Training Course on Email Forensics: Header Analysis and Phishing Investigations

Professional Development Training Course Outline

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

Course Introduction

Introduction

Email remains the primary vector for cyberattacks, making email forensics a critical skill for any organization facing sophisticated threats. Beyond simply reading messages, the true intelligence lies within the hidden metadata, complex routing paths, and the subtle clues that expose malicious intent. Training Course on Email Forensics: Header Analysis and Phishing Investigations provides a deep dive into the art and science of email header analysis and phishing investigations, equipping digital forensic professionals, incident responders, and cybersecurity analysts with the advanced techniques needed to unravel complex email-borne attacks. Participants will master the interpretation of intricate email headers, trace message origins, identify spoofing and impersonation attempts, and reconstruct the full lifecycle of a phishing campaign, transforming obscure data into undeniable digital evidence.

This comprehensive program moves beyond theoretical concepts, offering hands-on labs with real-world phishing samples and spam attacks. Attendees will gain proficiency in utilizing specialized email forensic tools, dissecting various email protocols (SMTP, POP3, IMAP), and understanding how email authentication mechanisms like SPF, DKIM, and DMARC impact an investigation. By the end of this course, you will be capable of swiftly and accurately dissecting suspicious emails, attributing attacks, and building robust cases for cybercrime prosecution or internal disciplinary actions. Elevate your defensive capabilities by becoming an expert in dismantling email-borne threats and fortifying your organization's digital perimeter.

Programme Curriculum

Training Course on Email Forensics: Header Analysis and Phishing Investigations

Introduction

Email remains the primary vector for cyberattacks, making email forensics a critical skill for any organization facing sophisticated threats. Beyond simply reading messages, the true intelligence lies within the hidden metadata, complex routing paths, and the subtle clues that expose malicious intent. Training Course on Email Forensics: Header Analysis and Phishing Investigations provides a deep dive into the art and science of email header analysis and phishing investigations, equipping digital forensic professionals, incident responders, and cybersecurity analysts with the advanced techniques needed to unravel complex email-borne attacks. Participants will master the interpretation of intricate email headers, trace message origins, identify spoofing and impersonation attempts, and reconstruct the full lifecycle of a phishing campaign, transforming obscure data into undeniable digital evidence.

This comprehensive program moves beyond theoretical concepts, offering hands-on labs with real-world phishing samples and spam attacks. Attendees will gain proficiency in utilizing specialized email forensic tools, dissecting various email protocols (SMTP, POP3, IMAP), and understanding how email authentication mechanisms like SPF, DKIM, and DMARC impact an investigation. By the end of this course, you will be capable of swiftly and accurately dissecting suspicious emails, attributing attacks, and building robust cases for cybercrime prosecution or internal disciplinary actions. Elevate your defensive capabilities by becoming an expert in dismantling email-borne threats and fortifying your organization's digital perimeter.

Course Duration

5 Days

Course Objectives

1. Understand Email Ecosystems: Comprehend the architecture and protocols (SMTP, POP3, IMAP) governing email transmission and storage.
2. Master Email Header Analysis: Deconstruct and interpret all critical email header fields (e.g., Received, From, To, Subject, Message-ID, X-Mailer, Authentication-Results).
3. Trace Email Origins: Accurately determine the true sender, sending server, and geographical location of an email based on header information.
4. Identify Email Spoofing & Impersonation: Recognize techniques used to falsify sender identities and conduct impersonation attacks.
5. Analyze Email Authentication Results: Interpret SPF, DKIM, and DMARC records and their role in verifying email legitimacy and detecting fraud.
6. Conduct Phishing Investigations: Systematically analyze phishing emails, identify malicious links, attachments, and social engineering tactics.

7. Extract & Analyze Email Attachments: Safely handle and forensically examine suspicious email attachments for malware or hidden data.
8. Reconstruct Email Timelines: Correlate timestamps from various header fields to build a precise chronological sequence of email events.
9. Investigate Email Client & Server Artifacts: Acquire and analyze email data from local clients (Outlook PST/OST, Thunderbird MBOX) and server logs.
10. Uncover Business Email Compromise (BEC) Indicators: Identify the subtle clues and patterns indicative of BEC and email account compromise.
11. Leverage Email Forensic Tools: Proficiency in using commercial and open-source tools for automated email parsing and analysis.
12. Address Legal & Ethical Considerations: Understand data privacy, chain of custody, and legal admissibility of email evidence.
13. Produce Comprehensive Forensic Reports: Generate clear, concise, and legally defensible reports on email investigations.

Organizational Benefits

1. Reduced Phishing Success Rates: Employees better equipped to identify and report phishing attempts.
2. Faster Incident Response: Rapid analysis of suspicious emails expedites threat containment and remediation.
3. Minimized Financial Loss: Quicker detection of BEC and other email fraud prevents financial damage.
4. Enhanced Cybersecurity Posture: Strengthened defenses against the most common attack vector.
5. Improved Compliance & Audit Trails: Better documentation and understanding of email-borne threats for regulatory adherence.
6. Stronger Insider Threat Detection: Ability to investigate data exfiltration or malicious communication via email.
7. Protection of Sensitive Data: Safeguard intellectual property and confidential information transmitted via email.
8. Reduced Litigation Risk: Provide robust, admissible digital evidence in legal cases stemming from email incidents.
9. Upskilled Security Team: Develop in-house expertise in a critical and highly demanded forensic area.
10. Proactive Threat Intelligence: Insights from investigations can inform and refine security awareness training and technical controls.

Target Participants

- Digital Forensic Investigators

- Incident Responders
- Cybersecurity Analysts (SOC Tier 2/3)
- Security Administrators
- Threat Intelligence Analysts
- Fraud Investigators
- IT Auditors
- Law Enforcement Officers
- eDiscovery Specialists
- Compliance Officers

Course Outline

Module 1: Fundamentals of Email Systems & Protocols

- **Email Architecture:** Mail User Agents (MUA), Mail Transfer Agents (MTA), Mail Delivery Agents (MDA).
- **Core Email Protocols:** SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol 3), IMAP (Internet Message Access Protocol).
- **Email Message Structure:** Envelope vs. Header vs. Body.
- **Introduction to Email Headers:** Basic fields and their initial interpretation.
- **Case Study: Tracing a Simple Email's Journey through Multiple Servers**

Module 2: Deep Dive into Email Header Analysis

- **Received: Header Analysis**: Understanding the crucial "travel log" of an email, reading from bottom-up.
- **From:, To:, Subject: Fields:** Identifying display vs. actual addresses, and common manipulation techniques.
- **Message-ID: & Date: Fields:** Unique identifiers and timestamp discrepancies.
- **Extended Headers (X-Mailer, X-Originating-IP, X-MS-TNEF):** Extracting client/server software and other forensic clues.
- **Case Study: Pinpointing the True Origin of a Malicious Email**

Module 3: Email Authentication & Anti-Spoofing Mechanisms

- **Sender Policy Framework (SPF):** Understanding SPF records, 'hardfail' vs. 'softfail', and their implications.
- **DomainKeys Identified Mail (DKIM):** Analyzing DKIM signatures, public keys, and cryptographic verification.
- **Domain-based Message Authentication, Reporting, and Conformance (DMARC):** Policy enforcement and reporting for email authentication.
- **Authenticated Received Chain (ARC):** Tracing the chain of custody through intermediate servers.
- **Case Study: Detecting an Email Spoofing Attack Using SPF/DKIM/DMARC Failures**

Module 4: Phishing Investigations: Identification & Analysis

- **Types of Phishing Attacks:** Spear phishing, whaling, smishing, vishing, business email compromise (BEC).

- **Identifying Malicious URLs & Link Analysis:** Decoding obfuscated links, identifying redirects, and sandbox techniques.
- **Analyzing Malicious Attachments:** Safe handling, static and dynamic analysis, file type identification.
- **Social Engineering Tactics:** Recognizing psychological manipulation in phishing emails.
- **Case Study: Dissecting a Sophisticated Phishing Email and its Payload**

Module 5: Email Content & Body Analysis

- **HTML vs. Plain Text Email Bodies:** Forensic implications of different formats.
- **Embedded Objects & Web Bugs:** Detecting tracking pixels and external content.
- **Keywords & Pattern Analysis:** Searching for indicators of compromise (IOCs) and specific phrases.
- **Language & Tone Analysis:** Identifying characteristics of BEC or impersonation attempts.
- **Case Study: Extracting Hidden Data and Malicious Scripts from an Email Body**

Module 6: Email Client & Server-Side Forensics

- **Local Email Client Forensics:** Acquiring and analyzing PST, OST (Outlook), MBOX (Thunderbird), EML, MSG files.
- **Server-Side Email Forensics:** Accessing email server logs (Exchange, Postfix, Gmail Logs) for routing and activity.
- **Cloud-Based Email Forensics:** Investigating O365 Unified Audit Logs, Google Workspace Vault, and other cloud email artifacts.
- **Recovering Deleted Emails:** Techniques for recovering deleted messages from client files or server backups.
- **Case Study: Investigating a User's Compromised Email Account on a Corporate Exchange Server**

Module 7: Advanced Email Forensic Tools & Techniques

- **Commercial Email Forensic Software:** Overview and hands-on with leading tools (e.g., Magnet AXIOM, FTK, EnCase email parsers).
- **Open-Source Tools & Scripting:** Utilizing Python scripts, PowerShell, and online header analyzers for rapid analysis.
- **Timeline Reconstruction:** Correlating email events with other system and network artifacts for comprehensive timelines.
- **Volatile Memory Analysis:** Extracting email-related artifacts from RAM.
- **Case Study: Automating the Analysis of Multiple Suspicious Emails in an Incident**

Module 8: Reporting, Legal & Remediation

- **Crafting a Defensible Email Forensic Report:** Structure, content, and language for legal proceedings.
- **Presenting Findings:** Communicating complex technical details to non-technical audiences (e.g., management, legal).
- **Legal & Ethical Considerations:** Data privacy, chain of custody, consent, and jurisdictional issues in email forensics.
- **Remediation & Prevention Strategies:** Implementing lessons learned from investigations to enhance email security.
- **Case Study: Preparing Expert Testimony for a BEC Fraud Case**

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

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