

SharkFest'17 US

Workflow-based Analysis of Wireshark Traces

Now we can all be experts

Paul Offord

Project Leader, TribeLab

SharkFest'17 US • Carnegie Mellon University • June 19-22, 2017

Agenda

- Recurring Gray Problems
- Principles and objectives of our approach
- Performance problem scenarios
- Performance analysis concepts
- Analysis strategy
- Worked example – get into some packets
- Q&A



The Issue

Recurring

It keeps happening

Gray

The causing technology
is unknown

Problem

Performance
Error
Incorrect output

*“It must be
the network”*



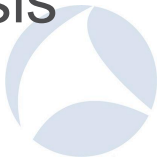
The Challenge

Ongoing Problem

- Static cause
- Recreate
- Short capture
- Easy analysis

Recurring Gray Problem

- Transient cause
- Can't recreate
- Long-term capture
- Challenging analysis



Analysis Principles

We look at **one symptom** at a time

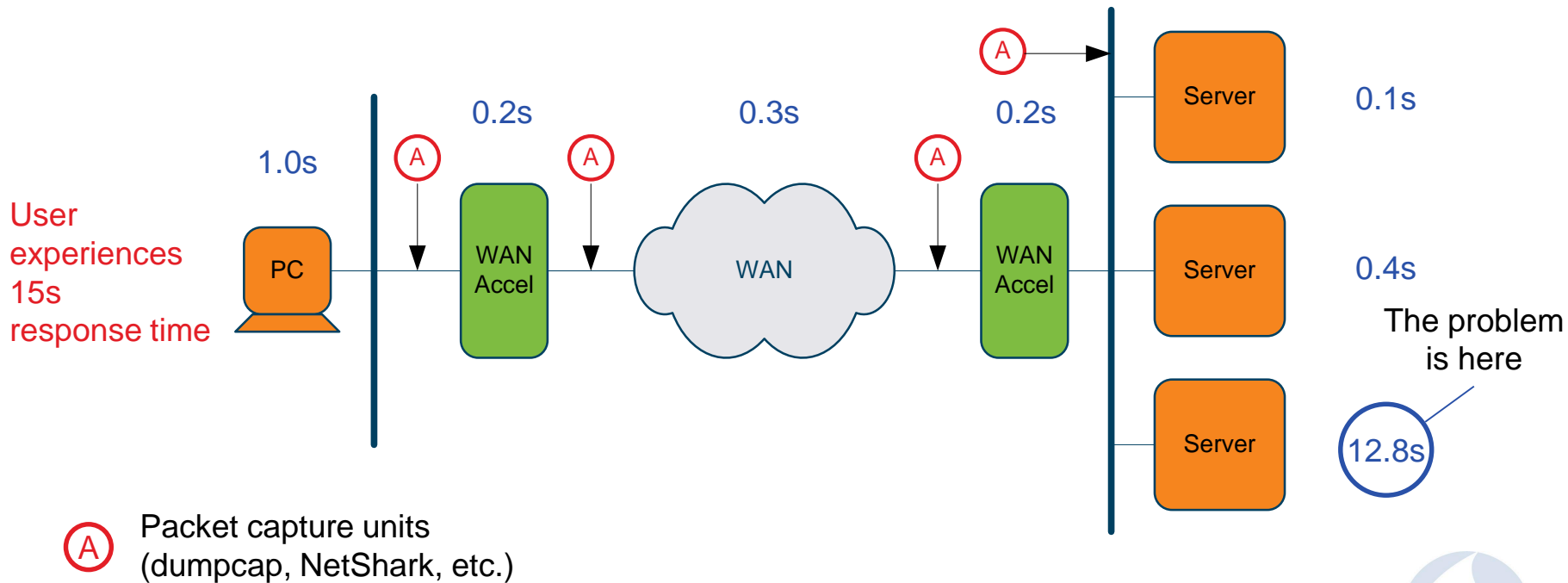
We study a **specific instance** of that symptom

We capture **live** problems

Produce **irrefutable evidence** of the cause



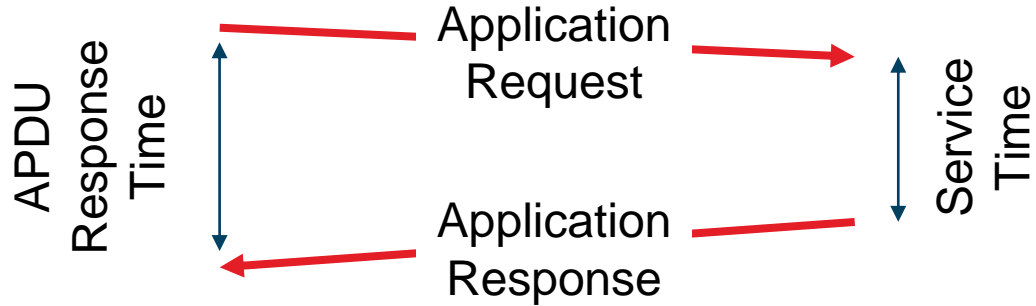
Analysis Objective



Process-to-Process Communication



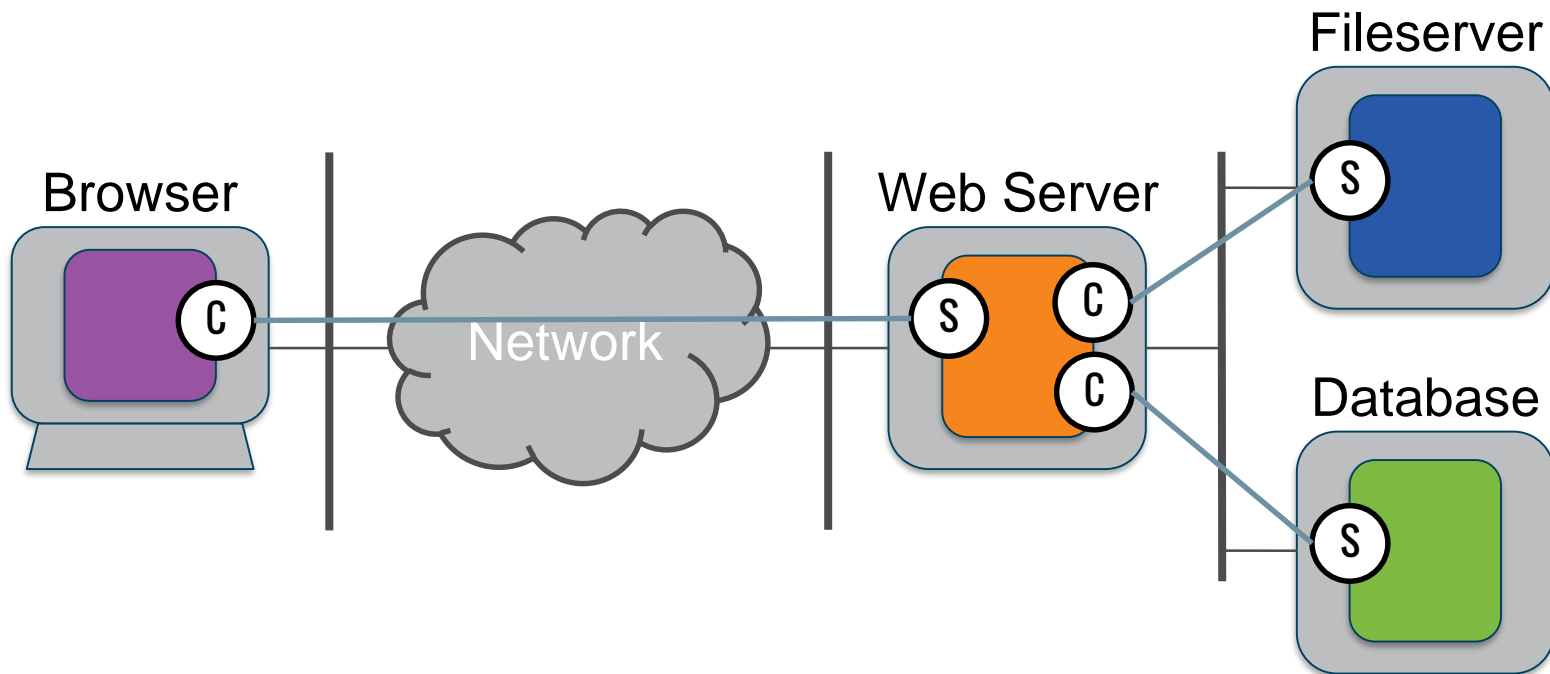
NB: Application messages (APDUs) not packets



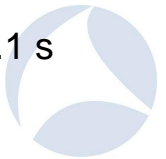
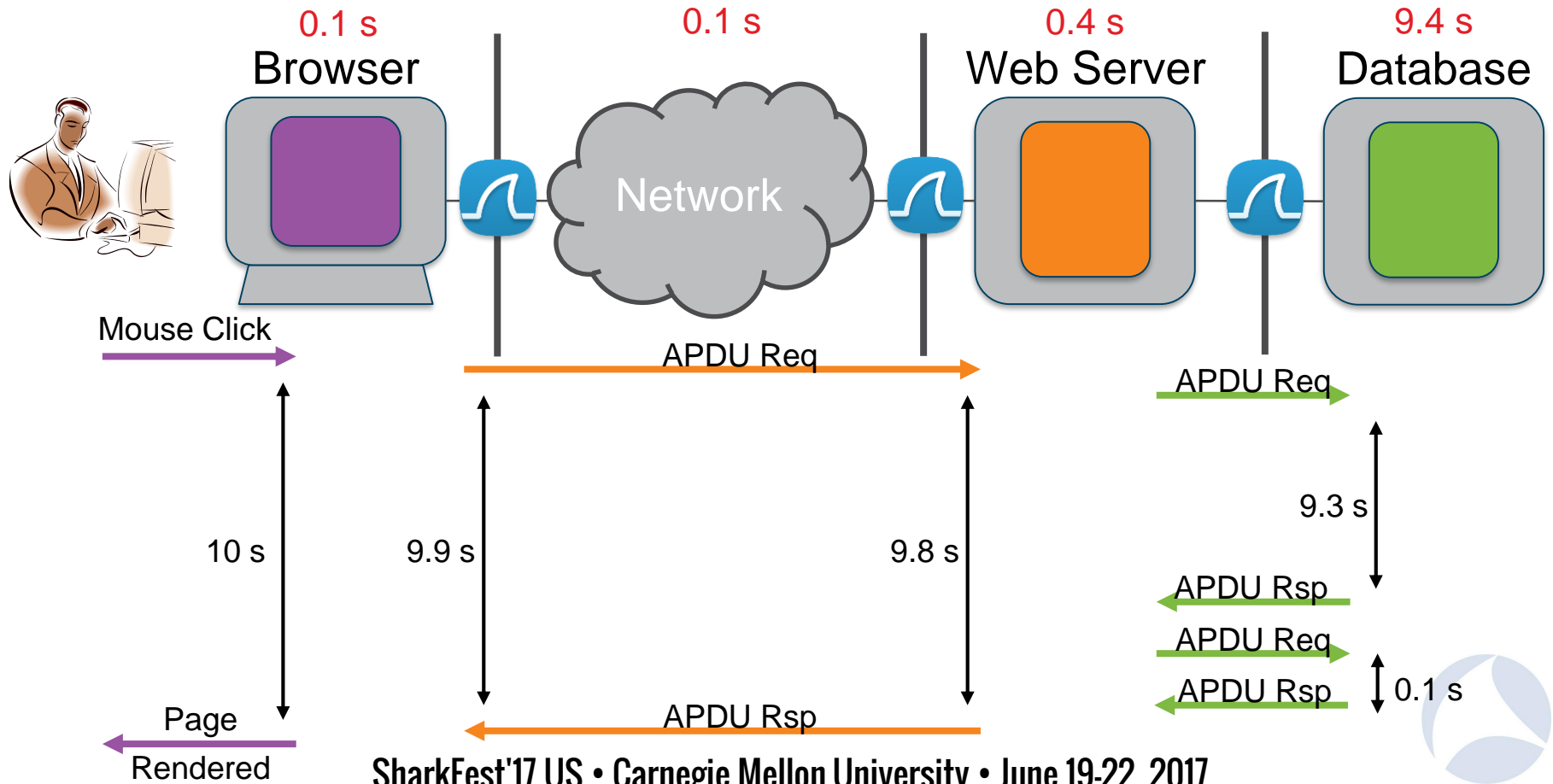
Increasing Time of Day



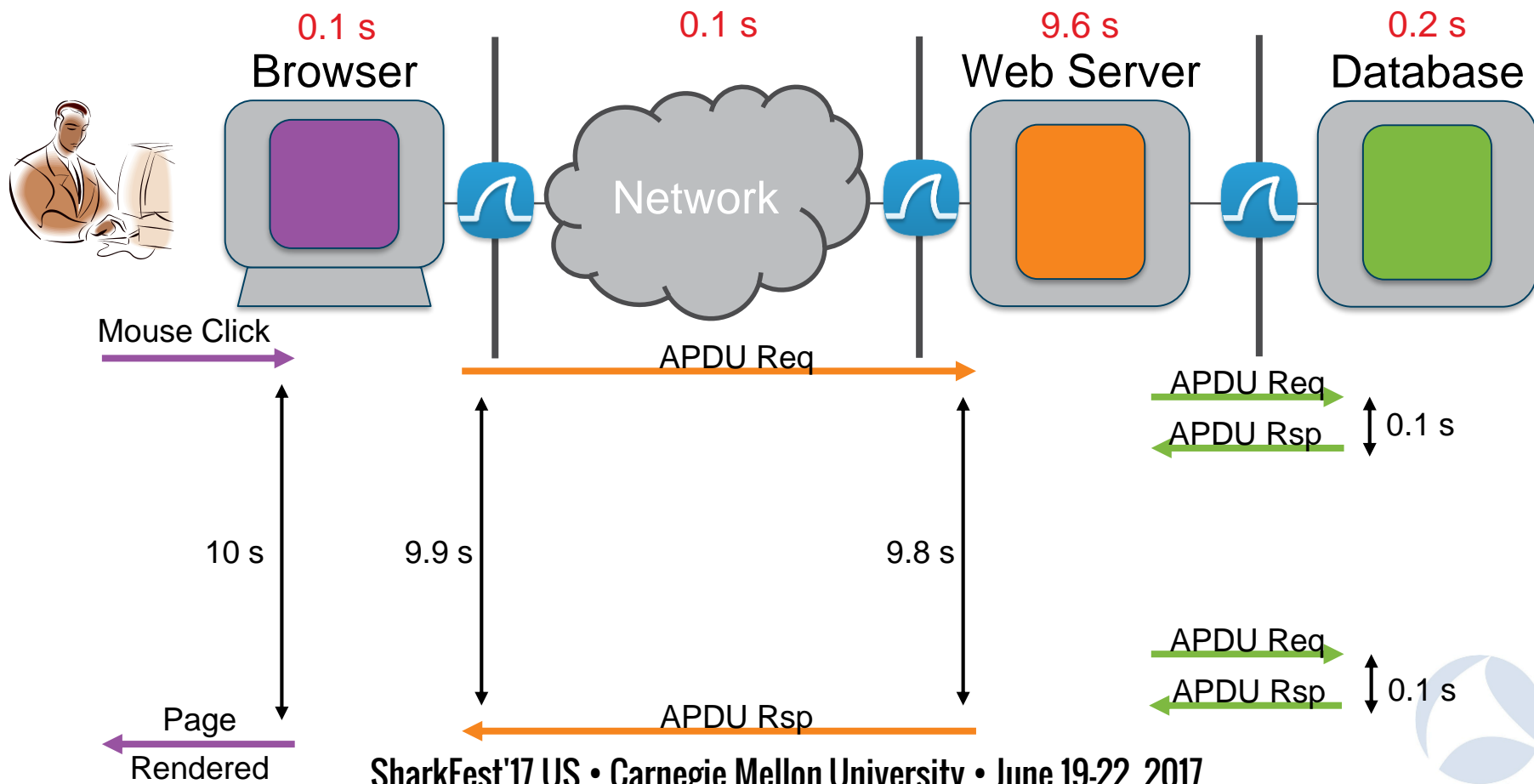
Client-Service Chains



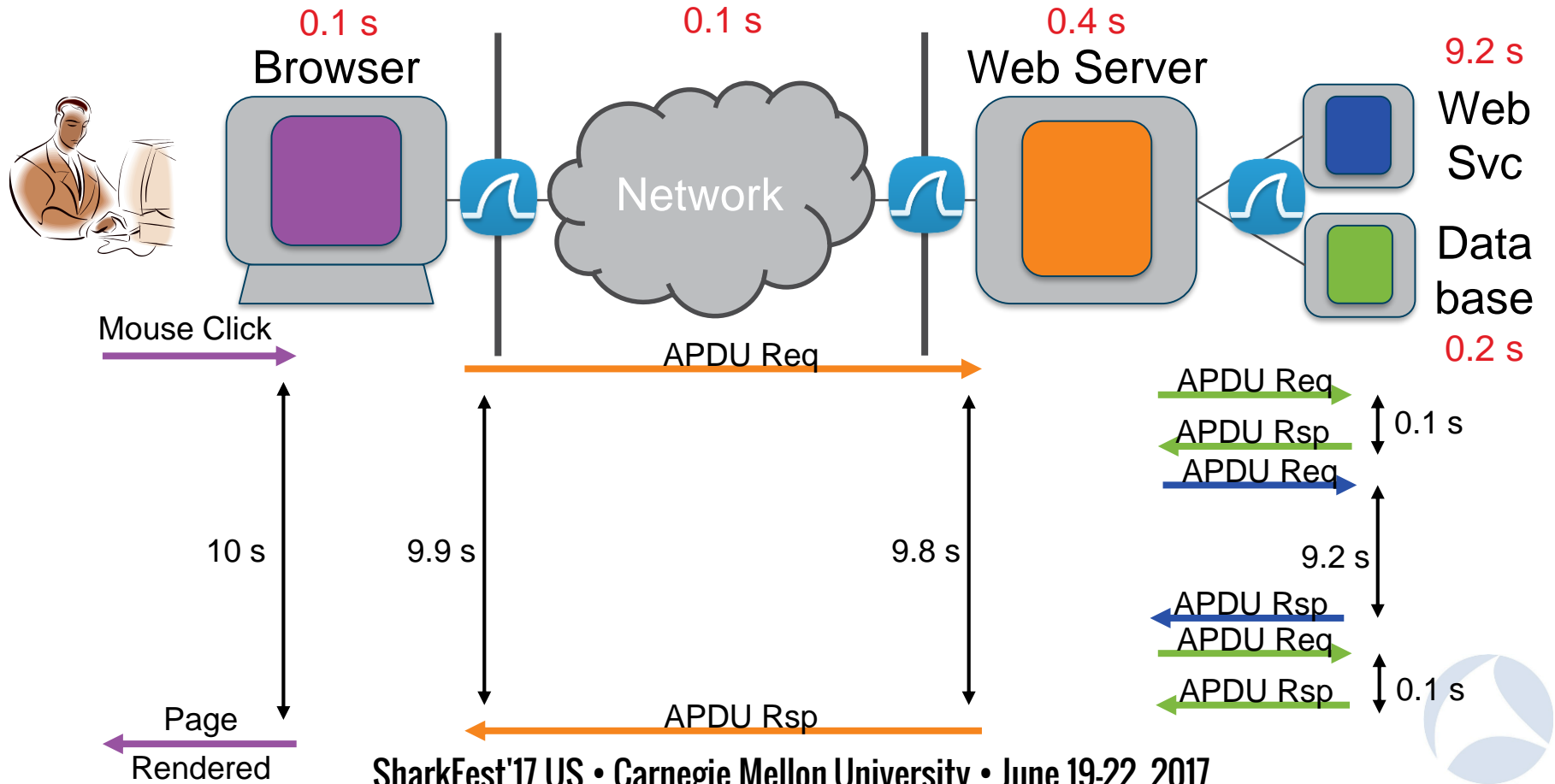
Slow Response - Scenario 1



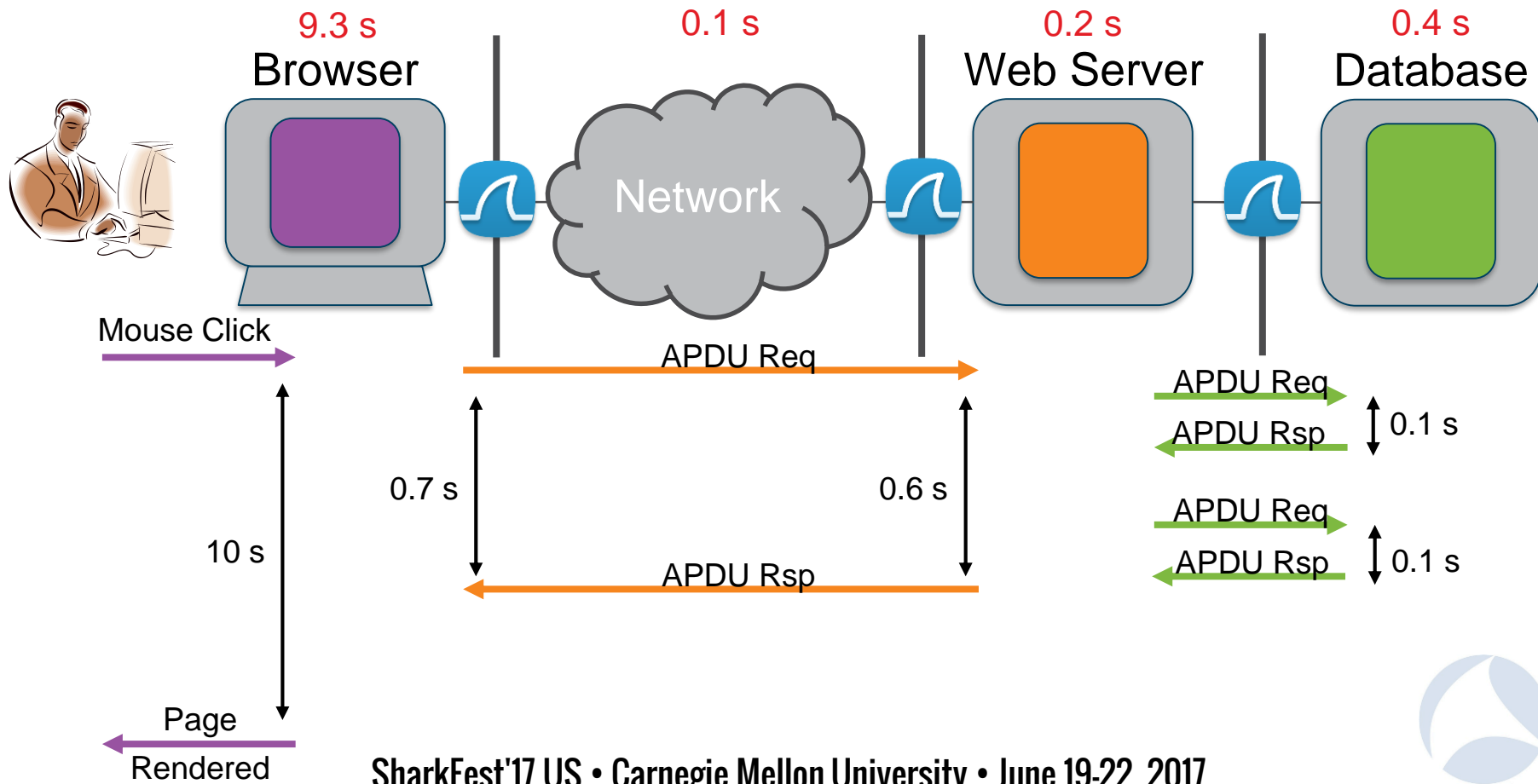
Slow Response - Scenario 2



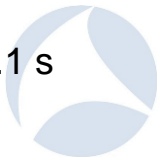
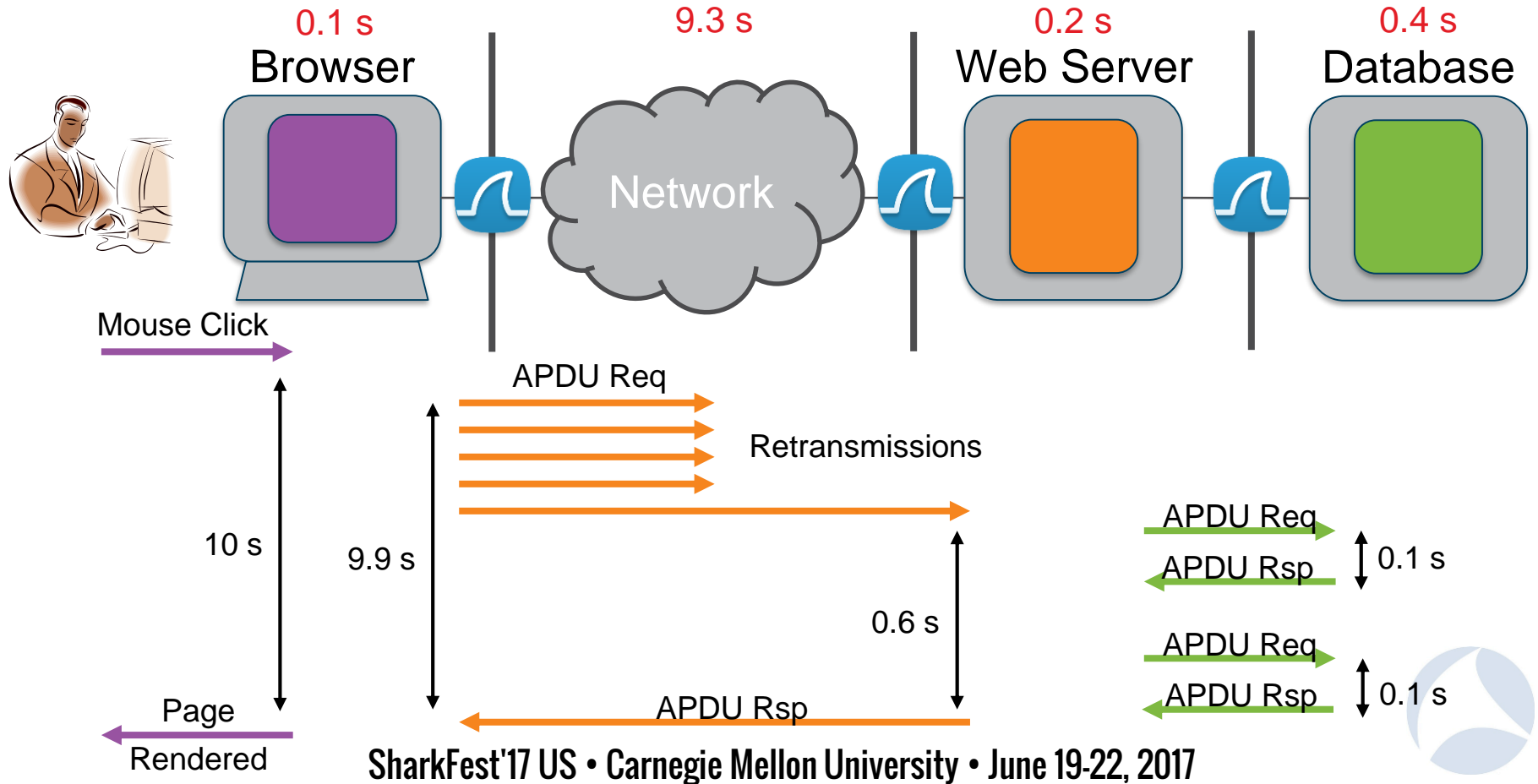
Slow Response - Scenario 2b



Slow Response - Scenario 3



Slow Response - Scenario 4



Multi-tier Correlation



SHARKFEST '13

Wireshark Developer and User Conference

Multi-tier Trace Correlation

Paul Offord

CTO, Advance7



[Home](#)

[Resources](#)

[Software](#)

[Downloads](#)

[About Us](#)

[Home](#) ▶ [Techniques](#) ▶ [NTAG](#)

Network Trace Analysis Guide

You've got a basic understanding of networking and you can drive Wireshark to a reasonable level (capture, display and filter). You can mimic the tips and tricks that you've seen demonstrated on YouTube and you are keen to get the most out of Wireshark. You're boss has asked you to take a look at a response time problem with an important business system. You've successfully captured trace data from multiple points in the end-to-end system but you are struggling to analyze it. Where do you start? Which tips and tricks are applicable? If this sounds familiar you've come to the right place.

The [Network Trace Analysis Guide](#) describes a systematic way to analyze traces captured from a multi-tier system, and the other resources on this page provide further help and guidance.



[News forum](#)

Resources

The [Network Trace Analysis Guide](#) electronic book in this course details a systematic way to carry out network trace analysis. The guide refers to a number of techniques that are described in the book [RPR: A Problem Diagnosis Method for IT Professionals](#), a copy of which we include here for completeness.



[Discussion Forum](#)

Post questions, feedback and general comments relating to the the [Network Trace Analysis Guide](#) on this forum.



[Network Trace Analysis Guide](#)

This guide is for anyone looking for a systematic way to analyze network trace data. We focus on the analysis of traces gathered in enterprise IT environments, but the principles and techniques should be applicable across a broad range of scenarios.



[RPR: A Problem Diagnosis Method for IT Professionals](#)

This is a PDF version of the RPR manual. The guide references some techniques described in this manual.

APDU vs. Packets

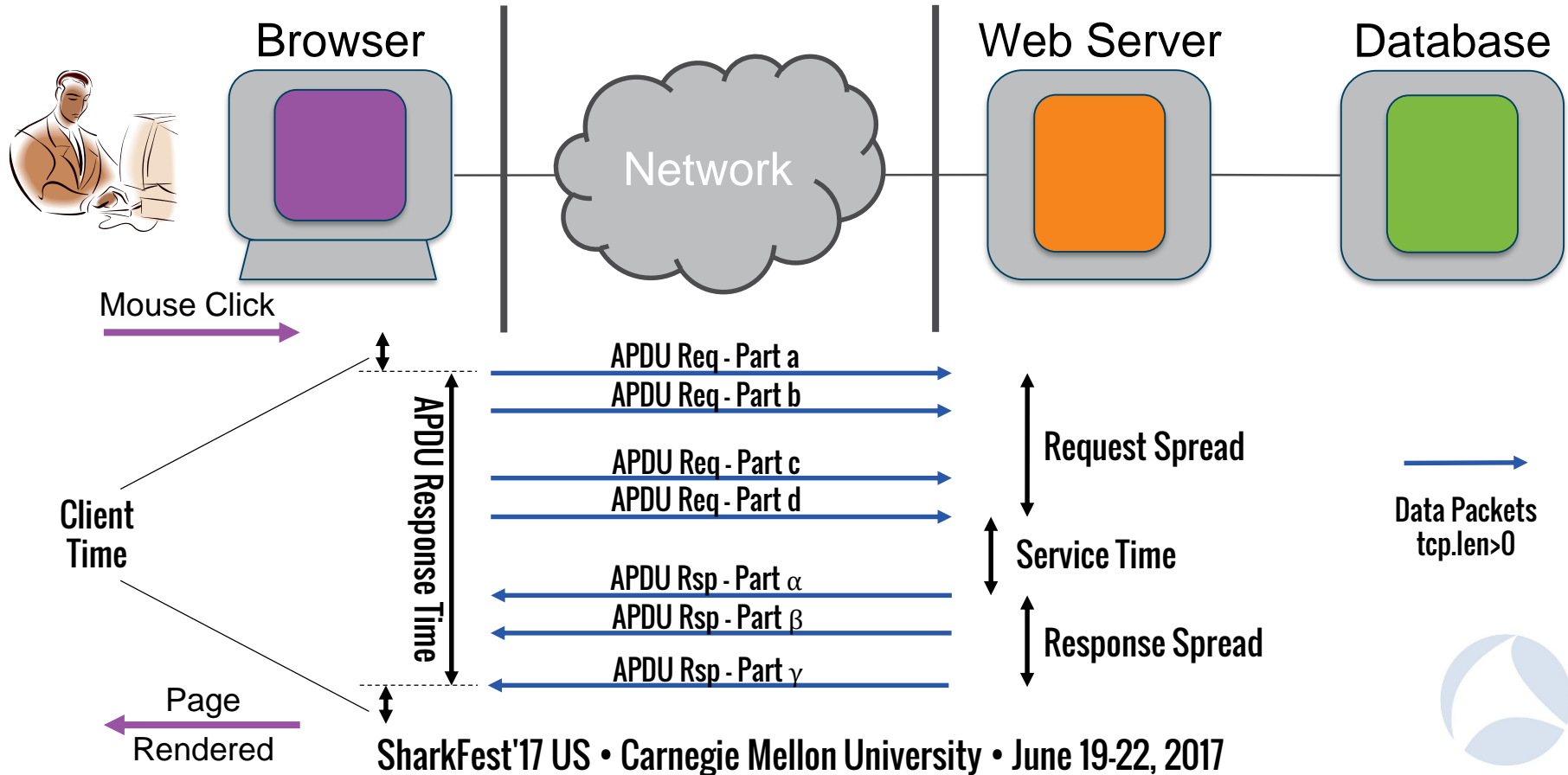
tcp.port==80 && tcp.len>0

Request APDU

No.	Time	Source	Destina	Dst Port	Src Port	Protocol	Info
55	15:39:10.69...	192...	192...	80	64133	HTTP	GET /MyApp/Student?page=86 HTTP/1.1
56	15:39:10.70...	192...	192...	64133	80	TCP	80 → 64133 [ACK] Seq=13885 Ack=4608 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
58	15:39:10.70...	192...	192...	64133	80	TCP	80 → 64133 [ACK] Seq=15345 Ack=4608 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
59	15:39:10.70...	192...	192...	64133	80	HTTP	HTTP/1.1 200 OK (text/html)
61	15:39:10.93...	192...	192...	80	64133	HTTP	GET /favicon.ico HTTP/1.1
62	15:39:10.93...	192...	192...	64133	80	HTTP	HTTP/1.1 302 Redirect (text/html)
64	15:39:14.03...	192...	192...	80	64133	HTTP	GET /MyApp/Student/Edit/979 HTTP/1.1
66	15:39:14.51...	192...	192...	64133	80	TCP	80 → 64133 [ACK] Seq=17415 Ack=5618 Win=64512 Len=1460 [TCP segment of a reassembled PDU]
68	15:39:14.51...	192...	192...	64133	80	TCP	80 → 64133 [ACK] Seq=18875 Ack=5618 Win=64512 Len=1460 [TCP segment of a reassembled PDU]
69	15:39:14.51...	192...	192...	64133	80	HTTP	HTTP/1.1 200 OK (text/html)
71	15:39:14.53...	192...	192...	80	64133	HTTP	GET /MyApp/bundles/jqueryval HTTP/1.1
72	15:39:14.54...	192...	192...	64133	80	TCP	80 → 64133 [ACK] Seq=20529 Ack=6296 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
74	15:39:14.54...	192...	192...	64133	80	HTTP	HTTP/1.1 404 Not Found (text/html)
81	15:39:14.70...	192...	192...	80	64134	HTTP	GET /favicon.ico HTTP/1.1
82	15:39:14.70...	192...	192...	64134	80	HTTP	HTTP/1.1 302 Redirect (text/html)
95	15:39:30.06...	192...	192...	80	64134	TCP	64134 → 80 [PSH, ACK] Seq=518 Ack=369 Win=65280 Len=885 [TCP segment of a reassembled PD...]
96	15:39:30.06...	192...	192...	80	64134	HTTP	POST /MyApp/Student/Edit/979 HTTP/1.1 (application/x-www-form-urlencoded)
98	15:39:30.07...	192...	192...	64134	80	HTTP	HTTP/1.1 302 Found (text/html)

Response APDU

Response Time Element (RTE) Model



TRANSUM and RTE

- TRANSUM is a Wireshark plugin
- Standard in Wireshark 2.4 (mid-late July)
- TribeLab Plugin for Wireshark 2.2



RTE Data

TRANSUM
adds a new
decode section

```
> Frame 51: 561 bytes on wire (4488 bits), 5
> Ethernet II, Src: Vmware_90:e0:d3 (00:0c:2
> Internet Protocol Version 4, Src: 192.168.
> Transmission Control Protocol, Src Port: 6
> Hypertext Transfer Protocol
∨ TRANSUM RTE Data
  [RTE Status: OK]
  [Req First Seg: 51]
  [Req Last Seg: 51]
  [Rsp First Seg: 53]
  [Rsp Last Seg: 55]
  [APDU Rsp Time: 1.011444000 seconds]
  [Service Time: 1.011305000 seconds]
  [Req Spread: 0.000000000 seconds]
  [Rsp Spread: 0.000139000 seconds]
  [Trace clip filter: tcp.stream==3 && fra
  [Calculation: Generic TCP]
```

RTE Summary

- **APDU Response Time**

- Client perspective
- Big number = There's a problem

- **Service Time**

- Service perspective
- Big number = There's a problem with the service

- **Spread Time**

- Network perspective
- Big number = There's a problem with the network



Simple Analysis Strategy

- No high APDU Response Times
 - Problem in the client program
- High Service Time
 - Confirm with matching traces
 - Translate data into something meaningful to service owner
 - Hit the service owner with the facts
- High Spread Time
 - Focus in the problem time frame
 - Use techniques *a la* Betty, Chris, Hansang, Jasper, Kary, Laura, etc.



Before we continue ...

Questions?



Introducing

Workbench

SharkFest'17 US • Carnegie Mellon University • June 19-22, 2017

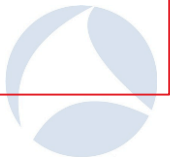


Workbench

- Any data
- Any tool
- Expert guidance

- In dev - Free trial
- FOC Community Edition

- Large volume filtering
- Marker finder
- Transformation
- Packet matching
- Side-by-side analysis



Main Features



Workflows

- Model work practices
- Adds context
- Adapts

- ▶ 14. What is the acceptable response time in...
- ▶ 15. How was Marc accessing Contoso? (INS...
- ▶ 16. What is the IP address of Marc's PC? (IN...
- ▶ 17. Have you added the trace data into the W...
- ▶ 18. We'll refer to traces that were captured o...
- ▶ 19. Did you capture traces on or near the ser...
- ▶ 20. We'll refer to these as the server-side trac...
- ▼ 21. Did Marc, you or anyone else send a mar...

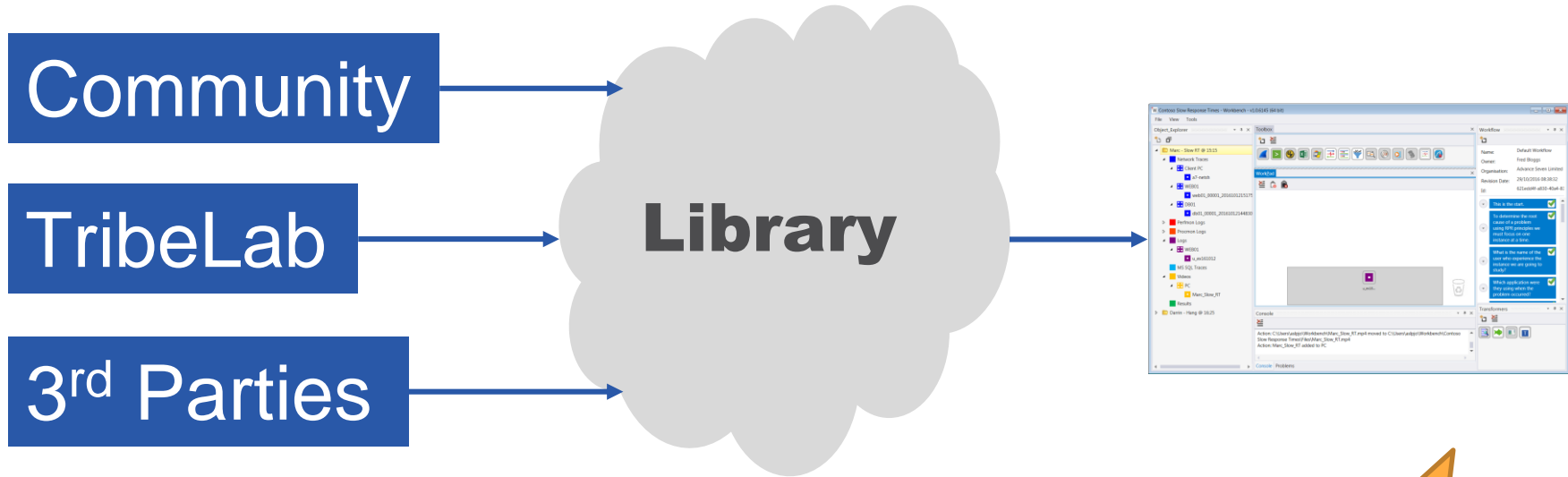
Did Marc, you or anyone else send a marker at the time of the problem?

Yes

No

Incomplete

Sharing Workflows



- Private
- Private and shared with colleagues
- Public



Now for the Main Course

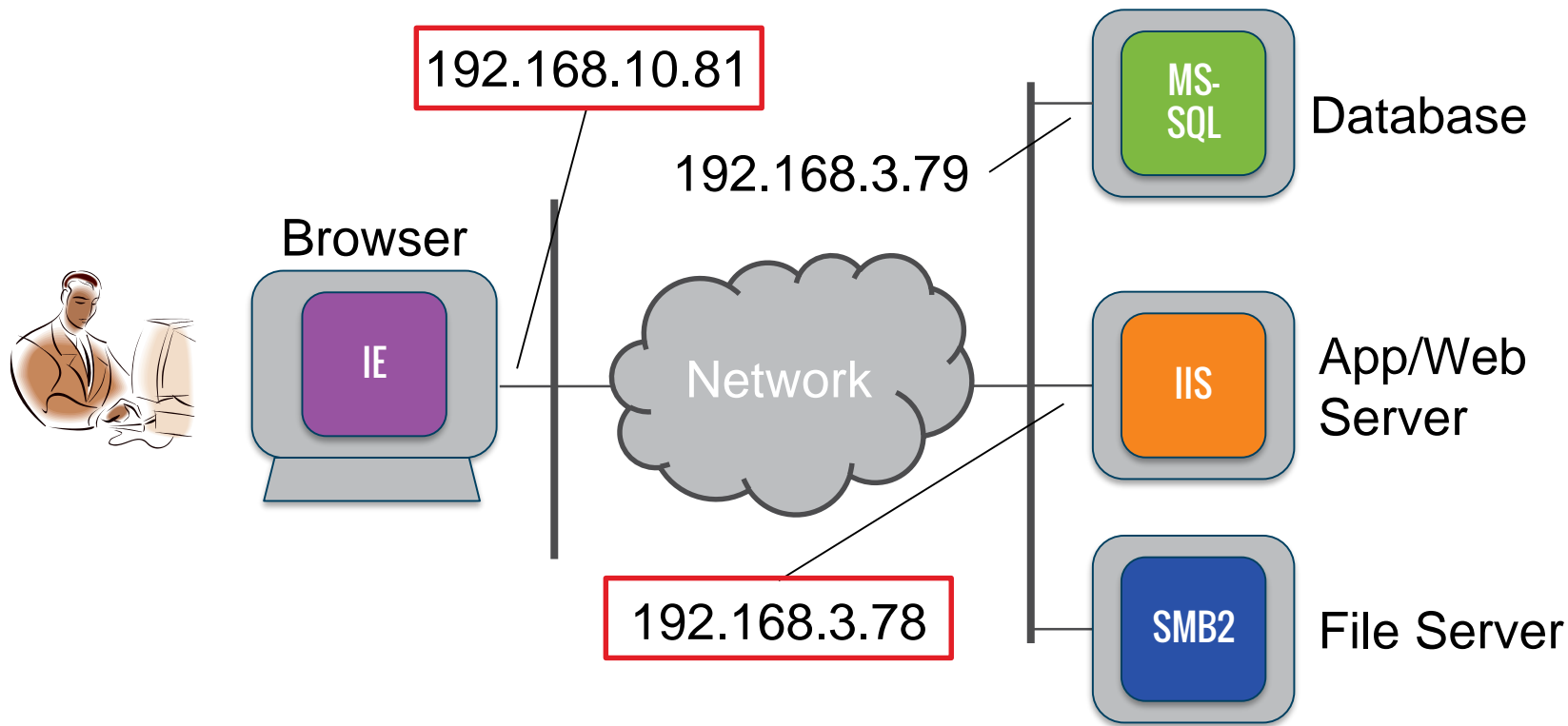
Use Case



The Symptom



Configuration

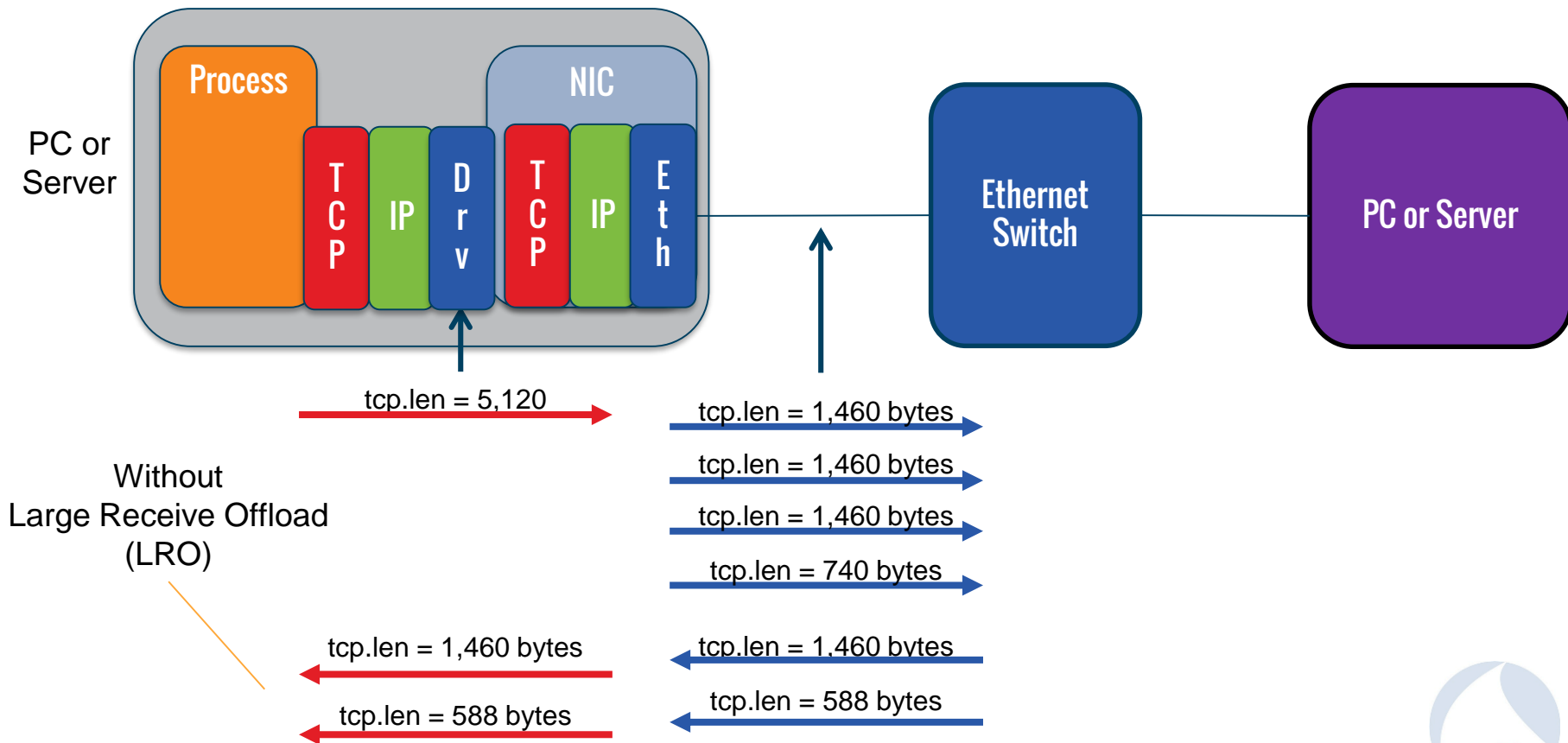


And now ...

Analyze the Data

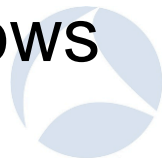


TCP Segmentation Offload (TSO)



Summary

- Recurring gray problems – “It’s the network”
- Analyzing the packet volumes is challenging
- Markers help a lot – see Matthew York, SF16
- Most applications - Request-Response pattern
- TRANSUM allows top-down performance analysis
- Workflow approach - fast, accurate & consistent
- Workbench platform allows sharing of workflows





Contact

- **Paul Offord**
- P +44 (0) 1279 211 668
- E paul@tribelab.com
- W www.tribelab.com
- T @paulofforda7

