



Window Panes

Wireshark's Three Panes

» Three panes of the capture window

- Packet List –Displays all packets in the current capture file
- Packet Details –Displays the current packet that is selected in the Packet List pane in granular detail
- Packet Bytes –Displays the data of the current packet that is selected in the Packet List pane in hex

The Packet List

capture 1.pcapng [Wireshark 1.10.7 (v1.10.7-0-g6b931a1 from master-1.10)]

View Go Capture Analyze Statistics Telephony Tools Internals Help

Expression... Clear Apply Save

Time	Source	Destination	Protocol	Length	Info
0.32983000	Cisco_e2:7b:47	Broadcast	ARP	60	who has 10.121.90.200? Tell 10.121.90.3
0.38158900	Cisco_e2:7b:47	Broadcast	ARP	60	who has 10.121.90.124? Tell 10.121.90.3
1.08546500	Cisco_e2:7b:47	Broadcast	ARP	60	who has 10.121.90.167? Tell 10.121.90.3
1.19410400	Cisco_e2:7b:47	Broadcast	ARP	60	who has 10.121.90.105? Tell 10.121.90.3
1.46517800	wistron_0c:37:9d	Broadcast	ARP	60	who has 10.121.90.64? Tell 10.121.90.149
1.46562900	Elitegro_1e:f7:ab	Broadcast	ARP	60	who has 10.121.90.149? Tell 10.121.90.64
1.53587000	Cisco_e2:7b:47	Broadcast	ARP	60	who has 10.121.90.171? Tell 10.121.90.3
1.79830700	Cisco_56:dd:c7	Broadcast	ARP	60	who has 10.121.90.105? Tell 10.121.90.2
2.42764800	Cisco_e2:7b:47	Broadcast	ARP	60	who has 10.121.90.99? Tell 10.121.90.3
2.62491000	HewlettP_91:46:ec	Broadcast	ARP	60	who has 10.121.90.187? Tell 10.121.90.116
2.96222500	NecInfro_ec:10:c0	Broadcast	ARP	60	who has 10.121.78.1? Tell 10.121.78.239
3.51347400	Cisco_e2:7b:47	Broadcast	ARP	60	who has 10.121.90.105? Tell 10.121.90.3
3.68774900	HewlettP_91:46:ec	Broadcast	ARP	60	who has 10.121.90.202? Tell 10.121.90.116
4.43352800	Cisco_56:dd:c7	Broadcast	ARP	60	who has 10.121.90.189? Tell 10.121.90.2
5.11334800	wistron_0c:39:23	Broadcast	ARP	60	who has 10.121.90.3? Tell 10.121.90.89
5.37906300	Cisco_e2:7b:47	Broadcast	ARP	60	who has 10.121.90.171? Tell 10.121.90.3

The Packet List

» Packets captured in order for review

- Data is captured in the packet list in the order it was seen, prepared for your analysis

» Reviewing column data

- Number
- Time
- Source and destination
- Protocol
- Info

The Packet Details

- [-] Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
- [-] Ethernet II, Src: Cisco_e2:7b:47 (10:f3:11:e2:7b:47), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 - [-] Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 - [-] Source: Cisco_e2:7b:47 (10:f3:11:e2:7b:47)
 - Type: ARP (0x0806)
 - Padding: 0000000000000000000000000000000000000000
- [-] Address Resolution Protocol (request)
 - Hardware type: Ethernet (1)
 - Protocol type: IP (0x0800)
 - Hardware size: 6
 - Protocol size: 4
 - Opcode: request (1)
 - Sender MAC address: cisco_e2:7b:47 (10:f3:11:e2:7b:47)
 - Sender IP address: 10.121.90.3 (10.121.90.3)
 - Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
 - Target IP address: 10.121.90.200 (10.121.90.200)

The Packet Details

» Review the selected packet

- Drill down into a selected packet to review other information found within it

» Review protocol fields and other data

- Headers
- Frame types
- Codes

The Packet Bytes

```
0000 ff ff ff ff ff ff 10 f3 11 e2 7b 47 08 06 00 01 ..... ..{G....
0010 08 00 06 04 00 01 10 f3 11 e2 7b 47 0a 79 5a 03 ..... ..{G.yZ.
0020 00 00 00 00 00 00 0a 79 5a c8 00 00 00 00 00 .....y Z.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 ..... .....
```

The Packet Bytes

» View the raw data

- Can be view in hexadecimal format or bits
- ASCII characters

Questions?