🧩 Wireshark vs. tcpdump – Comparison Chart by Jordan Butler

Feature	Wireshark	tcpdump
User Interface	GUI-based (Graphical User Interface)	CLI-based (Command-Line Interface)
Visualization	Offers deep packet inspection with filters, colors, graphs	Displays raw packet data line-by-line in the terminal
Platform Support	Cross-platform (Windows, macOS, Linux)	Cross-platform (mostly used on Unix/Linux)
Capture Capability	Captures live traffic and can analyze saved .pcap files	Captures live traffic and can save to/read from .pcap files
Filtering Syntax	Uses **display filters** (more complex but powerful)	Uses **capture filters** (simple and efficient)
Use Case	Best for detailed traffic analysis and education/training	Best for lightweight, quick analysis or scripting

---

✅ Summary of Requirements

✅ At least 2 Differences:

1. **Interface:** Wireshark has a graphical user interface (GUI), while tcpdump operates through the command line.
2. **Filtering Style:** Wireshark uses **display filters**, while tcpdump uses **capture filters**.

✅ At least 3 Similarities:

1. Both can **capture live network traffic**.
2. Both support saving and reading **.pcap files**.
3. Both are **cross-platform tools** and widely used in cybersecurity.