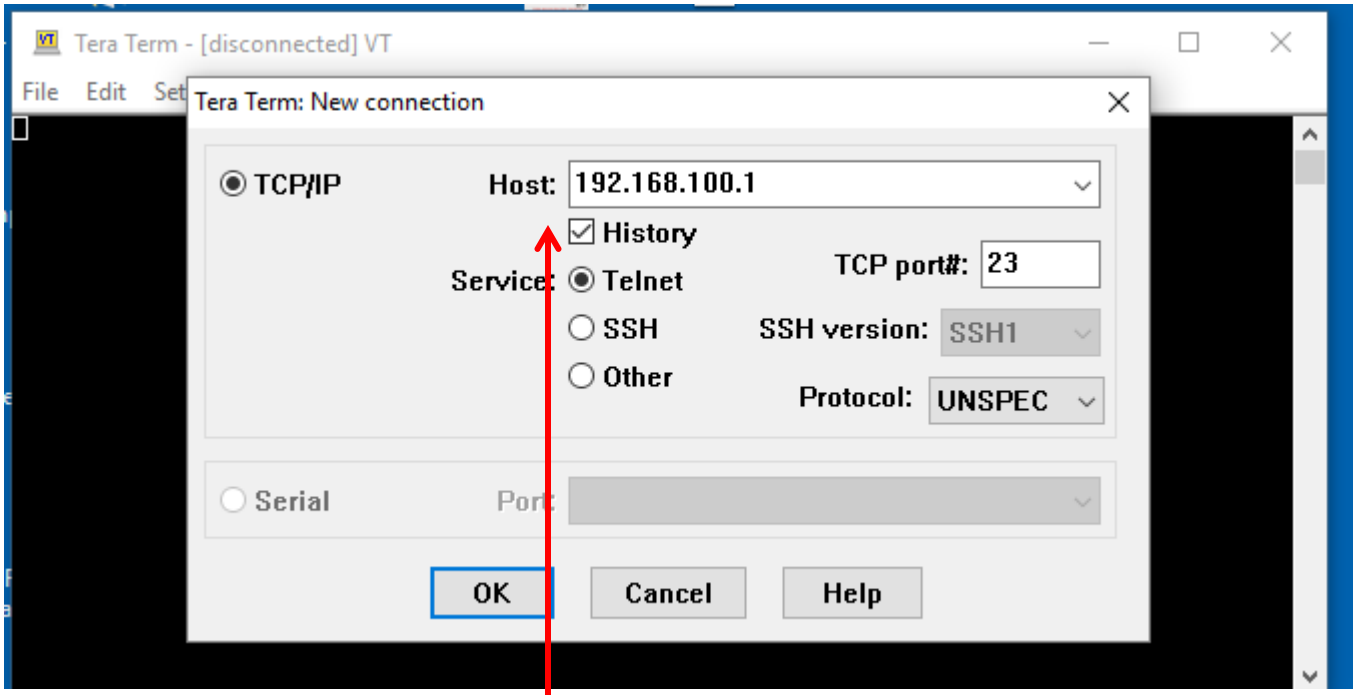
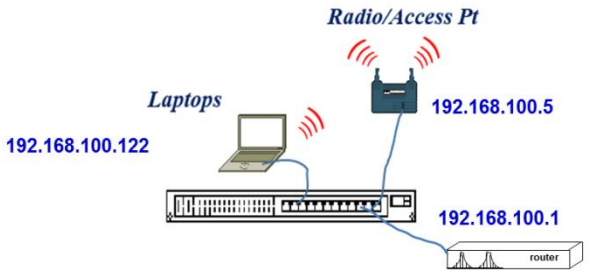
Telnet application protocol capture

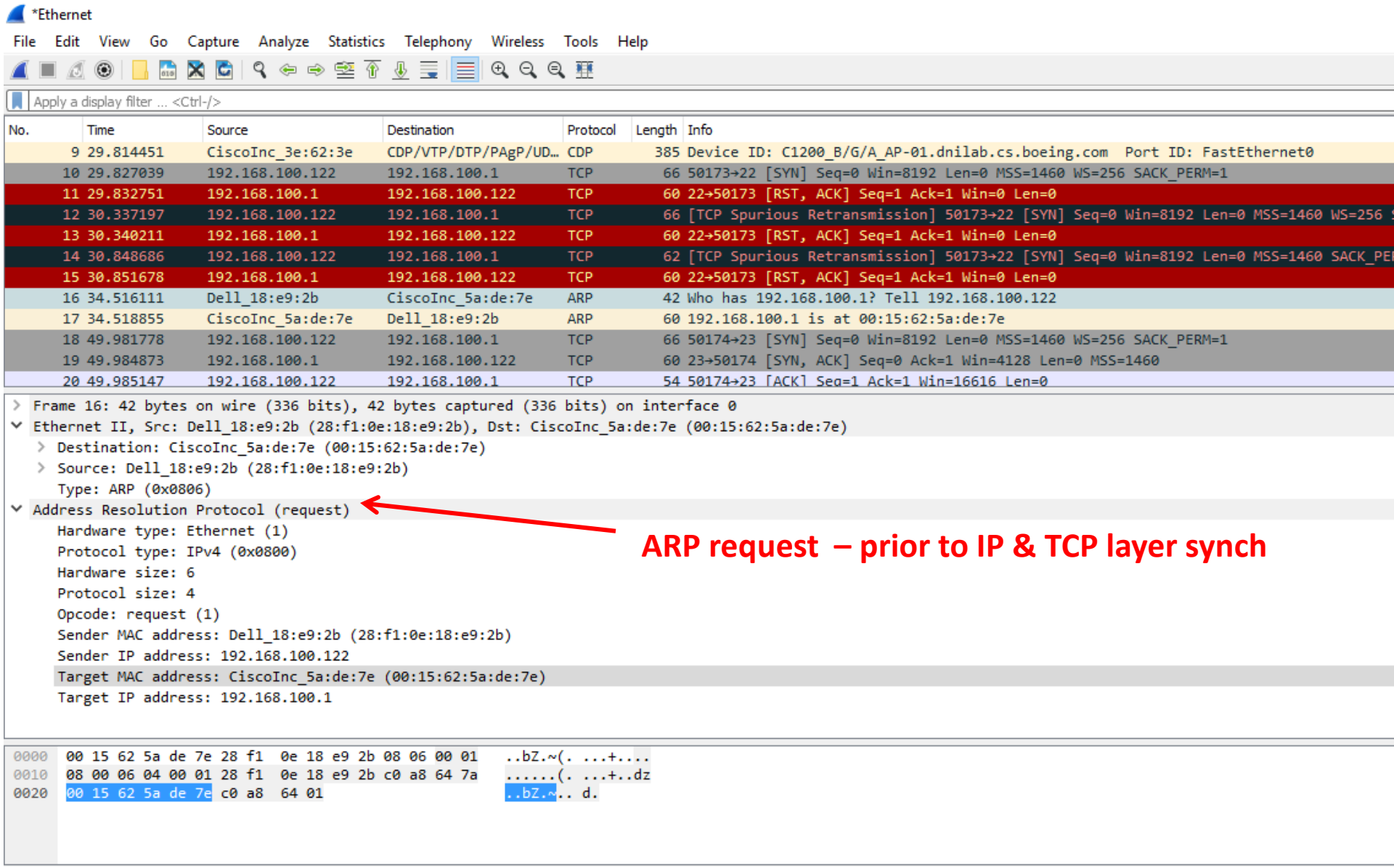


1. I already started Wireshark session live capturing in background which will "see" all frames on Ethernet.

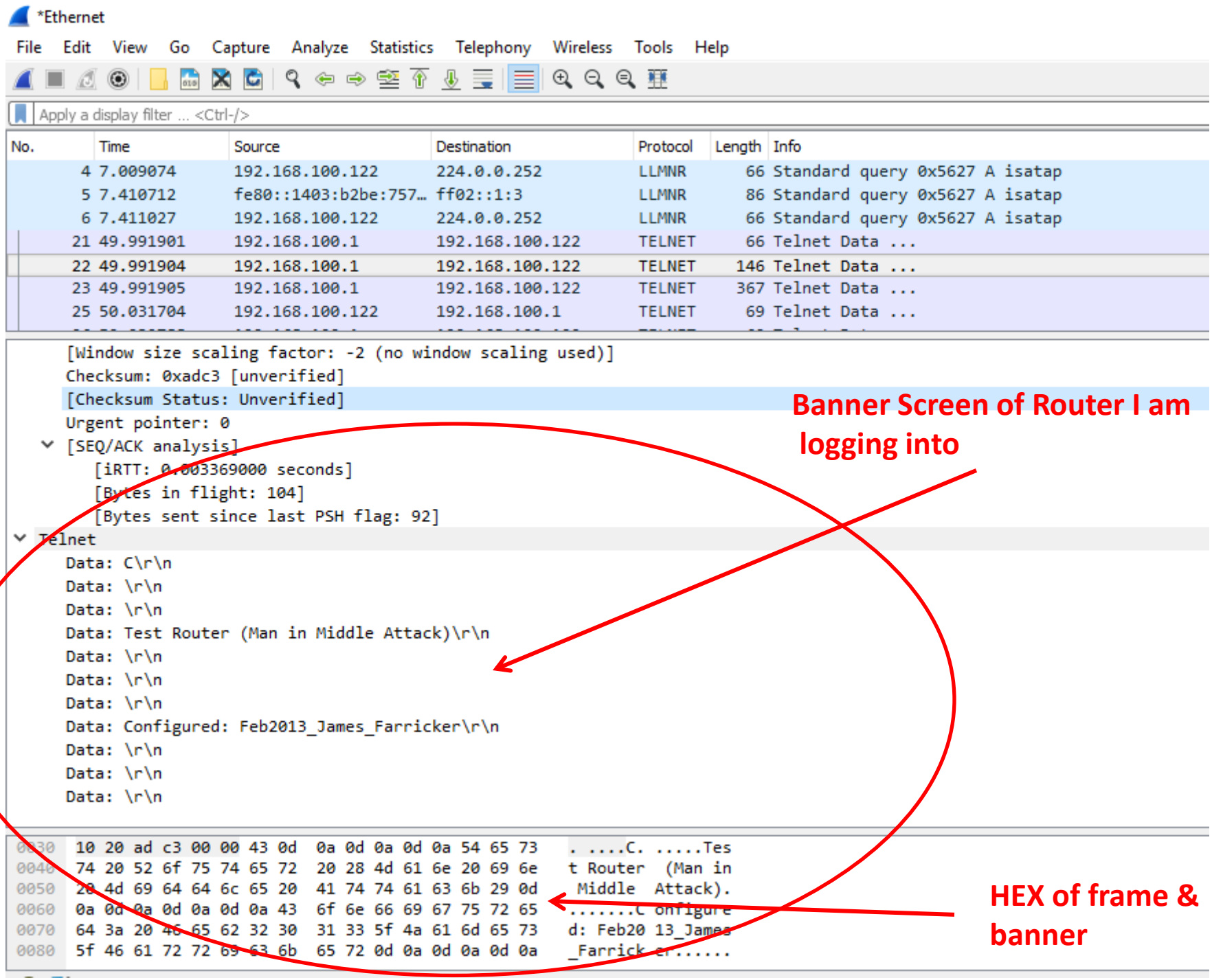
2. Using Telnet application (teraterm) of laptop (.122) entering IP add of 100.5 to HTTP into cisco router 192.168.100.1

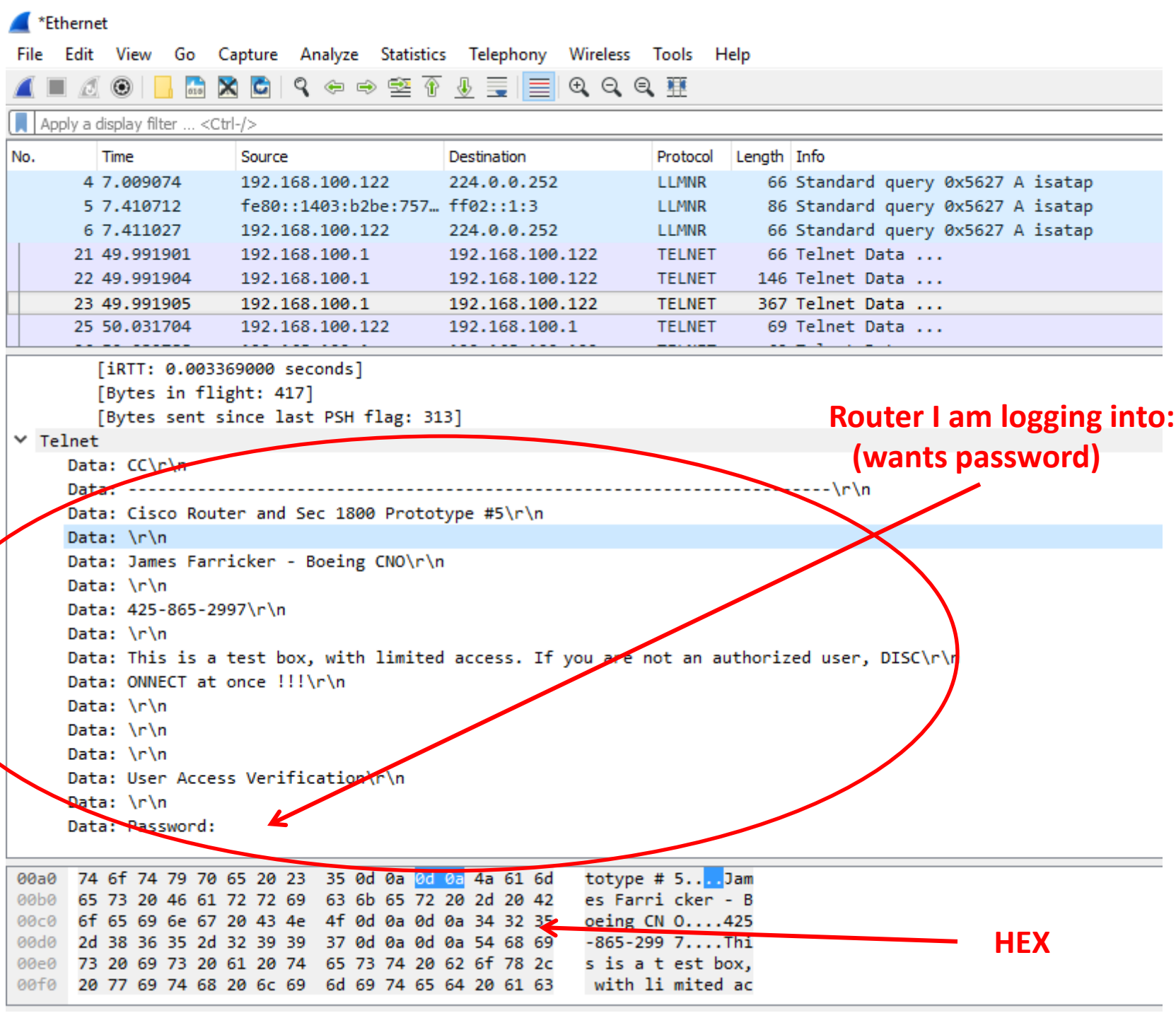


Telnet application protocol capture

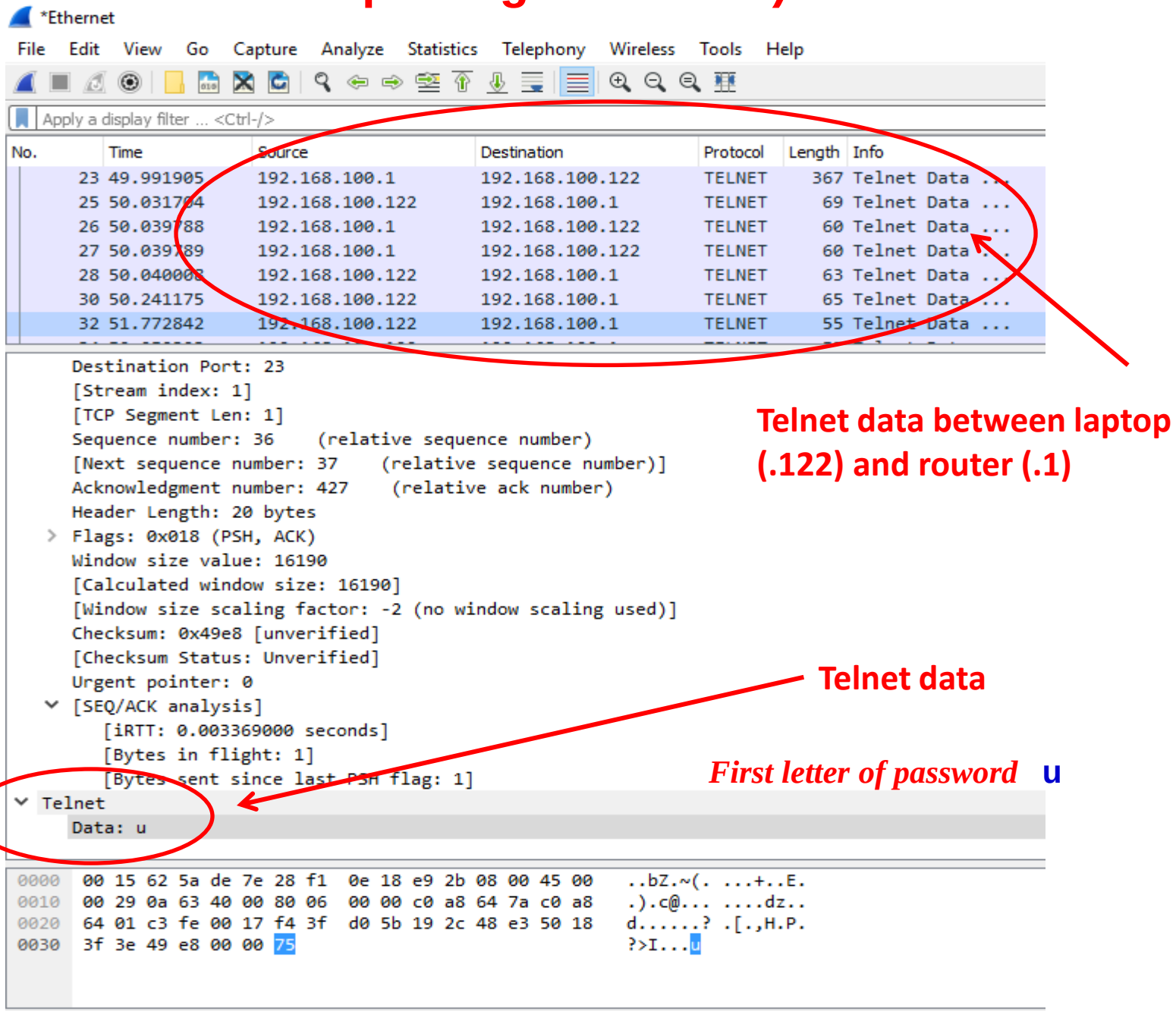


ARP request – prior to IP & TCP layer synch


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
4 7.009074 192.168.100.122 224.0.0.252 LLMNR 66 Standard query 0x5627 A isatap
5 7.410712 fe80::1403:b2be:757… ff02::1:3 LLMNR 86 Standard query 0x5627 A isatap
6 7.411027 192.168.100.122 224.0.0.252 LLMNR 66 Standard query 0x5627 A isatap
21 49.991901 192.168.100.1 192.168.100.122 TELNET 66 Telnet Data ...
22 49.991904 192.168.100.1 192.168.100.122 TELNET 146 Telnet Data ...
23 49.991905 192.168.100.1 192.168.100.122 TELNET 367 Telnet Data ...
25 50.031704 192.168.100.122 192.168.100.1 TELNET 69 Telnet Data ...
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0xadc3 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[iRTT: 0.003369000 seconds]
[Bytes in flight: 104]
[Bytes sent since last PSH flag: 92]
Telnet
Data: C\r\n
Data: \r\n
Data: \r\n
Data: Test Router (Man in Middle Attack)\r\n
Data: \r\n
Data: \r\n
Data: \r\n
Data: Configured: Feb2013_James_Farricker\r\n
Data: \r\n
Data: \r\n
Data: \r\n
0030 10 20 ad c3 00 00 43 0d 0a 0d 0a 0d 0a 54 65 73 . ....C. .....Tes
0040 74 20 52 6f 75 74 65 72 20 28 4d 61 6e 20 69 6e t Router (Man in
0050 20 4d 69 64 64 6c 65 20 41 74 74 61 63 6b 29 0d Middle Attack).
0060 0a 0d 0a 0d 0a 0d 0a 43 6f 6e 66 69 67 75 72 65 ....C onfigure
0070 64 3a 20 46 65 62 32 30 31 33 5f 4a 61 6d 65 73 d: Feb20 13_James
0080 5f 46 61 72 72 69 63 6b 65 72 0d 0a 0d 0a 0d 0a _Farrick er......
Banner Screen of Router I am logging into
HEX of frame & banner


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
4 7.009074 192.168.100.122 224.0.0.252 LLMNR 66 Standard query 0x5627 A isatap
5 7.410712 fe80::1403:b2be:757… ff02::1:3 LLMNR 86 Standard query 0x5627 A isatap
6 7.411027 192.168.100.122 224.0.0.252 LLMNR 66 Standard query 0x5627 A isatap
21 49.991901 192.168.100.1 192.168.100.122 TELNET 66 Telnet Data ...
22 49.991904 192.168.100.1 192.168.100.122 TELNET 146 Telnet Data ...
23 49.991905 192.168.100.1 192.168.100.122 TELNET 367 Telnet Data ...
25 50.031704 192.168.100.122 192.168.100.1 TELNET 69 Telnet Data ...
[iRTT: 0.003369000 seconds]
[Bytes in flight: 417]
[Bytes sent since last PSH flag: 313]
Telnet
Data: CC\r\n
Data: ----------\r\n
Data: Cisco Router and Sec 1800 Prototype #5\r\n
Data: \r\n
Data: James Farricker - Boeing CNO\r\n
Data: \r\n
Data: 425-865-2997\r\n
Data: \r\n
Data: This is a test box, with limited access. If you are not an authorized user, DISC\r\n
Data: ONNECT at once !!!\r\n
Data: \r\n
Data: \r\n
Data: \r\n
Data: User Access Verification\r\n
Data: \r\n
Data: Password:
Router I am logging into:
(wants password)
00a0 74 6f 74 79 70 65 20 23 35 0d 0a 0d 0a 4a 61 6d totype # 5....Jam
00b0 65 73 20 46 61 72 72 69 63 6b 65 72 20 2d 20 42 es Farri cker - B
00c0 6f 65 69 6e 67 20 43 4e 4f 0d 0a 0d 0a 34 32 35 oeing CN O....425
00d0 2d 38 36 35 2d 32 39 39 37 0d 0a 0d 0a 54 68 69 -865-299 7....Thi
00e0 73 20 69 73 20 61 20 74 65 73 74 20 62 6f 78 2c s is a t est box,
00f0 20 77 69 74 68 20 6c 69 6d 69 74 65 64 20 61 63 with li mited ac
HEX

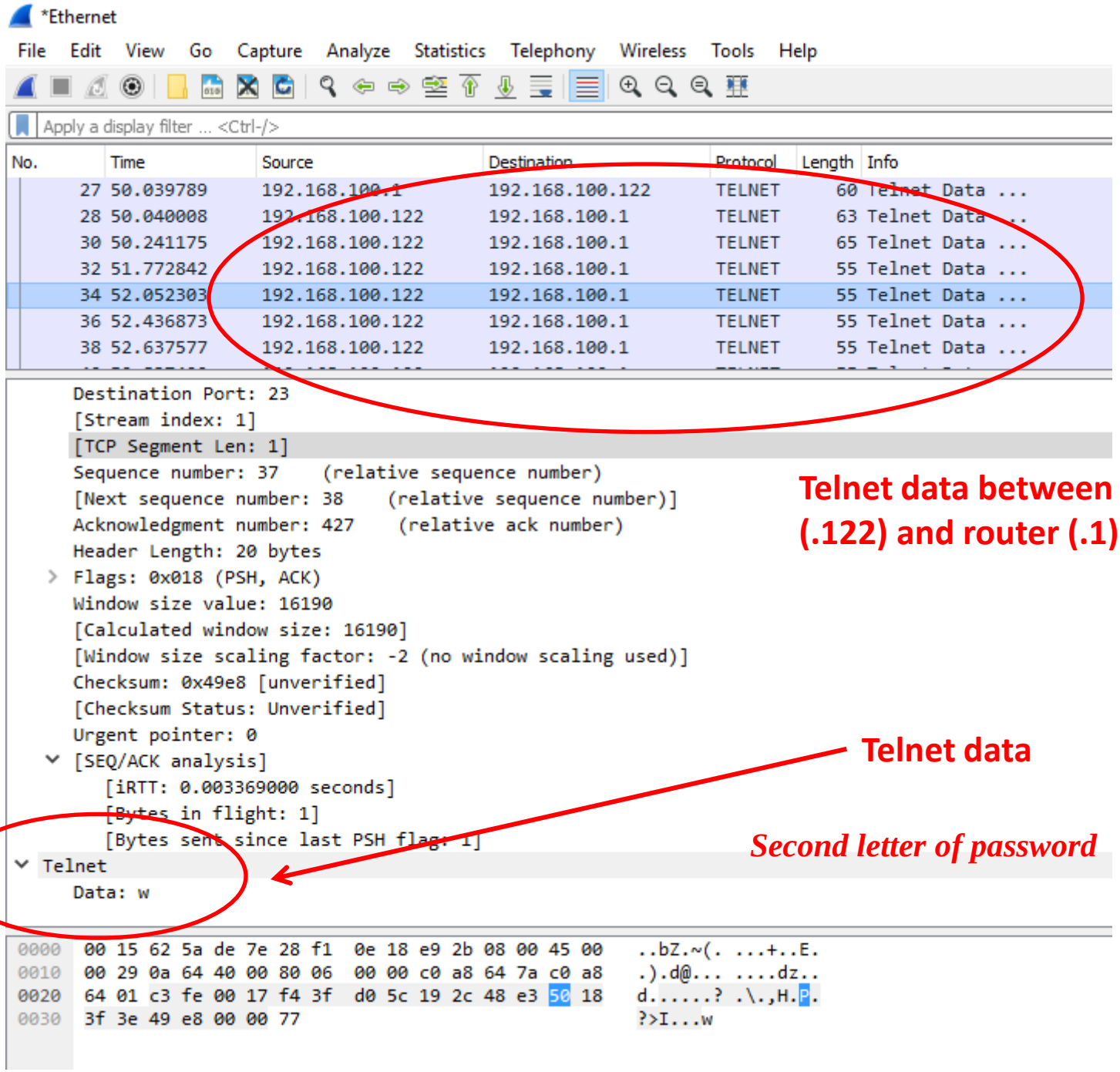
Capturing Password)



Telnet data between laptop (.122) and router (.1)

Telnet data

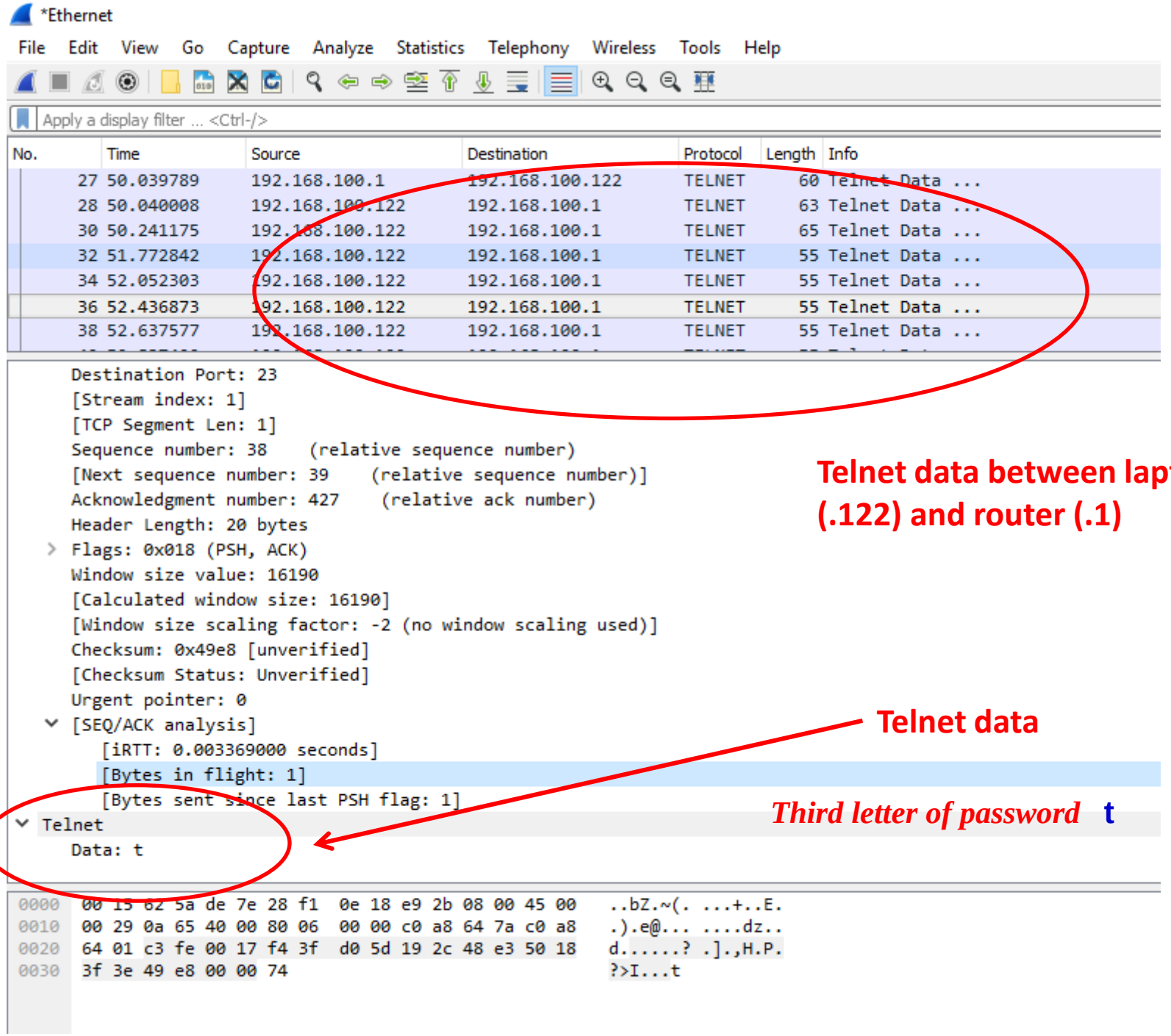
First letter of password **u**

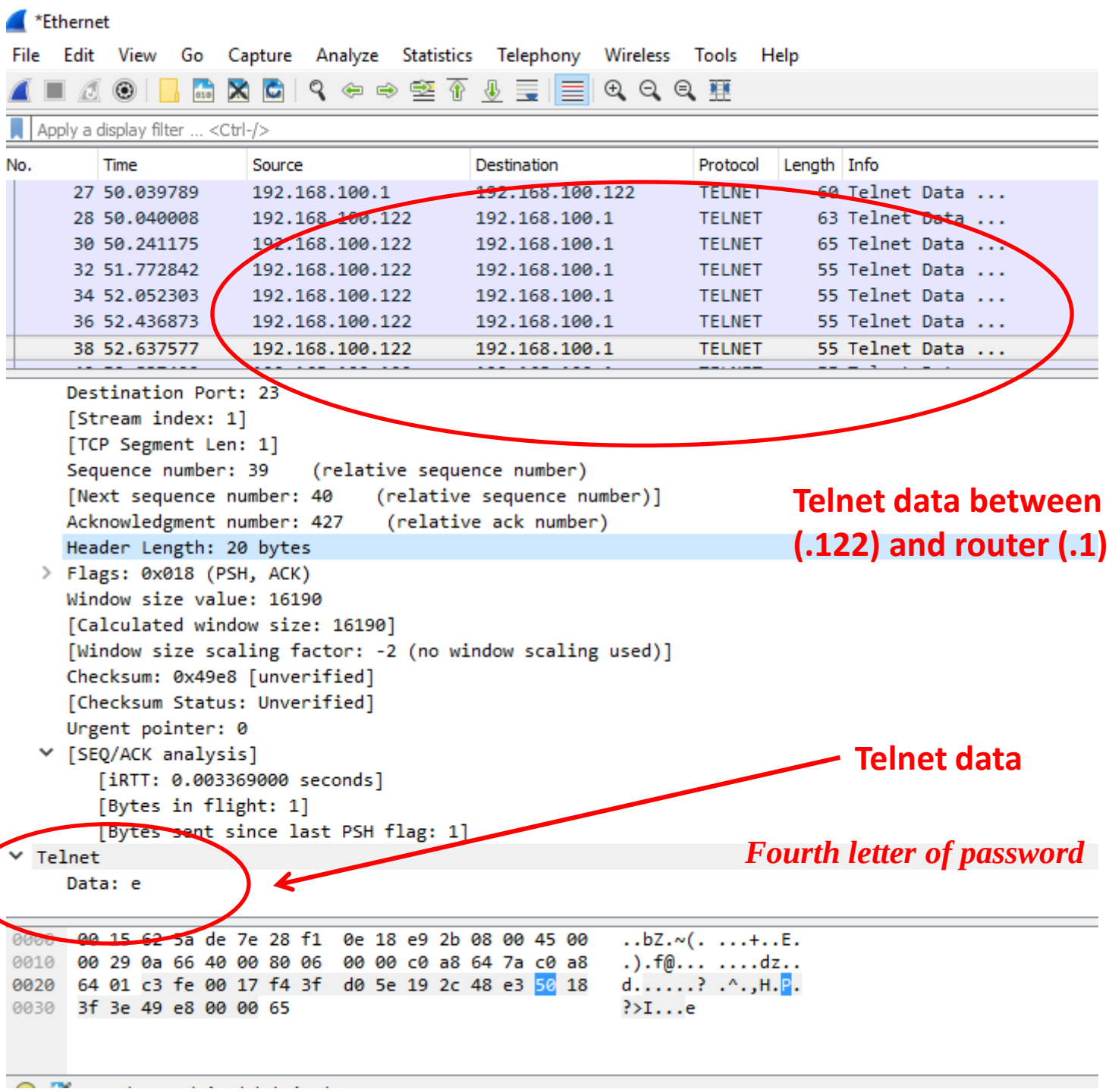


Telnet data between laptop (.122) and router (.1)

Telnet data

Second letter of password **w**

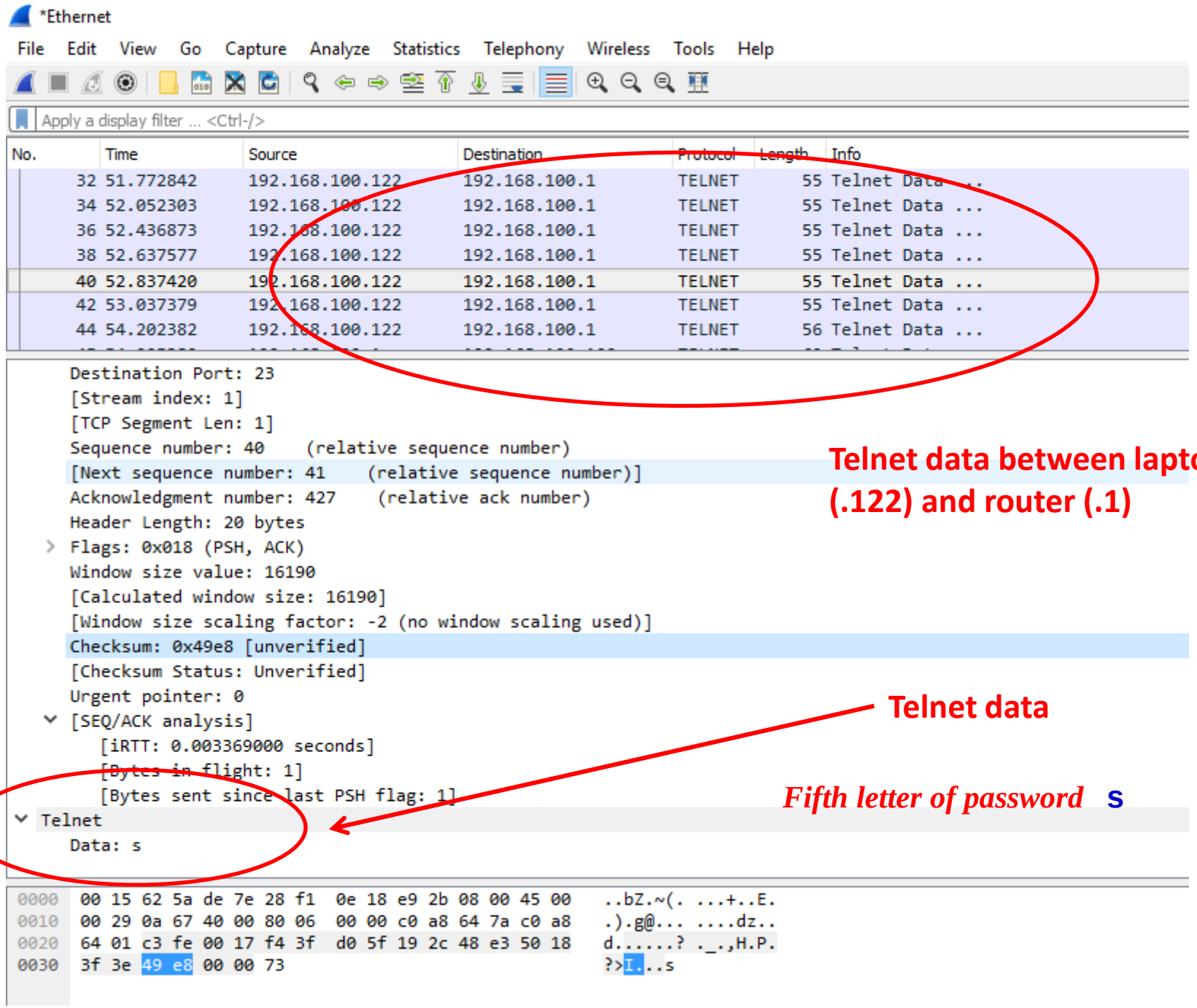

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
27 50.039789 192.168.100.1 192.168.100.122 TELNET 60 Telnet Data ...
28 50.040008 192.168.100.122 192.168.100.1 TELNET 63 Telnet Data ...
30 50.241175 192.168.100.122 192.168.100.1 TELNET 65 Telnet Data ...
32 51.772842 192.168.100.122 192.168.100.1 TELNET 55 Telnet Data ...
34 52.052303 192.168.100.122 192.168.100.1 TELNET 55 Telnet Data ...
36 52.436873 192.168.100.122 192.168.100.1 TELNET 55 Telnet Data ...
38 52.637577 192.168.100.122 192.168.100.1 TELNET 55 Telnet Data ...
Destination Port: 23
[Stream index: 1]
[TCP Segment Len: 1]
Sequence number: 38 (relative sequence number)
[Next sequence number: 39 (relative sequence number)]
Acknowledgment number: 427 (relative ack number)
Header Length: 20 bytes
Flags: 0x018 (PSH, ACK)
Window size value: 16190
[Calculated window size: 16190]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x49e8 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[iRTT: 0.003369000 seconds]
[Bytes in flight: 1]
[Bytes sent since last PSH flag: 1]
Telnet
Data: t
0000 00 15 62 5a de 7e 28 f1 0e 18 e9 2b 08 00 45 00 ..bZ.~(. ...+..E.
0010 00 29 0a 65 40 00 80 06 00 00 c0 a8 64 7a c0 a8 .).e@... ....dz..
0020 64 01 c3 fe 00 17 f4 3f d0 5d 19 2c 48 e3 50 18 d.....? .],H.P.
0030 3f 3e 49 e8 00 00 74 ?>I...t
Telnet data between laptop (.122) and router (.1)
Telnet data
Third letter of password t

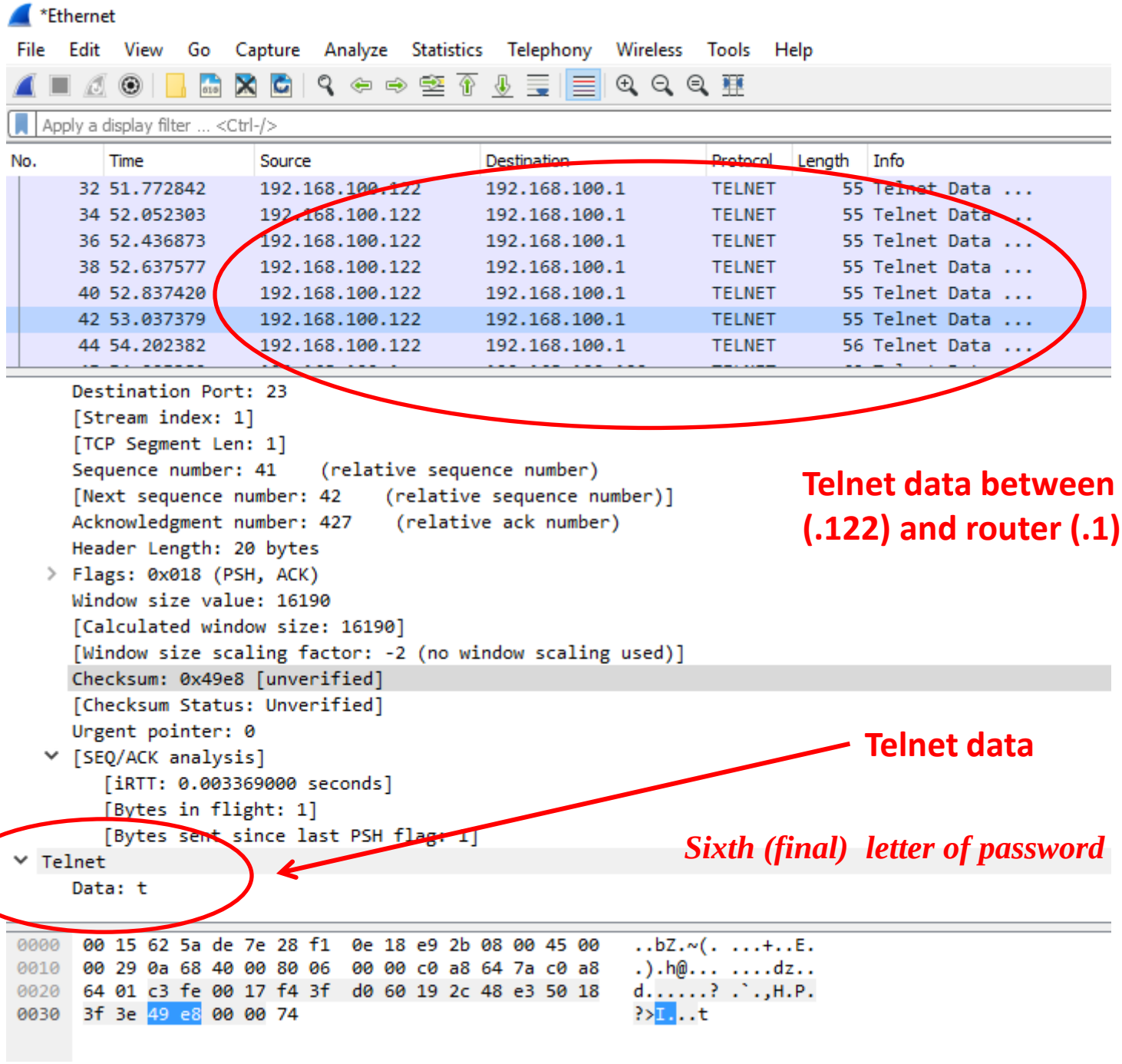


Telnet data between laptop (.122) and router (.1)

Telnet data

Fourth letter of password **e**

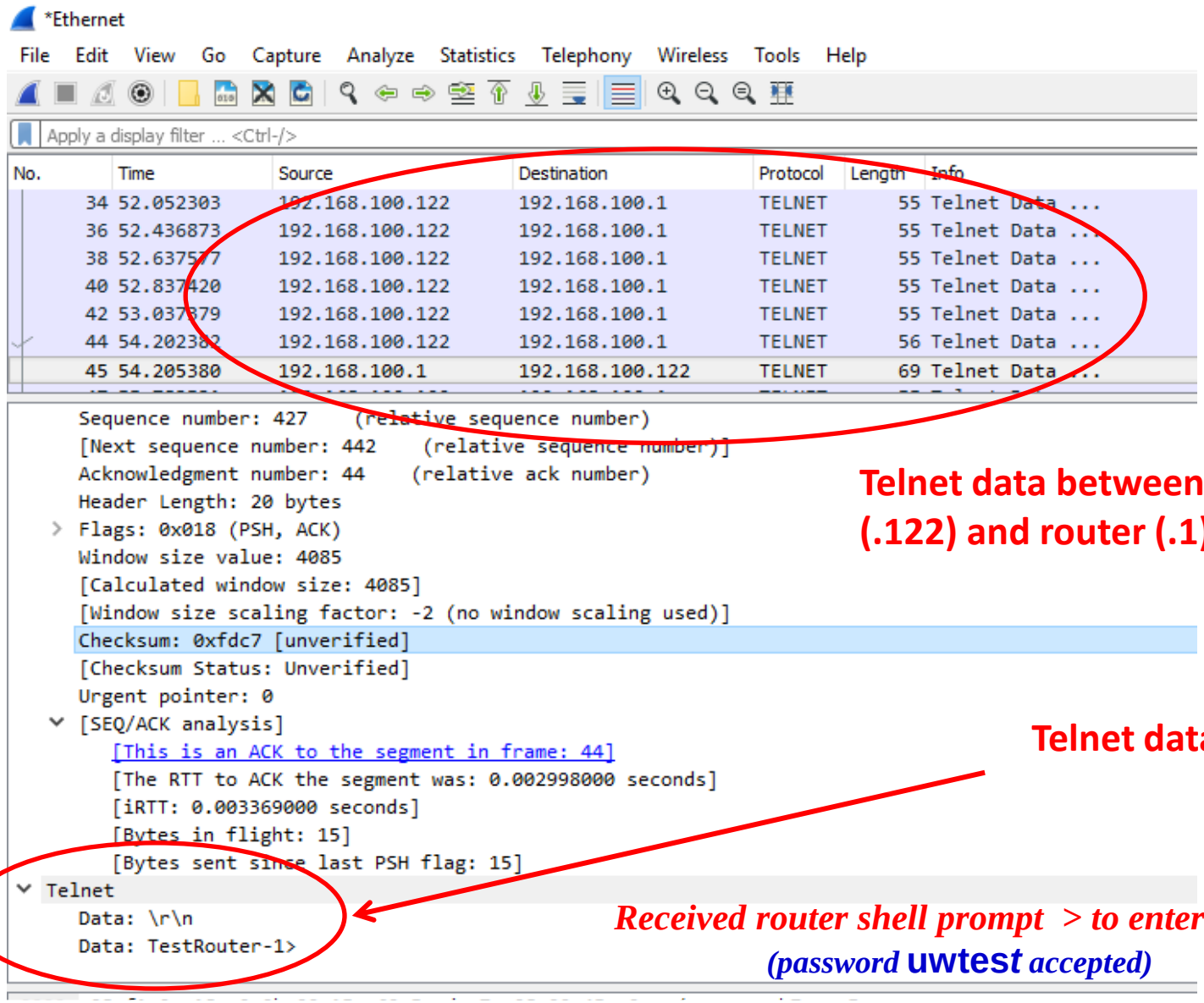

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
32 51.772842 192.168.100.122 192.168.100.1 TELNET 55 Telnet Data ...
34 52.052303 192.168.100.122 192.168.100.1 TELNET 55 Telnet Data ...
36 52.436873 192.168.100.122 192.168.100.1 TELNET 55 Telnet Data ...
38 52.637577 192.168.100.122 192.168.100.1 TELNET 55 Telnet Data ...
40 52.837420 192.168.100.122 192.168.100.1 TELNET 55 Telnet Data ...
42 53.037379 192.168.100.122 192.168.100.1 TELNET 55 Telnet Data ...
44 54.202382 192.168.100.122 192.168.100.1 TELNET 56 Telnet Data ...
Destination Port: 23
[Stream index: 1]
[TCP Segment Len: 1]
Sequence number: 40 (relative sequence number)
[Next sequence number: 41 (relative sequence number)]
Acknowledgment number: 427 (relative ack number)
Header Length: 20 bytes
Flags: 0x018 (PSH, ACK)
Window size value: 16190
[Calculated window size: 16190]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x49e8 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[iRTT: 0.003369000 seconds]
[Bytes in flight: 1]
[Bytes sent since last PSH flag: 1]
Telnet
Data: s
Telnet data between laptop (.122) and router (.1)
Telnet data
Fifth letter of password s
0000 00 15 62 5a de 7e 28 f1 0e 18 e9 2b 08 00 45 00 ..bZ.~(. ...+..E.
0010 00 29 0a 67 40 00 80 06 00 00 c0 a8 64 7a c0 a8 .).g@... ....dz..
0020 64 01 c3 fe 00 17 f4 3f d0 5f 19 2c 48 e3 50 18 d.....? ._.,H.P.
0030 3f 3e 49 e8 00 00 73 ?>I...s



Telnet data between laptop (.122) and router (.1)

Telnet data

Sixth (final) letter of password **t**



I entered password **uwtest** *as one word/entry – hit enter application breaks it up to send pw 1 character at time*