Scenario

In your role as a cybersecurity analyst, you have been asked to research the differences and similarities between Wireshark and tcpdump and create a chart that outlines your findings.

You'll focus on the two network protocol analyzers: Wireshark and tcpdump. Your goal is to gain a basic understanding of the Wireshark and tcpdump, how they work, and what their features are.

Network protocol analyzers help security analysts examine and understand the network traffic flows. A network protocol analyzer (packet sniffer) is a tool designed to capture and analyze data traffic within a network.