**[[1]](#footnote-1)Part 2: Search & Seizure of Electronic Evidence (UAE)**

The investigation of cybercrimes in the UAE requires a legally compliant and carefully structured process for the search and seizure of electronic evidence. This part of the manual outlines the procedural framework, legal backing, and practical steps to ensure that all actions are in line with applicable UAE laws, including Federal Decree-Law No. 35 of 2022 (Criminal Procedure), Federal Decree-Law No. 34 of 2021 (Combating Rumors and Cybercrime), and other relevant regulations. The primary goal is to ensure that electronic evidence is not only collected effectively but also remains admissible, authentic, and untampered throughout the legal process.

1. Legal Framework for Search & Seizure :

The legal authority to conduct search and seizure operations in cybercrime cases in the United Arab Emirates (UAE) is firmly rooted in **Federal Decree-Law No. 35 of 2022** on the **Criminal Procedure Law**, and is further supported by **Federal Decree-Law No. 34 of 2021** concerning **Combating Rumors and Cybercrimes**. These laws outline the boundaries, procedures, and safeguards that investigators must adhere to when handling digital evidence.

**A. Search and Seizure under Federal Decree-Law No. 35 of 2022 (Criminal Procedure Law)**

This law forms the **backbone of procedural safeguards** for criminal investigations, including those related to cyber offenses. Search and seizure powers are governed by several key provisions, primarily aimed at **protecting individual rights while enabling effective law enforcement**.

🔹 **Judicial Oversight and Warrant Requirement (Article 45 & 46)**  
Before any search or seizure is conducted, investigators must obtain **authorization from the Public Prosecution** or a **competent judicial authority**, except in exceptional circumstances (e.g., when a suspect is caught in the act—*flagrante delicto*).

* **Article 46(1)** states that searches must be limited to the **objects or persons specified** in the judicial order. This ensures that digital searches do not become fishing expeditions.
* **Article 46(2)** is especially critical for cybercrime investigations. It mandates that if the search involves **electronic devices or digital systems**, the process must:
  + Be done in a **manner that does not affect the stored data**
  + **Preserve the integrity and authenticity** of the information
  + Be **documented accurately**, including the method used to access or retrieve data

***⚖️ This provision directly addresses the need for forensic soundness in digital evidence handling, ensuring that data remains admissible in court.[[2]](#footnote-2)***

**B. Digital Evidence Handling under Federal Decree-Law No. 34 of 2021 (Cybercrime Law)**

This law complements the Criminal Procedure Law by explicitly addressing offenses involving **digital platforms, devices, and electronic data**. It provides **investigative and prosecutorial powers** relevant to cyberspace, and is tailored to the technical realities of online crime.

🔹 **Article 48 – Access and Preservation Powers**  
This provision allows competent authorities to:

* **Access, collect, copy, and preserve digital data** or systems relevant to the investigation
* Demand **real-time access** or **log data** from service providers or custodians
* Ensure that such actions are done **without compromising the integrity or confidentiality** of data unless authorized by law

🔹 **Article 50 – Obligations of Service Providers**  
This article empowers authorities to instruct **ISPs, hosting platforms, or tech companies** within UAE jurisdiction to:

* **Provide stored or transmitted data**
* Cooperate with the investigation by **preserving metadata, timestamps, and logs**
* Comply within legally specified timelines, failing which **penalties or sanctions** may be applied

***📌 In cross-border cases, data stored outside UAE may be accessed only via international cooperation tools like Mutual Legal Assistance Treaties (MLATs) or diplomatic channels.***

**C. Exceptions: Flagrante Delicto and Urgency Situations**

In cases where a suspect is **caught in the act (flagrante delicto)** or **there is an immediate threat to data being destroyed**, Article 47 allows law enforcement to conduct a search or seizure without prior judicial approval. However, such actions must be:

* **Promptly reported to the Public Prosecution**
* **Documented in detail**, including time, place, nature of the urgency, and data retrieved
* **Followed by judicial confirmation** for the search to remain legally valid[[3]](#footnote-3)

***⚠️ Officers must be cautious when invoking this exception. Abuse or failure to justify urgent action can lead to exclusion of the evidence and legal consequences.***

**✅ Checklist: Legal Compliance Before Search & Seizure of Digital Evidence**

Here's a quick-reference compliance checklist for investigators:

☐ Obtain judicial search warrant (unless caught in the act)

☐ Ensure warrant specifies digital devices/data to be searched or seized

☐ Avoid altering data during access—use forensic tools

☐ Maintain detailed records of methods and findings

☐ Notify and document emergency actions (if warrantless search occurs)

☐ Follow Article 48 for accessing/storing/copying data

☐ Seek cooperation from service providers under Article 50

☐ Preserve logs, timestamps, and metadata during seizure

☐ Maintain full chain of custody documentation

By adhering to these legal provisions, investigators can ensure that **digital evidence is admissible**, **rights of individuals are protected**, and the **credibility of the investigation remains intact**. In UAE's rapidly evolving legal-technical landscape, knowledge of these statutes is not optional—it is essential.

**2. Pre-Seizure Preparation**

Before initiating any seizure, law enforcement must engage in detailed preparation. This includes identifying the devices, accounts, or cloud services likely to contain relevant data, and ensuring all legal authorizations are in place.

✅ **Pre-Seizure Preparation Checklist:**

* ☐ Obtain a valid search warrant from the competent judicial authority
* ☐ Identify specific electronic devices/accounts to be searched
* ☐ Verify legal jurisdiction over the location/device
* ☐ Arrange for the presence of a digital forensics expert
* ☐ Carry necessary tools for imaging and data collection
* ☐ Prepare documentation forms (inventory, chain of custody, etc.)[[4]](#footnote-4)
* ☐ Check if encrypted or password-protected devices are involved

**3. On-Site Procedure During Seizure**

At the scene, investigators must ensure proper handling of all electronic devices to prevent data alteration or loss. This includes isolating devices from networks and preserving volatile data when necessary. It is essential to maintain a **non-intrusive approach**, capturing evidence without modifying its content or metadata.

✅ **On-Site Seizure Checklist:**

* ☐ Isolate the device from all networks (disable Wi-Fi, mobile data, etc.)
* ☐ Record device status (on/off, open applications, etc.)
* ☐ Take photographs/videos of the scene and device setup
* ☐ Document the serial numbers and device details
* ☐ Avoid shutting down devices unless necessary
* ☐ Use write blockers for storage devices before imaging
* ☐ Obtain signed receipt/inventory from the suspect (if cooperative)
* ☐ Log each step and personnel involved in the seizure process

**4. Types of Digital Evidence Commonly Seized**

The nature and scope of a cybercrime determine the type of electronic evidence law enforcement must seek. Each category of digital evidence holds a unique forensic value and can play a crucial role in proving criminal intent, identifying suspects, establishing timelines, and linking the accused to the offense. During any search operation, investigators must be equipped to identify and handle these sources of evidence with the highest standards of technical and legal care.

Below is a detailed breakdown of commonly encountered digital evidence in cybercrime investigations:

1. Computers and Laptops

These are often the primary devices used for executing or planning cybercrimes. They may contain:

* Emails and communication logs relevant to phishing, scams, or impersonation
* Browser history to identify visited websites or illicit platforms
* Stored documents, spreadsheets, or databases containing hacked data, financial fraud records, or illegal content
* Download folders and software logs showing use of encryption, VPNs, or data-wiping tools

***💡 Tip: Always ensure that imaging is done using forensic tools to avoid altering the system during access.***

2. Mobile Phones and Tablets

Modern mobile devices are often more informative than computers due to their constant use and location-tracking capabilities. They may provide:

* Call logs, SMS, and messaging app data (e.g., WhatsApp, Telegram, Signal)
* GPS and location history useful for placing the suspect at the scene
* Multimedia files (photos, videos, voice notes) linked to harassment, blackmail, or illegal content sharing
* App data and internet history, including crypto transactions, anonymous browsing, or dark web access

***⚠️ Volatile data on mobiles can be lost quickly. Immediate forensic acquisition is recommended on-site if legally permissible.***

3. Removable Media

These include USB drives, external hard disks, memory cards, and SD cards. While small and portable, they often contain highly sensitive data:

* Backups of systems or stolen data
* Executable malware or keyloggers for cyber intrusions
* Logs or screenshots documenting illegal activity

***🔒 Evidence from removable media must be hashed and sealed immediately to ensure forensic integrity.***

4. Cloud Storage Accounts and Email Services

As cloud computing becomes more prevalent, many criminals store data remotely to evade local seizure. Common services include Google Drive, iCloud, Dropbox, OneDrive, etc. Evidence found may include:

* Digital documents, media files, or logs of unauthorized access
* Shared folders or collaboration tools used for criminal planning
* Email headers and metadata, which help trace sender IPs and timestamps

***📌 Accessing foreign-hosted data requires adherence to Mutual Legal Assistance Treaties (MLAT) or diplomatic channels unless stored within UAE jurisdictions.***

5. Network Devices and Logs

Routers, modems, firewalls, and network switches may carry valuable information in the form of:

* Connection logs that trace IP addresses, session times, or intrusion attempts
* MAC address mappings that identify specific devices connected to a network
* Logs showing use of anonymizing tools like VPNs or proxy servers

***🧠 Ensure to clone configurations and logs before shutdown; network evidence is volatile and time-sensitive.***

6. Internet of Things (IoT) Devices

IoT devices such as smart speakers, home security cameras, smart TVs, fitness bands, and even connected appliances can serve as silent witnesses. Potential evidence includes:

* Audio/video recordings, which can establish suspect presence or timelines
* Device access logs, pinpointing when and how a device was used
* Cloud-linked activity history, retrievable with proper legal authority

***💡 In some cases, IoT data may also help verify alibis or detect anomalies in a suspect’s movement.***

**Evidence Handling Note**

Each of these digital assets must be:

* Identified accurately, without overlooking hidden or disguised devices
* Seized using appropriate forensic tools, avoiding manual handling or powering down unless necessary
* Documented thoroughly, including make/model, serial numbers, condition, and location
* Preserved in original state, with imaging and hashing performed as early as possible
* Transported securely to the forensic lab with chain of custody maintained throughout

Failing to handle any of these categories with precision can result in inadmissibility of crucial evidence or even compromise the entire investigation. Therefore, investigative officers must stay vigilant and up-to-date with evolving forms of digital storage and connectivity.

**5. Chain of Custody & Documentation**

Maintaining the chain of custody is one of the most critical components of digital evidence handling. It involves thorough documentation of **who collected what**, **when**, **from where**, and **how it was stored or transferred**.

✅ **Chain of Custody Checklist:**

* ☐ Assign a unique ID/tag to each device
* ☐ Record time, date, location of seizure
* ☐ Note names/designations of officers collecting evidence
* ☐ List all individuals who handle the device post-seizure
* ☐ Use tamper-evident bags or containers for transportation
* ☐ Include device condition and hash value (where applicable)
* ☐ Maintain a centralized logbook or digital trail

This documentation ensures **credibility and admissibility** in court and helps defend against any challenges raised regarding the authenticity or mishandling of the evidence.

**6. Transfer to Forensics Lab**

Once seized, the evidence must be transported securely to a designated forensic analysis facility. Handling must be minimal, and each movement should be logged. Ideally, all devices should be transported by trained personnel or in secure, sealed containers.

🚚 **Transport Protocols:**

* Use sealed evidence bags labelled with case ID
* Avoid exposure to extreme temperatures or magnetic fields
* Ensure secure vehicle transport with minimal stops
* Log handover at both dispatch and receiving ends

1. Federal Decree-Law No. 35 of 2022 on the Criminal Procedure Law, Federal Decree-Law No. 34 of 2021 concerning Combating Rumors and Cybercrimes [↑](#footnote-ref-1)
2. Federal Decree-Law No. 35 of 2022 on Criminal Procedure Law, art 45 & 46 [↑](#footnote-ref-2)
3. Federal Decree-Law No. 34 of 2021 (Cybercrime Law) , art 48 & 50 [↑](#footnote-ref-3)
4. Federal Decree-Law No. 35 of 2022 on the Criminal Procedure Law , art47 [↑](#footnote-ref-4)