

24. Network layer protocol header analysis using Wire shark – SMTP and ICMP.

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The main window is divided into three panes: Packet List, Packet Details, and Packet Bytes. The Packet List pane shows a list of captured packets, with the selected packet (No. 11) being an ICMP Echo (ping) request. The Packet Details pane shows the hierarchical structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol (ICMP). The Packet Bytes pane shows the raw data of the packet in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2a03:2880:f34f:121::	2409:40f4:39:8dd5:2::	TCP	74	80 → 52825 [ACK] Seq=1 Ack=1 Win=821 Len=0
2	0.000000	2a03:2880:f34f:121::	2409:40f4:39:8dd5:2::	TCP	74	80 → 52825 [ACK] Seq=1 Ack=53 Win=821 Len=0
3	0.204986	f2:32:91:e0:38:57	AzureWaveTec_f0:5a:83	ARP	42	Who has 192.168.19.15? Tell 192.168.19.254
4	0.204986	2a03:2880:f34f:121::	2409:40f4:39:8dd5:2::	TCP	281	80 → 52825 [PSH, ACK] Seq=1 Ack=53 Win=821 Len=207
5	0.205019	AzureWaveTec_f0:5a:83	f2:32:91:e0:38:57	ARP	42	192.168.19.15 is at f8:54:f6:f0:5a:83
6	0.247305	2409:40f4:39:8dd5:2::	2a03:2880:f34f:121::	TCP	74	52825 → 80 [ACK] Seq=53 Ack=208 Win=509 Len=0
7	0.328228	2409:40f4:39:8dd5:2::	2603:1040:5:3:19	TLSv1.2	102	Application Data
8	0.423166	2409:40f4:39:8dd5:2::	2409:40f4:39:8dd5:1::	ICMPv6	86	Neighbor Solicitation for 2409:40f4:39:8dd5:87 from f8:54:f6:f0:5a:83
9	0.531111	2409:40f4:39:8dd5:2::	2603:1040:5:3:19	TCP	102	Application Data
10	1.024274	2603:1040:5:3:19	2409:40f4:39:8dd5:2::	TCP	74	443 → 52449 [ACK] Seq=1 Ack=29 Win=501 Len=0
11	1.430044	2409:40f4:39:8dd5:2::	2409:40f4:39:8dd5:1::	ICMPv6	86	Neighbor Solicitation for 2409:40f4:39:8dd5:87 from f8:54:f6:f0:5a:83
12	1.435795	2409:40f4:39:8dd5:2::	2409:40f4:39:8dd5:2::	ICMPv6	78	Neighbor Advertisement 2409:40f4:39:8dd5:87 (rtr, sol)
13	2.764768	f600:f032:91ff:f6::	2409:40f4:39:8dd5:2::	ICMPv6	86	Neighbor Solicitation for 2409:40f4:39:8dd5:2da0:11f8:99e4:f42d from f2:32:91:e0:38:57
14	2.764907	2409:40f4:39:8dd5:2::	f600:f032:91ff:f6::	ICMPv6	86	Neighbor Advertisement 2409:40f4:39:8dd5:2da0:11f8:99e4:f42d (sol, ovr) is at f8:54:f6:f0:5a:83
15	3.891812	2603:1040:5:3:19	2409:40f4:39:8dd5:2::	TLSv1.2	101	Application Data
16	3.934191	2409:40f4:39:8dd5:2::	2603:1040:5:3:19	TCP	74	52449 → 443 [ACK] Seq=29 Ack=28 Win=253 Len=0
17	5.165188	192.168.19.15	20.189.173.26	TLSv1.2	1181	Application Data
18	5.167629	192.168.19.15	20.189.173.26	TCP	1354	53667 → 443 [ACK] Seq=128 Ack=1 Win=1021 Len=1300 [TCP PDU reassembled in 21]
19	5.167629	192.168.19.15	20.189.173.26	TCP	1354	53667 → 443 [ACK] Seq=2428 Ack=1 Win=1021 Len=1300 [TCP PDU reassembled in 21]
20	5.167629	192.168.19.15	20.189.173.26	TCP	1354	53667 → 443 [ACK] Seq=3728 Ack=1 Win=1021 Len=1300 [TCP PDU reassembled in 21]

Frame 11: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF... (BA400EA6-5...)
Ethernet II, Src: AzureWaveTec_f0:5a:83 (f8:54:f6:f0:5a:83), Dst: f2:32:91:e0:38:57 (f2:32:91:e0:38:57)
Internet Protocol Version 4, Src: 2409:40f4:39:8dd5:2da0:11f8:99e4:f42d, Dst: 2409:40f4:39:8dd5:1::87
Internet Control Message Protocol v6
Type: Neighbor Solicitation (135)
Code: 0
Checksum: 0x85fe [correct]
[Checksum Status: Good]
Reserved: 00000000
Target Address: 2409:40f4:39:8dd5:87
ICMPv6 Option (Source link-layer address : f8:54:f6:f0:5a:83)
Type: Source link-layer address (1)
Length: 1 (0 bytes)
Link-layer address: AzureWaveTec_f0:5a:83 (f8:54:f6:f0:5a:83)

SMTP

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The main window is divided into three panes: Packet List, Packet Details, and Packet Bytes. The Packet List pane shows a list of captured packets, with the selected packet (No. 101) being an SMTP packet. The Packet Details pane shows the hierarchical structure of the selected packet, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and SMTP. The Packet Bytes pane shows the raw data of the packet in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
101	0.120645	192.168.186.197	223.196.146.77	UDP	81	62236 → 443 Len=39
102	0.120662	192.168.186.197	223.196.146.77	UDP	80	62236 → 443 Len=38

Source: AzureWaveTec_a4:43:01 (a8:41:f4:a4:43:01)
Type: IPv4 (0x0800)
[Stream index: 0]
Internet Protocol Version 4, Src: 192.168.186.197, Dst: 216.239.38.223
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1195
Identification: 0x19cd (6605)
010. = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 62
Protocol: UDP (17)
Header Checksum: 0xa338 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.186.197
Destination Address: 216.239.38.223
[Stream index: 0]
User Datagram Protocol, Src Port: 62604, Dst Port: 443
Source Port: 62604
Destination Port: 443
Length: 1175
Checksum: 0xe7dc [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Stream Packet Number: 3]
[Timestamps]
UDP payload (1167 bytes)
Data (1167 bytes)
Data [...]: 45f48b9ec6180490719e858ebad1ae4f96227fd4808946eefc178cb9b7c4d4b7d0f6a5a5b1a9e9c6af67ae7a7
[Length: 1167]