Professional Certificate in Legal Technology and Data Analytics

E-Discovery and Digital Forensics

AALL, American Association of Law Libraries, is a professional organization that provides resources and support for law librarians and legal professionals, including those working in e-discovery and digital forensics. Access Control List (ACL) refers to a list of permissions and access rights assigned to users or groups, used to control and manage access to digital data and systems. Admissibility refers to the process of determining whether evidence is admissible in a court of law, taking into account factors such as relevance, reliability, and authenticity. AES, Advanced Encryption Standard, is a standard for encrypting data at rest and in transit, ensuring the confidentiality and integrity of digital information. AI, Artificial Intelligence, refers to the use of machine learning and algorithms to analyze and process large datasets, including those related to e-discovery and digital forensics. Algorithm refers to a set of instructions used to solve a problem or perform a task, such as data analysis or pattern recognition. Anti-forensics refers to the process of attempting to obscure or destroy digital evidence, making it difficult or impossible to recover or analyze. API, Application Programming Interface, refers to a set of protocols and tools used to build and integrate software applications, including those used in e-discovery and digital forensics. Application refers to a software program or system designed to perform a specific task or function, such as data analysis or document management. Archive refers to a collection of data or documents that are stored and preserved for long-term retention and access. Artificial Intelligence (AI) refers to the use of machine learning and algorithms to analyze and process large datasets, including those related to e-discovery and digital forensics. Authentication refers to the process of verifying the identity or authenticity of a user, system, or data source. Authorization refers to the process of granting or denying access to a system, data, or resource based on a user's identity or role. Automated Discovery refers to the use of software and algorithms to automate the e-discovery process, including data collection, processing, and review. Backup refers to a copy of data or systems that is stored and preserved in case of loss or disaster. Big Data refers to the large volumes of data that are generated and collected by organizations, including structured and unstructured data. Binary refers to a format of data that is composed of binary code, such as 0s and 1s. Bit refers to a single unit of binary data, such as a 0 or 1. Bloomberg Law refers to a database of legal information and resources that provides access to cases, statutes, and regulations. BYOD, Bring Your Own Device, refers to the policy of allowing employees to use their personal devices for work purposes, including accessing company data and systems. Cache refers to a temporary storage location for data or information that is frequently accessed or used. Case Law refers to the body of law that is based on judicial decisions and precedents, rather than statutes or regulations. Categorization refers to the process of organizing and classifying data or documents into categories or groups. Certification refers to the process of verifying the authenticity or validity of a digital signature or certificate. Chain of Custody refers to the record of handling and possession of evidence, from its initial collection to its final disposition. Cloud Computing refers to the model of delivering computing services over the internet, including storage, processing, and applications. Cloud Storage refers to the model of storing data in a remote location, accessible over the internet. Coding refers to the process of assigning codes or tags to data or documents to facilitate search and retrieval. Collection refers to the process of gathering and preserving evidence or data for use in investigations or

litigation. Computer Forensics refers to the application of scientific principles and methods to the analysis and examination of digital evidence. Confidentiality refers to the process of protecting -sensitive or privileged information from unauthorized access or disclosure. Cookie refers to a small file or piece of data that is stored on a user's device to track their activity or preferences. Cryptanalysis refers to the process of analyzing and breaking encryption methods to access or read encrypted data. Cryptography refers to the practice of protecting information by transforming it into an unreadable format, using algorithms and keys. Cybersecurity refers to the practice of protecting computer systems and networks from cyber threats and attacks. Data Analytics refers to the process of examining and analyzing data to extract insights and meaning. Data Breach refers to the incident of unauthorized access or disclosure of sensitive or confidential data. Data Center refers to a facility that houses and manages large amounts of data and computing resources. Data Governance refers to the process of managing and overseeing an organization's data assets, including security, quality, and compliance. Data Loss Prevention (DLP) refers to the process of detecting and preventing unauthorized access or transmission of sensitive or confidential data. Data Mapping refers to the process of creating a visual representation of an organization's data assets, including sources, flows, and storage locations. Data Migration refers to the process of transferring data from one system or location to another, including conversion and validation steps. Data Mining refers to the process of automatically discovering patterns and relationships in large datasets. Data Privacy refers to the practice of protecting personal and sensitive information from unauthorized access or disclosure. Data Protection refers to the process of safeguarding data from loss, theft, corruption, or unauthorized access. Data Quality refers to the process of ensuring that data is accurate, complete, and consistent, and meets the requirements of its intended use. Data Recovery refers to the process of restoring data that has been lost, deleted, or corrupted, including backup and restore procedures. Data Retention refers to the policy of storing and preserving data for a specified period of time, including compliance and regulatory requirements. Data Science refers to the field of study that combines statistics, computer science, and domain expertise to extract insights and knowledge from data. Data Security refers to the practice of protecting data from unauthorized access, use, disclosure, disruption, modification, or destruction. Data Storage refers to the process of storing and managing data in a secure and accessible manner, including backup and recovery procedures. Data Visualization refers to the process of creating graphical representations of data to facilitate understanding and insight. Database refers to a collection of organized data that is stored and managed in a way that allows for efficient retrieval and manipulation. Database Management System (DBMS) refers to a software system that is used to manage and interact with a database, including data definition, data manipulation, and data control. Deep Learning refers to a type of machine learning that uses neural networks to analyze and interpret data. Digital Evidence refers to electronic information that is stored or transmitted in a digital format, including emails, documents, and images. Digital Forensics refers to the application of scientific principles and methods to the analysis and examination of digital evidence. Digital Signature refers to a type of electronic signature that uses cryptography to authenticate the identity of a sender or signer. Digitization refers to the process of converting analog information into a digital format, including scanning and OCR (Optical Character Recognition). Discovery refers to the process of identifying, collecting, and preserving evidence or data for use in investigations or litigation. Document Management refers to the process of organizing, storing, and retrieving documents and records, including electronic and physical formats. Document Review refers to the process of examining and analyzing documents to identify relevant or privileged information. EDD, Electronic Discovery Reference Model, refers

to a framework that outlines the steps and best practices for e-discovery, including information governance, identification, preservation, collection, processing, review, and production. E-Discovery refers to the process of identifying, collecting, and preserving electronically stored information (ESI) for use in investigations or litigation. Email Archiving refers to the process of storing and preserving email messages and attachments for long-term retention and access. Encryption refers to the process of converting plaintext into ciphertext to protect confidentiality and integrity. End User refers to the individual who uses a computer system or application to perform a specific task or function. Evidence refers to any information or object that is relevant to a case or investigation, including physical and digital evidence. Expert System refers to a computer program that uses artificial intelligence to mimic the decision making abilities of a human expert. Extraction refers to the process of recovering or extracting data from a source system or storage device. File System refers to a method of organizing and storing files on a computer system, including directories and folders. Firewall refers to a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Forensic Analysis refers to the application of scientific principles and methods to the analysis and examination of evidence. Forensic Imaging refers to the process of creating a bit for bit copy of digital evidence, including hard drives and solid state drives. FTP, File Transfer Protocol, refers to a standard network protocol used to transfer files over the internet. Gateway refers to a network device that connects two or more networks together, including local area networks (LANs) and wide area networks (WANs). Gigabyte (GB) refers to a unit of measurement for digital information, equivalent to 1 billion bytes. Hash Value refers to a digital fingerprint that is unique to a specific file or data set, used to verify authenticity and integrity. HDD, Hard Disk Drive, refers to a type of non volatile storage device that uses magnetic or optical recording to store data. HTML, HyperText Markup Language, refers to a standard programming language used to create web pages and applications. Incident Response refers to the process of responding to and managing security incidents, including identification, containment, eradication, recovery, and lessons learned. Indexing refers to the process of creating a database or index of keywords or terms to facilitate search and retrieval. Information Governance refers to the process of managing and overseeing an organization's information assets, including security, quality, and compliance. Information Security refers to the practice of protecting information from unauthorized access, use, disclosure, disruption, modification, or destruction. Intellectual Property (IP) refers to creations of the mind, including patents, trademarks, copyrights, and trade secrets. Internet Protocol (IP) refers to a standard communication protocol used to connect devices on the internet. Intrusion Detection System (IDS) refers to a network security system that monitors and detects intrusions or attacks on a network. IoT, Internet of Things, refers to the network of physical devices that are embedded with sensors, software, and connectivity to collect and exchange data. IP Address, Internet Protocol Address, refers to a unique address that is assigned to a device on a network, used to identify and communicate with the device. ISO, International Organization for Standardization, refers to a global organization that develops and publishes standards for a wide range of topics, including information security and quality management. IT, Information Technology, refers to the use of computer systems and software to manage and process information. JPEG, Joint Photographic Experts Group, refers to a standard format for compressing and storing images. Keyword Search refers to the process of searching for documents or data that contain specific keywords or terms. LAN, Local Area Network, refers to a computer network that spans a small geographic area, such as a home, office, or building. Litigation Hold refers to a process of preserving and protecting evidence or data that is relevant to a case or investigation, including electronically stored

information (ESI). Machine Learning refers to a type of artificial intelligence that involves training algorithms to learn from data and make predictions or decisions. Malware refers to software that is designed to harm or exploit a computer system, including viruses, worms, and trojans. Metadata refers to information that is associated with a document or data set, including author, date created, and file size. Microfilm refers to a type of film that is used to store and preserve documents and records in a compact and space efficient manner. Migration refers to the process of transferring data from one system or location to another, including conversion and validation steps. Network refers to a collection of computer systems and devices that are connected together to share resources and exchange data. Network Security refers to the practice of protecting computer networks from unauthorized access, use, disclosure, disruption, modification, or destruction. OCR, Optical Character Recognition, refers to the process of converting scanned or printed documents into editable text. Offsite Storage refers to the process of storing and preserving data or documents in a remote location, including cloud storage and third party facilities. Online Storage refers to the process of storing and preserving data or documents in a cloud environment, including access and sharing capabilities. Operating System (OS) refers to a software program that manages and controls the hardware and software components of a computer system. Optical Disk refers to a type of storage device that uses laser technology to read and write data, including CDs, DVDs, and Blu ray discs. Password refers to a secret word or phrase that is used to authenticate a user or grant access to a system or resource. PDF, Portable Document Format, refers to a file format that is used to store and preserve documents in a fixed layout and format. Personal Data refers to information that is related to an identified or identifiable natural person, including names, addresses, and identification numbers. Phishing refers to a type of cyber attack that involves tricking or deceiving users into revealing sensitive or confidential information. Plaintiff refers to the party that initiates a lawsuit or claim against another party, including individuals and organizations. Privileged refers to information or communications that are protected from disclosure or discovery, including attorney client privilege and work product doctrine. Processing refers to the stage of e discovery where data is reviewed and analyzed to identify relevant or privileged information. Production refers to the stage of e discovery where data is delivered to the receiving party, including format, content, and timing. Protocol refers to a set of rules or procedures that govern the exchange of data between systems or devices. Quality Control refers to the process of monitoring and controlling the quality of data or products, including testing and validation steps. RAID, Redundant Array of Independent Disks, refers to a method of storing data on multiple disks to improve performance and reliability. RAM, Random Access Memory, refers to a type of computer memory that is used to store and access data temporarily while a program is running.