

# SHARKFEST 2015

WIRESHARK DEVELOPER AND USER CONFERENCE




 **COMPUTER HISTORY MUSEUM**

# TRANSUM

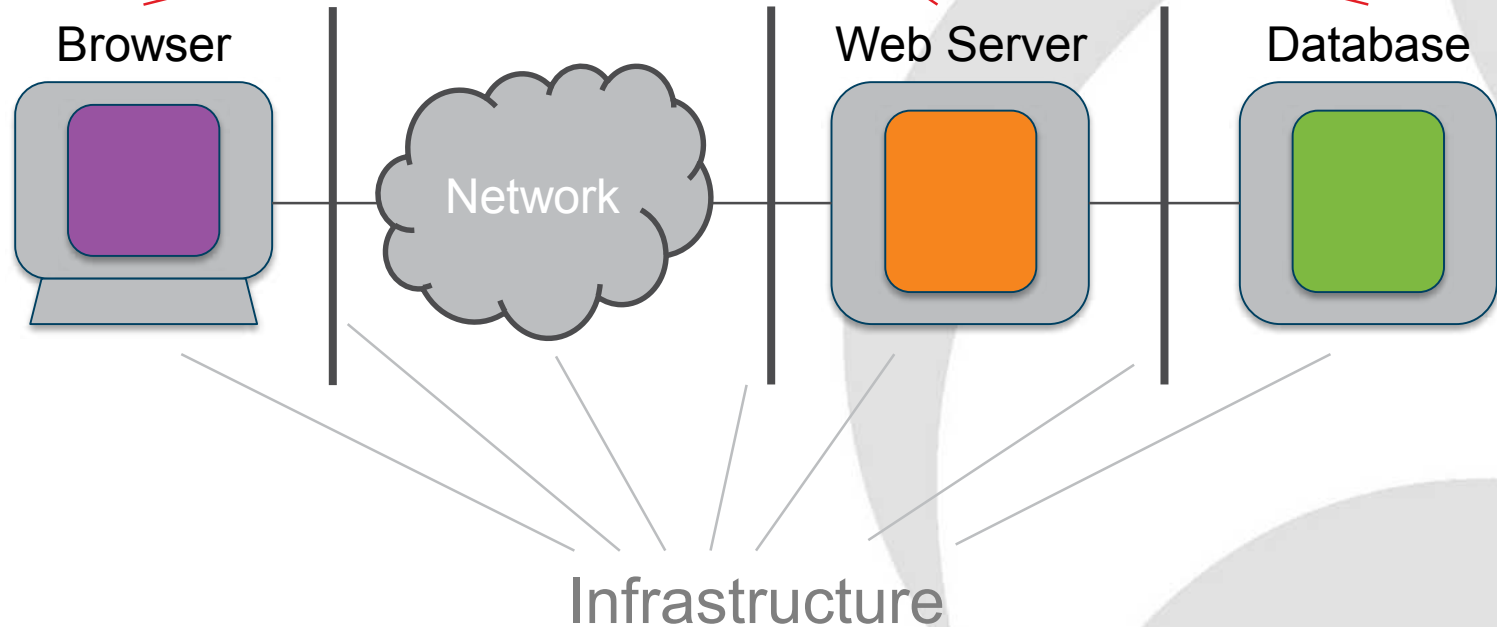
Paul Offord, Advance7

# Agenda

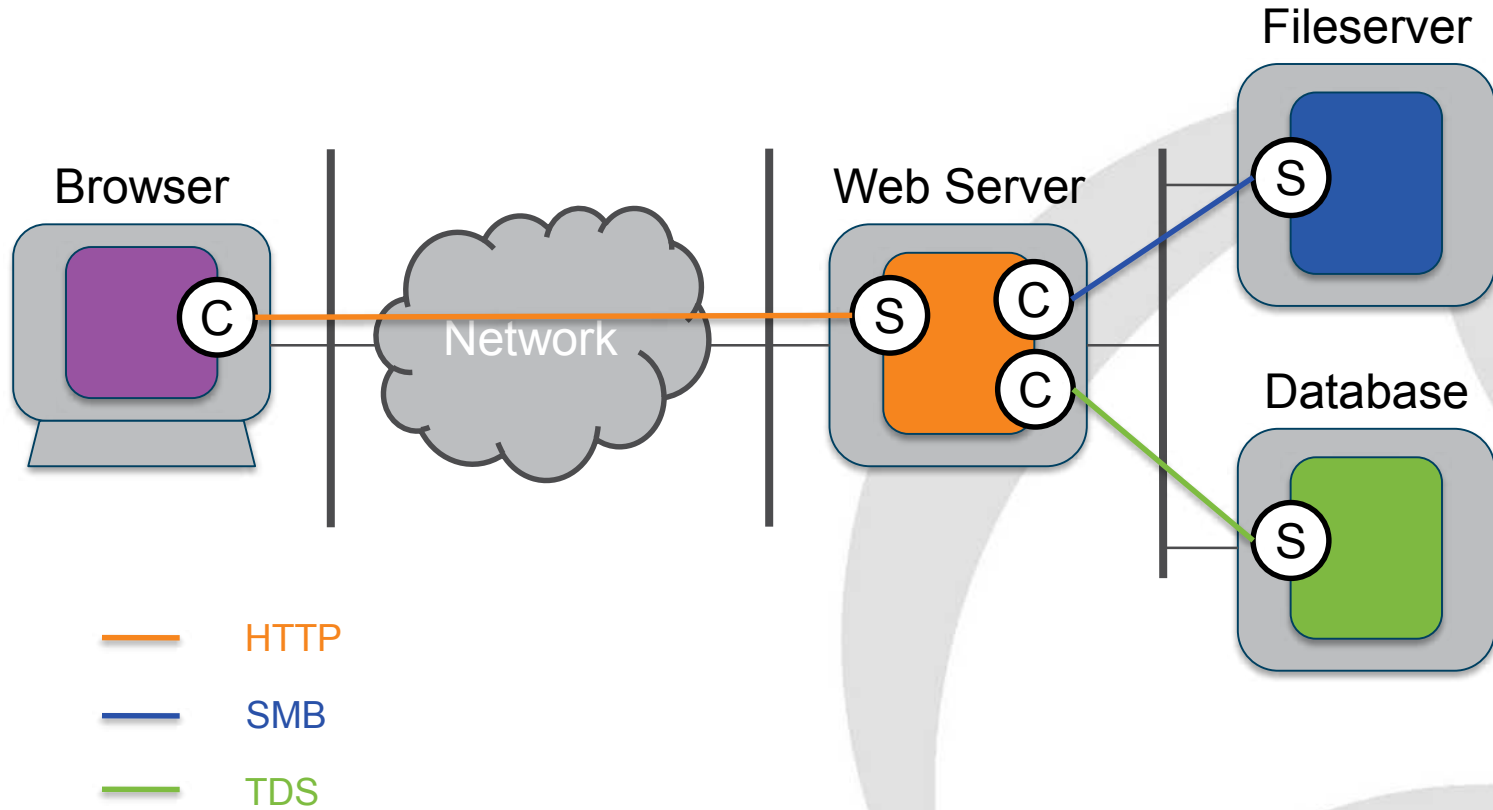
- Basic concept
  - RTE model
  - TRANSUM
  - Troubleshooting scenario
    - SMB file server
    - Web & database
- 

# System terminology

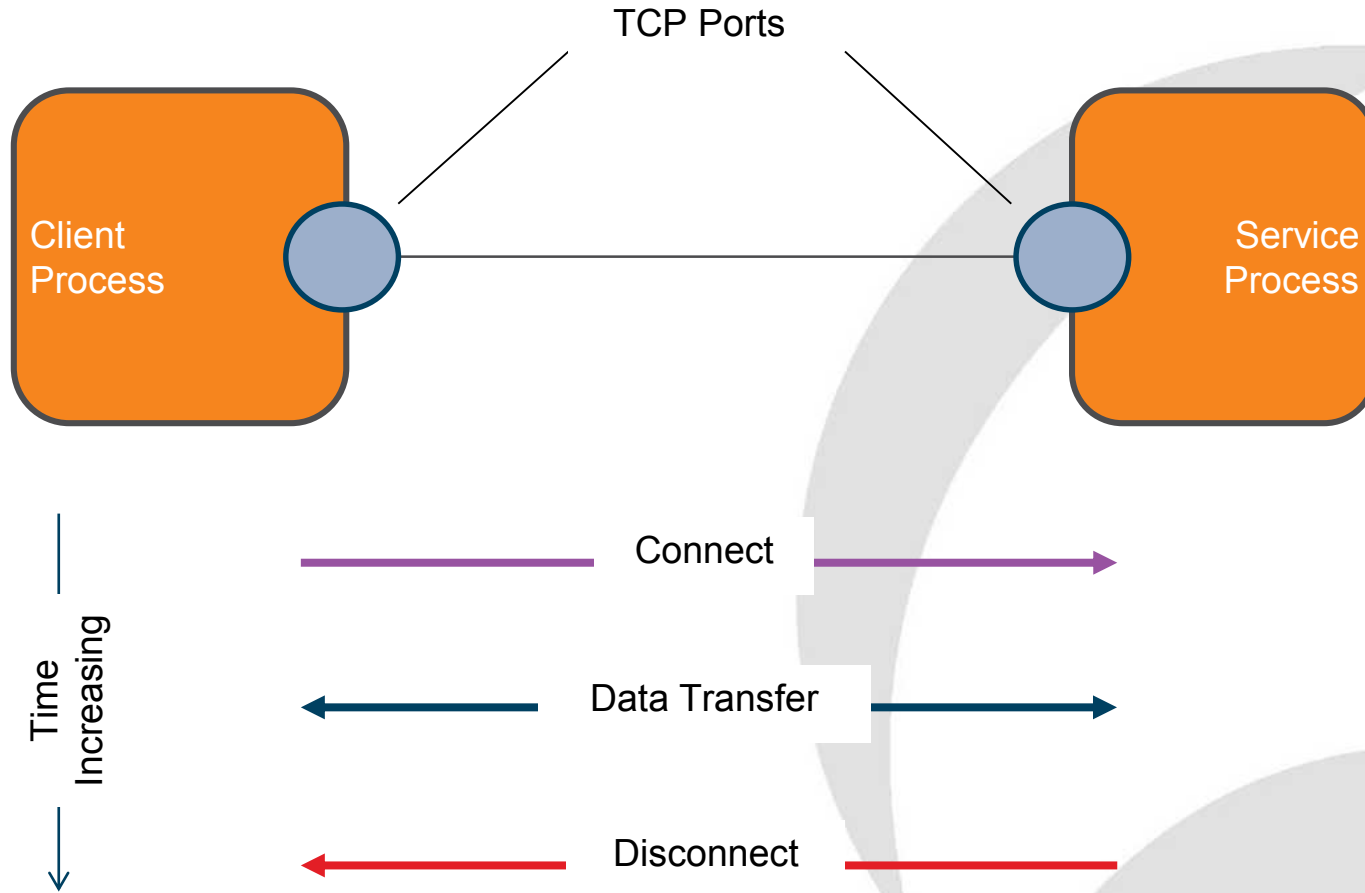
Programs running  
in Processes



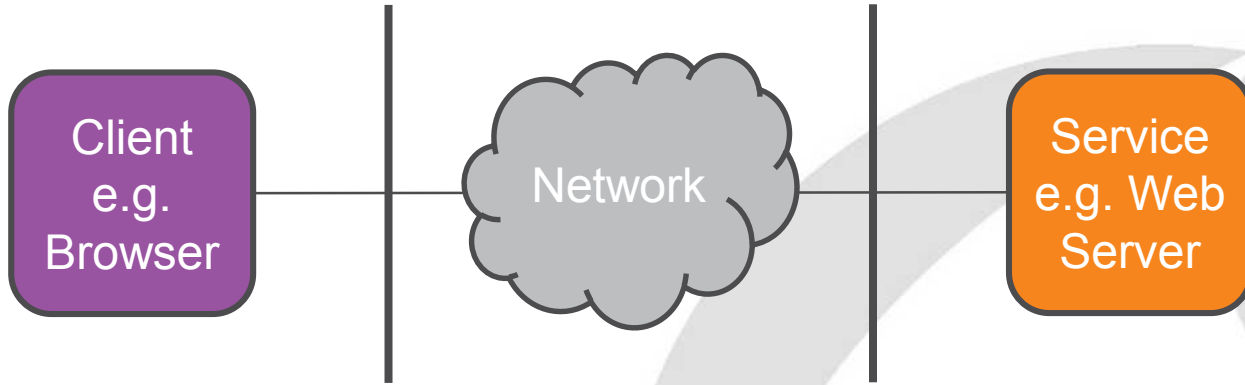
# Client and Service



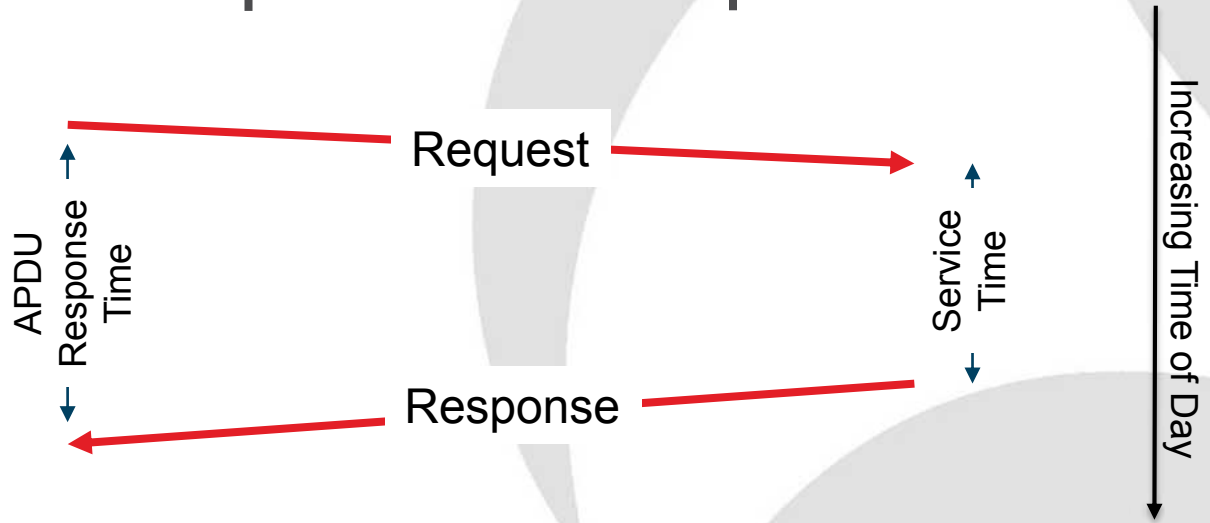
# Process-to-process communications



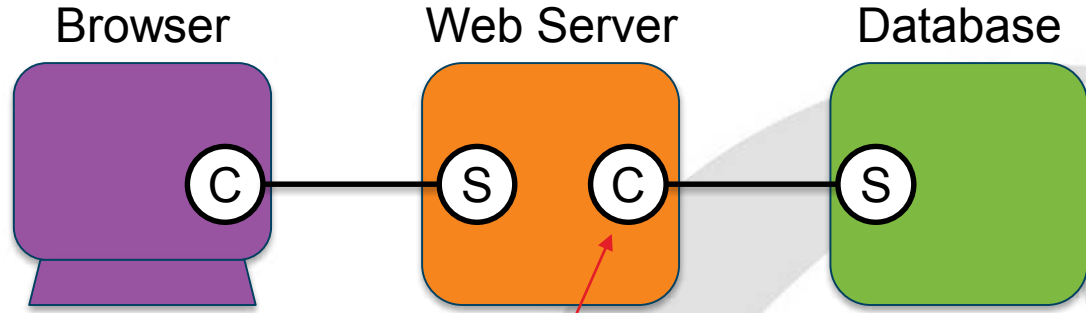
# APDU Request-Response Pairs



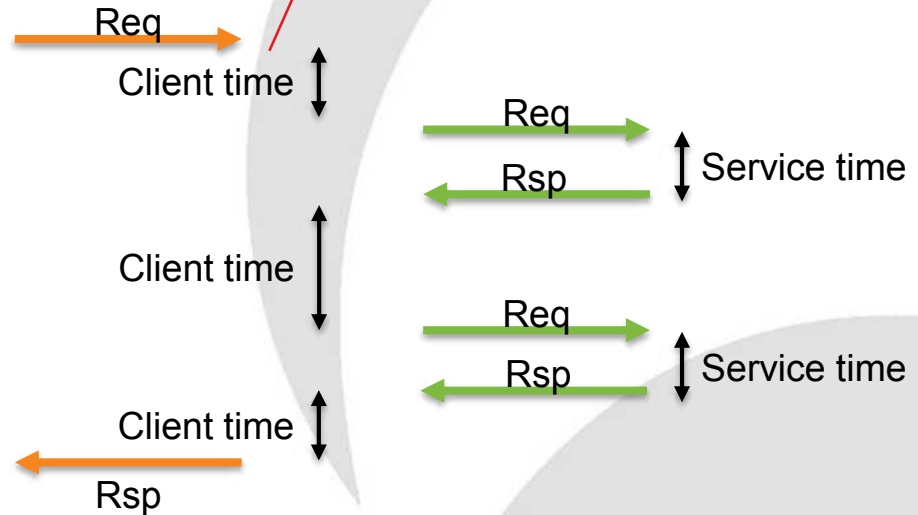
Note:  
App. Messages  
(APDUs)  
not packets



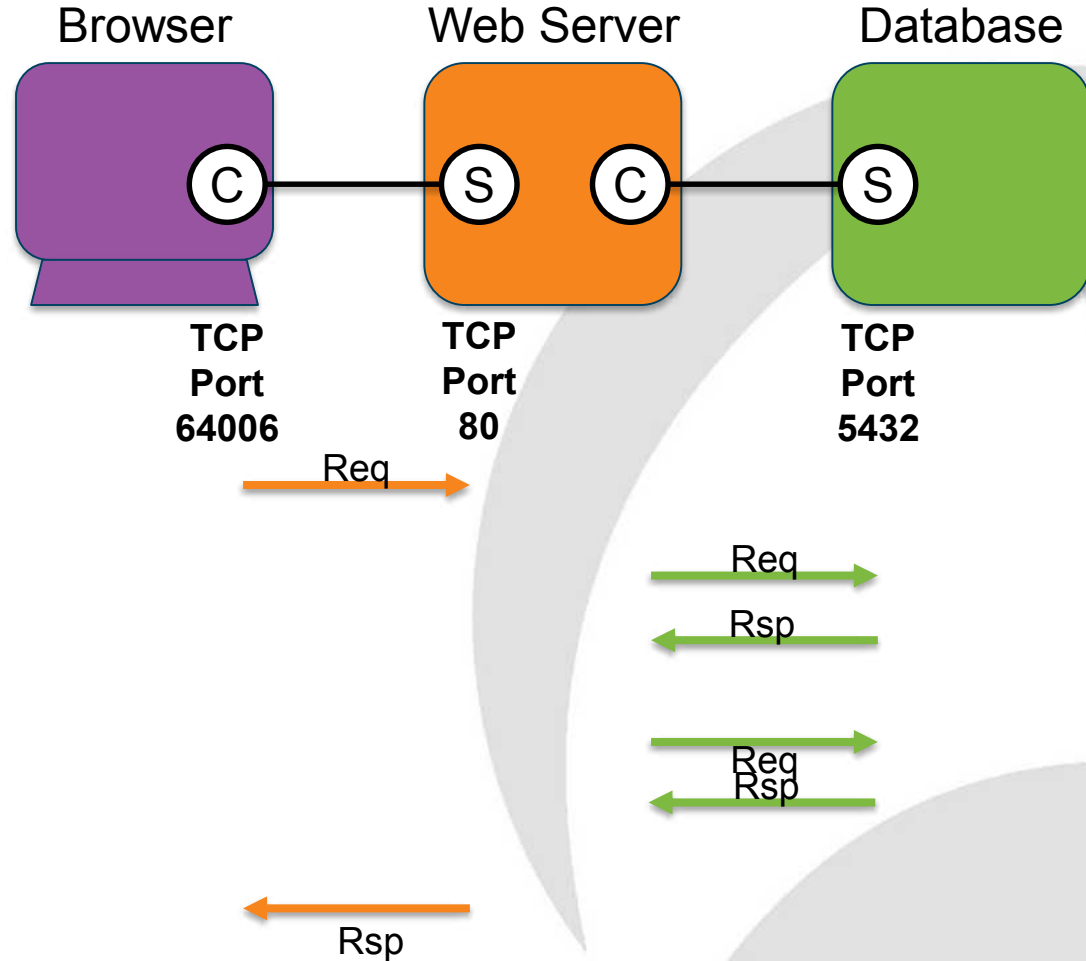
# Client and service time



Client time here refers to the Web Server as a client of the Database



# Service port numbers





# Client port, service port & direction

Filter: (tcp.port==80 && tcp.len>0) || icmp Expression... Clear Apply Save

No.	Time	Source	Destination	Src Port	Dst Port	Info
470	13:29:58.124513	192.168.1.70	192.168.1.77	64006	80	GET /TicketView.php?TicketNo=511127 HTTP/1.1
472	13:29:58.260861	192.168.1.77	192.168.1.70	80	64006	[TCP segment of a reassembled PDU]
473	13:29:58.264216	192.168.1.77	192.168.1.70	80	64006	[TCP segment of a reassembled PDU]
474	13:29:58.264883	192.168.1.77	192.168.1.70	80	64006	[TCP segment of a reassembled PDU]
475	13:29:58.265179	192.168.1.77	192.168.1.70	80	64006	HTTP/1.1 200 OK (text/html)
487	13:30:02.286050	192.168.1.70	192.168.1.77	64007	80	GET /TicketView.php?TicketNo=510760 HTTP/1.1
489	13:30:02.430607	192.168.1.77	192.168.1.70	80	64007	[TCP segment of a reassembled PDU]
490	13:30:02.430783	192.168.1.77	192.168.1.70	80	64007	[TCP segment of a reassembled PDU]
491	13:30:02.430922	192.168.1.77	192.168.1.70	80	64007	[TCP segment of a reassembled PDU]
493	13:30:02.434839	192.168.1.77	192.168.1.70	80	64007	[TCP segment of a reassembled PDU]
494	13:30:02.434950	192.168.1.77	192.168.1.70	80	64007	[TCP segment of a reassembled PDU]
495	13:30:02.435059	192.168.1.77	192.168.1.70	80	64007	HTTP/1.1 200 OK (text/html)
540	13:30:05.376557	192.168.1.70	192.168.1.77	64008	80	GET /TicketView.php?TicketNo=510005 HTTP/1.1
542	13:30:05.523119	192.168.1.77	192.168.1.70	80	64008	[TCP segment of a reassembled PDU]

Coming from the Client  
on TCP Port 64008

Going to the Service  
on TCP Port 80

# APDUs vs. packets

Request

No.	Time	Source	Destination	Src Port	Dst Port	Info
470	13:29:58.124513	192.168.1.70	192.168.1.77	64006	80	GET /TicketView.php?TicketNo=511127 HTTP/1.1
472	13:29:58.260861	192.168.1.77	192.168.1.70	80	64006	[TCP segment of a reassembled PDU]
473	13:29:58.264216	192.168.1.77	192.168.1.70	80	64006	[TCP segment of a reassembled PDU]
474	13:29:58.264883	192.168.1.77	192.168.1.70	80	64006	[TCP segment of a reassembled PDU]
475	13:29:58.265179	192.168.1.77	192.168.1.70	80	64006	HTTP/1.1 200 OK (text/html)
487	13:30:02.286050	192.168.1.70	192.168.1.77	64007	80	GET /TicketView.php?TicketNo=510760 HTTP/1.1
489	13:30:02.430607	192.168.1.77	192.168.1.70	80	64007	[TCP segment of a reassembled PDU]
490	13:30:02.430783	192.168.1.77	192.168.1.70	80	64007	[TCP segment of a reassembled PDU]
491	13:30:02.430922	192.168.1.77	192.168.1.70	80	64007	[TCP segment of a reassembled PDU]
493	13:30:02.434839	192.168.1.77	192.168.1.70	80	64007	[TCP segment of a reassembled PDU]
494	13:30:02.434950	192.168.1.77	192.168.1.70	80	64007	[TCP segment of a reassembled PDU]
495	13:30:02.435059	192.168.1.77	192.168.1.70	80	64007	HTTP/1.1 200 OK (text/html)
540	13:30:05.376557	192.168.1.70	192.168.1.77	64008	80	GET /TicketView.php?TicketNo=510005 HTTP/1.1
542	13:30:05.523119	192.168.1.77	192.168.1.70	80	64008	[TCP segment of a reassembled PDU]

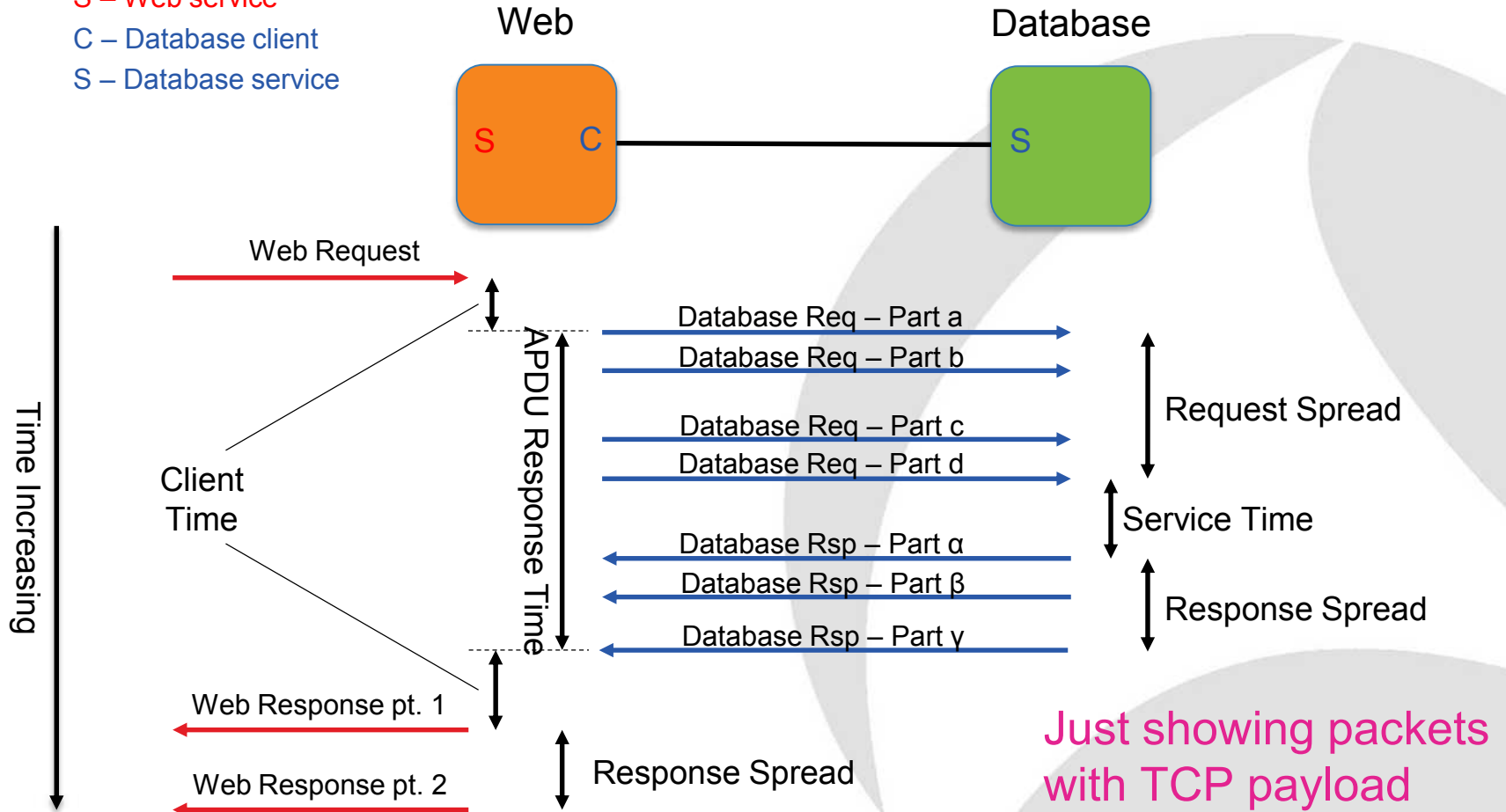
Response

Request APDU => 1 packet

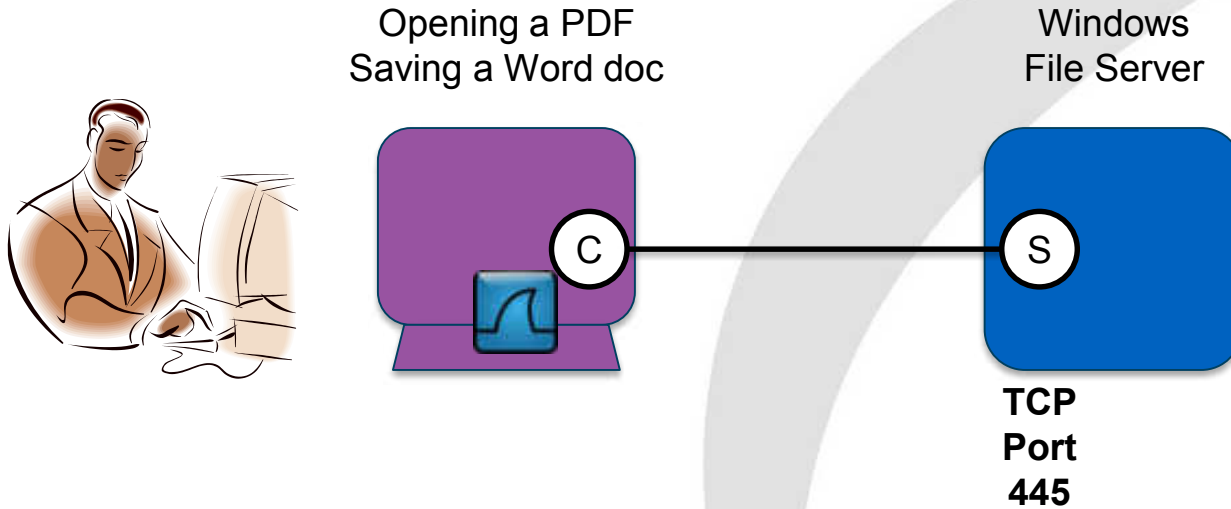
Response APDU => 4 packets

# Response Time Elements model

S – Web service  
C – Database client  
S – Database service



# Windows file server access





# File server read

No.	Time	Source	Destination	Src Port	Dst Port	Frame Len	Info
257	12:41:54.414362	10.100.20.7	10.100.20.224	55065	445	171	Read Request Len:12288 Off:8192 File
258	12:41:54.414702	10.100.20.224	10.100.100.20.7	445	55065	1414	[TCP segment of a reassembled PDU]
259	12:41:54.414715	10.100.20.224	10.100.100.20.7	445	55065	1414	[TCP segment of a reassembled PDU]
260	12:41:54.414742	10.100.20.224	10.100.100.20.7	445	55065	1414	[TCP segment of a reassembled PDU]
261	12:41:54.414749	10.100.20.224	10.100.100.20.7	445	55065	1414	[TCP segment of a reassembled PDU]
262	12:41:54.414754	10.100.20.224	10.100.100.20.7	445	55065	1414	[TCP segment of a reassembled PDU]
263	12:41:54.414768	10.100.20.224	10.100.100.20.7	445	55065	1414	[TCP segment of a reassembled PDU]
264	12:41:54.414800	10.100.20.224	10.100.100.20.7	445	55065	1414	[TCP segment of a reassembled PDU]
265	12:41:54.414805	10.100.20.224	10.100.100.20.7	445	55065	1414	[TCP segment of a reassembled PDU]
266	12:41:54.414820	10.100.20.224	10.100.100.20.7	445	55065	1414	[TCP segment of a reassembled PDU]
267	12:41:54.414825	10.100.20.224	10.100.100.20.7	445	55065	186	Read Response

## Response Spread

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:

```
Credits granted. 1
+ F Packet 267 001
  C... .. 0x00000000
  Message ID: 696
  Process Id: 0x0000feff
  Tree Id: 0x00000005
  Session Id: 0x0000040000000001
  Signature: 00000000000000000000000000000000
  [Response to: 257]
  [Time from request: 0.000463000 seconds]
+ Read Response (0x08)
```

Includes Rsp Spread

# File server write

No.	Time	Source	Destination	Src Port	Dst Port	Frame Len	Info
452	18:18:15.487444	10.100.20.14	10.100.20.224	61326	445	1514	[TCP segment of a reassembled PDU]
453	18:18:15.487483	10.100.20.14	10.100.20.224	61326	445	1514	[TCP segment of a reassembled PDU]
454	18:18:15.487501	10.100.20.14	10.100.20.224	61326	445	1514	[TCP segment of a reassembled PDU]
455	18:18:15.487518	10.100.20.14	10.100.20.224	61326	445	1514	[TCP segment of a reassembled PDU]
456	18:18:15.487537	10.100.20.14	10.100.20.224	61326	445	1514	[TCP segment of a reassembled PDU]
457	18:18:15.487556	10.100.20.14	10.100.20.224	61326	445	1514	[TCP segment of a reassembled PDU]
458	18:18:15.487574	10.100.20.14	10.100.20.224	61326	445	1514	[TCP segment of a reassembled PDU]
459	18:18:15.487591	10.100.20.14	10.100.20.224	61326	445	1514	[TCP segment of a reassembled PDU]
460	18:18:15.487609	10.100.20.14	10.100.20.224	61326	445	1514	[TCP segment of a reassembled PDU]
461	18:18:15.487627	10.100.20.14	10.100.20.224	61326	445	1514	[TCP segment of a reassembled PDU]
462	18:18:15.487644	10.100.20.14	10.100.20.224	61326	445	1329	write Request Len:15759 Off:0 File:
471	18:18:15.498146	10.100.20.224	10.100.20.14	445	61326	138	write Response

## Request Spread

Show TCP summary in protocol tree:

Validate the TCP checksum if possible:

Allow subdissector to reassemble TCP streams:

---

Analyze TCP sequence numbers:

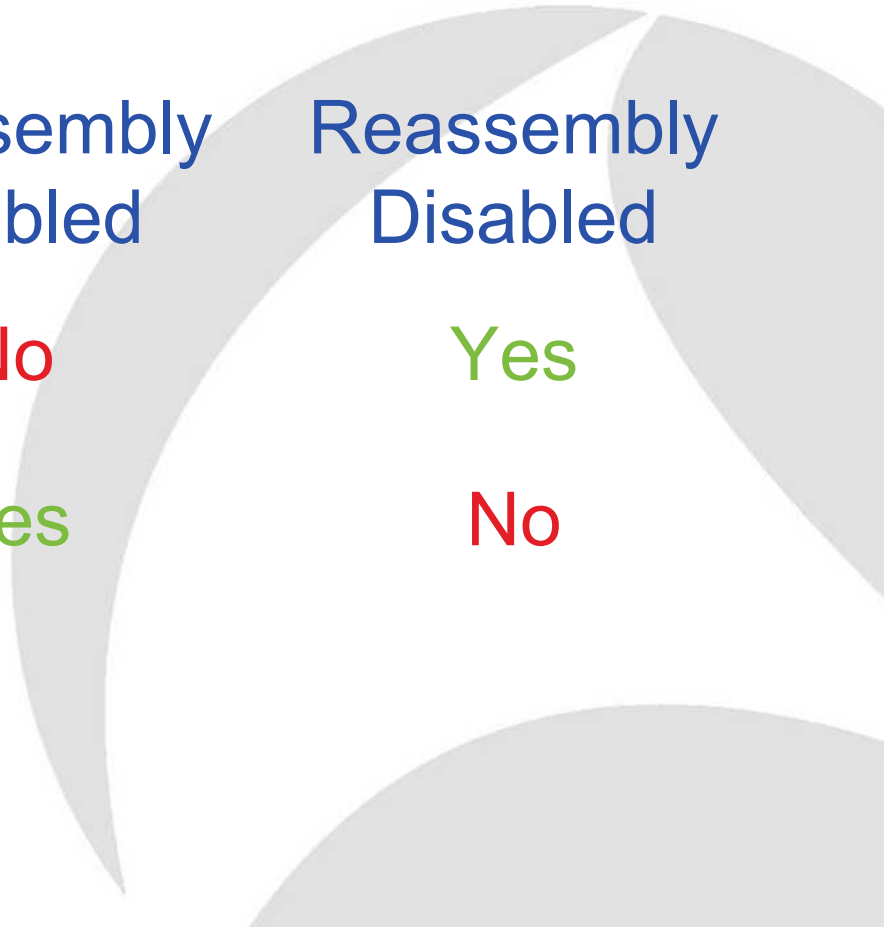
Relative sequence numbers:

Credits granted: 1  
 Packet 471 0001  
 Chain offset: 0x00000000  
 Message ID: 815  
 Process Id: 0x0000feff  
 Tree Id: 0x00000005  
 Session Id: 0x0000040000000005  
 Signature: 00000000000000000000000000000000  
 [Response to: 462]  
 [Time from request: 0.010502000 seconds]  
 Write Response (0x09)  
 StructureSize: 0x0011

Req Spread not included

# The issue

	Reassembly Enabled	Reassembly Disabled
Request Spread	No	Yes
Response Spread	Yes	No



# What that means in practice

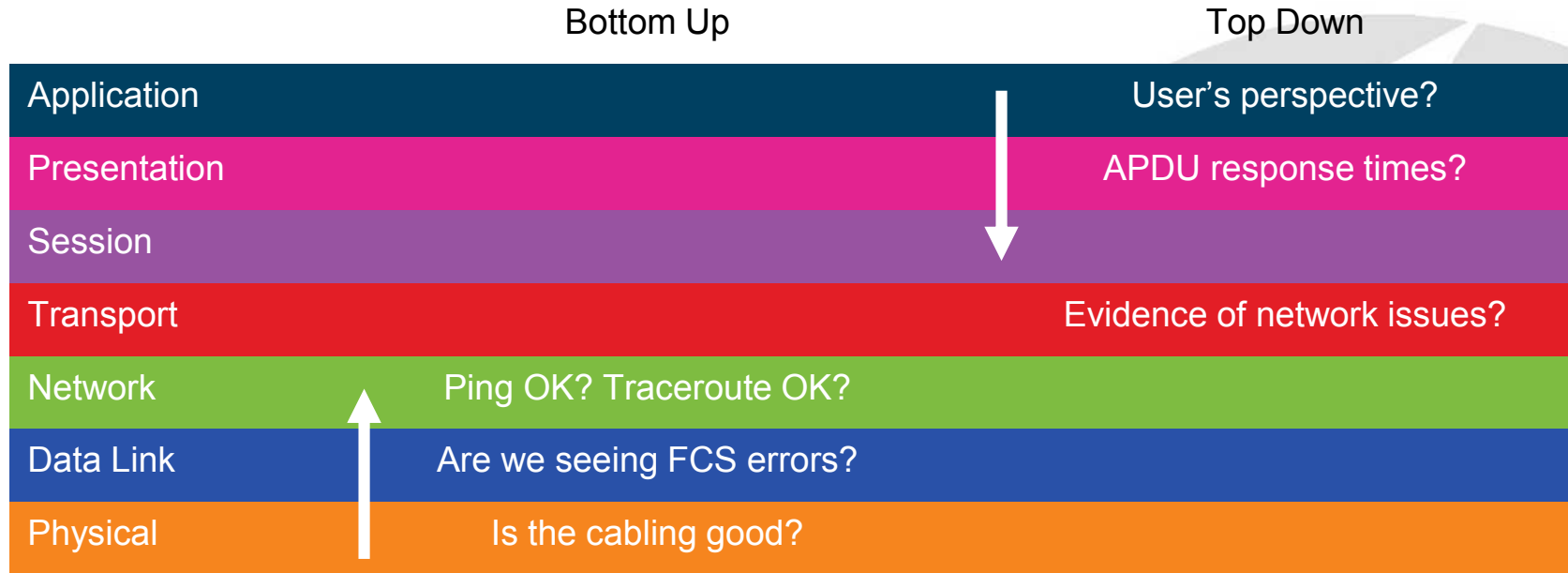
	Reassembly Enabled	Reassembly Disabled
Accurate Read APDU Rsp Time	Yes	No
Accurate Write APDU Rsp Time	No	Yes
Accurate Read Service Time	No	Yes
Accurate Write Service Time	Yes	No



**Time for  
Questions**



# Bottom up vs. top down



**Faster & more reliable**

# What's needed

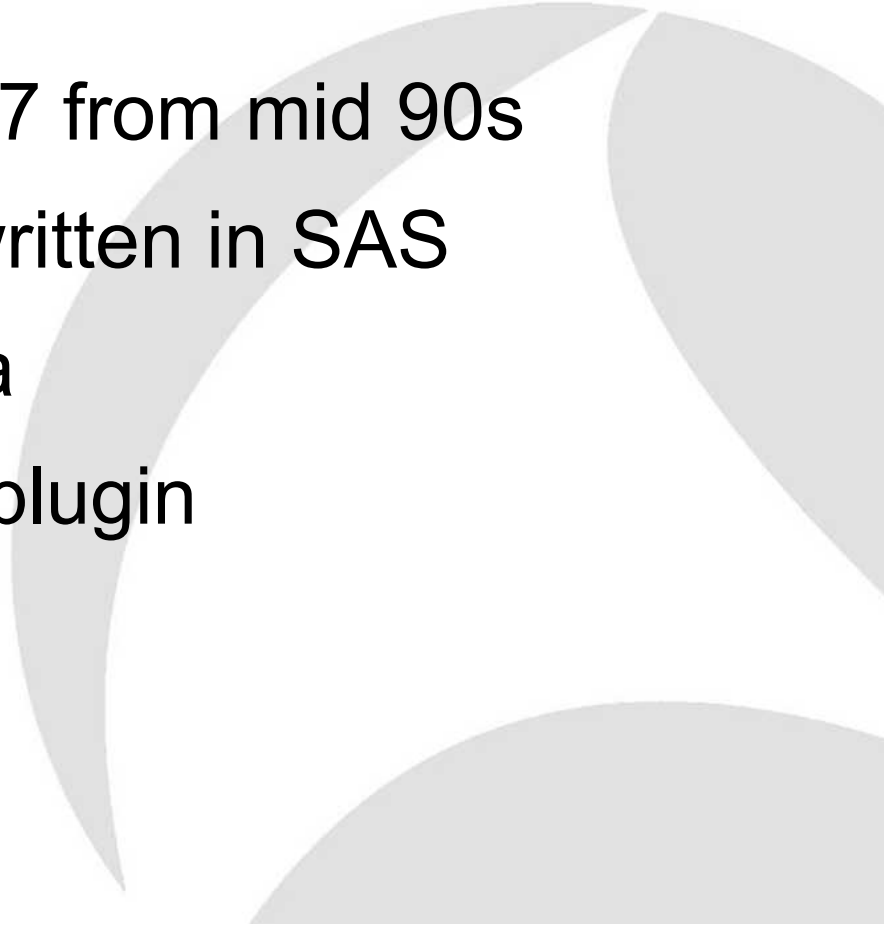
## Client Perspective of Performance

- APDU response time
- First request to last response

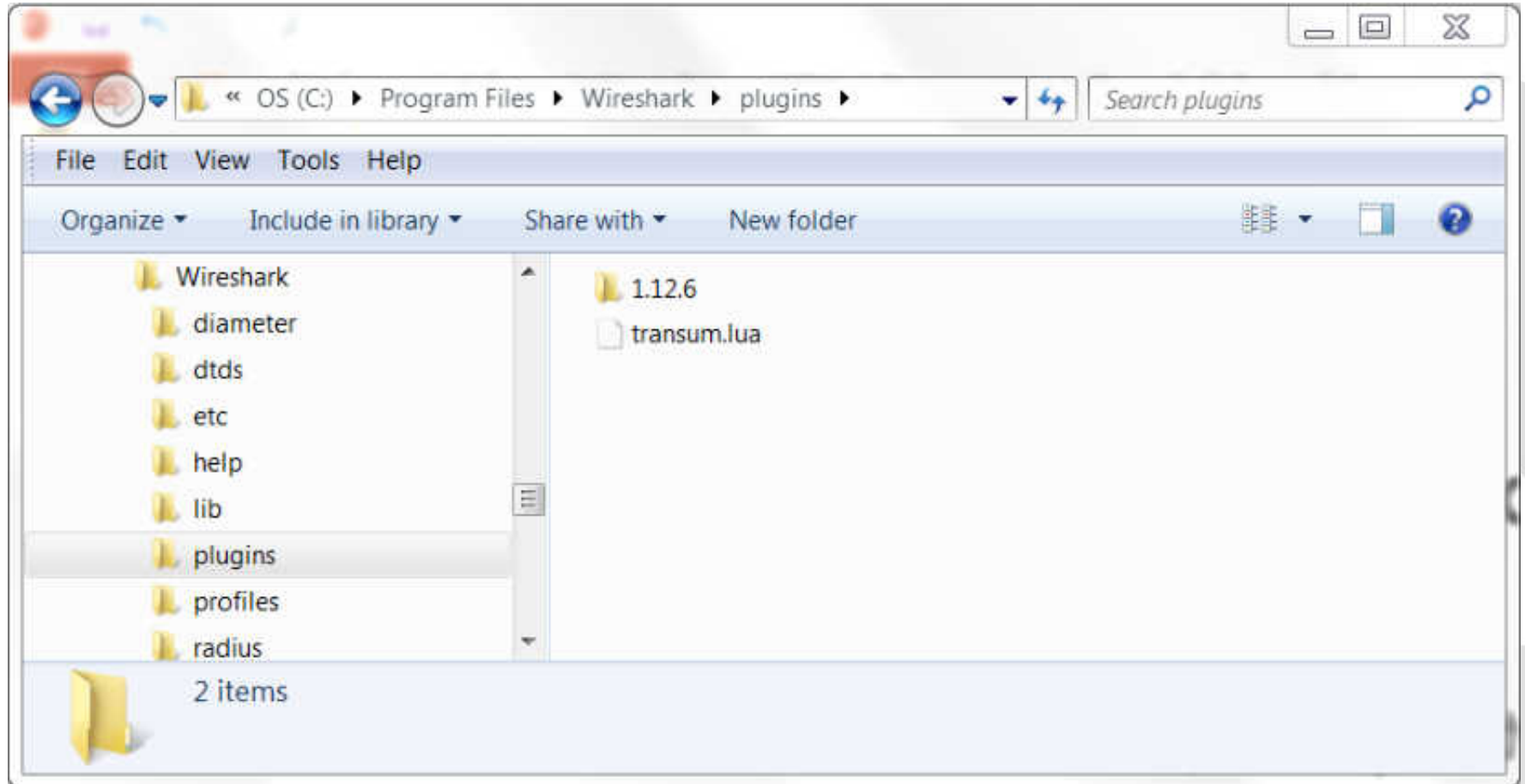
## Service Performance Perspective

- Service time
- Last request to first response

# TRANSUM history

- Developed by Advance7 from mid 90s
  - Started as a program written in SAS
  - Recently ported to Java
  - Now a Wireshark LUA plugin
- 

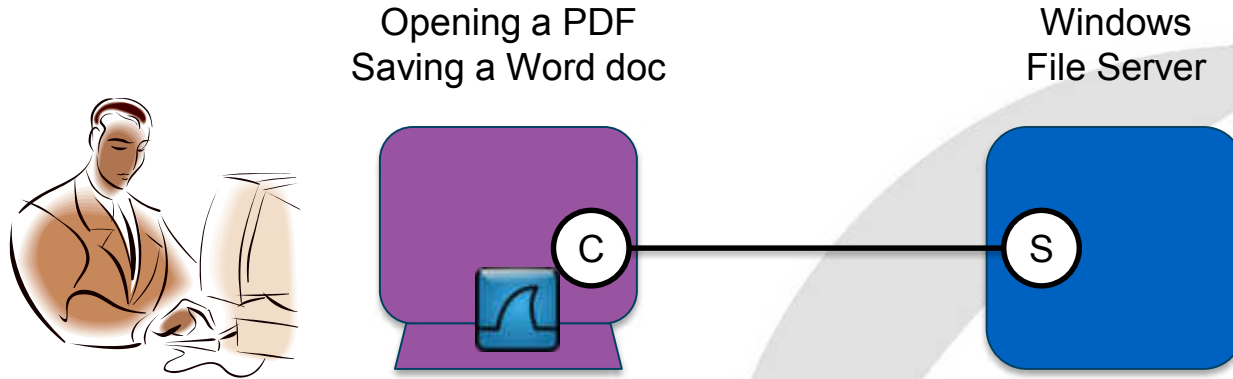
# Wireshark LUA plugin



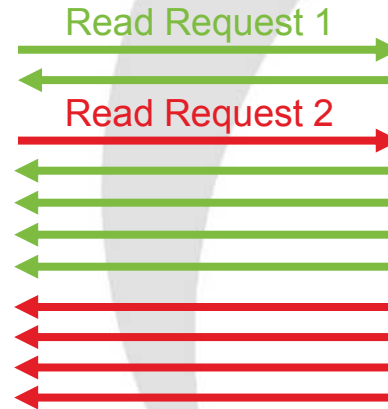
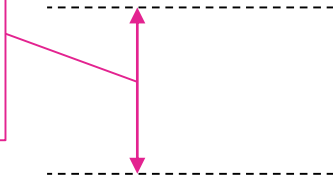


**Checking  
PDF Read performance  
with TRANSUM**

# SMB multi-credit & congestion



This appears as  
Service Time in  
RTE Data



# Generic TCP example

