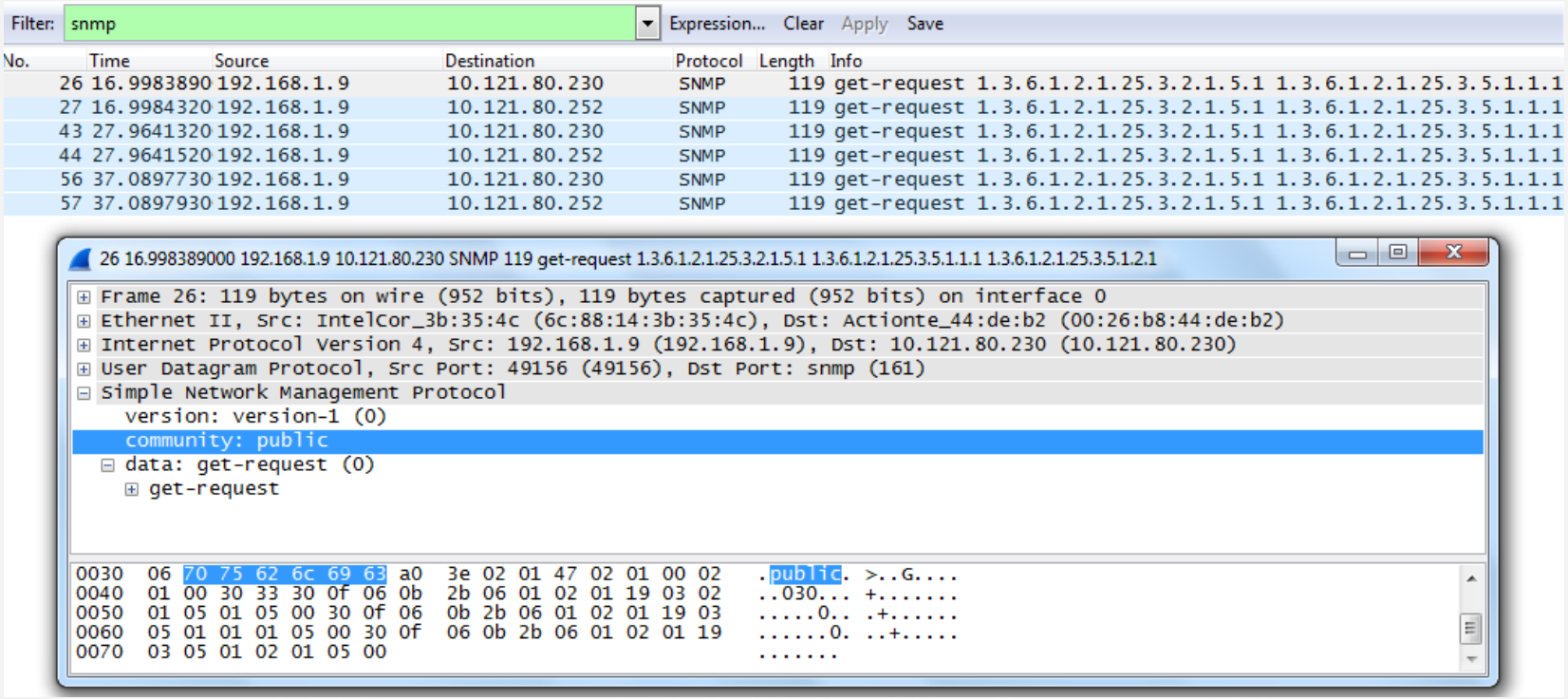
Protocol Analysis

Ethernet in the CCIE Lab

- Why is protocol analysis important?
- What do we do with captured data?
  - After capturing, we need to display the data
- Analyzing 101
  - We may need to filter traffic
  - Inspection of the traffic involves looking at the sum of all parts

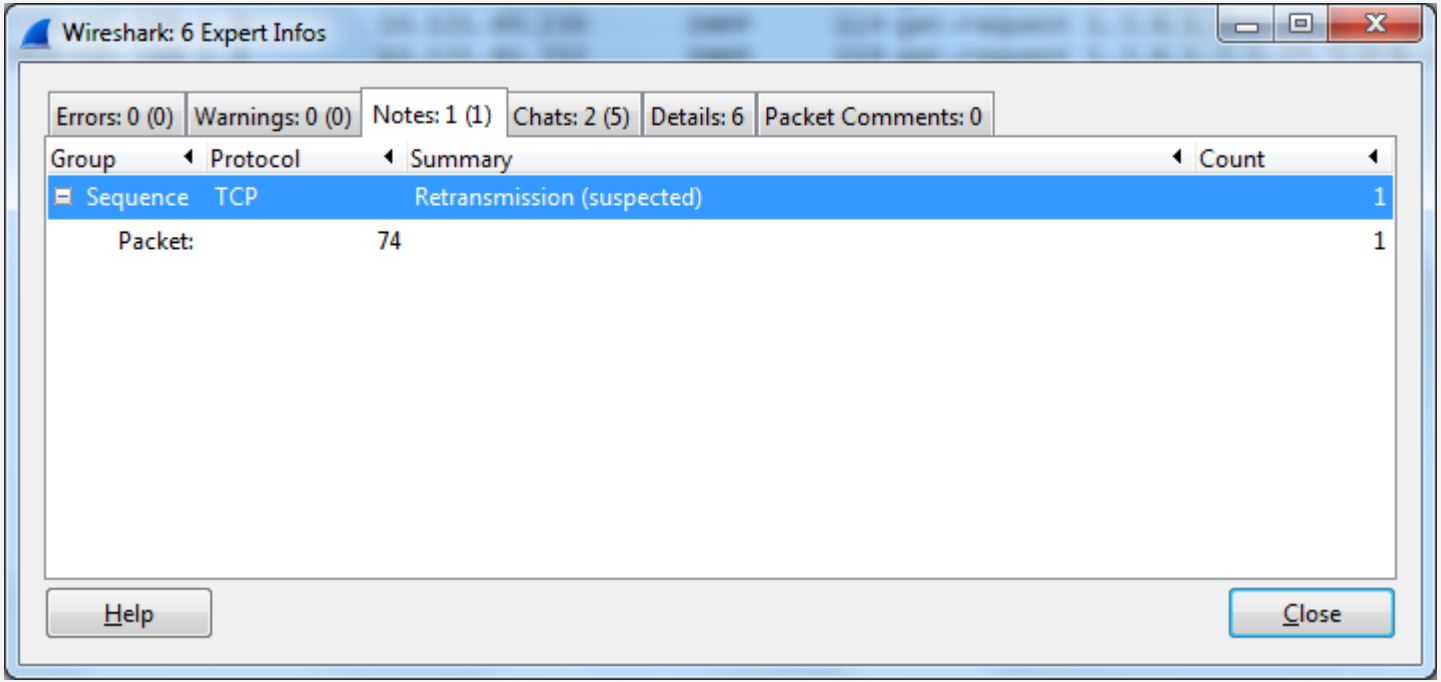
Wireshark & Protocol Analysis



Protocol Analysis

- Data captured for analysis can reveal many issues
  - Bandwidth
  - Corruption
  - Incorrect path
  - Latency
  - Many others
- Understanding protocols
  - For example, you will need to know the specific differences between TCP and UDP (on the same OSI layer)
  - You will need to know how protocols operate at different layers of the OSI model

Analysis Tools



What Will We Find?

- Can protocol analysis solve issues?
  - Deep packet inspection
  - Reviewing data patterns
  - Reviewing timestamps
  - Communication patterns