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.

Wireshark

tcpdump

Similarities

It does packet analysis, and it can decode data payloads if the encryption keys are identified, and it can recognize data payloads from file transfers such as smtp, http, etc.

It's best for detailed investigation and forensic analysis

Can capture live packets.

Both are used in incident response, network security and digital forensic.

Open-source software.

Tcpdump only provides do a simple analysis of such types of traffic, such as DNS queries.

It's best for quick captures, server-side debugging, automation