Wireshark Developer and User Conference

Troubleshooting Tips and Tricks for TCP/IP Networks

June 16, 2011

Laura Chappell
Founder | Chappell University/Wireshark University
laura@chappellU.com

SHARKFEST **'11**
Stanford University
June 13-16, 2011

The “Top 10” Issues

1. Packet loss
2. Client, server and wire latency
3. Window scaling issues (RFC 1323)
4. Service response issues and application behavior
5. Network design issues (wired/wireless)
6. Path issues (such as QoS)
7. Itty Bitty Stinking Packets (Low MSS Value)
8. Fragmentation
9. Timing problems
10. Interconnecting devices

Hot Tips for TCP/IP Troubleshooting

- **Build** a troubleshooting profile*
- **Recolor** Window Update packets to green background (should not be “Bad TCP” coloring)
- **Filter** on ports, not protocols (e.g., use `tcp.port==80` rather than `http`)
- **Always** watch the time column – some networking is just ugly
- **Watch for both** Retransmissions and Fast Retransmissions in the Expert**

** See Laura’s Lab Kit v10*

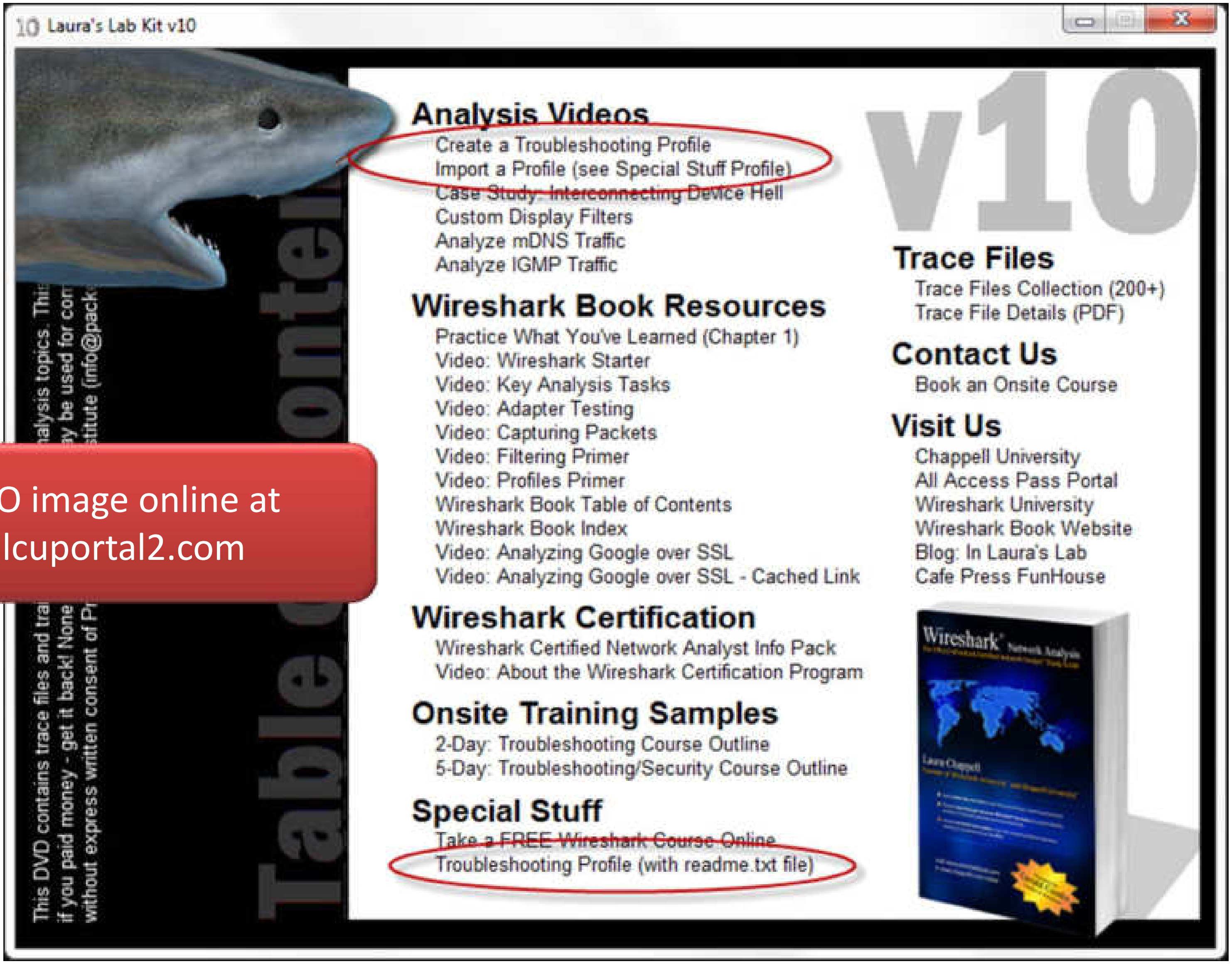
*** as noted in the session – filter on tcp.analysis.retransmissions will show both standard and fast retransmissions!*

Hot Tips for TCP/IP Troubleshooting

- **Recognize** a "short TCP handshake" – data is contained in the third handshake packet
- **Expand** the Conversation window to view Duration
- **Enable** TCP Conversation Timestamps (TCP protocol setting) – column?
- **Click** through the IO Graph – Don't troubleshoot red herrings
- **Know** the definition of each TCP analysis flag
- **Watch** the handshakes!

** See Laura's Lab Kit v10*

Your TCP/IP Troubleshooting Profile


Laura's Lab Kit v10
Table of Conten
This DVD contains trace files and tra
if you paid money - get it back! None
without express written consent of Pr
alysis topics. Thi
ay be used for co
stitute (info@pack
v10

Analysis Videos

Create a Troubleshooting Profile
Import a Profile (see Special Stuff Profile)
Case Study: Interconnecting Device Hell
Custom Display Filters
Analyze mDNS Traffic
Analyze IGMP Traffic

Wireshark Book Resources

Practice What You've Learned (Chapter 1)
Video: Wireshark Starter
Video: Key Analysis Tasks
Video: Adapter Testing
Video: Capturing Packets
Video: Filtering Primer
Video: Profiles Primer
Wireshark Book Table of Contents
Wireshark Book Index
Video: Analyzing Google over SSL
Video: Analyzing Google over SSL - Cached Link

Wireshark Certification

Wireshark Certified Network Analyst Info Pack
Video: About the Wireshark Certification Program

Onsite Training Samples

2-Day: Troubleshooting Course Outline
5-Day: Troubleshooting/Security Course Outline

Special Stuff

Take a FREE Wireshark Course Online
Troubleshooting Profile (with readme.txt file)

Trace Files

Trace Files Collection (200+)
Trace File Details (PDF)

Contact Us

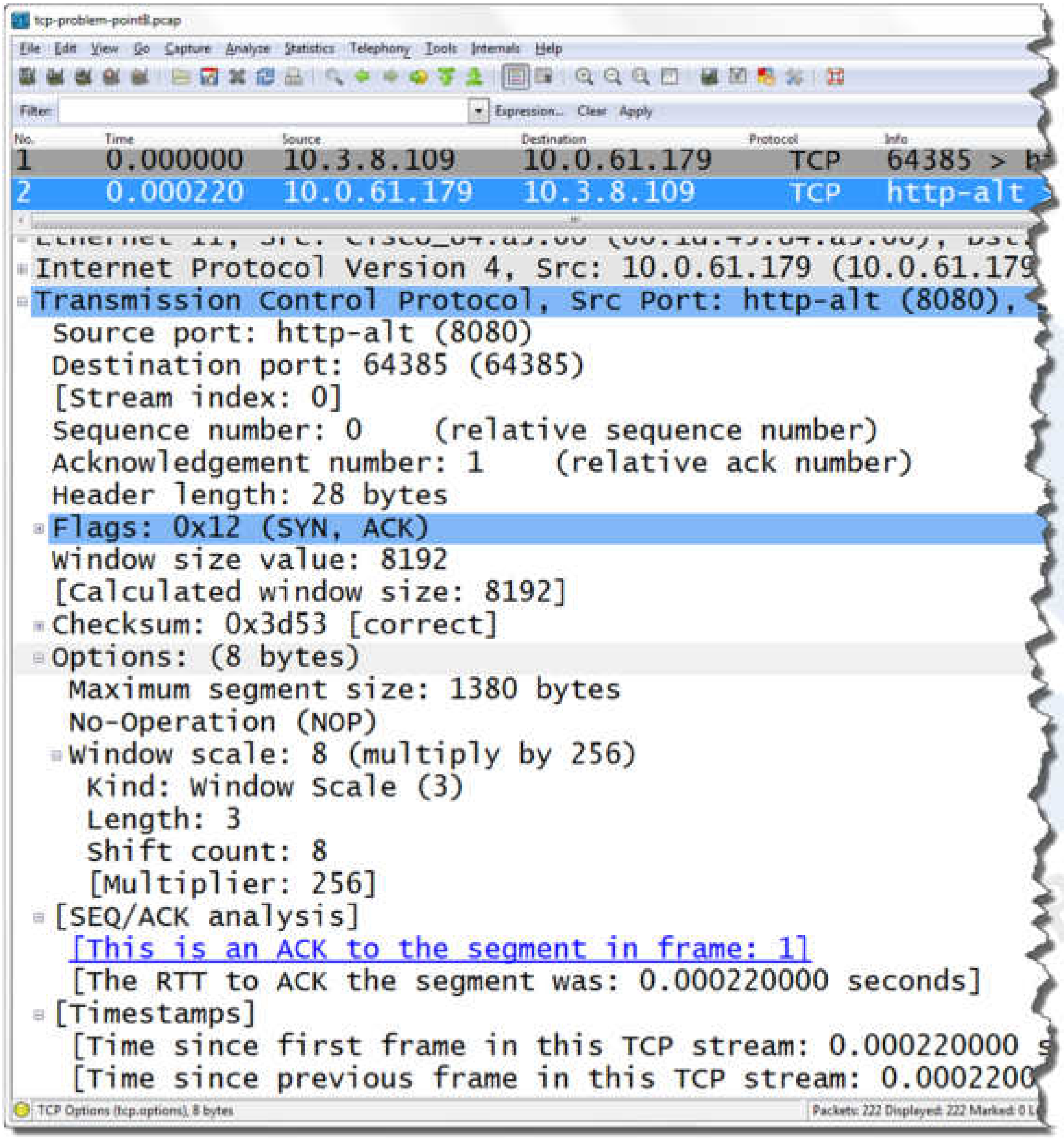
Book an Onsite Course

Visit Us

Chappell University
All Access Pass Portal
Wireshark University
Wireshark Book Website
Blog: In Laura's Lab
Cafe Press FunHouse

ISO image online at lcuportal2.com

The All-Important Handshake



```
No.  Time      Source        Destination   Protocol  Info
1    0.000000  10.3.8.109    10.0.61.179   TCP       64385 > h
2    0.000220  10.0.61.179   10.3.8.109    TCP       http-alt >
```

```
Ethernet II, Src: Cisco_64:a5:00 (00:1d:45:64:a5:00), Dst:
Internet Protocol Version 4, Src: 10.0.61.179 (10.0.61.179
Transmission Control Protocol, Src Port: http-alt (8080),
  Source port: http-alt (8080)
  Destination port: 64385 (64385)
  [Stream index: 0]
  Sequence number: 0    (relative sequence number)
  Acknowledgement number: 1    (relative ack number)
  Header length: 28 bytes
  Flags: 0x12 (SYN, ACK)
  Window size value: 8192
  [Calculated window size: 8192]
  Checksum: 0x3d53 [correct]
  Options: (8 bytes)
    Maximum segment size: 1380 bytes
    No-Operation (NOP)
    Window scale: 8 (multiply by 256)
      Kind: Window Scale (3)
      Length: 3
      Shift count: 8
      [Multiplier: 256]
  [SEQ/ACK analysis]
    [This is an ACK to the segment in frame: 1]
    [The RTT to ACK the segment was: 0.000220000 seconds]
  [Timestamps]
    [Time since first frame in this TCP stream: 0.000220000 s
    [Time since previous frame in this TCP stream: 0.000220
```

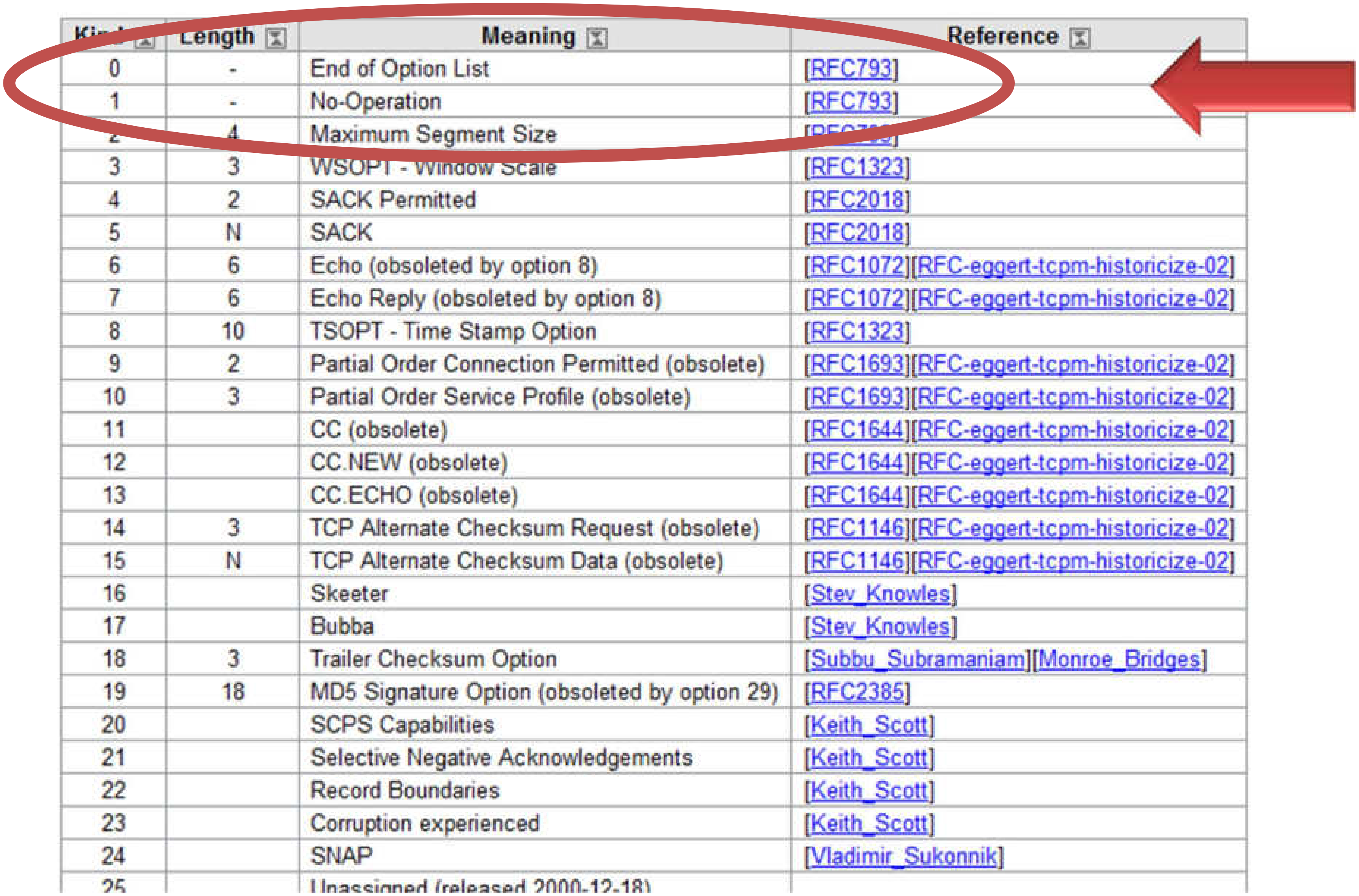
```
TCP Options (tcp.options), 8 bytes        Packets: 222 Displayed: 222 Marked: 0 L
```

Focus on:

- Window Size
- Options

TCP Options

www.iana.org/assignments/tcp-parameters/tcp-parameters.xml



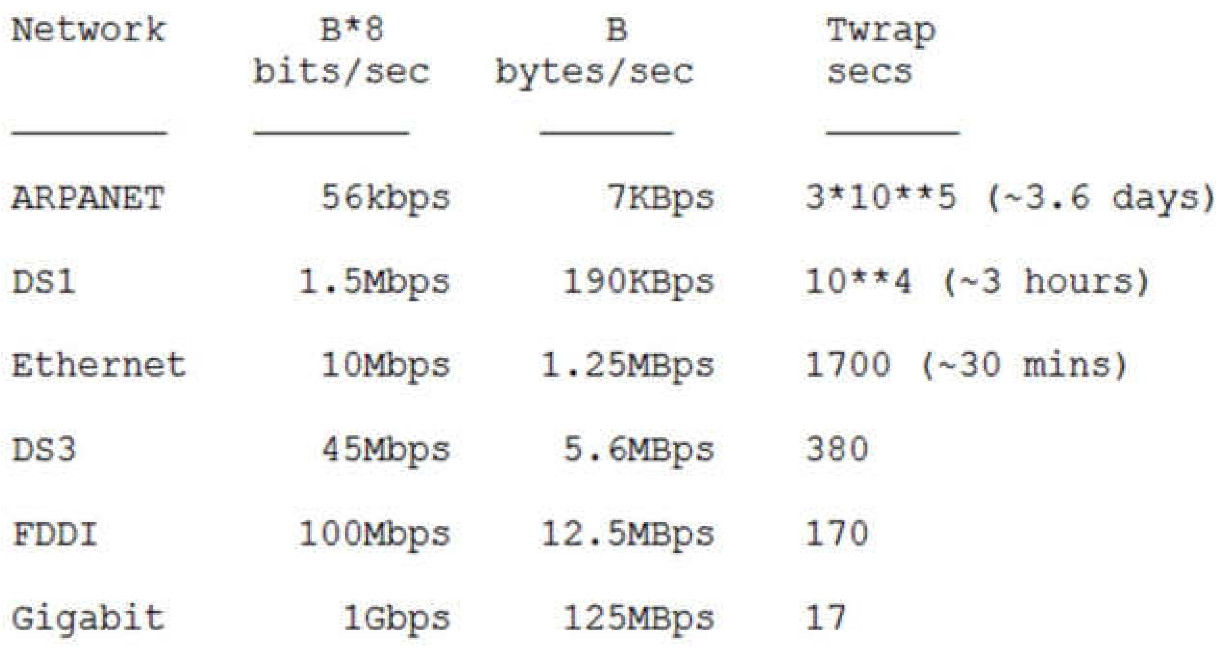
Kind	Length	Meaning	Reference
0	-	End of Option List	[RFC793]
1	-	No-Operation	[RFC793]
2	4	Maximum Segment Size	[RFC793]
3	3	WSOPT - Window Scale	[RFC1323]
4	2	SACK Permitted	[RFC2018]
5	N	SACK	[RFC2018]
6	6	Echo (obsoleted by option 8)	[RFC1072][RFC-eggert-tcpm-historicize-02]
7	6	Echo Reply (obsoleted by option 8)	[RFC1072][RFC-eggert-tcpm-historicize-02]
8	10	TSOPT - Time Stamp Option	[RFC1323]
9	2	Partial Order Connection Permitted (obsolete)	[RFC1693][RFC-eggert-tcpm-historicize-02]
10	3	Partial Order Service Profile (obsolete)	[RFC1693][RFC-eggert-tcpm-historicize-02]
11		CC (obsolete)	[RFC1644][RFC-eggert-tcpm-historicize-02]
12		CC.NEW (obsolete)	[RFC1644][RFC-eggert-tcpm-historicize-02]
13		CC.ECHO (obsolete)	[RFC1644][RFC-eggert-tcpm-historicize-02]
14	3	TCP Alternate Checksum Request (obsolete)	[RFC1146][RFC-eggert-tcpm-historicize-02]
15	N	TCP Alternate Checksum Data (obsolete)	[RFC1146][RFC-eggert-tcpm-historicize-02]
16		Skeeter	[Stev_Knowles]
17		Bubba	[Stev_Knowles]
18	3	Trailer Checksum Option	[Subbu_Subramaniam][Monroe_Bridges]
19	18	MD5 Signature Option (obsoleted by option 29)	[RFC2385]
20		SCPS Capabilities	[Keith_Scott]
21		Selective Negative Acknowledgements	[Keith_Scott]
22		Record Boundaries	[Keith_Scott]
23		Corruption experienced	[Keith_Scott]
24		SNAP	[Vladimir_Sukonnik]
25		Unassigned (released 2000-12-18)	

The Ideal Handshake…

- MSS is decent size
- Window Scaling is enabled and shift factor is OK (watch out for a shift factor of 0)
- SACK is enabled
- Timestamp is on for high speed links (PAWS)
- Taken at client, the RTT is acceptable

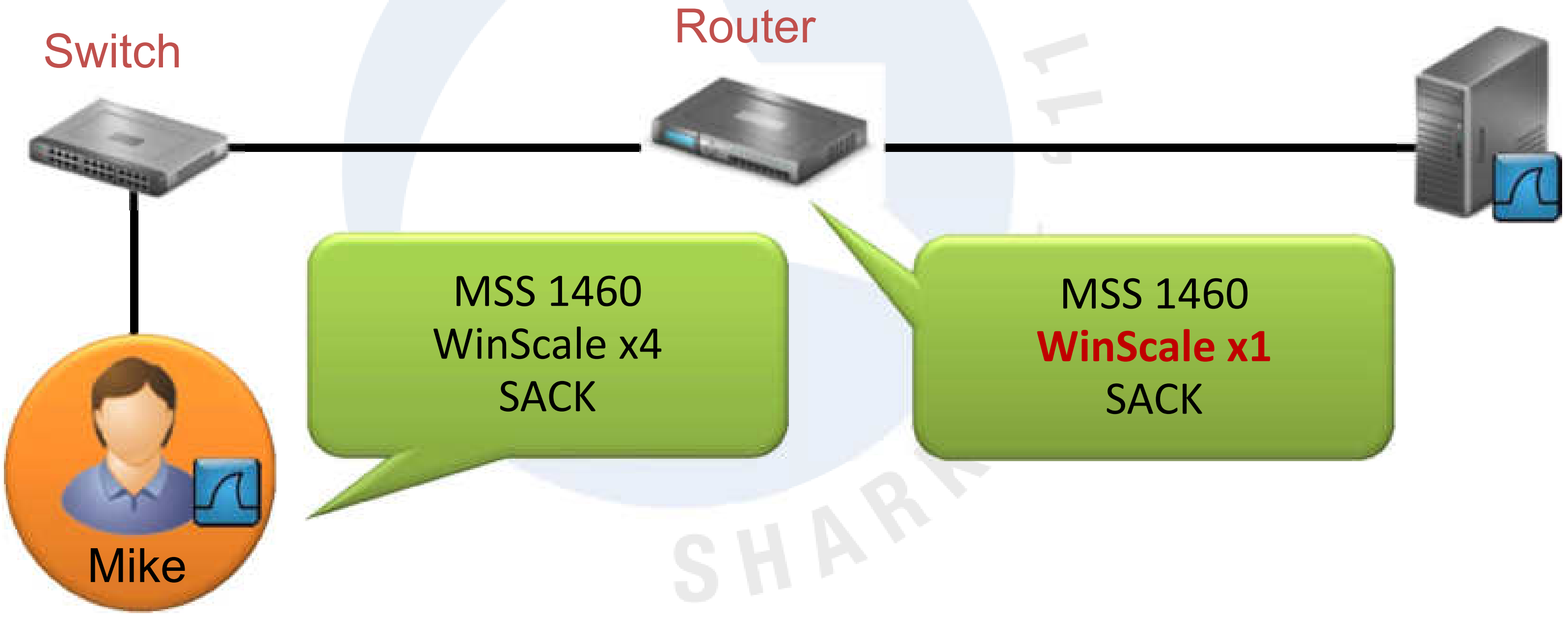
PAWS (RFC 1323)

- Protection Against Wrapped Sequence Numbers

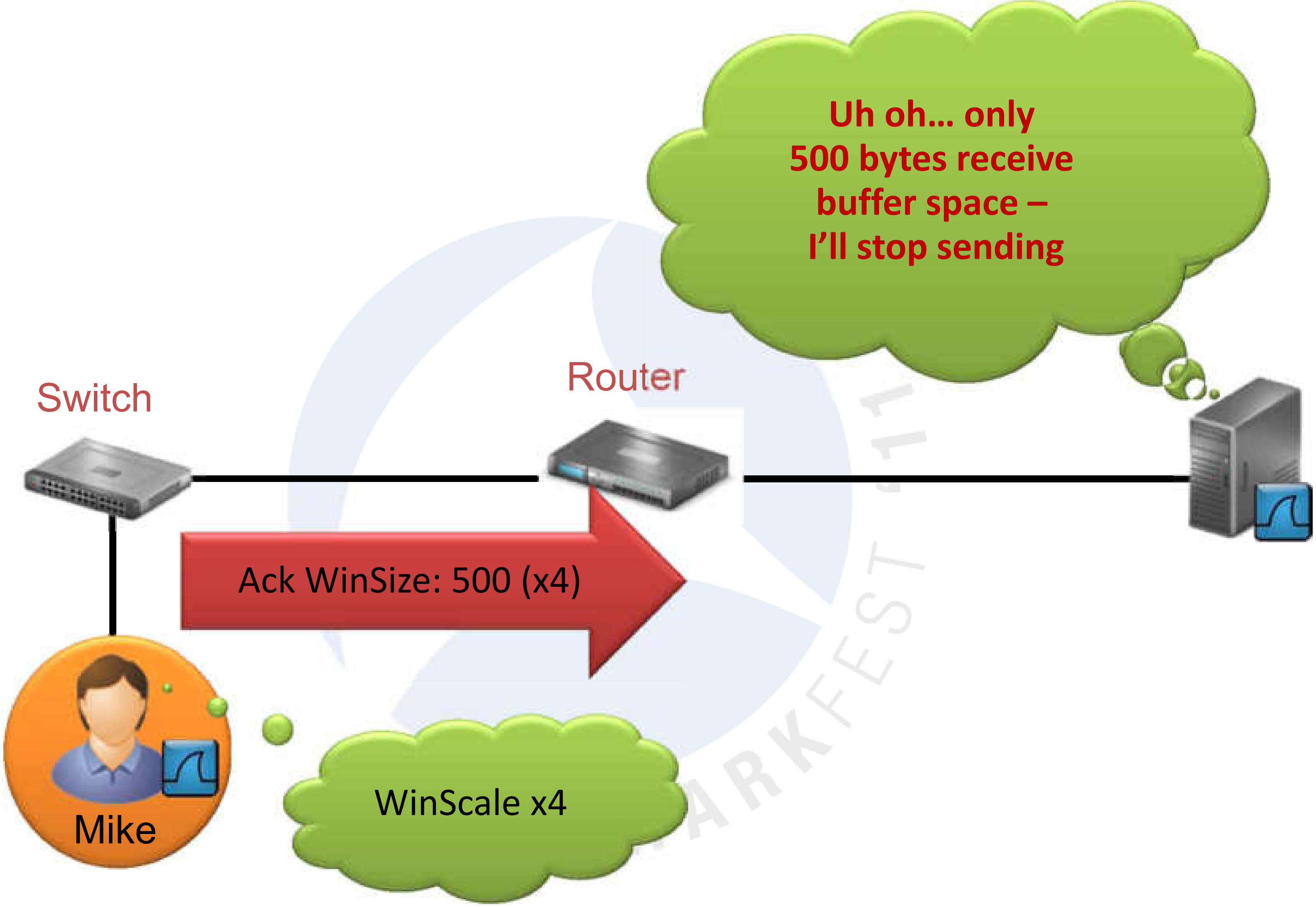


Network	B*8	B	Twrap
	bits/sec	bytes/sec	secs
ARPANET	56kbps	7KBps	3*10**5 (~3.6 days)
DS1	1.5Mbps	190KBps	10**4 (~3 hours)
Ethernet	10Mbps	1.25MBps	1700 (~30 mins)
DS3	45Mbps	5.6MBps	380
FDDI	100Mbps	12.5MBps	170
Gigabit	1Gbps	125MBps	17

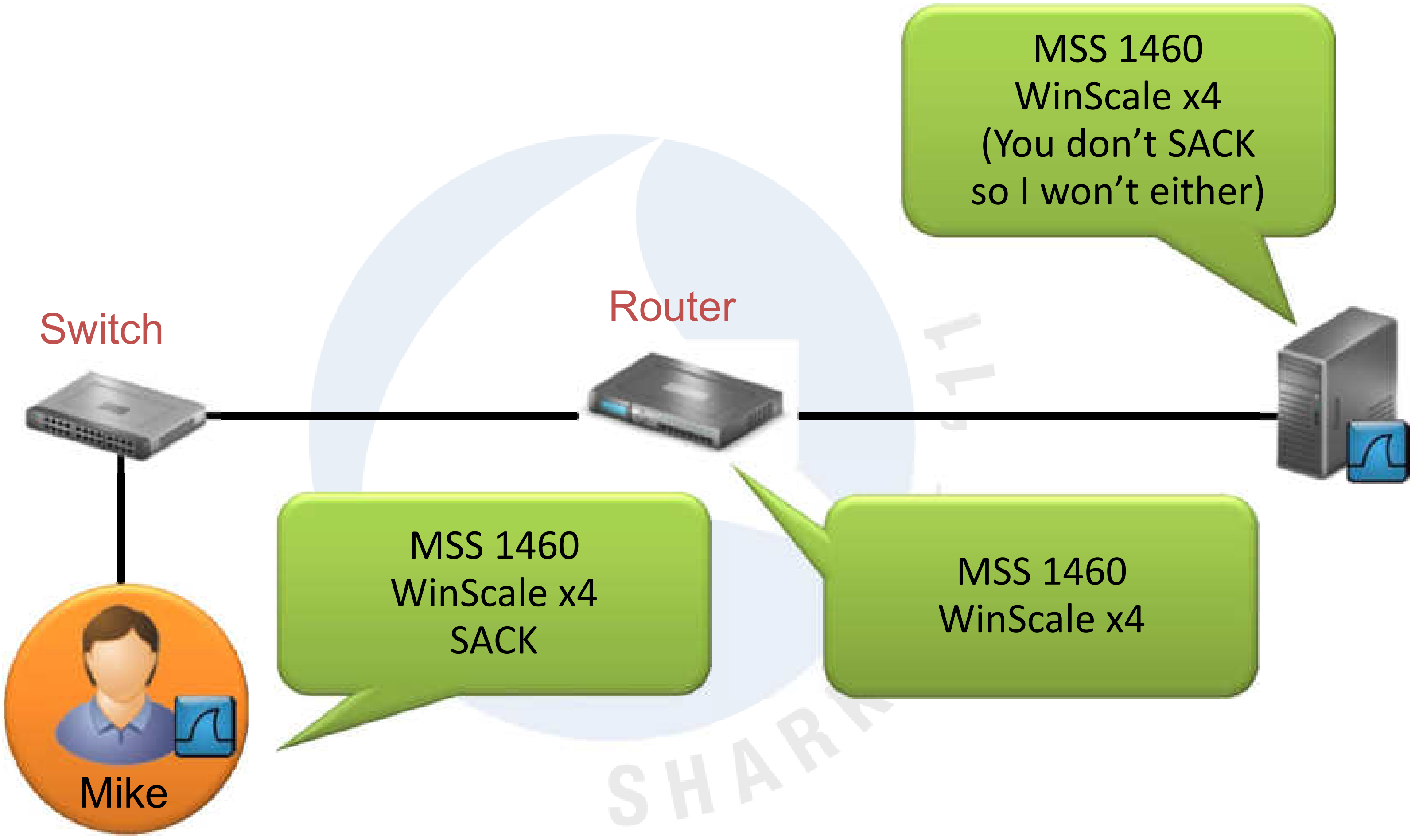
The Problem Handshake #1



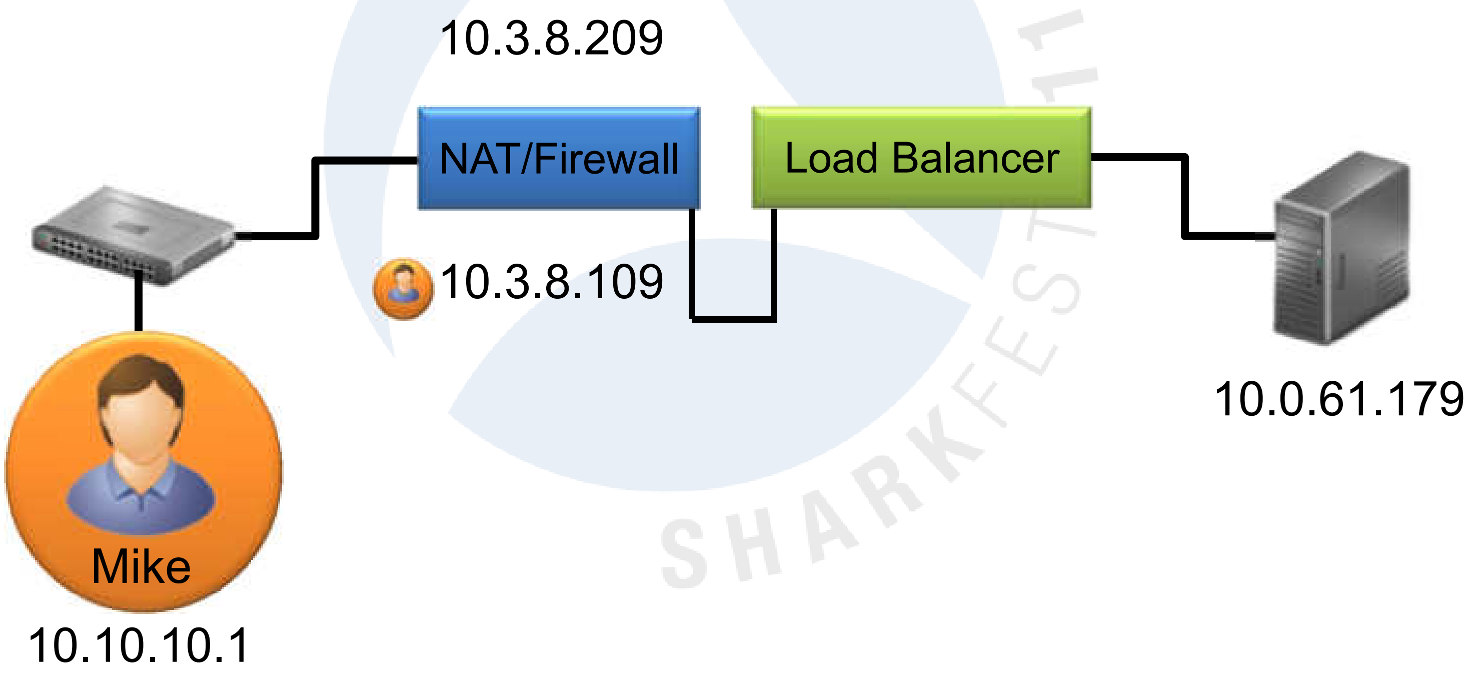
The Problem Handshake #1



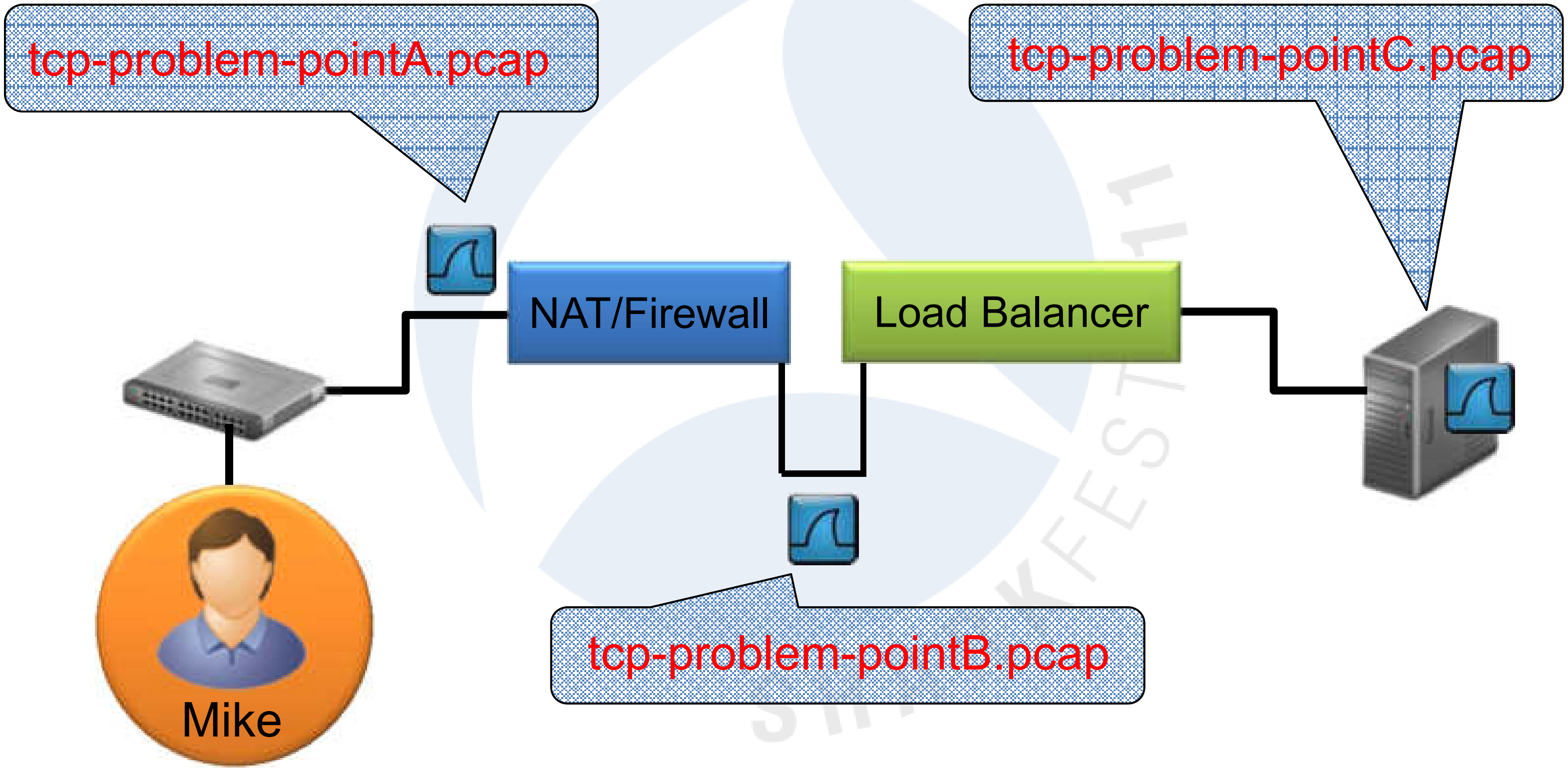
The Problem Handshake #2



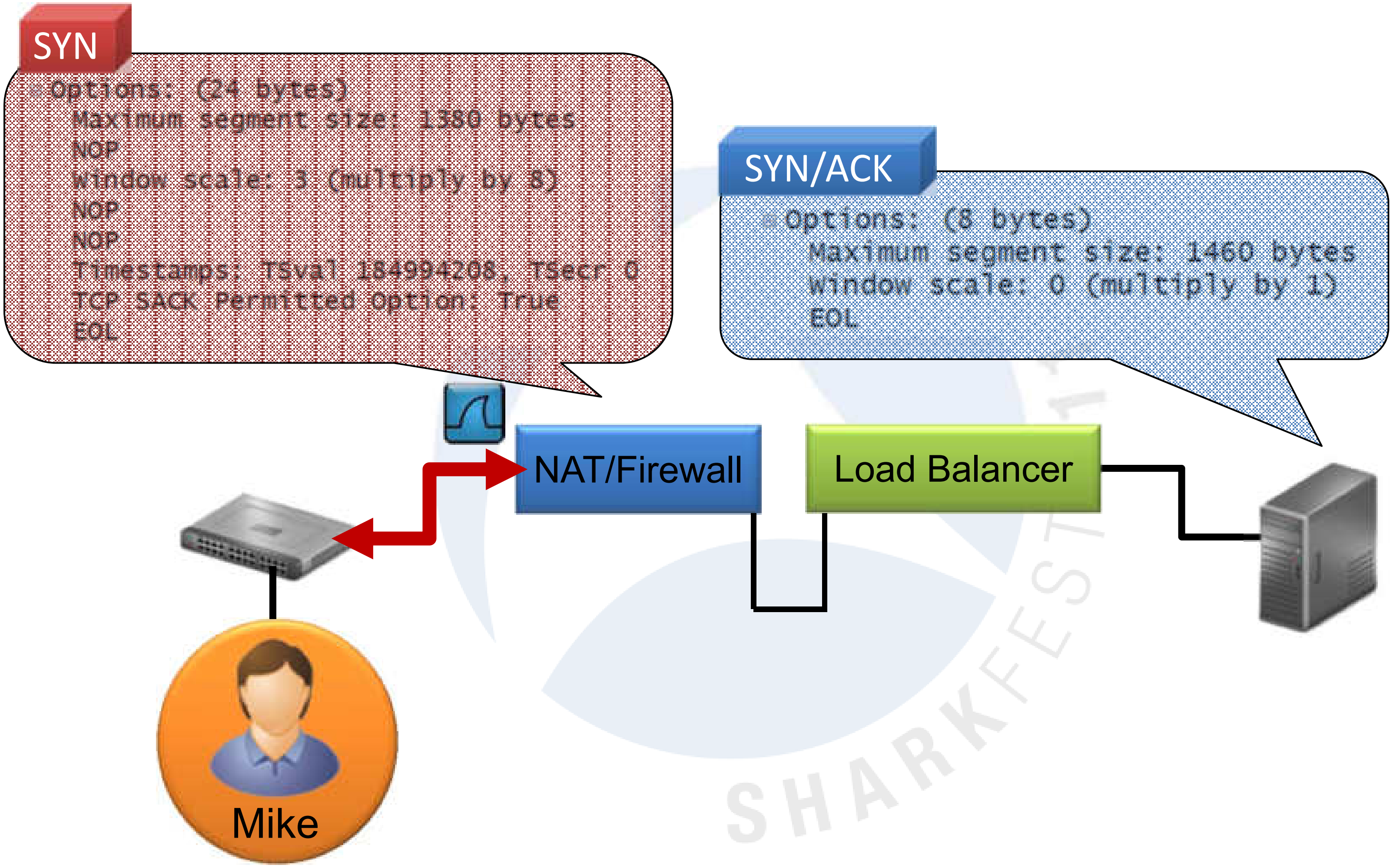
Let’s Analyze a Problem



Let’s Analyze a Problem



Connection at Point A



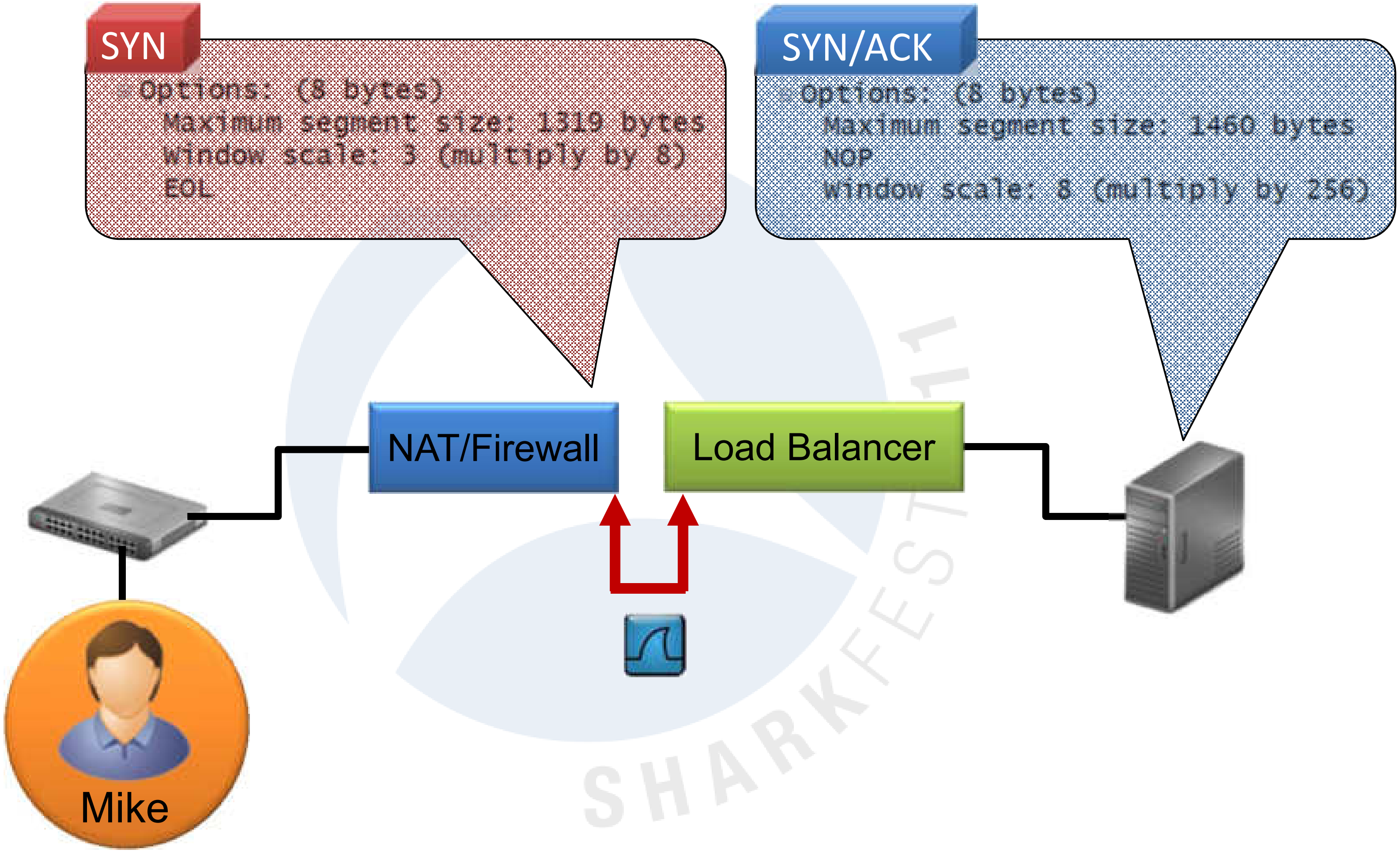
SYN

```
⊟Options: (24 bytes)
   Maximum segment size: 1380 bytes
   NOP
   Window scale: 3 (multiply by 8)
   NOP
   NOP
   Timestamps: TSval 184994208, TSecr 0
   TCP SACK Permitted Option: True
   EOL
```

SYN/ACK

```
⊟Options: (8 bytes)
   Maximum segment size: 1460 bytes
   Window scale: 0 (multiply by 1)
   EOL
```

Connection at Point B



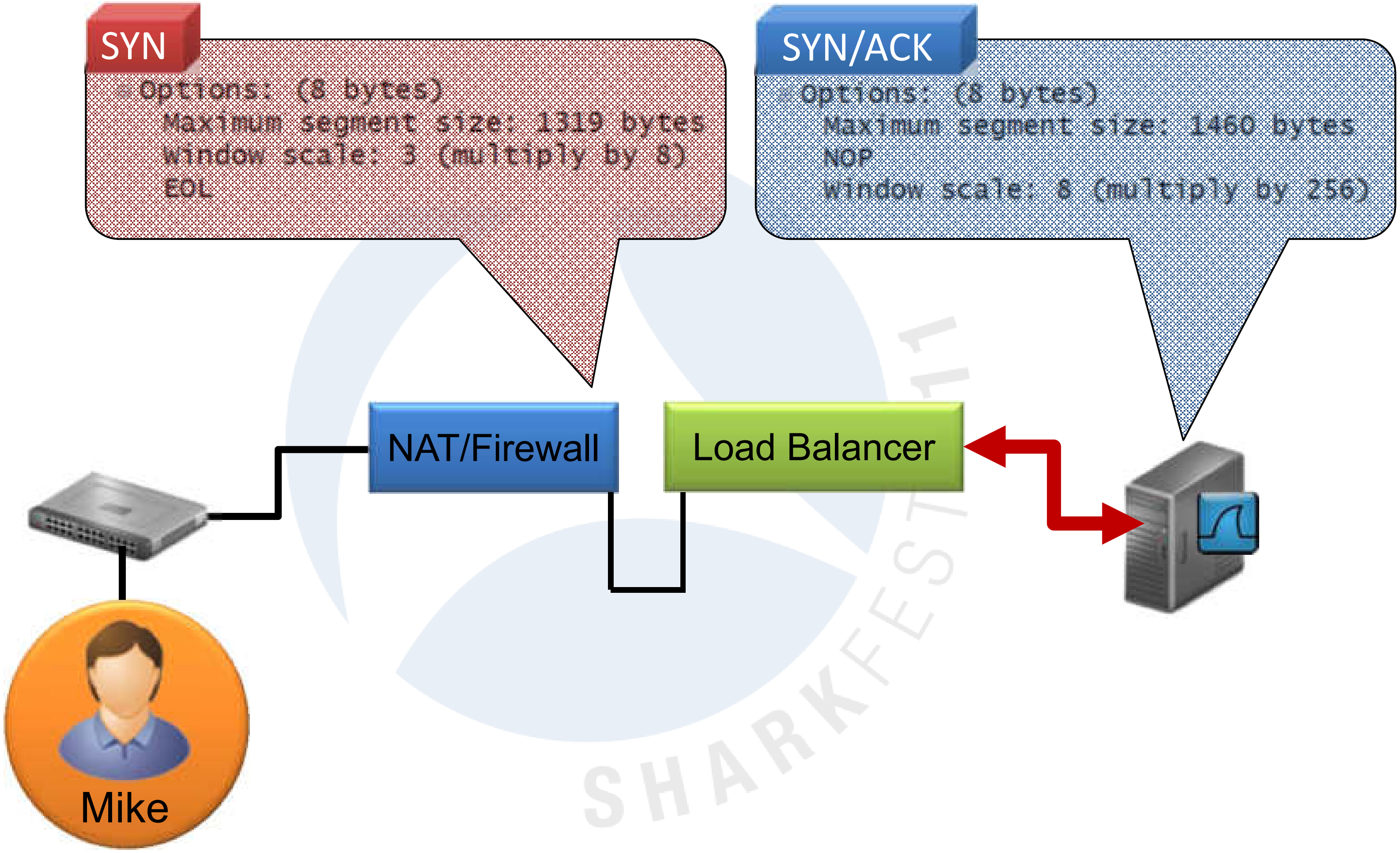
SYN

```
Options: (8 bytes)
  Maximum segment size: 1319 bytes
  Window scale: 3 (multiply by 8)
  EOL
```

SYN/ACK

```
Options: (8 bytes)
  Maximum segment size: 1460 bytes
  NOP
  Window scale: 8 (multiply by 256)
```

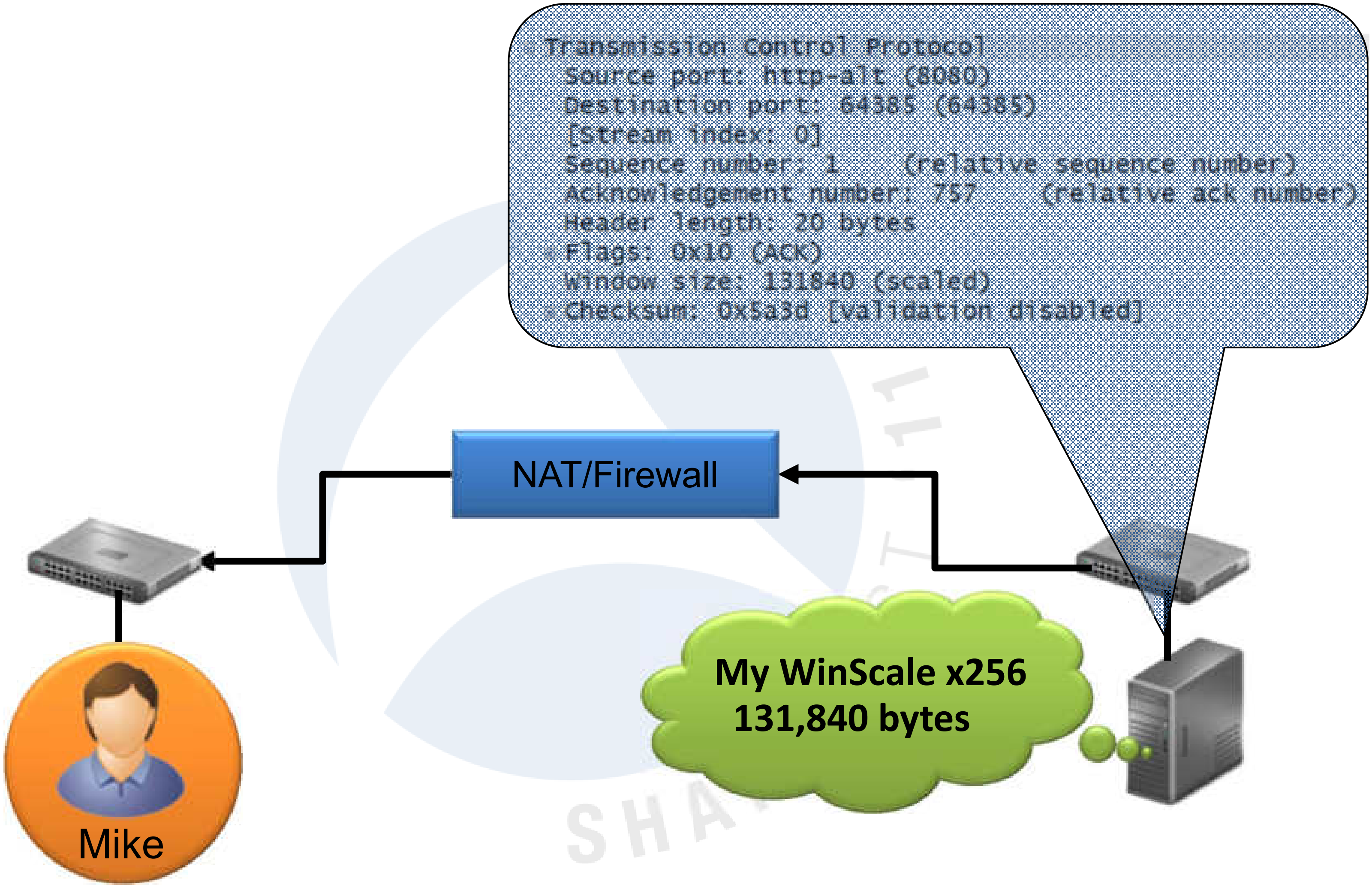
Connection at Point C



```
Options: (8 bytes)
   Maximum segment size: 1319 bytes
   Window scale: 3 (multiply by 8)
   EOL
```

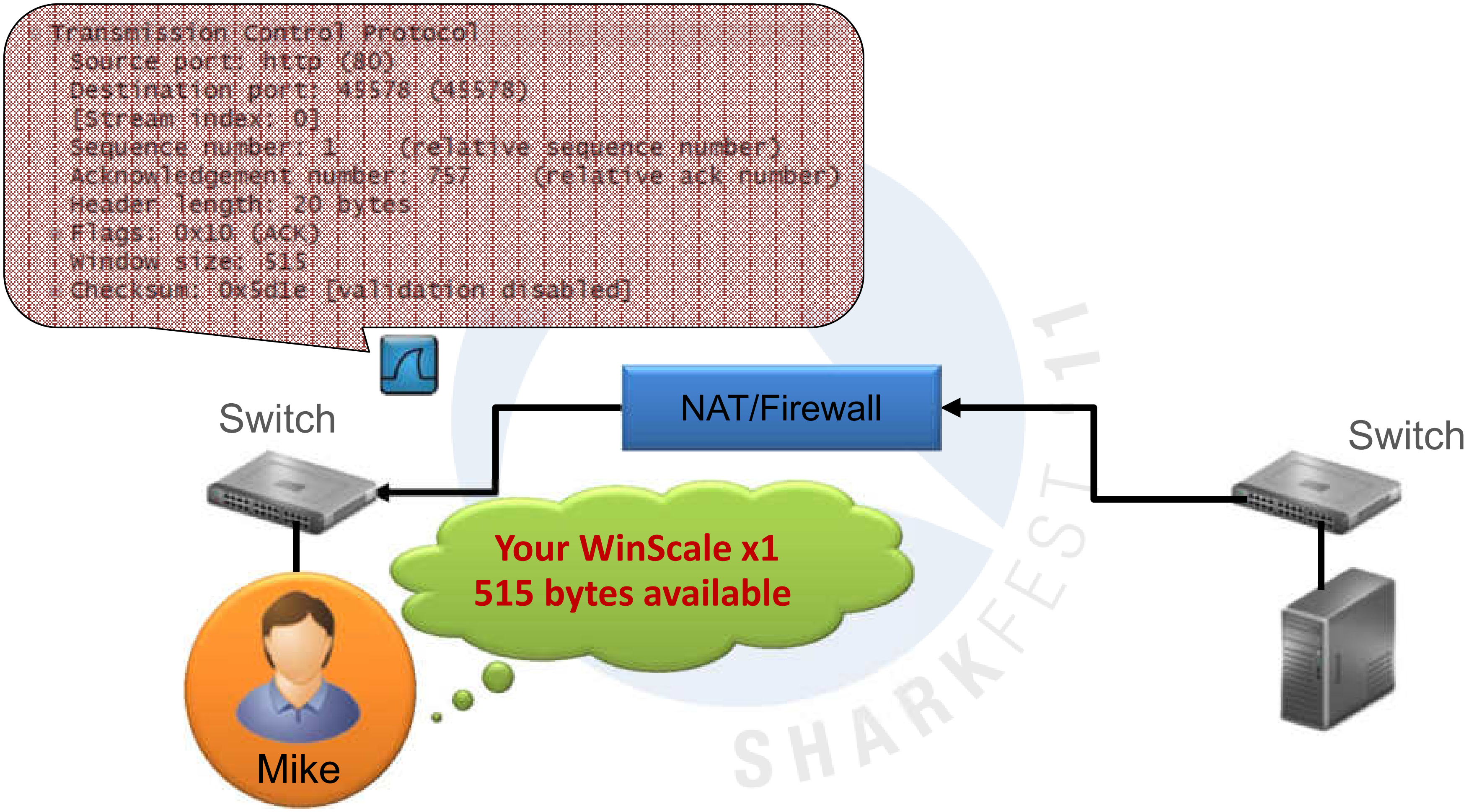
```
Options: (8 bytes)
   Maximum segment size: 1460 bytes
   NOP
   Window scale: 8 (multiply by 256)
```

The Beliefs



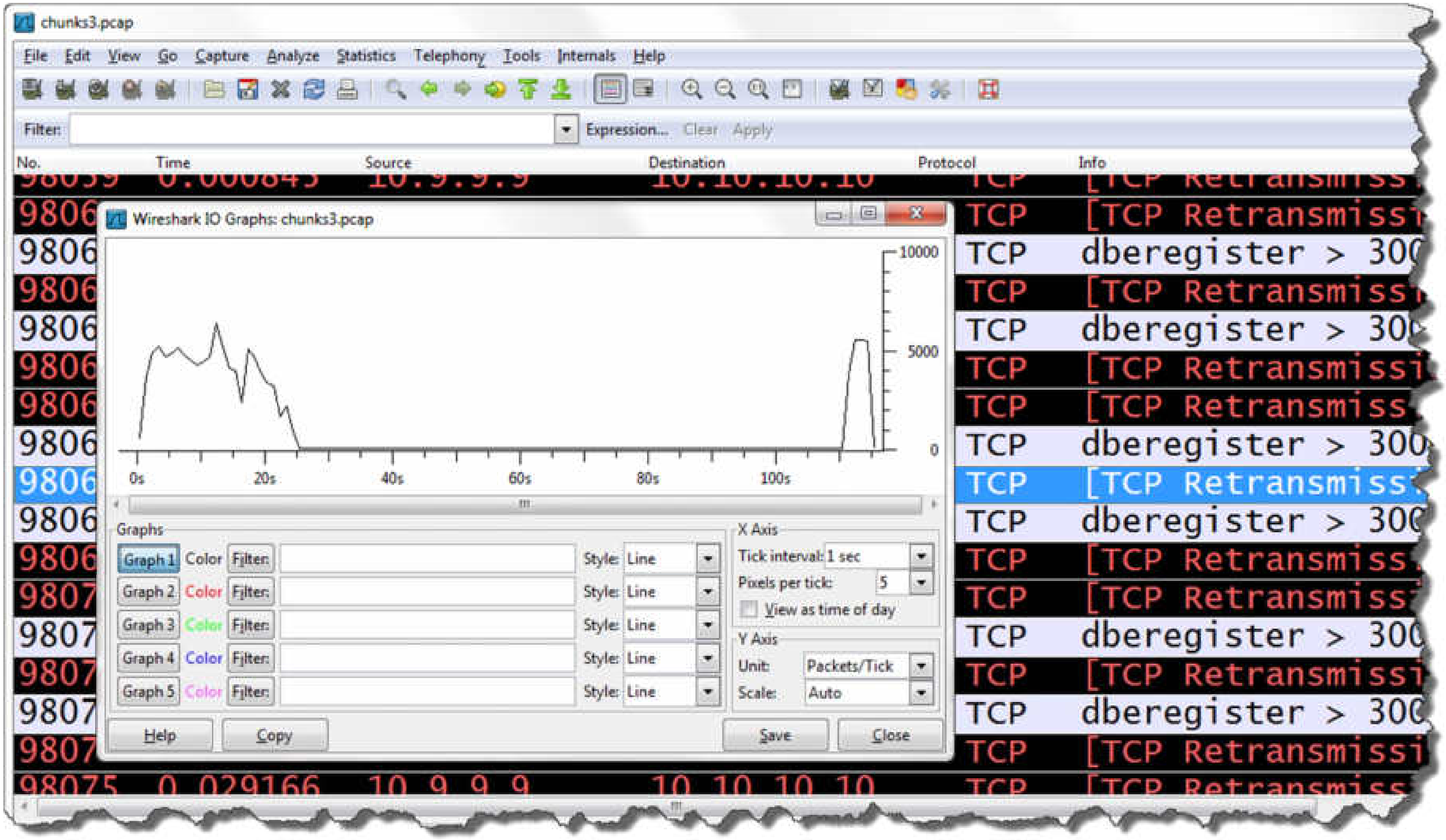
```
Transmission Control Protocol
  Source port: http-alt (8080)
  Destination port: 64385 (64385)
  [Stream index: 0]
  Sequence number: 1    (relative sequence number)
  Acknowledgement number: 757    (relative ack number)
  Header length: 20 bytes
  Flags: 0x10 (ACK)
  Window size: 131840 (scaled)
  Checksum: 0x5a3d [validation disabled]
```

The Beliefs



```
Transmission Control Protocol
  Source port: http (80)
  Destination port: 45578 (45578)
  [Stream index: 0]
  Sequence number: 1    (relative sequence number)
  Acknowledgement number: 757    (relative ack number)
  Header length: 20 bytes
  Flags: 0x10 (ACK)
  Window size: 515
  Checksum: 0x5d1e [validation disabled]
```

What About this Issue?



```
No.     Time       Source     Destination   Protocol  Info
98059   0.000843   10.9.9.9   10.10.10.10   TCP       [TCP Retransmiss
9806                                        TCP       [TCP Retransmissi
9806                                        TCP       dberegister > 30(
9806                                        TCP       [TCP Retransmiss
9806                                        TCP       dberegister > 30(
9806                                        TCP       [TCP Retransmissi
9806                                        TCP       [TCP Retransmiss
9806                                        TCP       dberegister > 30(
9806                                        TCP       [TCP Retransmiss
9806                                        TCP       dberegister > 30(
9806                                        TCP       [TCP Retransmiss
9807                                        TCP       [TCP Retransmiss
9807                                        TCP       dberegister > 30(
9807                                        TCP       [TCP Retransmissi
9807                                        TCP       dberegister > 30(
9807                                        TCP       [TCP Retransmissi
98075   0.029166   10.9.9.9   10.10.10.10   TCP       [TCP Retransmiss
```

Graph 1–5: Style: Line

Tick interval: 1 sec

Pixels per tick: 5

☐ View as time of day

Unit: Packets/Tick

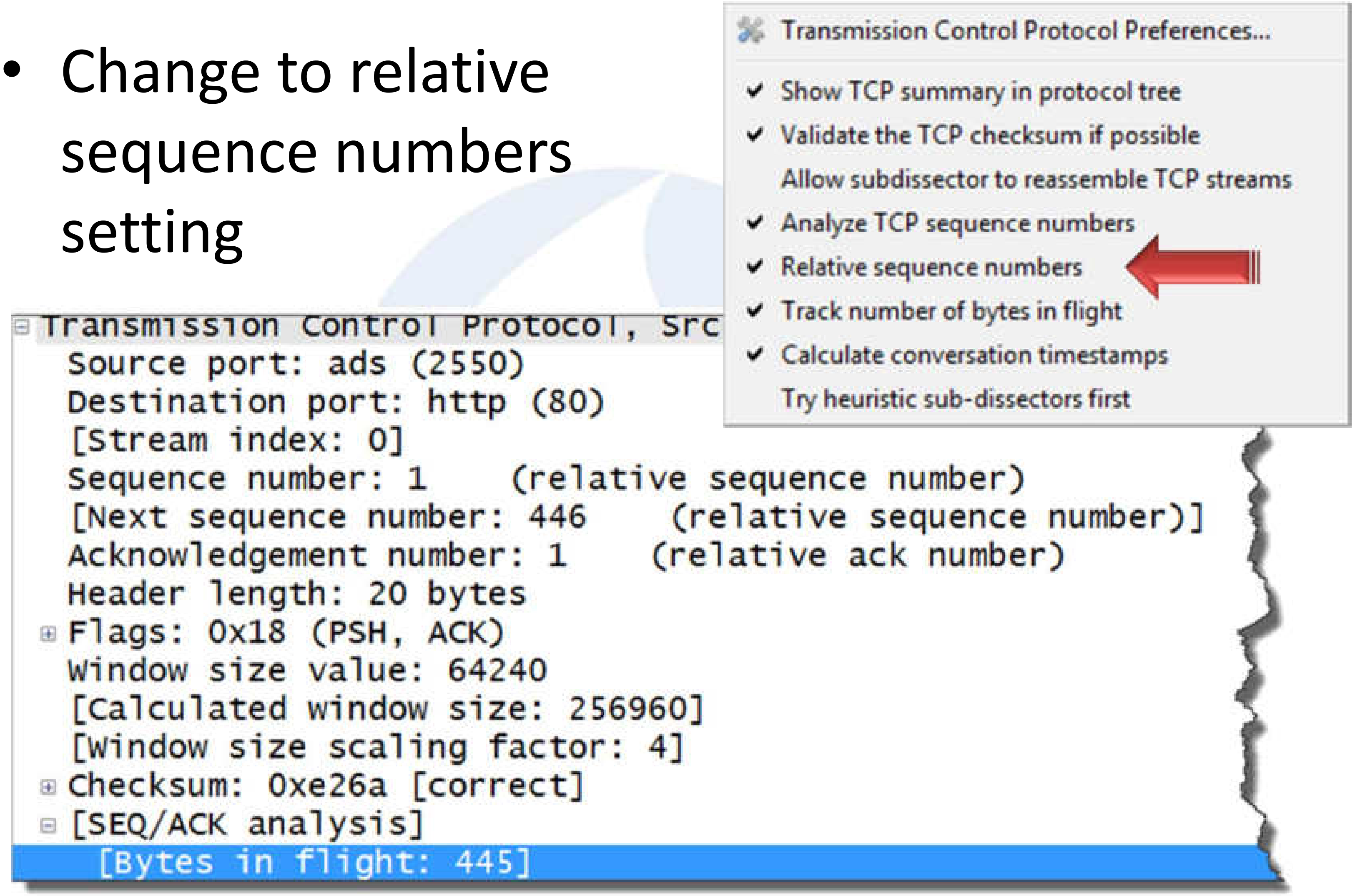
Scale: Auto

Use Wireshark TCP Analysis Flags

- **tcp.analysis.flags**
- tcp.analysis.lost_segment
- tcp.analysis.retransmission
- tcp.analysis.fast_retransmission
- tcp.analysis.duplicate_ack
- tcp.analysis.out_of_order
- tcp.analysis.window_full
- tcp.analysis.zero_window

BTW: TCP Preferences Change

- Change to relative sequence numbers setting

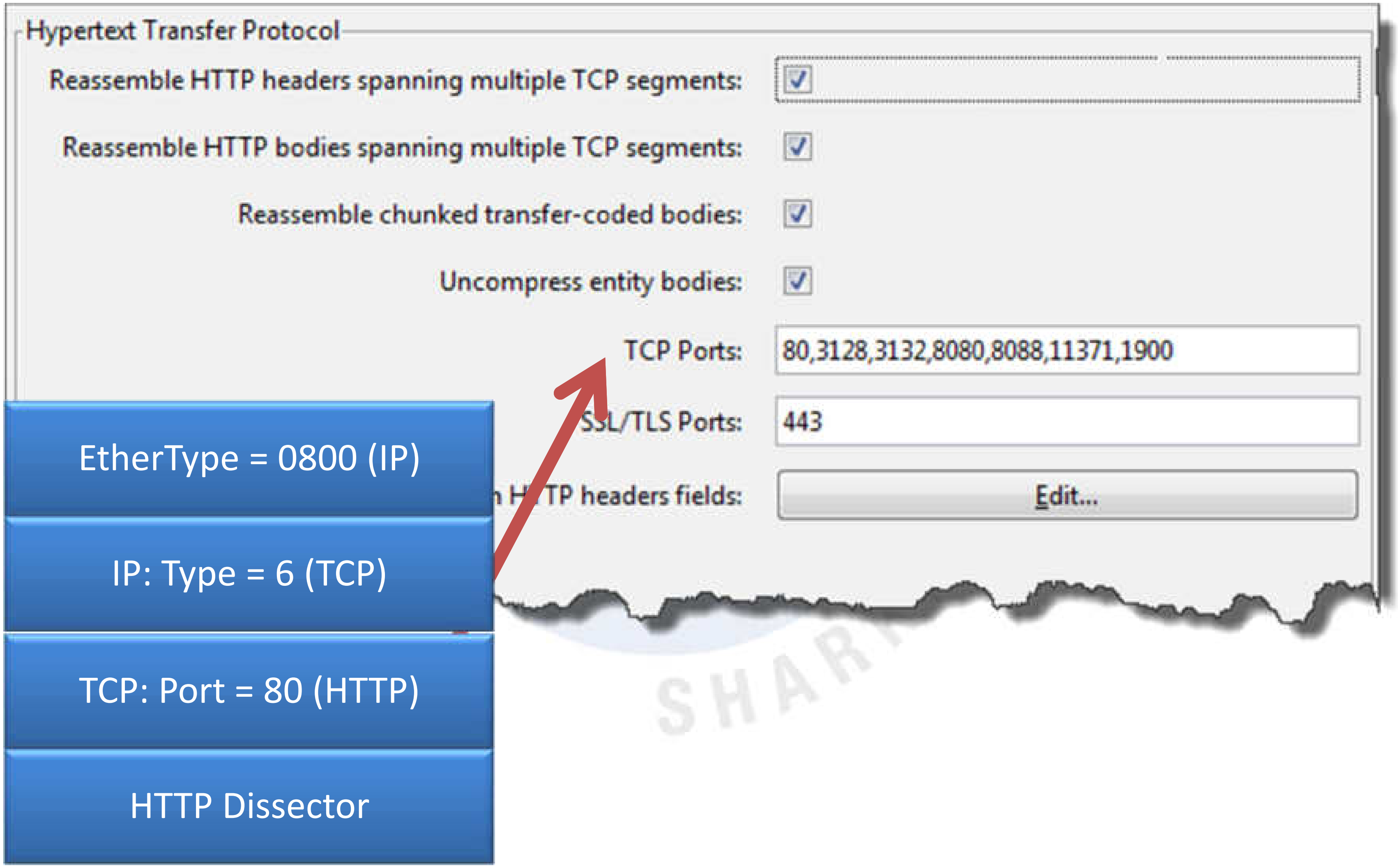


Transmission Control Protocol Preferences...

- ✓ Show TCP summary in protocol tree
- ✓ Validate the TCP checksum if possible
- Allow subdissector to reassemble TCP streams
- ✓ Analyze TCP sequence numbers
- ✓ Relative sequence numbers
- ✓ Track number of bytes in flight
- ✓ Calculate conversation timestamps
- Try heuristic sub-dissectors first

```
⊟ Transmission Control Protocol, Src
    Source port: ads (2550)
    Destination port: http (80)
    [Stream index: 0]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 446    (relative sequence number)]
    Acknowledgement number: 1    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x18 (PSH, ACK)
    Window size value: 64240
    [Calculated window size: 256960]
    [Window size scaling factor: 4]
  ⊞ Checksum: 0xe26a [correct]
  ⊟ [SEQ/ACK analysis]
      [Bytes in flight: 445]
```

BTW: Using a Heuristic Dissector



Hypertext Transfer Protocol

Reassemble HTTP headers spanning multiple TCP segments: ☑

Reassemble HTTP bodies spanning multiple TCP segments: ☑

Reassemble chunked transfer-coded bodies: ☑

Uncompress entity bodies: ☑

TCP Ports: 80,3128,3132,8080,8088,11371,1900

SSL/TLS Ports: 443

n HTTP headers fields: Edit...

EtherType = 0800 (IP)

IP: Type = 6 (TCP)

TCP: Port = 80 (HTTP)

HTTP Dissector

Questions?

laura@chappellU.com
(download the ISO of LLK10 at
lcuportal.com)

Online Dating

Because crabs are filtered through the Internet