Here’s the **comprehensive, sentence-by-sentence breakdown** of your **Chain of Custody** document, rewritten into professional **CompTIA A+ 220-1102 study notes**. Every important point has been retained, expanded, and explained with exam context. The formatting is professional and optimized for Word.

**Chain of Custody – Study Notes**

**1. Topic Overview**

The chain of custody refers to the record of how evidence is collected, handled, stored, and preserved from the moment of attainment to its final presentation in court. This ensures the evidence remains authentic, untampered, and legally acceptable. Although the concept existed long before digital forensics, it fully applies to computers and electronic devices today.

**2. Definition and Importance**

* Chain of custody documents every action taken on evidence: collection, transfer, storage, analysis, and destruction.
* Its purpose is to prove integrity—ensuring evidence presented in court is the same as originally collected.
* Without proper chain of custody, evidence can be ruled inadmissible due to risk of tampering.

**3. Traditional Example (Physical Evidence)**

* In law enforcement, a weapon (e.g., gun) is collected using gloves or tools to prevent contamination.
* The weapon is placed in an evidence bag, labeled, and signed with collection details (date, time, location, officer’s name).
* This marks the start of the chain of custody for that item.

**4. Digital Forensics Application**

* The same principle applies when collecting computers, laptops, hard drives, or mobile devices.
* Example: If a suspect’s laptop is seized, it must be bagged, tagged, and documented.
  + That laptop goes to the police station where its brought over to forensic technicians for analysis.
  + When transferred to a forensic lab, Lab technicians must **sign for evidence bag** in order to maintain that chain of custody over the laptop.

**5. Derived Evidence (Disk Images)**

* Forensic best practice: never analyze the original evidence directly.
* Instead, create a **bit-by-bit disk image** (exact replica).
  + That disk image becomes a new form of evidence and it need its own chain of custody.
* That image becomes its own piece of evidence and requires its own chain of custody.

**6. Evidence Protection (Specialized Bags)**

* Sensitive digital evidence (hard drives, circuit boards, SSDs) must be placed in **anti-static evidence bags** to prevent electrostatic discharge (ESD) damage.
* Devices with wireless capability (smartphones, tablets) are stored in **Faraday bags**, is used to shield devices from outside signals to which block external radio signals to prevent data from being altered, deleted, or added to a device.
  + For example, if you collected a suspect’s smartphone, you need to put it inside a Faraday bag to prevent somebody from being able to send a remote wipe command to that device and destroying al the data it contains.
* Purpose: prevent remote commands like a **remote wipe** that could destroy data.

**7. Dual-Bagging Smartphones**

* Common practice: place the device in a standard evidence bag, then place that inside a Faraday bag for layered protection.
* Ensures both physical integrity and digital signal blocking.

**8. Evidence Lifecycle**

* Evidence may need to be preserved for **months or years** during investigations, audits, or trials.
* To help with this process you should always create a good method of identifying the different pieces of evidence collected.
  + For each evidence collected it needs to be identified, bagged, sealed, labeled, and stored.
* The sheer size and scope of evidence can also be a lot to deal with.
  + Evidence must be properly stored and protected for its entire lifecycle.
* Proper storage includes:
  + Controlled environment (humidity and temperature).
  + Physical security (locks, guards, surveillance).
* Ensure evidence is properly stored with the right humidity and temperature controls in place and that way, the evidence can remain secure and safe.
* Large cases (e.g., Enron, WorldCom scandals) may involve **thousands of files, drives, and boxes of evidence**, all requiring cataloging.

**9. Risks of Improper Storage**

* Magnetic media like backup tapes degrade if not stored properly.
* Example: VHS tapes from the 1980s became unreadable after decades due to poor storage conditions.
* In legal contexts, improper storage could destroy critical case evidence.

**10. Cataloging Evidence**

* Evidence must be labeled and cataloged for easy retrieval.
* **Metadata** (data about data) is used to track items.
  + **Using a code or numbering system with difference evidence to collect.**
  + Example labeling convention: “ChainOfCustody\_2021-11-26\_19:45” — includes case, date, and time.
  + Then we can use that reference to find a short description of the contents of that evidence.
* Proper cataloging ensures evidence can be located quickly during trials.

**11. Legal Hold**

* A **legal hold** preserves data when litigation (lawsuit) is reasonably anticipated.
* Once placed, data cannot be deleted or destroyed.
  + Preserve the data.
* IT systems, servers, or computers may be seized and held for the duration of a case.
  + Until the legal hold is removed you can’t get those systems back.

**12. Business Impact of Legal Holds**

* If a web hosting company’s shared server contains illegal files, law enforcement may seize the entire server.
* This can disrupt services for months or years.
* Businesses should plan for such scenarios using or have spare hardware and good backups of all system:
  + Spare hardware.
  + Robust backup systems.
  + Business continuity planning to minimize downtime.

**Real-Life Implementation Example**

Scenario: Law enforcement seizes a suspect’s smartphone during an investigation. The officer places it in a standard evidence bag, then a Faraday bag, logs the details, and signs the chain of custody record. At the forensic lab, technicians create a disk image of the phone’s storage, which is logged as a new piece of evidence with its own chain. Throughout trial preparation, all handling is logged. Meanwhile, the original phone remains secured in a temperature- and humidity-controlled evidence locker with restricted access.