Forensic Imaging and Data Carving Techniques Training Course

Professional Development Training Course Outline

Category	Criminology	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In the intricate world of digital forensics and incident response, the ability to accurately and forensically acquire data is the cornerstone of any successful investigation. Training course on Forensic Imaging & Data Carving Techniques is designed to equip participants with the essential skills to create bit-for-bit copies of digital media, ensuring the integrity and admissibility of evidence. From compromised hard drives to volatile memory, mastering these techniques is crucial for preserving the digital crime scene and preventing inadvertent data alteration, which can render evidence inadmissible in legal proceedings.

Beyond merely capturing data, this course delves into the art of data carving, a powerful technique for recovering deleted, fragmented, or hidden files from raw disk images, even when file system metadata is corrupted or missing. Through extensive hands-on labs and practical scenarios, attendees will learn to utilize cutting-edge forensic software and methodologies to extract critical artifacts that traditional file recovery methods might miss. By mastering both forensic imaging and data carving, professionals will significantly enhance their capacity to uncover crucial evidence in complex cybercrime investigations, data breach analyses, and insider threat cases, contributing directly to organizational cyber resilience and threat intelligence.

Programme Curriculum

Forensic Imaging and Data Carving Techniques Training Course

Introduction

In the intricate world of digital forensics and incident response, the ability to accurately and forensically acquire data is the cornerstone of any successful investigation. Forensic Imaging and Data Carving Techniques Training Course is designed to equip participants with the essential skills to create bit-for-bit copies of digital media, ensuring the integrity and admissibility of evidence.

From compromised hard drives to volatile memory, mastering these techniques is crucial for preserving the digital crime scene and preventing inadvertent data alteration, which can render evidence inadmissible in legal proceedings.

Beyond merely capturing data, this course delves into the art of data carving, a powerful technique for recovering deleted, fragmented, or hidden files from raw disk images, even when file system metadata is corrupted or missing. Through extensive hands-on labs and practical scenarios, attendees will learn to utilize cutting-edge forensic software and methodologies to extract critical artifacts that traditional file recovery methods might miss. By mastering both forensic imaging and data carving, professionals will significantly enhance their capacity to uncover crucial evidence in complex cybercrime investigations, data breach analyses, and insider threat cases, contributing directly to organizational cyber resilience and threat intelligence.

Course Duration

5days

Course Objectives

1. Master forensically sound imaging techniques for diverse storage media (HDDs, SSDs, USBs).
2. Utilize write-blockers effectively to ensure evidence integrity during acquisition.
3. Perform live forensic imaging to capture volatile data from running systems.
4. Understand and apply cryptographic hashing algorithms (MD5, SHA-1, SHA-256) for image verification.
5. Differentiate between physical, logical, and targeted imaging and their appropriate use cases.
6. Execute advanced data carving techniques to recover deleted and fragmented files.Identify and interpret file signatures and headers/footers for effective data carving.
7. Employ specialized data carving tools (e.g., Foremost, Scalpel, PhotoRec) for various file types.
8. Recover data from unallocated space and slack space on digital media
9. Reconstruct fragmented files from raw data streams.
10. Document all imaging and carving procedures to maintain a robust chain of custody.
11. Address challenges related to damaged or corrupted media during acquisition and carving.
12. Integrate imaging and carving results into comprehensive digital forensic reports.

Organizational Benefits

- Enhanced Evidence Admissibility: Ensuring collected evidence meets legal standards for court.
- Improved Data Recovery Capabilities: Retrieving crucial information even from damaged or intentionally deleted sources.
- Faster Incident Response: Efficient and accurate data acquisition speeds up investigations.

- Strengthened Cyber Investigations: Deeper insights into malicious activities and user behavior.
- Reduced Litigation Risk: Avoiding challenges to evidence integrity in legal proceedings.
- Protection of Intellectual Property: Recovering proprietary data in theft or espionage cases.
- Proactive Threat Hunting: Uncovering hidden artifacts that indicate ongoing threats.
- Cost-Effective Solutions: Empowering internal teams to perform sophisticated forensic tasks.
- Enhanced Organizational Resilience: Building capability to thoroughly investigate and recover from cyber incidents.
- Valuable Skillset Development: Cultivating highly specialized forensic expertise within the workforce. Enhanced Employee Competence: Building a highly skilled workforce proficient in evidence integrity.

Target Participants

1. Digital Forensics Investigators
2. Incident Response Team Members
3. Cybersecurity Analysts
4. Law Enforcement Digital Evidence Units
5. e-Discovery Professionals
6. IT Security Managers
7. Auditors and Compliance Officers
8. Malware Analysts
9. System Administrators with Forensic Responsibilities
10. Individuals aspiring to a career in Digital Forensics

Course Outline

Module 1: Fundamentals of Forensic Imaging

- **Introduction to Digital Evidence & Imaging:** Why bit-for-bit copies are crucial.
- **Forensic Soundness & Write-Blocking:** Principles and practical application of hardware/software write-blockers.
- **Types of Forensic Images:** Physical, logical, and targeted imaging strategies.
- **Hashing for Integrity:** MD5, SHA-1, SHA-256 for verification and authentication.
- **Case Study:** Simulating the initial acquisition of a compromised desktop hard drive with proper write-blocking.

Module 2: Disk Imaging Techniques & Tools

- **Acquisition from HDDs & SSDs:** Best practices for modern storage technologies.
- **Imaging Removable Media:** USB drives, SD cards, and external hard drives.
- **Common Imaging Tools (Open Source & Commercial):** FTK Imager, EnCase, dd, Guymager.
- **Image File Formats:** Raw (dd), E01 (EnCase), AFF, and their characteristics.

- **Case Study:** Creating a forensically sound image of a suspect's laptop.

Module 3: Live System Imaging & Volatile Data

- **Challenges of Live Acquisition:** Volatility, system state changes, anti-forensics.
- **Memory Acquisition Tools:** Volatility Framework, Winpmem, DumpIt.
- **Network Activity Capture:** NetFlow, packet capture (Wireshark) for volatile network data.
- **Process & Registry Acquisition:** Capturing live system state information.
- **Case Study:** Performing a live acquisition of a web server actively under attack.

Module 4: Introduction to Data Carving

- **Concept of Data Carving:** Recovering data without file system metadata.
- **Unallocated Space & Slack Space:** Where "deleted" data resides.
- **File Signatures & Headers/Footers:** How carving tools identify file types.
- **Challenges of Data Carving:** Fragmentation, partial overwrites, unknown file types.
- **Case Study:** Identifying and attempting to recover a "deleted" document from a raw disk image.

Module 5: Data Carving Tools & Techniques

- **Foremost & Scalpel:** Command-line tools for carving specific file types.
- **PhotoRec & TestDisk:** Recovery of images, videos, and other media.
- **Bulk Extractor:** Extracting specific patterns like email addresses, URLs, credit card numbers.
- **Advanced Carving Concepts:** Custom signatures and reassembly strategies.
- **Case Study:** Using multiple carving tools to maximize recovery from a severely damaged drive.

Module 6: Fragmented File Reconstruction

- **Understanding File Fragmentation:** How files are scattered across disk.
- **Techniques for Reassembly:** Heuristic carving, sequential carving, gap carving.
- **Tools for Fragmented File Recovery:** Commercial and advanced open-source solutions.
- **Challenges of Large Fragmented Files:** Video, database, and encrypted files.

- **Case Study:** Reconstructing a fragmented video file from an unallocated cluster.

Module 7: Analysis & Verification of Carved Data

- **Validation of Recovered Files:** Ensuring integrity and usability of carved data.
- **File Type Identification (Trid, ExifTool):** Verifying carved file types.
- **Content Analysis of Carved Data:** Reviewing retrieved information for investigative leads.
- **Correlation with Other Artifacts:** Integrating carving results into the larger investigation.
- **Case Study:** Analyzing carved image files for metadata and potential evidence.

Module 8: Reporting & Best Practices

- **Documenting Imaging Procedures:** Comprehensive logs and hash verifications.
- **Reporting Carving Results:** Clearly presenting recovered data and methodologies.
- **Legal Considerations for Carved Data:** Admissibility and potential challenges.
- **Continuous Learning & Tool Updates:** Staying current with evolving techniques and software.
- **Case Study:** Preparing a forensic report detailing imaging and carving findings for a legal team.

Training Methodology

This training course will employ a blended learning approach incorporating:

- Interactive lectures and presentations
- Hands-on exercises and case studies
- Individual and group simulation projects
- Discussions and knowledge sharing
- Practical application of simulation software
- Real-world examples and industry best practices

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org **or call** *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com