Training Course on Investigating Mobile Device BYOD (Bring Your Own Device) Incidents

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$2,200 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Introduction

This critical training course is specifically tailored for digital forensic investigators, incident response teams, cybersecurity analysts, HR professionals, and legal counsel grappling with the unique and complex challenges of Bring Your Own Device (BYOD) incidents. The widespread adoption of BYOD policies, while offering flexibility and cost savings, introduces a minefield of security risks, data leakage concerns, privacy dilemmas, and legal complexities. When a data breach, intellectual property theft, corporate policy violation, or cybercrime occurs on an employee's personal device, traditional forensic approaches are often hampered by issues of data ownership, privacy expectations, legal consent, and technical segregation of personal and corporate data. Training Course on Investigating Mobile Device BYOD (Bring Your Own Device) Incidents provides the strategic and technical expertise to navigate these intricate landscapes, ensuring effective and legally defensible investigations.

The curriculum delves into the multifaceted aspects of BYOD environments, covering mobile device management (MDM) solutions, containerization technologies, cloud data synchronization, and the segregation of corporate and personal data. Through a blend of policy analysis, simulated incident scenarios, hands-on tool usage, and examination of real-world BYOD incidents, participants will master methodologies for forensically sound data acquisition (remote and physical), selective data extraction, and the critical interpretation of digital artifacts while respecting employee privacy. The course places significant emphasis on legal compliance, particularly with Kenya's Data Protection Act 2019, labor laws, and privacy regulations, ensuring that all investigative actions are conducted ethically, legally, and in a manner that preserves the

admissibility of evidence in any subsequent legal or disciplinary proceedings.

Programme Curriculum

Training Course on Investigating Mobile Device BYOD (Bring Your Own Device) Incidents

Introduction

This critical training course is specifically tailored for digital forensic investigators, incident response teams, cybersecurity analysts, HR professionals, and legal counsel grappling with the unique and complex challenges of Bring Your Own Device (BYOD) incidents. The widespread adoption of BYOD policies, while offering flexibility and cost savings, introduces a minefield of security risks, data leakage concerns, privacy dilemmas, and legal complexities. When a data breach, intellectual property theft, corporate policy violation, or cybercrime occurs on an employee's personal device, traditional forensic approaches are often hampered by issues of data ownership, privacy expectations, legal consent, and technical segregation of personal and corporate data. Training Course on Investigating Mobile Device BYOD (Bring Your Own Device) Incidents provides the strategic and technical expertise to navigate these intricate landscapes, ensuring effective and legally defensible investigations.

The curriculum delves into the multifaceted aspects of BYOD environments, covering mobile device management (MDM) solutions, containerization technologies, cloud data synchronization, and the segregation of corporate and personal data. Through a blend of policy analysis, simulated incident scenarios, hands-on tool usage, and examination of real-world BYOD incidents, participants will master methodologies for forensically sound data acquisition (remote and physical), selective data extraction, and the critical interpretation of digital artifacts while respecting employee privacy. The course places significant emphasis on legal compliance, particularly with Kenya's Data Protection Act 2019, labor laws, and privacy regulations, ensuring that all investigative actions are conducted ethically, legally, and in a manner that preserves the admissibility of evidence in any subsequent legal or disciplinary proceedings.

Course Duration

10 Days

Course Objectives

1. Understand the security risks, legal implications, and privacy challenges inherent in BYOD environments.
2. Develop and review BYOD policies to ensure clear expectations regarding data ownership, privacy, and forensic access.

3. Implement mobile device management (MDM) and enterprise mobility management (EMM) solutions for forensic readiness in BYOD settings.
4. Perform forensically sound data acquisition (logical and physical) from BYOD devices while respecting legal and privacy boundaries.
5. Distinguish and segregate corporate data from personal data on a BYOD device during forensic analysis.
6. Investigate data leakage and unauthorized data access incidents on BYOD devices.
7. Analyze application-specific data and cloud synchronization artifacts relevant to corporate data on personal devices.
8. Identify malicious activity, policy violations, and insider threats originating from BYOD devices.
9. Navigate the legal complexities of consent, warrants, and employee privacy rights (including Kenya's Data Protection Act 2019) in BYOD investigations.
10. Utilize specialized mobile forensic tools and techniques for targeted data extraction from BYOD devices.
11. Reconstruct incident timelines and user activity patterns on BYOD devices.
12. Prepare legally admissible forensic reports that address the unique challenges of BYOD investigations.
13. Develop an effective BYOD incident response plan incorporating forensic best practices.

Organizational Benefits

1. Mitigate Data Breach Risks: Reduce the likelihood and impact of data loss from BYOD devices.
2. Strengthen Compliance: Ensure BYOD policies and investigations align with legal and regulatory frameworks (e.g., Kenya DPA 2019).
3. Enhanced Incident Response Capability: Quickly and effectively investigate security incidents involving personal employee devices.
4. Protect Intellectual Property: Safeguard sensitive company data and intellectual property residing on BYOD endpoints.
5. Reduced Legal Exposure: Minimize the risk of lawsuits related to employee privacy violations during investigations.
6. Improved Employee Trust: Implement clear policies and transparent investigative practices to maintain employee confidence.
7. Optimized Forensic Processes: Develop efficient and targeted data acquisition methods for BYOD scenarios.
8. Cost-Effective Security: Leverage existing employee devices while maintaining a secure environment.
9. Proactive Threat Intelligence: Gain insights into common BYOD-related threats and vulnerabilities.

10. Robust Litigation Support: Produce forensically sound and legally defensible evidence for disciplinary actions or court cases.

Target Participants

- Digital Forensic Investigators
- Cybersecurity Incident Responders
- IT Security Managers
- Human Resources Professionals (involved in disciplinary actions)
- Legal Counsel (Corporate, Labor, Privacy Law)
- Compliance Officers
- Data Protection Officers (DPOs)
- Mobile Device Management (MDM) Administrators
- Internal Audit & Fraud Examiners
- Risk Management Professionals

Course Outline

Module 1: Introduction to BYOD & Its Risks (BYOD Landscape)

- Definition and Benefits of BYOD for Organizations
- Key Risks and Challenges: Data Leakage, Malware, Compliance, Privacy
- The Blurred Lines: Personal vs. Corporate Data on a Single Device
- Legal and Ethical Considerations of BYOD Adoption
- **Case Study**: Analyzing a recent high-profile data breach linked to a BYOD device.

Module 2: Developing a Forensically Sound BYOD Policy (Policy & Governance)

- Essential Components of a Robust BYOD Policy
- Defining Acceptable Use and Prohibited Activities
- Data Ownership Clauses and Consent for Forensic Access
- Remote Wipe, Data Segregation, and Incident Response Clauses
- **Case Study**: Reviewing a sample BYOD policy and identifying its strengths and weaknesses for forensic purposes, particularly within the Kenyan legal context.

Module 3: Mobile Device Management (MDM) & EMM Forensics (MDM & EMM)

- Overview of MDM/EMM Solutions (e.g., Microsoft Intune, VMware Workspace ONE, Jamf Pro)
- Forensic Capabilities of MDM: Remote Wipe, Selective Wipe, Device Lock, Inventory
- Configuration Profiles and Policy Enforcement
- Log Data from MDM/EMM for Incident Analysis
- **Case Study**: Simulating an incident response involving an MDM-managed BYOD device.

Module 4: Data Segregation & Containerization (Data Separation)

- Techniques for Separating Personal and Corporate Data (e.g., Knox, Secure Folder, Work Profiles)
- Understanding Containerization Technologies and Their Limitations
- Forensic Challenges of Accessing Data within Containers

- Best Practices for Implementing Data Segregation
- **Case Study**: Investigating a BYOD device with a secure container to extract corporate data.

Module 5: Forensic Acquisition Strategies for BYOD (Acquisition Methods)

- Logical Acquisition for BYOD Devices (Backups, ADB, iTunes)
- Selective Data Acquisition vs. Full Disk Imaging for Privacy Compliance
- Remote Acquisition Tools and Techniques for BYOD
- Physical Acquisition Considerations (JTAG, Chip-Off) in Extreme Cases
- **Case Study**: Performing a targeted logical acquisition of corporate email data from an Android BYOD.

Module 6: Mobile OS Forensics in BYOD Context (OS Artifacts)

- Android OS Artifacts Relevant to BYOD Incidents (App usage, Logs, File Systems)
- iOS OS Artifacts Relevant to BYOD Incidents (Logs, Databases, Backups)
- Identifying Corporate Applications and Data Paths
- Understanding User Activity on Both Personal and Work Profiles
- **Case Study**: Analyzing iOS artifacts to determine if a corporate app was used in a policy violation.

Module 7: Cloud Data & Synchronization Forensics (Cloud Data)

- Data Synchronized from BYOD to Cloud Services (OneDrive, Google Drive, iCloud)
- Forensic Acquisition of Cloud Data (Legal Process, Cloud Connectors)
- Identifying Corporate Data in Personal Cloud Accounts
- Challenges of Cloud Forensics in a BYOD Context
- **Case Study**: Investigating potential data exfiltration via a cloud storage app on a BYOD device.

Module 8: App Analysis for BYOD Incidents (App Analysis)

- Analyzing Mobile Applications for Corporate Data Exposure
- Identifying Unauthorized Applications and Shadow IT
- Examining Application Permissions and Network Communications
- Behavioral Analysis of Suspicious Apps on BYOD
- **Case Study**: Analyzing a personal messaging app on a BYOD device for unauthorized sharing of corporate data.

Module 9: Network Forensics & BYOD (Network Connectivity)

- Analyzing Network Connection Logs (Wi-Fi, Bluetooth, VPN) from BYOD
- Identifying Connections to Corporate Networks vs. Personal Networks
- Correlating Network Traffic with Device Activity
- Investigating Data Exfiltration over Network Channels
- **Case Study**: Tracing a BYOD device's connection to an unsecured Wi-Fi network where a data leak occurred.

Module 10: Insider Threat & Data Leakage Investigations (Insider Threat)

- Identifying Red Flags for Insider Threat on BYOD Devices
- Investigating Data Exfiltration through Messaging, Email, or File Sharing Apps
- Analyzing USB Connections and External Storage Transfers
- Detecting Attempts to Circumvent Security Controls

- **Case Study**: Investigating an employee suspected of intellectual property theft using their personal device.

Module 11: Malware & BYOD Incident Response (Malware on BYOD)

- Identifying Malware Infection on BYOD Devices
- Analyzing Mobile Malware (Android, iOS) in a BYOD Context
- Impact of Malware on Corporate Data and Network Security
- Remediation Strategies for Malware-Infected BYODs
- **Case Study**: Responding to a BYOD device infected with a banking Trojan that targeted corporate credentials.

Module 12: Legal & Ethical Considerations in BYOD Forensics (Legal & Ethics)

- **Kenya's Data Protection Act 2019**: Key Principles (Lawfulness, Purpose Limitation, Data Minimization)
- Employee Privacy Rights vs. Employer's Right to Protect Data
- Obtaining Valid Consent for Forensic Examination
- Legal Implications of Remote Wiping and Device Seizure
- **Case Study**: Navigating a scenario where an employee refuses consent for BYOD examination, considering Kenyan legal precedents.

Module 13: Reporting BYOD Forensic Findings (Reporting & Documentation)

- Structuring BYOD Forensic Reports for Legal and HR Audiences
- Clearly Delineating Personal vs. Corporate Data in Findings
- Documenting Consent, Scope, and Limitations of the Investigation
- Presenting Visual Aids for Clarity (Timelines, Data Flows)
- **Case Study**: Drafting a report on a BYOD incident, ensuring compliance with the Kenya Data Protection Act.

Module 14: Expert Witness & Legal Admissibility (Courtroom Presentation)

- Preparing for Testimony in BYOD-Related Disputes
- Defending Forensic Methodologies and Findings
- Addressing Challenges to Data Authenticity and Integrity
- Cross-Examination Strategies for BYOD Cases
- **Case Study**: Mock cross-examination based on a BYOD incident report, focusing on privacy and consent.

Module 15: BYOD Incident Response Planning & Readiness (IR & Readiness)

- Developing a Comprehensive BYOD Incident Response Plan
- Integrating Forensic Readiness into BYOD Policy Implementation
- Training Employees on BYOD Best Practices and Policy Adherence
- Ongoing Monitoring and Proactive Measures for BYOD Security
- **Case Study**: Creating a BYOD incident response playbook for a hypothetical organization.

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.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
03 Aug 2026	14 Aug 2026	Online	$2,200
10 Aug 2026	21 Aug 2026	Online	$2,200
17 Aug 2026	28 Aug 2026	Online	$2,200
24 Aug 2026	04 Sep 2026	Online	$2,200
31 Aug 2026	11 Sep 2026	Online	$2,200
07 Sep 2026	18 Sep 2026	Online	$2,200
14 Sep 2026	25 Sep 2026	Online	$2,200
21 Sep 2026	02 Oct 2026	Online	$2,200

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

Register Online Now

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