# SharkFest'17 US

# Workflow-based Analysis of Wireshark Traces

*Now we can all be experts*

**Paul Offord**

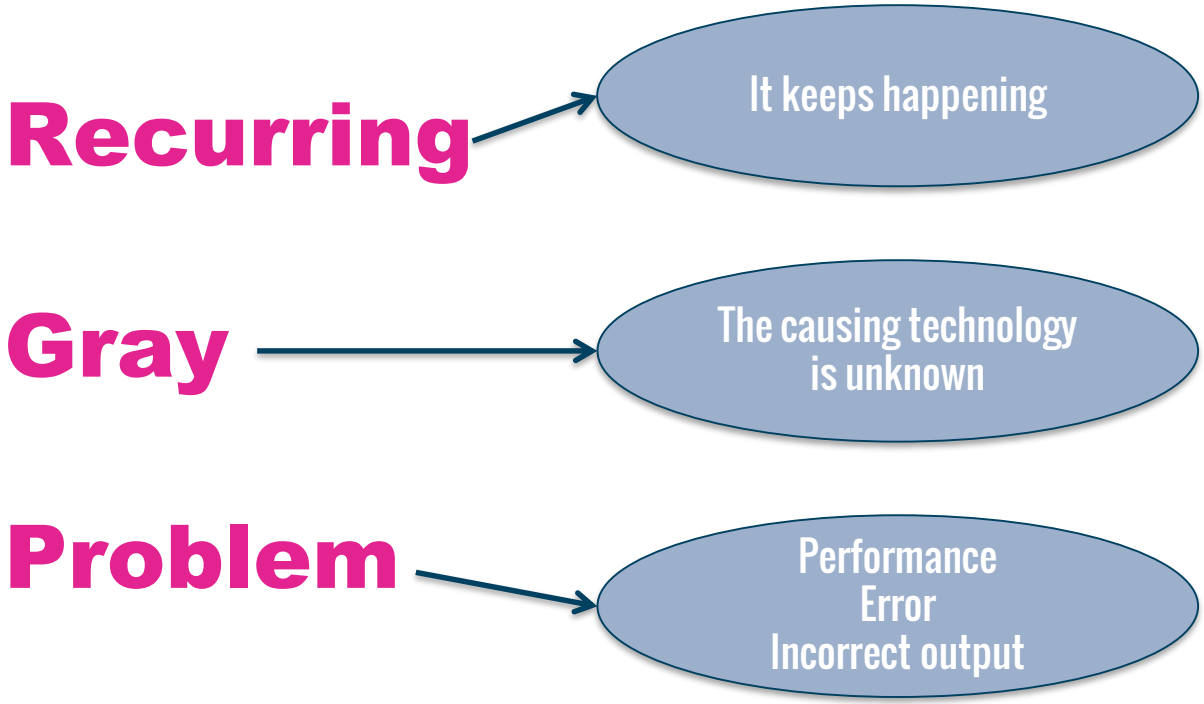
Project Leader, TribeLab

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




*"It must be the network"*

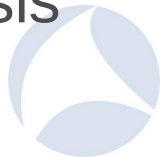
# The Challenge

## Ongoing Problem

- Static cause
- Recreate
- Short capture
- Easy analysis

## Recurring Gray Problem

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



# Analysis Principles

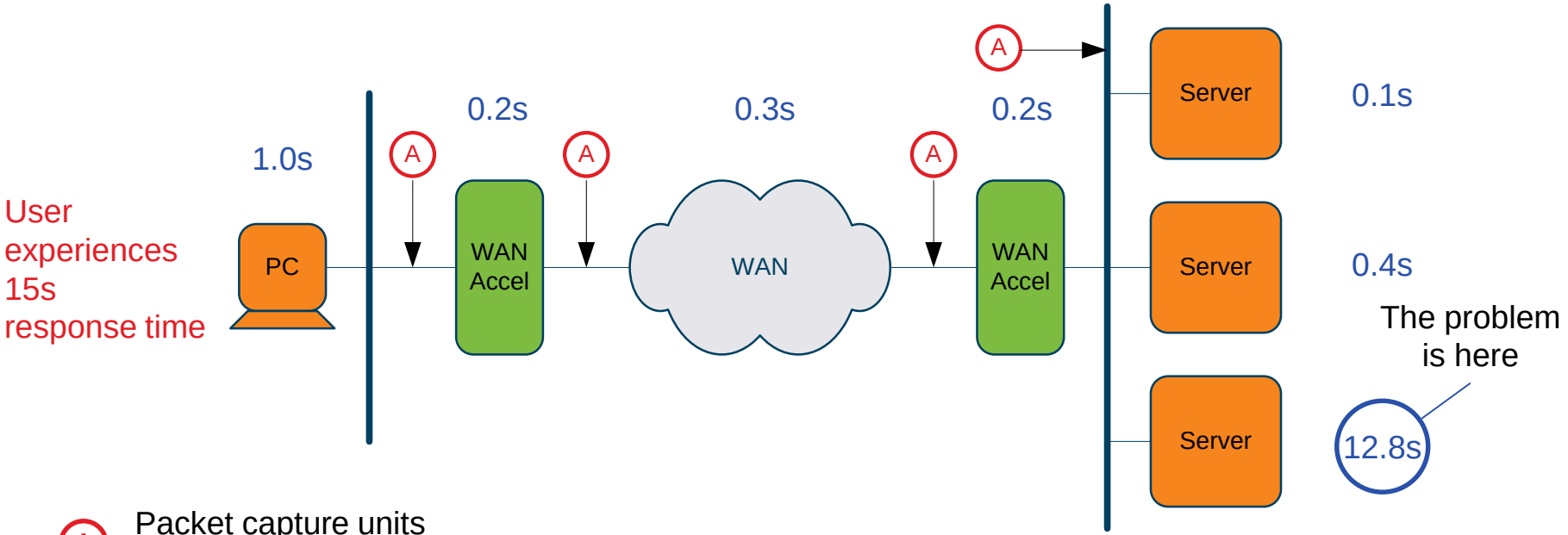
We look at one symptom at a time

We study a specific instance of that symptom

We capture live problems

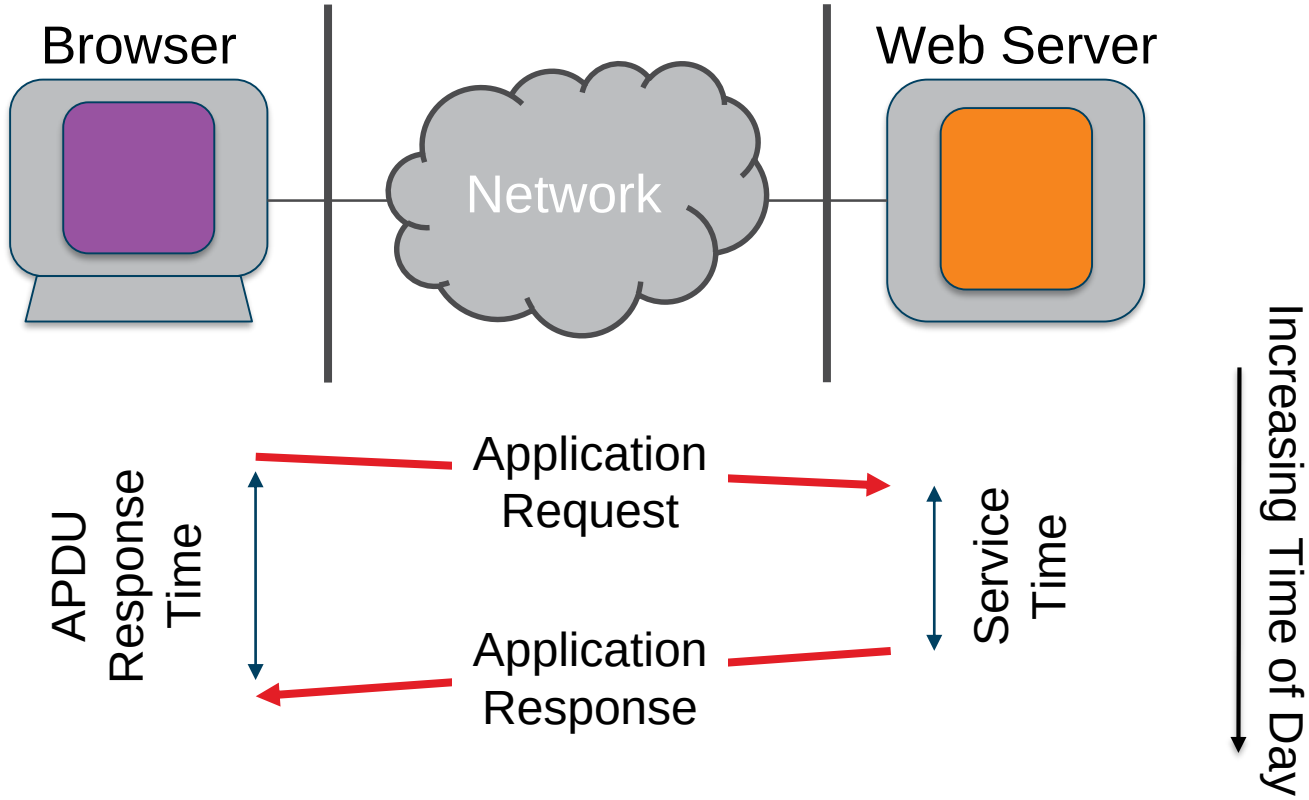
Produce irrefutable evidence of the cause

# Analysis Objective

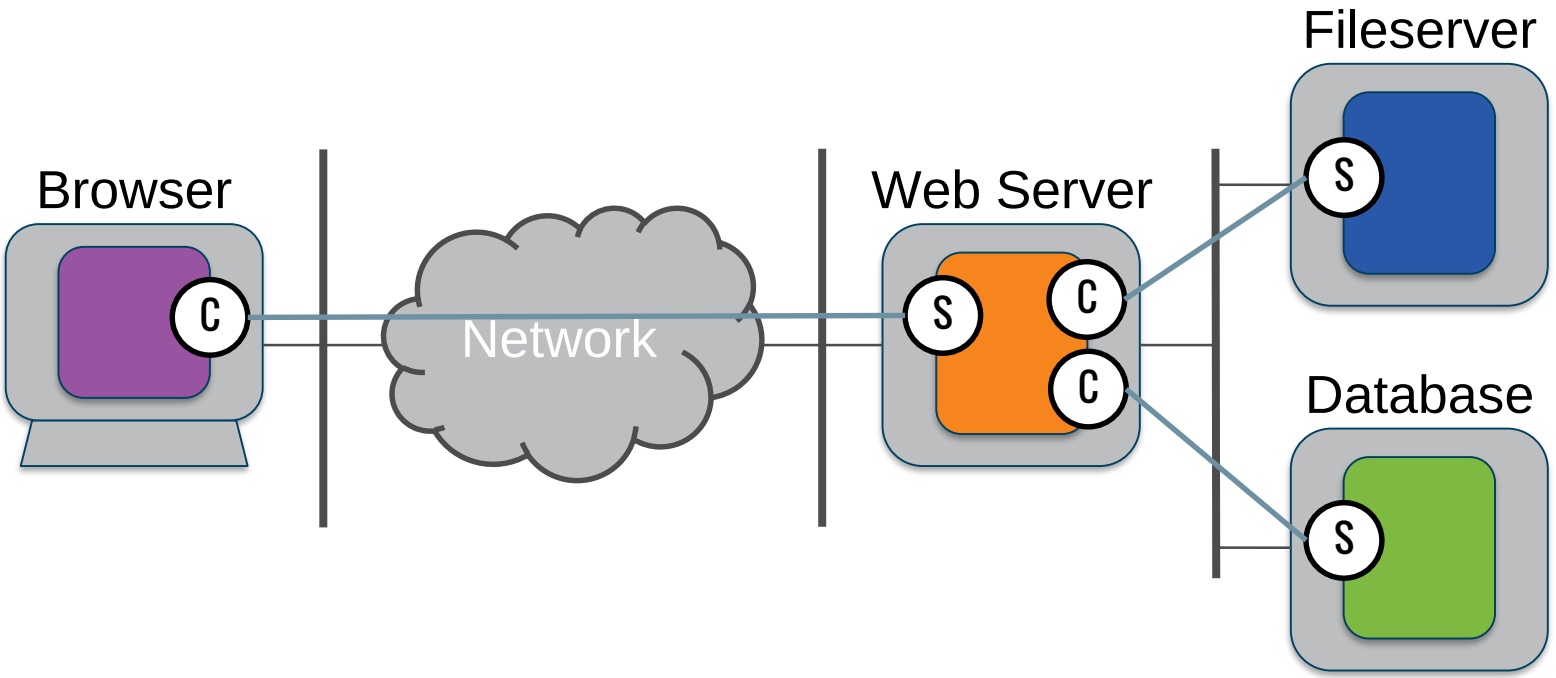


# Process-to-Process Communication

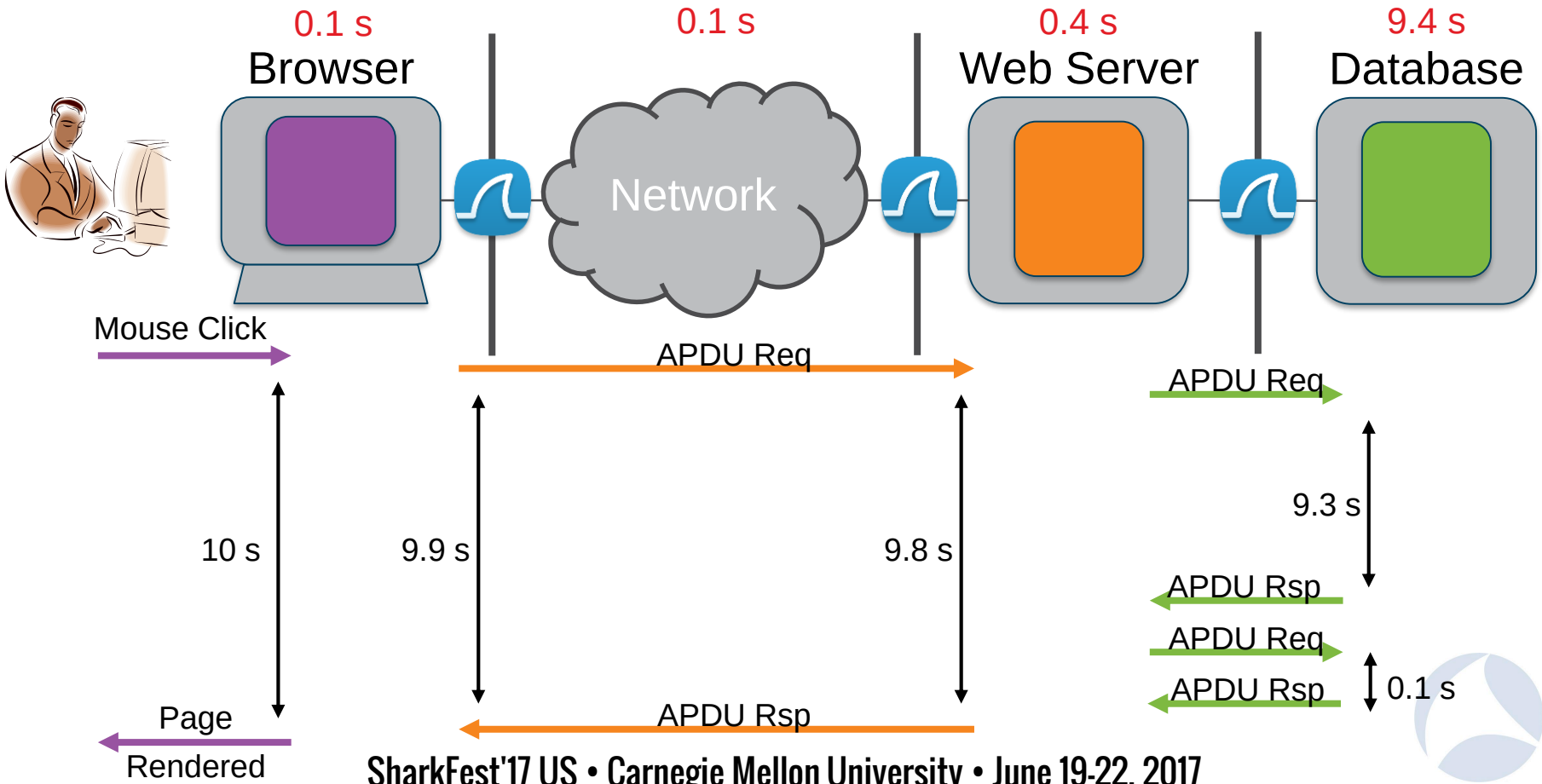
**NB:** Application messages (APDUs) not packets



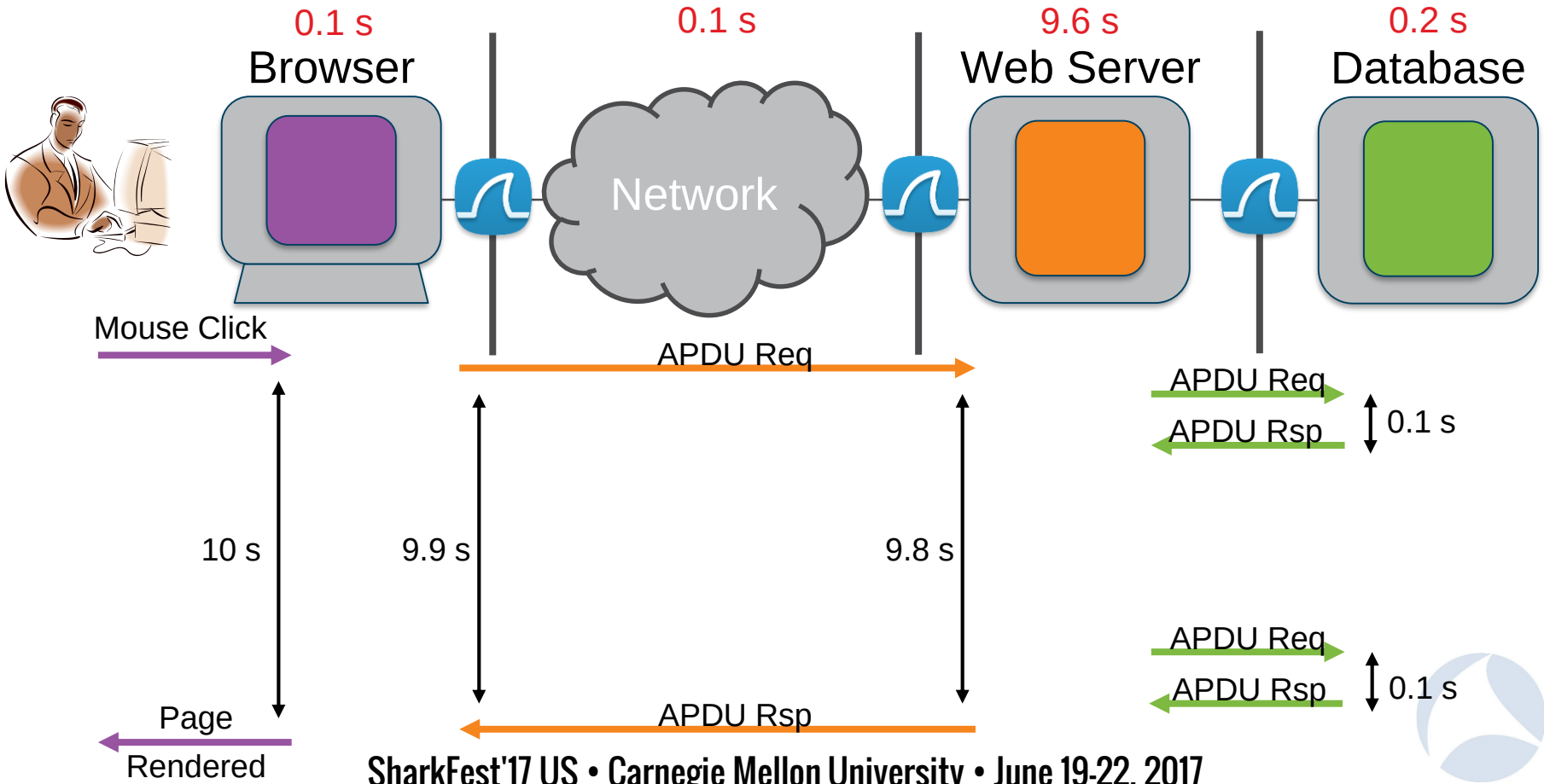
# Client-Service Chains



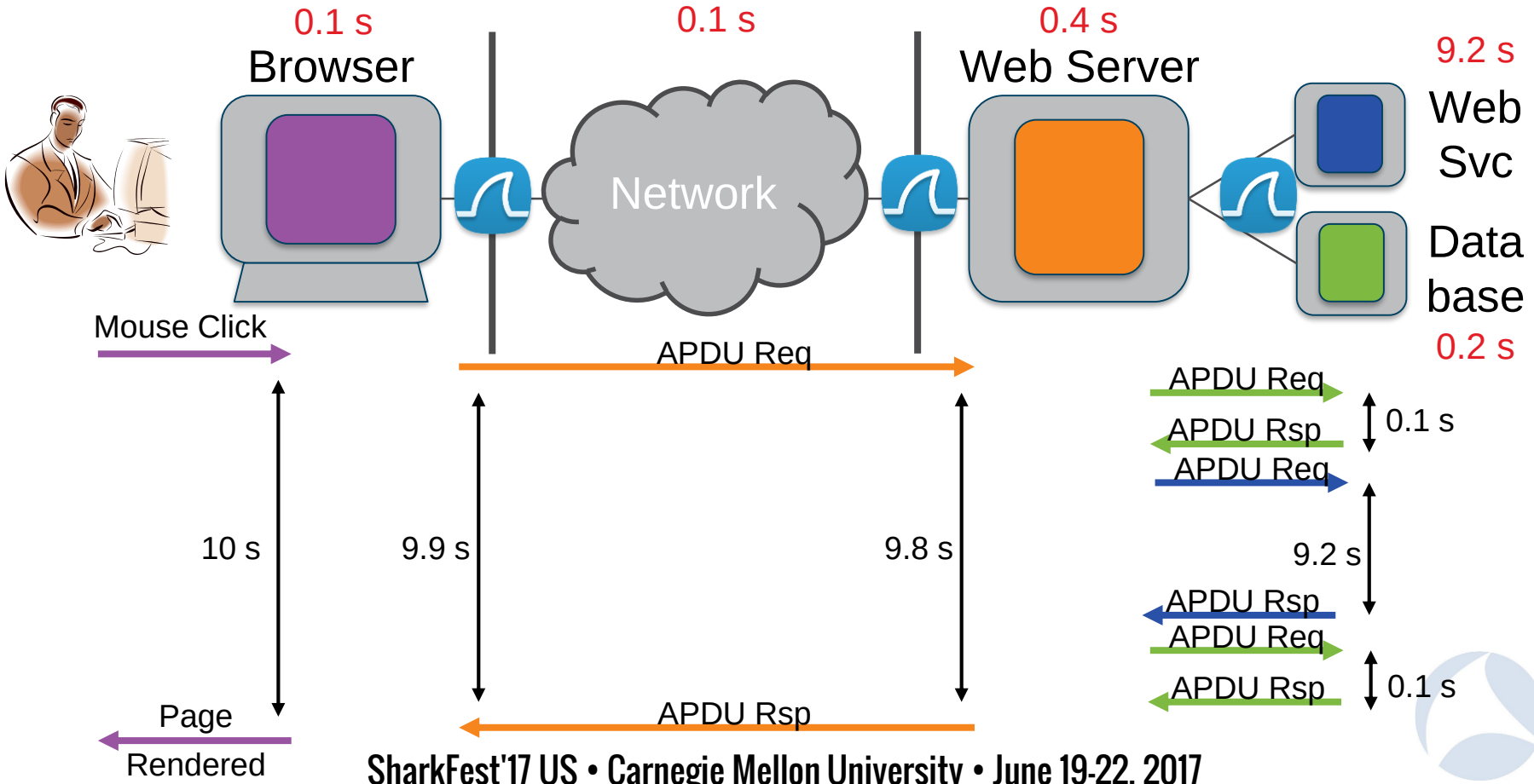
# Slow Response - Scenario 1



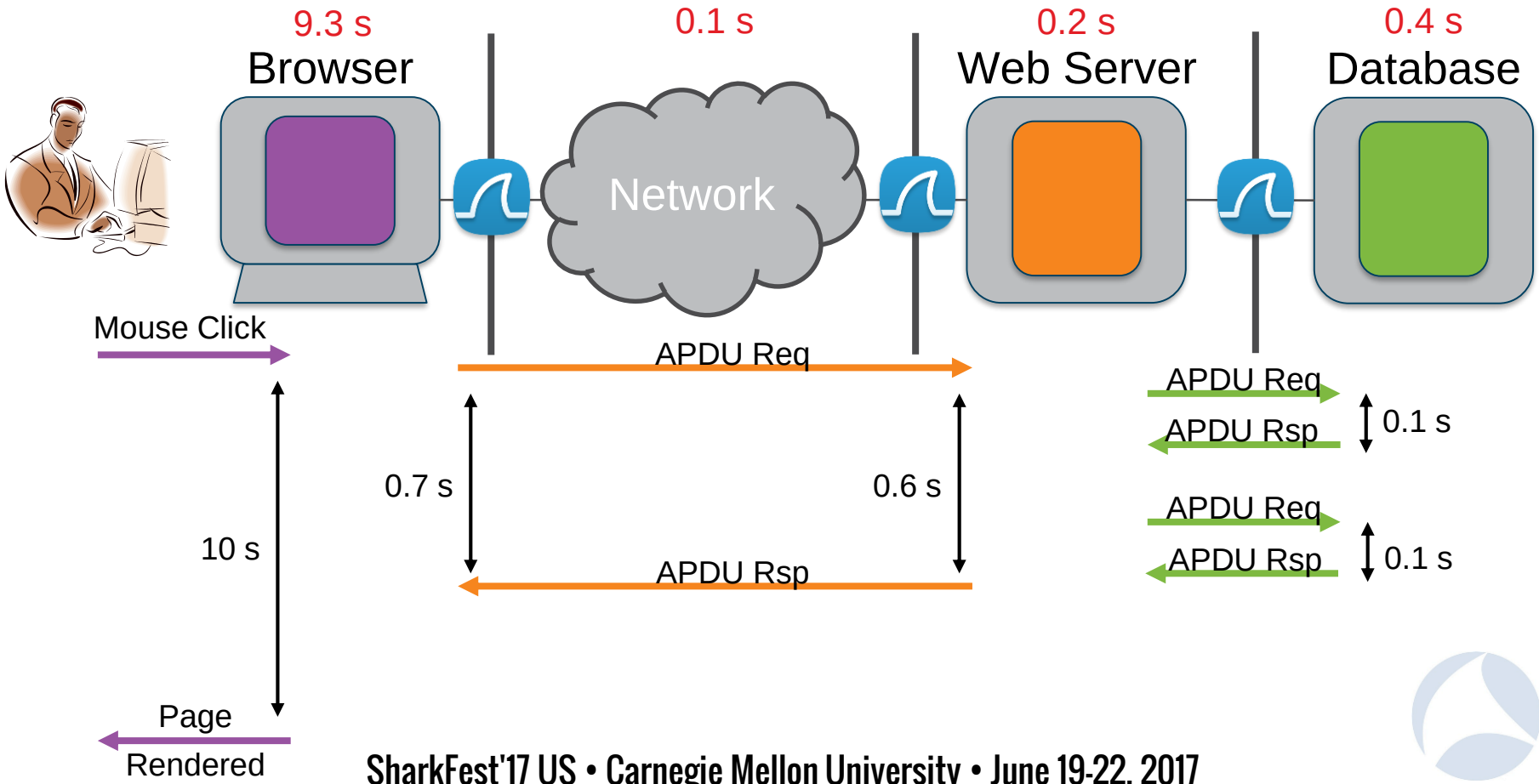
# Slow Response - Scenario 2



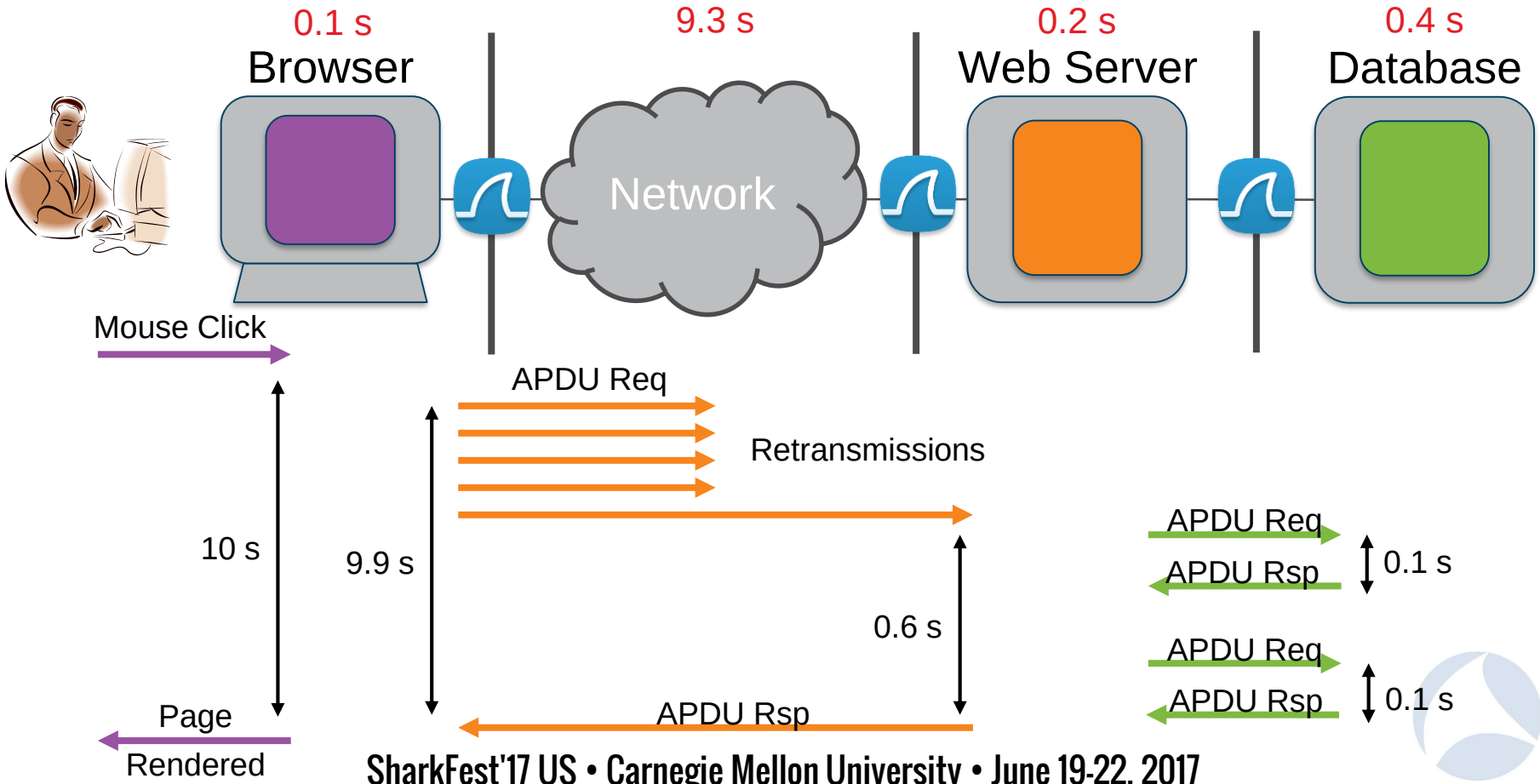
# Slow Response - Scenario 2b



# Slow Response - Scenario 3



# Slow Response - Scenario 4



# Multi-tier Correlation


tribelab

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.

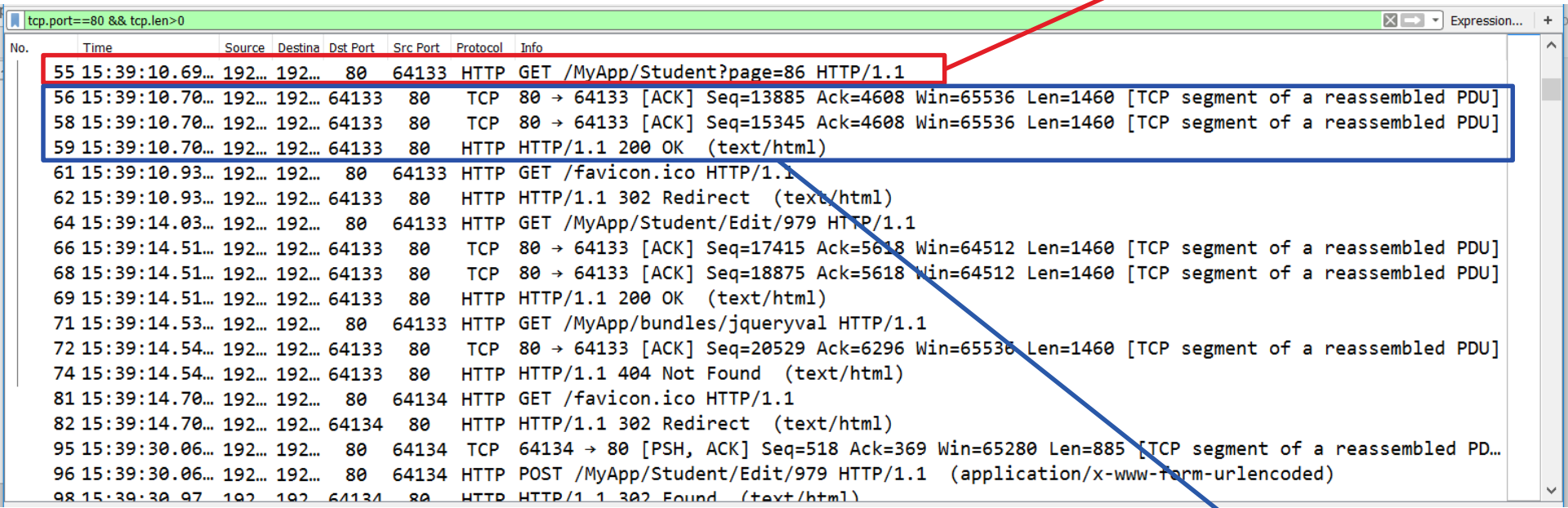
RPR: A Problem Diagnosis Method for IT Professionals

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

# APDU vs. Packets

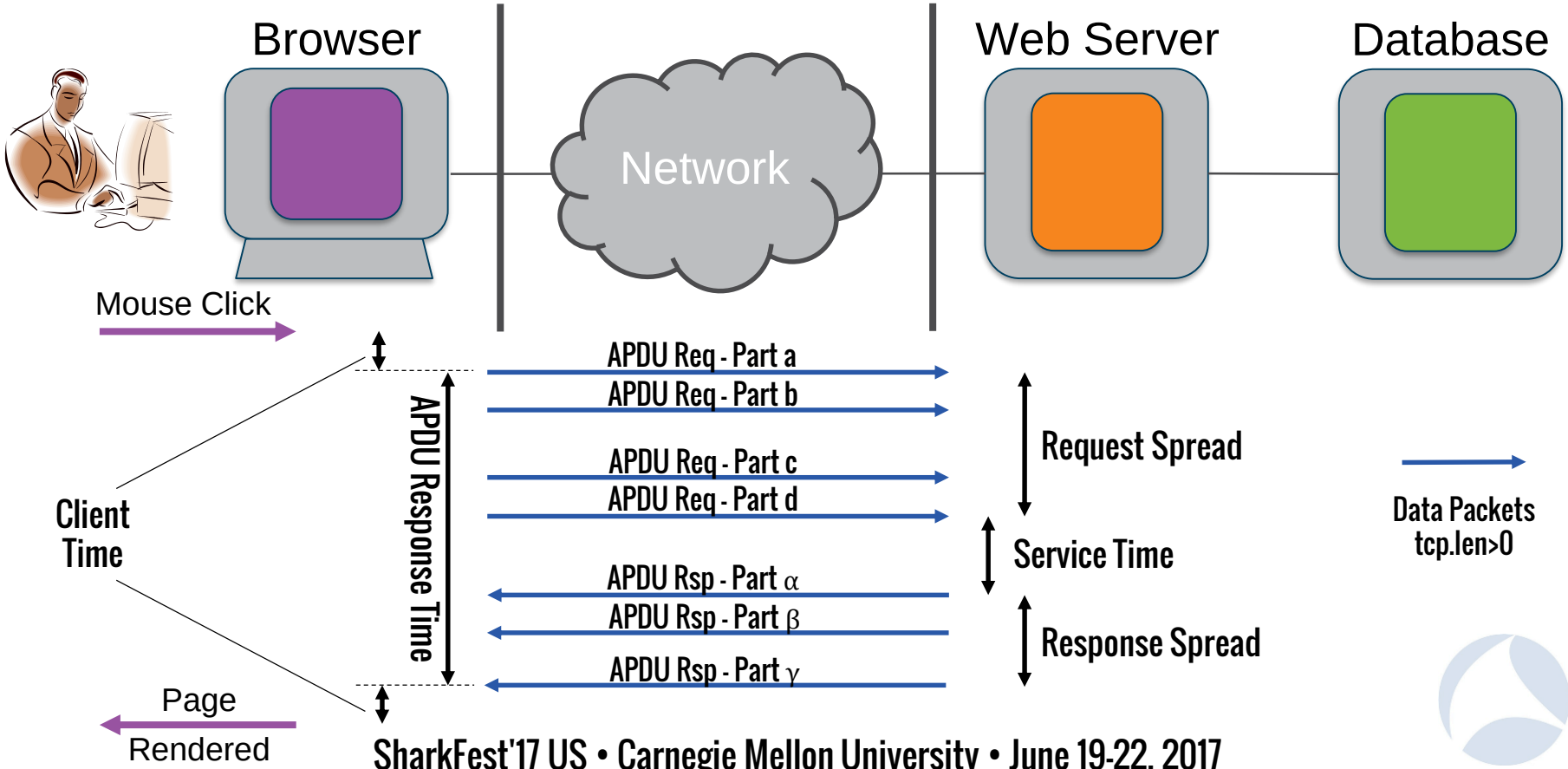
tcp.port==80 && tcp.len>0

Request APDU




Response APDU

# Response Time Element (RTE) Model

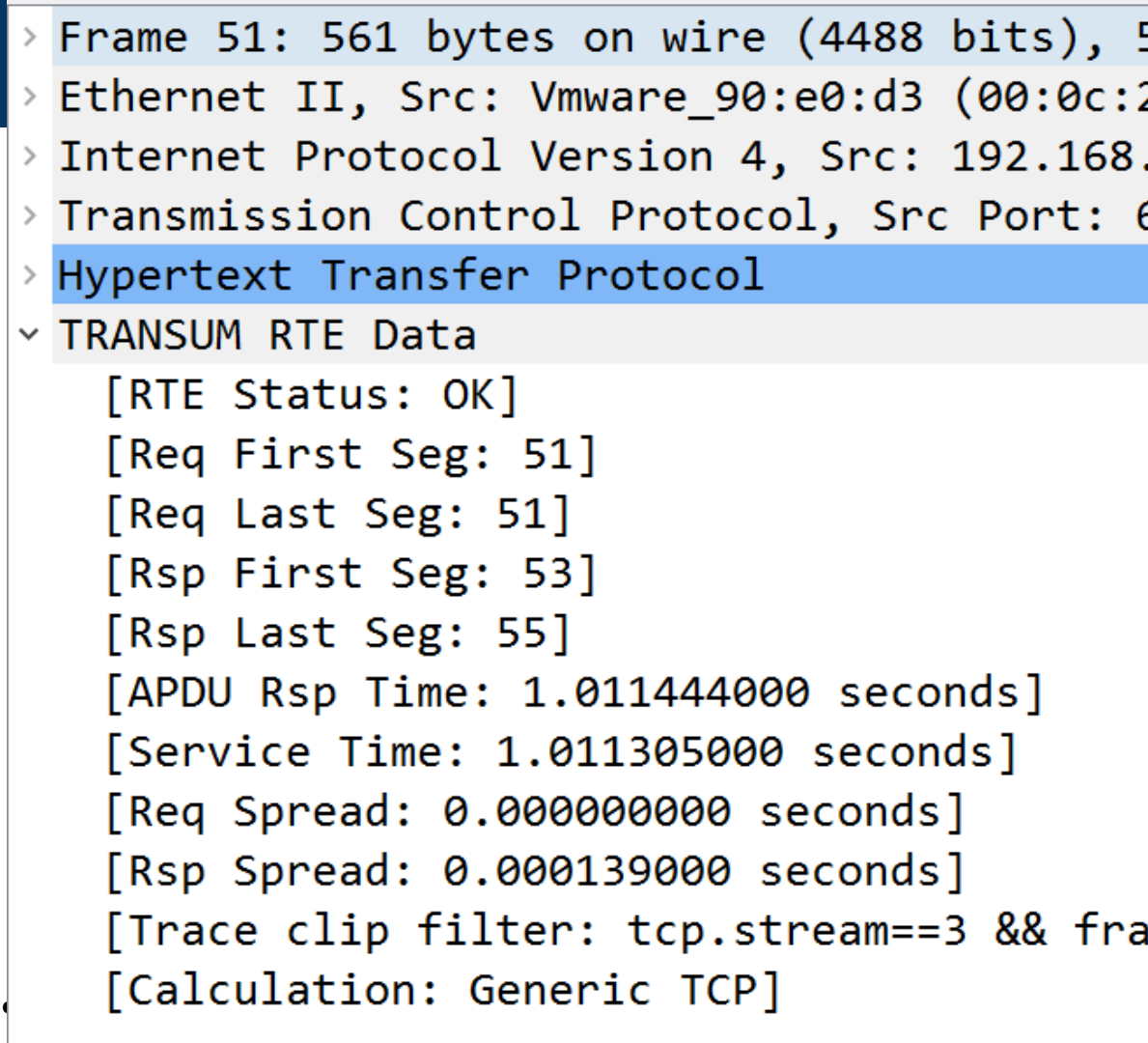


# TRANSUM and RTE

- 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



# 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

# Workbench

- Any data
- Any tool
- Expert guidance

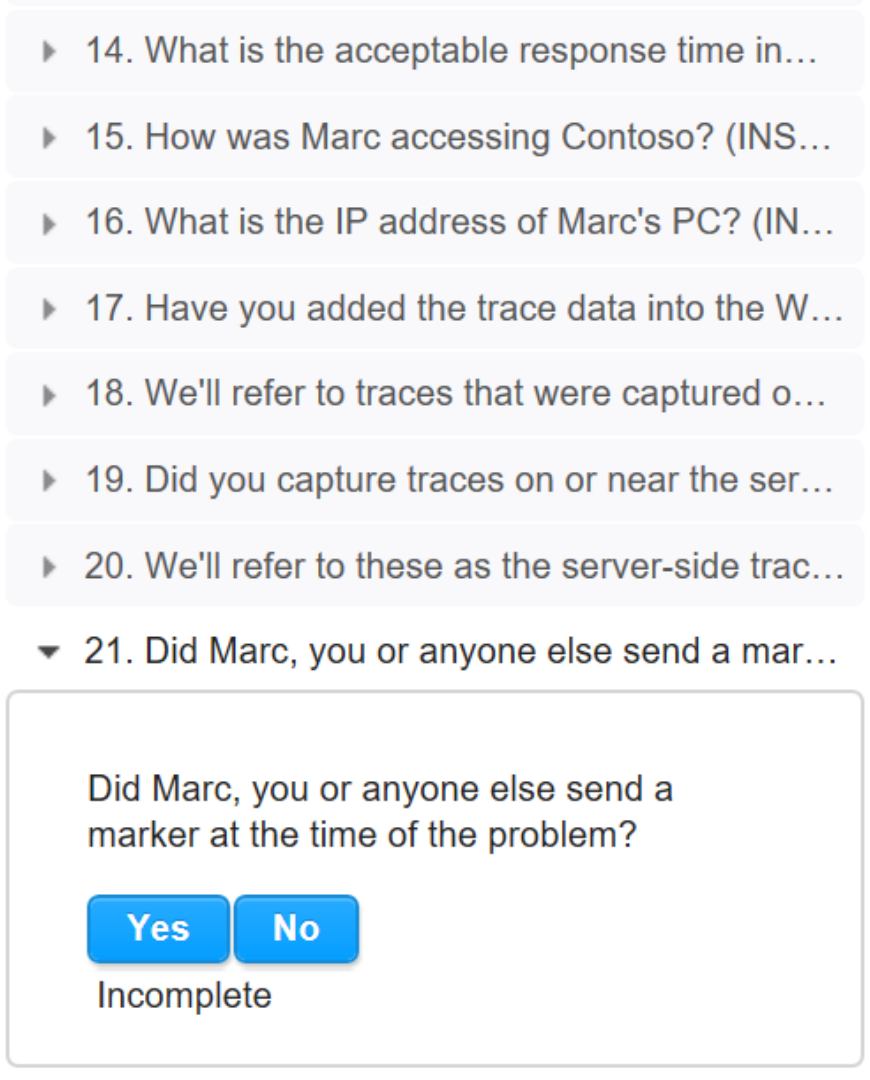
- In dev - Free trial
- FOC Community Edition

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

# Main Features

# Workflows

- Model work practices
- Adds context
- Adapts



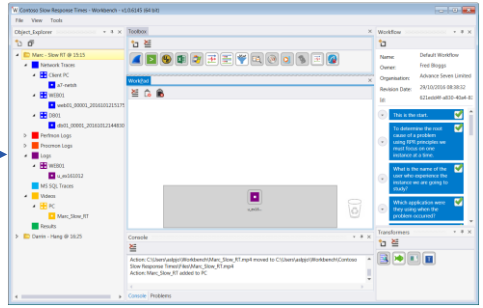
# Sharing Workflows

Community

TribeLab

3rd Parties

**Library**



- Private
- Private and shared with colleagues
- Public

In Development

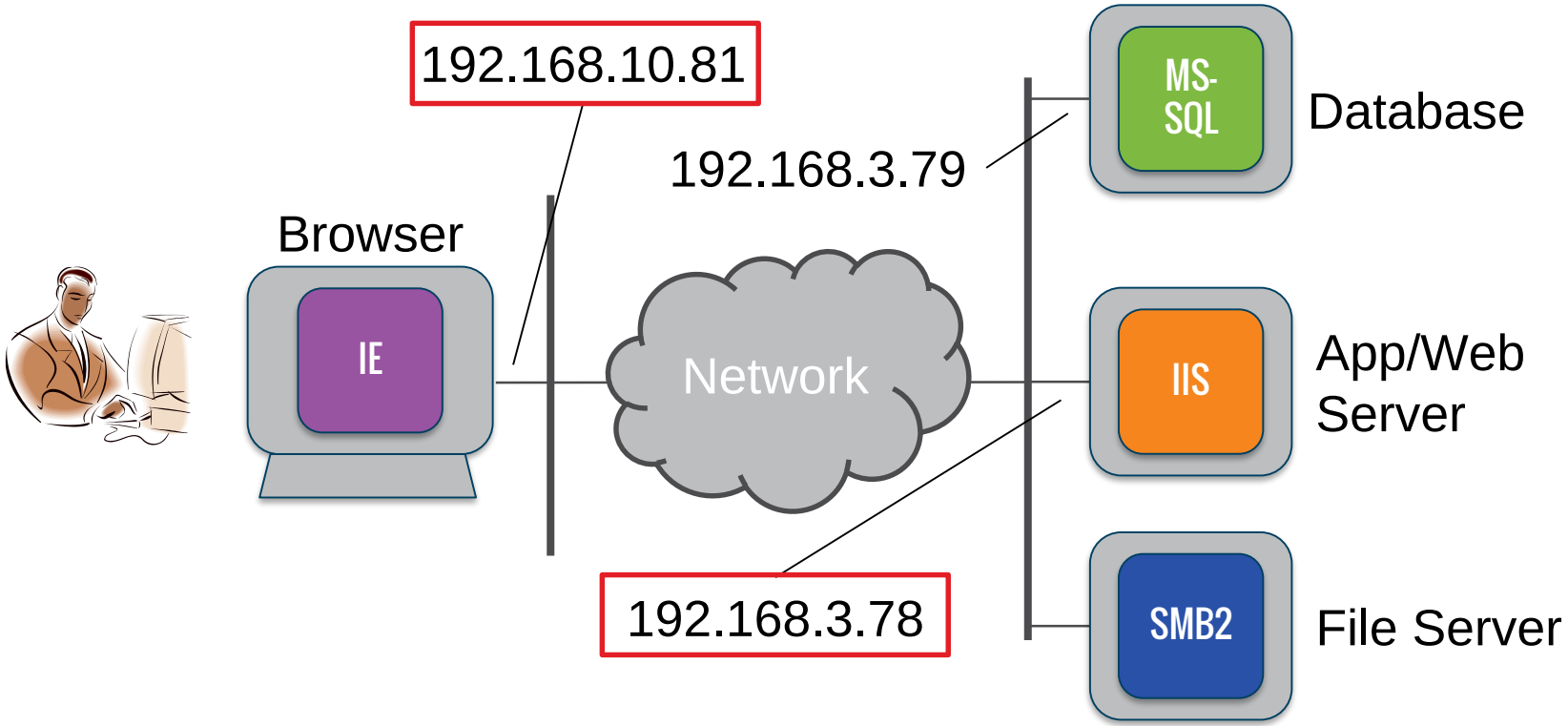
# Now for the Main Course

Use Case

# Video

The Symptom

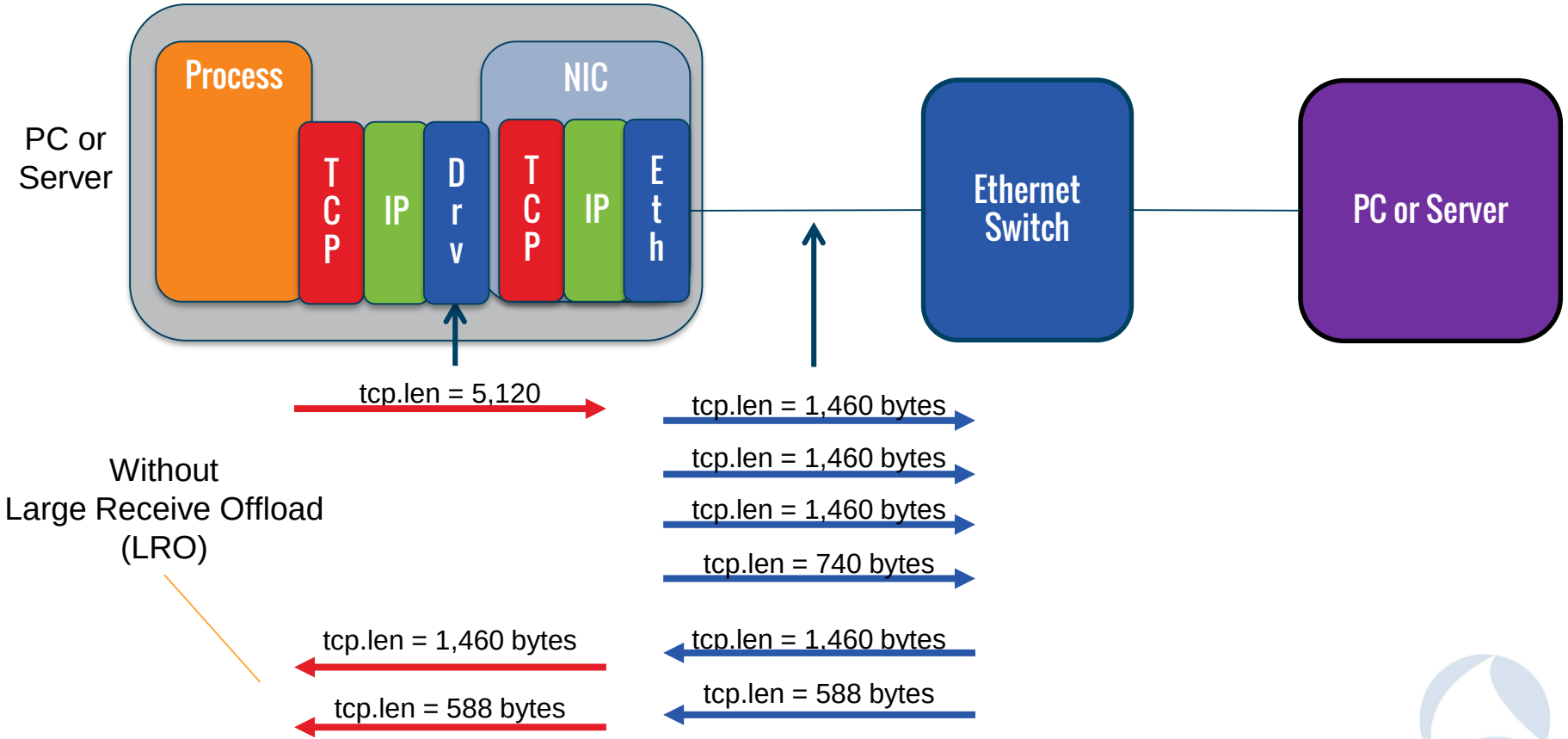
# Configuration



# 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