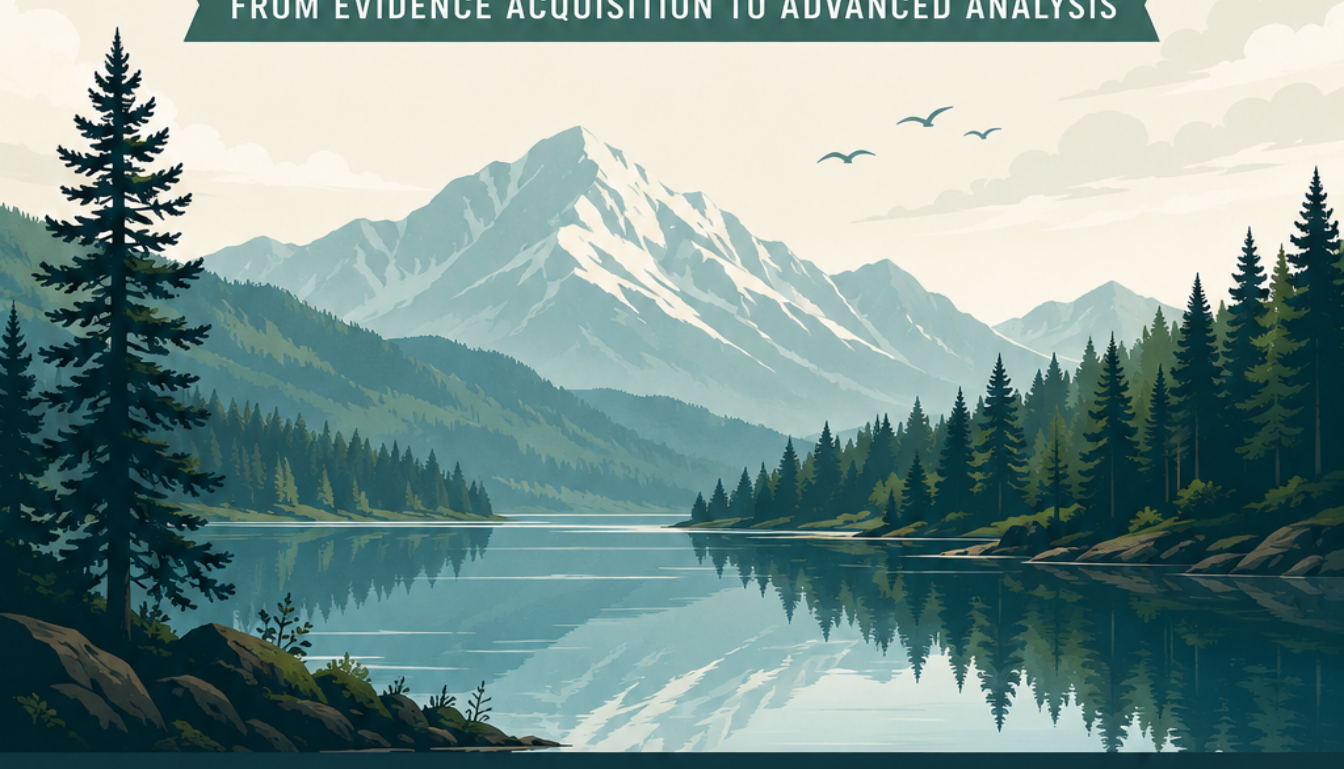
DIGITAL FORENSICS

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/digitalforensicsapracticalguidetomoderninvestigations

This version was published on 2026-07-12

Contents

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

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]

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

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

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

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

5.1 Execution Artifacts

5.2 File System Artifacts

5.3 Removable Device Evidence

5.4 Browser Activity

5.5 Event Log Corroboration

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

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

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

Privacy Laws, GDPR, and International Jurisdiction

AI-Assisted Investigations: Machine Learning in Forensics

AI Admissibility: Current Legal Standards and Validation Requirements

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

Summary

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.