Datastat Research
Building Capacity in Training and Research

DATASTAT TRAINING IN

OFFICIAL COURSE PROSPECTUS

Center for Advanced Research & Professional Development

Nairobi Training Center • Global Virtual Academy • Corporate On-Site

LEGAL INSTITUTE

Digital Evidence Management and Electronic Discovery (eDiscovery) Training Course

Comprehensive Course Syllabus, Practical Modules & Upcoming Schedules

PROGRAM SPECIFICATIONS & HIGHLIGHTS

DURATION
5 Days Practical Hands-on

DELIVERY MODES
In-Person Class & Live Virtual

CERTIFICATION
Accredited Certificate of Completion

INTAKES / DATES
Multiple Cohort Schedules Included

PREPARED FOR:

Valued Participant

Email: training@datastatresearch.org | Issued: November 21, 2026

Academic & Professional Training Year: 2026

DATASTAT TRAINING INSTITUTE

P.O. Box 102802-00101, Nairobi, Kenya

Training Centers: Nairobi • Mombasa • Kigali • Dubai • Live Virtual Academy

Tel: +254 724 527 104 | +254 734 969 612

Email: training@datastatresearch.org

www.datastatresearch.org

Digital Evidence Management and Electronic Discovery (eDiscovery) Training Course

Legal Institute • 5 Days Intensive • Accredited Certification

Course Overview

Digital Evidence Management and Electronic Discovery (eDiscovery) Training Course is programme designed to equip participants with the knowledge and practical skills required to identify, collect, preserve, process, analyse, review, and present digital evidence in legal proceedings, corporate investigations, regulatory audits, and litigation matters.

Key Skills & Software Tools Covered

Digital Evidence Preservation • eDiscovery Management • Electronic Forensics • Litigation Support Analysis

Upcoming Training Schedules

Confirmed cohort intakes and venues. Both physical in-person classroom and live virtual online seats are available.

TRAINING DATES	LOCATION / VENUE	FORMAT / DURATION	INVESTMENT (FEE)
23 Nov 2026 – 27 Nov 2026	Nairobi	Classroom / 5d	**$1,500 USD / KES 110,000**
23 Nov 2026 – 27 Nov 2026	Kigali	Classroom / 5d	**$3,000 USD / KES 110,000**
23 Nov 2026 – 27 Nov 2026	Dubai	Classroom / 5d	**$5,000 USD / KES 110,000**
23 Nov 2026 – 27 Nov 2026	Cape Town	Classroom / 5d	**$4,500 USD / KES 110,000**
23 Nov 2026 – 27 Nov 2026	Addis Ababa	Classroom / 5d	**$3,000 USD / KES 110,000**
23 Nov 2026 – 27 Nov 2026	Singapore	Classroom / 5d	**$5,000 USD / KES 110,000**
23 Nov 2026 – 27 Nov 2026	Istanbul	Classroom / 5d	**$5,000 USD / KES 110,000**
23 Nov 2026 – 27 Nov 2026	Bangkok	Classroom / 5d	**$5,000 USD / KES 110,000**
23 Nov 2026 – 27 Nov 2026	Accra	Classroom / 5d	**$4,000 USD / KES 110,000**
30 Nov 2026 – 4 Dec 2026	Nairobi	Classroom / 5d	**$1,500 USD / KES 110,000**
30 Nov 2026 – 4 Dec 2026	Kigali	Classroom / 5d	**$3,000 USD / KES 110,000**
30 Nov 2026 – 4 Dec 2026	Dubai	Classroom / 5d	**$5,000 USD / KES 110,000**

* Corporate discounts and customized cohort scheduling are available for teams of 3 or more participants.

Course Curriculum & Modules

Digital Evidence Management and Electronic Discovery (eDiscovery) Training Course

Introduction

Digital Evidence Management and Electronic Discovery (eDiscovery) Training Course is programme designed to equip participants with the knowledge and practical skills required to identify, collect, preserve, process, analyse, review, and present digital evidence in legal proceedings, corporate investigations, regulatory audits, and litigation matters. As organisations increasingly depend on digital platforms, cloud computing, electronic communications, mobile devices, and enterprise information systems, the volume and complexity of electronically stored information (ESI) continue to grow. Effective digital evidence management and electronic discovery have therefore become essential capabilities for legal practitioners, forensic investigators, compliance professionals, information technology specialists, and corporate risk managers. This course explores modern digital forensics, eDiscovery workflows, electronic records management, forensic data acquisition, metadata preservation, chain of custody, data integrity, legal hold management, and information governance to ensure that electronic evidence remains authentic, reliable, accessible, and legally defensible.

The programme further examines the legal, technical, operational, and ethical considerations involved in managing electronic evidence throughout its lifecycle. Participants will gain practical insights into eDiscovery technology, forensic imaging, email discovery, cloud evidence collection, mobile device forensics, data processing, predictive coding, Technology-Assisted Review (TAR), artificial intelligence in eDiscovery, cybersecurity investigations, and digital evidence admissibility. Particular attention is given to preserving evidential integrity, maintaining defensible documentation, managing cross-border data transfers, protecting personal information, and complying with applicable data protection and electronic evidence laws. Through practical exercises, simulated investigations, technology demonstrations, and real-world case studies, participants will develop the competencies required to manage complex digital investigations, reduce litigation costs, strengthen regulatory compliance, and support informed legal decision-making.

Course Duration

5 days

Course Objectives

By the end of this training course, participants will be able to:

- Understand the fundamental principles of digital evidence management, electronic discovery, and digital forensics.
- Identify, locate, classify, and preserve electronically stored information (ESI) across different digital environments.
- Apply best practices in forensic data acquisition, imaging, extraction, and evidence preservation.
- Establish and maintain a defensible chain of custody for electronic evidence.
- Implement effective legal hold procedures and electronic records preservation strategies.
- Understand eDiscovery workflows, including identification, preservation, collection, processing, review, and production.
- Apply metadata analysis and file integrity verification techniques using digital forensic tools.
- Conduct effective email discovery, mobile device evidence collection, and cloud data investigations.
- Utilise AI-powered eDiscovery, predictive coding, and Technology-Assisted Review (TAR) to improve document review efficiency.
- Evaluate digital evidence authenticity, reliability, relevance, admissibility, and evidential weight.
- Manage data privacy, confidentiality, cybersecurity, and regulatory compliance risks during investigations.
- Develop defensible electronic evidence documentation, reporting, and disclosure procedures.
- Optimise digital investigation processes through automation, information governance, and cost-effective eDiscovery strategies.

Target Audience

- Lawyers, advocates, legal advisers, and litigation support professionals.
- Digital forensic investigators and forensic analysts.
- IT managers, system administrators, and cybersecurity professionals.
- Corporate compliance officers and regulatory affairs specialists.
- Records managers and information governance professionals.
- Law enforcement officers and criminal investigation personnel.
- Risk management, internal audit, and fraud investigation professionals.
- Data protection officers, privacy specialists, and legal technology consultants.

Course Modules

Module 1: Fundamentals of Digital Evidence Management and eDiscovery

- Introduction to digital evidence management and electronic discovery principles.
- Understanding electronically stored information (ESI) and digital evidence classifications.
- The electronic evidence lifecycle and information management frameworks.
- Roles and responsibilities of legal, technical, and forensic investigation teams.
- Challenges associated with digital evidence collection, preservation, and disclosure.
- Case Study: A multinational organisation faces commercial litigation involving thousands of electronic documents.

Module 2: Digital Evidence Identification, Collection and Preservation

- Identifying potential digital evidence sources across enterprise IT environments.
- Forensic acquisition of computers, servers, storage devices, and removable media.
- Mobile device evidence collection and preservation techniques.
- Cloud-based evidence collection and remote data acquisition.
- Implementing secure evidence storage, hashing, and data integrity verification.
- Case Study: A financial institution investigates suspected employee fraud involving corporate emails, mobile communications, and cloud storage.

Module 3: Chain of Custody and Digital Evidence Integrity

- Understanding chain of custody principles and legal requirements.
- Maintaining comprehensive digital evidence collection logs.
- Applying cryptographic hashing techniques for evidence authentication.
- Preventing unauthorised access, alteration, deletion, and evidence contamination.
- Developing defensible evidence handling and transfer procedures.
- Case Study: During a corporate fraud investigation, discrepancies emerge between the original digital evidence and forensic copies presented by investigators.

Module 4: Electronic Discovery (eDiscovery) Processes and Workflows

- Understanding the Electronic Discovery Reference Model (EDRM).
- Identifying, preserving, collecting, processing, reviewing, and producing ESI.
- Developing effective litigation readiness and legal hold procedures.
- Managing document review, deduplication, and data filtering.
- Establishing defensible eDiscovery project management frameworks.
- Case Study: A company receives a court order requiring the production of electronic communications covering five years.

Module 5: Digital Forensics, Metadata and Advanced Evidence Analysis

- Understanding file systems, metadata structures, and digital artefacts.
- Examining email headers, timestamps, access logs, and communication records.
- Applying forensic analysis techniques to deleted and recovered files.
- Analysing internet activity, digital transactions, and user access histories.
- Using forensic software for evidence examination and technical reporting.
- Case Study: Investigators suspect an employee has transferred confidential company documents to an external competitor.

Module 6: eDiscovery Technology, Artificial Intelligence and Predictive Coding

- Introduction to modern eDiscovery platforms and litigation support technologies.
- Applying artificial intelligence (AI) and machine learning in document classification.
- Understanding predictive coding and Technology-Assisted Review (TAR).
- Using automated deduplication, email threading, and conceptual analytics.
- Evaluating technology-driven review accuracy, transparency, and defensibility.
- Case Study: A legal department must review 500,000 electronic documents within a strict litigation deadline.

Module 7: Legal, Regulatory and Data Privacy Considerations

- Understanding legal requirements governing electronic evidence and disclosure.
- Digital evidence admissibility, authenticity, relevance, and evidential weight.
- Data protection, confidentiality, and privacy considerations in eDiscovery.
- Managing cross-border data transfers and international data access restrictions.
- Addressing cybersecurity, privilege, retention, and regulatory compliance risks.
- Case Study: A multinational organisation faces litigation requiring access to employee communications stored in several countries.

Module 8: Digital Evidence Reporting, Presentation and Litigation Readiness

- Preparing comprehensive digital forensic investigation reports.
- Developing defensible evidence inventories and disclosure schedules.
- Presenting digital evidence to courts, tribunals, and regulatory authorities.
- Managing expert witnesses and technical explanations of digital findings.
- Establishing organisational eDiscovery policies and continuous improvement frameworks.
- Case Study: A digital forensic investigator is appointed as an expert witness in a complex intellectual property dispute.

Training Methodology

- 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@datastatresearch.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 DATASTAT CONSULTANCY LTD account, as indicated in the invoice so as to enable us prepare better for you.

Certification & Learning Methodology

- Hands-on practical delivery with real-world datasets, case studies, and lab exercises.
- Post-training mentorship, access to class resources, and customized follow-up support.
- Participants who successfully complete the course receive an accredited Datastat Certificate of Completion.

How to Enroll & Reserve Your Seat

1. Online Registration: Visit https://datastatresearch.org/courses/digital-evidence-management-and-electronic-discovery-ediscovery-training-course to register onlin
2. Email Booking: Send participant details to training@datastatresearch.org for official invoice & reservation.
3. Support & Assistance: Inquire via phone +254 724 527 104 | +254 734 969 612.