



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

Filter: snmp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
26	16.9983890	192.168.1.9	10.121.80.230	SNMP	119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1
27	16.9984320	192.168.1.9	10.121.80.252	SNMP	119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1
43	27.9641320	192.168.1.9	10.121.80.230	SNMP	119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1
44	27.9641520	192.168.1.9	10.121.80.252	SNMP	119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1
56	37.0897730	192.168.1.9	10.121.80.230	SNMP	119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1
57	37.0897930	192.168.1.9	10.121.80.252	SNMP	119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1

26 16.998389000 192.168.1.9 10.121.80.230 SNMP 119 get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1

- Frame 26: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface 0
- Ethernet II, Src: IntelCor_3b:35:4c (6c:88:14:3b:35:4c), Dst: Actionte_44:de:b2 (00:26:b8:44:de:b2)
- Internet Protocol Version 4, Src: 192.168.1.9 (192.168.1.9), Dst: 10.121.80.230 (10.121.80.230)
- User Datagram Protocol, Src Port: 49156 (49156), Dst Port: snmp (161)
- Simple Network Management Protocol
 - version: version-1 (0)
 - community: public
 - data: get-request (0)
 - get-request

0030 06 70 75 62 6c 69 63 a0 3e 02 01 47 02 01 00 02 .public. >..G....
0040 01 00 30 33 30 0f 06 0b 2b 06 01 02 01 19 03 02 ..030... +.....
0050 01 05 01 05 00 30 0f 06 0b 2b 06 01 02 01 19 030.. +.....
0060 05 01 01 01 05 00 30 0f 06 0b 2b 06 01 02 01 190.. ..+.....
0070 03 05 01 02 01 05 00

Protocol Analysis

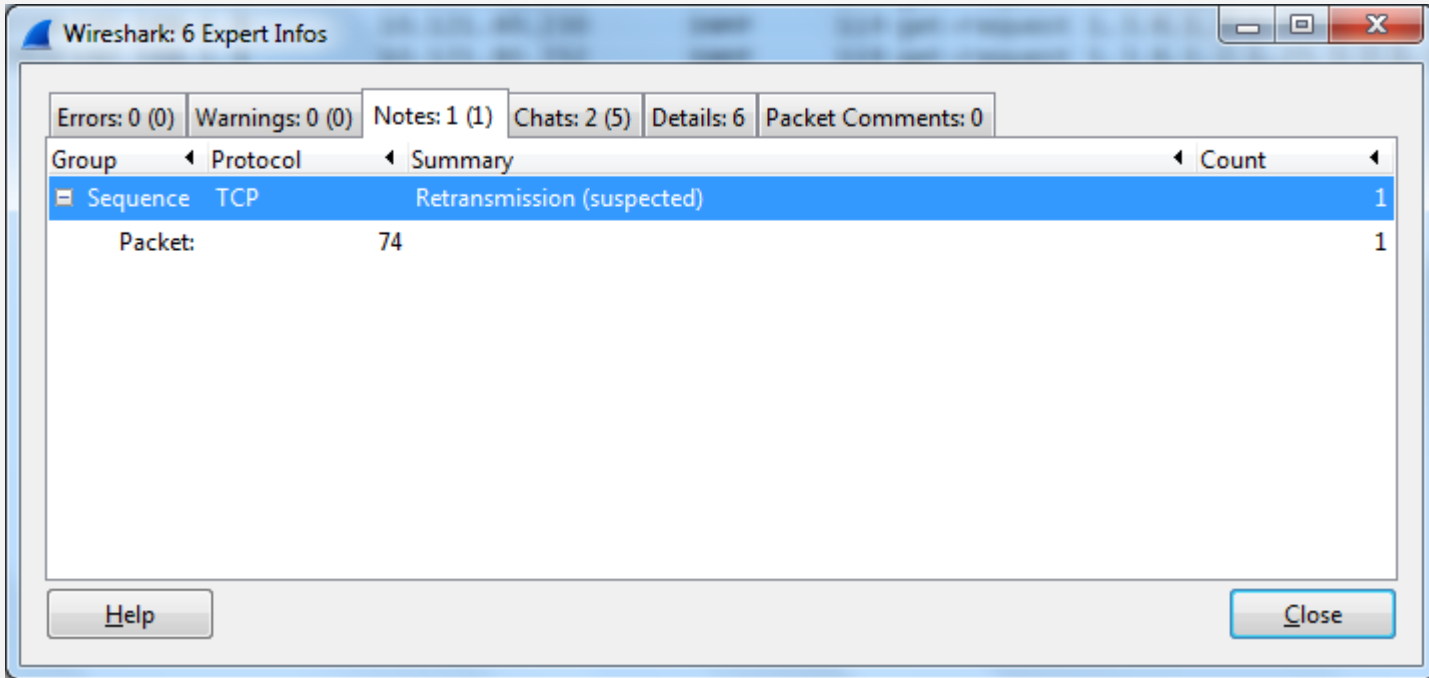
» Data captured for analysis can reveal many issues

- 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