**PART 1: INTRODUCTION TO ELECTRONIC EVIDENCE**

**1.1 Definition of Electronic Evidence**

Electronic evidence, also referred to as **digital evidence**, is any information stored, transmitted, extracted, or derived using digital means that holds probative value and can be used in legal proceedings. It includes data generated or communicated via electronic devices, networks, or platforms.

As per **Federal Decree-Law No. 35 of 2022** (Law of Evidence), electronic evidence encompasses any documentation produced or stored electronically, including emails, e-signatures, electronic records, and other digital correspondence. The law equates the legal weight of electronic documents with traditional paper-based records, provided they meet **authenticity and integrity** standards.

***Judicial Interpretation in the UAE:******UAE courts interpret electronic evidence broadly. This includes metadata, blockchain records, log files, chat messages, and multimedia files. Courts accept these if their origin, integrity, and reliability can be established (See Article 10 of Federal Decree-Law No. 35 of 2022).***

**1.2 Importance of Electronic Evidence**

* **Key Role in Cyber and Financial Crimes**:  
  In cases like **hacking**, **phishing**, **data theft**, **money laundering**, and **embezzlement**, electronic evidence is often the **only or primary form of evidence**.
* **Traceability and Reconstruction**:  
  Digital footprints (logs, timestamps, metadata) allow investigators to **reconstruct events**, establish timelines, and **identify perpetrators**.
* **Application Across Case Types**:  
  Electronic evidence is relevant in a wide array of investigations—**online harassment**, **IP infringement**, **terrorism**, **defamation**, and **electronic forgery**.
* **Judicial Confidence**:  
  UAE courts have **increasing confidence** in digital evidence due to statutory clarity and the technical capabilities of forensic experts.

**1.3 Types of Electronic Evidence**

Although not always categorised statutorily, electronic evidence can be grouped as:

**A. Volatile Data**

* Data that **disappears when power is turned off**.
* Examples: RAM content, active processes, temporary files.

**B. Non-Volatile Data**

* Data that remains **stored** until deliberately deleted.
* Examples: Emails, stored documents, databases, logs, social media data.

**Note**: Federal Decree-Law No. 35 of 2022 mentions evidence in forms such as:

* Electronic records
* E-signatures and seals
* Emails and messaging app content
* Blockchain entries
* Modern means of communication

**1.4 Sources of Electronic Evidence**

Digital evidence may be obtained from a wide range of **device-based** and **cloud/online** sources:

**A. Device-Based Sources**

* Computers, laptops
* Mobile phones, tablet
* IoT devices (e.g., CCTV cameras, smartwatches)

**B. Online/Cloud-Based Sources**

* Email platforms (Gmail, Outlook, etc.)
* Messaging apps (WhatsApp, Telegram, Signal)
* Social media accounts (Instagram, Facebook, X)
* Cloud storage (Google Drive, OneDrive, iCloud)

**C. Other Sources**

* **Server logs**
* **GPS/location data**
* **Exchangeable Image File Format (EXIF) data** in digital images
* **Blockchain and smart contracts**

**1.5 Legal Framework Governing Electronic Evidence in the UAE**

The UAE has enacted several key statutes governing the **admissibility, use, and authenticity** of digital evidence:

**📜 Federal Decree-Law No. 35 of 2022**

* Law of Evidence in Civil and Commercial Transactions
* Establishes rules for electronic evidence, recognition of e-signatures and e-records (Articles 53–64)
* Equates electronic and paper evidence if authenticity and integrity are proven

**📜 Federal Decree-Law No. 46 of 2021**

* On Electronic Transactions and Trust Services
* Defines legal validity of electronic documents and **qualified e-signatures**
* Recognizes **advanced digital trust services** (Digital ID, e-Seals)

**📜 Federal Decree-Law No. 34 of 2021**

* On Combatting Cybercrimes
* Criminalizes acts like hacking, e-fraud, defamation, data breaches
* Permits collection and analysis of digital evidence for prosecution

**📜 DIFC Data Protection Law No. 5 of 2020**

* Applies to entities within [Dubai International Financial Centre](https://en.wikipedia.org/wiki/Dubai_International_Financial_Centre) (DIFC) jurisdiction.
* Focuses on **data privacy**, retention, and breach response
* Supports lawful handling of personal data during investigations

**📜 UAE Penal Code and Criminal Procedure Code**

* Apply general evidentiary principles and due process
* Allow use of electronic records in criminal cases if legally obtained
* Support chain-of-custody, expert evaluation, and judicial review

***Note: While the GDPR and Budapest Convention are not binding in the UAE, their principles often influence cross-border cooperation and privacy protocols in digital evidence handling.***

**1.6 Role of Law Enforcement and Regulatory Authorities**

Several authorities are entrusted with managing and processing electronic evidence:

**🔹 Cybercrime Units (Police)**

* Conduct digital forensics
* Seize, preserve, and analyse digital devices and accounts
* Coordinate with prosecutors on admissibility

**🔹 Public Prosecutor**

* Supervises lawful seizure, extraction, and use of digital evidence
* Ensures chain of custody and relevance in trial.
* Issues warrants/orders for data access and removal of illegal content

**🔹 TDRA (Telecommunications and Digital Government Regulatory Authority)**

* Regulates trust services, qualified digital signatures
* Publishes approved electronic trust tools
* Issues licenses and enforces compliance standards

**🔹 Court-Appointed Experts**

* Digital forensic professionals may be appointed under Article 53 onwards of the Evidence Law
* Provide reports on authenticity, alteration, or source of electronic records

**1.7 Ethical Considerations in Handling Digital Evidence**

Ethical and legal compliance is crucial during collection and analysis:

**✅ Privacy Rights**

* Investigators must respect **data protection laws** and **personal rights**
* Unauthorised surveillance or data access may render evidence inadmissible

**✅ Proportionality**

* Seizure must be **specific to the case**
* Overcollection may violate privacy and lead to exclusion of evidence

**✅ Preservation of Original State**

* Evidence must not be altered, tampered, or modified
* Chain of custody must be documented in full.