Training Course on Digital Forensics for Remote Work Environments

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,100 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Introduction

The rapid shift to remote and hybrid work models has dramatically expanded an organization's attack surface, presenting unprecedented challenges for digital forensic investigations and incident response. Endpoints are dispersed, network visibility is fragmented, and critical data increasingly resides in cloud services outside the traditional perimeter. Training Course on Digital Forensics for Remote Work Environments provides an essential deep dive into digital forensics for remote work environments, equipping digital forensic investigators, incident responders, and cybersecurity professionals with the unique methodologies and practical skills needed to effectively collect, preserve, analyze, and report on digital evidence from geographically distributed systems. Participants will learn to navigate the complexities of remote data acquisition, leverage cloud-native forensic capabilities, and interpret artifacts from virtualized environments, transforming distributed data into cohesive actionable intelligence.

This intensive program moves beyond conventional on-premises forensics, focusing on the nuances of remote live acquisitions, the forensic analysis of VPN and remote access logs, investigating data exfiltration across cloud collaboration platforms, and the challenges of maintaining chain of custody in a decentralized landscape. Through extensive hands-on labs, real-world remote incident scenarios, and the application of cutting-edge remote forensic tooling and EDR solutions, attendees will gain proficiency in examining laptops, virtual desktops, cloud accounts, and home networks for signs of compromise, insider threats, and data breaches. By the end of this course, you will be capable of leading complex investigations in the remote era, building robust, legally defensible cases and fortifying your organization's security posture in the distributed workspace.

Programme Curriculum

Training Course on Digital Forensics for Remote Work Environments

Introduction

The rapid shift to remote and hybrid work models has dramatically expanded an organization's attack surface, presenting unprecedented challenges for digital forensic investigations and incident response. Endpoints are dispersed, network visibility is fragmented, and critical data increasingly resides in cloud services outside the traditional perimeter. Training Course on Digital Forensics for Remote Work Environments provides an essential deep dive into digital forensics for remote work environments, equipping digital forensic investigators, incident responders, and cybersecurity professionals with the unique methodologies and practical skills needed to effectively collect, preserve, analyze, and report on digital evidence from geographically distributed systems. Participants will learn to navigate the complexities of remote data acquisition, leverage cloud-native forensic capabilities, and interpret artifacts from virtualized environments, transforming distributed data into cohesive actionable intelligence.

This intensive program moves beyond conventional on-premises forensics, focusing on the nuances of remote live acquisitions, the forensic analysis of VPN and remote access logs, investigating data exfiltration across cloud collaboration platforms, and the challenges of maintaining chain of custody in a decentralized landscape. Through extensive hands-on labs, real-world remote incident scenarios, and the application of cutting-edge remote forensic tooling and EDR solutions, attendees will gain proficiency in examining laptops, virtual desktops, cloud accounts, and home networks for signs of compromise, insider threats, and data breaches. By the end of this course, you will be capable of leading complex investigations in the remote era, building robust, legally defensible cases and fortifying your organization's security posture in the distributed workspace.

Course Duration

5 Days

Course Objectives

1. Understand Remote Work Attack Vectors: Identify common vulnerabilities and attack paths specific to remote and hybrid work environments.
2. Master Remote Data Acquisition: Safely and forensically acquire data from geographically dispersed endpoints (laptops, desktops, virtual machines) with integrity.
3. Perform Cloud-Native Forensics: Leverage APIs and native logging capabilities of cloud platforms (SaaS, IaaS) for evidence collection and analysis.

4. Analyze VPN & Remote Access Logs: Interpret VPN connection logs, RDP session data, and other remote access artifacts for suspicious activity and unauthorized access.
5. Investigate Cloud Collaboration Platforms: Extract and analyze forensic artifacts from platforms like Microsoft 365, Google Workspace, Slack, and Zoom.
6. Detect Data Exfiltration in Remote Environments: Identify methods and evidence of data theft across diverse remote channels (e.g., personal cloud storage, unsanctioned file transfers).
7. Utilize Endpoint Detection & Response (EDR) for Forensics: Integrate EDR telemetry, remote response capabilities, and historical data into investigations.
8. Address Virtual Desktop Infrastructure (VDI) Forensics: Acquire and analyze evidence from persistent and non-persistent VDI environments.
9. Maintain Chain of Custody Remotely: Implement best practices for preserving evidence integrity and documenting the chain of custody in remote scenarios.
10. Assess BYOD (Bring Your Own Device) Challenges: Understand the complexities of investigating personal devices used for work purposes.
11. Correlate Disparate Cloud & Endpoint Data: Integrate findings from various remote and cloud sources to build a comprehensive timeline of events.
12. Develop Remote Incident Response Playbooks: Formulate strategic approaches and procedures for responding to incidents in distributed workforces.
13. Generate Legally Admissible Remote Forensic Reports: Produce clear, detailed, and defensible reports suitable for legal or HR actions.

Organizational Benefits

1. Rapid Remote Incident Response: Swiftly detect, contain, and remediate security incidents involving remote employees.
2. Minimized Data Breach Impact: Reduce potential financial and reputational damage from data loss in distributed environments.
3. Enhanced Forensic Capability: Develop in-house expertise to conduct investigations regardless of employee location.
4. Improved Security Posture: Insights from investigations inform better security controls for remote work.
5. Stronger Compliance & Audit Readiness: Demonstrate robust incident handling for regulatory requirements.
6. Protection of Intellectual Property: Safeguard sensitive data accessed or stored by remote employees.
7. Better Insider Threat Detection: Uncover malicious or negligent activity by remote insiders.
8. Optimized Tooling & Processes: Leverage remote forensics tools and methodologies effectively.
9. Reduced Travel & Logistical Costs: Efficiently conduct investigations without requiring physical presence.

10. Increased Business Resilience: Maintain investigative capabilities even in a fully remote or hybrid operational model.

Target Participants

- Digital Forensic Investigators
- Incident Response Team Members
- Cybersecurity Analysts (SOC Tier 2/3)
- IT Security Managers
- Cloud Security Engineers
- Compliance Officers
- Legal Counsel (involved in digital investigations)
- eDiscovery Specialists
- Threat Hunters
- Network Security Engineers

Course Outline

Module 1: The Remote Work Landscape & Forensic Challenges

- **Evolution of Remote Work:** Understanding its impact on cybersecurity and forensics.
- **Expanded Attack Surface:** Dispersed endpoints, fragmented networks, cloud services.
- **Unique Challenges in Remote Forensics:** Data acquisition, chain of custody, legal jurisdiction.
- **Forensic Readiness for Remote Environments:** Planning and preparation.
- **Case Study:** Analyzing a ransomware attack originating from a remote employee's compromised home network.

Module 2: Remote Endpoint Data Acquisition

- **Live Acquisition Techniques:** Capturing volatile data from online remote endpoints.
- **Remote Imaging Tools:** Using enterprise-level tools for full disk images over network (e.g., Magnet AXIOM Cyber, F-Response, FTK Enterprise).
- **Targeted Remote Collection:** Acquiring specific files, logs, or memory.
- **Challenges of Network Latency & Bandwidth:** Optimizing remote acquisition strategies.
- **Case Study:** Performing a live acquisition of a remote employee's laptop suspected of insider threat activity.

Module 3: Cloud-Native Forensics & SaaS Investigations

- **Cloud Service Models (SaaS, PaaS, IaaS):** Forensic considerations for each.
- **Cloud Provider Logs & APIs:** Leveraging AWS CloudTrail, Azure Activity Logs, Google Cloud Audit Logs.
- **Forensics in Microsoft 365:** Exchange Online, SharePoint Online, OneDrive for Business audit logs.
- **Google Workspace Forensics:** Google Drive, Gmail, Google Chat audit trails.
- **Case Study:** Investigating unauthorized access and data downloads from a compromised Microsoft 365 account.

Module 4: Remote Access & VPN Log Analysis

- **VPN Connection Logs:** Analyzing timestamps, source IPs, user identities, and session duration.
- **Remote Desktop Protocol (RDP) Forensics:** RDP cache, event logs, registry artifacts.
- **Virtual Private Network (VPN) Exploits:** Forensic indicators of VPN credential theft or unauthorized access.
- **Secure Shell (SSH) & Other Remote Access Methods:** Log analysis and artifact collection.
- **Case Study:** Tracing an attacker's initial access and lateral movement through VPN and RDP logs.

Module 5: Forensics of Cloud Collaboration & Communication Platforms

- **Slack/Microsoft Teams Forensics:** Extracting chat logs, file shares, and channel activity.
- **Zoom/Webex Forensics:** Analyzing meeting logs, recordings, and participant data.
- **Cloud Storage Forensics:** Investigating file synchronization services (Dropbox, Box, etc.) for data exfiltration.
- **Metadata in Cloud Files:** Importance of cloud-generated metadata for timelines.
- **Case Study:** Uncovering evidence of data sharing with an external party via a cloud collaboration platform.

Module 6: Endpoint Detection & Response (EDR) for Remote Forensics

- **EDR as a Forensic Data Source:** Leveraging continuous recording and telemetry.
- **Remote Live Response Capabilities:** Process termination, file quarantine, host isolation.
- **Threat Hunting with EDR:** Proactively searching for anomalous behavior on remote endpoints.
- **Integrating EDR Data with Traditional Forensics:** Correlating alerts with disk artifacts.
- **Case Study:** Using EDR to identify and respond to malware infection on a remote endpoint, then collect forensic data.

Module 7: Virtual Desktop Infrastructure (VDI) Forensics

- **VDI Architectures:** Persistent vs. Non-Persistent desktops, stateless environments.
- **Forensic Challenges in VDI:** Ephemeral nature, shared infrastructure, host-level vs. guest-level forensics.
- **Acquisition from Hypervisors:** Capturing VM snapshots and disk images.
- **Analyzing VDI-Specific Artifacts:** Connection brokers, profiles, and associated logs.
- **Case Study:** Investigating a data breach within a non-persistent VDI environment.

Module 8: Legal, Reporting & Best Practices for Remote Investigations

- **Chain of Custody in Distributed Environments:** Documenting remote data handling.
- **Jurisdictional Challenges:** Data privacy laws (GDPR, CCPA) across different locations.
- **Forensic Report Writing:** Tailoring reports for remote context, clarity for stakeholders.
- **Communication & Collaboration in Remote IR Teams:** Tools and strategies.
- **Case Study:** Presenting forensic findings from a complex remote insider threat investigation to legal counsel.

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 *+254724527104*

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
03 Aug 2026	07 Aug 2026	Online	$1,100

Start Date	End Date	Location	Price
10 Aug 2026	14 Aug 2026	Online	$1,100
17 Aug 2026	21 Aug 2026	Online	$1,100
24 Aug 2026	28 Aug 2026	Online	$1,100
31 Aug 2026	04 Sep 2026	Online	$1,100
07 Sep 2026	11 Sep 2026	Online	$1,100
14 Sep 2026	18 Sep 2026	Online	$1,100
21 Sep 2026	25 Sep 2026	Online	$1,100

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

Register Online Now

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