



Pakete lügen nicht - Wireshark

# Protokoll Analyse mit Wireshark

Rolf Leutert, Leutert NetServices  
Stefan Rüeger, Studerus AG



# Vorstellung



Rolf Leutert, Network Consultant  
Leutert NetServices  
8058 Zürich-Flughafen

- Netzwerk Analyse & Troubleshooting
- Protokoll Schulungen TCP/IP, WLAN, VoIP, IPv6
- Wireshark® Certified Network Analyst 2010
- Wireshark® Instructor seit 2006
- Sniffer® certified Instructor seit 1990

[leutert@wireshark.ch](mailto:leutert@wireshark.ch)  
[www.wireshark.ch](http://www.wireshark.ch)





# Agenda



- Einführung in die Fehlersuche
- Wireshark Packet Analyser
- Einführung in die TCP Analyse
- Fehlersuche Fall 1 : Session Hang-Up
- Fehlersuche Fall 2 : Slow Printing
- Fehlersuche Fall 3 : Bad WAN Throughput
- Kurshinweise

# Einführung in die Fehlersuche

Eingrenzung der Fehlerquellen

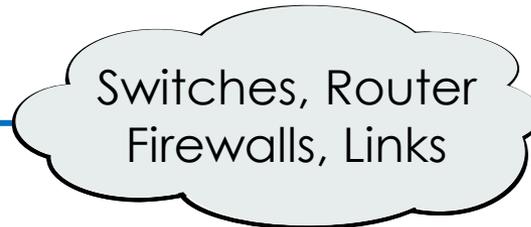
Workstation



Überlast (CPU/RAM)  
Fehlkonfiguration  
Software (OS/Applik.)  
Interner Firewall  
Interne Security SW (AV)  
Bediener Fehler

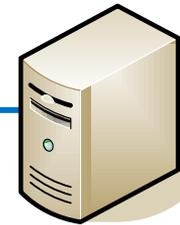


Netzwerk



Überlast (CPU/RAM)  
Fehlkonfiguration  
Software (FW/OS)  
Bandbreiten  
---  
LAN, WLAN, WAN, ISP  
---  
Lange Laufzeit  
Paketverlust  
Session Abbruch

Server



Überlast (CPU/RAM)  
Fehlkonfiguration  
Software (OS/Applik.)  
Interner Firewall  
Interne Security SW (AV)  
Services DNS/DHCP usw.



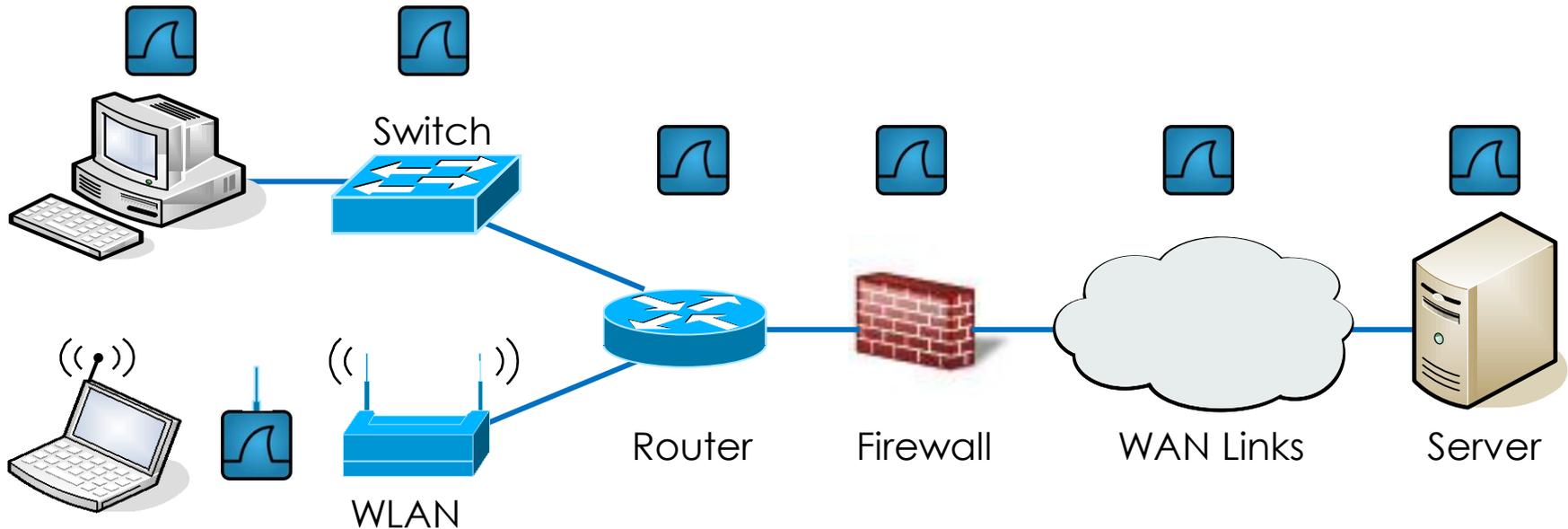
+

# Wireshark Packet Analyser



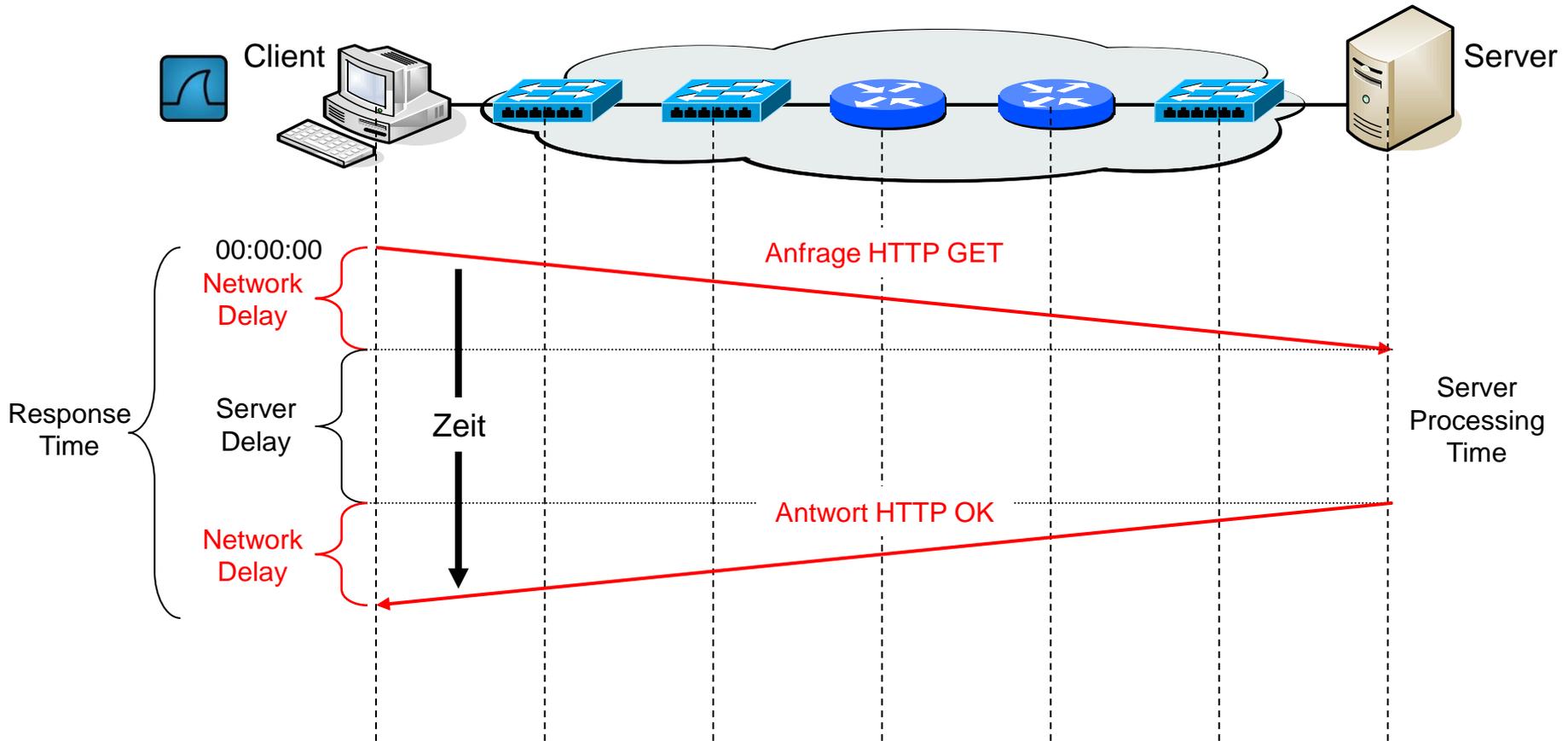
- Der am meisten eingesetzte Protocol Analyser weltweit
- **Open-Source Software**, d.h. kostenlos einsetzbar, privat oder kommerziell
- Decodiert gegen 1'000 verschiedene Netzwerk-Protokolle
- Unterstützt von allen gängigen Betriebssystemen: **Windows, Unix, Linux, MAC...**
- Download von [www.wireshark.org](http://www.wireshark.org)
- In 5 Minuten installiert, runterladen und installieren mit **default** Einstellungen
- Kann Tracefiles öffnen, welche mit **TCPdump** aufgezeichnet wurden

# Wireshark Packet Analyser



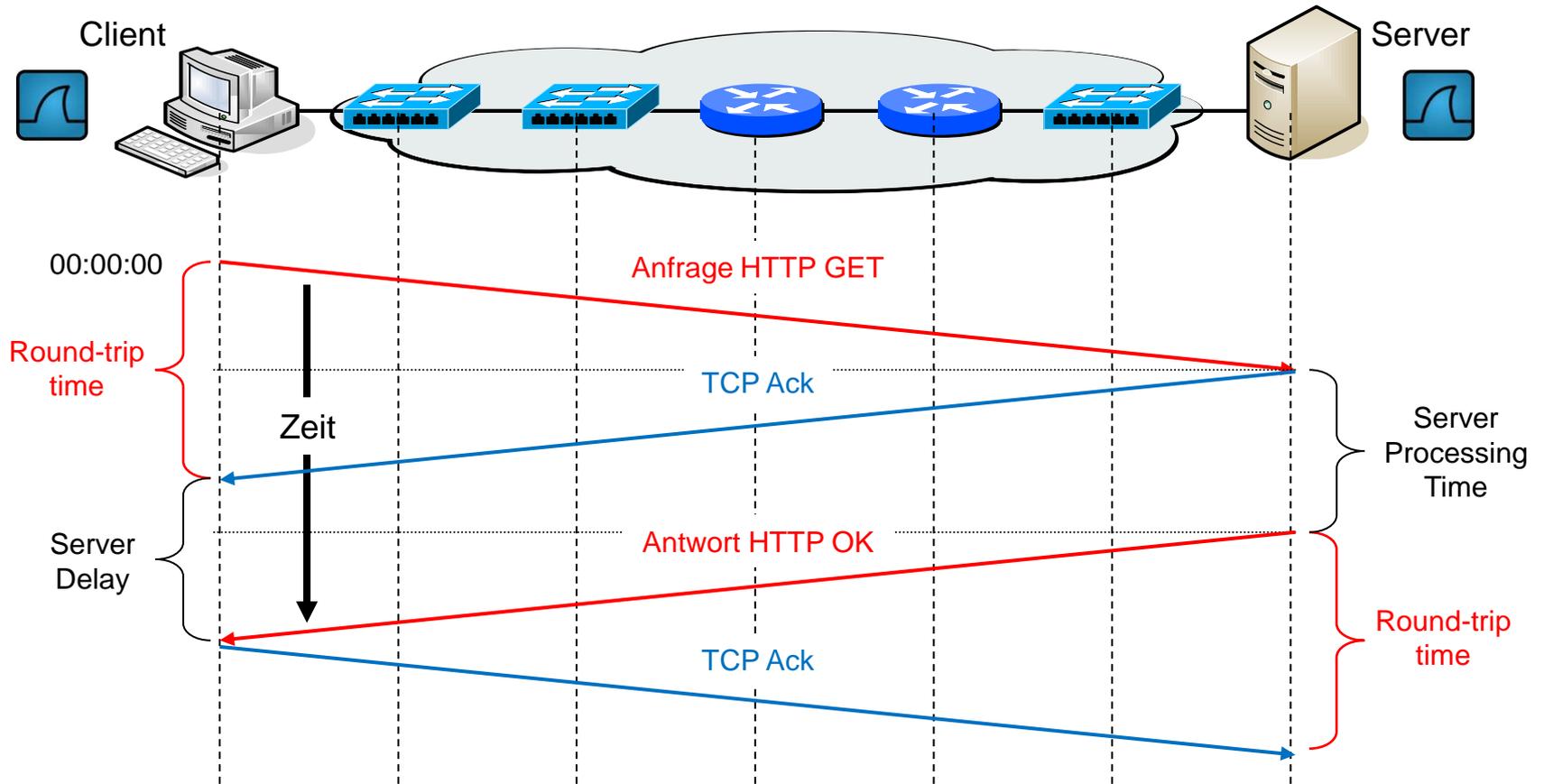
- Wireshark kann Daten an zahlreichen **Messpunkten** aufzeichnen
- Einige Netzwerkkomponenten haben **TCPdump** bereits **integriert**
- Der **Aufzeichnungsort** kann für die Analyse wichtig sein
- TCP Felder sind **end-to end** und können somit auf dem ganzen Datenpfad analysiert werden (good news)

# Einführung in die TCP Analyse

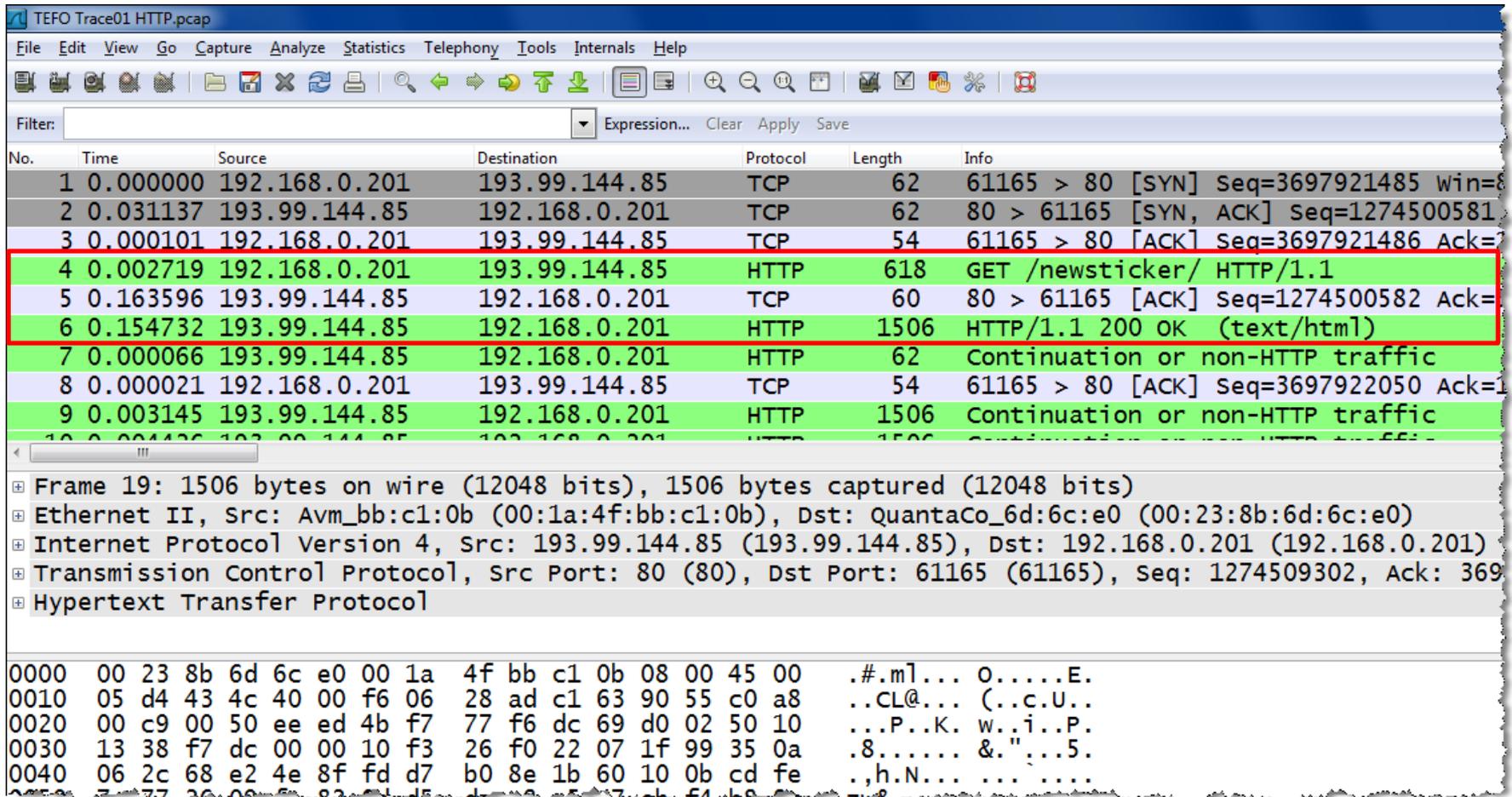


$$\text{Response Time} = 2 \times \text{Network Propagation Delay} + \text{Server Processing Time}$$

# Einführung in die TCP Analyse



# Einführung in die TCP Analyse



TEFO Trace01 HTTP.pcap

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.201	193.99.144.85	TCP	62	61165 > 80 [SYN] Seq=3697921485 win=8
2	0.031137	193.99.144.85	192.168.0.201	TCP	62	80 > 61165 [SYN, ACK] Seq=1274500581
3	0.000101	192.168.0.201	193.99.144.85	TCP	54	61165 > 80 [ACK] Seq=3697921486 Ack=7
4	0.002719	192.168.0.201	193.99.144.85	HTTP	618	GET /newsticker/ HTTP/1.1
5	0.163596	193.99.144.85	192.168.0.201	TCP	60	80 > 61165 [ACK] seq=1274500582 Ack=7
6	0.154732	193.99.144.85	192.168.0.201	HTTP	1506	HTTP/1.1 200 OK (text/html)
7	0.000066	193.99.144.85	192.168.0.201	HTTP	62	Continuation or non-HTTP traffic
8	0.000021	192.168.0.201	193.99.144.85	TCP	54	61165 > 80 [ACK] Seq=3697922050 Ack=1
9	0.003145	193.99.144.85	192.168.0.201	HTTP	1506	Continuation or non-HTTP traffic
10	0.004126	193.99.144.85	192.168.0.201	HTTP	1506	Continuation or non-HTTP traffic

Frame 19: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 bits)

- Ethernet II, Src: Avm\_bb:c1:0b (00:1a:4f:bb:c1:0b), Dst: QuantaCo\_6d:6c:e0 (00:23:8b:6d:6c:e0)
- Internet Protocol Version 4, Src: 193.99.144.85 (193.99.144.85), Dst: 192.168.0.201 (192.168.0.201)
- Transmission Control Protocol, Src Port: 80 (80), Dst Port: 61165 (61165), Seq: 1274509302, Ack: 369
- Hypertext Transfer Protocol

```
0000 00 23 8b 6d 6c e0 00 1a 4f bb c1 0b 08 00 45 00  .#.m]... 0.....E.
0010 05 d4 43 4c 40 00 f6 06 28 ad c1 63 90 55 c0 a8  ..CL@... (.c.U..
0020 00 c9 00 50 ee ed 4b f7 77 f6 dc 69 d0 02 50 10  ...P..K. w..i..P.
0030 13 38 f7 dc 00 00 10 f3 26 f0 22 07 1f 99 35 0a  .8..... &."...5.
0040 06 2c 68 e2 4e 8f fd d7 b0 8e 1b 60 10 0b cd fe  .,h.N... ... ..
0050 77 77 2c 09 5f 83 51 d5 d1 09 57 7c b4 b8 00 77 8
```

## Fehlersuche Fall 1 : Session Hang-Up



**Betriebswichtige** Anwendung zur Personalplanung in einem Spital:

- Der Bildschirm **blockiert** mitten in der Anwendung
- Probleme nur im **WLAN**, Clients am Ethernet funktionieren einwandfrei
- Alle anderen Anwendungen funktionieren einwandfrei über **WLAN**
- Dadurch fühlt sich der Lieferant des **WLAN** nicht zuständig
- Der Lieferant der Anwendung bietet keine Unterstützung, die Software sei **‚nicht WLAN fähig‘**

# Fehlersuche Fall 1 : Session Hang-Up

No.	Time	Source	Destination	Protocol	Length	Info
8403	0.000002		d0:c2:82:06:04:41	802.11	40	Acknowledgement, Flags=.....C
8404	0.006002	192.168.212.80	192.168.201.74	TNS	135	Request, Data (6), Data
8405	0.000001		00:19:d2:8f:57:a1	802.11	40	Acknowledgement, Flags=.....C
8406	0.000010	192.168.201.74	192.168.212.80	TNS	131	Response, Data (6), Data
8407	0.000001		d0:c2:82:06:04:41	802.11	40	Acknowledgement, Flags=.....C
8408	0.004892	192.168.212.80	192.168.201.74	TNS	135	Request, Data (6), Data
8409	0.000001		00:19:d2:8f:57:a1	802.11	40	Acknowledgement, Flags=.....C
8410	0.000011	192.168.201.74	192.168.212.80	TNS	134	Response, Data (6), Data
8411	0.000000		d0:c2:82:06:04:41	802.11	40	Acknowledgement, Flags=.....C
8412	0.001034	192.168.212.80	192.168.201.74	TNS	1497	Request, Data (6), Data
8413	0.000001		00:19:d2:8f:57:a1	802.11	40	Acknowledgement, Flags=.....C
8414	0.000455	192.168.201.74	192.168.212.80	TNS	172	[TCP ACKed lost segment] Response
8415	0.000002		d0:c2:82:06:04:41	802.11	40	Acknowledgement, Flags=.....C
8416	0.000122	192.168.212.80	192.168.201.74	TCP	120	[TCP Keep-Alive] bbn-mmx > ncube-
8417	0.000001		00:19:d2:8f:57:a1	802.11	40	Acknowledgement, Flags=.....C
8418	0.000339	192.168.201.74	192.168.212.80	TCP	126	[TCP Keep-Alive ACK] ncube-1m > b
8419	0.000000		d0:c2:82:06:04:41	802.11	40	Acknowledgement, Flags=.....C
8425	0.000018		d0:c2:82:06:04:41	802.11	40	Acknowledgement, Flags=.....C
8434	0.039896	192.168.212.80	192.168.201.74	TNS	1497	[TCP Retransmission] Request, Dat

# Fehlersuche Fall 1 : Session Hang-Up

Eingrenzung der Fehlerquellen

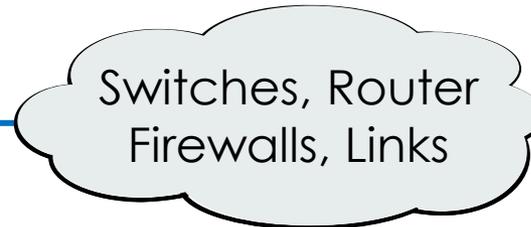
Workstation



Überlast (CPU/RAM)  
Fehlkonfiguration  
Software (OS/Applik.)  
Interner Firewall  
Interne Security SW (AV)  
Bediener Fehler



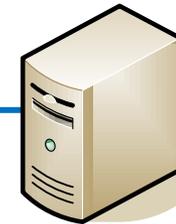
Netzwerk



Überlast (CPU/RAM)  
Fehlkonfiguration  
Software (FW/OS)  
Bandbreiten  
---  
LAN, WLAN, WAN, ISP  
---

Lange Laufzeit  
Paketverlust  
Session Abbruch

Server

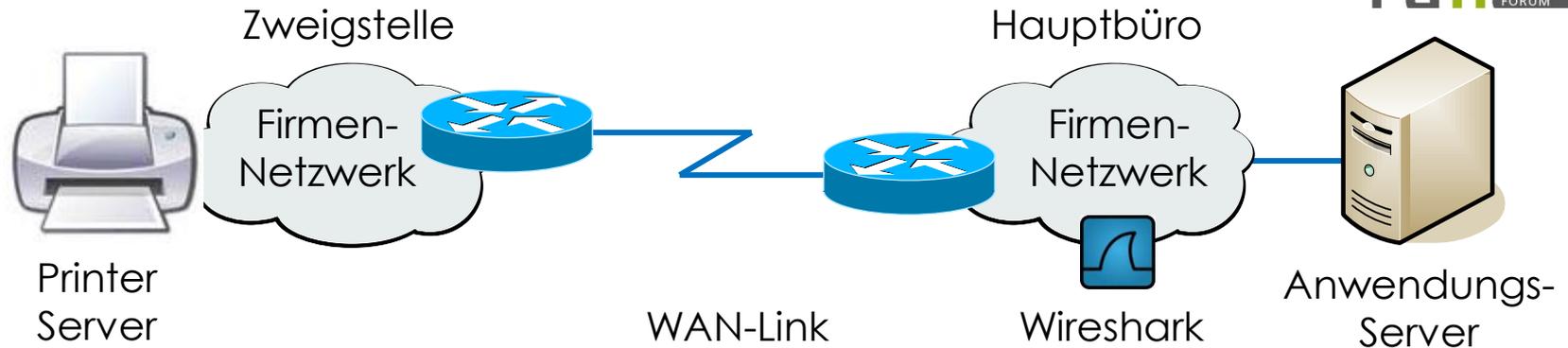


Überlast (CPU/RAM)  
Fehlkonfiguration  
Software (OS/Applik.)  
Interner Firewall  
Interne Security SW (AV)  
Services DNS/DHCP usw.



+

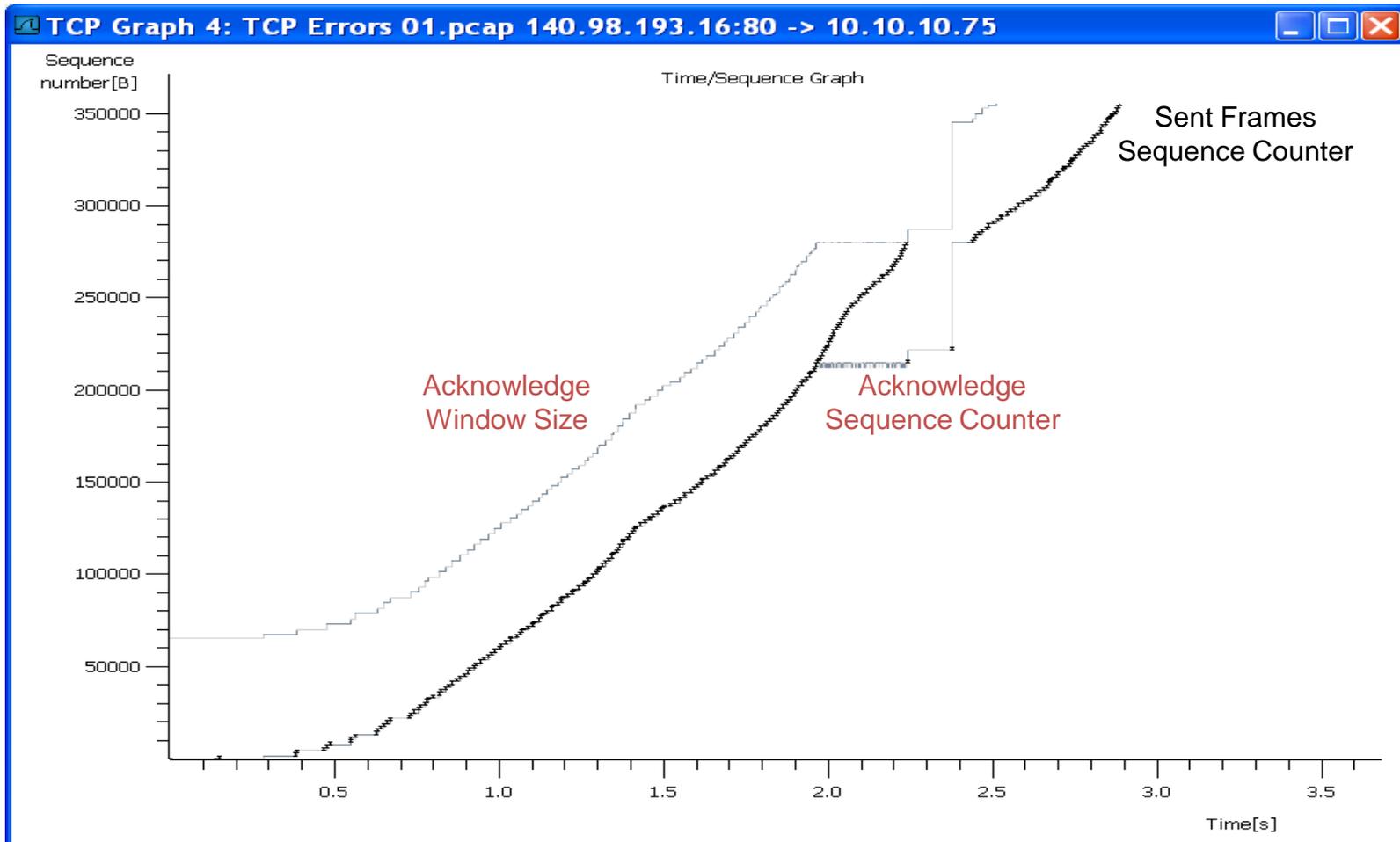
## Fehlersuche Fall 2 : Slow Printing



Handelsfirma mit Hauptbüro und Zweigstellen angebunden über **WAN**

- Warenlieferungen von Zweigstellen, **dezentraler Druck** von Lieferscheinen
- Der Ausdruck von Lieferpapieren dauert Minuten und **verzögert Abläufe**
- Die Druckjobs werden vom zentralen **SAP Server** zur Zweigstelle geschickt
- Vermutet wird ein **Bandbreite-Problem** im WAN
- WAN Bandbreite wurde bereits auf 1Mbps verdoppelt, **ohne Erfolg!**
- Situation dauert schon **Monate**

# Fehlersuche Fall 2 : Slow Printing



# Fehlersuche Fall 2 : Slow Printing

Eingrenzung der Fehlerquellen

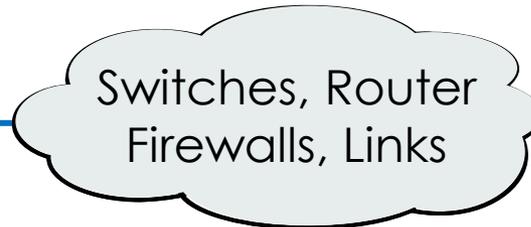
Workstation



Überlast (CPU/RAM)  
Fehlkonfiguration  
Software (OS/Applik.)  
Interner Firewall  
Interne Security SW (AV)  
Bediener Fehler

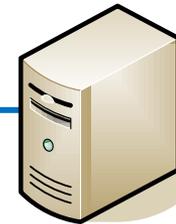


Netzwerk



Überlast (CPU/RAM)  
Fehlkonfiguration  
Software (FW/OS)  
Bandbreiten  
---  
LAN, WLAN, WAN, ISP  
---  
Lange Laufzeit  
Paketverlust  
Session Abbruch

Server

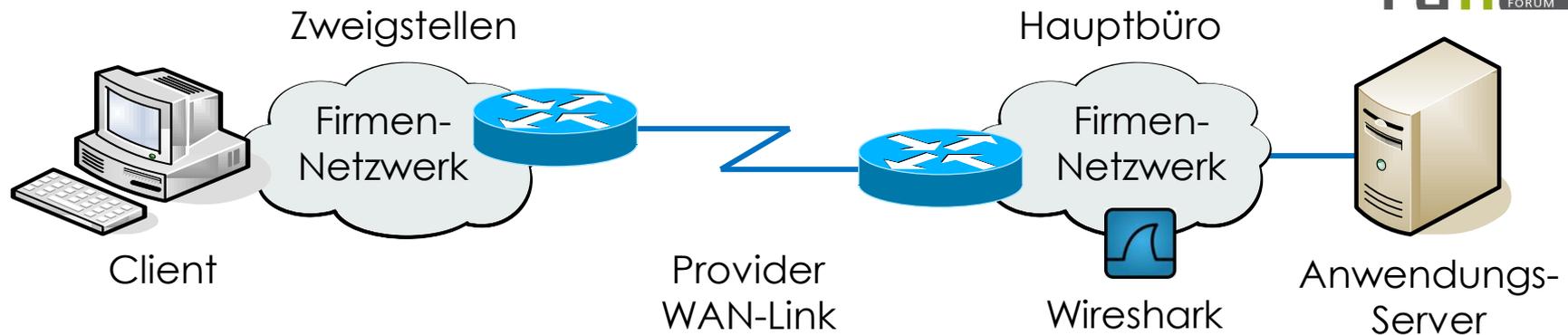


Überlast (CPU/RAM)  
Fehlkonfiguration  
Software (OS/Applik.)  
Interner Firewall  
Interne Security SW (AV)  
Services DNS/DHCP usw.



+

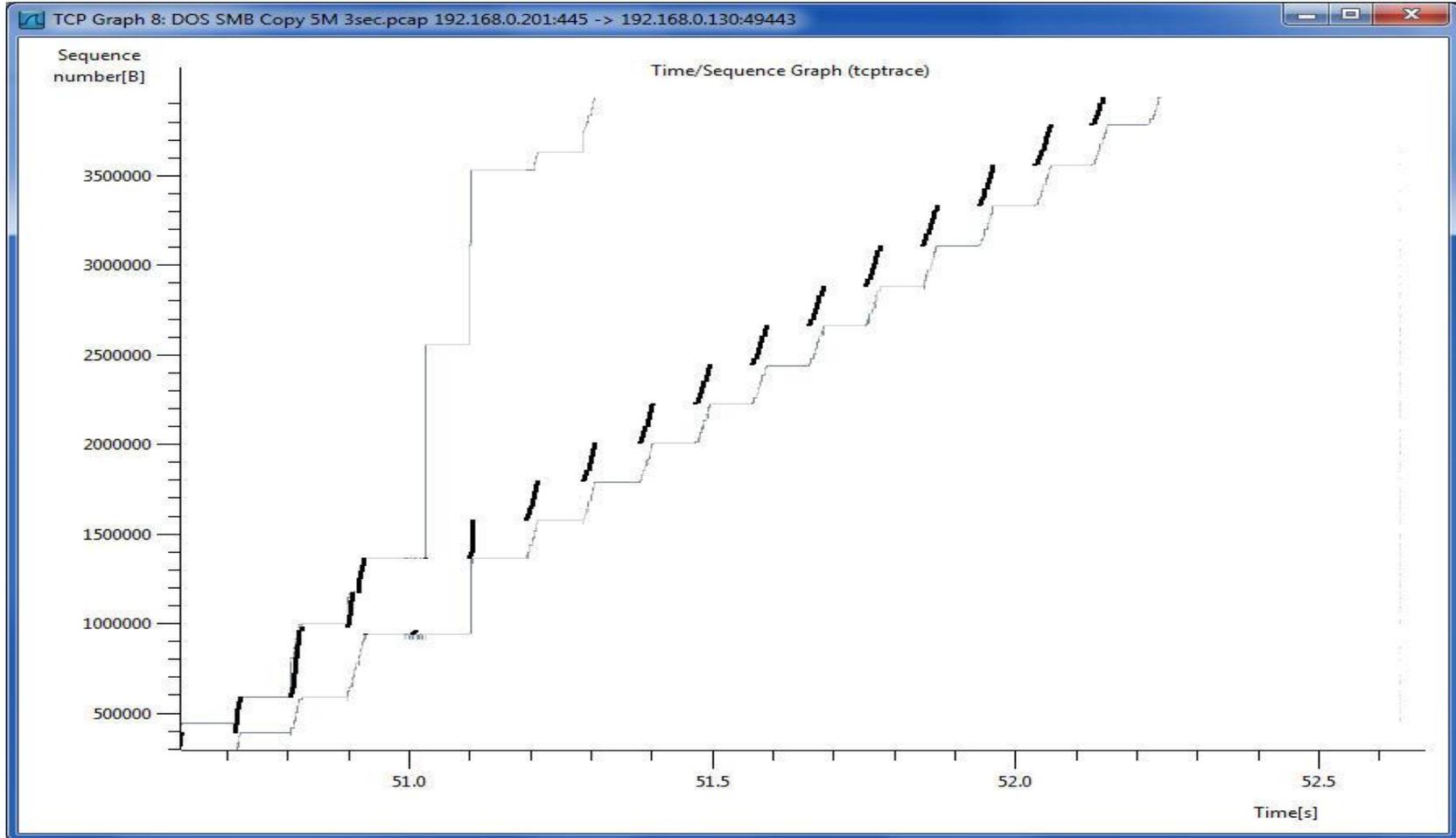
## Fehlersuche Fall 3 : Bad WAN Throughput



Grosse schweizerische Herstellerfirma mit [weltweiten Niederlassungen](#)

- Niederlassungen sind über [WAN-Provider](#) mit [45Mbps](#) Links angeschlossen
- Die Links werden für regelmässige [Softwareupdates](#) der Clients verwendet.
- Die Übertragung [dauert zu lange](#), kann über Nacht nicht beendet werden
- Grobe Berechnungen ergeben eine Durchsatz von nur [1Mbps](#)
- Der Kunde vermutet [Daten-Drosselung](#) durch den WAN-Provider

# Fehlersuche Fall 3 : Bad WAN Throughput



# Fehlersuche Fall 3 : Bad WAN Throughput

Eingrenzung der Fehlerquellen

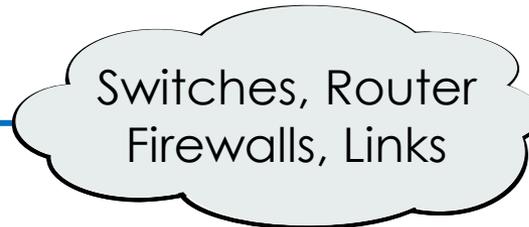
Workstation



Überlast (CPU/RAM)  
Fehlkonfiguration  
Software (OS/Applik.)  
Interner Firewall  
Interne Security SW (AV)  
Bediener Fehler

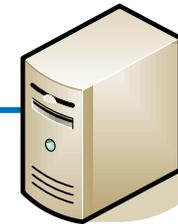


Netzwerk



Überlast (CPU/RAM)  
Fehlkonfiguration  
Software (FW/OS)  
Bandbreiten  
---  
LAN, WLAN, WAN, ISP  
---  
Lange Laufzeit  
Paketverlust  
Session Abbruch

Server



Überlast (CPU/RAM)  
**Fehlkonfiguration**  
Software (OS/Applik.)  
Interner Firewall  
Interne Security SW (AV)  
Services DNS/DHCP usw.



+

# Danke für Ihre Aufmerksamkeit



Gerne begrüßen wir Sie an einem Kurs von Leutert NetServices

Grundkurse bei Studerus:

- **NET-Analyse** mit Wireshark
- **IPv6-Protokoll** Einführung

LAB-Kurse bei HSR  
(Hochschule Rapperswil)

- **TCP/IP Protokoll**
- **WLAN Analyse**
- **IPv6 Praxisworkshop**



Registrieren sie sich für den technischen Newsletter [www.wireshark.ch](http://www.wireshark.ch)