Here’s the **comprehensive, sentence-by-sentence study breakdown** of your **Order of Volatility Notes** document. I’ve carefully retained all details, expanded them into professional notes, and aligned them with CompTIA A+ 220-1102 exam relevance. The formatting is professional and clean for Word.

**Order of Volatility – Study Notes**

**1. Topic Overview**

The **order of volatility** refers to the sequence in which digital evidence should be collected during an investigation. The principle is that evidence most likely to be lost or altered should be acquired first. This concept is critical in digital forensics and directly tied to **incident response**.

**2. Data Acquisition Definition**

* Data acquisition involves the **method and tools** used to create forensically sound copies of data from a source device, such as system memory or hard drives.
* Forensics emphasizes that data copies must preserve integrity and be admissible in legal proceedings.

**3. Legal Authority Considerations**

* Before acquisition, investigators must confirm **legal right to search or seize a device**.
* Company-owned devices typically permit evidence collection.
* **BYOD (Bring Your Own Device)** policies complicate matters: if the device is employee-owned, the company may lack legal authority to access it without explicit permission.
* Evidence collected without authorization is likely inadmissible in court.

**4. Physical vs Digital Evidence Challenges**

* Digital crime scenes add complexity beyond physical evidence.
* Example: A powered-on computer contains volatile data that disappears if shut down. Investigators must decide whether to collect evidence live or after shutdown. Each choice carries risks and benefits depending on data type.

**5. Why Order of Volatility Matters**

* Some evidence exists only temporarily and disappears if not collected immediately.
* Collect the most volatile evidence first, then progress toward more stable evidence sources.

**6. RFC 3227 Guidelines – Evidence Collection Order**

The formal order of volatility, based on **RFC 3227: Guidelines for Evidence Collection and Archiving**, is:

1. **Registers and cache** – Extremely volatile; overwritten rapidly, collect first.
2. **Routing tables, ARP caches, process tables, kernel statistics, and memory (RAM).**
3. **Temporary file systems** – Includes Linux swap partitions or Windows pagefile.
4. **Disks** – Hard drives, SSDs, onboard persistent storage.
5. **Remote logging and monitoring data** – Stored offsite in SIEM/log servers.
6. **Physical configurations and network topologies** – Rarely change but provide investigative context.
7. **Archival media** – Backup tapes, CDs, DVDs, printouts, external drives (least volatile).

**7. Evidence Type Breakdown**

* **Registers and cache**: Available only while powered on; lost instantly when off.
* **RAM (routing tables, ARP, processes, kernel stats):** Volatile; lost when powered down. Must be live-collected.
* **Temporary file systems:** Often overwritten or deleted during operation; may contain swapped-out memory data.
* **Persistent storage (disks):** Allow for frequent updates and changes to their contents but are not nearly as rapid as processor registers and cache, RAM and temporary file systems.
  + **Can be easily collected when the device is powered down.**
    - As long as is not encrypted.
  + If encrypted the device should be collected while it is actively mounted if the analyst does not have a copy of the encryption key.
* **Remote logs:** Less volatile, stored offsite, but still needed for context.
  + **This data is not on the same system that’s subject to the investigation.**
  + Can be in your SIEM and its offsite where you can collect it, even though it’s not going to be affected by the system.
* **Network topologies/configs:** Rarely change, useful for reconstructing environment.
* **Archival media:** Safest/most stable, last priority for collection.
  + **Offline**
  + **Include backup tapes, CD’s, DVD’s, printouts, and external hard drives.**
  + **Leaast likely to be modified during the time of our collection.**

**8. Windows Registry Special Considerations**

* Not all of the Windows Registry is stored on disk. Some parts exist **only in RAM** during operation.
* Example: **HKLM\Hardware Hive** resides only in memory and records connected hardware (drives, USBs).
* Must collect via memory dump, otherwise lost at shutdown.
* Useful for detecting malware infections from USBs or data exfiltration attempts.

**9. Best Practice for Registry Analysis**

* Recommended to analyze registry both:
  1. From a memory dump (to capture volatile hives).
  2. From the hard drive (to capture persistent hives).
* Ensures no critical data is missed.

**10. Real-Life Example**

Scenario: Investigators suspect data exfiltration via USB drive. During live collection, they dump the system’s memory, extract the **Hardware Hive**, and confirm a specific USB thumb drive was connected just before the incident. Without following order of volatility and performing a memory dump, this evidence would have been lost upon shutdown.

Similarly if somebody used a thumb drive to conduct a data exfiltration from our server you could also find evidence of that in the hardware hive too.

**Exam Inclusion Notification**

Yes, the **Order of Volatility** is included in **CompTIA A+ 220-1102 (Domain 4: Operational Procedures)**. Candidates must:

* Understand the importance of evidence collection sequencing.
* Recognize what types of evidence are most volatile (registers, cache, RAM).
* Differentiate between volatile and non-volatile data sources.
* Apply RFC 3227 guidelines in a forensic or incident response scenario.