

# Assignment 1

## Wireshark Fundamentals

By Ziming Song

[zs2815@nyu.edu](mailto:zs2815@nyu.edu)

### Part 1: tr-chappellu.pcapng

#### a. Find the most active TCP conversation in the file (by bits per second)

The most active TCP conversation is the first one marked as blue. The bits/s from A to B at 108kbps and the bits/s from B to A at 1250kbps. The filter method is marked with red boxes.

The image shows a Wireshark packet capture analysis of a file named tr-chappellu.pcapng. The main display area shows a list of packets, with the first packet (627) highlighted in blue. The packet details pane on the right shows the 'TCP - 23' section, which is also highlighted in blue. The 'Statistics' pane on the left shows the 'TCP' section selected. The 'Filter' field on the right is empty. The 'Columns to display' list on the right shows 'Bits/s A → B' and 'Bits/s B → A' selected. The 'Filter by' dropdown is set to 'Greater than'.

Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
627	141.101.125.193	80	14	9 kB	5	6	753 bytes	8	9 kB	8.655147	0.0554	108 kbps	1250 kbps
643	207.171.187.117	80	122	119 kB	21	38	3 kB	84	116 kB	32.827897	1.1597	20 k	Columns to display
642	207.171.187.117	80	127	127 kB	20	41	4 kB	86	123 kB	32.822986	1.5346	19 k	Address A
641	207.171.187.117	80	85	85 kB	19	27	2 kB	58	83 kB	32.613127	1.2735	15 k	Port A
640	207.171.187.117	80	54	49 kB	18	18	2 kB	36	47 kB	32.546263	1.1913	12 k	Address B
644	207.171.187.117	80	56	55 kB	22	18	1 kB	38	53 kB	32.860271	1.2247	9204 bi	Port B
629	184.73.250.227	80	66	26 kB	7	34	14 kB	32	12 kB	8.677919	25.2886	4492 bi	Packets
630	184.73.250.227	80	18	5 kB	8	9	2 kB	9	3 kB	28.41827	5.6151	3222 bi	Bytes
626	141.101.125.193	80	13	9 kB	4	5	699 bytes	8	9 kB	8.654991	1.9666	2843 bi	Stream ID
623	69.59.180.202	80	22	12 kB	2	10	4 kB	12	9 kB	8.391690	15.0490	1881 bi	Total Packets
625	69.59.180.202	80	16	7 kB	3	8	2 kB	8	5 kB	8.560092	14.8757	1073 bi	Percent Filtered
622	198.66.239.146	80	10	1 kB	1	6	745 bytes	4	609 bytes	8.300312	16.0406	371 bi	Packets A → B
628	184.73.250.227	80	6	354 bytes	6	4	228 bytes	2	126 bytes	8.677734	5.7864	315 bi	Bytes A → B
636	184.73.250.227	80	7	420 bytes	14	5	294 bytes	2	126 bytes	30.943974	8.7332	269 bi	Packets B → A
637	184.73.250.227	80	7	420 bytes	15	5	294 bytes	2	126 bytes	30.944359	8.7317	269 bi	Bytes B → A
638	184.73.250.227	80	7	420 bytes	16	5	294 bytes	2	126 bytes	30.945213	8.7322	269 bi	Rel Start
639	184.73.250.227	80	7	420 bytes	17	5	294 bytes	2	126 bytes	30.945595	8.7330	269 bi	Duration
631	184.73.250.227	80	7	420 bytes	9	5	294 bytes	2	126 bytes	30.686331	8.9924	261 bi	Bits/s A → B
632	184.73.250.227	80	7	420 bytes	10	5	294 bytes	2	126 bytes	30.693344	8.9839	261 bi	Bits/s B → A
633	184.73.250.227	80	7	420 bytes	11	5	294 bytes	2	126 bytes	30.693721	8.9833	261 bi	Filter by
634	184.73.250.227	80	7	420 bytes	12	5	294 bytes	2	126 bytes	30.694101	8.9844	261 bi	Less than
635	184.73.250.227	80	7	420 bytes	13	5	294 bytes	2	126 bytes	30.694478	8.9830	261 bi	Greater than
621	198.66.239.146	80	9	538 bytes	0	6	356 bytes	3	182 bytes	0.000000	14.3434	198 bi	Equal

Conversation Settings

- ☐ Name resolution
- ☐ Absolute start time
- ☐ Limit to display filter

Copy

Follow Stream...

Graph...

Protocol

- ☐ Bluetooth
- ☐ DCCP
- ☐ Ethernet
- ☐ FC
- ☐ FDDI
- ☐ IEEE 802.11
- ☐ IEEE 802.15.4
- ☐ IPv4
- ☐ IPv6
- ☐ IPX
- ☐ JXTA
- ☐ MPTCP
- ☐ NCP
- ☐ openSAFETY
- ☐ RSVP
- ☐ SCTP
- ☒ SLL
- ☒ TCP

Filter list for specific type

TCP - 23

Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s	→ B	Bits/s B → A
3627	141.101.125.193	80	14	9 kB	5	6	753 bytes	8	9 kB	8.655147	0.0554	108	1250 kbps	803 kbps
3643	207.171.187.117	80	122	119 kB	21	38	3 kB	84	116 kB	32.827897	1.1597	20	0 kbps	0 kbps
3642	207.171.187.117	80	127	127 kB	20	41	4 kB	86	123 kB	32.822086	1.5346	19	0 kbps	0 kbps
3641	207.171.187.117	80	85	85 kB	19	27	2 kB	58	83 kB	32.613127	1.2735	15	0 kbps	0 kbps
3644	207.171.187.117	80	56	55 kB	22	18	1 kB	38	53 kB	32.860271	1.2247	9204	0 kbps	0 kbps
3640	207.171.187.117	80	54	49 kB	18	18	2 kB	36	47 kB	32.546263	1.1913	12	0 kbps	0 kbps
3626	141.101.125.193	80	13	9 kB	4	5	699 bytes	8	9 kB	8.654991	1.9666	2843	0 kbps	0 kbps
3623	69.59.180.202	80	22	12 kB	2	10	4 kB	12	9 kB	8.391690	15.0490	1881	0 kbps	0 kbps
3630	184.73.250.227	80	18	5 kB	8	9	2 kB	9	3 kB	28.411827	5.6151	3222	0 kbps	0 kbps
3629	184.73.250.227	80	66	26 kB	7	34	14 kB	32	12 kB	8.677919	25.2886	4492	0 kbps	0 kbps
3625	69.59.180.202	80	16	7 kB	3	8	2 kB	8	5 kB	8.560092	14.8757	1073	0 kbps	0 kbps
3622	198.66.239.146	80	10	1 kB	1	6	745 bytes	4	609 bytes	8.300312	16.0406	371	0 kbps	0 kbps
3628	184.73.250.227	80	6	354 bytes	6	4	228 bytes	2	126 bytes	8.677334	5.7864	315	0 kbps	0 kbps
3636	184.73.250.227	80	7	420 bytes	14	5	294 bytes	2	126 bytes	30.943974	8.7332	269	0 kbps	0 kbps
3637	184.73.250.227	80	7	420 bytes	15	5	294 bytes	2	126 bytes	30.944359	8.7317	269	0 kbps	0 kbps
3638	184.73.250.227	80	7	420 bytes	16	5	294 bytes	2	126 bytes	30.945213	8.7322	269	0 kbps	0 kbps
3639	184.73.250.227	80	7	420 bytes	17	5	294 bytes	2	126 bytes	30.945595	8.7330	269	0 kbps	0 kbps
3631	184.73.250.227	80	7	420 bytes	9	5	294 bytes	2	126 bytes	30.686331	8.9924	261	0 kbps	0 kbps
3632	184.73.250.227	80	7	420 bytes	10	5	294 bytes	2	126 bytes	30.693344	8.9839	261	0 kbps	0 kbps
3633	184.73.250.227	80	7	420 bytes	11	5	294 bytes	2	126 bytes	30.693721	8.9833	261	0 kbps	0 kbps
3634	184.73.250.227	80	7	420 bytes	12	5	294 bytes	2	126 bytes	30.694101	8.9844	261	0 kbps	0 kbps
3635	184.73.250.227	80	7	420 bytes	13	5	294 bytes	2	126 bytes	30.694478	8.9830	261	0 kbps	0 kbps
3621	198.66.239.146	80	9	538 bytes	0	6	356 bytes	3	182 bytes	0.000000	14.3434	198	0 kbps	0 kbps

Filter by

- ☐ Less than
- ☐ Greater than
- ☐ Equal

Enter filter value

- b. What is the total amount of bytes transferred from A to B and from B to A in the most active TCP conversation? (Hint: right-click on the conversation, select **Apply as Filter > Selected > A → B**. Save the packets once the filter is applied) 753 bytes transferred from A to B. 8649 bytes<sup>1</sup> transferred from B to A. For a total of 9402 bytes.[2]

The filter method is marked with red boxes. The result is marked with yellow boxes.

TCP - 23

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Bytes B → A	Bits/s A → B	Bits/s B → A
24.6.173.220	35627	141.101.125.193	80	14	9 kB	5	6	753 bytes	9 kB	108 kbps	1250 kbps
24.6.173.220	35643	207.171.187.117	80	122	119 kB	21	38	3 kB	116 kB	20 kbps	803 kbps
24.6.173.220	35642	207.171.187.117	80	127	127 kB	20	41	4 kB	123 k	Columns to display	0 kbps
24.6.173.220	35641	207.171.187.117	80	85	85 kB	19	27	2 kB	83 k	✓ Address A	1 kbps
24.6.173.220	35644	207.171.187.117	80	56	55 kB	22	18	1 kB	53 k	✓ Port A	9 kbps
24.6.173.220	35640	207.171.187.117	80	54	49 kB	18	18	2 kB	47 k	✓ Address B	3 kbps
24.6.173.220	35626	141.101.125.193	80	13	9 kB	4	5	699 bytes	9 k	✓ Port B	0 kbps
24.6.173.220	35623	69.59.180.202	80	22	12 kB	2	10	4 kB	9 k	✓ Packets	8 bits/s
24.6.173.220	35630	184.73.250.227	80	18	5 kB	8	9	2 kB	3 k	✓ Bytes	5 bits/s
24.6.173.220	35629	184.73.250.227	80	66	26 kB	7	34	14 kB	12 k	✓ Stream ID	0 bits/s
24.6.173.220	35625	69.59.180.202	80	16	7 kB	3	8	2 kB	5 k	✓ Total Packets	5 bits/s
24.6.173.220	35622	198.66.239.146	80	10	1 kB	1	6	745 bytes	609 byte	✓ Percent Filtered	3 bits/s
24.6.173.220	35628	184.73.250.227	80	6	354 bytes	6	4	228 bytes	126 byte	✓ Packets A → B	0 bits/s
24.6.173.220	35636	184.73.250.227	80	7	420 bytes	14	5	294 bytes	126 byte	✓ Bytes A → B	0 bits/s
24.6.173.220	35637	184.73.250.227	80	7	420 bytes	15	5	294 bytes	126 byte	✓ Packets B → A	0 bits/s
24.6.173.220	35638	184.73.250.227	80	7	420 bytes	16	5	294 bytes	126 byte	✓ Bytes B → A	0 bits/s
24.6.173.220	35639	184.73.250.227	80	7	420 bytes	17	5	294 bytes	126 byte	Rel Start	0 bits/s
24.6.173.220	35631	184.73.250.227	80	7	420 bytes	9	5	294 bytes	126 byte	Duration	0 bits/s
24.6.173.220	35632	184.73.250.227	80	7	420 bytes	10	5	294 bytes	126 byte	✓ Bits/s A → B	0 bits/s
24.6.173.220	35633	184.73.250.227	80	7	420 bytes	11	5	294 bytes	126 byte	✓ Bits/s B → A	0 bits/s
24.6.173.220	35634	184.73.250.227	80	7	420 bytes	12	5	294 bytes	126 byte	Filter Bytes B → A by	0 bits/s
24.6.173.220	35635	184.73.250.227	80	7	420 bytes	13	5	294 bytes	126 byte	Less than	0 bits/s
24.6.173.220	35621	198.66.239.146	80	9	538 bytes	0	6	356 bytes	182 byte	Greater than	0 bits/s
										Equal	0 bits/s

Get data in bytes:

<sup>1</sup> I got this result using method mentioned in this question on my Windows 11 computer. It is weird that I can only get '9k bytes' on my macOS computer.

TCP · 23									
Address A	Port A	Address B	Port B	Bytes	Stream ID	Bytes A → B	Bytes B → A	Rate A → B	Rate B → A
24.6.173.220	35627	141.101.125.193	80	9 kB	5	753 bytes		1250 kbp	
24.6.173.220	35643	207.171.187.117	80	119 kB	21	3 kB		803 kbp	
24.6.173.220	35642	207.171.187.117	80	127 kB	20	4 kB		640 kbp	
24.6.173.220	35641	207.171.187.117	80	85 kB	19	2 kB		521 kbp	
24.6.173.220	35640	207.171.187.117	80	49 kB	18	2 kB			
24.6.173.220	35644	207.171.187.117	80	55 kB	22	1 kB			

Related result on clipboard:

```
"24.6.173.220",35627,"141.101.125.193",80,14,9402,5,0,0,6,753,8,8649,8.655147,0.055350000000000676,108834,1250081
```

### c. Calculate the Round-Trip Time (RTT) between A and B by inspecting the TCP Handshake.

Take TCP conversation mentioned in Part1(a) as an example. [6]

1. Set Filter and see the result. The filter method is marked with red boxes. The result is marked with yellow boxes.

TCP · 23									
Address A	Port A	Address B	Port B	Bytes	Stream ID	Bytes A → B	Bytes B → A	Rate A → B	Rate B → A
24.6.173.220	35627	141.101.125.193	80	9 kB					
24.6.173.220	35643	207.171.187.117	80	119 kB					
24.6.173.220	35642	207.171.187.117	80	127 kB					
24.6.173.220	35641	207.171.187.117	80	85 kB					

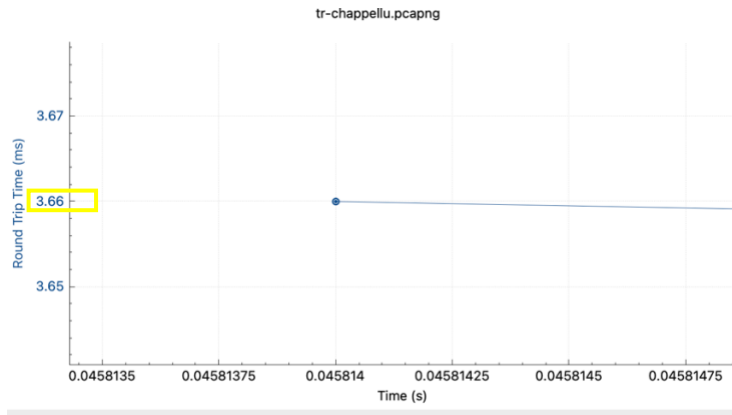
No.	Time	Source	Destination	Protocol	Length	Info
51	8.655147	24.6.173.220	141.101.125.193	TCP		66 35627 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
52	8.675883	141.101.125.193	24.6.173.220	TCP		66 80 → 35627 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=1024
54	8.676020	24.6.173.220	141.101.125.193	TCP		54 35627 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
56	8.676466	24.6.173.220	141.101.125.193	HTTP		471 GET /legacy/graphics/promo/reader_2_728x90.png HTTP/1.1
60	8.695587	141.101.125.193	24.6.173.220	TCP		60 80 → 35627 [ACK] Seq=1 Ack=418 Win=16384 Len=0
61	8.700961	141.101.125.193	24.6.173.220	TCP		1514 80 → 35627 [ACK] Seq=1 Ack=418 Win=16384 Len=1460 [TCP segment of a reassemb
62	8.700972	141.101.125.193	24.6.173.220	TCP		1514 80 → 35627 [ACK] Seq=1461 Ack=418 Win=16384 Len=1460 [TCP segment of a reasse
63	8.704621	24.6.173.220	141.101.125.193	TCP		54 35627 → 80 [ACK] Seq=418 Ack=2921 Win=65700 Len=0
64	8.705626	141.101.125.193	24.6.173.220	TCP		1514 80 → 35627 [ACK] Seq=2921 Ack=418 Win=16384 Len=1460 [TCP segment of a reasse
65	8.705630	141.101.125.193	24.6.173.220	TCP		1514 80 → 35627 [ACK] Seq=4381 Ack=418 Win=16384 Len=1460 [TCP segment of a reasse
66	8.705640	141.101.125.193	24.6.173.220	TCP		1514 80 → 35627 [ACK] Seq=5841 Ack=418 Win=16384 Len=1460 [TCP segment of a reasse
67	8.705643	141.101.125.193	24.6.173.220	HTTP		953 HTTP/1.1 404 Not Found (text/html)
68	8.710054	24.6.173.220	141.101.125.193	TCP		54 35627 → 80 [ACK] Seq=418 Ack=8200 Win=65700 Len=0
69	8.710497	24.6.173.220	141.101.125.193	TCP		54 35627 → 80 [RST, ACK] Seq=418 Ack=8200 Win=0 Len=0

2. According to result in yellow boxes. Calculate time.

time = 8.700961 – 8.655147 = 0.045814

3. Find RTT using statistics. RTT = 3.66ms

Statistics · Telephony · Wireless									
appellu.pcapng									
Info									
1	Packet Lengths	66	35627 → 80	[SYN]	Seq=0	Win=8192	Len=0	MSS=1460	WS=4
2	I/O Graphs	66	80 → 35627	[SYN, ACK]	Seq=0	Ack=1	Win=14600	Len=0	MSS=1460
1	Service Response Time	54	35627 → 80	[ACK]	Seq=1	Ack=1	Win=65700	Len=0	
2	DHCP (BOOTP) Statistics	471	GET /legacy/graphics/promo/reader_2_728x90.png	HTTP/1.1					
2	NetPerfMeter Statistics	60	80 → 35627	[ACK]	Seq=1	Ack=418	Win=16384	Len=0	
1	ONC-RPC Programs	1514	80 → 35627	[ACK]	Seq=1	Ack=418	Win=16384	Len=1460	[TCP segment of a reasse
2	29West	1514	80 → 35627	[ACK]	Seq=1461	Ack=418	Win=16384	Len=1460	[TCP segment of a reasse
2	ANCP	54	35627 → 80	[ACK]	Seq=418	Ack=2921	Win=65700	Len=0	
2	BACnet	1514	80 → 35627	[ACK]	Seq=2921	Ack=418	Win=16384	Len=1460	[TCP segment of a reasse
1	Collectd	1514	80 → 35627	[ACK]	Seq=4381	Ack=418	Win=16384	Len=1460	[TCP segment of a reasse
2	DNS	953	HTTP/1.1 404 Not Found (text/html)						
1	Flow Graph	54	35627 → 80	[ACK]	Seq=418	Ack=8200	Win=65700	Len=0	
1	HART-IP	54	35627 → 80	[RST, ACK]	Seq=418	Ack=8200	Win=0	Len=0	
1	HPFEEDS								
1	HTTP								
1	HTTP2								
1	Sametime								
1	TCP Stream Graphs								
1	UDP Multicast Streams								
1	Reliable Server Pooling (RSerPool)								
1	SOME/IP								
1	F5								
1	IPv4 Statistics								



- d. What are selective acknowledgments? Are they permitted in this conversation? Please justify your answer.

Selective acknowledgments is a sender and receiver side optimization to TCP. It is a mechanism that allows the sender to retransmit only what is missing at the receiver's end, so that the receiver can acknowledge non-consecutive data.[3]

Yes, they permitted. This can be proved by information marked in red boxes.

No.	Time	Source	Destination	Protocol	Length	Info
53	8.675884	141.101.125.193	24.6.173.220	TCP	66	80 → 35626 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=102
54	8.676020	24.6.173.220	141.101.125.193	TCP	54	35627 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
55	8.676063	24.6.173.220	141.101.125.193	TCP	54	35626 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
56	8.676466	24.6.173.220	141.101.125.193	HTTP	471	GET /legacy/graphics/promo/reader_2_728x90.png HTTP/1.1
58	8.677734	24.6.173.220	184.73.250.227	TCP	66	35628 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
59	8.677919	24.6.173.220	184.73.250.227	TCP	66	35629 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
60	8.695587	141.101.125.193	24.6.173.220	TCP	60	80 → 35627 [ACK] Seq=1 Ack=418 Win=16384 Len=0
61	8.700961	141.101.125.193	24.6.173.220	TCP	1514	80 → 35627 [ACK] Seq=1 Ack=418 Win=16384 Len=1460 [TCP segment of a reassembled data stream]
62	8.700972	141.101.125.193	24.6.173.220	TCP	1514	80 → 35627 [ACK] Seq=1461 Ack=418 Win=16384 Len=1460 [TCP segment of a reassembled data stream]
63	8.704621	24.6.173.220	141.101.125.193	TCP	54	35627 → 80 [ACK] Seq=418 Ack=2921 Win=65700 Len=0
64	8.705626	141.101.125.193	24.6.173.220	TCP	1514	80 → 35627 [ACK] Seq=2921 Ack=418 Win=16384 Len=1460 [TCP segment of a reassembled data stream]
65	8.705630	141.101.125.193	24.6.173.220	TCP	1514	80 → 35627 [ACK] Seq=4381 Ack=418 Win=16384 Len=1460 [TCP segment of a reassembled data stream]
66	8.705640	141.101.125.193	24.6.173.220	TCP	1514	80 → 35627 [ACK] Seq=5841 Ack=418 Win=16384 Len=1460 [TCP segment of a reassembled data stream]
67	8.705643	141.101.125.193	24.6.173.220	HTTP	953	HTTP/1.1 404 Not Found (text/html)
68	8.710054	24.6.173.220	141.101.125.193	TCP	54	35627 → 80 [ACK] Seq=418 Ack=8200 Win=65700 Len=0
69	8.710497	24.6.173.220	141.101.125.193	TCP	54	35627 → 80 [RST, ACK] Seq=418 Ack=8200 Win=0 Len=0
70	8.772282	184.73.250.227	24.6.173.220	TCP	66	80 → 35629 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM WS=256

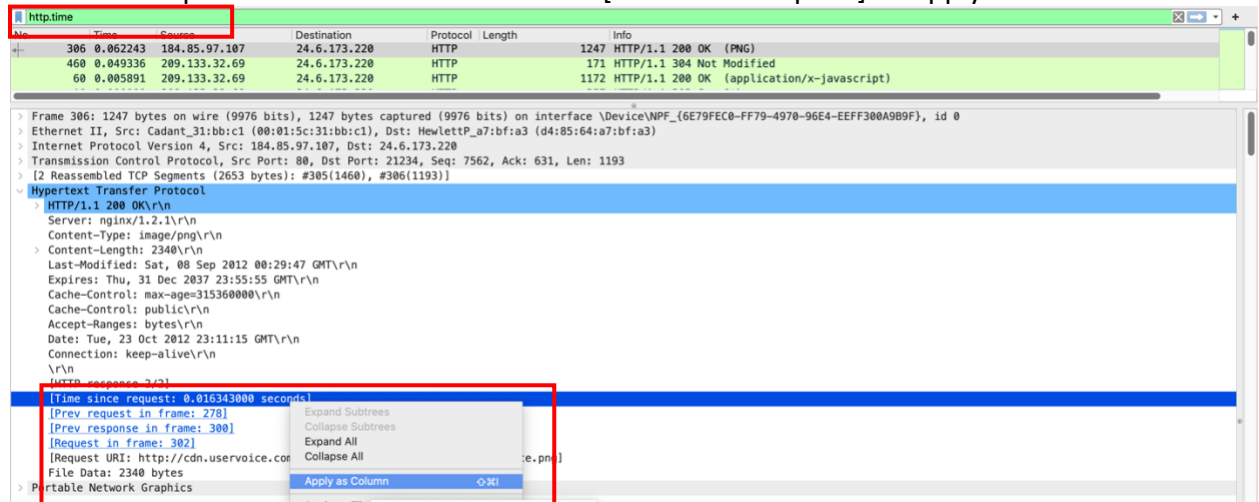
1000	.... = Header Length: 32 bytes (8)	0000	00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45
> Flags:	0x002 (SYN)	0010	00 34 29 99 40 00 00 06 00 00 18 06 ad dc b8
Window:	8192	0020	fa e3 8b 2d 00 50 3f 97 e1 9d 00 00 00 00 80
[Calculated window size:	8192]	0030	20 00 79 36 00 00 02 04 05 b4 01 03 03 02 01
Checksum:	0x7936 [unverified]	0040	04 02
[Checksum Status:	Unverified]		
Urgent Pointer:	0		
Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP)			
> TCP Option - Maximum segment size: 1460 bytes			
> TCP Option - No-Operation (NOP)			
> TCP Option - Window scale: 2 (multiply by 4)			
> TCP Option - No-Operation (NOP)			
> TCP Option - No-Operation (NOP)			
> TCP Option - SACK permitted			
Kind: SACK Permitted (4)			
Length: 2			
> [Timestamps]			

## Part 2: tr-http-pcapnet.pcapng

- a. Use a filter to display the HTTP response time for each HTTP request.



1. Use filter 'http.time'. Select one row and click [Time since request] -> 'Apply as Column'



2. Then you can see results in 'Times since request' column.

The screenshot shows the Wireshark interface with the 'Times since request' column added to the packet list. The column contains values representing the time since the request for each packet. The values are highlighted in yellow in the original image.

No.	Time	Source	Destination	Protocol	Length	Time since request	Info
306	0.062243	184.85.97.107	24.6.173.220	HTTP	1247	0.016343000	HTTP/1.1 200 OK (PNG)
460	0.049336	209.133.32.69	24.6.173.220	HTTP	171	0.019483000	HTTP/1.1 304 Not Modified
60	0.005891	209.133.32.69	24.6.173.220	HTTP	1172	0.022387000	HTTP/1.1 200 OK (application/javascript)
10	0.000000	209.133.32.69	24.6.173.220	HTTP	357	0.026416000	HTTP/1.1 303 See Other
264	0.004740	173.194.79.82	24.6.173.220	HTTP	1265	0.039248000	HTTP/1.1 200 OK
275	0.015879	173.194.79.82	24.6.173.220	HTTP	1156	0.039559000	HTTP/1.1 200 OK
300	0.023501	184.85.97.107	24.6.173.220	HTTP	315	0.039826000	HTTP/1.1 200 OK (application/javascript)
285	0.015856	173.194.79.82	24.6.173.220	HTTP	1072	0.040068000	HTTP/1.1 200 OK
291	0.005978	173.194.79.82	24.6.173.220	HTTP	1290	0.041366000	HTTP/1.1 200 OK
472	0.060336	173.194.79.82	24.6.173.220	HTTP	1028	0.041555000	HTTP/1.1 200 OK
473	0.001666	173.194.79.82	24.6.173.220	HTTP	484	0.042814000	HTTP/1.1 200 OK
474	0.000003	173.194.79.82	24.6.173.220	HTTP	917	0.043575000	HTTP/1.1 200 OK
327	0.028524	173.194.79.82	24.6.173.220	HTTP	1120	0.044075000	HTTP/1.1 200 OK
467	0.033683	173.194.79.82	24.6.173.220	HTTP	492	0.044714000	HTTP/1.1 200 OK
270	0.000976	173.194.79.82	24.6.173.220	HTTP	770	0.044871000	HTTP/1.1 200 OK
330	0.001224	173.194.79.82	24.6.173.220	HTTP	799	0.045642000	HTTP/1.1 200 OK
213	0.013052	173.194.79.82	24.6.173.220	HTTP	74	0.045645000	HTTP/1.1 200 OK (text/plain)
111	0.073779	209.133.32.69	24.6.173.220	HTTP	90	0.045771000	HTTP/1.1 200 OK (PNG)
144	0.017508	173.194.79.82	24.6.173.220	HTTP	1423	0.048456000	HTTP/1.1 200 OK (text/css)
252	0.008247	173.194.79.82	24.6.173.220	HTTP	526	0.055420000	HTTP/1.1 200 OK
229	0.017477	173.194.79.82	24.6.173.220	HTTP	96	0.059737000	HTTP/1.1 200 OK
233	0.001051	173.194.79.82	24.6.173.220	HTTP	524	0.059962000	HTTP/1.1 200 OK
267	0.003922	173.194.79.82	24.6.173.220	HTTP	554	0.061540000	HTTP/1.1 200 OK
165	0.000002	173.194.79.82	24.6.173.220	HTTP	750	0.069426000	HTTP/1.1 200 OK (text/css)
164	0.021326	173.194.79.82	24.6.173.220	HTTP	90	0.070623000	HTTP/1.1 200 OK (text/plain)
483	2.162666	209.133.32.69	24.6.173.220	HTTP	1173	0.073502000	HTTP/1.1 200 OK (text/html)
412	0.909854	209.133.32.69	24.6.173.220	HTTP	1173	0.075087000	HTTP/1.1 200 OK (text/html)
260	0.001008	173.194.79.82	24.6.173.220	HTTP	893	0.084204000	HTTP/1.1 200 OK
185	0.006844	173.194.79.82	24.6.173.220	HTTP	1391	0.087146000	HTTP/1.1 200 OK (text/css)
202	0.005311	173.194.79.82	24.6.173.220	HTTP	850	0.087638000	HTTP/1.1 200 OK (text/plain)
257	0.014255	173.194.79.82	24.6.173.220	HTTP	1171	0.088422000	HTTP/1.1 200 OK
217	0.018109	173.194.79.82	24.6.173.220	HTTP	472	0.117898000	HTTP/1.1 200 OK (text/plain)
427	5.894745	209.133.32.69	24.6.173.220	HTTP	1173	0.123874000	HTTP/1.1 200 OK (text/html)
246	0.011890	209.133.32.69	24.6.173.220	HTTP	500	0.158562000	HTTP/1.1 200 OK (PNG)
347	0.010756	173.194.79.82	24.6.173.220	HTTP	75	0.173648000	HTTP/1.1 200 OK
52	1.894592	209.133.32.69	24.6.173.220	HTTP	1457	1.866336000	HTTP/1.1 200 OK (text/html)
450	1.386918	209.133.32.69	24.6.173.220	HTTP	764	1.987546000	HTTP/1.1 200 OK (text/html)

## b. Define and explain the significance of each HTTP response status code.

200 OK: The request succeeded.

303 See Other: The server sent this response to direct the client to get the requested resource at another URI with a GET request.

304 Not Modified: This is used for caching purposes. It tells the client that the response has not been modified, so the client can continue to use the same cached version of the response.[4]

Each HTTP response status code is marked in the picture in Part2(a) in yellow box.

- c. Apply a filter that lists packets wherein the HTTP response time is greater than one second.

Use filter 'http.time>1' based on Part2(a) [5]

http.time > 1							
No.	Time	Source	Destination	Protocol	Length	Time since request	Info
52	0.000000	209.133.32.69	24.6.173.220	HTTP	1457	1.866336000	HTTP/1.1 200 OK (text/html)
450	18.580866	209.133.32.69	24.6.173.220	HTTP	764	1.987546000	HTTP/1.1 200 OK (text/html)

## Part 3: tr-http-pcaprnet.pcapng

- a. Use a filter to display the FTP request and response packets.

Use filter 'ftp'

ftp							[X] [Left Arrow] [Right Arrow] +	
No.	Time	Source	Destination	Protocol	Length	Info		
4	0.960308	78.41.115.130	192.168.1.72	FTP		95 Response: 220 anga.funkfeuer.at FTP server ready.		
6	14.371553	192.168.1.72	78.41.115.130	FTP		65 Request: USER fred		
7	14.576704	78.41.115.130	192.168.1.72	FTP		84 Response: 530 User fred access denied.		
9	23.202885	192.168.1.72	78.41.115.130	FTP		66 Request: USER marty		
10	23.391590	78.41.115.130	192.168.1.72	FTP		85 Response: 530 User marty access denied.		
12	27.722470	192.168.1.72	78.41.115.130	FTP		60 Request: QUIT		
13	27.910753	78.41.115.130	192.168.1.72	FTP		68 Response: 221 Goodbye.		

- b. List the server and client IP addresses and port numbers.

	IP address	Port number
server	78.41.115.130	21
client	192.168.1.72	39322

- c. Use another filter to display only the FTP response codes for the packets.

Define and explain the significance of the response codes.

Use filter 'ftp.response.code'

ftp.response.code						
No.	Time	Source	Destination	Protocol	Length	Info
4	0.960308	78.41.115.130	192.168.1.72	FTP		95 Response: 220 anga.funkfeuer.at FTP server ready.
13	27.910753	78.41.115.130	192.168.1.72	FTP		68 Response: 221 Goodbye.
10	23.391590	78.41.115.130	192.168.1.72	FTP		85 Response: 530 User marty access denied.
7	14.576704	78.41.115.130	192.168.1.72	FTP		84 Response: 530 User fred access denied.

Select one row. Find Response Code, click 'Apply as Column'

ftp.response.code							
No.	Time	Source	Destination	Protocol	Length	Info	
4	0.960308	78.41.115.130	192.168.1.72	FTP		95 Response: 220 anga.funkfeuer.at FTP server ready.	
13	27.910753	78.41.115.130	192.168.1.72	FTP		68 Response: 221 Goodbye.	
10	23.391590	78.41.115.130	192.168.1.72	FTP		85 Response: 530 User marty access denied.	
7	14.576704	78.41.115.130	192.168.1.72	FTP		84 Response: 530 User fred access denied.	

> Frame 4: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface \Device\NPF\_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}, id 0  
 > Ethernet II, Src: PaceAmer\_11:e2:b9 (ac:5d:10:11:e2:b9), Dst: HewlettP\_7:bf:a3 (d4:85:64:a7:bf:a3)  
 > Internet Protocol Version 4, Src: 78.41.115.130, Dst: 192.168.1.72  
 > Transmission Control Protocol, Src Port: 21, Dst Port: 39322, Seq: 1, Ack: 1, Len: 41  
 > File Transfer Protocol (FTP)  
 > 220 anga.funkfeuer.at FTP server ready.\r\n

Response code: Service  
 Response arg: anga.funk  
 [Current working directory: ]

Expand Subtrees  
 Collapse Subtrees  
 Expand All  
 Collapse All  
 Apply as Column

See the column 'Response Code' as a result.

ftp.response.code							
No.	Time	Source	Destination	Protocol	Length	Response code	Info
4	0.960308	78.41.115.130	192.168.1.72	FTP		95 Service ready for new user	Response: 220 anga.funkfeuer.at FTP server ready.
13	27.910753	78.41.115.130	192.168.1.72	FTP		68 Service closing control connection	Response: 221 Goodbye.
10	23.391590	78.41.115.130	192.168.1.72	FTP		85 Not logged in	Response: 530 User marty access denied.
7	14.576704	78.41.115.130	192.168.1.72	FTP		84 Not logged in	Response: 530 User fred access denied.

220 Service ready for new user: The server sent this code to a new user that the server is ready to connect new clients.

221 Goodbye: Service closing control connection

530 Not logged in: The code is sent to respond to requests/commands from user to log-in before commands is executed.

**d. Is the FTP termination initiated by server or client? Please justify your answer.**

FTP termination initiated by client according to the picture below. The client send request to quit first. Then server respond to quit request.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.960308	78.41.115.130	192.168.1.72	FTP	95	Response: 220 anga.funkfeuer.at FTP server ready.
6	14.371553	192.168.1.72	78.41.115.130	FTP	65	Request: USER fred
7	14.576704	78.41.115.130	192.168.1.72	FTP	84	Response: 530 User fred access denied.
9	23.202885	192.168.1.72	78.41.115.130	FTP	66	Request: USER marty
10	23.391590	78.41.115.130	192.168.1.72	FTP	85	Response: 530 User marty access denied.
12	27.722470	192.168.1.72	78.41.115.130	FTP	60	Request: QUIT
13	27.910753	78.41.115.130	192.168.1.72	FTP	68	Response: 221 Goodbye.

**e. How secure is FTP?**

FTP is not secure because it relies on plain text without encryption.

## Part 4: tr-bootp.pcapng

**a. What layer of the OSI model can DHCP Discover packets be found? What type of packet is DHCP Discover? List the source and destination IP addresses and port numbers.**

Application Layer.

DHCP Discover is UDP broadcast packet which source IP address is 0.0.0.0 and destination IP address is 255.255.255.255 or the specific subnet broadcast address.

For DHCP Discover:

	IP address	Port number
source	0.0.0.0	68
destination	255.255.255.255	67

2	5.166954	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xa69b8b3f
3	6.194089	192.168.1.254	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xa69b8b3f
4	6.195104	0.0.0.0	255.255.255.255	DHCP	348	DHCP Request - Transaction ID 0xa69b8b3f
5	6.224160	192.168.1.254	192.168.1.72	DHCP	347	DHCP ACK - Transaction ID 0xa69b8b3f
6	9.283405	192.168.1.72	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xa6234b6

Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF\_{6E79FEC0-FF79-4970-96E4-EFF300A9B9F}, id 0

Ethernet II, Src: HewlettP a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

User Datagram Protocol, Src Port: 68, Dst Port: 67

Dynamic Host Configuration Protocol (Discover)

**b. How many DHCP packets are exchanged between the client and server before the client receives an IP address? Define and explain the commands used in the DHCP handshake.**

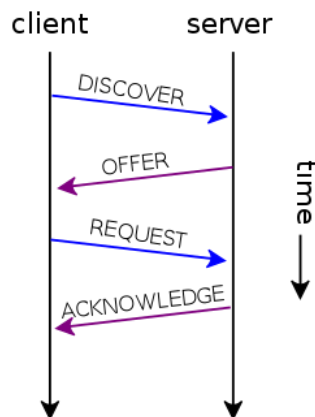
4 DHCP packets.

Discover: DHCP client broadcasts a DHCPDISCOVER message on the network subnet to discover DHCP available server.

Offer: DHCP server reserves an IP address for the client and makes a lease offer by sending a DHCPOFFER message to the client.

Request: DHCP client replies with a DHCPREQUEST message, broadcast to the server, requesting the offered address, in response to the DHCP offer.

ACK: DHCP server acknowledge the request, sending a DHCPACK packet with lease duration and other configuration information to the client.



**c. What is the significance of DHCP Release packet?**

DHCP Release packet is a message sent by a DHCP client to DHCP server to release IP address that was previously assigned to it. DHCP Release packet is significant because it allows the DHCP server to reclaim the IP address and make it available for other clients.

**d. Explain the communication flow between a DHCP client and server on a network that has two DHCP servers.**

When a DHCP client sends a discover message requesting an IP address, both DHCP servers on the network receive the request. Client will use the first server to respond with an offer message. The client then sends a request message to the server which made the offer, indicating that it has accepted the offer. The server then sends an ACK message to the client, confirming that the IP address has been assigned.

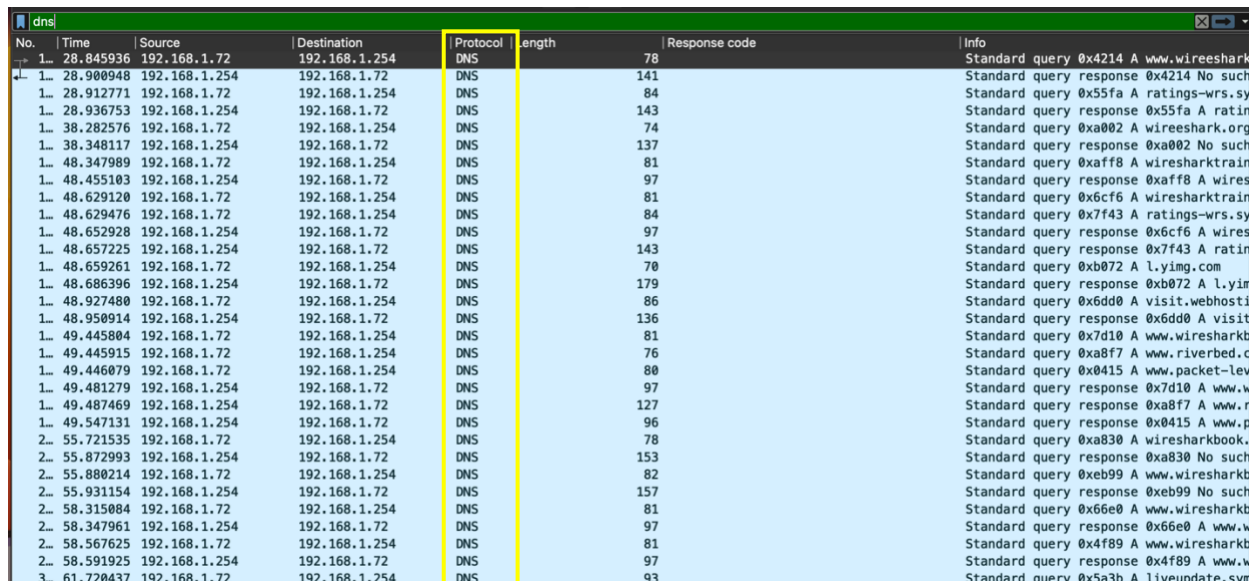
Once the client has received ACK message with IP address, it will continue to use that address until its lease expires or it sends a release message.



## Part 5: tr-bootp.pcapng

- a. Use a filter to display DNS traffic only.

Use filter 'dns'

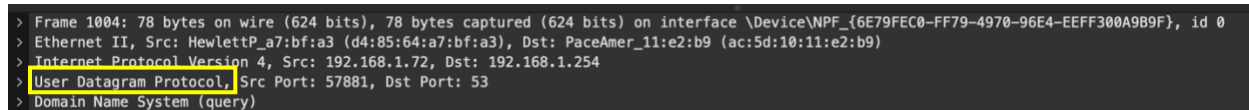


A screenshot of the Wireshark packet list window with the filter 'dns' applied. The list shows 31 packets, all of which are DNS queries. The columns displayed are No., Time, Source, Destination, Protocol, Length, Response code, and Info. The 'Protocol' column is highlighted in yellow. The 'Info' column shows details like 'Standard query 0x4214 A www.wireeshark.org'.

No.	Time	Source	Destination	Protocol	Length	Response code	Info
1	28.845936	192.168.1.72	192.168.1.254	DNS	78		Standard query 0x4214 A www.wireeshark.org
2	28.900948	192.168.1.254	192.168.1.72	DNS	141		Standard query response 0x4214 No such name A www.wireeshark.org SOA a0.org.afiliastest.info
3	28.912771	192.168.1.72	192.168.1.254	DNS	84		Standard query 0x55fa A ratings-wrs.symantec.com
4	28.936753	192.168.1.254	192.168.1.72	DNS	143		Standard query response 0x55fa A ratings-wrs.symantec.com CNAME ratings-wrs.symantec.com
5	38.282576	192.168.1.72	192.168.1.254	DNS	74		Standard query 0xa002 A wireeshark.org
6	38.348117	192.168.1.254	192.168.1.72	DNS	137		Standard query response 0xa002 No such name A wireeshark.org SOA a0.org.afiliastest.info
7	48.347989	192.168.1.72	192.168.1.254	DNS	81		Standard query 0xa002 A wireeshark.org
8	48.455103	192.168.1.254	192.168.1.72	DNS	97		Standard query response 0xa002 No such name A wireeshark.org SOA a0.org.afiliastest.info
9	48.629120	192.168.1.72	192.168.1.254	DNS	81		Standard query 0xa002 A wireeshark.org
10	48.629476	192.168.1.254	192.168.1.72	DNS	84		Standard query response 0xa002 No such name A wireeshark.org SOA a0.org.afiliastest.info
11	48.652928	192.168.1.254	192.168.1.72	DNS	97		Standard query response 0xa002 No such name A wireeshark.org SOA a0.org.afiliastest.info
12	48.657225	192.168.1.254	192.168.1.72	DNS	143		Standard query response 0xa002 No such name A wireeshark.org SOA a0.org.afiliastest.info
13	48.659261	192.168.1.72	192.168.1.254	DNS	70		Standard query 0xb072 A l.yimg.com
14	48.686396	192.168.1.254	192.168.1.72	DNS	179		Standard query response 0xb072 A l.yimg.com
15	48.927480	192.168.1.72	192.168.1.254	DNS	86		Standard query 0xb072 A l.yimg.com
16	48.950914	192.168.1.254	192.168.1.72	DNS	136		Standard query response 0xb072 A l.yimg.com
17	49.445804	192.168.1.72	192.168.1.254	DNS	81		Standard query 0xb072 A l.yimg.com
18	49.445915	192.168.1.254	192.168.1.72	DNS	76		Standard query response 0xb072 A l.yimg.com
19	49.446079	192.168.1.72	192.168.1.254	DNS	80		Standard query 0xb072 A l.yimg.com
20	49.481279	192.168.1.254	192.168.1.72	DNS	97		Standard query response 0xb072 A l.yimg.com
21	49.487469	192.168.1.72	192.168.1.254	DNS	127		Standard query response 0xb072 A l.yimg.com
22	49.547131	192.168.1.254	192.168.1.72	DNS	96		Standard query response 0xb072 A l.yimg.com
23	55.721535	192.168.1.72	192.168.1.254	DNS	78		Standard query 0xa830 A wireeshark.org
24	55.872993	192.168.1.254	192.168.1.72	DNS	153		Standard query response 0xa830 No such name A wireeshark.org SOA a0.org.afiliastest.info
25	55.880214	192.168.1.72	192.168.1.254	DNS	82		Standard query 0xb072 A l.yimg.com
26	55.931154	192.168.1.254	192.168.1.72	DNS	157		Standard query response 0xb072 A l.yimg.com
27	58.315084	192.168.1.72	192.168.1.254	DNS	81		Standard query 0xb072 A l.yimg.com
28	58.347961	192.168.1.254	192.168.1.72	DNS	97		Standard query response 0xb072 A l.yimg.com
29	58.567625	192.168.1.72	192.168.1.254	DNS	81		Standard query 0xb072 A l.yimg.com
30	58.591925	192.168.1.254	192.168.1.72	DNS	97		Standard query response 0xb072 A l.yimg.com
31	61.720437	192.168.1.72	192.168.1.254	DNS	93		Standard query 0x5a3b A liveupdate.symantec.com

- b. Which transport layer protocol is used for DNS queries?

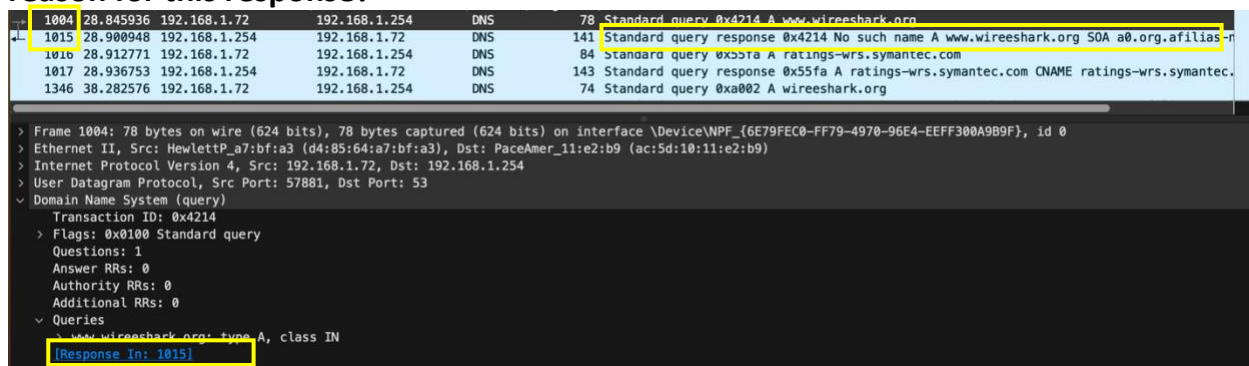
UDP



A screenshot of the Wireshark packet details window for packet 1004. The 'User Datagram Protocol' section is expanded, showing 'Src Port: 57881, Dst Port: 53'. The 'Domain Name System (query)' section is also expanded, showing 'Transaction ID: 0x4214'.

Frame	Time	Source	Destination	Protocol	Length	Response code	Info
1004	28.845936	192.168.1.72	192.168.1.254	DNS	78		Standard query 0x4214 A www.wireeshark.org

- c. What is the response for the DNS query of packet number 1004? What is the reason for this response?



A screenshot of the Wireshark packet details window for packet 1015. The 'Domain Name System (query)' section is expanded, showing 'Transaction ID: 0x4214' and 'Flags: 0x0100 Standard query'. The 'Answers' section is also expanded, showing 'No such name A www.wireeshark.org SOA a0.org.afiliastest.info'.

Frame	Time	Source	Destination	Protocol	Length	Response code	Info
1004	28.845936	192.168.1.72	192.168.1.254	DNS	78		Standard query 0x4214 A www.wireeshark.org
1015	28.900948	192.168.1.254	192.168.1.72	DNS	141		Standard query response 0x4214 No such name A www.wireeshark.org SOA a0.org.afiliastest.info
1016	28.912771	192.168.1.72	192.168.1.254	DNS	84		Standard query 0x55fa A ratings-wrs.symantec.com
1017	28.936753	192.168.1.254	192.168.1.72	DNS	143		Standard query response 0x55fa A ratings-wrs.symantec.com CNAME ratings-wrs.symantec.com
1346	38.282576	192.168.1.72	192.168.1.254	DNS	74		Standard query 0xa002 A wireeshark.org

Find response in 1015. The response is 'no such name'. The reason is marked in the picture above. 'No such name A www.wireeshark.org SOA a0.org.afiliastest.info'.

## Reference

- [1] Wireshark User's Guide: Version 3.5.1
- [2] <https://ask.wireshark.org/question/14573/how-do-i-see-statisticsconversationsbytes-values-in-full-rather-than-abbreviated-as-n-k/>
- [3] <https://www.geeksforgeeks.org/selective-acknowledgments-sack-in-tcp/>
- [4] <https://developer.mozilla.org/en-US/docs/Web/HTTP/Status>
- [5] <https://www.youtube.com/watch?v=FMRI6ua2MjE>
- [6] Discuss this Question with Jiaran Liu
- [7] [https://en.wikipedia.org/wiki/Dynamic\\_Host\\_Configuration\\_Protocol](https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol)