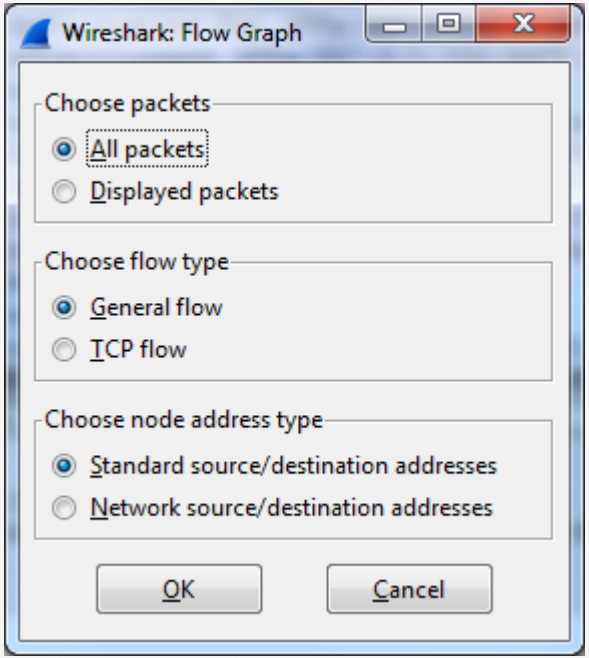
Flow Graphs

Wireshark Flow Graph

- What is the flow graph?
- Why use the flow graph?
  - To analyze a capture or filtered data to extract the flow from source to destination and view the conversation
- What can you find?
  - Timeouts
  - Dropped connections
  - Other

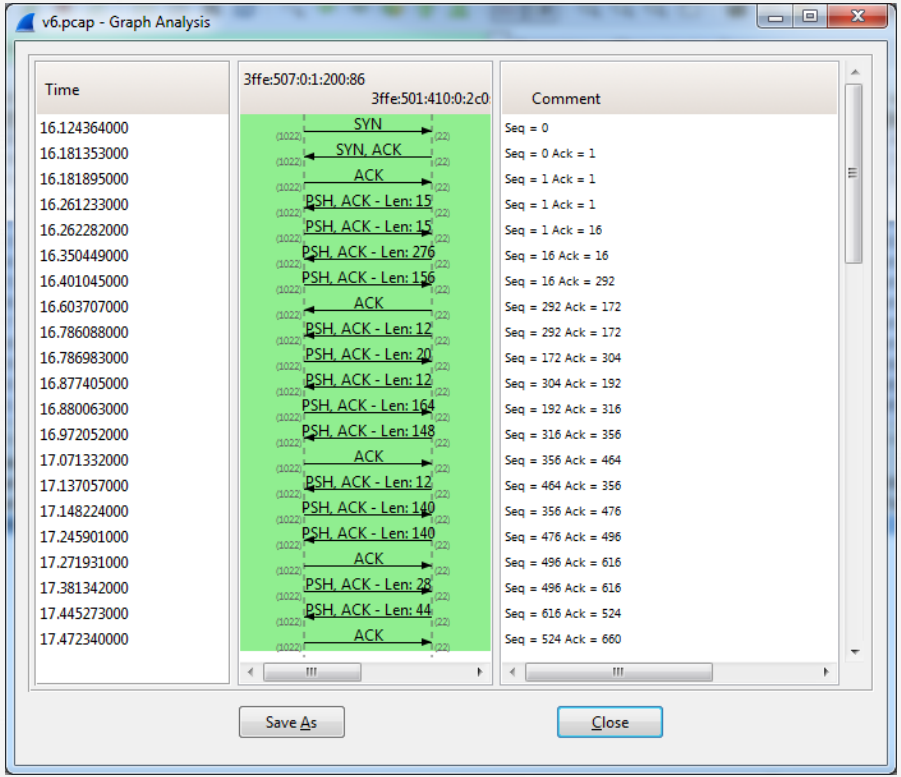
Wireshark Flow Graph



Wireshark Flow Graph

- Analyze the traffic flow
  - TCP flow extraction – TCP stream
  - Understanding all flow concepts
- TCP handshake
  - Use to establish a connection
  - SYN – SYN/ACK – ACK
  - Others (FIN, RST, etc.)

Analyzing a Flow Graph



Questions?