**[[1]](#footnote-0)PART 4 : LEGAL ANALYSIS OF DIGITAL EVIDENCE**

**Legal Overview**

The analysis of digital evidence is a legally sensitive and technically demanding phase in cybercrime investigations. In the UAE, this process is regulated by **Federal Decree-Law No. 34 of 2021** on Combatting Cybercrimes and **Federal Decree-Law No. 35 of 2022** on the Law of Evidence, alongside procedural rules issued by enforcement agencies such as the **Ministry of Interior (MOI)**, **Dubai Police Cybercrime Unit**, and **TRA** (Telecommunications and Digital Government Regulatory Authority).

The law mandates that digital evidence — whether social media communications, IP logs, emails, or device contents — must be handled in a forensically sound manner, with strict adherence to the chain of custody, authenticity protocols, and court-admissible formats. This section provides a legal-anchored guide to the technical analysis provided in the Part 3 of this Manual.

**3.1 Social Media & Messaging Platforms**

Social media posts and private communications on platforms like WhatsApp, Facebook, Instagram, and Telegram are critical in cybercrime cases. As per **Articles 34 and 38 of Decree-Law No. 34 of 2021**, any data intercepted, retrieved, or preserved must be legally sanctioned, obtained through court order or user consent, and its integrity proven through digital logs or metadata. The data is only admissible if collected in accordance with the UAE Evidence Law (**Articles 9 to 12 of Decree-Law No. 35/2022**) and supported by a valid certificate of authenticity.

**Checklist: Legal Compliance & Investigation Steps**

* ✅ Identify accounts, usernames, or handles linked to the offence
* ✅ Secure preservation request to platform (if possible) before deletion
* ✅ Route lawful data access requests via TRA or MLAT procedures
* ✅ Maintain digital trail: timestamps, IP logs, metadata
* ✅ Record platform terms of service and retention policy for admissibility.

**3.2 Domain Name & Hosting Records**

Domains used in phishing, data theft, or illegal access cases can be legally traced and seized. **Articles 25 and 27 of Decree-Law No. 34 of 2021** permit law enforcement to obtain server logs, domain registrar details, and hosting location. Admissibility under **Decree-Law No. 35 of 2022** requires proving the link between domain use and the criminal act.

**Checklist: Legal Compliance & Investigation Steps**

* ✅ Conduct Whois look-up (ensure it's dated and recorded)
* ✅ Request DNS logs and IP-mapping from registrar under TRA guidelines
* ✅ Confirm link to accused via payment methods, email, or login patterns
* ✅ Record chain of server access logs
* ✅ Use MLA/Mutual Legal Assistance if hosted outside UAE

**3.3 Email Communication**

Emails are governed by **Articles 9–12 of the Federal Decree-Law No. 35/2022**. If extracted properly, with full headers and verified metadata, emails can serve as digital documentary evidence in court. The authenticity of sender identity, timestamps, and content integrity must be proven with hash values and server logs.

**Checklist: Legal Compliance & Investigation Steps**

* ✅ Retrieve emails using court-sanctioned access or user consent
* ✅ Ensure full headers (Received, IPs, user-agent) are extracted
* ✅ Generate hash values for content integrity
* ✅ Document email flow and source server with timestamp log
* ✅ Secure Certificate of Authenticity under Article 11

**3.4 IP Address Tracing**

Every online action leaves behind an IP trail. Under **Articles 34–36 of Decree-Law No. 34/2021**, UAE law enforcement can trace IPs, access subscriber records from ISPs, and link online acts to physical locations. Logs must be preserved with timestamp and verification from the TRA or police CERT unit.

**Checklist: Legal Compliance & Investigation Steps**

* ✅ Extract originating IP from server/email/social media log
* ✅ Submit formal data request to ISP or TRA
* ✅ Cross-match with call data, geolocation, and SIM details
* ✅ Note VPN or anonymizer use and indicate circumvention methods
* ✅ Document log authenticity, source system, and collection date

**3.5 Mobile Numbers & SIM Cards**

Mobile numbers are often used in OTP-based frauds, impersonation, and location tracking. Law enforcement can request CDRs, location data, and SIM history from telecom providers like Etisalat and Du, as per TRA and MOI directives, backed by legal orders under Decree-Law No. 34/2021.

**Checklist: Legal Compliance & Investigation Steps**

* ✅ Identify phone number or SIM via suspect device or email linkage
* ✅ Request CDRs, tower location data, SMS logs
* ✅ Preserve SIM registration, KYC, and change logs
* ✅ Maintain paper trail of requisition and logs
* ✅ Map number use against dates/times of incident

**3.6 Cryptocurrency & Virtual Assets**

Digital currency crimes are prosecuted under the UAE’s **AML-CFT Law (Cabinet Decision No. 10 of 2019)** and Decree-Law No. 34 of 2021. Transactions must be traced through the blockchain, wallets identified, and VASPs (like Binance UAE) coordinated with. The UAE has MoUs with major exchanges for data cooperation.

**Checklist: Legal Compliance & Investigation Steps**

* ✅ Identify wallet addresses, transaction hashes
* ✅ Request data from VASPs under UAE AML framework
* ✅ Match wallet ownership to suspect using KYC & IP logs
* ✅ Document freezing or monitoring orders under court direction
* ✅ Secure and preserve screenshots and JSON logs from blockchain

**3.7 File Metadata & Hash Verification**

Electronic files (images, PDFs, videos) are admissible under **Decree-Law No. 35/2022**, provided their integrity is proven. Metadata like creation date, last accessed time, geotag, and author can link suspects to files. Hashing ensures files have not been tampered with.

**Checklist: Legal Compliance & Investigation Steps**

* ✅ Extract metadata from all evidentiary files (Exif, properties)
* ✅ Generate SHA-256 or SHA-512 hash of file at first point of contact
* ✅ Record details in chain of custody log
* ✅ Validate no change in hash during storage and analysis
* ✅ Attach forensic analyst certificate for integrity

**3.8 Device Forensics (Mobile, Laptop, HDD)**

Digital devices are core evidence sources. Under **Article 36 of Decree-Law No. 34/2021**, devices must be seized legally and processed using certified tools. Legal admissibility under **Decree-Law No. 35/2022** depends on chain of custody, imaging methods, and handling logs.

**Checklist: Legal Compliance & Investigation Steps**

* ✅ Seize device with proper warrant or consent
* ✅ Log serial number, model, and condition at seizure site
* ✅ Create bit-by-bit image before accessing content
* ✅ Maintain forensic chain of custody with handler signatures
* ✅ Use certified forensic tools (EnCase, FTK, Cellebrite) and document results.

1. [↑](#footnote-ref-0)