

Contents

<i>Foreword</i>		<i>x</i>
<i>About the Authors</i>		<i>xi</i>
<i>Introduction</i>		<i>xix</i>
<i>Assessment Test</i>		<i>xxiv</i>
Chapter 1	Computer Hardware	1
	Computer Hardware Components	2
	The Boot Process	11
	Partitions	16
	File Systems	19
	Summary	20
	Exam Essentials	21
	Review Questions	22
	Answers to Review Questions	26
Chapter 2	File Systems	29
	FAT Basics	30
	The Physical Layout of FAT	31
	The Function of FAT	50
	NTFS (New Technology File System)	65
	CD File Systems	68
	Summary	69
	Exam Essentials	70
	Review Questions	71
	Answers to Review Questions	75
Chapter 3	First Response	77
	Planning and Preparation	78
	The Physical Location	79
	Personnel	79
	Computer Systems	80
	Deciding What to Take with You Before You Leave	82
	Search Authority	84
	Handling Evidence at the Scene	85
	Securing the Scene	85
	Recording and Photographing the Scene	85
	Shutting Down Computers	85
	Bagging and Tagging	92

	Summary	95
	Exam Essentials	95
	Review Questions	97
	Answers to Review Questions	101
Chapter 4	Acquiring Digital Evidence	103
	Creating EnCase Forensic Boot Disks	105
	Booting a Computer Using the EnCase Boot Disk	107
	Steps to Follow	108
	Drive-to-Drive DOS Acquisition	110
	Steps to Follow	110
	Supplemental Information	114
	Network and Parallel Cable Acquisitions	116
	Steps to Follow	119
	FastBloc Acquisitions	129
	Steps to Follow	129
	LinEn Acquisitions	135
	Steps to Follow	137
	Enterprise and FIM Acquisitions	140
	Helpful Hints	144
	Summary	145
	Exam Essentials	146
	Review Questions	148
	Answers to Review Questions	152
Chapter 5	EnCase Concepts	155
	EnCase Evidence File Format	156
	CRC and MD5	157
	Evidence File Components and Function	158
	Evidence File Verification	161
	Hashing Disks and Volumes	167
	EnCase Case Files	169
	EnCase Backup File (cbak)	170
	EnCase Configuration Files	173
	Summary	176
	Exam Essentials	177
	Review Questions	178
	Answers to Review Questions	182
Chapter 6	EnCase Environment	183
	EnCase Layout	184
	Creating a Case	185
	Tree Pane Navigation	189

xvi Contents

Table Pane Navigation	194
Table View Tab	194
Report Tab	202
Gallery Tab	202
Disk Tab	204
Timeline Tab	206
Code Tab	209
View Pane Navigation	209
Text View	209
Hex View	209
Picture View	211
Report View	212
Console View	212
Details View	213
Lock	213
Dixon Box	213
Navigation Data (GPS)	215
Find Feature	216
Other Views	217
Adjusting Panes	218
Other Case-Level Views	222
Global Views	224
EnCase Options	228
Summary	233
Exam Essentials	234
Review Questions	236
Answers to Review Questions	239
Chapter 7 Understanding, Searching for, and Bookmarking Data	241
Understanding Data	243
Binary Numbers	243
Hexadecimal	249
Characters	252
ASCII	252
Unicode	253
Searching for Data	254
Creating and Managing Keywords	255
GREP Keywords	264
Starting a Search	272
Viewing Search Hits and Bookmarking your Findings	275
Bookmarking	279
Summary	297
Exam Essentials	299

	Review Questions	300
	Answers to Review Questions	304
Chapter 8	File Signature Analysis and Hash Analysis	307
	File Signature Analysis	308
	Understanding Application Binding	308
	Creating a New File Signature	310
	Conducting a File Signature Analysis	313
	Hash Analysis	318
	MD5 Hash	319
	Hash Sets and Hash Libraries	319
	Hash Analysis	322
	Summary	328
	Exam Essentials	329
	Review Questions	330
	Answers to Review Questions	333
Chapter 9	Windows Operating System Artifacts	335
	Dates and Times	336
	Time Zones	337
	Windows 64-Bit Time Stamp	338
	Adjusting for Time Zone Offsets	342
	Recycle Bin	347
	Link Files	357
	Windows 2000 and XP Folders	363
	Recent Folder	366
	Desktop Folder	367
	My Documents	368
	Send To Folder	368
	Temp Folder	369
	Favorites Folder	369
	Cookies Folder	371
	History Folder	372
	Temporary Internet Files	376
	Swap File	380
	Hibernation File	381
	Print Spooling	382
	Legacy Operating System Artifacts	386
	Summary	390
	Exam Essentials	393
	Review Questions	395
	Answers to Review Questions	399

xviii Contents

Chapter 10	Advanced EnCase	401
	Locating and Mounting Partitions	403
	Mounting Files	412
	Registry	417
	Registry History	417
	Registry Organization and Terminology	418
	Using EnCase to Mount and View the Registry	423
	Registry Research Techniques	425
	EnScript and Filters	437
	EnScript Navigation and Paths	438
	Editing, Copying, Moving, and Deleting EnScripts	439
	Running EnScripts	440
	Filters, Conditions, and Queries	440
	E-mail	442
	Base64 Encoding	449
	EnCase Decryption Suite (EDS)	456
	Virtual File System (VFS)	458
	Exporting Applications	462
	Restoration	465
	Physical Disk Emulator (PDE)	468
	Putting It All Together	472
	Summary	475
	Exam Essentials	478
	Review Questions	479
	Answers to Review Questions	483
Appendix A	Creating Paperless Reports	485
Glossary		499
<i>Index</i>		507