

Chain of custody

(NIST 800-72)

- Document
 - Who collected it? (i.e., devices, media, associated peripherals, etc.)
 - How and where? (i.e., how was the evidence collected and where it was located)
 - Who took possession of it? (i.e., individual in charge of seizing evidence)
 - How was it stored and protected in storage? (i.e., evidence-custodian procedures)
 - Who took it out of storage and why? (i.e., on-going documentation of individual's

name and purpose for checking-out evidence)

Collection & Packaging & Transportation

- Collection
 - Leave on or off depending on current state
 - Put into sealed bag/container, label as required
 - Add powerbank / power source if powered on
 - Search for associated devices
 - Collect cables and manuals
- Packaging Procedure
 - Properly document, label, and inventory evidence before packaging.
 - Pack avoiding damage
- Transportation Procedure
 - Avoid magnetic sources (e.g., radio transmitters, speaker magnets).
 - Avoid conditions of excessive heat, cold, or humidity while in transit.
 - Avoid shock and excessive vibrations