**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:

Following the gathering, digital evidence and data must be securely kept in dedicated devices. Transportation, handling, storage device acquisition, and cloud provisioning are all part of this process.  The transit process is meticulously planned by law enforcement and forensic specialists. This includes transportation methods, travel routes, security staff, and any equipment required to preserve evidence while in transit. A chain of custody is also maintained, detailing who handled, analysed, and studied the evidence as well as the date and time of transfer. This is important because the prosecutor will have to present it to the judge along with the rest of the evidence. Proper risk management measures should be used to guarantee that evidence is transported safely from the scene to the lab or location where it will be evaluated.  Finally, fault-tolerant, data redundancy, and strong access restrictions must be maintained to guarantee that data is not purposefully destroyed or corrupted by insiders in order to influence the decision. Data duplicators, such as the **Cellebrite UFED Ruggedized Storage**, the **Voyager M3 Evidence Drying Cabinet**, and the **CRU WiebeTech Digital Forensic Storage**, provide a safe storage medium as well as features like encryption, in-built write-blockers, and biometric access.

Following the storage phase, the digital evidence can be reproduced and distributed to multiple forensic personnel for analysis and to expedite the inquiry. Of course, the sharing will be recorded and thoroughly documented in the chain of custody document. The following steps may be included in the analysis phase:

1. **Data Extraction:** The analysis process begins once the evidence has been securely stored. The initial stage tends to be to extract data from the electronic devices and media that have been seized. Files, emails, photos, logs, and other pertinent data can all be extracted**. Eg: Cellebrite UFED**
2. **Data Recovery:** is used to recover deleted or hidden data that could not be recovered on the scene**. For example, Magnet AXIOM**
3. **Data Decryption:** Tools like **Elcomsoft Phone Breaker** can be used to retrieve encrypted data from mobile devices and cloud services if the suspect's device has advanced countermeasures like data encryption. It can also decrypt passwords and encrypted backups, among other things.
4. **Metadata Examination:** Metadata such as file timestamps and user activity logs can give useful contextual information. Hardware tools aid in the analysis of information in order to build timelines and user behaviours. For example, **Logicube Forensic ComboDock F8** may be used in combination with forensic software to examine information while avoiding accidental changes.
5. **Data Carving:** Data carving is the process of recovering lost or damaged files by extracting fragmented or unallocated data from the storage medium. For example, when integrated with forensic software, the **Tableau TD3 Forensic Duplicator** may be used for data carving activities to retrieve buried or destroyed data.
6. **Link Analysis:** Link analysis uncovers correlations and patterns by identifying and visualizing connections between various pieces of data. **Palantir Gotham**, for example, has link analysis features that enable investigators to connect and analyse data pieces to identify these links.
7. **Malware Analysis:** In the instance of desktops and laptops that have been infected with malware as a precautionary step by the accused, hardware-based write blockers such as **Tableau Forensic Bridges** can be used to collect data from infected devices for future examination in a controlled environment.

Some of the real-life instances where the use of such hardware forensic tools were instrumental in solving cybercrime cases are as follows:

1. Hardware forensic tools were used extensively during the investigation into the Russian hacking of the Democratic National Committee (DNC) in the run-up to the 2016 U.S. Presidential Election. To build replicas of hacked systems, investigators employed hardware write blocks and forensic imaging tools. This enabled them to scan the servers for malicious code, track down the attack pathways, and discover evidence tying the incursion to particular hacker groups.
2. Hardware forensic tools are employed in financial fraud investigations to assess digital information connected to insider trading and other financial crimes. Investigators can unearth evidence of unlawful trading operations, communication with accomplices, and covert financial transactions by capturing forensic photographs of suspects' computers and mobile devices utilizing hardware write blocks.
3. Hardware forensic techniques were critical in evaluating compromised industrial control systems in the context of the Stuxnet virus, a sophisticated cyberweapon meant to target Iran's nuclear program. To protect the integrity of compromised computers, investigators deployed specialized hardware write blocks and imaging tools. Experts were able to identify the worm's origins and unearth evidence pointing to state-sponsored cyber espionage and sabotage by examining the worm's code and behaviour in a controlled environment.
4. Hardware forensic methods have been utilized to recover lost or stolen digital assets in situations involving cryptocurrency-related crimes. Specialized instruments were used by investigators to examine damaged hard drives, USB devices, and storage media carrying Bitcoin wallets. They successfully recovered monies and traced transactions to identify suspects engaged in Bitcoin theft by meticulously extracting and rebuilding wallet data.

The 2 most commonly used Hardware forensic tools are 1) Hardware Imagers and 2) Write Blockers. They form the core components along with additional features.

Hardware Imagers:

They are the primary devices used by the cyber forensics team to produce a bit-by-bit copy of data from suspects' equipment such as hard drives, USB sticks, floppy discs, and so on. Aside from assisting with data collecting, they also aid in data validation and integrity checks.

Some key features of Hardware imagers are:

* **Bit-by-bit Copy**: Every sector, file, and piece of data is replicated exactly as it was on the original device, producing a flawless and accurate reproduction.
* **Write-Blocking**: Many hardware imagers support write-blocking. During the imaging process, write-blocking blocks any write (modification) operations to the source media, preserving the original evidence and preventing unintentional alterations.
* **Verification**: Hash values act as a digital fingerprint that can be used to validate the forensic image's integrity. Hence common cryptographic algorithms like MD5, SHA-1, or SHA-256 are utilized to compute hashes of the copied data.

Due to their desirable feature, they play a key role in the investigation of cybercrimes:

* **Chain of Custody:** Hardware imagers help protect the chain of custody by making an identical forensic duplicate. While the original material stays unaltered, the forensic picture becomes a legally admissible copy that can be used for analysis.
* **Analysis and Examination:** Forensic images made by hardware imagers provide a robust and secure platform for investigators to study and examine digital evidence. This enables investigators to undertake in-depth investigations without interfering with the source media.
* **Verification and Validation:** The hash values obtained throughout the imaging process allow investigators to validate the forensic image's integrity. Examiners can guarantee that the duplicate is identical to the original by comparing hash values before and after imaging.
* **Court Admissibility:**  In court processes, forensic photographs taken using hardware imagers are considered reliable evidence. They are regarded as accurate replicas of the original evidence, making them significant assets in court.

Write Blockers:

Write blockers are critical hardware devices in digital forensics that restrict any rewrite (modification) to the source digital media during evidence acquisition. These devices are intended to protect data integrity, maintain the chain of custody, and ensure that the original evidence is not tampered with as investigators gather information from other storage devices. Let's look at write blocks and their significance in maintaining data integrity throughout digital investigations.

Some key features of Write blockers are:

* **Write-Blocking Circuitry:** Write blockers feature specialized circuitry that enables data to be read from the source medium (such as a hard drive) but prevents data from being written back to it.
* **Multiple Interfaces:** Write blockers support a variety of interfaces, including SATA, USB, FireWire, and IDE, enabling them to connect to a wide range of storage devices.
* **Read-Only Mode:** Write blockers function only in read-only mode, preventing any unintentional or purposeful modifications to the source material.

Their contribution to the forensic inquiry can be characterized as follows, given that their primary duty is to maintain the integrity of the obtained data:

1. **Preservation of Original Data:** The basic purpose of write blockers is to ensure that the original data on the source media is not altered. These devices prevent any unintentional or intentional alterations by stopping write operations.
2. **Maintaining Chain of Custody:**  Write blocks are critical in keeping the chain of custody, which is an important part of processing evidence. Write blockers protect the integrity and validity of the evidence by preventing any alterations to the original media.
3. **Admissible Evidence:** Data obtained with write blockers is regarded as forensically sound and legally admissible in court. The evidence is gathered without any likelihood of contamination or tampering, which increases its trustworthiness.
4. **Safe and uninterrupted:** While write-blocking is engaged, investigators can safely connect digital media to various forensic equipment and software for examination. This ensures that no changes are made throughout the assessment.