Training Course on Artificial Intelligence/Machine Learning Forensics

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The pervasive integration of Artificial Intelligence (AI) and Machine Learning (ML) across industries has introduced unprecedented efficiencies and capabilities, yet it has also opened new frontiers for sophisticated cyber threats. As AI models become integral to critical decision-making processes, the risk of **AI model tampering**, **adversarial attacks**, and **data poisoning** escalates dramatically. Digital forensics, traditionally focused on human-generated data, must now evolve to encompass the unique challenges of investigating incidents involving **compromised AI systems** and **manipulated algorithms**. Training Course on Artificial Intelligence/Machine Learning Forensics provides comprehensive knowledge and practical skills for forensic professionals to navigate this complex landscape, ensuring **AI system integrity** and maintaining **digital trust**.

This course delves deep into the methodologies and tools required to conduct thorough **AI/ML forensic investigations**, identifying indicators of **model drift**, **data manipulation**, and **adversarial machine learning attacks**. Participants will gain expertise in **evidence collection from AI pipelines**, **MLOps environments**, and **inference endpoints**, learning to reconstruct attack paths and attribute malicious activities within AI systems. Through a blend of theoretical understanding and hands-on case studies, this training equips participants with the crucial capabilities to safeguard **AI security**, ensuring accountability and **trustworthiness in AI deployments** in an increasingly AI-driven world.

Programme Curriculum

Training Course on Artificial Intelligence/Machine Learning Forensics

Introduction

The pervasive integration of Artificial Intelligence (AI) and Machine Learning (ML) across industries has introduced unprecedented efficiencies and capabilities, yet it has also opened new frontiers for sophisticated cyber threats. As AI models become integral to critical decision-making

processes, the risk of **AI model tampering**, **adversarial attacks**, and **data poisoning** escalates dramatically. Digital forensics, traditionally focused on human-generated data, must now evolve to encompass the unique challenges of investigating incidents involving **compromised AI systems** and **manipulated algorithms**. Training Course on Artificial Intelligence/Machine Learning Forensics provides comprehensive knowledge and practical skills for forensic professionals to navigate this complex landscape, ensuring **AI system integrity** and maintaining **digital trust**.

This course delves deep into the methodologies and tools required to conduct thorough **AI/ML forensic investigations**, identifying indicators of **model drift**, **data manipulation**, and **adversarial machine learning attacks**. Participants will gain expertise in **evidence collection from AI pipelines**, **MLOps environments**, and **inference endpoints**, learning to reconstruct attack paths and attribute malicious activities within AI systems. Through a blend of theoretical understanding and hands-on case studies, this training equips participants with the crucial capabilities to safeguard **AI security**, ensuring accountability and **trustworthiness in AI deployments** in an increasingly AI-driven world.

Course Duration

10 days

Course Objectives

1. Understand the core principles and methodologies of digital forensics applied to Artificial Intelligence and Machine Learning systems.
2. Develop advanced techniques to detect and analyze various forms of AI model tampering, including **model inversion**, **extraction attacks**, and **transferability attacks**.
3. Gain proficiency in recognizing, analyzing, and mitigating **adversarial examples**, **data poisoning**, and **model evasion attacks**.
4. Learn specialized methods for **evidence collection** from diverse AI/ML components, including **training datasets**, **model weights**, **inference logs**, and **MLOps platforms**.
5. Understand how to conduct forensic analysis within **MLOps pipelines**, identifying vulnerabilities and compromises in continuous integration/continuous deployment (CI/CD) of AI.
6. Develop skills to reconstruct the sequence of events and identify the root cause of **AI security breaches** and **model compromises**.
7. Become adept at using cutting-edge **AI forensics tools** and frameworks for automated analysis and anomaly detection in AI systems.
8. Investigate instances of **algorithmic bias** introduced through tampering or flawed training data, ensuring **ethical AI investigation**.
9. Analyze and mitigate risks associated with **AI supply chain compromises**, from data provenance to third-party model integration.
10. Learn to meticulously document and present **AI forensic reports** that are legally sound and actionable for incident response and legal proceedings.
11. Integrate proactive security measures and **threat intelligence** into AI/ML development lifecycles to prevent future tampering incidents.
12. Understand the emerging challenges and forensic techniques specific to investigating **Large Language Model (LLM) manipulation** and **generative AI misuse**.
13. Grasp the **legal and ethical implications** of AI forensics, adhering to data privacy and regulatory frameworks in investigations.

Organizational Benefits

- Strengthen the organization's defenses against emerging AI-specific cyber threats and sophisticated model tampering attempts.
- Mitigate potential financial losses and reputational damage resulting from compromised AI systems and data breaches.
- Develop internal expertise to rapidly detect, analyze, and respond to AI/ML security incidents, minimizing downtime and impact.
- Meet growing regulatory requirements and industry standards related to AI accountability, transparency, and data integrity.
- Safeguard proprietary AI models, algorithms, and sensitive training data from theft, manipulation, and unauthorized access.
- Foster confidence among stakeholders, customers, and partners by demonstrating a commitment to secure and trustworthy AI.
- Position the organization as a leader in AI security, attracting top talent and reinforcing market leadership in AI innovation.

Target Audience

1. Digital Forensics Investigators.
2. Cybersecurity Analysts.
3. ML Engineers and Data Scientists.
4. Incident Response Teams.
5. Security Architects.
6. Compliance and Risk Officers.
7. Legal Professionals.
8. Red Teams and Penetration Testers.

Course Outline

Module 1: Foundations of AI/ML and Digital Forensics

- Introduction to AI/ML concepts and their application in various industries.
- Overview of traditional digital forensics principles and their limitations in AI environments.
- Understanding the AI/ML lifecycle: data collection, training, deployment, and inference.
- Key differences between traditional digital evidence and AI-specific artifacts.
- **Case Study:** The evolution of digital forensics from network intrusions to targeted AI attacks on critical infrastructure.

Module 2: AI/ML Threat Landscape and Attack Vectors

- Categorization of AI/ML specific threats: adversarial attacks, data poisoning, model evasion, model inversion, membership inference.
- Exploration of attack surfaces in AI systems
- Understanding the motivations and techniques of threat actors targeting AI.
- Impact assessment of AI model tampering on business operations and data integrity.
- **Case Study:** A rogue employee injects poisoned data into a financial fraud detection model, leading to approved fraudulent transactions.

Module 3: Legal and Ethical Considerations in AI Forensics

- Regulatory frameworks and data privacy laws (e.g., GDPR, CCPA) impacting AI investigations.
- Ethical dilemmas in AI forensics.
- Chain of custody for AI-generated evidence and its legal admissibility.
- International cooperation and jurisdiction in cross-border AI cybercrime.

- **Case Study:** A law enforcement agency faces legal challenges due to bias detected in an AI-powered facial recognition system used for suspect identification.

Module 4: AI/ML Forensic Readiness and Preparation

- Establishing an AI/ML forensic framework within an organization.
- Developing incident response plans tailored for AI model tampering.
- Logging and telemetry strategies for AI/ML systems to capture forensic artifacts.
- Proactive threat modeling for AI systems
- **Case Study:** An organization implements comprehensive AI logging after a near-miss incident involving subtle model manipulation detected through unusual inference patterns.

Module 5: Data Acquisition from AI/ML Systems

- Techniques for collecting training datasets, validation sets, and inference data.
- Forensic imaging and acquisition of model weights and architecture files.
- Capturing API calls, runtime environments, and MLOps pipeline logs.
- Challenges of volatile memory acquisition in AI inference environments.
- **Case Study:** Forensic acquisition of a cloud-based ML model under attack, requiring specialized tools for distributed data collection.

Module 6: Analyzing Training Data Tampering (Data Poisoning)

- Methods for detecting and analyzing data poisoning attacks on training datasets.
- Statistical analysis and anomaly detection in large-scale datasets.
- Techniques for identifying corrupted or maliciously injected data points.
- Reconstructing the source and impact of data poisoning attacks.
- **Case Study:** A national security agency investigates a data poisoning attack on a satellite image classification AI, leading to misidentification of critical infrastructure.

Module 7: Model Integrity and Tampering Analysis

- Verification of model checksums, hashes, and digital signatures.
- Techniques for detecting unauthorized modifications to model weights and architecture.
- Model fingerprinting and watermarking for intellectual property protection.
- Reverse engineering AI models to understand their behavior and identify backdoors.
- **Case Study:** A pharmaceutical company discovers that a competitor has stolen and slightly modified its proprietary drug discovery AI model.

Module 8: Adversarial Example Forensics

- Understanding the generation and characteristics of adversarial examples.
- Detection techniques for adversarial inputs at inference time.
- Analyzing the impact of adversarial perturbations on model predictions.
- Traceability of adversarial attacks to their origin and intent.
- **Case Study:** An autonomous vehicle encounters an adversarial sticker on a stop sign, causing its AI to misinterpret the sign and run a red light.

Module 9: MLOps and AI Pipeline Forensics

- Investigating compromises within the MLOps development and deployment pipeline.
- Analyzing CI/CD logs, version control systems, and container registries for anomalies.
- Forensic analysis of MLOps orchestration tools
- Identifying insider threats and supply chain vulnerabilities in MLOps.

- **Case Study:** An investigation reveals that a malicious library was injected into an MLOps pipeline, leading to the deployment of a backdoored AI model.

Module 10: Cloud AI Forensics and Security

- Specific forensic challenges and techniques for AI systems deployed in cloud environments.
- Leveraging cloud provider logs for AI investigations.
- Securing and investigating serverless AI functions and managed AI services.
- Data residency, jurisdiction, and compliance in cloud AI forensics.
- **Case Study:** A financial institution's cloud-based credit scoring AI is compromised, and forensics focuses on unauthorized API calls and data exfiltration from cloud storage.

Module 11: Generative AI and LLM Forensics

- Forensic challenges unique to Large Language Models (LLMs) and generative AI.
- Detecting prompt injection attacks, data leakage from LLMs, and model hallucination for malicious intent.
- Analyzing the provenance of generated content and identifying AI-generated deepfakes.
- Investigating the misuse of generative AI for misinformation campaigns and fraud.
- **Case Study:** A political campaign's public communication is disrupted by AI-generated deepfake audio and video, requiring forensic analysis to trace the source.

Module 12: AI Forensic Reporting and Expert Testimony

- Structuring comprehensive and legally defensible AI forensic reports.
- Presenting complex technical findings clearly to non-technical stakeholders.
- Preparing for and delivering expert testimony in legal proceedings related to AI incidents.
- Ethical considerations for AI forensic experts in court.
- **Case Study:** An expert witness presents a detailed AI forensic report in a court case involving intellectual property theft of an AI algorithm.

Module 13: Remediation, Recovery, and Future of AI Forensics

- Strategies for AI model rollback, data remediation, and system recovery.
- Implementing long-term security enhancements for AI systems.
- Emerging trends in AI security and the evolving landscape of AI forensics.
- The role of explainable AI (XAI) in forensic investigations.
- **Case Study:** Post-incident recovery of a supply chain optimization AI, including data cleansing, model retraining, and implementation of robust model monitoring.

Module 14: Practical AI Forensics Lab - Hands-on Scenarios

- Simulated environment for hands-on investigation of various AI model tampering scenarios.
- Using open-source and commercial AI forensic tools for analysis.
- Step-by-step guidance on evidence acquisition, analysis, and reporting in a lab setting.
- Troubleshooting common challenges in AI forensic investigations.
- **Case Study:** Participants work through a scenario involving a manipulated AI medical diagnosis system, tasked with identifying the tampering method and impact.

Module 15: Capstone Project: End-to-End AI/ML Forensic Investigation

- Participants work in teams on a comprehensive AI/ML forensic case study from inception to final report.
- Applying all learned methodologies and tools to a realistic, multi-faceted incident.
- Developing an incident response strategy and remediation plan.

- Presentation of findings and recommendations to a panel of experts.
- **Case Study:** An AI-powered fraud detection system in a major bank is suspected of compromise, and teams must conduct a full forensic investigation and present their findings.

Training Methodology

This training course employs a **blended learning approach** to maximize participant engagement and skill acquisition. It combines:

- **Instructor-Led Sessions**: Expert-led lectures, discussions, and interactive Q&A sessions.
- **Hands-on Labs and Practical Exercises**: Extensive practical exercises and simulated scenarios using industry-standard tools and custom-built AI environments.
- **Real-World Case Studies**: In-depth analysis of actual AI/ML tampering incidents and their forensic investigation.
- **Group Discussions and Collaborative Learning**: Fostering peer-to-peer learning and knowledge sharing.
- **Capstone Project**: A comprehensive, team-based project to apply all learned concepts in a realistic investigation.
- **Demonstrations**: Live demonstrations of AI/ML attack techniques and forensic tools.
- **Guest Speakers**: Insights from leading experts in AI security, forensics, and legal fields.

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

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

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

Register Online Now

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