CYBR2100 Reflection – Week 4

What I Learned

This week I learned how the NIST Incident Response Lifecycle provides a structured process for handling cybersecurity incidents. The cycle includes preparation, detection and analysis, containment, eradication, recovery, and lessons learned. What stood out to me most was the focus on scope and authorization, which ensures that responders only collect the minimum necessary evidence. Collecting too much data can expose unrelated user information, slow down analysis, and even create new risks, while narrow and scoped collection preserves privacy and still provides enough information to defend the system. The *Ethics in Technology* eBook highlighted that harm prevention is a key part of ethical responsibility, and the minimum-necessary principle fits directly into that theme. I also learned that integrity and provenance are just as important as speed; evidence must be defensible and usable if it ever ends up in court or a compliance investigation. The NIST Computer Security Resource Center emphasizes that clear authorization and careful documentation keep incident handling professional and accountable.

How I'll Apply It

If a small business I worked for experienced a ransomware breach, my first-hour priorities would focus on minimal and scoped evidence. I would capture one copy of the suspicious email or file that likely delivered the ransomware, since that shows how the attacker got in. I would also capture a short log extract from the authentication system around the time the breach was detected, limited to the affected users, to confirm unauthorized access attempts. What I would avoid is taking a full image of every employee's workstation, because that would sweep in far too much personal or irrelevant data. Staying within scope and consent protects privacy and still gives investigators enough to start containment and recovery.

Muddiest Point

One thing I am still unclear on is how authorization should work during a very fast-moving incident like a zero-day attack. If evidence needs to be collected immediately to preserve volatile data, waiting for formal approvals could slow the response. But acting without authorization could cross ethical and legal boundaries. My question is: what is the right balance between speed and authorization when time is critical and every minute counts?

Portfolio Note

- I will add my Incident & Evidence Note to show how I can document actions clearly while staying within scope and authorization.
- I will include a short rationale on why I only collected the minimum necessary evidence, to demonstrate ethical boundaries and privacy protection.
- This matters because strong evidence practices protect users' rights while still giving investigators what they need to contain and recover from an incident.

AI Use Note

I used ChatGPT as a structured writing partner. I provided my lecture notes and the assignment requirements, then asked the tool to guide me through the reflection step by step with targeted questions. This let me organize my thoughts more effectively while keeping the final writing in my own words. I see AI as a professional support tool — I controlled the content and direction, but used ChatGPT to make the process faster, clearer, and more organize