My First-Hour Priorities

What I Capture:

- Log files and volatile memory: These are time sensitive and can be lost quickly they may contain evidence of active processes or attacker presence.
- System time and clock drift: Essential for constructing an accurate timeline during the investigation.
- Running processes and open network connections: Helps identify potential malware, suspicious activity, or lateral movement.
- External device connections or mounted volumes: May indicate data exfiltration or point of compromise.

What I Avoid:

- Rebooting or patching systems: This could destroy volatile data or change the system state.
- Making forensic changes before imaging: Preserves evidence integrity and legal admissibility.

Incident & Evidence Note (Final)

On September 10, 2025, at 1:45 PM ET, I was alerted to abnormal outbound traffic originating from host `HR-PC-004`. Upon arrival, I captured a memory image using FTK Imager and verified with SHA-256 hash. I documented all running processes, network connections, and pulled 48 hours of relevant system and application logs. No physical signs of tampering were found. All evidence was transferred to secure storage at `/evidence/case-019/`, with hashes recorded and chain-of-custody documentation signed and timestamped.

Integrity & Privacy Controls

All evidence files were hashed using SHA-256 and stored on an encrypted external drive within a restricted access evidence vault. Personally identifiable information was redacted from final notes and shared documents. Redacted documents are separately hashed and version-controlled. Chain-of-custody is maintained through digital logs and physical sign off sheets. No original files were modified during the investigation.

Evidence Links

- In-Class Note (PDF)
- Reflection (PDF)

Reflection

If I could revisit this investigation, I would prioritize capturing volatile memory earlier and automate part of the process using a live response toolkit. I underestimated the time it takes to validate external device access via registry entries. In future scenarios, I’d document more in real time instead of backfilling notes after data capture. Pre configured forensic scripts would have saved time under pressure.