**Introduction**:

As cyber criminals improve their evasion techniques and investigators find it increasingly difficult to navigate the delicate yet complicated domain of safely extracting digital pieces of evidence from the suspect's devices while also maintaining data integrity and ensuring the original data is unharmed, there is a case to be made for the adoption of some sophisticated tools that complement their software counterparts. These tools are employed at all stages of the chain, including extraction, validation, and analysis, and they greatly assist law enforcement organizations all over the world. We give a few examples of such devices, grouped by use case and application area.

1. Evidence and Data Acquisition:

This is the first of many steps in an investigation. Officers proceed to gather and document all devices and things deemed essential to the investigation after obtaining a search warrant. Second, the investigative team should include experts who have expertise in recovering any vital information from the suspect's devices without contaminating them. In order to obtain a complete snapshot of the condition of the suspects' computers, they use a variety of technologies, including Write Blockers, Disk Imagers, Mobile Device extraction, and Network Forensic Devices.

With write blocking enabled, forensic imaging tools can readily gather a bit-by-bit copy of memory storage, hard disks, SSD, CPU registers, caches, etc, and all metadata associated with files. Furthermore, all network traffic is captured and collected, including IP packets, headers, and browser history. To make the task at hand easier, it is critical to plan out and quantify the scope of the gathering phase.

1. Validation:

After securely gathering all necessary data for the inquiry, it is vital to validate the data. This is usually done with custom/proprietary software, but there are some tools at our disposal to assess and methodically validate the data. To eliminate inconsistencies, the hashes of recorded forensic data are compared to the original data. This is vital for ensuring the integrity and validity of digital evidence obtained by ensuring that the data has not been altered or tampered with during the investigation process. Some famous examples of such machines are

1. **Tableau TX1 Forensic Imager:** This hardware tool features built-in hashing and validation capabilities, allowing investigators to calculate and verify hash values of acquired images**.** Its user-friendly interface and reliable performance make it a preferred tool for ensuring evidence integrity.
2. **CRU WiebeTech UltraDock v5:** This hardware tool offers hardware-based write blocking and hash calculation features. It ensures that evidence remains unaltered during acquisition and allows for subsequent validation.
3. **Cellebrite UFED Touch:** While primarily known for mobile device forensics, Cellebrite's UFED Touch can also perform evidence validation by calculating hash values of acquired data and verifying their integrity.
4. Storage and Analysis: