

Download Laura's Trace Files at [www.wiresharktraining.com/sharkfest09](http://www.wiresharktraining.com/sharkfest09)

# Tips and Tricks: Case Studies

## Laura Chappell

Founder, Wireshark University

<http://www.wiresharktraining.com> | [laura@wiresharktraining.com](mailto:laura@wiresharktraining.com)

Presenter, Wireshark Jumpstart Series

<http://www.chappellseminars.com> | [laura@chappellseminars.com](mailto:laura@chappellseminars.com)

## SHARKFEST '09

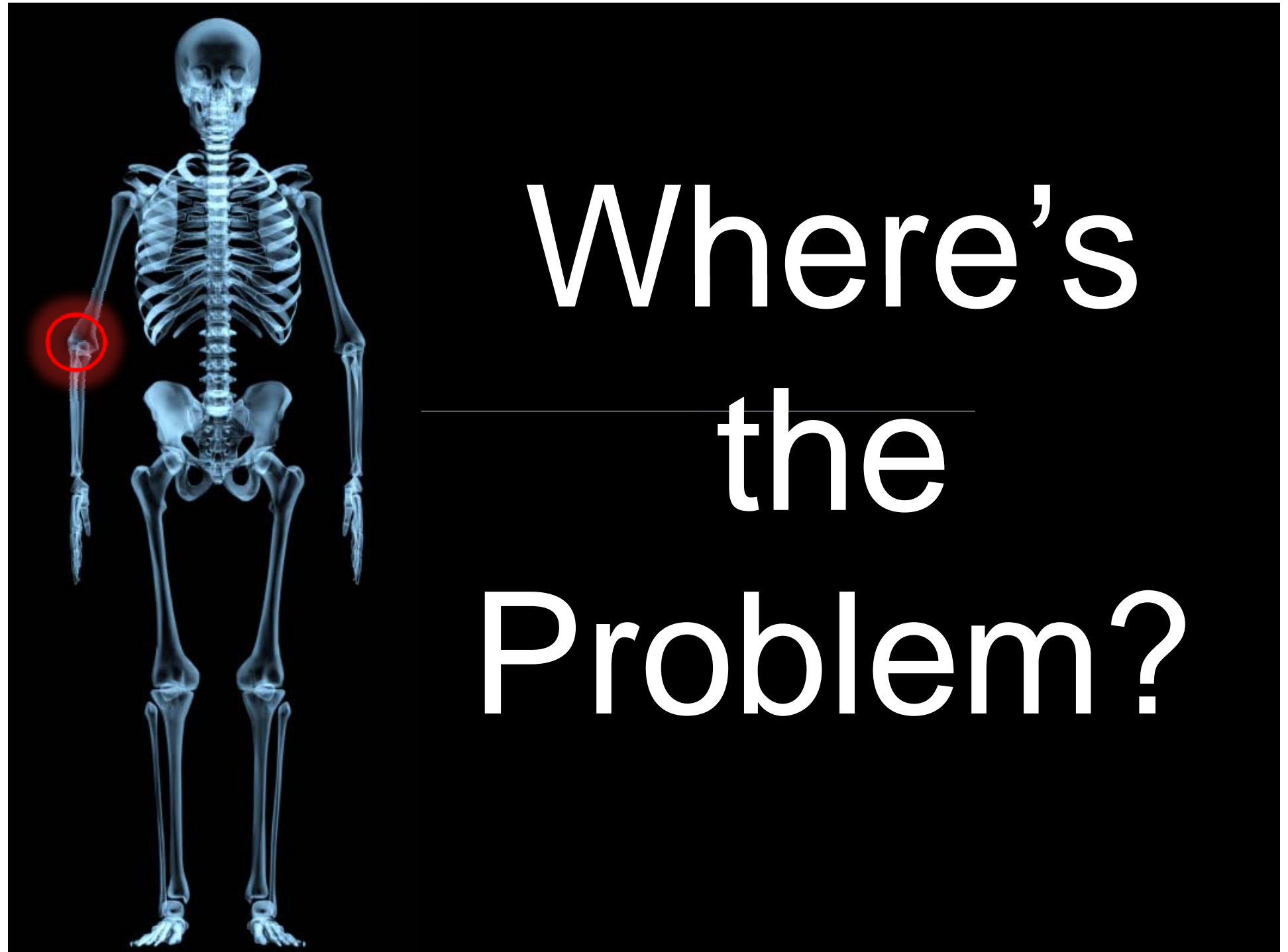
Stanford University

June 15<sup>th</sup>, 2009 10:45-12:15



# In this Session

- **Attacking Enterprise Problems**
- **The Case of the Lousy Latency**
- **The Case of the Sputtering Stream**



Where's  
the  
Problem?



# Packet Pigs

# The Case of the Lousy Latency

**Video-based application requires consistent availability of 20 Mbps throughput to run properly.**

**The latency is measured at 100ms.**

**It looks terrible now.**

# Tcp1323Opts

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\  
Parameters

Add a new Registry DWORD for Tcp1323Opts

## Tcp1323Opts

**Key:** Tcpip\Parameters

**Value Type:** REG\_DWORD—number (flags)

**Valid Range:** 0, 1, 2, 3

0 (disable RFC 1323 options)

**1 (window scaling enabled only)**

2 (timestamps enabled only)

3 (both options enabled)

**Default:** No value.

# TcpWindowSize

**Key:** Tcpip\Parameters

**Value Type:** REG\_DWORD—Number of bytes

**Valid Range:** 0–0x3FFFFFFF (1073741823 decimal; however, values greater than 64 KB can only be achieved when connecting to other systems that support RFC 1323 window scaling)

**Default:** This parameter does not exist by default.

# Calculating Bandwidth\*Delay Product

## Bandwidth\*delay product:

- measures amount of data that will fill the pipe
- defines the buffer space at sender and receiver to gain maximum throughput on the TCP connection over the path
- defines the amount of unacknowledged data TCP must handle to keep pipe full

$$\begin{array}{r} 100 \text{ (Mbps)} \\ \times 0.1 \text{ (RTT)} \\ \hline 10 \text{ Mb} \end{array}$$

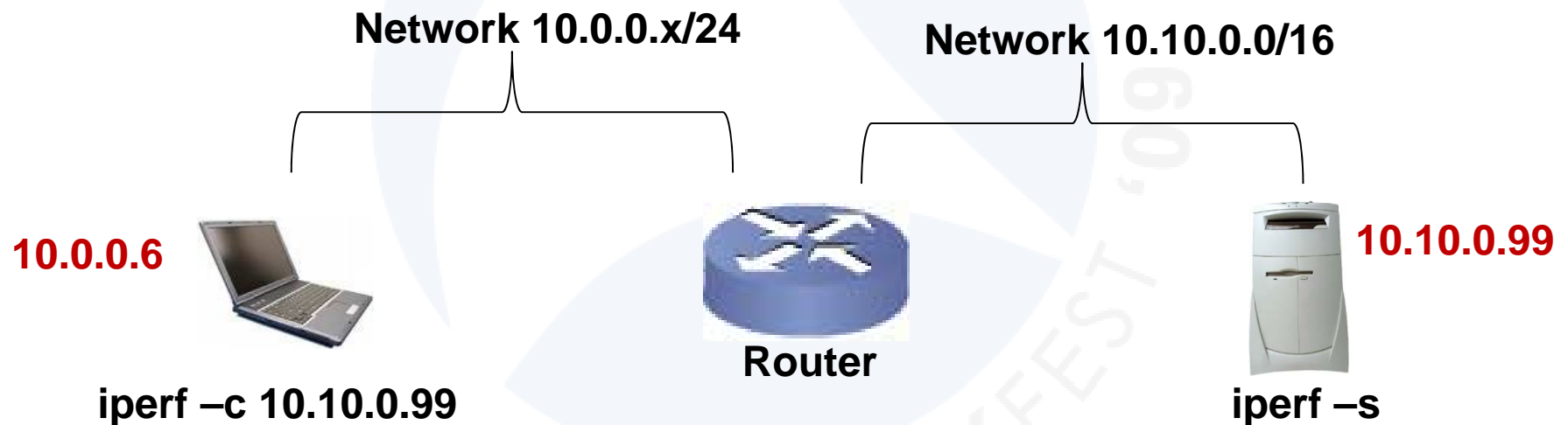
Convert to bytes:

$$10,000,000/8 = 1,250,000$$

~The optimal send/receive buffer sizes are 1.5\*BDP (or 1,875,000 bytes)

# The iPerf Lab Test

The Effects of Latency, TCP Receive Window Size and Window Scaling



# Lab Test Results: Throughput/Scaling Relationship

Lab Test	Delay	A: 1323 On B: rWin- 1,875,000	iperf -s rWin at 1,875,000	iperf -c rWin at 1,875,000	Results
#1: Local iPerf					94.5, 90, 92, 94, 94

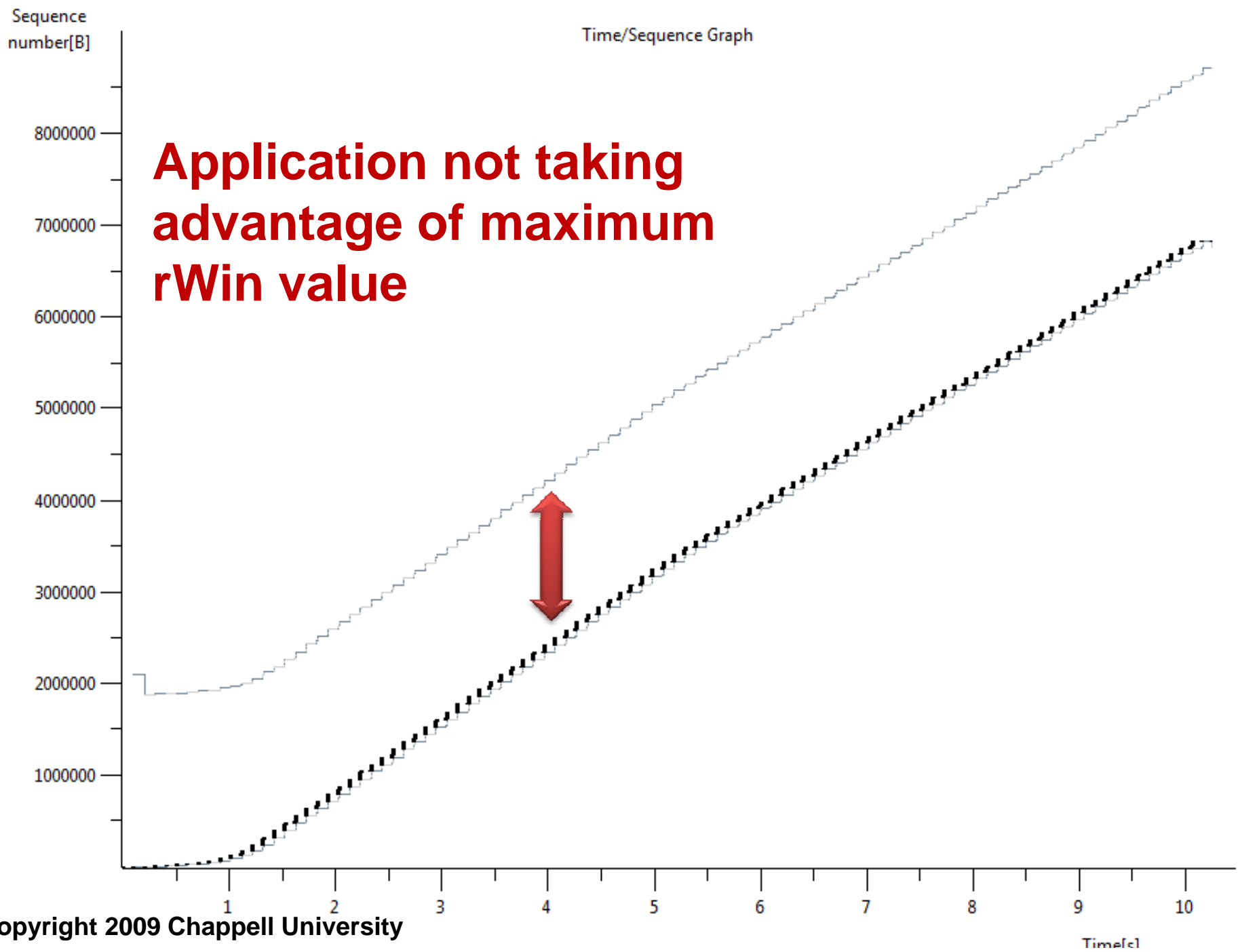
# Lab Test Results: Throughput/Scaling Relationship

Lab Test	Delay	A: 1323 On B: rWin- 1,875,000	iperf -s rWin at 1,875,000	iperf -c rWin at 1,875,000	Results
#1: Local iPerf					94.5, 90, 92, 94, 94
#2: iPerf at 100ms delay	100 ms				4.6, 4.8, 4.58, 4.61, 4.62

# Lab Test Results: Throughput/Scaling Relationship

Lab Test	Delay	A: 1323 On B: rWin- 1,875,000	iperf -s rWin at 1,875,000	iperf -c rWin at 1,875,000	Results
#1: Local iPerf					94.5, 90, 92, 94, 94
#2: iPerf at 100ms delay	100 ms				4.6, 4.8, 4.58, 4.61, 4.62
#3: iPerf w/delay + reg change	100 ms	Reg sets (x32) 1323 on 1,875,000 rWin			5.6, 4.6, 4.7, 4.7, 4.7

**Enabled Window Scaling and increased  
rWin Setting at operating system (XP)**



**Application not taking advantage of maximum rWin value**

# Lab Test Results: Throughput/Scaling Relationship

Lab Test	Delay	A: 1323 On B: rWin- 1,875,000	iperf -s rWin at 1,875,000	iperf -c rWin at 1,875,000	Results
#6: iPerf to 10.10.16.16 w/delay + rWin at receiver set	100 ms	“	Receive window (-w) set at 1,875,000		5.0

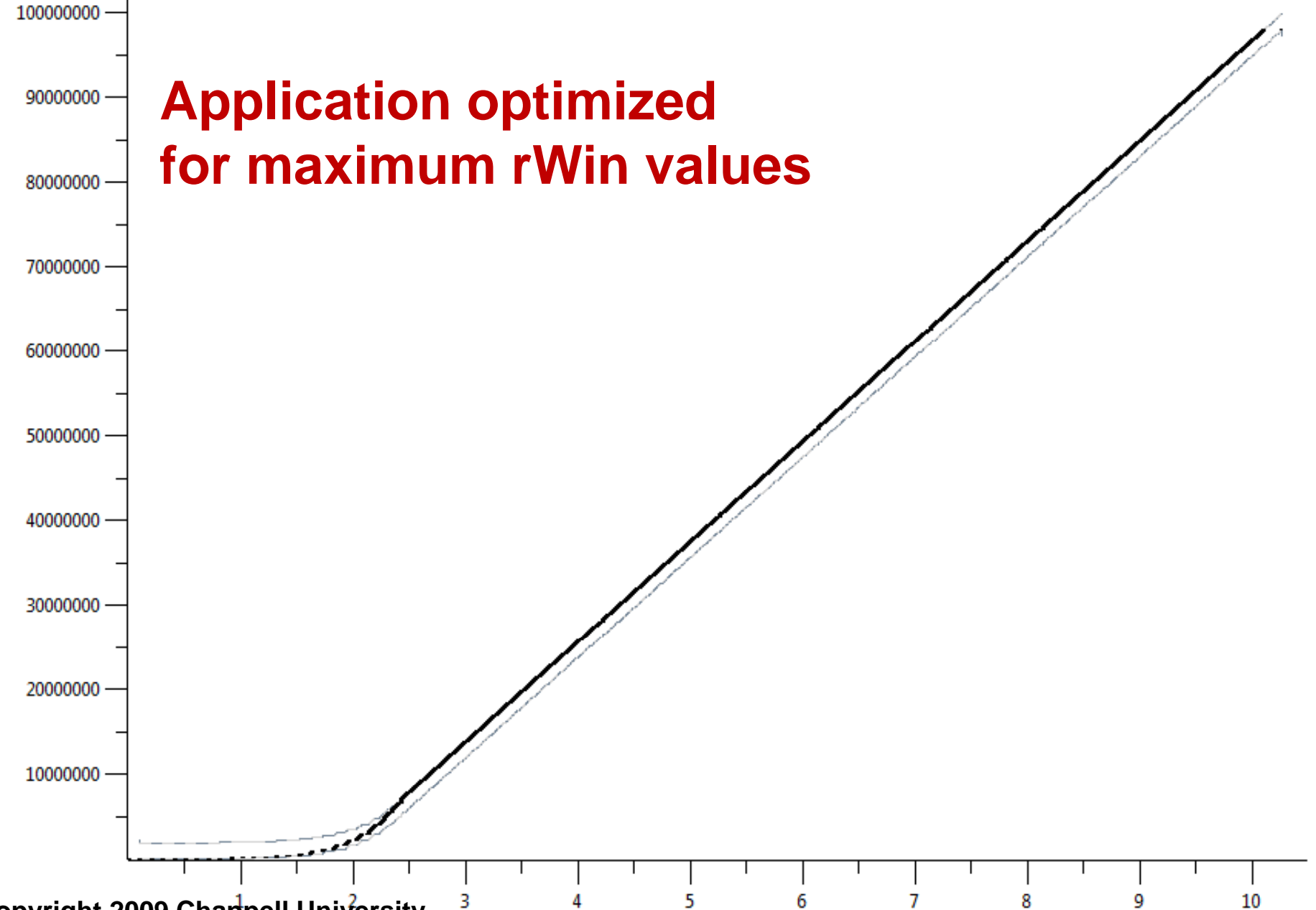
# Lab Test Results: Throughput/Scaling Relationship

Lab Test	Delay	A: 1323 On B: rWin- 1,875,000	iperf -s rWin at 1,875,000	iperf -c rWin at 1,875,000	Results
#6: iPerf to 10.10.16.16 w/delay + rWin at receiver set	100 ms	“	Receive window (-w) set at 1,875,000		5.0
#7: iPerf to 10:10:16:16 w/delay + rWin at receiver set	100 ms	“	“	Sender window (-w) set at 1,875,000	77.6

Sequence  
number[B]

Time/Sequence Graph

**Application optimized  
for maximum rWin values**



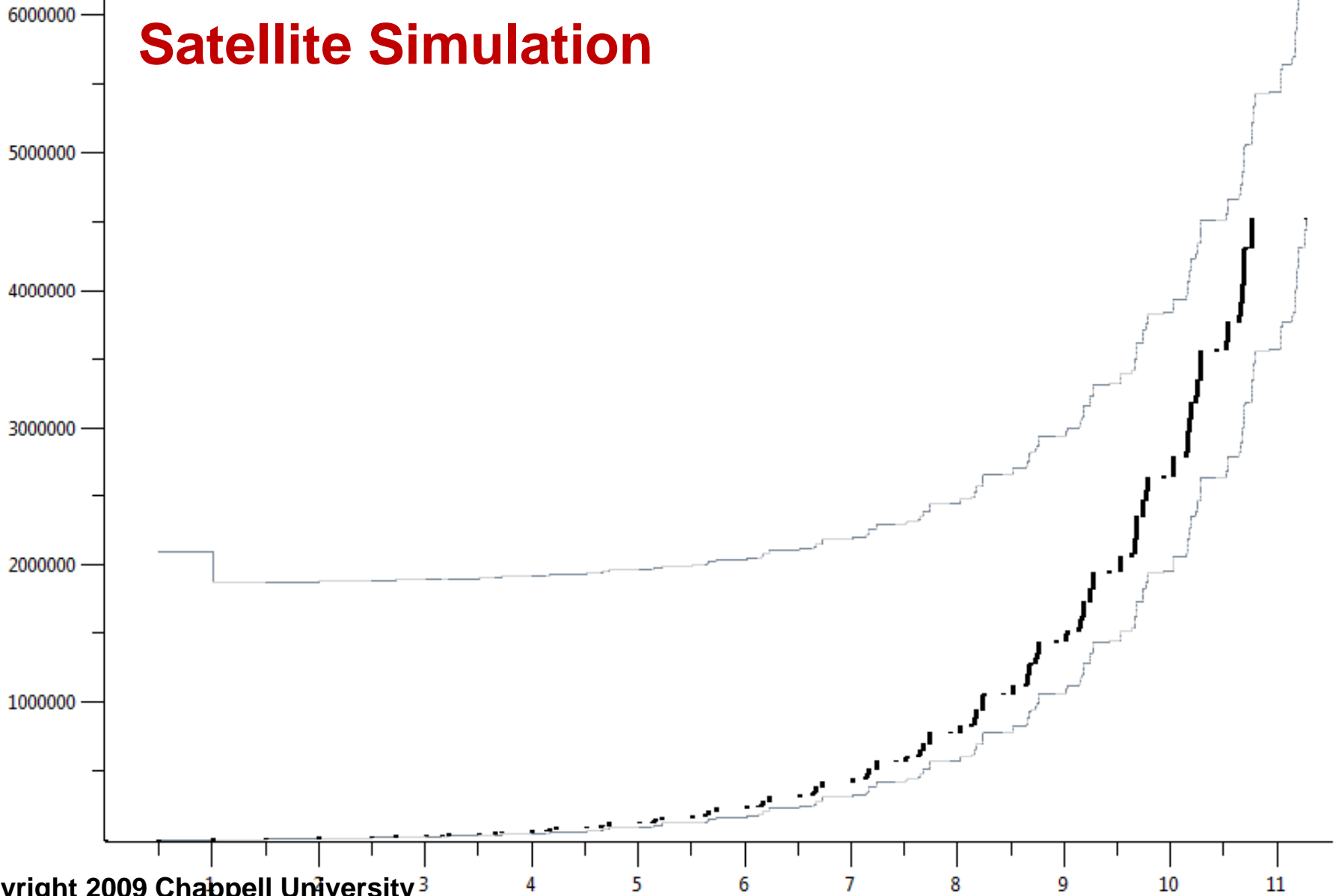
# Lab Test Results: Throughput/Scaling Relationship

Lab Test	Delay	A: 1323 On B: rWin- 1,875,000	iperf -s rWin at 1,875,000	iperf -c rWin at 1,875,000	Results
#6: iPerf to 10.10.16.16 w/delay + rWin at receiver set	100 ms	“	Receive window (-w) set at 1,875,000		5.0
#7: iPerf to 10:10:16:16 w/delay + rWin at receiver set	100 ms	“	“	Sender window (-w) set at 1,875,000	77.6
#8: iPerf to 10:10:16:16 w/delay – satellite link speed simulation	800 ms	“	“	“	1.2

Sequence  
number[B]

Time/Sequence Graph

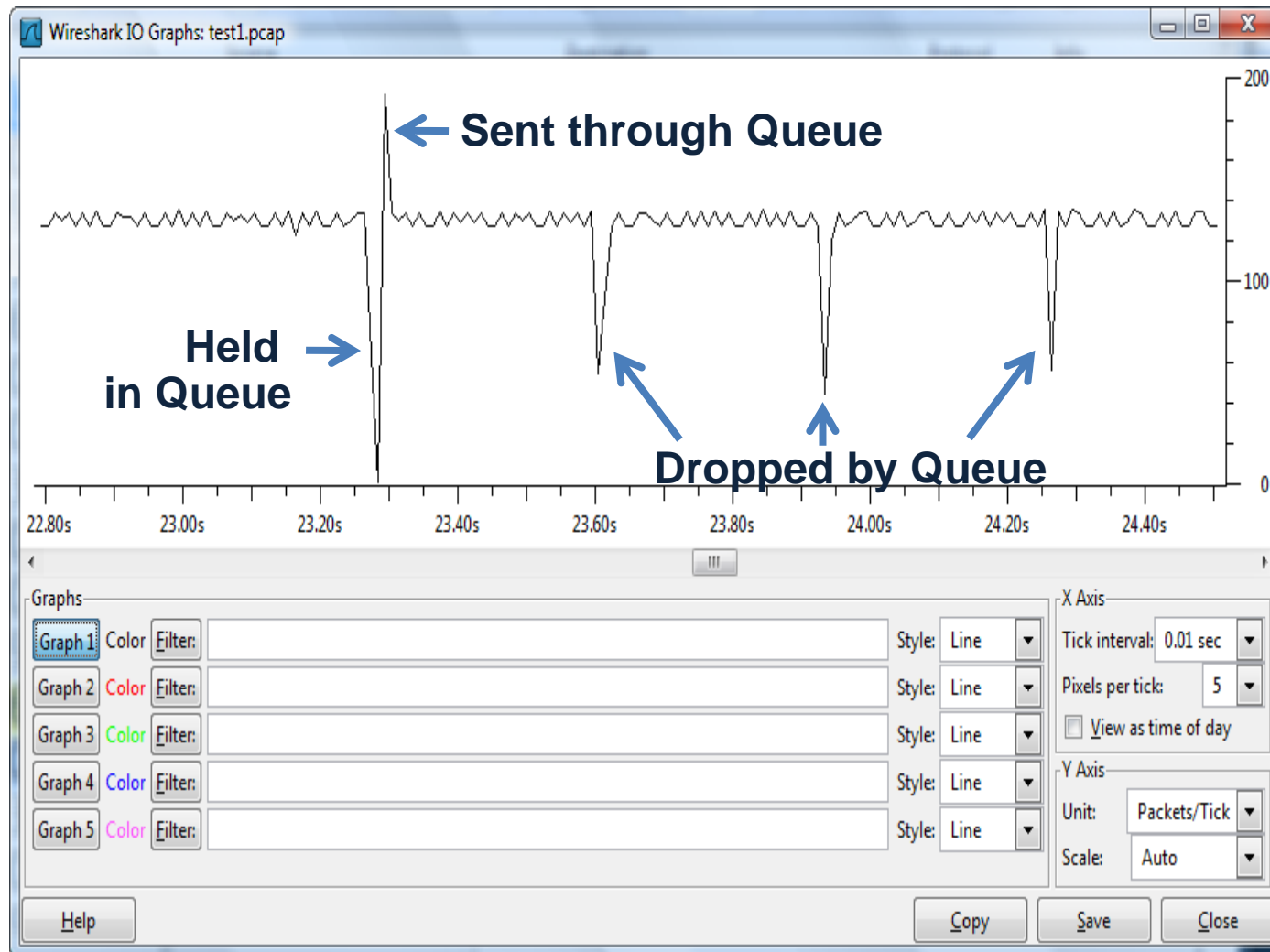
# Satellite Simulation



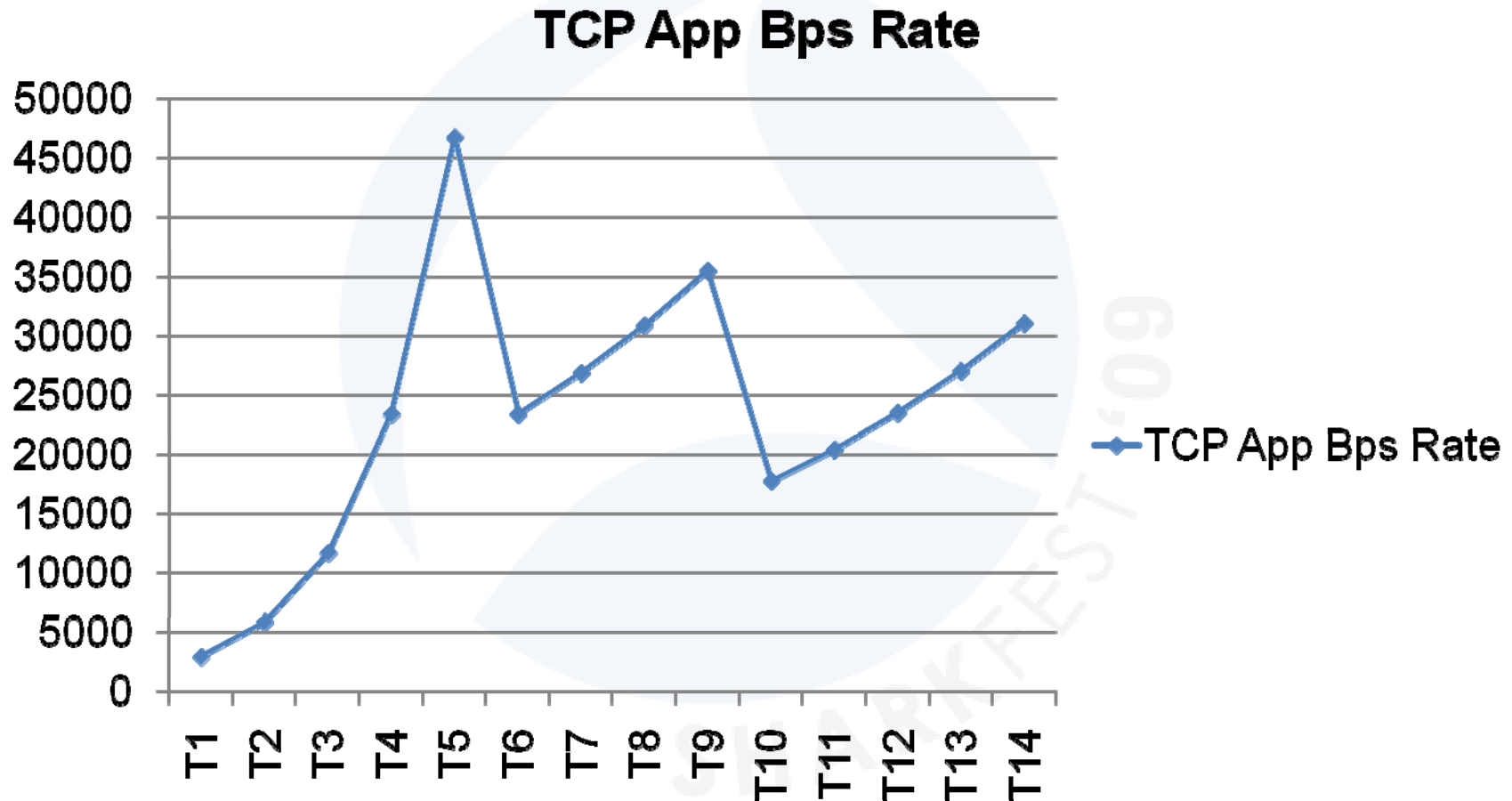
# The Case of the Sputtering Stream



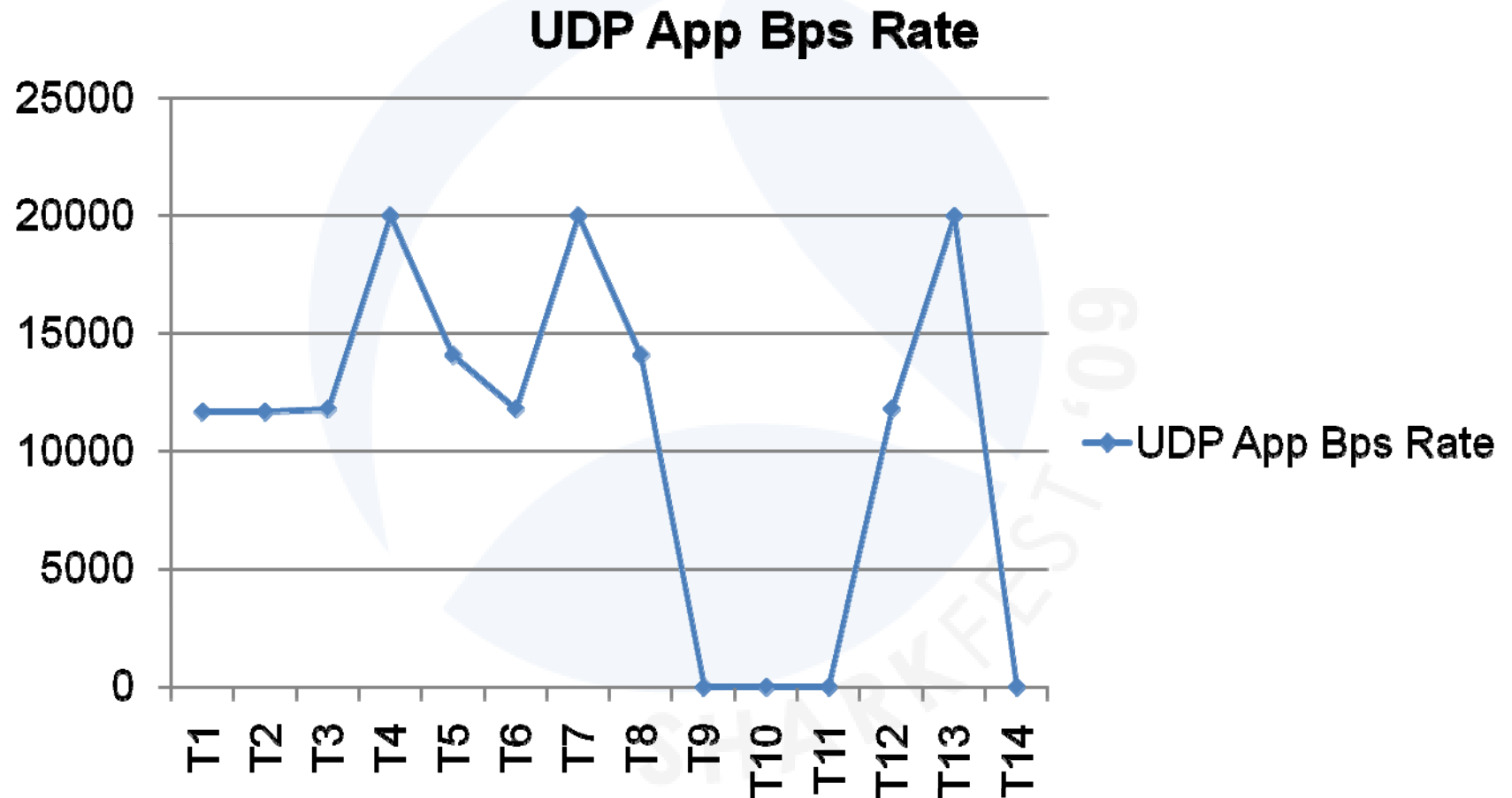
# Path Issues - Who's "Special?"



# TCP Packet Loss



# UDP: In the Hands of the Developers



# HOT in the Enterprise



**Bad cops  
are  
everywhere!**

# Now...

- Enough of this slide stuff...

SHARKFEST '09

# Links

- Wireshark Weekly Tips  
<http://www.wiresharktraining.com/tips.html>
- Bandwidth\*Delay Product Calculator  
<http://www.speedguide.net/bdp.php>
- Yes – I tweet – “laurachappell”
- Yes – I blog - [feeds2.feedburner.com/InsideLaurasLab](http://feeds2.feedburner.com/InsideLaurasLab)
- Yes – I Facebook – “laurachappell”

# Thank You!

- Please sign up for the Wireshark Jumpstart courses at [chappellseminars.com](http://chappellseminars.com)!