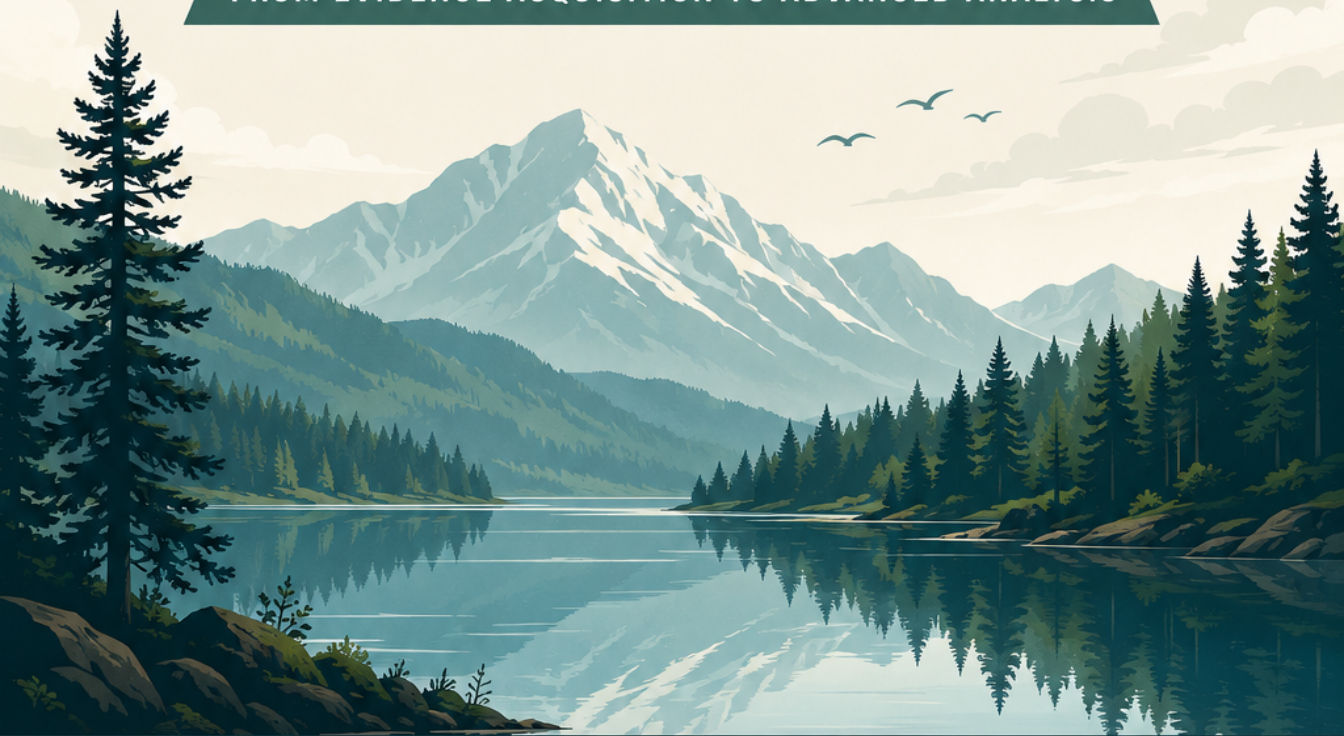


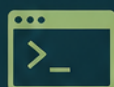
DIGITAL FORENSICS

A PRACTICAL GUIDE TO MODERN INVESTIGATIONS

FROM EVIDENCE ACQUISITION TO ADVANCED ANALYSIS



HANDS-ON
TECHNIQUES



COMMAND-LINE
EXAMPLES



REAL-WORLD
CASE STUDIES



INDUSTRY-STANDARD
TOOLS



BEST PRACTICES
FOR COURT

YAMAMOTO DAIKI

Digital Forensics: A Practical Guide to Modern Investigations

From Evidence Acquisition to Advanced Analysis

Steve T. Publications

This book is available at

<https://leanpub.com/digitalforensicsapragticalguidetomoderninvestigations>

This version was published on 2026-07-12



This is a [Leanpub](#) book. Leanpub empowers authors and publishers with the Lean Publishing process. [Lean Publishing](#) is the act of publishing an in-progress ebook using lightweight tools and many iterations to get reader feedback, pivot until you have the right book and build traction once you do.

© 2026 Steve T. Publications

Contents

From Evidence Acquisition to Advanced Analysis	1
Introduction: The Digital Crime Scene	2
Why This Book Exists	2
How to Use This Book	2
What You Will Need	2
Tool Version Matrix	2
Managing Tool Version Drift	2
A Note on Ethics and Legality	2
The Road Ahead	3
Running Case Studies	3
Chapter 1: Foundations of Digital Forensics	4
What Is Digital Forensics (and What It Is Not)	4
The Four Pillars: Identification, Preservation, Analysis, Presentation .	4
A Brief History: From Enron to Modern Cybercrime	4
The Investigator’s Mindset: Scientific Method Meets Detective Work .	4
Legal Foundations and Admissibility Standards	4
Summary	5
Chapter 2: Evidence Handling and Chain of Custody	6
Identifying Digital Evidence: Sources, Types, and Prioritization	6
The Chain of Custody Framework	6
The Evidence Acquisition Workflow	6
Write Blockers: Hardware and Software Solutions	6
Forensic Imaging: Bit-by-Bit Copies and Image Formats	6
Hashing and Integrity Verification (MD5, SHA-1, SHA-256, BKA)	6
Troubleshooting and Performance: Imaging Challenges	7
Chain of Custody Field Checklist	7
Summary	7

Chapter 3: File Systems and Operating System Artifacts 8

NTFS Internals: MFT, USN Journal, \$LogFile, and Alternate Data Streams 8

ext4 Forensics: Inodes, Journals, and Extents 8

APFS and HFS+: macOS File System Artifacts 8

Deleted Files, Slack Space, and Unallocated Space Recovery 8

Sleuth Kit and Autopsy: Command-Line File System Analysis 8

Cross-Platform Artifact Comparison Matrix 9

Summary 9

Chapter 4: Windows Forensic Artifacts 10

Registry Hive Analysis: SAM, SOFTWARE, SYSTEM, and NTUSER.DAT 10

Prefetch, ShimCache, Amcache, and ShellBags 10

Event Log Forensics: EVTX Parsing and Key Event IDs 10

LNK Files, Jump Lists, and Recent File Artifacts 10

Windows Memory Artifacts and Dump Analysis Preparation 10

Summary 10

Chapter 5: Linux and macOS Forensic Artifacts 12

Shell History, Bash RC Files, and Cron Artifacts 12

Package Manager Logs: APT, YUM, DNF, and Homebrew 12

System Logs: syslog, journalctl, and auth.log Analysis 12

macOS-Specific Artifacts: LaunchDaemons, Spotlight, and Time Machine 12

Container and VM Forensics Considerations 12

Summary 12

Chapter 6: Memory Forensics 14

The Volatility Framework: Installation and Profile Management 14

Process Tree Analysis and Hollowing Detection 14

Network Connection Extraction from Memory 14

Malware Artifact Discovery: Strings, DLLs, and Code Injection 14

Rekall, MemProcFS, and Commercial Alternatives 14

Troubleshooting and Performance: Volatility 3 Common Issues 14

Summary 15

Memory Acquisition Field Checklist 15

Chapter 7: Mobile Device Forensics 16

Acquisition Methods: Physical, Logical, File System, and Cloud 16

Open-Source iOS Extraction: libimobiledevice Sequential Workflow 16

iOS Forensics: SQLite Databases, Keychain, and Backup Parsing 16

CONTENTS

Android Forensics: ADB, DDMS, and App Data Extraction	16
Cellebrite UFED and Commercial Tool Ecosystems	16
WhatsApp, Signal, and Encrypted Messaging Analysis	17
Mobile Forensics Field Checklist	17
Summary	17
Chapter 8: Network Forensics	18
Packet Capture Fundamentals: tcpdump, Wireshark, and tshark	18
Zeek (Bro) for Network Forensic Analysis	18
Reconstructing Sessions: HTTP, DNS, SMTP, and TLS	18
Network Timeline Reconstruction	18
KAPE and Velociraptor for Remote Collection	18
Summary	18
Chapter 9: Cloud and Email Forensics	20
Cloud Forensics Challenges: Ephemeral Infrastructure and Shared Responsibility	20
AWS, Azure, and GCP Artifact Collection	20
Automated Cloud Log Ingestion and Analysis	20
Email Header Analysis and Message Reconstruction	20
Exchange, Gmail, and IMAP/POP3 Forensic Techniques	20
Cloud Logging and SIEM Integration	20
Summary	21
Chapter 10: Browser Artifacts and Application Forensics	22
Chrome, Firefox, and Edge Artifact Analysis	22
Browser History, Cookies, Cache, and IndexedDB	22
Flash, Java, and Plugin Artifacts	22
Office Document Metadata and Hidden Content	22
Application-Specific Forensics: Discord, Slack, Teams	22
Summary	22
Chapter 11: Malware Investigation and Incident Response	24
Incident Response Frameworks: NIST, SANS, and ISO 27035	24
Static Analysis: YARA Rules, Strings, and PE Header Examination . . .	24
Dynamic Analysis: Sandboxing and Network Monitoring	24
Memory-Based Malware Detection Techniques	24
Threat Hunting with Sigma Rules and Velociraptor	24
Summary	25
Incident Response Triage Checklist	25

Chapter 12: Timeline Reconstruction and Log Analysis 26
 Plaso (log2timeline) and SuperTimeline Construction 26
 MACB Times and File System Timestamps 26
 Multi-Source Correlation Techniques 26
 Bulk Extractor for Keyword and Pattern Extraction 26
 Automated Timeline Generation and Visualization 26
 Troubleshooting and Performance: Plaso at Scale 26
 Summary 27

Chapter 13: Anti-Forensics and Countermeasures 28
 Data Hiding Techniques: Steganography, Hidden Partitions, and
 Timestamping 28
 Wiping and Destruction Tools: DBAN, shred, and sdelete 28
 Anti-Forensics Detection Strategies 28
 Rootkits, Bootkits, and Firmware-Level Attacks 28
 Living-off-the-Land Binary (LOTL) Investigations 28
 Summary 28

Chapter 14: Forensic Reporting, Legal Issues, and Emerging Trends . . 30
 Writing Defensible Forensic Reports 30
 Annotated Sample Forensic Report 30
 Expert Testimony and Cross-Examination Preparation 38
 Privacy Laws, GDPR, and International Jurisdiction 38
 AI-Assisted Investigations: Machine Learning in Forensics 38
 AI Admissibility: Current Legal Standards and Validation Requirements 38
 The Future: Quantum Computing, IoT, and Next-Generation Challenges 38
 Summary 38

Conclusion: The Investigator’s Path Forward 39

References 40

From Evidence Acquisition to Advanced Analysis

About this book: This is a comprehensive, hands-on guide to digital forensics that takes you from the foundational principles of evidence handling through advanced investigative methodologies used by professional investigators. Every chapter provides actionable techniques, real-world case studies, step-by-step walkthroughs, and command-line examples using industry-standard tools. Whether you are a student entering the field, a security professional expanding your skill set, or an experienced investigator looking for current best practices, this book delivers practical knowledge you can apply immediately in the lab, in incident response, and in court.

Introduction: The Digital Crime Scene

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Why This Book Exists

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

How to Use This Book

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

What You Will Need

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Tool Version Matrix

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Managing Tool Version Drift

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

A Note on Ethics and Legality

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

The Road Ahead

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Running Case Studies

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Chapter 1: Foundations of Digital Forensics

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

What Is Digital Forensics (and What It Is Not)

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

The Four Pillars: Identification, Preservation, Analysis, Presentation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

A Brief History: From Enron to Modern Cybercrime

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

The Investigator's Mindset: Scientific Method Meets Detective Work

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Legal Foundations and Admissibility Standards

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Chapter 2: Evidence Handling and Chain of Custody

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Identifying Digital Evidence: Sources, Types, and Prioritization

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

The Chain of Custody Framework

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

The Evidence Acquisition Workflow

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Write Blockers: Hardware and Software Solutions

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Forensic Imaging: Bit-by-Bit Copies and Image Formats

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Hashing and Integrity Verification (MD5, SHA-1, SHA-256, BKA)

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Troubleshooting and Performance: Imaging Challenges

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Chain of Custody Field Checklist

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Chapter 3: File Systems and Operating System Artifacts

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

NTFS Internals: MFT, USN Journal, \$LogFile, and Alternate Data Streams

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

ext4 Forensics: Inodes, Journals, and Extents

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

APFS and HFS+: macOS File System Artifacts

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Deleted Files, Slack Space, and Unallocated Space Recovery

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Sleuth Kit and Autopsy: Command-Line File System Analysis

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Cross-Platform Artifact Comparison Matrix

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Chapter 4: Windows Forensic Artifacts

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Registry Hive Analysis: SAM, SOFTWARE, SYSTEM, and NTUSER.DAT

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Prefetch, ShimCache, Amcache, and ShellBags

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Event Log Forensics: EVTX Parsing and Key Event IDs

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

LNK Files, Jump Lists, and Recent File Artifacts

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Windows Memory Artifacts and Dump Analysis Preparation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Chapter 5: Linux and macOS Forensic Artifacts

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Shell History, Bash RC Files, and Cron Artifacts

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Package Manager Logs: APT, YUM, DNF, and Homebrew

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

System Logs: syslog, journalctl, and auth.log Analysis

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

macOS-Specific Artifacts: LaunchDaemons, Spotlight, and Time Machine

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Container and VM Forensics Considerations

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Chapter 6: Memory Forensics

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

The Volatility Framework: Installation and Profile Management

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Process Tree Analysis and Hollowing Detection

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Network Connection Extraction from Memory

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Malware Artifact Discovery: Strings, DLLs, and Code Injection

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Rekall, MemProcFS, and Commercial Alternatives

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Troubleshooting and Performance: Volatility 3 Common Issues

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Memory Acquisition Field Checklist

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Chapter 7: Mobile Device Forensics

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Acquisition Methods: Physical, Logical, File System, and Cloud

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Open-Source iOS Extraction: libimobiledevice Sequential Workflow

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

iOS Forensics: SQLite Databases, Keychain, and Backup Parsing

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Android Forensics: ADB, DDMS, and App Data Extraction

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Cellebrite UFED and Commercial Tool Ecosystems

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

WhatsApp, Signal, and Encrypted Messaging Analysis

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Mobile Forensics Field Checklist

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Chapter 8: Network Forensics

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Packet Capture Fundamentals: tcpdump, Wireshark, and tshark

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Zeek (Bro) for Network Forensic Analysis

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Reconstructing Sessions: HTTP, DNS, SMTP, and TLS

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Network Timeline Reconstruction

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

KAPE and Velociraptor for Remote Collection

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Chapter 9: Cloud and Email Forensics

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Cloud Forensics Challenges: Ephemeral Infrastructure and Shared Responsibility

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

AWS, Azure, and GCP Artifact Collection

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Automated Cloud Log Ingestion and Analysis

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Email Header Analysis and Message Reconstruction

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Exchange, Gmail, and IMAP/POP3 Forensic Techniques

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Cloud Logging and SIEM Integration

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Chapter 10: Browser Artifacts and Application Forensics

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Chrome, Firefox, and Edge Artifact Analysis

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Browser History, Cookies, Cache, and IndexedDB

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Flash, Java, and Plugin Artifacts

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Office Document Metadata and Hidden Content

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Application-Specific Forensics: Discord, Slack, Teams

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Chapter 11: Malware Investigation and Incident Response

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Incident Response Frameworks: NIST, SANS, and ISO 27035

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Static Analysis: YARA Rules, Strings, and PE Header Examination

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Dynamic Analysis: Sandboxing and Network Monitoring

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Memory-Based Malware Detection Techniques

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Threat Hunting with Sigma Rules and Velociraptor

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Incident Response Triage Checklist

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Chapter 12: Timeline Reconstruction and Log Analysis

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Plaso (log2timeline) and SuperTimeline Construction

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

MACB Times and File System Timestamps

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Multi-Source Correlation Techniques

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Bulk Extractor for Keyword and Pattern Extraction

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Automated Timeline Generation and Visualization

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Troubleshooting and Performance: Plaso at Scale

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Chapter 13: Anti-Forensics and Countermeasures

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Data Hiding Techniques: Steganography, Hidden Partitions, and Timestomping

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Wiping and Destruction Tools: DBAN, shred, and sdelete

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Anti-Forensics Detection Strategies

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Rootkits, Bootkits, and Firmware-Level Attacks

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Living-off-the-Land Binary (LOTL) Investigations

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Chapter 14: Forensic Reporting, Legal Issues, and Emerging Trends

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Writing Defensible Forensic Reports

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Annotated Sample Forensic Report

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

1. EXECUTIVE SUMMARY [Written last; summarizes findings for non-technical readers without revealing methodology details that could be challenged]

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

2. CASE INFORMATION [Provides context for the reader and establishes the scope of authority]

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

3. EXAMINATION ITEMS [Documents every piece of evidence with hash values for admissibility]

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

4. METHODOLOGY [Documents tools, versions, and procedures for Daubert compliance]

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

5. FINDINGS [Organized by category; each finding states what was found, where it was found, and how it was determined]

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

5.1 Execution Artifacts

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

5.2 File System Artifacts

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

5.3 Removable Device Evidence

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

5.4 Browser Activity

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

5.5 Event Log Corroboration

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

5.6 Limitations and Caveats [Required for credibility; shows intellectual honesty]

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

6. CONCLUSIONS [States what the evidence shows without speculation about intent or legal conclusions]

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

7. APPENDICES

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Expert Testimony and Cross-Examination Preparation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Privacy Laws, GDPR, and International Jurisdiction

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

AI-Assisted Investigations: Machine Learning in Forensics

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

AI Admissibility: Current Legal Standards and Validation Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

The Future: Quantum Computing, IoT, and Next-Generation Challenges

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

Conclusion: The Investigator's Path Forward

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.

References

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/digitalforensicsapracticalguidetomoderninvestigations>.