This week I learned about the four phases of the NIST incident lifecycle; 1. Preparation, 2. Detection and Analysis, 3. Containment, eradication and recovery, and 4. Post-incident Activity. Each phase provides support to each other as it creates a reliable and structured response when it comes to reacting to a cybercrime. The term ‘minimum necessary’ is critical when it comes down to collecting evidence during an investigation as we are dealing with sensitive information and people’s private information data. Overcollection of information usually leads to the risk of leaking the personally identifiable information or credentials, possibly halting or damaging any ongoing investigation. It also can lead to a damaged reputation if people were to find out that their personal information was damaged. Being ethical in the field of technology means not only safeguarding their systems, but their personal information. Maintaining a balance along with some restraint means that incident responders can build trust and reduce any negative consequences that weren’t intentional.

In not only a campus environment but also a business environment, if there were ever reports of a phishing email being received there would be two steps I would take. The first step would be to safely obtain the suspicious email and obtain the log entries which show any authentication attempts about the same time of delivery. I would also make sure to ONLY capture the suspicious email and avoid grabbing ALL the emails that were in the same inbox as the phishing email as that would exceed the scope or the purpose of the investigation. The goal is to be focused on the targeted evidence while respecting privacy and being compliant.

Overall, the thought that was looming in my mind is how much is needed when it comes down to documenting information. In the redaction process, how much information can be removed before the provided evidence loses all value during the investigation? It’s something that I thought of especially when it’s a small company that has limited resources and they want to provide the best service possible to its employees.

In the portfolio, I will be publishing:

- My question in the muddiest point section. While Hocking College and other colleges or large companies are able to provide, the smaller companies and businesses may not be able to.
- I will also be including what I personally would capture and avoid as a priority. It shows my point of view in how I would approach an investigation, something I feel would be serious to admit as we deal with privacy in the field of Cybersecurity.