**What I learned:** This week I learned about the NIST incident response lifecycle, which provides a structured approach for handling cybersecurity incidents from start to finish. It consists of distinct phases including Preparation, Detection and Analysis, Containment (with Eradication and Recovery), and Post-Incident Activity. Each phase has a specific role: for example, Preparation involves setting up policies and tools in advance, while Post-Incident involves learning lessons to improve future response. A key takeaway is the importance of collecting and using only the **minimum necessary** information during an incident. By focusing on just the data needed to investigate and resolve the problem, we protect privacy and reduce potential harm. This idea ties into the course eBook’s harm-prevention theme: even in a crisis, we should avoid causing additional harm (like unnecessary exposure of sensitive data) by being selective and ethical in our actions. I also realized that following established policy and procedures (such as maintaining a strict chain of custody for evidence) is crucial to ensure evidence integrity and trust in the incident handling process. Overall, the NIST framework taught me how to respond systematically while keeping ethics and harm prevention in mind.

**How I’ll apply it:** I can apply these principles in a realistic scenario at Hocking College’s campus IT department. For instance, imagine a faculty computer on campus shows signs of a malware infection after the professor opened a suspicious email. In the first hour of responding to this incident, I would capture two important items:

**(1)** a copy of the malicious email (with headers and attachments) as evidence, and

**(2)** a forensic image or memory dump of the compromised computer. Both items are within the scope of the investigation and allowed by campus policy, helping to preserve crucial evidence without overreaching. At the same time, I would avoid accessing or copying unrelated personal files or emails on that computer that aren’t relevant to the incident. That third item is outside our immediate scope and collecting it would violate the user’s privacy without consent. By focusing only on the necessary evidence (the phishing email and system data) and avoiding extraneous information, I respect privacy and keep the response targeted. This approach ensures we gather what’s needed to contain and understand the incident while upholding ethical standards and college policies.

**Muddiest point:** One area I’m still a bit unclear about is how to properly maintain the chain of custody for digital evidence in a fast-moving incident. I know we need to document who handles evidence and when, but in practice, if multiple team members are involved quickly, it seems challenging to keep the chain-of-custody record up to date. For example, if I image a compromised drive and then hand that image to another analyst for investigation, how do we ensure the transfer is documented thoroughly and that the evidence remains admissible? My question is:

**What are the best practices to ensure an unbroken chain of custody for digital evidence when several responders must handle it during an urgent incident?**

**Portfolio Note:**  
- I will include a concise incident response checklist or summary of the NIST lifecycle in my portfolio to demonstrate my understanding of structured incident handling and ethical best practices. (This artifact matters because it shows I can internalize industry standards and communicate them clearly.)  
- I also plan to publish the fictional Hocking College incident scenario and my first-hour response plan as a case study. This will highlight my ability to apply theoretical knowledge to a real-world situation while respecting privacy and policy, which is a valuable skill for cybersecurity roles.