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.

**Exam Inclusion Notification**

Yes, **Chain of Custody** is directly included in the **CompTIA A+ 220-1102 exam objectives (Domain 4: Operational Procedures)**. Candidates are expected to:

* Explain chain of custody and why evidence integrity must be preserved.
* Identify proper handling, storage, and cataloging methods for digital evidence.
* Recognize the importance of legal holds, evidence bags, Faraday bags, and business continuity planning.

Would you like me to now create a **10-question CompTIA A+ style quiz** on *Chain of Custody* to reinforce this content?

**CompTIA A+ 220-1102 – Chain of Custody Quiz (7 Questions)**

**1.** While seizing a suspect’s smartphone that may receive a remote wipe command, what is the best immediate handling procedure?

A. Label it, photograph it, and leave it powered on in an evidence locker

B. Power it off and hand it directly to a manager without documentation

C. Place it in a standard evidence bag, then into a Faraday bag, and log the seizure

D. Enable airplane mode and keep analyzing it at the scene

**2.** Which action most directly maintains a defensible chain of custody during evidence transfers?

A. Boot the system to view logs for context before packaging

B. Record each handoff with date/time, names, signatures, and purpose

C. Copy a few “important” files from the original drive to speed analysis

D. Email the image file to yourself for safekeeping

**3.** A forensic examiner must acquire a compromised server’s storage. Which approach is correct?

A. Drag-and-drop the user folders to an external disk

B. Clone only the \Users (or /home) directory to save time

C. Mount the original disk read/write to check its contents first

D. Create a bit-by-bit image and treat the image as new evidence with its own chain

**4.** Your team must store hundreds of backup tapes as evidence for years. Which storage plan best minimizes risk?

A. Maintain temperature/humidity controls, lock the storage, and fully catalog items

B. Place tapes on open shelves with basic labels so they’re easy to grab

C. Keep each tape powered and connected to avoid magnetic decay

D. Stack boxes near HVAC vents for airflow and convenience

**5.** Legal counsel anticipates litigation related to customer data. Which statement best describes a legal hold’s effect?

A. Normal deletion schedules continue so storage isn’t impacted

B. Relevant data should be destroyed quickly to avoid exposure

C. Normal deletion is suspended and relevant data is preserved; systems may be seized

D. Legal holds apply only to public-facing records, not internal data

**6.** You’re cataloging multiple devices and media collected from a site. Which is the best cataloging practice?

A. Use a coded naming scheme with date/time (e.g., CaseID\_YYYY-MM-DD\_HHMM) plus a short description

B. Assign generic names like “evidence1,” “evidence2,” and keep details in your head

C. Avoid paperwork by storing one photo of the pile of devices

D. Keep the evidence index in your personal email for easy access

**7.** Police seize your company’s shared server as evidence under a legal hold. What business continuity step is most appropriate?

A. Take no action—servers are typically returned within 48 hours

B. Use spare hardware and tested backups to migrate client workloads

C. Purge client data to lower the risk of further seizure

D. Refuse to cooperate and keep the production server online

**Answer Key & Explanations**

**1. Correct: C — Place it in a standard evidence bag, then into a Faraday bag, and log the seizure.**

Why correct: A Faraday bag blocks radio signals to prevent remote wipes or tampering; the standard evidence bag preserves physical integrity, and immediate logging starts the chain of custody.

Why others are wrong:

A. Leaves risk of remote access/tamper; no signal isolation.

B. No documentation; breaks chain of custody.

D. Airplane mode can alter device state; continuing analysis at the scene risks contamination.

**2. Correct: B — Record each handoff with date/time, names, signatures, and purpose.**

Why correct: Chain of custody requires a complete, signed record of every transfer to preserve evidence integrity.

Why others are wrong:

A. Booting changes state and can alter evidence.

C. Selective copying alters/omits data; not forensically sound.

D. Emailing evidence is insecure and breaks evidentiary controls.

**3. Correct: D — Create a bit-by-bit image and treat the image as new evidence with its own chain.**

Why correct: A sector-for-sector image captures all data (including slack/unallocated) and the image itself must be logged as evidence.

Why others are wrong:

A/B. Partial, file-level copies are incomplete and non-forensic.

C. Mounting read/write risks altering timestamps/data.

**4. Correct: A — Maintain temperature/humidity controls, lock the storage, and fully catalog items.**

Why correct: Long-term integrity of magnetic media requires environmental controls, physical security, and detailed cataloging.

Why others are wrong:

B. Open shelves lack environmental/physical controls.

C. Tapes aren’t “powered”; this is nonsensical and unsafe.

D. HVAC vents can cause fluctuating conditions and physical risks.

**5. Correct: C — Normal deletion is suspended and relevant data is preserved; systems may be seized.**

Why correct: A legal hold pauses routine purges and preserves potentially relevant data; authorities may seize systems for the case’s duration.

Why others are wrong:

A. Directly contradicts hold requirements.

B. Destruction under hold risks sanctions/spoliation.

D. Holds apply to any potentially relevant data, not just public.

**6. Correct: A — Use a coded naming scheme with date/time plus a short description.**

Why correct: Consistent identifiers and metadata enable fast retrieval and defensible tracking in court.

Why others are wrong:

B. Generic names and memory aren’t defensible or scalable.

C. A single photo isn’t a catalog; lacks item-level traceability.

D. Personal email is insecure and not an approved repository.

**7. Correct: B — Use spare hardware and tested backups to migrate client workloads.**

Why correct: Business continuity planning anticipates seizures; alternate hardware and backups allow service restoration without the seized server.

Why others are wrong:

A. Timing is unpredictable; inaction risks prolonged outage.

C. Deleting client data is destructive and potentially unlawful.

D. Noncompliance with a legal hold can trigger severe penalties.

If you want, I can generate a **follow-up mini-lab** (checklist + forms) that includes a sample **chain-of-custody log**, **evidence label template**, and a **cataloging convention** you can practice with for the exam and real-world use.