# Data Networks WS 18/19

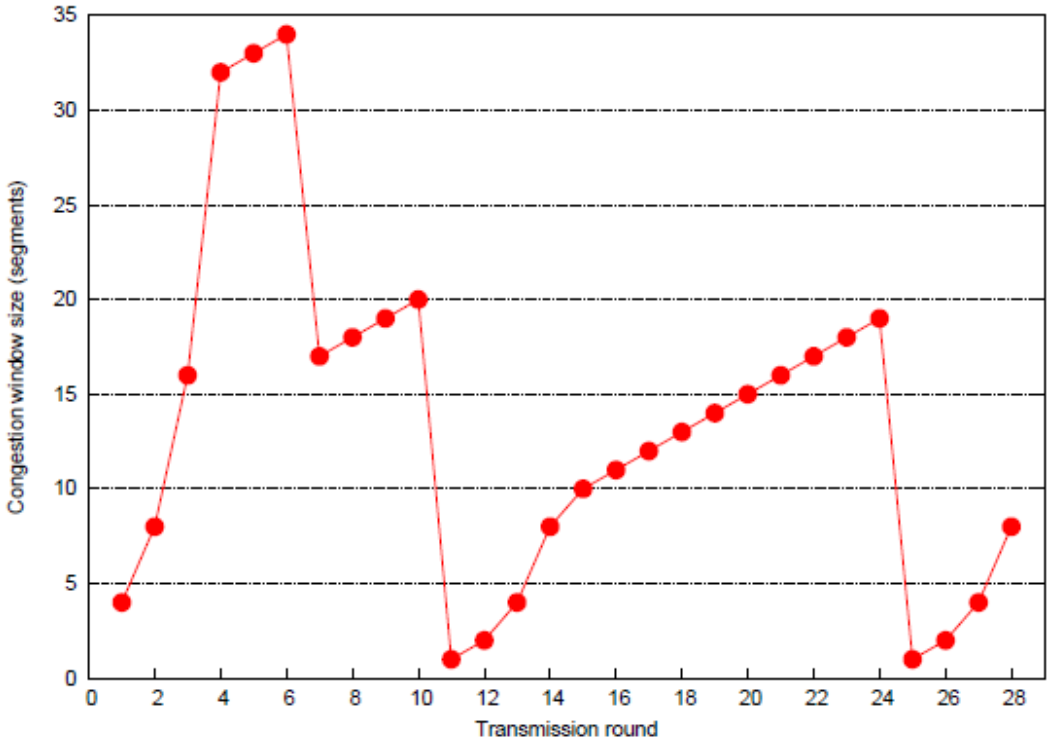
# INTERNET ARCHITECTURE:

## Assignment 5

Chirag Bhuvaneshwara - 2571703

Florena Raja – 2566418

Question 1: TCP congestion window size




(a) What is the size of the window in the first transmission round?

The size of the window is 4, as we can see that in the first transmission round, packets worth window size 4 are transmitted.

(b) Identify the time intervals when TCP slow start is operating.

Slow start is operating in the following range of transmission rounds: 1-4, 11-14 & 25-28. Here, the window size is increased exponentially i.e after each of the transmission rounds in the slow start interval, the congestion window size is doubled. This is done in order to increase the throughput as much as possible and quickly find the point where packet loss occurs or if within the threshold, switch to congestion avoidance mode.

(c) Identify the time intervals when TCP congestion avoidance is used.

Congestion avoidance is used in the following range of transmission rounds: 4-6, 7-10 & 15-24. Here, the window size is increased linearly. This linear increase is started once the exponential increase in the congestion window size is not possible as it goes above the threshold.

Basically, there is exponential increase till we reach the threshold and this is followed by congestion avoidance provided there is no packet loss.

(d) After the 6th transmission round, is the segment loss detected by a triple duplicate acknowledgment or by a timeout?

Congestion avoidance takes effect in TCP Reno only when there are dup acks, but not with time out. In the graph after $6^{th}$ transmission round TCP shifts to congestion avoidance, therefore loss segment is detected by triple dup acks.

(e) After the 10th transmission round, is the segment loss detected by a triple duplicate acknowledgment or by a timeout?

Here the segment loss is detected by timeout, as we can see that the congestion window size is reset to 1 i.e CWND=1 which means that TCP Reno is again back in slow start.

(f) What is the initial value of Threshold at the first transmission round?

Threshold = 32. This is because congestion avoidance begins when the threshold is reached and that only happens at 4th transmission round when CWND = Threshold = 32. So the threshold is 32 for all transmission rounds from 1 to 4.

(g) What is the value of Threshold at the 8th transmission round?

Threshold at 8th transmission round = 34/2 = 17. Till 4th transmission round threshold is 32 as described in (f). At transmission round 6, packet loss is detected due to 3 Duplicate ACKs and threshold is set to CWND/2 i.e 34/2 = 17.

(h) What is the value of Threshold at the 12th transmission round?

Threshold at 12th transmission round = 20/2 = 10. Since CWND at 10th transmission round was 20 and since timeout occurred at 10th transmission round, threshold is set to CWND/2 = 20/2 = 10. Threshold is not updated till congestion avoidance starts and ends in the 24th transmission round => threshold is 10 at 12th transmission round.

(i) During which transmission round is the 30th segment sent?

30th segment sent in 4th transmission round. In transmission rounds of 1,2,3,4 the no. of segments sent are: 4, 8, 16 and 32 respectively. Total segments sent at the end of 3rd transmission round = 4+8+16 = 28 segments. Therefore, 30th segment sent among the 32 segments in the 4th transmission round.

(j) Assuming a packet loss is detected after the 28th round by the reception of a triple duplicate acknowledgement, what will be the values of the congestion window size and Threshold?

At 28th transmission round, CWND = 8.

The updated entries after reception of triple duplicate ACKs:

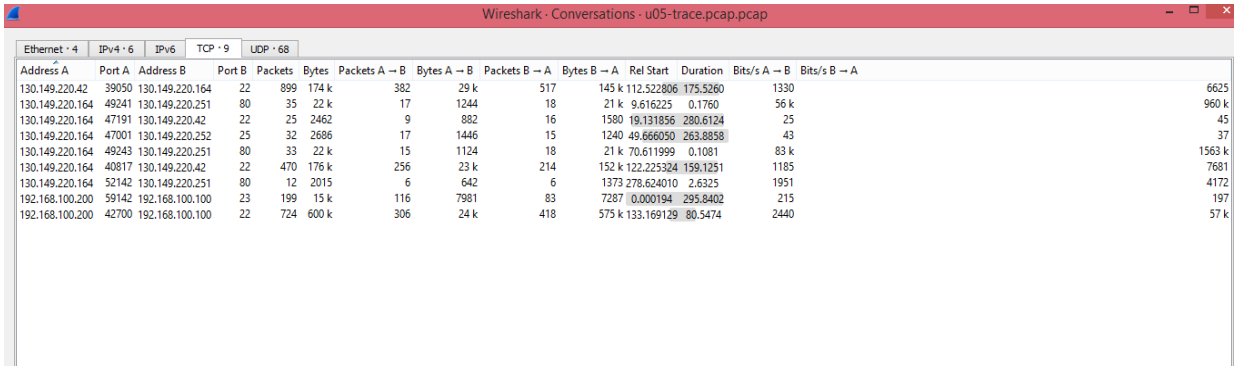
New congestion window size = 8/2 = 4, threshold = CWND/2 = 8/2 = 4

Question 2: TCP connections

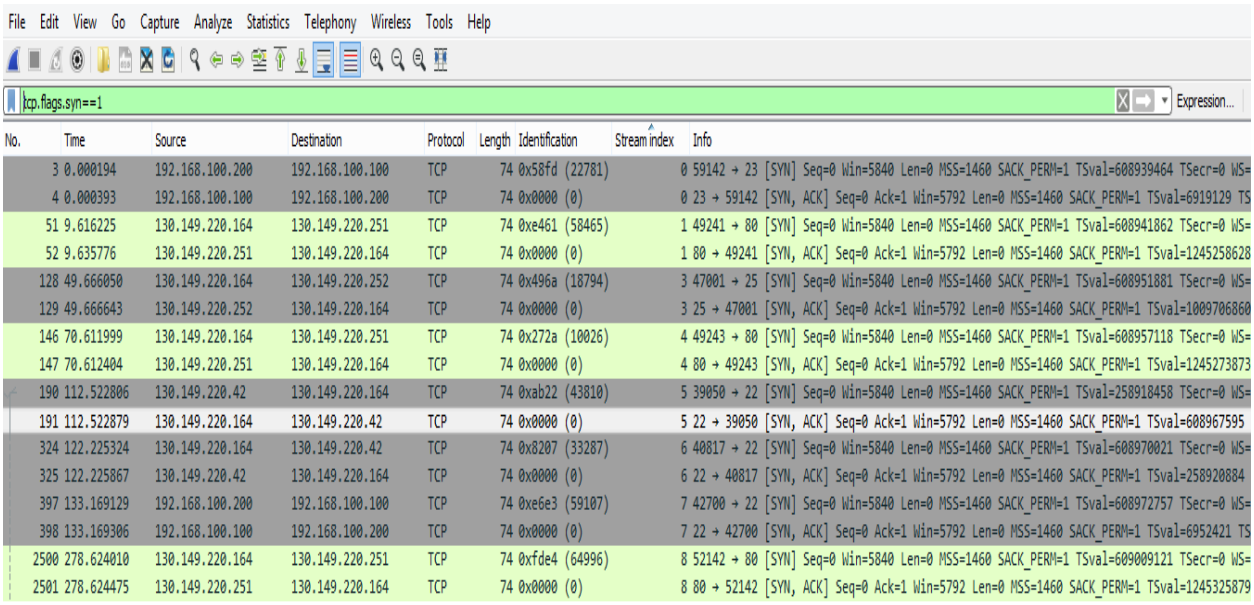
a) 9 , TCP connections are at least in part contained in the trace.

Information gotten from Statistics tab and then the conversations option.

From statistics-> conversations.



b) Filter : tcp.flags.syn==1; filtered applied to get the first TCP connection.




| No. | Time | Source | Destination | Protocol | Length | Identification | Stream index | Info |
|---|---|---|---|---|---|---|---|---|
| 3 | 0.000194 | 192.168.100.200 | 192.168.100.100 | TCP | 74 | 0x58fd (22781) | 0 | 59142 → 23 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=608939464 TSecr=0 WS= |
| 4 | 0.000393 | 192.168.100.100 | 192.168.100.200 | TCP | 74 | 0x0000 (0) | 0 | 23 → 59142 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=6919129 TS |
| 51 | 9.616225 | 130.149.220.164 | 130.149.220.251 | TCP | 74 | 0xe461 (58465) | 1 | 49241 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=608941862 TSecr=0 WS= |
| 52 | 9.635776 | 130.149.220.251 | 130.149.220.164 | TCP | 74 | 0x0000 (0) | 1 | 80 → 49241 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=1245258628 |
| 128 | 49.666050 | 130.149.220.164 | 130.149.220.252 | TCP | 74 | 0x496a (18794) | 3 | 47001 → 25 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=608951881 TSecr=0 WS= |
| 129 | 49.666643 | 130.149.220.252 | 130.149.220.164 | TCP | 74 | 0x0000 (0) | 3 | 25 → 47001 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=1009706860 |
| 146 | 70.611999 | 130.149.220.164 | 130.149.220.251 | TCP | 74 | 0x272a (10026) | 4 | 49243 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=608957118 TSecr=0 WS= |
| 147 | 70.612404 | 130.149.220.251 | 130.149.220.164 | TCP | 74 | 0x0000 (0) | 4 | 80 → 49243 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=1245273873 |
| 190 | 112.522806 | 130.149.220.42 | 130.149.220.164 | TCP | 74 | 0xab22 (43810) | 5 | 39050 → 22 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=258918458 TSecr=0 WS= |
| 191 | 112.522879 | 130.149.220.164 | 130.149.220.42 | TCP | 74 | 0x0000 (0) | 5 | 22 → 39050 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=608967595 |
| 324 | 122.225324 | 130.149.220.164 | 130.149.220.42 | TCP | 74 | 0x8207 (33287) | 6 | 40817 → 22 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=608970021 TSecr=0 WS= |
| 325 | 122.225867 | 130.149.220.42 | 130.149.220.164 | TCP | 74 | 0x0000 (0) | 6 | 22 → 40817 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=258920884 |
| 397 | 133.169129 | 192.168.100.200 | 192.168.100.100 | TCP | 74 | 0xe6e3 (59107) | 7 | 42700 → 22 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=608972757 TSecr=0 WS= |
| 398 | 133.169306 | 192.168.100.100 | 192.168.100.200 | TCP | 74 | 0x0000 (0) | 7 | 22 → 42700 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=6952421 TS |
| 2500 | 278.624010 | 130.149.220.164 | 130.149.220.251 | TCP | 74 | 0xfde4 (64996) | 8 | 52142 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=609009121 TSecr=0 WS= |
| 2501 | 278.624475 | 130.149.220.251 | 130.149.220.164 | TCP | 74 | 0x0000 (0) | 8 | 80 → 52142 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=1245325879 |

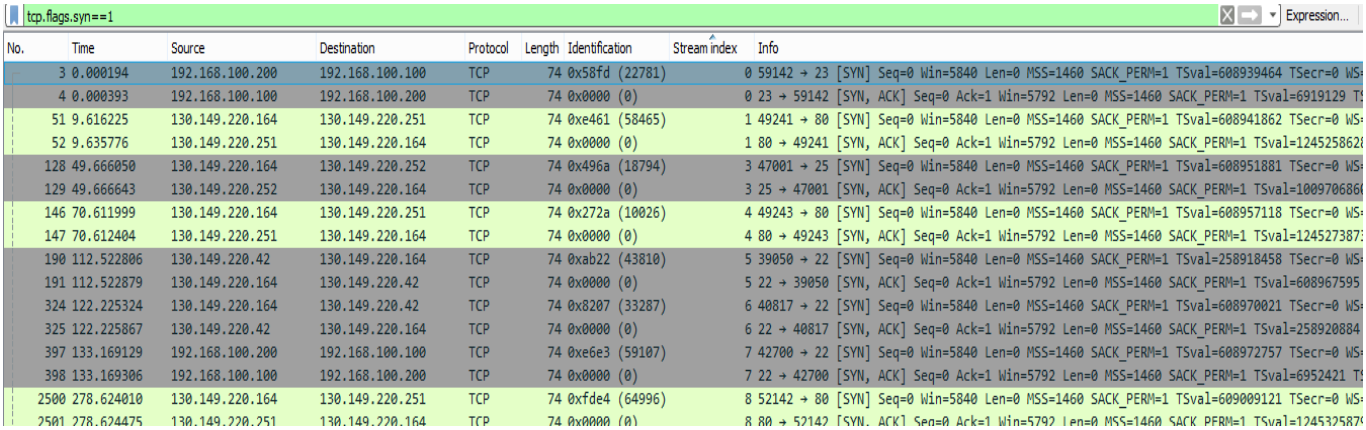
| Stream Index | source IP | destination IP | conn. start | conn. end | Display filter |
|---|---|---|---|---|---|
| 0 | 192.168.100.200 | 192.168.100.100 | 0.000194 | 0.000393 | tcp.flags.syn==1 |

c ) Using the Follow TCP Stream analyzer one can obtain the stream index under the TCP section. The stream index can be set as a column to view all the stream indices.

Later using tcp.stream eq interger display filter we can filter out TCP connection with the stream indices also with tcp.flags.syn==1.

Also with column stream index, it can be sorted in ascending order.

In the given trace the indices range from 0-8.




| Stream Index | source IP | destination IP | conn. start | conn. end |
|---|---|---|---|---|
| 0 | 192.168.100.200 | 192.168.100.100 | 0.000194 | 295.840417 |
| 1 | 130.149.220.164 | 130.149.220.251 | 9.616225 | 9.792222 |
| 2 | 130.149.220.42 | 130.149.220.164 | 19.132343 | 299.744244 |
| 3 | 130.149.220.164 | 130.149.220.252 | 49.666050 | 313.5518888 |
| 4 | 130.149.220.164 | 130.149.220.25 | 70.611999 | 70.719710 |
| 5 | 130.149.220.42 | 130.149.220.164 | 112.522806 | 288.048851 |
| 6 | 130.149.220.164 | 130.149.220.42 | 122.225324 | 281.350445 |
| 7 | 192.168.100.200 | 192.168.100.100 | 133.169129 | 213.716505 |
| 8 | 130.149.220.164 | 130.149.220.251 | 278.624010 | 281.256498 |

d)

Ethernet · 4 | IPv4 · 6 | IPv6 | TCP · 9 | UDP · 68

| Address A | Port A | Address B | Port B | Packets | Bytes | Packets A → B | Bytes A → B | Packets B → A | Bytes B → A | Rel Start | Duration | Bits/s A → B | Bits/s B → A |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 130.149.220.164 | 35487 | 130.149.220.253 | 53 | 2 | 224 | 1 | 87 | 1 | 137 | 9.589148 | 0.0008 | — | |
| 130.149.220.164 | 32956 | 130.149.220.253 | 53 | 2 | 226 | 1 | 88 | 1 | 138 | 49.664915 | 0.0007 | — | |
| 130.149.220.164 | 59289 | 130.149.220.253 | 53 | 2 | 224 | 1 | 87 | 1 | 137 | 67.614232 | 0.0006 | — | |
| 130.149.220.164 | 35045 | 130.149.220.253 | 53 | 2 | 253 | 1 | 87 | 1 | 166 | 112.851200 | 0.0008 | — | |
| 130.149.220.164 | 34364 | 130.149.220.253 | 53 | 2 | 232 | 1 | 91 | 1 | 141 | 112.852512 | 0.0004 | — | |
| 130.149.220.164 | 60128 | 130.149.220.253 | 53 | 2 | 368 | 1 | 98 | 1 | 270 | 113.739254 | 0.0008 | — | |
| 130.149.220.164 | 43042 | 130.149.220.253 | 53 | 2 | 234 | 1 | 92 | 1 | 142 | 113.741196 | 0.0006 | — | |
| 130.149.220.164 | 48833 | 130.149.220.253 | 53 | 2 | 238 | 1 | 94 | 1 | 144 | 113.742039 | 0.0005 | — | |
| 130.149.220.164 | 59780 | 130.149.220.253 | 53 | 2 | 368 | 1 | 98 | 1 | 270 | 113.742708 | 0.0005 | — | |
| 130.149.220.164 | 48920 | 130.149.220.253 | 53 | 2 | 238 | 1 | 94 | 1 | 144 | 113.743387 | 0.0005 | — | |
| 130.149.220.164 | 42023 | 130.149.220.253 | 53 | 2 | 234 | 1 | 92 | 1 | 142 | 113.744106 | 0.0003 | — | |
| 130.149.220.164 | 48377 | 130.149.220.253 | 53 | 2 | 312 | 1 | 105 | 1 | 207 | 113.790484 | 0.0007 | — | |
| 130.149.220.164 | 56572 | 130.149.220.253 | 53 | 2 | 234 | 1 | 92 | 1 | 142 | 113.791379 | 0.0005 | — | |
| 130.149.220.164 | 60101 | 130.149.220.253 | 53 | 2 | 256 | 1 | 93 | 1 | 163 | 113.792091 | 0.0006 | — | |
| 130.149.220.164 | 53277 | 130.149.220.253 | 53 | 2 | 368 | 1 | 98 | 1 | 270 | 113.793118 | 0.0007 | — | |
| 130.149.220.164 | 52581 | 130.149.220.253 | 53 | 2 | 238 | 1 | 94 | 1 | 144 | 113.793958 | 0.0005 | — | |
| 130.149.220.164 | 48412 | 130.149.220.253 | 53 | 2 | 234 | 1 | 92 | 1 | 142 | 113.794577 | 0.0004 | — | |
| 130.149.220.164 | 50651 | 130.149.220.253 | 53 | 2 | 368 | 1 | 98 | 1 | 270 | 113.795146 | 0.0005 | — | |
| 130.149.220.164 | 41152 | 130.149.220.253 | 53 | 2 | 234 | 1 | 92 | 1 | 142 | 113.795800 | 0.0005 | — | |
| 130.149.220.164 | 59153 | 130.149.220.253 | 53 | 2 | 238 | 1 | 94 | 1 | 144 | 113.796424 | 0.0005 | — | |
| 130.149.220.164 | 41625 | 130.149.220.253 | 53 | 2 | 312 | 1 | 105 | 1 | 207 | 113.798674 | 0.0006 | — | |
| 130.149.220.164 | 36487 | 130.149.220.253 | 53 | 2 | 234 | 1 | 92 | 1 | 142 | 113.799424 | 0.0005 | — | |
| 130.149.220.164 | 54048 | 130.149.220.253 | 53 | 2 | 368 | 1 | 98 | 1 | 270 | 113.800434 | 0.0005 | — | |

Information gotten from Statistics tab and then the conversations option.

From statistics-> conversations.

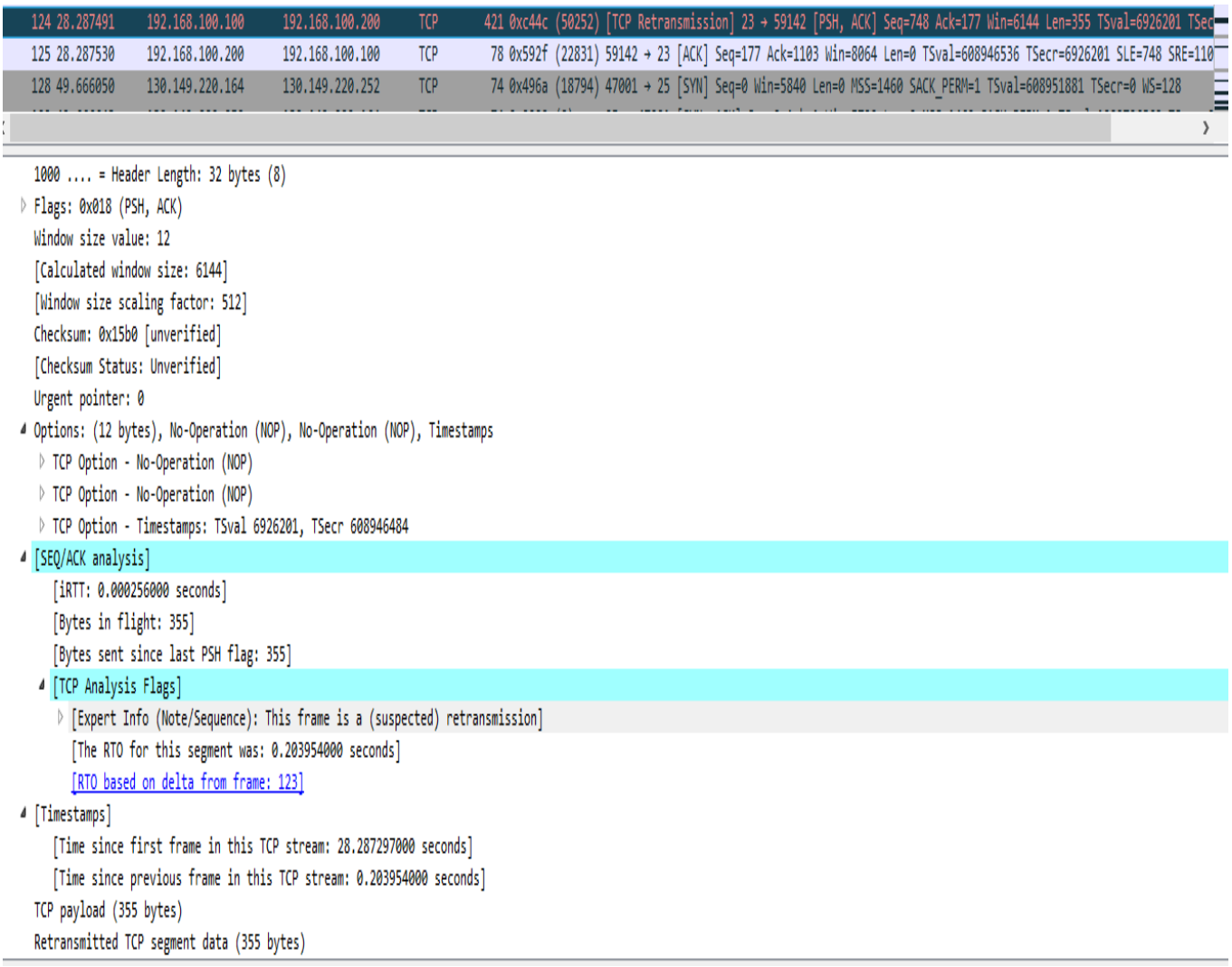
UDP flow 68

e) TCP connection exhibiting a packet loss

tcp && !http2 && !telnet && !ssh && !smtp

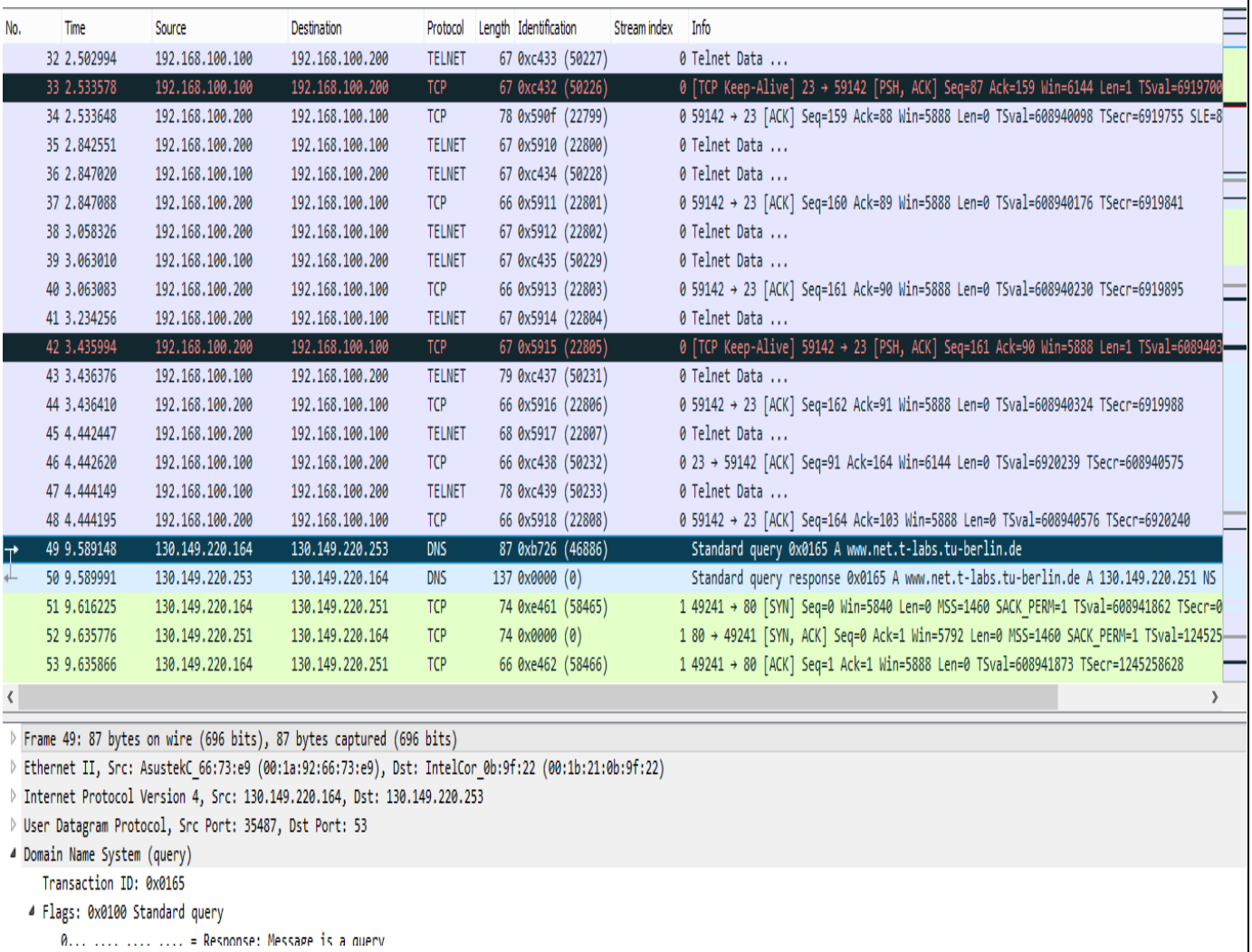
| No. | Time | Source | Destination | Protocol | Length | Identification | Info |
|---|---|---|---|---|---|---|---|
| 3 | 0.000194 | 192.168.100.200 | 192.168.100.100 | TCP | 74 | 0x58fd (22781) | 59142 → 23 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=608939464 TSecr=0 WS=128 |
| 4 | 0.000393 | 192.168.100.100 | 192.168.100.200 | TCP | 74 | 0x0000 (0) | 23 → 59142 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=6919129 TSecr=6089 |
| 5 | 0.000450 | 192.168.100.200 | 192.168.100.100 | TCP | 66 | 0x58fe (22782) | 59142 → 23 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=608939465 TSecr=6919129 |
| 7 | 0.000901 | 192.168.100.100 | 192.168.100.200 | TCP | 66 | 0xc425 (50213) | 23 → 59142 [ACK] Seq=1 Ack=28 Win=6144 Len=0 TSval=6919129 TSecr=608939465 |
| 10 | 0.108947 | 192.168.100.200 | 192.168.100.100 | TCP | 66 | 0x5900 (22784) | 59142 → 23 [ACK] Seq=28 Ack=13 Win=5888 Len=0 TSval=608939492 TSecr=6919156 |
| 12 | 0.311005 | 192.168.100.200 | 192.168.100.100 | TCP | 66 | 0x5901 (22785) | 59142 → 23 [ACK] Seq=28 Ack=52 Win=5888 Len=0 TSval=608939542 TSecr=6919207 |
| 14 | 0.311731 | 192.168.100.100 | 192.168.100.200 | TCP | 66 | 0xc429 (50217) | 23 → 59142 [ACK] Seq=52 Ack=150 Win=6144 Len=0 TSval=6919207 TSecr=608939542 |
| 17 | 0.360053 | 192.168.100.200 | 192.168.100.100 | TCP | 78 | 0x5904 (22788) | 59142 → 23 [ACK] Seq=150 Ack=55 Win=5888 Len=0 TSval=608939555 TSecr=6919207 SLE=13 SRE=52 |
| 22 | 0.952219 | 192.168.100.200 | 192.168.100.100 | TCP | 66 | 0x5907 (22791) | 59142 → 23 [ACK] Seq=153 Ack=58 Win=5888 Len=0 TSval=608939696 TSecr=6919360 |
| 23 | 0.952349 | 192.168.100.100 | 192.168.100.200 | TCP | 66 | 0xc42d (50221) | [TCP Dup ACK 21#1] 23 → 59142 [ACK] Seq=85 Ack=156 Win=6144 Len=0 TSval=6919367 TSecr=60893969 |

At stream index 23,we can find a TCP Dup ACK


124 28.287491 192.168.100.100 192.168.100.200 TCP 421 0xc44c (50252) [TCP Retransmission] 23 → 59142 [PSH, ACK] Seq=748 Ack=177 Win=6144 Len=355 TSval=6926201 TSec
125 28.287530 192.168.100.200 192.168.100.100 TCP 78 0x592f (22831) 59142 → 23 [ACK] Seq=177 Ack=1103 Win=8064 Len=0 TSval=608946536 TSecr=6926201 SLE=748 SRE=110
128 49.666050 130.149.220.164 130.149.220.252 TCP 74 0x496a (18794) 47001 → 25 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=608951881 TSecr=0 WS=128
1000 .... = Header Length: 32 bytes (8)
Flags: 0x018 (PSH, ACK)
Window size value: 12
[Calculated window size: 6144]
[Window size scaling factor: 512]
Checksum: 0x15b0 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
TCP Option - No-Operation (NOP)
TCP Option - No-Operation (NOP)
TCP Option - Timestamps: TSval 6926201, TSecr 608946484
[SEQ/ACK analysis]
[iRTT: 0.000256000 seconds]
[Bytes in flight: 355]
[Bytes sent since last PSH flag: 355]
[TCP Analysis Flags]
[Expert Info (Note/Sequence): This frame is a (suspected) retransmission]
[The RTO for this segment was: 0.203954000 seconds]
[RTO based on delta from frame: 123]
[Timestamps]
[Time since first frame in this TCP stream: 28.287297000 seconds]
[Time since previous frame in this TCP stream: 0.203954000 seconds]
TCP payload (355 bytes)
Retransmitted TCP segment data (355 bytes)

Question 3: DNS Resolution-

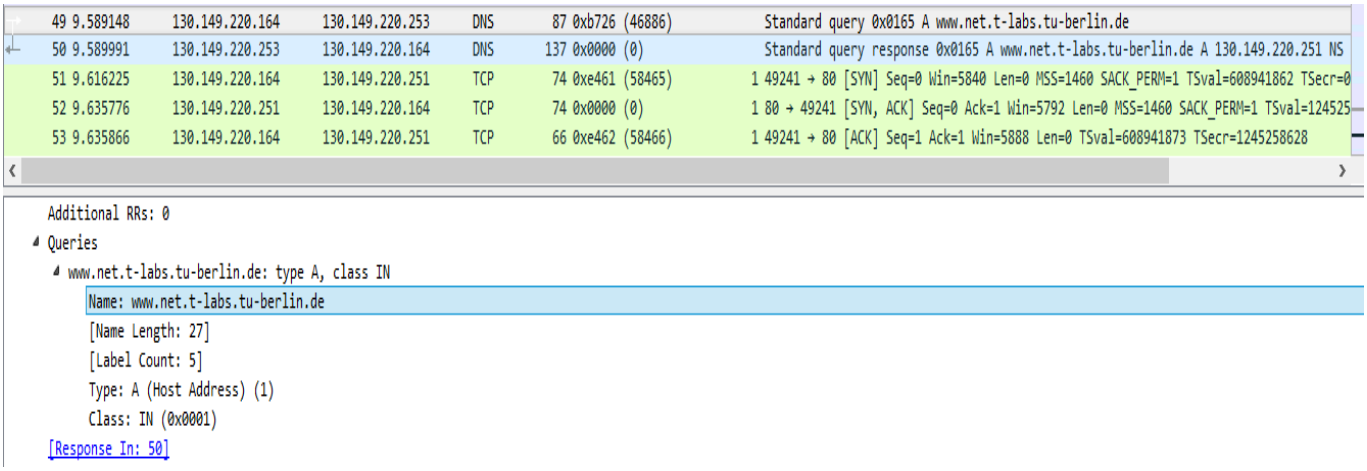
a) By manually scrolling through the trace, we got the DNS name of the host



| No. | Time | Source | Destination | Protocol | Length | Identification | Stream index | Info |
|---|---|---|---|---|---|---|---|---|
| 32 | 2.502994 | 192.168.100.100 | 192.168.100.200 | TELNET | 67 | 0xc433 (50227) | 0 | Telnet Data ... |
| 33 | 2.533578 | 192.168.100.100 | 192.168.100.200 | TCP | 67 | 0xc432 (50226) | 0 | [TCP Keep-Alive] 23 → 59142 [PSH, ACK] Seq=87 Ack=159 Win=6144 Len=1 TSval=6919700 |
| 34 | 2.533648 | 192.168.100.200 | 192.168.100.100 | TCP | 78 | 0x590f (22799) | 0 | 59142 → 23 [ACK] Seq=159 Ack=88 Win=5888 Len=0 TSval=608940098 TSecr=6919755 SLE=8 |
| 35 | 2.842551 | 192.168.100.200 | 192.168.100.100 | TELNET | 67 | 0x5910 (22800) | 0 | Telnet Data ... |
| 36 | 2.847020 | 192.168.100.100 | 192.168.100.200 | TELNET | 67 | 0xc434 (50228) | 0 | Telnet Data ... |
| 37 | 2.847088 | 192.168.100.200 | 192.168.100.100 | TCP | 66 | 0x5911 (22801) | 0 | 59142 → 23 [ACK] Seq=160 Ack=89 Win=5888 Len=0 TSval=608940176 TSecr=6919841 |
| 38 | 3.058326 | 192.168.100.200 | 192.168.100.100 | TELNET | 67 | 0x5912 (22802) | 0 | Telnet Data ... |
| 39 | 3.063010 | 192.168.100.100 | 192.168.100.200 | TELNET | 67 | 0xc435 (50229) | 0 | Telnet Data ... |
| 40 | 3.063083 | 192.168.100.200 | 192.168.100.100 | TCP | 66 | 0x5913 (22803) | 0 | 59142 → 23 [ACK] Seq=161 Ack=90 Win=5888 Len=0 TSval=608940230 TSecr=6919895 |
| 41 | 3.234256 | 192.168.100.200 | 192.168.100.100 | TELNET | 67 | 0x5914 (22804) | 0 | Telnet Data ... |
| 42 | 3.435994 | 192.168.100.200 | 192.168.100.100 | TCP | 67 | 0x5915 (22805) | 0 | [TCP Keep-Alive] 59142 → 23 [PSH, ACK] Seq=161 Ack=90 Win=5888 Len=1 TSval=6089403 |
| 43 | 3.436376 | 192.168.100.100 | 192.168.100.200 | TELNET | 79 | 0xc437 (50231) | 0 | Telnet Data ... |
| 44 | 3.436410 | 192.168.100.200 | 192.168.100.100 | TCP | 66 | 0x5916 (22806) | 0 | 59142 → 23 [ACK] Seq=162 Ack=91 Win=5888 Len=0 TSval=608940324 TSecr=6919988 |
| 45 | 4.442447 | 192.168.100.200 | 192.168.100.100 | TELNET | 68 | 0x5917 (22807) | 0 | Telnet Data ... |
| 46 | 4.442620 | 192.168.100.100 | 192.168.100.200 | TCP | 66 | 0xc438 (50232) | 0 | 23 → 59142 [ACK] Seq=91 Ack=164 Win=6144 Len=0 TSval=6920239 TSecr=608940575 |
| 47 | 4.444149 | 192.168.100.100 | 192.168.100.200 | TELNET | 78 | 0xc439 (50233) | 0 | Telnet Data ... |
| 48 | 4.444195 | 192.168.100.200 | 192.168.100.100 | TCP | 66 | 0x5918 (22808) | 0 | 59142 → 23 [ACK] Seq=164 Ack=103 Win=5888 Len=0 TSval=608940576 TSecr=6920240 |
| 49 | 9.589148 | 130.149.220.164 | 130.149.220.253 | DNS | 87 | 0xb726 (46886) | | Standard query 0x0165 A www.net.t-labs.tu-berlin.de |
| 50 | 9.589991 | 130.149.220.253 | 130.149.220.164 | DNS | 137 | 0x0000 (0) | | Standard query response 0x0165 A www.net.t-labs.tu-berlin.de A 130.149.220.251 NS |
| 51 | 9.616225 | 130.149.220.164 | 130.149.220.251 | TCP | 74 | 0xe461 (58465) | 1 | 49241 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=608941862 TSecr=0 |
| 52 | 9.635776 | 130.149.220.251 | 130.149.220.164 | TCP | 74 | 0x0000 (0) | 1 | 80 → 49241 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=124525 |
| 53 | 9.635866 | 130.149.220.164 | 130.149.220.251 | TCP | 66 | 0xe462 (58466) | 1 | 49241 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=608941873 TSecr=1245258628 |

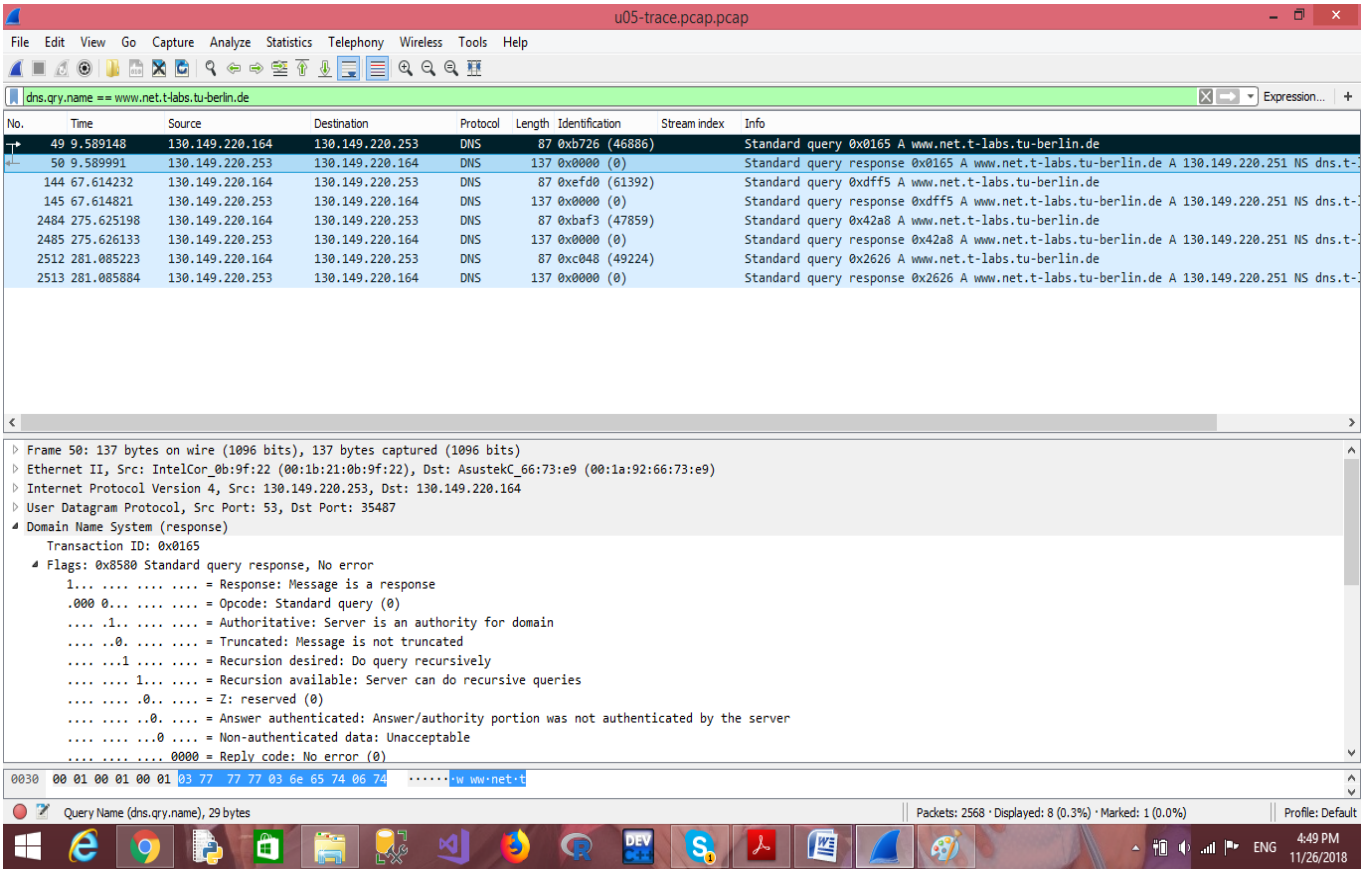
```
▷ Frame 49: 87 bytes on wire (696 bits), 87 bytes captured (696 bits)
▷ Ethernet II, Src: AsustekC_66:73:e9 (00:1a:92:66:73:e9), Dst: IntelCor_0b:9f:22 (00:1b:21:0b:9f:22)
▷ Internet Protocol Version 4, Src: 130.149.220.164, Dst: 130.149.220.253
▷ User Datagram Protocol, Src Port: 35487, Dst Port: 53
◢ Domain Name System (query)
    Transaction ID: 0x0165
  ◢ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
```

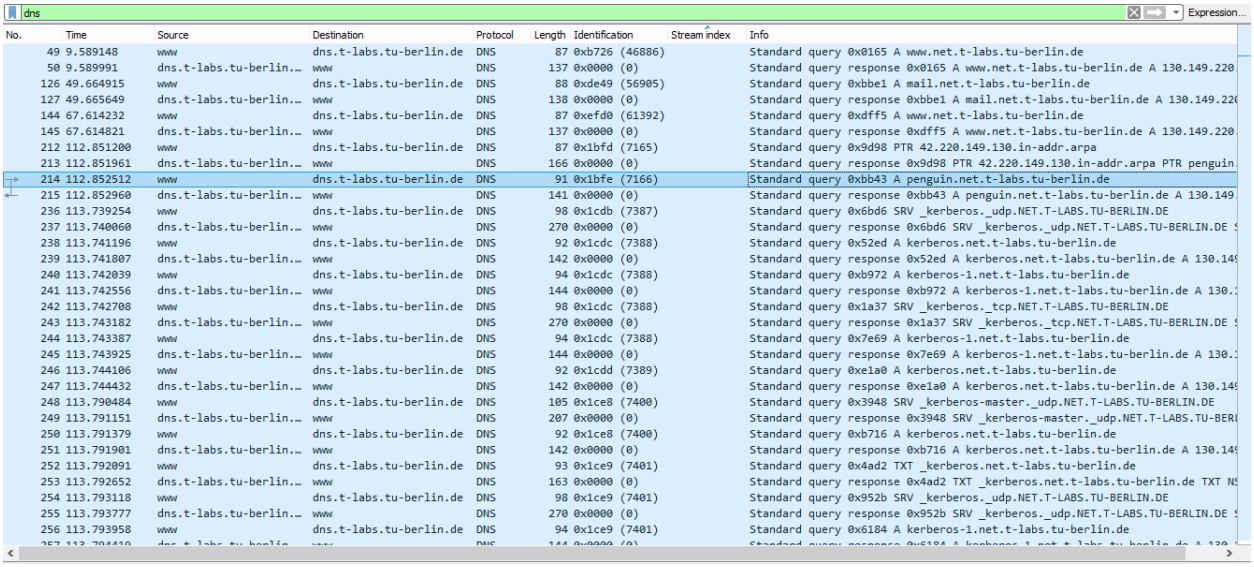
Name: www.net.t-labs.tu-berlin.de




b)

Using the filter dns.qry.name == www.net.t-labs.tu-berlin.de





| No. | Time | Source | Destination | Protocol | Length | Identification | Stream index | Info |
|---|---|---|---|---|---|---|---|---|
| 49 | 9.589148 | www | dns.t-labs.tu-berlin.de | DNS | 87 | 0xb726 (46886) | | Standard query 0x0165 A www.net.t-labs.tu-berlin.de |
| 50 | 9.589991 | dns.t-labs.tu-berlin… | www | DNS | 137 | 0x0000 (0) | | Standard query response 0x0165 A www.net.t-labs.tu-berlin.de A 130.149.220 |
| 126 | 49.664915 | www | dns.t-labs.tu-berlin.de | DNS | 88 | 0xde49 (56905) | | Standard query 0xbbe1 A mail.net.t-labs.tu-berlin.de |
| 127 | 49.665649 | dns.t-labs.tu-berlin… | www | DNS | 138 | 0x0000 (0) | | Standard query response 0xbbe1 A mail.net.t-labs.tu-berlin.de A 130.149.22 |
| 144 | 67.614232 | www | dns.t-labs.tu-berlin.de | DNS | 87 | 0xefd0 (61392) | | Standard query 0xdff5 A www.net.t-labs.tu-berlin.de |
| 145 | 67.614821 | dns.t-labs.tu-berlin… | www | DNS | 137 | 0x0000 (0) | | Standard query response 0xdff5 A www.net.t-labs.tu-berlin.de A 130.149.220 |
| 212 | 112.851200 | www | dns.t-labs.tu-berlin.de | DNS | 87 | 0x1bfd (7165) | | Standard query 0x9d98 PTR 42.220.149.130.in-addr.arpa |
| 213 | 112.851961 | dns.t-labs.tu-berlin… | www | DNS | 166 | 0x0000 (0) | | Standard query response 0x9d98 PTR 42.220.149.130.in-addr.arpa PTR penguin |
| 214 | 112.852512 | www | dns.t-labs.tu-berlin.de | DNS | 91 | 0x1bfe (7166) | | Standard query 0xbb43 A penguin.net.t-labs.tu-berlin.de |
| 215 | 112.852960 | dns.t-labs.tu-berlin… | www | DNS | 141 | 0x0000 (0) | | Standard query response 0xbb43 A penguin.net.t-labs.tu-berlin.de A 130.149 |
| 236 | 113.739254 | www | dns.t-labs.tu-berlin.de | DNS | 98 | 0x1cdb (7387) | | Standard query 0x6bd6 SRV _kerberos._udp.NET.T-LABS.TU-BERLIN.DE |
| 237 | 113.740060 | dns.t-labs.tu-berlin… | www | DNS | 270 | 0x0000 (0) | | Standard query response 0x6bd6 SRV _kerberos._udp.NET.T-LABS.TU-BERLIN.DE |
| 238 | 113.741196 | www | dns.t-labs.tu-berlin.de | DNS | 92 | 0x1cdc (7388) | | Standard query 0x52ed A kerberos.net.t-labs.tu-berlin.de |
| 239 | 113.741807 | dns.t-labs.tu-berlin… | www | DNS | 142 | 0x0000 (0) | | Standard query response 0x52ed A kerberos.net.t-labs.tu-berlin.de A 130.14 |
| 240 | 113.742039 | www | dns.t-labs.tu-berlin.de | DNS | 94 | 0x1cdc (7388) | | Standard query 0xb972 A kerberos-1.net.t-labs.tu-berlin.de |
| 241 | 113.742556 | dns.t-labs.tu-berlin… | www | DNS | 144 | 0x0000 (0) | | Standard query response 0xb972 A kerberos-1.net.t-labs.tu-berlin.de A 130. |
| 242 | 113.742708 | www | dns.t-labs.tu-berlin.de | DNS | 98 | 0x1cdc (7388) | | Standard query 0x1a37 SRV _kerberos._tcp.NET.T-LABS.TU-BERLIN.DE |
| 243 | 113.743182 | dns.t-labs.tu-berlin… | www | DNS | 270 | 0x0000 (0) | | Standard query response 0x1a37 SRV _kerberos._tcp.NET.T-LABS.TU-BERLIN.DE |
| 244 | 113.743387 | www | dns.t-labs.tu-berlin.de | DNS | 94 | 0x1cdc (7388) | | Standard query 0x7e69 A kerberos-1.net.t-labs.tu-berlin.de |
| 245 | 113.743925 | dns.t-labs.tu-berlin… | www | DNS | 144 | 0x0000 (0) | | Standard query response 0x7e69 A kerberos-1.net.t-labs.tu-berlin.de A 130. |
| 246 | 113.744106 | www | dns.t-labs.tu-berlin.de | DNS | 92 | 0x1cdd (7389) | | Standard query 0xe1a0 A kerberos.net.t-labs.tu-berlin.de |
| 247 | 113.744432 | dns.t-labs.tu-berlin… | www | DNS | 142 | 0x0000 (0) | | Standard query response 0xe1a0 A kerberos.net.t-labs.tu-berlin.de A 130.14 |
| 248 | 113.790484 | www | dns.t-labs.tu-berlin.de | DNS | 105 | 0x1ce8 (7400) | | Standard query 0x3948 SRV _kerberos-master._udp.NET.T-LABS.TU-BERLIN.DE |
| 249 | 113.791151 | dns.t-labs.tu-berlin… | www | DNS | 207 | 0x0000 (0) | | Standard query response 0x3948 SRV _kerberos-master._udp.NET.T-LABS.TU-BER |
| 250 | 113.791379 | www | dns.t-labs.tu-berlin.de | DNS | 92 | 0x1ce8 (7400) | | Standard query 0xb716 A kerberos.net.t-labs.tu-berlin.de |
| 251 | 113.791901 | dns.t-labs.tu-berlin… | www | DNS | 142 | 0x0000 (0) | | Standard query response 0xb716 A kerberos.net.t-labs.tu-berlin.de A 130.14 |
| 252 | 113.792091 | www | dns.t-labs.tu-berlin.de | DNS | 93 | 0x1ce9 (7401) | | Standard query 0x4ad2 TXT _kerberos.net.t-labs.tu-berlin.de |
| 253 | 113.792652 | dns.t-labs.tu-berlin… | www | DNS | 163 | 0x0000 (0) | | Standard query response 0x4ad2 TXT _kerberos.net.t-labs.tu-berlin.de TXT N |
| 254 | 113.793118 | www | dns.t-labs.tu-berlin.de | DNS | 98 | 0x1ce9 (7401) | | Standard query 0x952b SRV _kerberos._udp.NET.T-LABS.TU-BERLIN.DE |
| 255 | 113.793777 | dns.t-labs.tu-berlin… | www | DNS | 270 | 0x0000 (0) | | Standard query response 0x952b SRV _kerberos._udp.NET.T-LABS.TU-BERLIN.DE |
| 256 | 113.793958 | www | dns.t-labs.tu-berlin.de | DNS | 94 | 0x1ce9 (7401) | | Standard query 0x6184 A kerberos-1.net.t-labs.tu-berlin.de |

by enabling name resolution Edit - Preferences - Name Resolution.

| hostIP | DNS name |
|---|---|
| 130.149.220.164 | www.net.t-labs.tu-berlin.de |
| 130.149.220.253 | www.net.t-labs.tu-berlin.de |

Question 4: Application Layer

a) (i) What is the user doing / what is requested?

Here we've chosen the first connection from the list of stream indices.

connection with stream Index 0

connection with stream index 1: the user is requesting with GET /index.shtml HTTP/1.0 and the apache servers response is HTTP/1.1 200 OK with the display of the index.shtml.

Connection with index 8 : requests for two GET /~jan/random.bulk HTTP/1.0 and GET /~jan/random.bulk HTTP/1.0, both the request are served by the apache server.

Connection with Index 4 : requests GET /index.shtml HTTP/1.0 and request is served by apache server.

connection with stream index 3 : looks like a mail user agent.

Opening a connection with the server : reply with the code 220.

The following codes can be observed:

| Command | Reply Code |
|---|---|
| DATA | 354 |
| HELO | 250 |
| MAIL FROM | 250 |
| QUIT | 221 |
| RCPT TO | 250 |

Connections with stream index 5, 6 and 7 display the SSH service/traffic.

(ii) Which information is disclosed (passwords, etc.)?

connection with stream index 0 has following information disclosed

puffin login: bbaaddgguuyy

Password: breakin

connection with stream index 2 has tcp stream with scrambled data/ in encrypted form.

b) The application layer semantic of the packets 18-20 is Telnet.

Packet 18: Telnet :Won't Echo ; Command-Won't – The sender of packet 18 with command Won't Echo refuses to start echoing the data characters it is receiving over the Telnet connection it has made, that is refuse to send the data characters back to the sender.

Packet 19: Telnet: Will Echo – Command –Will

The packet 19 containing this command requests to start , or confirms that it can start echoing data characters that it receives over the Telnet connection back to the sender from which it received the data characters.

Packet 20: Telnet: Do Echo- Command –Do

So the sender of the command Do requests that the receiver of this command start echoing, data characters it receives over the Telnet connection back to the sender.

The sender of this command REQUESTS that the receiver of this

IETF standards- RFC: 854