Training Course on Digital Forensics for Archivists and Special Collections

Professional Development Training Course Outline

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

Course Introduction

The rapidly expanding volume of **born-digital** and **digitized archival collections** presents unprecedented challenges and opportunities for cultural heritage institutions. As the digital landscape evolves, so too do the threats of data loss, corruption, and cyberattacks, making **digital preservation** a paramount concern. Training Course on Digital Forensics for Archivists and Special Collections aims to equip professionals with the essential knowledge and **practical skills** to **identify, acquire, analyze, and preserve digital evidence** from a diverse range of media. By bridging the gap between traditional archival principles and cutting-edge **digital forensics methodologies**, we empower archivists to ensure the **authenticity, integrity, and accessibility** of invaluable digital records for future generations, transforming them into proactive guardians of our collective **digital heritage**.

This specialized program recognizes that traditional archival training often lacks the specific technical expertise required to navigate the complexities of **electronic records management** and **cybersecurity** in a heritage context. Participants will delve into the intricacies of **data recovery**, **metadata analysis**, and **chain of custody protocols**, tailored specifically for the unique challenges of **special collections** and historical data. Through a blend of theoretical understanding and **hands-on exercises**, this course fosters a robust foundation in **e-discovery**, **incident response**, and **long-term digital stewardship**, mitigating risks and building resilience in the face of persistent digital threats.

Programme Curriculum

Training Course on Digital Forensics for Archivists and Special Collections

Introduction

The rapidly expanding volume of **born-digital** and **digitized archival collections** presents unprecedented challenges and opportunities for cultural heritage institutions. As the digital

landscape evolves, so too do the threats of data loss, corruption, and cyberattacks, making **digital preservation** a paramount concern. Training Course on Digital Forensics for Archivists and Special Collections aims to equip professionals with the essential knowledge and **practical skills** to **identify, acquire, analyze, and preserve digital evidence** from a diverse range of media. By bridging the gap between traditional archival principles and cutting-edge **digital forensics methodologies**, we empower archivists to ensure the **authenticity, integrity, and accessibility** of invaluable digital records for future generations, transforming them into proactive guardians of our collective **digital heritage**.

This specialized program recognizes that traditional archival training often lacks the specific technical expertise required to navigate the complexities of **electronic records management** and **cybersecurity** in a heritage context. Participants will delve into the intricacies of **data recovery**, **metadata analysis**, and **chain of custody protocols**, tailored specifically for the unique challenges of **special collections** and historical data. Through a blend of theoretical understanding and **hands-on exercises**, this course fosters a robust foundation in **e-discovery**, **incident response**, and **long-term digital stewardship**, mitigating risks and building resilience in the face of persistent digital threats.

Course Duration

10 days

Course Objectives

1. Understand core principles of **long-term digital preservation**, including fixity, provenance, and authenticity in a forensic context.
2. Learn techniques for **forensic imaging**, **data acquisition**, and the **secure handling of digital media** from diverse sources (e.g., legacy systems, portable devices, cloud storage).
3. Establish rigorous **chain of custody documentation** for all digital evidence to ensure its legal admissibility and evidential integrity.
4. Proficiently **extract and analyze metadata** (EXIF, file system, application-specific) to reconstruct timelines, establish provenance, and identify data anomalies.
5. Gain hands-on experience with industry-standard **open-source and commercial digital forensics tools** for data recovery, carving, and analysis.
6. Apply digital forensic principles within existing **ERM frameworks** and policies for effective lifecycle management of born-digital archives.
7. Develop a foundational understanding of **incident response planning** and initial steps for mitigating data breaches and cyberattacks on archival systems.
8. Grasp the **legal and ethical considerations** surrounding digital evidence, including privacy, copyright, and **e-discovery compliance** in a cultural heritage context.
9. Learn techniques for **recovering deleted or corrupted files** and restoring digital collections from various storage media.
10. Identify potential **cybersecurity vulnerabilities** and risks inherent in managing and preserving **digital special collections**.
11. Contribute to the development of **digital forensics policies** and best practices within archival institutions.
12. Foster effective communication and collaboration with IT and cybersecurity professionals for comprehensive **digital asset protection**.
13. Explore the impact of **AI in digital forensics**, **blockchain for provenance**, and other **trending technologies** on archival practices.

Organizational Benefits

- Proactively safeguard valuable born-digital and digitized cultural heritage against data loss, corruption, and cyber threats.
- Ensure the trustworthiness and reliability of digital collections, critical for research, legal, and historical purposes.
- Equip staff with the skills to identify vulnerabilities and respond effectively to security incidents, minimizing reputational and financial damage.
- Meet growing requirements for digital evidence preservation and e-discovery in potential legal disputes.
- Efficiently manage digital storage and access by implementing sound digital forensics and preservation strategies.
- Position the institution as a leader in **digital stewardship** and the ethical management of digital cultural heritage.
- Upskill archival professionals with critical **21st-century digital skills**, fostering a more resilient and technologically proficient team.

Target Audience

1. Archivists & Special Collections Librarians
2. Records Managers
3. Digital Preservation Specialists
4. Curators of Digital Art & Media
5. IT Professionals in Cultural HeritageLibrarians with Digital Collections Responsibilities
6. Researchers & Academics
7. Legal & Compliance Officers in Heritage Institutions

15 Modules with 5 Bullets per Module with Case Studies

Module 1: Introduction to Digital Forensics & Archival Context

- Defining digital forensics and its relevance to archival science.
- Understanding the unique challenges of born-digital and digitized collections.
- Overview of legal and ethical considerations in digital evidence.
- Distinction between digital preservation and digital forensics.
- The evolving landscape of digital threats to cultural heritage.
- **Case Study:** The challenges of preserving early web archives and identifying deleted content.

Module 2: Foundations of Digital Evidence

- Types of digital evidence: volatile vs. non-volatile data.
- Understanding file systems (NTFS, FAT, HFS+, Ext) and their forensic implications.
- Introduction to data storage concepts: sectors, clusters, slack space.
- Data integrity and fixity: hashing (MD5, SHA) for verification.
- The importance of documentation in digital forensics.
- **Case Study:** Analyzing a compromised workstation from a special collection researcher to determine data exfiltration.

Module 3: Digital Acquisition & Imaging Techniques

- Principles of forensically sound data acquisition.
- Methods for creating bit-stream images (forensic copies).
- Tools for acquisition: FTK Imager, Guymager, dd.
- Acquiring data from various media: hard drives, USB drives, optical media.
- Live vs. dead acquisitions and their respective considerations.

- **Case Study:** Acquiring data from a legacy floppy disk containing early born-digital manuscripts.

Module 4: Chain of Custody & Evidence Handling

- Establishing and maintaining a robust chain of custody.
- Proper storage and transportation of digital evidence.
- Documentation requirements for every step of the process.
- Legal admissibility of digital evidence in court.
- Best practices for laboratory setup and security.
- **Case Study:** Tracing the chain of custody for a collection of politically sensitive emails from acquisition to archival ingest.

Module 5: File System Analysis & Data Recovery

- In-depth analysis of file system structures for hidden or deleted data.
- Techniques for recovering deleted files and fragments (file carving).
- Understanding the Recycle Bin and its forensic significance.
- Identifying and reconstructing fragmented files.
- Tools for file system analysis: Autopsy, Sleuth Kit.
- **Case Study:** Recovering deleted drafts of a prominent author's digital manuscripts from a reformatted hard drive.

Module 6: Metadata Forensics for Archival Context

- Types of metadata: descriptive, structural, administrative, preservation.
- Extracting and interpreting EXIF data from images and videos.
- Analyzing document metadata (Microsoft Office, PDF) for provenance.
- Timelines and event reconstruction from metadata.
- The role of metadata in authenticating digital objects.
- **Case Study:** Using metadata to establish the original creation date and author of a disputed digital photograph in a historical collection.

Module 7: Email & Communication Forensics

- Understanding email headers and their forensic value.
- Recovering and analyzing deleted emails.
- Forensics of instant messaging and social media data.
- Tools for email analysis: EnCase, Autopsy.
- Legal and ethical considerations in communication forensics.
- **Case Study:** Investigating an email correspondence within a political special collection to establish the timeline of events.

Module 8: Operating System Artifacts & Registry Analysis

- Identifying and interpreting operating system artifacts (Windows, macOS, Linux).
- Analyzing the Windows Registry for user activity and system configuration.
- Browser history, downloads, and cached content analysis.
- User account forensics and login activity.
- Understanding system logs and event viewers.
- **Case Study:** Reconstructing user activity on an archival workstation to determine if unauthorized access to sensitive records occurred.

Module 9: Mobile Device Forensics (Introduction)

- Overview of mobile device types and operating systems.
- Challenges in mobile device data acquisition (lock screens, encryption).
- Extracting data from mobile devices: logical vs. physical acquisitions.
- Analyzing call logs, SMS, and application data.
- Tools and techniques for basic mobile forensics.
- **Case Study:** Acquiring and analyzing data from a period-appropriate mobile phone found within a personal papers collection.

Module 10: Network Forensics for Archival Security

- Introduction to network fundamentals and protocols.
- Identifying and analyzing network traffic patterns.
- Detecting unauthorized access and data exfiltration attempts.
- Packet analysis using Wireshark.
- Securing archival networks against common cyber threats.
- **Case Study:** Analyzing network logs to determine the source of a suspected ransomware attack on an institutional repository.

Module 11: Malware Analysis & Threat Detection

- Understanding different types of malware (viruses, ransomware, spyware).
- Basic principles of static and dynamic malware analysis.
- Identifying indicators of compromise (IOCs).
- Strategies for preventing malware infections in archival environments.
- Incident response for malware outbreaks.
- **Case Study:** Analyzing a suspicious file found in a born-digital collection to determine if it contains malicious code.

Module 12: Cloud Forensics & Digital Archiving

- Challenges and opportunities of cloud storage for archives.
- Acquiring data from cloud services (e.g., Google Drive, Dropbox).
- Legal and jurisdictional issues in cloud forensics.
- Securing cloud-based archival repositories.
- Forensic considerations for hybrid cloud environments.
- **Case Study:** Investigating data stored in a cloud-based collaboration platform used by a historical organization to uncover missing records.

Module 13: E-Discovery & Legal Holds in Archival Practice

- Introduction to e-discovery and its stages (preservation, collection, processing, review, production).
- Implementing legal holds for potentially relevant digital records.
- Role of archivists in e-discovery processes.
- Data redaction and privilege review considerations.
- Collaboration with legal counsel during e-discovery.
- **Case Study:** Participating in a mock e-discovery exercise related to a historical legal case, identifying relevant digital documents from an archive.

Module 14: Digital Forensics Policies & Program Development

- Developing institutional policies for digital forensics and preservation.
- Establishing a digital forensics incident response plan.
- Building a digital forensics toolkit and lab.

- Training and awareness programs for staff.
- Long-term planning for digital preservation and forensic readiness.
- **Case Study:** Developing a sample digital forensics policy for a hypothetical university special collections department.

Module 15: Emerging Trends & Future Challenges

- The impact of Artificial Intelligence (AI) on digital forensics.
- Blockchain technology for provenance and data integrity.
- Forensics of the Internet of Things (IoT) devices in archives.
- Big data forensics and scalable solutions.
- The future of digital stewardship in an increasingly complex digital world.
- **Case Study:** Discussing the challenges and potential solutions for preserving and forensically analyzing complex interactive digital exhibits.

Training Methodology

This course employs a blended learning approach, combining theoretical instruction with extensive hands-on practical exercises and real-world case studies to ensure deep understanding and skill development.

- **Interactive Lectures & Discussions:** Engaging presentations followed by open forums for questions and knowledge sharing.
- **Demonstrations:** Live demonstrations of digital forensics tools and techniques.
- **Hands-on Labs:** Practical exercises using specialized forensic software and simulated digital environments. Participants will work with various forms of digital media.
- **Case Study Analysis:** In-depth analysis of real and hypothetical scenarios relevant to archival and special collections.
- **Group Activities & Problem Solving:** Collaborative tasks to reinforce learning and encourage peer interaction.
- **Practical Assignments:** Take-home exercises to apply learned concepts.
- **Expert Guest Speakers:** Insights from leading professionals in digital forensics, archival science, and cybersecurity.
- **Resource Sharing:** Provision of comprehensive course materials, relevant readings, and a curated list of tools and resources.

Register as a group from 3 participants for a Discount

Send us an email: Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
07 Sep 2026	18 Sep 2026	Physical	$3,000
14 Sep 2026	25 Sep 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
28 Sep 2026	09 Oct 2026	Physical	$3,000

Start Date	End Date	Location	Price
05 Oct 2026	16 Oct 2026	Physical	$3,000
12 Oct 2026	23 Oct 2026	Physical	$3,000
19 Oct 2026	30 Oct 2026	Physical	$3,000
26 Oct 2026	06 Nov 2026	Physical	$3,000

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

Register Online Now

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