File System Forensic Analysis

Brian Carrier

Addison-Wesley

Upper Saddle River, NJ • Boston • Indianapolis • San Francisco
New York • Toronto • Montreal • London • Munich • Paris • Madrid
Capetown • Sydney • Tokyo • Singapore • Mexico City

Contents

	Foreword	xiii
	Preface	xv
	Acknowledgments	xix
PART I	**FOUNDATIONS**	
Chapter 1	Digital Investigation Foundations	3
	Digital Investigations and Evidence	3
	Digital Crime Scene Investigation Process	5
	Data Analysis	10
	Overview of Toolkits	13
	Summary	15
	Bibliography	16
Chapter 2	Computer Foundations	17
	Data Organization	17
	Booting Process	27
	Hard Disk Technology	29
	Summary	44
	Bibiography	45
Chapter 3	Hard Disk Data Acquisition	47
	Introduction	47
	Reading the Source Data	49
	Writing the Output Data	56

	A Case Study Using dd	60
	Summary	66
	Bibliography	66
PART II	**VOLUME ANALYSIS**	
Chapter 4	Volume Analysis	69
	Introduction	69
	Background	70
	Analysis Basics	75
	Summary	80
Chapter 5	PC-based Partitions	81
	DOS Partitions	81
	Apple Partitions	101
	Removable Media	107
	Bibliography	109
Chapter 6	Server-based Partitions	111
	BSD Partitions	111
	Sun Solaris Slices	127
	GPT Partitions	139
	Summary	145
	Bibliography	145
Chapter 7	Multiple Disk Volumes	147
	RAID	147
	Disk Spanning	156
	Bibliography	170
PART III	**FILE SYSTEM ANALYSIS**	
Chapter 8	File System Analysis	173
	What Is a File System?	173
	File System Category	177
	Content Category	178
	Metadata Category	186

	File Name Category	198
	Application Category	205
	Application-level Search Techniques	206
	Specific File Systems	207
	Summary	208
	Bibliography	209
Chapter 9	**FAT Concepts and Analysis**	**211**
	Introduction	211
	File System Category	213
	Content Category	221
	Metadata Category	227
	File Name Category	239
	The Big Picture	244
	Other Topics	247
	Summary	250
	Bibliography	251
Chapter 10	**FAT Data Structures**	**253**
	Boot Sector	253
	FAT32 FSINFO	259
	FAT	260
	Directory Entries	261
	Long File Name Directory Entries	267
	Summary	271
	Bibliography	271
Chapter 11	**NTFS Concepts**	**273**
	Introduction	273
	Everything is a File	274
	MFT Concepts	274
	MFT Entry Attribute Concepts	279
	Other Attribute Concepts	284
	Indexes	290
	Analysis Tools	296
	Summary	297
	Bibliography	297

Chapter 12	NTFS Analysis	301
	File System Category	301
	Content Category	311
	Metadata Category	316
	File Name Category	333
	Application Category	339
	The Big Picture	344
	Other Topics	348
	Summary	349
	Bibliography	350
Chapter 13	NTFS Data Structures	351
	Basic Concepts	351
	Standard File Attributes	359
	Index Attributes and Data Structures	369
	File System Metadata Files	378
	Summary	395
	Bibliography	396
Chapter 14	Ext2 and Ext3 Concepts and Analysis	397
	Introduction	397
	File System Category	399
	Content Category	408
	Metadata Category	412
	File Name Category	423
	Application Category	437
	The Big Picture	441
	Other Topics	445
	Summary	447
	Bibliography	447
Chapter 15	Ext2 and Ext3 Data Structures	449
	Superblock	449
	Group Descriptor Tables	455
	Block Bitmap	456
	Inodes	457
	Extended Attributes	462
	Directory Entry	467
	Symbolic Link	470

	Hash Trees	470
	Journal Data Structures	472
	Summary	478
	Bibliography	478
Chapter 16	**UFS1 and UFS2 Concepts and Analysis**	**479**
	Introduction	479
	File System Category	481
	Content Category	488
	Metadata Category	492
	File Name Category	497
	The Big Picture	500
	Other Topics	504
	Summary	506
	Bibliography	506
Chapter 17	**UFS1 and UFS2 Data Structures**	**509**
	UFS1 Superblock	509
	UFS2 Superblock	515
	Cylinder Group Summary	520
	UFS1 Group Descriptor	521
	UFS2 Group Descriptor	524
	Block and Fragment Bitmaps	525
	UFS1 Inodes	527
	UFS2 Inodes	530
	UFS2 Extended Attributes	532
	Directory Entries	534
	Summary	536
	Bibliography	536
Appendix A	**The Sleuth Kit and Autopsy**	**537**
	The Sleuth Kit	537
	Autopsy	544
	Bibliography	545
	Index	**547**