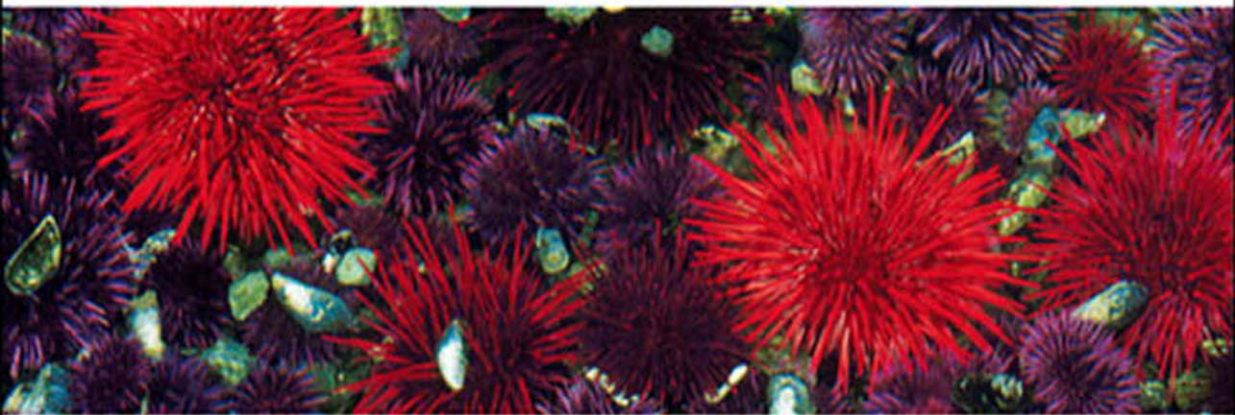


"This is the foundation book for file system analysis. Brian Carrier has done what needed to be done for this field."



—From the Foreword by **Mark M. Pollitt**, President, Digital Evidence Professional Services, Inc., and Retired Director of the FBI's Regional Computer Forensic Laboratory Program

# FILE SYSTEM FORENSIC ANALYSIS



BRIAN CARRIER

# **File System Forensic Analysis**

# File System Forensic Analysis

## Table of Contents

Contents

Foreword

Preface

Acknowledgments

### PART I: FOUNDATIONS

#### Chapter 1 Digital Investigation Foundations

Digital Investigations and Evidence

Digital Crime Scene Investigation Process

Data Analysis

Overview of Toolkits

Summary

Bibliography

#### Chapter 2 Computer Foundations

Data Organization

Booting Process

Hard Disk Technology

Summary

Bibliography

#### Chapter 3 Hard Disk Data Acquisition

Introduction

Reading the Source Data

Writing the Output Data

A Case Study Using dd

Summary

# Table of Contents

Bibliography

## PART II: VOLUME ANALYSIS

### Chapter 4 Volume Analysis

Introduction

Background

Analysis Basics

Summary

### Chapter 5 PC-based Partitions

DOS Partitions

Apple Partitions

Removable Media

Bibliography

### Chapter 6 Server-based Partitions

BSD Partitions

Sun Solaris Slices

GPT Partitions

Summary

Bibliography

### Chapter 7 Multiple Disk Volumes

RAID

Disk Spanning

Bibliography

## PART III: FILE SYSTEM ANALYSIS

### Chapter 8 File System Analysis

What Is a File System?

File System Category

Content Category

Metadata Category

File Name Category

# **Table of Contents**

- Application Category
- Application-level Search Techniques
- Specific File Systems
- Summary
- Bibliography

## **Chapter 9 FAT Concepts and Analysis**

- Introduction
- File System Category
- Content Category
- Metadata Category
- File Name Category
- The Big Picture
- Other Topics
- Summary
- Bibliography

## **Chapter 10 FAT Data Structures**

- Boot Sector
- FAT32 FSINFO
- FAT
- Directory Entries
- Long File Name Directory Entries
- Summary
- Bibliography

## **Chapter 11 NTFS Concepts**

- Introduction
- Everything is a File
- MFT Concepts
- MFT Entry Attribute Concepts
- Other Attribute Concepts

# Table of Contents

Indexes

Analysis Tools

Summary

Bibliography

## Chapter 12 NTFS Analysis

File System Category

Content Category

Metadata Category

File Name Category

Application Category

The Big Picture

Other Topics

Summary

Bibliography

## Chapter 13 NTFS Data Structures

Basic Concepts

Standard File Attributes

Index Attributes and Data Structures

File System Metadata Files

Summary

Bibliography

## Chapter 14 Ext2 and Ext3 Concepts and Analysis

Introduction

File System Category

Content Category

Metadata Category

File Name Category

Application Category

The Big Picture

# **Table of Contents**

Other Topics

Summary

Bibliography

## **Chapter 15 Ext2 and Ext3 Data Structures**

Superblock

Group Descriptor Tables

Block Bitmap

Inodes

Extended Attributes

Directory Entry

Symbolic Link

Hash Trees

Journal Data Structures

Summary

Bibliography

## **Chapter 16 UFS1 and UFS2 Concepts and Analysis**

Introduction

File System Category

Content Category

Metadata Category

File Name Category

The Big Picture

Other Topics

Summary

Bibliography

## **Chapter 17 UFS1 and UFS2 Data Structures**

UFS1 Superblock

UFS2 Superblock

Cylinder Group Summary

# **Table of Contents**

UFS1 Group Descriptor  
UFS2 Group Descriptor  
Block and Fragment Bitmaps  
UFS1 Inodes  
UFS2 Inodes  
UFS2 Extended Attributes  
Directory Entries  
Summary  
Bibliography

## **Appendix A: The Sleuth Kit and Autopsy**

The Sleuth Kit

Autopsy

Bibliography

Index