Packet Capture and Replay Tools

1. What is the function of a tcpdump tool?

2. What are filters as used in a tcpdump operation?

3. What are the common definitive types of filters applied in a tcpdump?

4. What happens when the file output function for a tcpdump is not enabled?

5. What are the key differences between Wireshark and tcpdump?

6. If a user wishes to run a network analysis on a Google Chromebook using both Wireshark and tcpdump, how would they go about it?

7. How is tcpreplay different from tcpdump?

8. In what way can tcpreplay be a useful or malicious tool?

9. How might tcpreplay compromise network security?