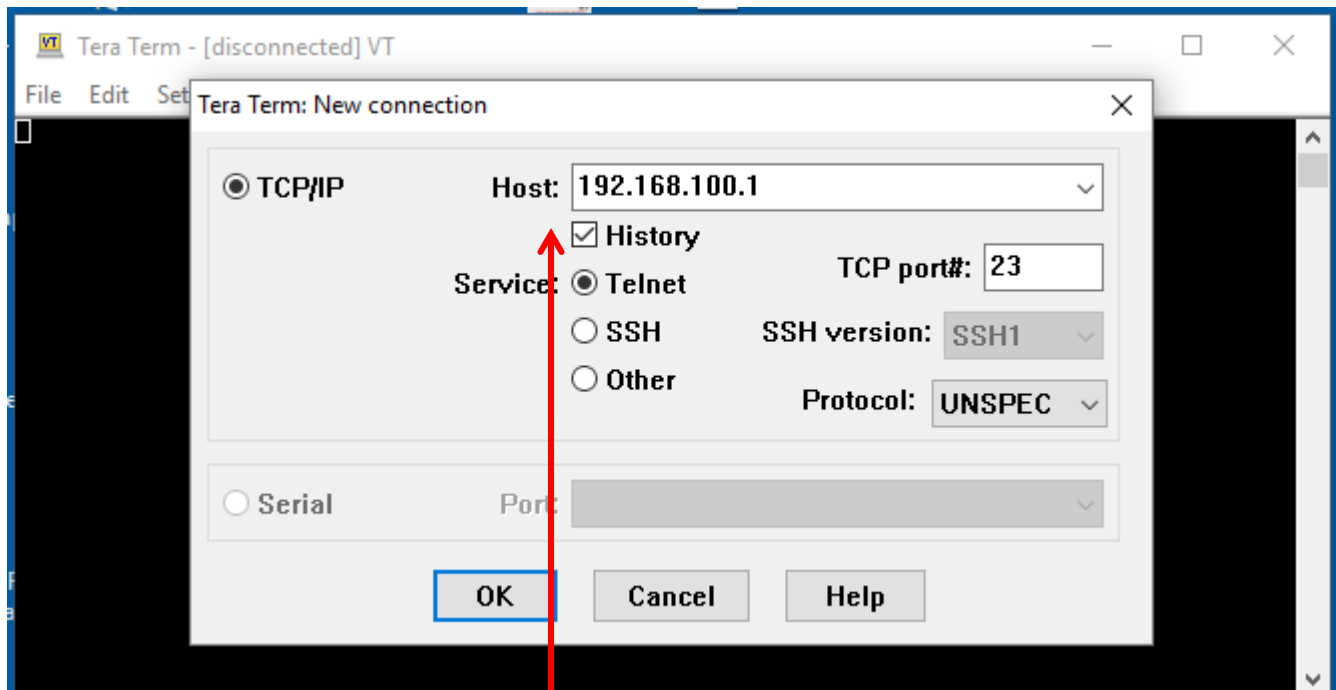


# Telnet application protocol capture



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

\*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
9	29.814451	CiscoInc_3e:62:3e	CDP/VTP/DTP/PAGP/UD...	CDP	385	Device ID: C1200_B/G/A_AP-01.dnilab.cs.boeing.com Port ID: FastEthernet0
10	29.827039	192.168.100.122	192.168.100.1	TCP	66	50173→22 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
11	29.832751	192.168.100.1	192.168.100.122	TCP	60	22→50173 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
12	30.337197	192.168.100.122	192.168.100.1	TCP	66	[TCP Spurious Retransmission] 50173→22 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256
13	30.340211	192.168.100.1	192.168.100.122	TCP	60	22→50173 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
14	30.848686	192.168.100.122	192.168.100.1	TCP	62	[TCP Spurious Retransmission] 50173→22 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
15	30.851678	192.168.100.1	192.168.100.122	TCP	60	22→50173 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
16	34.516111	Dell_18:e9:2b	CiscoInc_5a:de:7e	ARP	42	Who has 192.168.100.1? Tell 192.168.100.122
17	34.518855	CiscoInc_5a:de:7e	Dell_18:e9:2b	ARP	60	192.168.100.1 is at 00:15:62:5a:de:7e
18	49.981778	192.168.100.122	192.168.100.1	TCP	66	50174→23 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
19	49.984873	192.168.100.1	192.168.100.122	TCP	60	23→50174 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=1460
20	49.985147	192.168.100.122	192.168.100.1	TCP	54	50174→23 [ACK] Seq=1 Ack=1 Win=16616 Len=0

> Frame 16: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

▼ Ethernet II, Src: Dell\_18:e9:2b (28:f1:0e:18:e9:2b), Dst: CiscoInc\_5a:de:7e (00:15:62:5a:de:7e)

- > Destination: CiscoInc\_5a:de:7e (00:15:62:5a:de:7e)
- > Source: Dell\_18:e9:2b (28:f1:0e:18:e9:2b)
- Type: ARP (0x0806)

▼ Address Resolution Protocol (request)

- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: request (1)
- Sender MAC address: Dell\_18:e9:2b (28:f1:0e:18:e9:2b)
- Sender IP address: 192.168.100.122
- Target MAC address: CiscoInc\_5a:de:7e (00:15:62:5a:de:7e)
- Target IP address: 192.168.100.1

ARP request – prior to IP & TCP layer synch

```
0000 00 15 62 5a de 7e 28 f1 0e 18 e9 2b 08 06 00 01 ..bZ.~(. ...+...
0010 08 00 06 04 00 01 28 f1 0e 18 e9 2b c0 a8 64 7a .....(. ...+..dz
0020 00 15 62 5a de 7e c0 a8 64 01 ..bZ.~... d.
```



Apply a display filter ... &lt;Ctrl-/&gt;

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: 0xad3 [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**



Apply a display filter ... &lt;Ctrl-/&gt;

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  totyp# 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)

\*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
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 ...
26	50.039788	192.168.100.1	192.168.100.122	TELNET	60	Telnet Data ...
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 ...

Destination Port: 23  
[Stream index: 1]  
[TCP Segment Len: 1]  
Sequence number: 36 (relative sequence number)  
[Next sequence number: 37 (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  
v [SEQ/ACK analysis]  
[iRTT: 0.003369000 seconds]  
[Bytes in flight: 1]  
[Bytes sent since last PSH flag: 1]  
v Telnet  
Data: u

0000 00 15 62 5a de 7e 28 f1 0e 18 e9 2b 08 00 45 00 ..bZ.~(. ...+..E.  
0010 00 29 0a 63 40 00 80 06 00 00 c0 a8 64 7a c0 a8 ..).c@... ....dz..  
0020 64 01 c3 fe 00 17 f4 3f d0 5b 19 2c 48 e3 50 18 d.....? .[,H.P.  
0030 3f 3e 49 e8 00 00 75 ?>I...u

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

Telnet data

First letter of password u



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: 37 (relative sequence number)

[Next sequence number: 38 (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: w

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

**Telnet data**

*Second letter of password* **w**

```

0000 00 15 62 5a de 7e 28 f1 0e 18 e9 2b 08 00 45 00 ..bZ.~(. ...+..E.
0010 00 29 0a 64 40 00 80 06 00 00 c0 a8 64 7a c0 a8 ..).d@... ....dz..
0020 64 01 c3 fe 00 17 f4 3f d0 5c 19 2c 48 e3 50 18 d.....? \.,H.P.
0030 3f 3e 49 e8 00 00 77 ?>I...w

```



Apply a display filter ... &lt;Ctrl-/&gt;

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

&gt; 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

v [SEQ/ACK analysis]

[iRTT: 0.003369000 seconds]

[Bytes in flight: 1]

[Bytes sent since last PSH flag: 1]

v Telnet

Data: t

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

Telnet data

Third letter of password **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
```



\*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: 39 (relative sequence number)  
[Next sequence number: 40 (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  
v [SEQ/ACK analysis]  
[iRTT: 0.003369000 seconds]  
[Bytes in flight: 1]  
[Bytes sent since last PSH flag: 1]  
v Telnet  
Data: e

0000 00 15 62 5a de 7e 28 f1 0e 18 e9 2b 08 00 45 00 ..bZ.~(. ...+..E.  
0010 00 29 0a 66 40 00 80 06 00 00 c0 a8 64 7a c0 a8 .).f@... ....dz..  
0020 64 01 c3 fe 00 17 f4 3f d0 5e 19 2c 48 e3 50 18 d.....? .^.,H.P.  
0030 3f 3e 49 e8 00 00 65 ?>I...e

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

Telnet data

Fourth letter of password e





Apply a display filter ... &lt;Ctrl-/&gt;

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

```



Apply a display filter ... &lt;Ctrl-/&gt;

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: 41 (relative sequence number)

[Next sequence number: 42 (relative sequence number)]

Acknowledgment number: 427 (relative ack number)

Header Length: 20 bytes

&gt; 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

v [SEQ/ACK analysis]

[iRTT: 0.003369000 seconds]

[Bytes in flight: 1]

[Bytes sent since last PSH flag: 1]

v Telnet

Data: t

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

**Telnet data**

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

```

0000  00 15 62 5a de 7e 28 f1 0e 18 e9 2b 08 00 45 00  ..bZ.~(. ...+..E.
0010  00 29 0a 68 40 00 80 06 00 00 c0 a8 64 7a c0 a8  .).h@... ..dz..
0020  64 01 c3 fe 00 17 f4 3f d0 60 19 2c 48 e3 50 18  d.....? .`.H.P.
0030  3f 3e 49 e8 00 00 74                                ?>I...t

```

\*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
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 ...
45	54.205380	192.168.100.1	192.168.100.122	TELNET	69	Telnet Data ...

Sequence number: 427 (relative sequence number)  
[Next sequence number: 442 (relative sequence number)]  
Acknowledgment number: 44 (relative ack number)  
Header Length: 20 bytes  
> Flags: 0x018 (PSH, ACK)  
Window size value: 4085  
[Calculated window size: 4085]  
[Window size scaling factor: -2 (no window scaling used)]  
Checksum: 0xfdc7 [unverified]  
[Checksum Status: Unverified]  
Urgent pointer: 0  
v [SEQ/ACK analysis]  
[This is an ACK to the segment in frame: 44]  
[The RTT to ACK the segment was: 0.002998000 seconds]  
[iRTT: 0.003369000 seconds]  
[Bytes in flight: 15]  
[Bytes sent since last PSH flag: 15]  
v Telnet  
Data: \r\n  
Data: TestRouter-1>

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

Telnet data

Received router shell prompt > to enter cmds (password uwtest accepted)

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

Details at: [http://www.wireshark.org/docs/wsug\\_html\\_chunked/ChAdvChecksums.html](http://www.wireshark.org/docs/wsug_html_chunked/ChAdvChecksums.html) (tcp.checksum), 2 bytes