tcpdump cumpcat wireshark

Wireshark is actually a GUI tool that calls a command-line
executable called
dumpcap
, which captures the packets and saves them to a disk file.
Wireshark reads this file and presents the processed packets to the user interface.
An alternative to Wireshark is to use the dumpcap or
tcpdump
executable
directly (these are covered in
Chapter 8
,
Command-line and Other Utilities
)
or a high performance capture appliance offered by numerous vendors.