telemetry SCPU boot**

Mark Morgan Lloyd (markMLI.in@telemetry.co.uk) writes [KDGT Telemetry](#) uses type 0xdb to store a protected-mode binary image of the code to be run on a 'x86-based SCPU (Supervisory CPU) module from the DT800 range.

dd Hidden CTOS Memdump?**de Dell PowerEdge Server utilities (FAT fs)****df DG/UX virtual disk manager partition**

Glenn Steen (glenn.steen@ap1.se) writes When I made an old Aviion 2000 triple-boot (DOS, DG/UX and Linux) I saw that Linux FDISK reported the DG/UX virtual disk manager partition as type 0xdf.

e0 Reserved by [STMicroelectronics](#) for a filesystem called ST AVFS.**e1 DOS access or SpeedStor 12-bit FAT extended partition****e3 DOS R/O or SpeedStor****e4 SpeedStor 16-bit FAT extended partition < 1024 cyl.****e5 Reserved****e6 Reserved****eb BeOS**

BeOS is an operating system that runs on Power PCs and, since recently, on Intel PCs. See <http://www.be.com/>.

ee Indication that this legacy MBR is followed by an EFI header**ef Partition that contains an EFI file system**

Bob Griswold (rogris@Exchange.Microsoft.com) writes MS plans on using EE and EF in the future for support of non-legacy BIOS booting. Mark Doran (mark.doran@intel.com) adds these types are used to support the Extensible Firmware Interface specification (EFI); go to developer.intel.com and search for EFI. (For the types ee and ef, see Tables 16-6 and 16-7 of the EFI specification, EFISpec_091.pdf.)

f0 Linux/PA-RISC boot loader

Paul Bame (bame@endor.fc.hp.com) writes the F0 partition will be located in the first 2GB of a drive and used to store the [Linux/PA-RISC](#) boot loader and boot command line, optionally including a kernel and ramdisk.

f1 SpeedStor**f2 DOS 3.3+ secondary partition****f3 Reserved****f4 SpeedStor large partition****f4 Prologue single-volume partition****f5 Prologue multi-volume partition**

The type F4 partition contains one volume, and is not used anymore. The type F5 partition contains 1 to 10 volumes (called MD0 to MD9). It supports one or more systems (Prologue 3, 4, 5, Twin Server). Each volume can have as file system the NGF file system or TwinFS file system. NGF (old) volume size at most 512 MB, at most 895 files per directory, at most 256 directories per volume. TwinFS (new) volume size up to 4 GB. No limit in number of files and directories. See [Prologue](#).

f6 Reserved**fb VMware File System partition****fc VMware Swap partition**

[VMware](#) offers virtual machines in which one can run Linux, Windows, FreeBSD. These partition IDs announced by Dan Scales (scales@vmware.com).

fd Linux raid partition with auto detect using persistent superblock

See the [HOWTO](#) and the [kernel patches](#). Earlier, 86 was used instead of fd.

fe SpeedStor > 1024 cyl. or LANstep

fe IBM PS/2 IML (Initial Microcode Load) partition, located at the end of the disk.

fe Windows NT Disk Administrator hidden partition

Mark Morgan Lloyd (markMLI.in@telemetry.co.uk) writes Windows NT Disk Administrator marks hidden partitions (i.e. present but not to be accessed) as type 0xfe. A primary partition of this type is also used by IBM to hold an image of the "Reference Diskettes" on many of their machines, particularly newer PS/2 systems (at a rough guess, anything built after about 1994). This clash can cause major confusion and grief if running NT on IBM kit. When this Reference Partition is activated, it changes its type into 1 (FAT12) and hides all other partitions by adding 0x10 to the type.

fe Linux Logical Volume Manager partition (old)

This has been in use since the early LVM days back in 1997, and has now (Sept. 1999) been renamed 0x8e.

ff Xenix Bad Block Table

Index

Absolute Sectors	403	Copying Folders.....	245
Acquiring Macs.....	108	CRC	416, 417
Acquiring UNIX.....	108	Cyclical Redundancy Check ...See CRC	
Active Code-Page	252	Cylinder.....	402
Active Processes.....	302, 304	Dates.....	349
Archive	337	DBX.....	271, 275
Big-Endian Unicode	252	Default Export Folder	176
BIOS.....	402	Devices	199
Bookmarks	198, 345	Disk	233, 404
Bookmarks tab	198	DOS	406
Boot Procedure	66, 68	Drive.....	404
Boot Sector	406	Drive Geometry.....	402
Case Management.....	177	DriveSpace	298, 304
Case sensitive.....	251	Dynamic Disk	37, 123
Cases	197	EnCase Boot Disk	61
CDFS File System.....	411	EnCase for DOS	69
CD-R	141, 146	EnCase Network Boot Disk	67, 68, 91
CD-ROM.....	141, 146	EnScript	41, 277, 304
CD-RW	141, 146	Blocks	439
Cluster	407	Break	441
Cluster Bitmaps.....	407	Classes	442
Code Page	319	Comments	432
Colors Options	180	Conditionals.....	439
Compression	414	Constructors	442
Console	234, 281, 304	Data Types	433
Console mode	129, 130	Dates	434
Copy / Unerase	241	Declarations.....	432
Copy Folders	245	Destructors	442

Copyright © 2004 Guidance Software, Inc.
May not be copied or reproduced without the written permission of Guidance Software, Inc.

Do Loops.....	440	Global Options	178
EntryClass.....	444	GREP	252
Enumerated Types.....	433	Tokens	252
FileClass	444	GREP Examples.....	426
Filters	446	hash	70
Floating Point.....	433	Hash.....	162, 415
For Loops.....	440	Hash Library.....	170
Functions	441	Hash Sets	162, 208
Integers	433	Hashing.....	70
Language Overview.....	431	Head.....	403
Operator Precedence	437	Hex.....	232
Operators	436	HFS	411
Programs	445	Home Plate	197
Runtime Library.....	447	HTML	385, 398
Statements.....	439	HTML pages	291, 304
Strings.....	434	Include Tab	287, 304
While Loops	439	INFO2.....	294, 304
EnScript Types	209	Initialize Case.....	173
Evidence File		Integers	349
Compressed.....	414	interface	175
Definition	417	Interface	196
Export the Report.....	385, 398	Internet History EScript.....	293, 304
EXT2 File System	410	Inter-Partition Space	407
Extended DOS Partition	406	Keywords	202, 249
FastBloc	111	Lock Box	236
FAT.....	410	Locking.....	70
File Entries	408	Logical File Size	409
File Group Bookmark	360, 363	Logical Restore	333
File Signature	416	logical volume	329
File Signatures	201, 246	Lost Files.....	156
File Slack.....	408	Master Boot Record	406
File Types.....	200	Master File Table	156
File Viewers.....	201, 245	MD5.....	415, 417
Filters.....	234	Message Board.....	25
Filters.....	40, 282, 304, 446	MFT	156
Flash media.....	142, 146	Mode	76
Floppy Disks.....	141, 146	Network Cable Acquisition	94
Folder Information Bookmark.....	354	New Case	175
Fonts	314	Notable File Bookmark.....	356
Fonts Options	181	Notes Bookmark	352
foreign language keywords	322	NSRL Hash Sets.....	167
Functions.....	441	NTFS compressed files.....	275
Gallery View	226	NTFS Compression	39

NTFS File Permissions	38	Search Hits	202, 264
NTFS File System	410	Sector.....	403
OLE Files.....	269	Security IDs.....	203
Open Files	305	Security key	
Open Ports	301, 304	Drivers	50
Palm PDAs.....	129	Parallel Port.....	47
parallel port	83	USB	47
Partition Boot Sector	406	Security Key	46
Partition Table	406	Server mode	74
Physical File Size	409	Signature Analysis	157
Physical Restore	331	Software RAID	122
physical volume.....	329	Sorting.....	220
Picture	233	Storage	401
Pictures	349	Styles	350
preview	79	Subject	401
Programs.....	445	Superdisks	141, 146
PST Files.....	35	System Snapshot.....	299, 304
Queries.....	234, 284, 304	Table View	210
query		Technical Support.....	25
start.....	284, 304	Temporary Folder	176
stop	284, 304	Text	232, 348
RAM	402	Text Fragment.....	347
RAM Slack.....	409	Text Styles	206, 313
Raw Image	191	Time Zone Support	35
recover	241	Timeline View.....	228
Recover Folders.....	151	to Drive.....	99
Recover NTFS Folders	154	Track	403
Recovering Partitions	289, 304	UFS	411
Regional Settings	325	unerase	241
Registry	268	Unicode	35, 252
Report.....	233	Updates	55
Report View.....	230	UTF7	253
restore	329	UTF-8.....	252
ROM	402	verify.....	190, 418
Root Folder	407	Verifying	190
RTF	385, 398	View Search Hits.....	265
RTL Reading	252	Volatile Data.....	299, 304
SafeBack.....	106	Volume	404
Script Security	182, 183	Web	291, 304
Scripts	207	Windows	350
SCSI.....	127	Zip Disks	139, 146
Search	257	Zipped	270, 275