Here is the **comprehensive, sentence-by-sentence breakdown** of your **Data Collection Procedures Notes** document. I’ve expanded each point into structured CompTIA A+ 220-1102 style study notes. The formatting is professional and aligned for Word use with no unnecessary spacing.

**Data Collection Procedures – Study Notes**

**1. Importance of Evidence Collection in Incident Response**

* During an incident response, evidence must be collected to analyze the cyberattack.
* Example: If a server is infected with malware, you must clear the infection and restore operations. However, doing so without evidence collection erases proof of the attack, preventing identification of the attacker.
* Proper data collection ensures both **business continuity** (system restored) and **forensic integrity** (evidence preserved).

**2. Use of Digital Forensic Collection Techniques**

* To avoid losing evidence, forensic imaging tools are used to make an **exact copy** of the affected system’s data.
* This copy is preserved for later analysis while allowing the server to return to production.
* Preserved forensic images may also be required for **law enforcement investigations** or **criminal prosecution**.

**3. Core Evidence Collection Activities**

* **Capture and hash system images**: Tools like *FTK Imager* create an exact copy of a hard drive. Hashing ensures the image remains unchanged during analysis.
* **Forensic analysis**: Specialized tools such as *FTK* (Forensic Toolkit) or *EnCase* analyze captured images.
* **Screenshots**: Capture the state of the machine at the time of seizure (e.g., what was on the desktop, active sessions, or alerts).
* **Network traffic logs and packet captures**: Review to trace attacker movement across the network.
* **CCTV footage**: If physical access is suspected, collect video recordings for timeline reconstruction.

**4. Order of Volatility Considerations**

* Evidence must be collected in order of volatility (most likely to change → least likely):
  1. Processor cache and registers.
  2. System memory (RAM).
  3. Swap files/pagefiles.
  4. Persistent storage (hard drives, SSDs).
* Since attackers can modify evidence while present on a machine, collection should occur as quickly as possible.

**5. Witness and Administrator Statements**

* Collect observations from individuals who noticed suspicious activity.
* Example: An end user reporting, *“My mouse started jumping all over the screen.”* Such details provide context for the incident and help validate technical findings.

**6. Review of Licensing and Documentation**

* Verify system licenses to ensure compliance with vendor agreements.
* Review documentation to confirm systems are configured and operating as designed.
* Misconfigurations or licensing gaps may contribute to security weaknesses.

**7. Tracking Man-Hours and Expenses**

* Record time and financial resources spent on the incident response process.
* Cost evaluation is critical since data breaches in large organizations often result in **multi-million-dollar losses**.
* Costs include both:
  + **Direct response costs** (investigation, containment, recovery).
  + **Indirect losses** (value of stolen or destroyed data).

**8. Forensic Imaging Demonstration**

* Future training may demonstrate the actual process of creating a forensic disk image.
* While the CompTIA Security+ or A+ exams will not require performing disk imaging, candidates should understand the concept and purpose of forensic imaging.
* Exposure to tools like *Forensic Toolkit* and *EnCase* gives insight into professional forensic workflows.

**Real-Life Implementation Example**

Scenario: An enterprise experiences a ransomware infection on its main database server. The IT incident response team immediately:

1. Creates a forensic image of the server’s drives using *FTK Imager*, hashing the image to confirm integrity.
2. Collects RAM dumps to preserve volatile data.
3. Captures screenshots of the ransomware note displayed on-screen.
4. Correlates suspicious logins in **SIEM logs** with network traffic captures.
5. Interviews the database administrator, who reports seeing unusual high CPU usage before the attack.
6. Compiles a detailed cost report showing $2 million in losses, including downtime and data theft.

This approach preserves critical evidence for prosecution while also restoring business operations.

**Exam Inclusion Notification**

Yes, **Data Collection Procedures** are included in the **CompTIA A+ 220-1102 exam objectives (Domain 4: Operational Procedures)**. Candidates must:

* Understand how to properly collect and preserve evidence.
* Apply order of volatility principles.
* Recognize forensic tools and imaging processes.
* Document observations, costs, and witness statements.
* Appreciate the importance of legal considerations in evidence handling.