**Section 1, Step 19** – Take a Screenshot of the Terminal windows showing the number of packets captured by the *tcpdump* utility.

*Paste screenshot of the Terminal window from Section 1, Step 19 here*

**Section 2, Step 6** – Take a Screenshot of the Wireshark window with the filtered view for SMB network traffic.

*Paste screenshot of the Wireshark window from Section 2, Step 6 here*

**Section 2, Step 7** – Take a Screenshot of the Wireshark window with the filtered view for HTTP network traffic.

*Paste screenshot of the Wireshark window from Section 2, Step 7 here*

**Questions**

1. How could an attacker utilize this captured traffic to prepare for and instigate an attack on the network (or the devices on the network)?
2. *tcpdump* was run on and captured traffic generated by the Kali machine on that local network – Could the Kali machine have “sniffed” traffic generated by the OWASP BWA machine to another server also in the DMZ network? Why or why not? (Hint: it may help to look back at the pod topology at the beginning of the lab document)
3. Provide two distinct defenses that can be used to defeat “sniffing” – AND indicate at least one technique for each you may use as an attacker to sidestep or defeat those protections.