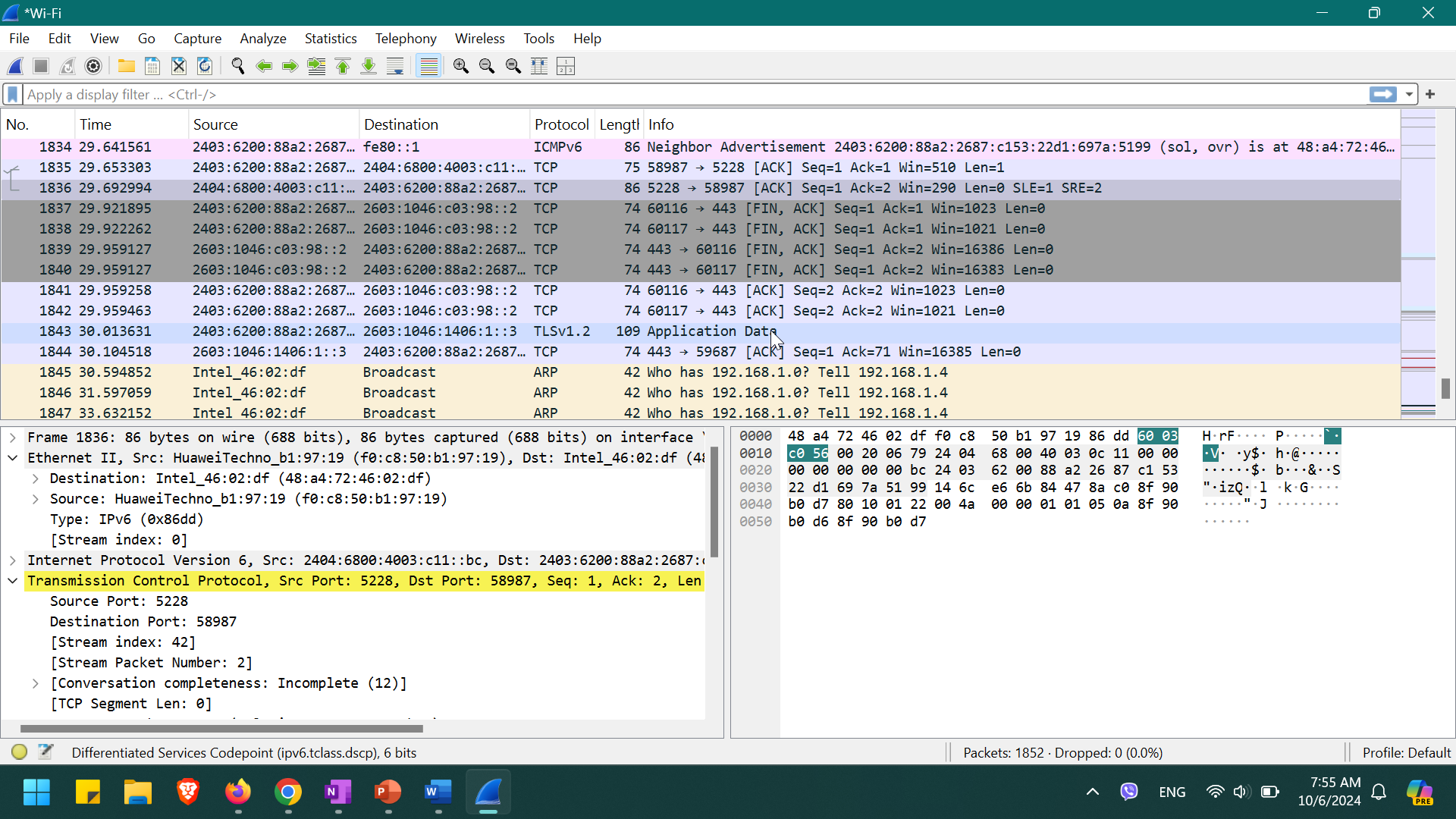
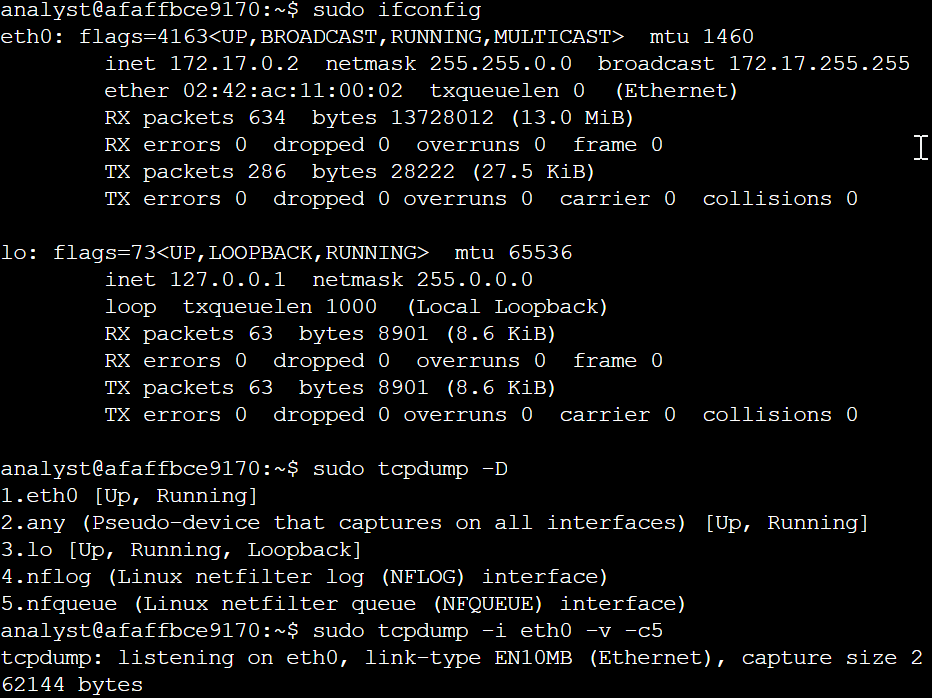
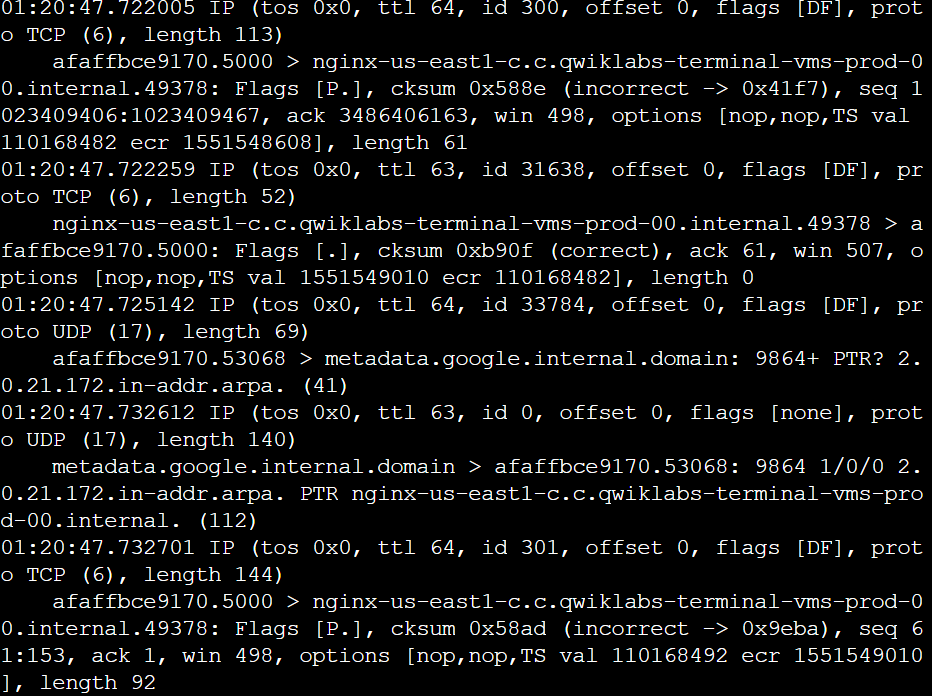
**Incident handler's journal**

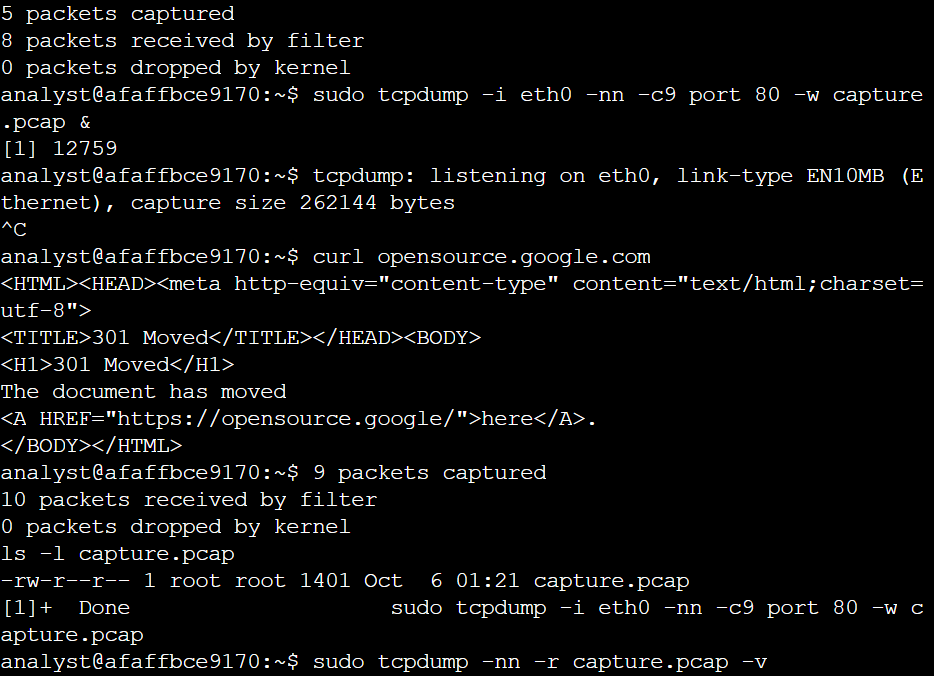
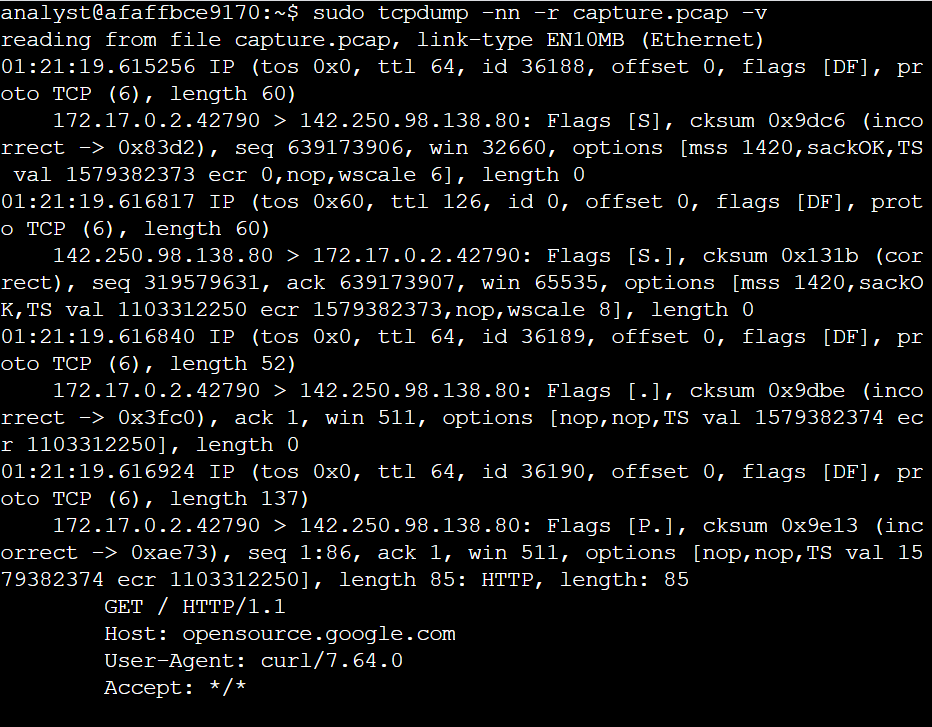
**Entry Logs**

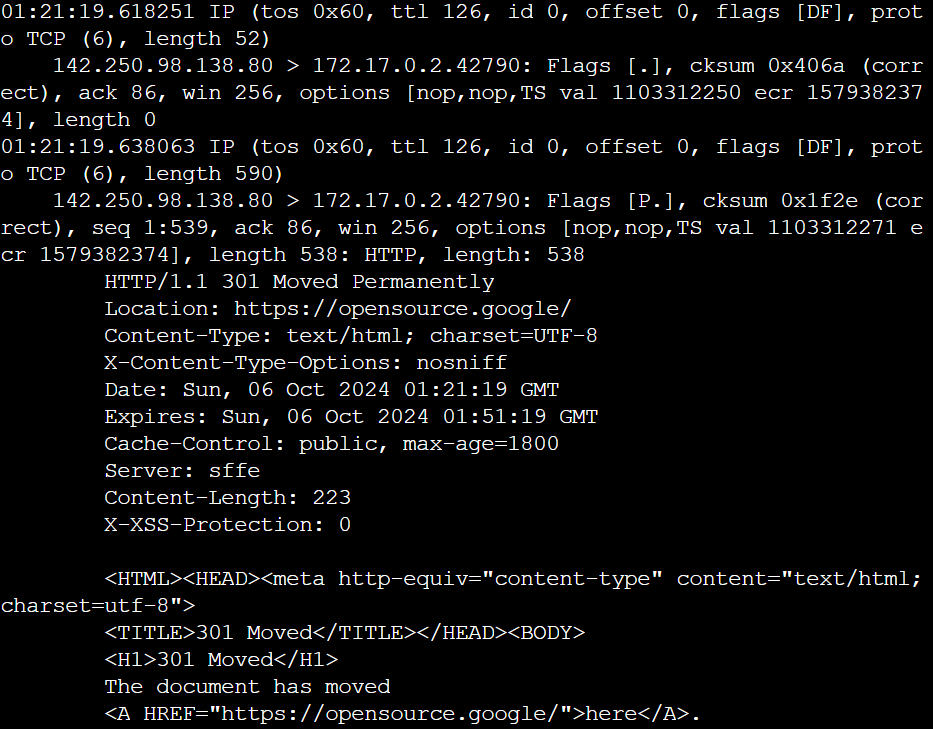
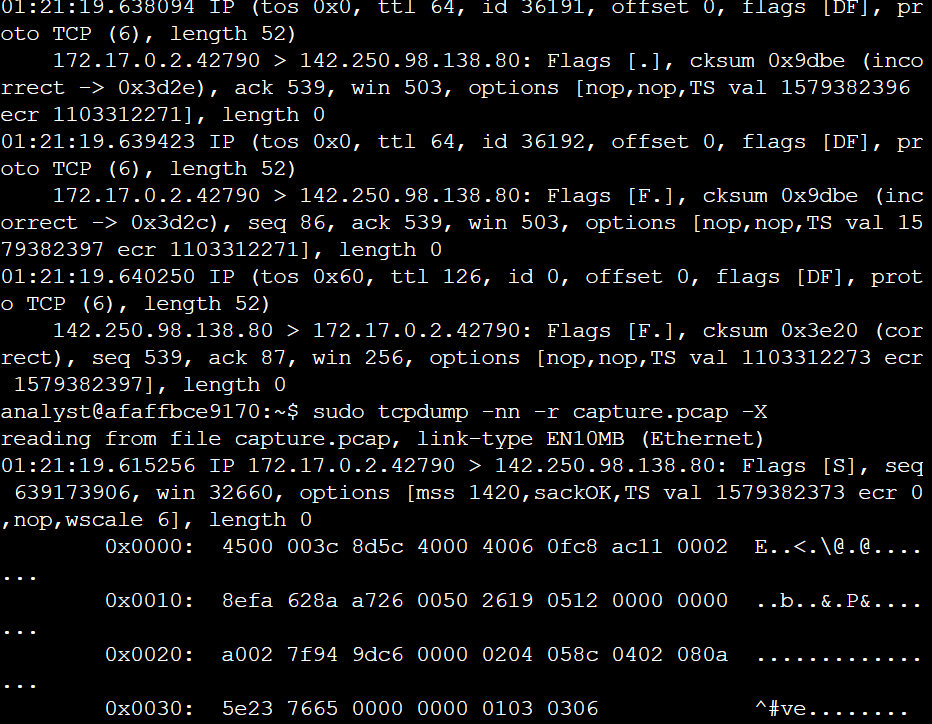
|  |  |
| --- | --- |
| **Date:** Oct 6 2024 | **Entry:** #1 |
| Description | Analyzing a packet capture file |
| Tool(s) used | For this activity, I used Wireshark to analyze a packet capture file. Wireshark is a network protocol analyzer that uses a graphical user interface. The value of Wireshark in cybersecurity is that it allows security analysts to capture and analyze network traffic. This can help in detecting and investigating malicious activity. |
| The 5 W's | * **Who**: N/A * **What**: N/A * **Where**: N/A * **When**: N/A * **Why**: N/A |
| Additional notes | I've never used Wireshark before, so I was excited to begin this exercise and analyze a packet capture file. At first glance, the interface was very overwhelming. I can see why it's such a powerful tool for understanding network traffic. |

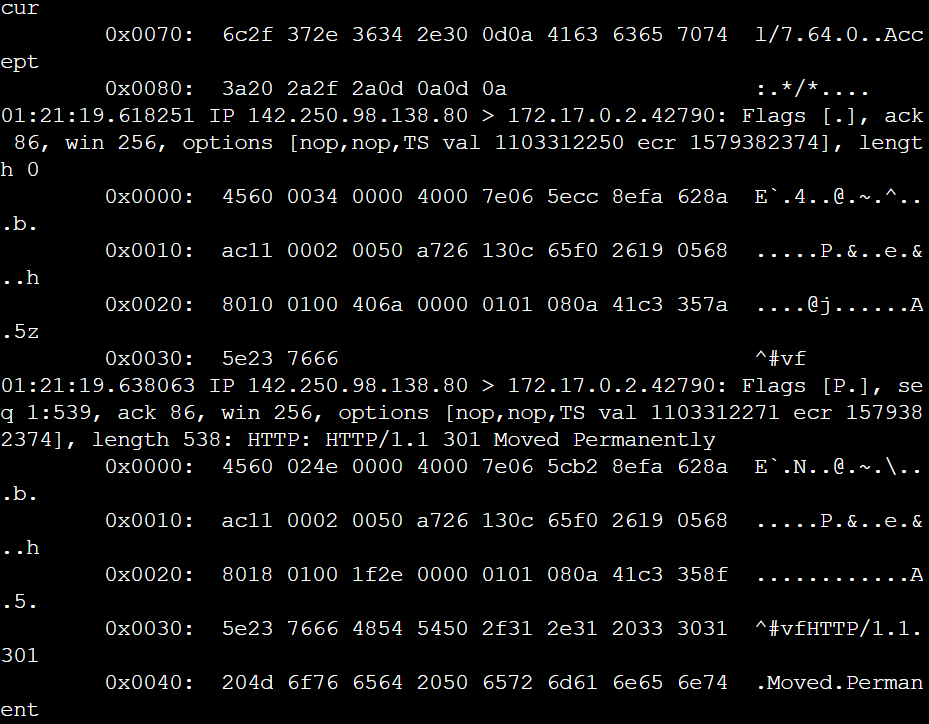
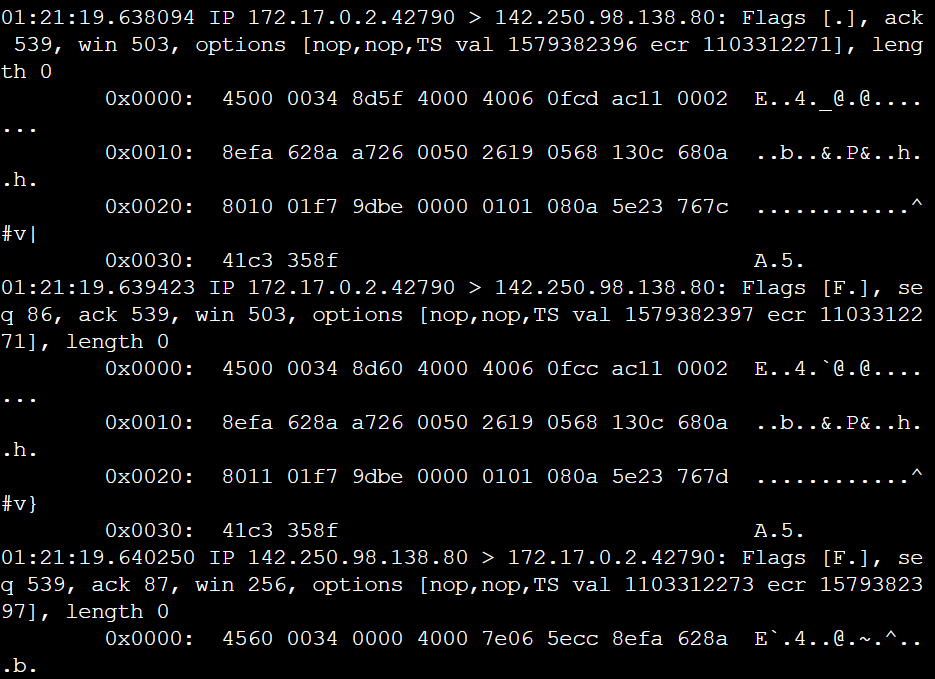


|  |  |
| --- | --- |
| **Date:** Oct 6 2024 | **Entry:**  #2 |
| Description | Capturing my first network packet |
| Tool(s) used | For this activity, I used tcpdump to capture and analyze network traffic. Tcpdump is a network protocol analyzer that's accessed using the command-line interface. Similar to Wireshark, the value of tcpdump in cybersecurity is that it allows security analysts to capture, filter, and analyze network traffic. |
| The 5 W's | * **Who**: N/A * **What**: N/A * **Where**: N/A * **When**: N/A * **Why**: N/A |
| Additional notes | I'm still new to using the command-line interface, so using it to capture and filter network traffic was a challenge. I got stuck a couple of times because I used the wrong commands. But after carefully following the instructions and redoing some steps, I was able to get through this activity and capture network traffic. |

|  |
| --- |
| Reflections/Notes:  I really found the activity using tcpdump challenging. I am new to using the command line, and learning the syntax for a tool like tcpdump was a big learning curve. At first, I felt very frustrated because I wasn't getting the right output. I redid the activity and figured out where I went wrong. What I learned from this was to carefully read the instructions and work through the process slowly.  After taking this course, my understanding of incident detection and response has definitely evolved. At the beginning of the course, I had some basic understanding of what detection and response entailed, but I didn't fully understand the complexity involved. As I progressed through the course, I learned about the lifecycle of an incident; the importance of plans, processes, and people; and tools used. Overall, I feel that my understanding has changed, and I am equipped with more knowledge and understanding about incident detection and response. |