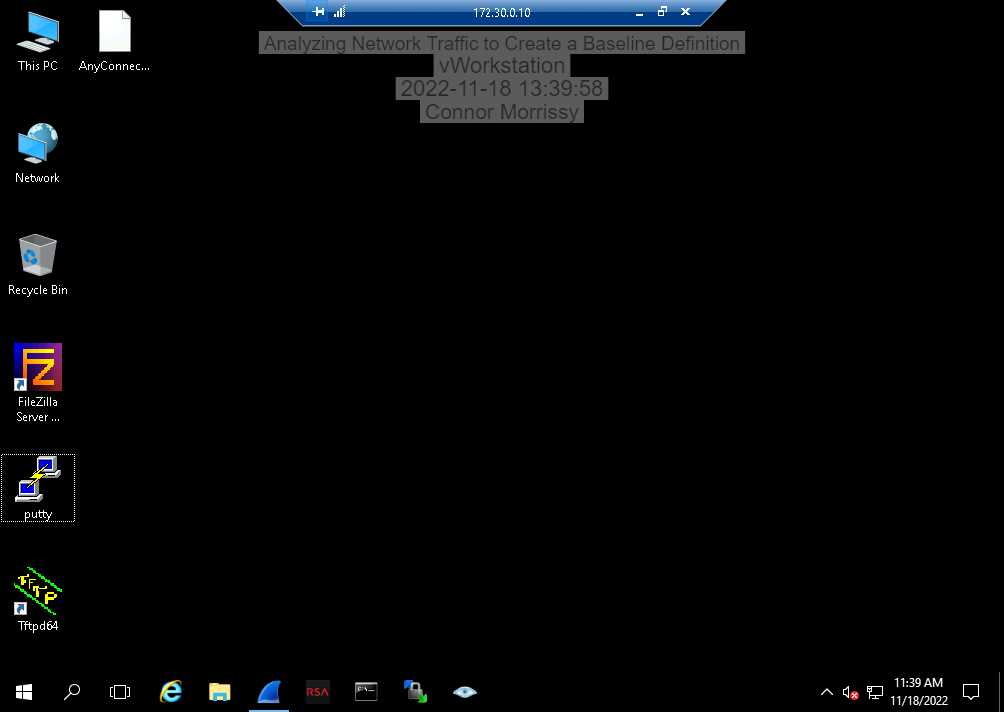
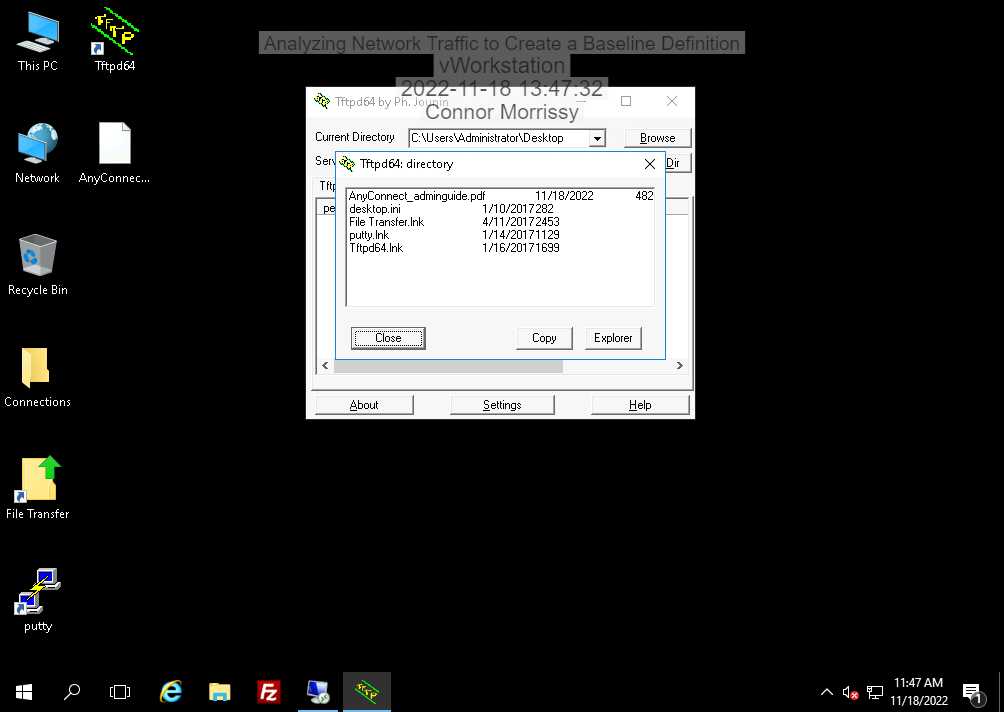
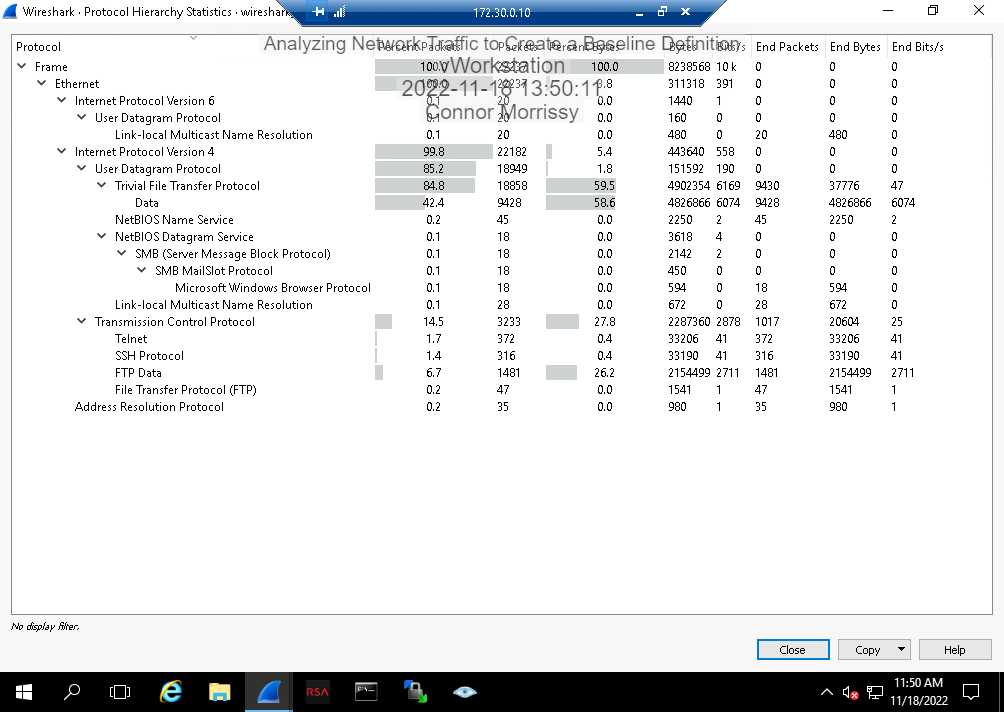
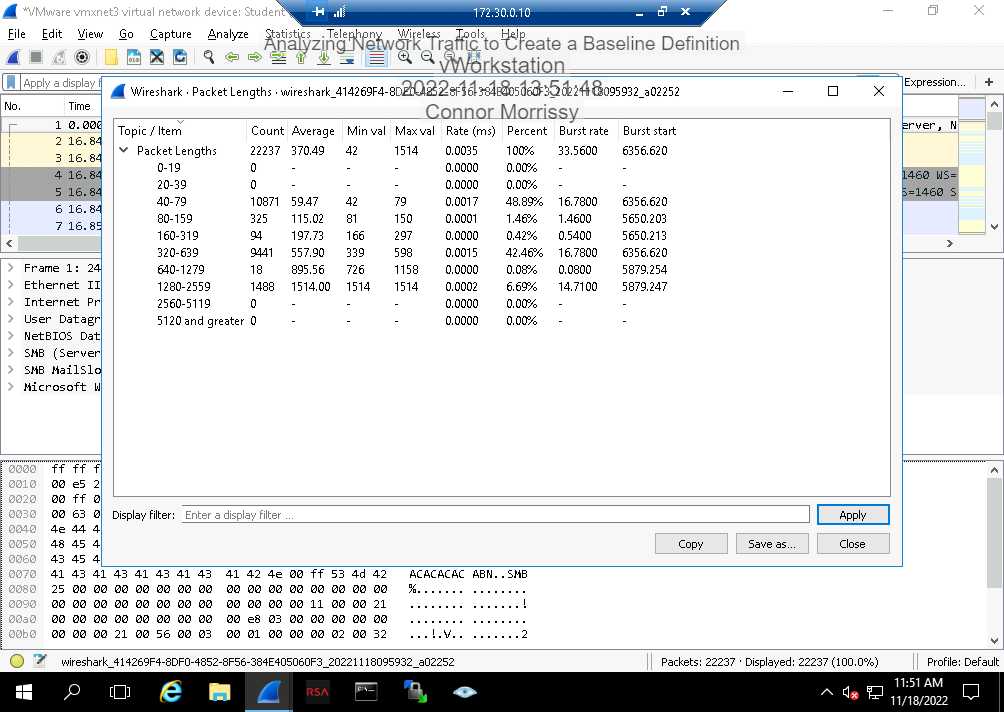
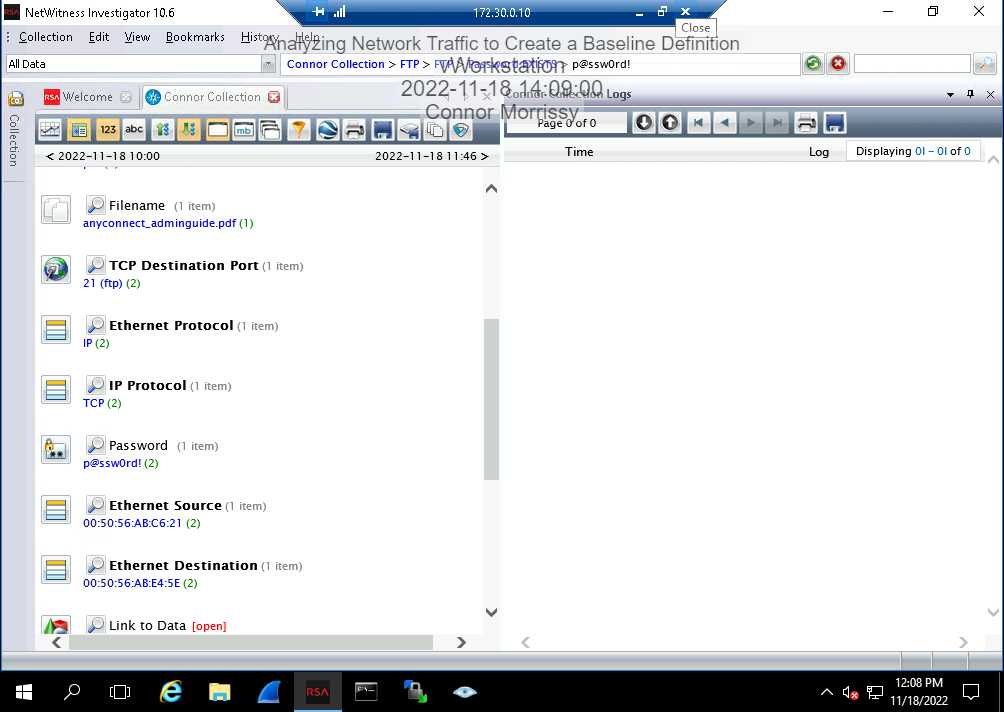
**Section 1:**

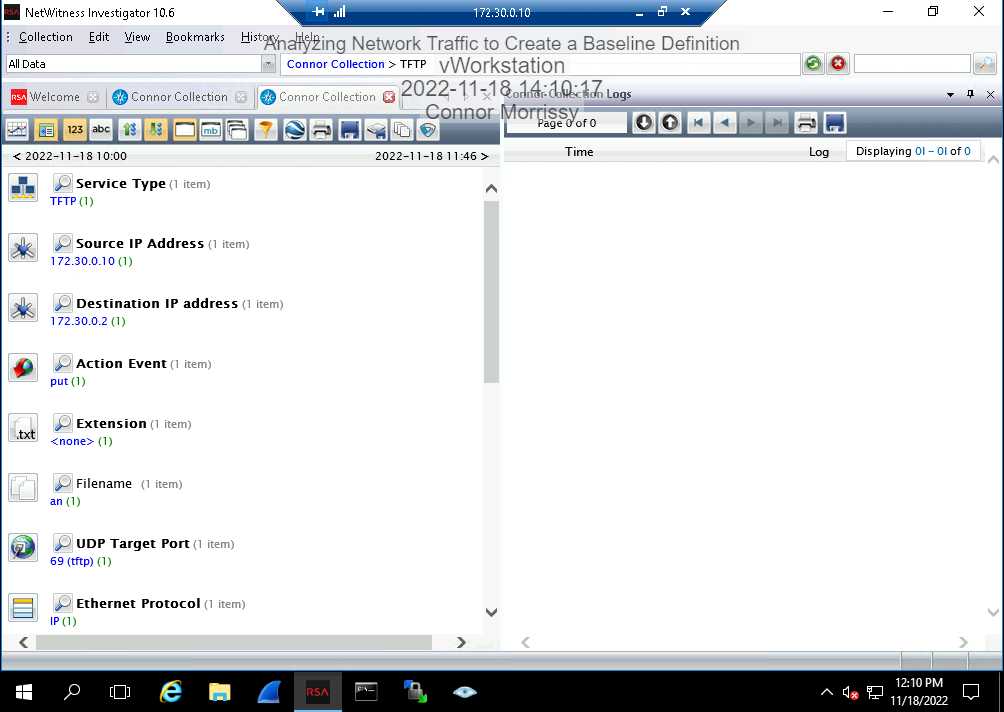


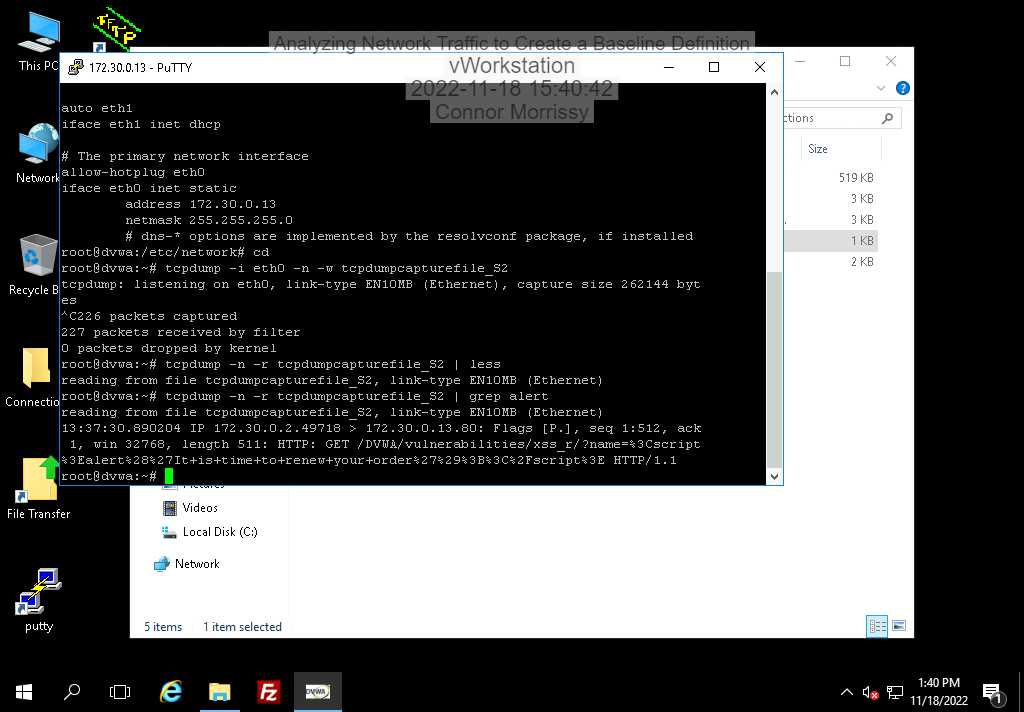


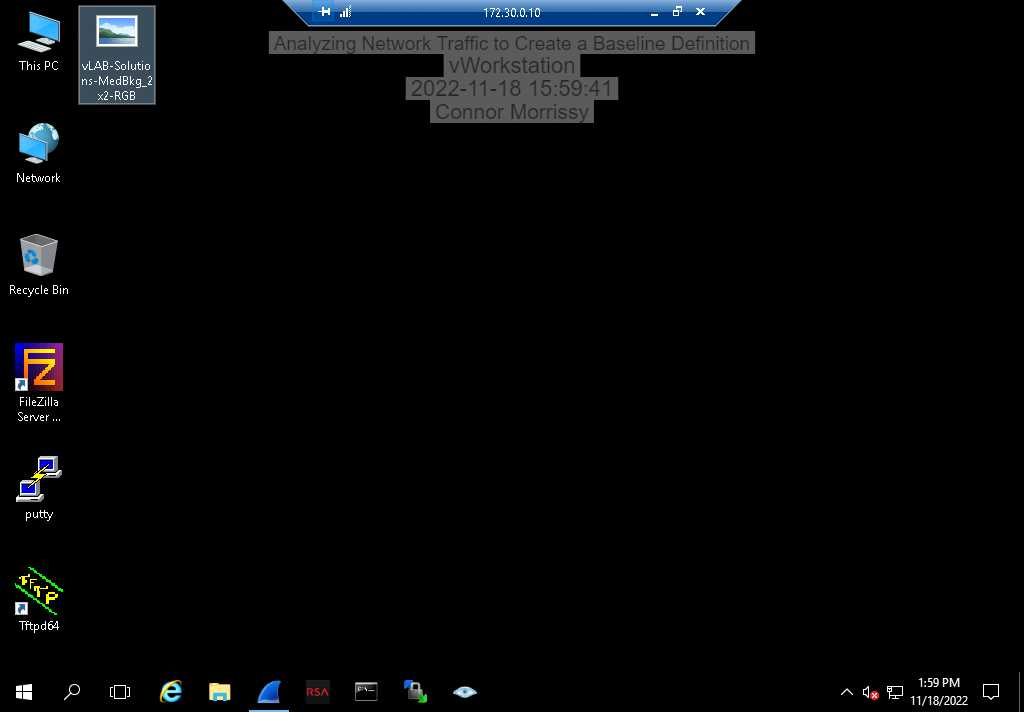


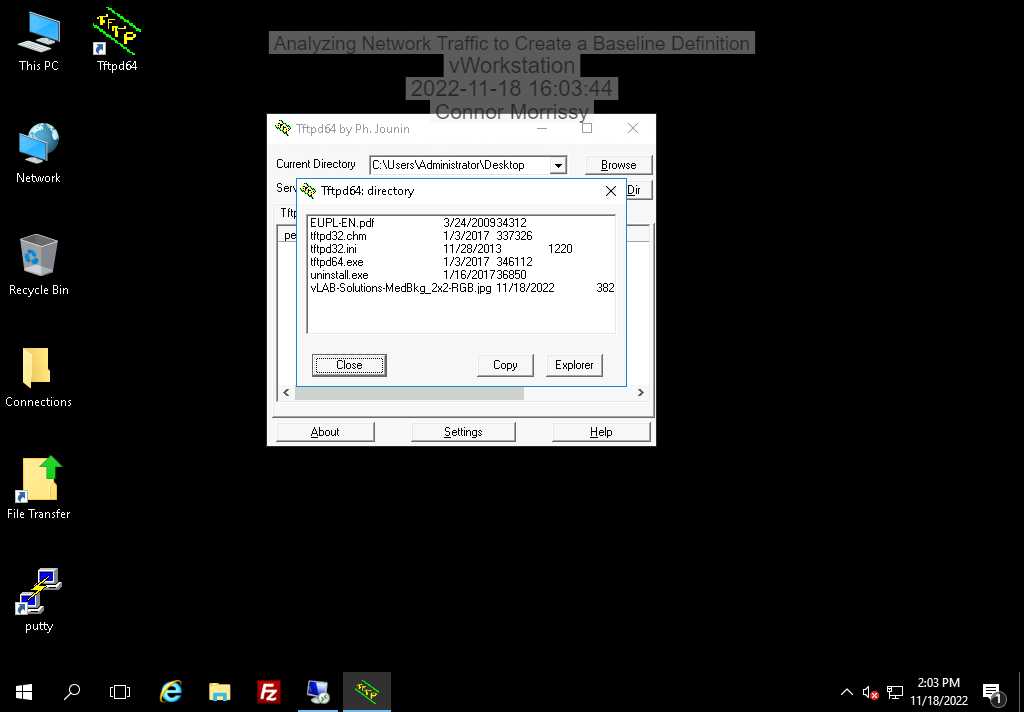


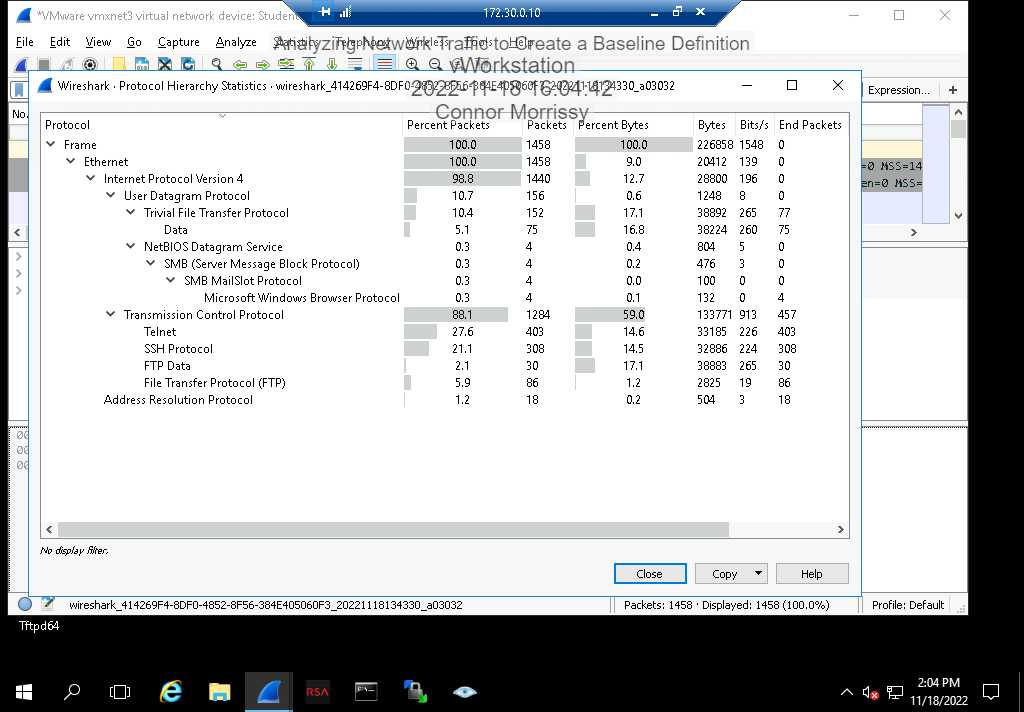


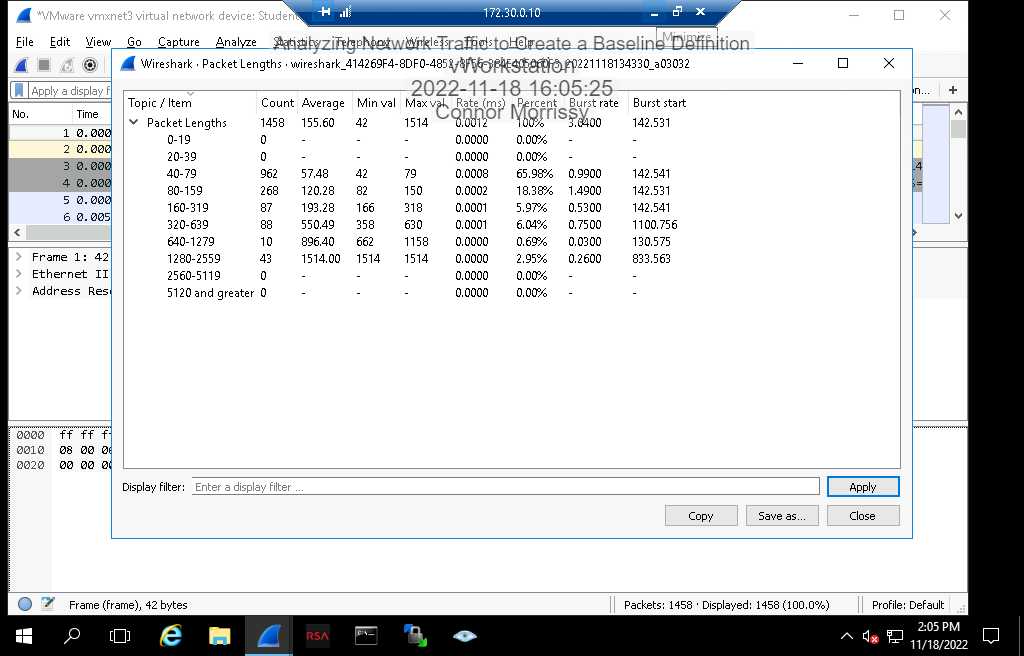


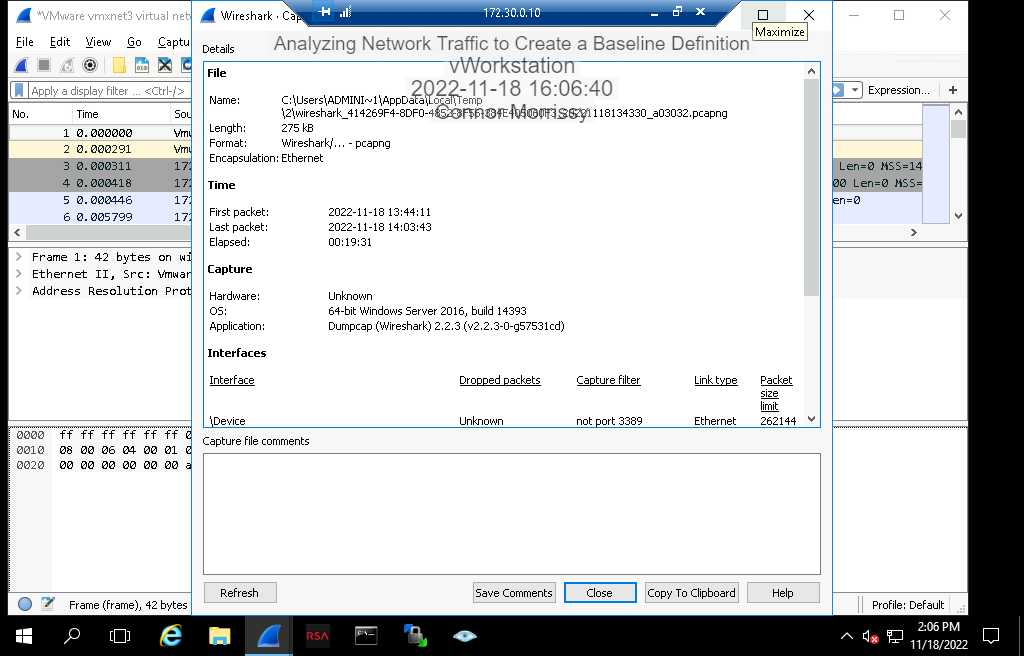
**Section 2:**

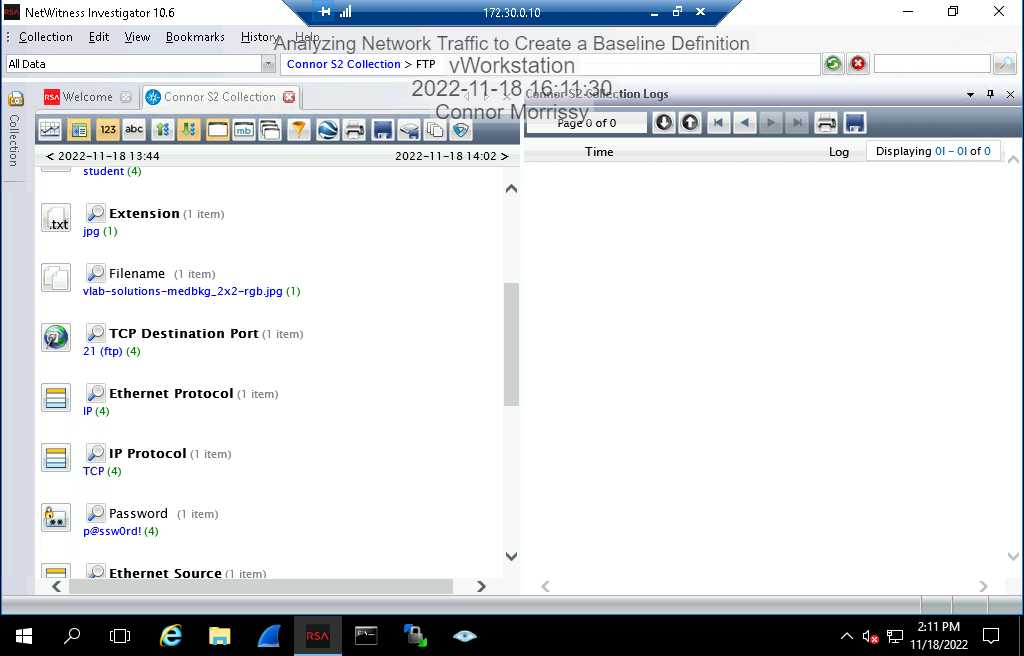


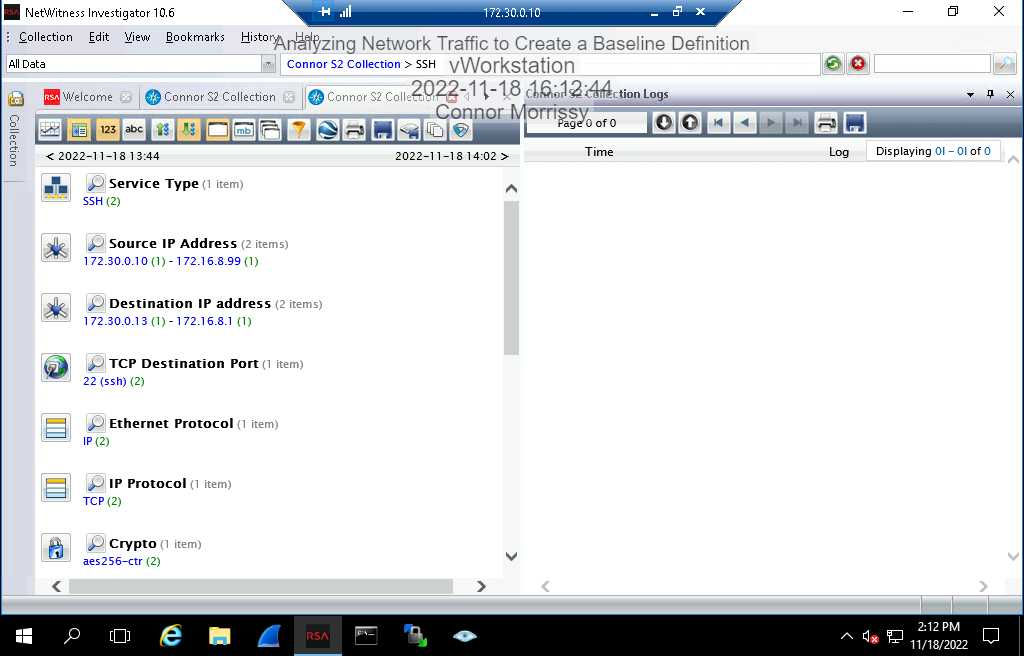


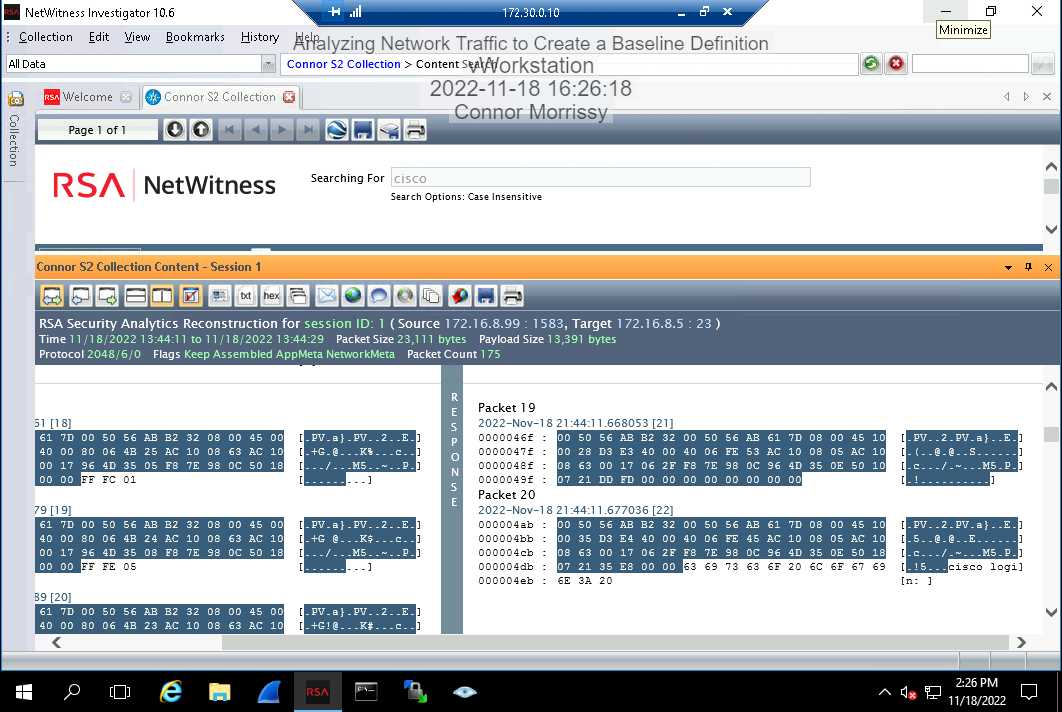












**Section 3:**

1. You would want to filter certain ports because not all ports will accept FTP packets. This way you only get the information you want.
2. Command to filter only FTP traffic: sudo tcpdump ftp  
   Command to view only student information: sudo tcpdump student
3. Performing multiple baseline readings over time can give you a sense of how the network normally runs and functions. Multiple readings are usually required to get to this point and create a baseline. The packet capture file in this lab was not enough to create a baseline, you would need to create multiple. By knowing the normal statistics, it will be easy to see when something is out of the ordinary.