Training Course on Digital Forensics in Aviation Security Incidents

Professional Development Training Course Outline

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

Course Introduction

The **aviation sector** is increasingly reliant on complex **digital systems**, making it a prime target for sophisticated **cyber threats** and security breaches. From **air traffic control** and **aircraft systems** to **passenger data** and **ground operations**, the integrity of these digital assets is paramount for **aviation safety** and national security. Training Course on Digital Forensics in Aviation Security Incidents is designed to equip aviation security professionals, IT specialists, and law enforcement with the critical skills needed to effectively respond to, investigate, and mitigate the impact of digital incidents within this highly sensitive domain.

In an era of escalating **cybercrime** and **digital attacks**, the ability to proficiently conduct **digital forensic investigations** is no longer optional but a fundamental requirement for maintaining robust **aviation security**. This course delves into the unique challenges of acquiring, preserving, analyzing, and reporting **digital evidence** from various aviation-specific systems, ensuring compliance with **international regulations** and **legal frameworks**. Participants will gain hands-on experience with cutting-edge **forensic tools** and methodologies to address incidents ranging from **data breaches** and **ransomware attacks** to **insider threats** and **cyber espionage** impacting aviation infrastructure.

Programme Curriculum

Training Course on Digital Forensics in Aviation Security Incidents

Introduction

The **aviation sector** is increasingly reliant on complex **digital systems**, making it a prime target for sophisticated **cyber threats** and security breaches. From **air traffic control** and **aircraft systems** to **passenger data** and **ground operations**, the integrity of these digital assets is paramount for

aviation safety and national security. Training Course on Digital Forensics in Aviation Security Incidents is designed to equip aviation security professionals, IT specialists, and law enforcement with the critical skills needed to effectively respond to, investigate, and mitigate the impact of digital incidents within this highly sensitive domain.

In an era of escalating **cybercrime** and **digital attacks**, the ability to proficiently conduct **digital forensic investigations** is no longer optional but a fundamental requirement for maintaining robust **aviation security**. This course delves into the unique challenges of acquiring, preserving, analyzing, and reporting **digital evidence** from various aviation-specific systems, ensuring compliance with **international regulations** and **legal frameworks**. Participants will gain hands-on experience with cutting-edge **forensic tools** and methodologies to address incidents ranging from **data breaches** and **ransomware attacks** to **insider threats** and **cyber espionage** impacting aviation infrastructure.

Course Duration

5 days

Course Objectives

1. Acquire and preserve **volatile** and **non-volatile digital evidence** from aviation systems (e.g., flight recorders, avionics, ground control networks, passenger systems) following **chain of custody** best practices.
2. Develop systematic **incident response** protocols for aviation security incidents, including **containment, eradication, and recovery** strategies.
3. Perform in-depth **network forensics** to identify **indicators of compromise (IoCs)**, analyze **network logs**, and trace malicious activity across aviation networks.
4. Utilize **malware analysis** techniques (static and dynamic) to understand the nature and impact of **aviation-specific malware** and **advanced persistent threats (APTs)**.
5. Apply **cloud forensics** principles and tools to investigate incidents involving **aviation cloud infrastructure** and **data storage**.
6. Extract and analyze digital evidence from **mobile devices** used in aviation operations, including smartphones, tablets, and specialized equipment.
7. Understand and counter **anti-forensics techniques** used by adversaries to evade detection and hinder investigations in aviation incidents.
8. Guarantee the **legal admissibility** of digital evidence collected, adhering to **international legal frameworks** and **cybercrime legislation**.
9. Develop clear, concise, and legally sound **forensic reports** for stakeholders, including management, legal teams, and law enforcement.
10. Utilize forensic findings to identify vulnerabilities and strengthen the overall **cybersecurity posture** of aviation organizations.
11. Integrate **threat intelligence** and **OSINT (Open Source Intelligence)** into digital forensic investigations for proactive threat hunting in aviation.
12. Participate in realistic **cyber incident simulations** and **tabletop exercises** specific to aviation security challenges.
13. Navigate and apply relevant **aviation security regulations** (e.g., ICAO Annex 17, EASA) and **data privacy laws (GDPR)** in digital forensics investigations.

Organizational Benefits

- Rapid and effective response to **aviation cyber incidents**, minimizing downtime and financial losses.

- Proactive identification and mitigation of **digital vulnerabilities** within critical aviation systems.
- Ensuring all **digital evidence** is collected and preserved to **legal standards**, bolstering legal defensibility.
- Developing an internal capacity for **threat hunting** and early detection of sophisticated attacks.
- Utilizing forensic insights to reinforce **aviation cybersecurity infrastructure** and policies.
- Safeguarding **passenger data**, operational information, and intellectual property from **data breaches**.
- Maintaining public and stakeholder confidence in the security and reliability of aviation operations.
- Reducing the reliance on external forensic experts and minimizing the financial impact of **cyberattacks**.

Target Audience

1. Aviation Security Personnel.
2. IT and Cybersecurity Professionals.
3. Law Enforcement Agencies.
4. Regulatory Compliance Officers.
5. Legal Professionals.
6. Auditors and Risk Managers.
7. Airline and Airport Management.
8. Military and Government Security Officials

Course Outline

Module 1: Foundations of Digital Forensics in Aviation

- Introduction to Digital Forensics principles and methodologies.
- Understanding the unique digital landscape of aviation (avionics, ground systems, air traffic control).
- Types of digital evidence relevant to aviation security incidents.
- The Digital Forensic Investigation Lifecycle in an aviation context.
- Legal and ethical considerations for digital evidence in aviation.
- **Case Study:** Analysis of a simulated **DDoS attack** on an airline's booking system and the initial evidence identification.

Module 2: Digital Evidence Identification and Collection in Aviation

- Techniques for identifying and acquiring volatile data from live aviation systems.
- Best practices for acquiring non-volatile data from hard drives, SSDs, and specialized aviation equipment.
- Tools and methods for creating forensic images and ensuring data integrity.
- Handling fragmented, encrypted, and corrupted digital evidence in aviation environments.
- Establishing and maintaining a robust **chain of custody** for aviation-related digital evidence.
- **Case Study:** Collection of evidence from an **airline employee's workstation** suspected of an insider threat data exfiltration.

Module 3: File System and Data Carving Forensics

- Deep dive into various file systems prevalent in aviation IT infrastructure (NTFS, Ext4, HFS+).

- Techniques for recovering deleted files, hidden partitions, and slack space.
- Metadata analysis for uncovering crucial information about aviation documents and communications.
- Advanced data carving and signature analysis for reconstructing lost or damaged aviation data.
- Understanding and mitigating **anti-forensics** techniques impacting file systems.
- **Case Study:** Recovering deleted flight plan modifications from a compromised **airport operations server**.

Module 4: Network Forensics and Traffic Analysis in Aviation

- Fundamentals of network protocols and their role in aviation communications.
- Collecting and analyzing network traffic using tools like Wireshark and network intrusion detection systems (NIDS).
- Identifying suspicious network patterns, anomalies, and **indicators of compromise (IoCs)** in aviation networks.
- Investigating common network-based attacks (e.g., **Man-in-the-Middle attacks**, **port scanning**) targeting aviation.
- Log analysis from various aviation network devices (routers, switches, firewalls).
- **Case Study:** Tracing the origin of a **malicious command-and-control communication** impacting an aircraft's ground maintenance system.

Module 5: Malware and Threat Analysis for Aviation Security

- Understanding different types of **malware** relevant to aviation (e.g., **ransomware**, **spyware**, **rootkits**).
- Static malware analysis techniques for examining suspicious aviation-related executables and scripts.
- Dynamic malware analysis using sandboxing environments to observe malware behavior.
- Identifying **malware signatures** and developing effective detection and prevention strategies.
- Analyzing sophisticated **APTs** targeting aviation infrastructure and intellectual property.
- **Case Study:** Dissecting a **ransomware strain** that encrypted critical operational data at a regional airport.

Module 6: Specialized Aviation Digital Forensics

- **Mobile device forensics** for smartphones, tablets, and specialized aviation equipment (e.g., electronic flight bags).
- **Cloud forensics** techniques for investigating incidents in aviation cloud environments (e.g., data storage, SaaS applications).
- Forensics of **Internet of Things (IoT)** devices in aviation (e.g., smart airport systems, drone security).
- Analysis of data from aircraft entertainment systems and passenger Wi-Fi networks.
- Introduction to **Industrial Control System (ICS) forensics** for aviation operational technology.
- **Case Study:** Extracting communication logs from an **unauthorized drone's control unit** found near airport premises.

Module 7: Legal, Reporting, and Expert Witness Considerations

- Review of international and national **aviation security regulations** (e.g., ICAO, EASA, TSA).

- Compliance with **data privacy laws** such as GDPR and CCPA in handling passenger and employee data.
- Structuring and writing comprehensive, legally defensible **forensic reports**.
- Preparing for and delivering **expert witness testimony** in legal proceedings.
- Ethical responsibilities and professional conduct for digital forensic investigators in aviation.
- **Case Study:** Preparing a forensic report for a **data breach incident** involving passenger manifest data, ensuring legal compliance.

Module 8: Advanced Topics and Future Trends

- **Threat intelligence** integration for proactive **cyber threat hunting** in aviation.
- Introduction to **Artificial Intelligence (AI)** and **Machine Learning (ML)** in digital forensics.
- **Blockchain forensics** and its potential applications in aviation security.
- Emerging **cyber threats** and their potential impact on the aviation industry (e.g., **quantum computing threats**).
- Developing and implementing a **forensic readiness** plan for aviation organizations.
- **Case Study:** Simulating a **sophisticated cyber-physical attack** on an **air traffic control system** and developing a rapid response strategy.

Training Methodology

This training course employs a blended learning approach, combining theoretical knowledge with extensive hands-on practical application.

- **Interactive Lectures:** Engaging presentations covering core concepts and methodologies.
- **Practical Labs & Exercises:** Hands-on experience with industry-standard digital forensic tools and simulated aviation security incident scenarios.
- **Case Studies:** Real-world examples and in-depth analysis of past aviation security incidents to reinforce learning.
- **Group Discussions:** Collaborative learning and knowledge sharing among participants.
- **Tabletop Exercises & Simulations:** Realistic simulations of aviation cyber incidents to test response capabilities and decision-making under pressure.
- **Expert Demonstrations:** Live demonstrations of forensic techniques and tool usage by experienced practitioners.
- **Q&A Sessions:** Opportunities for participants to clarify doubts and engage with instructors.

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