Access Control Devices:

**For investigators** to secure, safeguard, and manage access to digital evidence and hardware components, access control technologies are essential in hardware forensic investigation. In hardware forensic investigation, access control tools are used in the following five significant ways.

Evidence Integrity and Chain of Custody: By preventing illegal access to physical devices, access control systems assist safeguard the integrity of digital evidence. They make sure that only authorized people can handle the evidence, minimizing the possibility of tampering and upholding a transparent chain of custody throughout the course of the inquiry.

Data security: Hardware forensic investigations frequently involve private information and data. Through the use of access control technologies, this data is shielded from illegal access, allowing only trained investigators with the required access to view and evaluate the evidence.

Authorization and Authentication: With the use of access control technologies, investigators can put strong authentication measures in place, like username/password combinations, biometrics, or multi-factor authentication. This makes sure that only persons with permission can access hardware components and the data they hold.

Access control technologies frequently offer logging and auditing features that enable investigators to keep track of and document access attempts and hardware actions. These logs can be incredibly helpful for keeping track of suspicious activity, spotting potential threats, and keeping a record of all the steps performed during the investigation.

Remote Access Management: In some circumstances, remote access to equipment situated in various geographic areas may be necessary for hardware forensic investigations. Investigators can undertake analysis and data collection without physically gaining access to the hardware with the help of access control solutions that provide safe remote access. This is especially helpful when there is a need for instant access yet travel may not be possible or timely.

**For hacker**

Unauthorized Access: A shady investigator could utilize access control techniques to get access without authorization to confidential information or hardware components. This can entail evading security measures, breaking into secured networks, or utilizing credentials without the necessary authority.

Evidence tampering: An unscrupulous investigator may utilize access control mechanisms to tamper with or manipulate the evidence to support a specific narrative or outcome, rather than maintaining the integrity of digital evidence. This can entail changing timestamps, removing or including files, or changing data.

Planting False Evidence: Through the unauthorized use of access control mechanisms, an investigator may be able to place false evidence on hardware devices, swaying the course of the inquiry or implicating innocent people.

Data Theft: While inspecting hardware equipment, an unethical investigator may use access control techniques to steal confidential or private data. This might be done for selfish reasons or to harm people or organizations' reputations.

Unauthorized Remote Access: From a distance, access control tools that enable remote access may be used to gain access to systems or hardware components. This could be done to avoid being discovered during the investigation or to carry out malevolent acts covertly.

Hacking and Exploitation: In some circumstances, access control tools may be used to exploit security flaws in hardware devices, get beyond security precautions, or carry out hostile hacking operations unrelated to the forensic inquiry.

Examples:

**Resource:**

[Investigative Uses of Technology: Devices, Tools, and Techniques (ojp.gov)](https://www.ojp.gov/pdffiles1/nij/213030.pdf)