

Netztechnik I

TINF

Wireshark Trace Analyse

Markus Götzl
Dipl.-Inform. (FH)
mail@markusgoetzl.de

Wireshark

- ▶ Wireshark Ressourcen
- ▶ Mitschnitt (Trace) erzeugen
- ▶ Trace Analyse

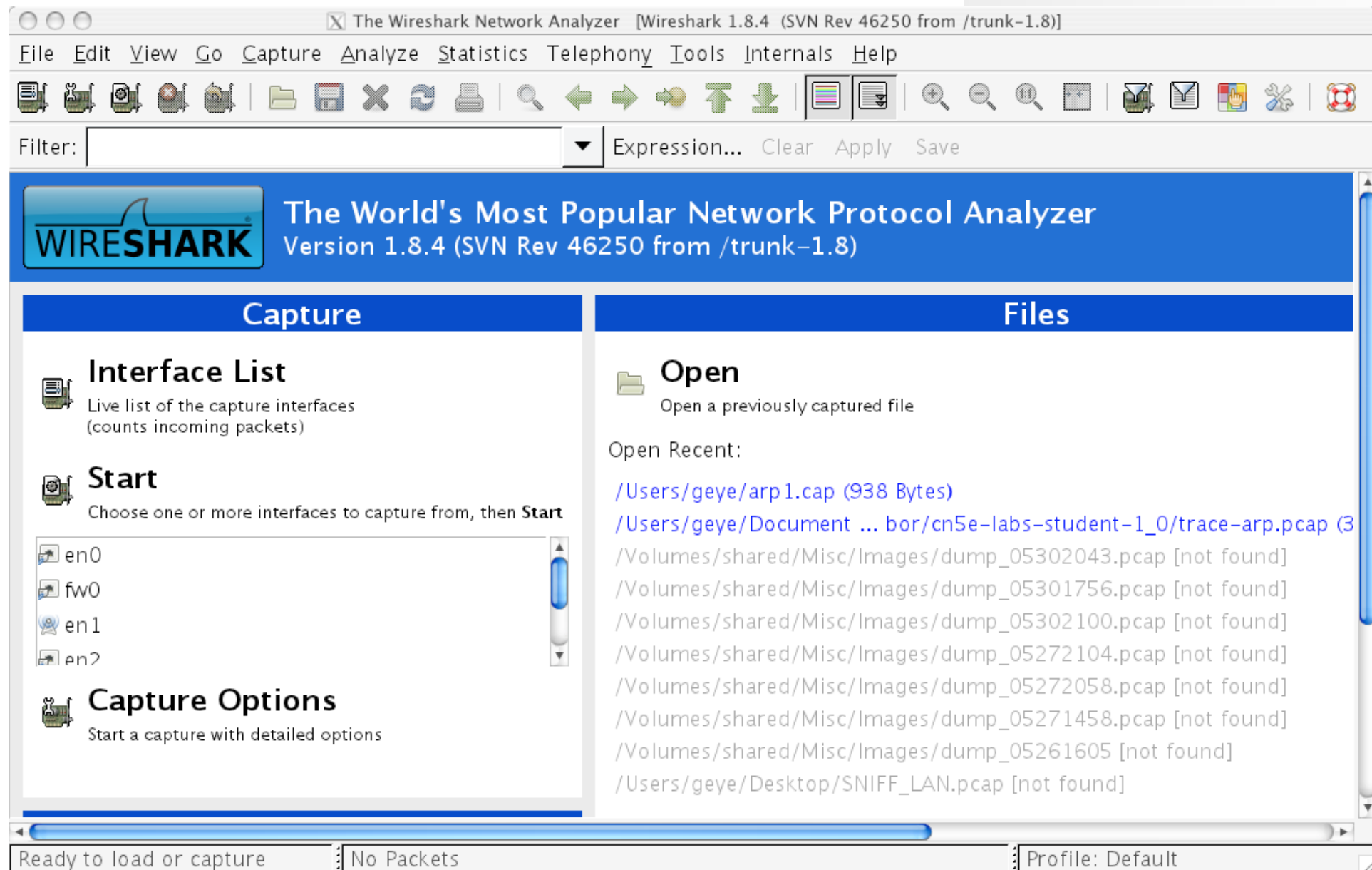
- ▶ Wireshark Homepage:
 - <http://www.wireshark.org>
- ▶ Wireshark Downloads:
 - <http://www.wireshark.org/download.html>
- ▶ Wireshark Dokumentation
 - <http://www.wireshark.org/docs/>

Finden des Netzwerk-Interfaces und des Gateways

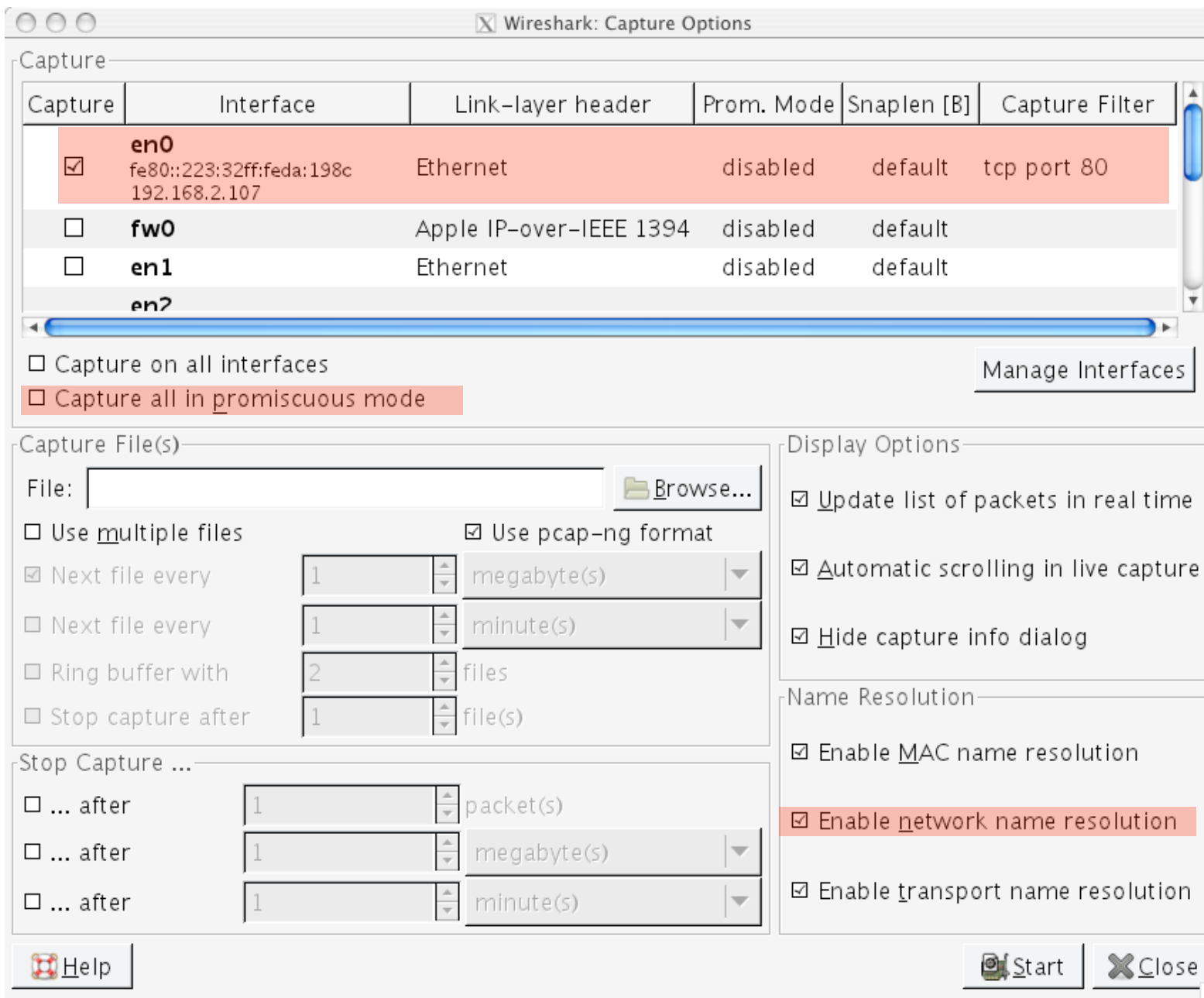
```
Themis:~ root# route -n get default
route to: default
destination: default
mask: default
gateway: 192.168.2.1
interface: en0
```

- ▶ Linux: route
- ▶ Windows: route print
- ▶ Mac: route -n get default

Wireshark starten



Einen Trace erstellen mit Filter "TCP Port 80"



The image shows the 'Wireshark: Capture Options' dialog box. The 'Capture' section has a table with the following data:

Capture	Interface	Link-layer header	Prom. Mode	Snaplen [B]	Capture Filter
<input checked="" type="checkbox"/>	en0 fe80::223:32ff:feda:198c 192.168.2.107	Ethernet	disabled	default	tcp port 80
<input type="checkbox"/>	fw0	Apple IP-over-IEEE 1394	disabled	default	
<input type="checkbox"/>	en1	Ethernet	disabled	default	
	en2				

Below the table, there are checkboxes for 'Capture on all interfaces' (unchecked) and 'Capture all in promiscuous mode' (checked). A 'Manage Interfaces' button is to the right.

The 'Capture File(s)' section includes a 'File:' field with a 'Browse...' button, and checkboxes for 'Use multiple files' (unchecked), 'Use pcap-ng format' (checked), 'Next file every' (1 megabyte(s)), 'Next file every' (1 minute(s)), 'Ring buffer with' (2 files), and 'Stop capture after' (1 file(s)).

The 'Stop Capture ...' section has three rows, each with a checkbox and a time/size selection: '... after' (1 packet(s)), '... after' (1 megabyte(s)), and '... after' (1 minute(s)).

The 'Display Options' section has checkboxes for 'Update list of packets in real time' (checked), 'Automatic scrolling in live capture' (checked), and 'Hide capture info dialog' (checked).

The 'Name Resolution' section has checkboxes for 'Enable MAC name resolution' (checked), 'Enable network name resolution' (checked), and 'Enable transport name resolution' (checked).

At the bottom, there are 'Help', 'Start', and 'Close' buttons.

► Capture - Options:

- Interface wählen
- "Capture all in promiscuous mode" abwählen
- Filter: tcp port 80
- "Enable network name resolution" wählen

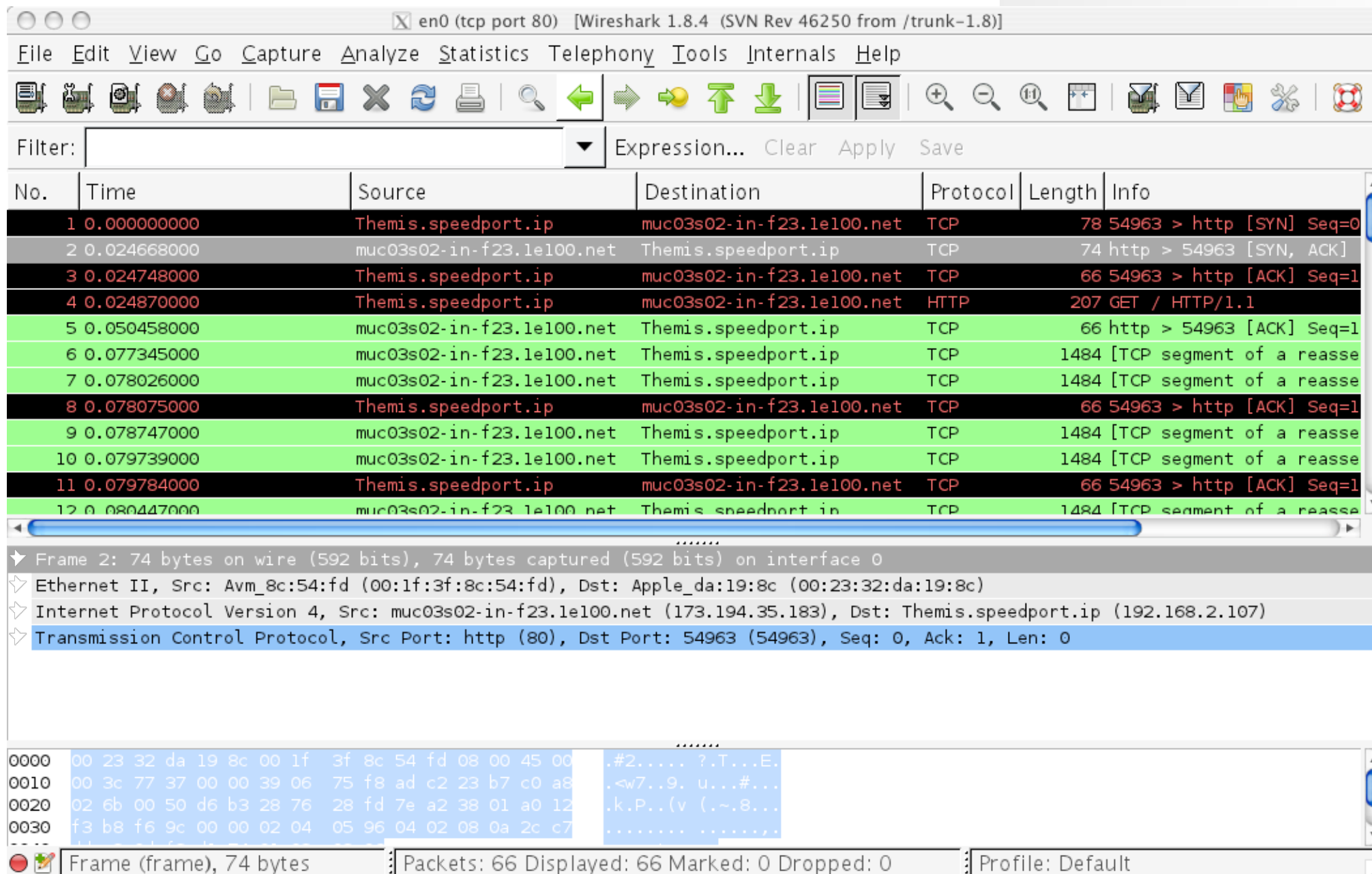
http Request:

```
Themis:~ geye$ curl www.google.de
```

```
<!doctype html><html itemscope="itemscope" itemtype="http://schema.org/WebPage">
<head><meta itemprop="image" content="/images/google_favicon_128.png"><title>Goo
gle</title><script>(function(){
window.google={kEI:"0wFAU0DhDIOctQbQxIDoDg",getEI:function(a){for(var b;a&&(!a.g
etAttribute||!(b=a.getAttribute("eid")));)a=a.parentNode;return b||google.kEI},h
ttps:function(){return"https:"+(window.location.protocol.indexOf("https:")>0?"":
"https://")+(window.location.protocol=="https:"?"":window.location.protocol+"//")
+window.location.hostname+(window.location.port?" ":"")+window.location.pathname+
window.location.search+window.location.hash}};})();
```

- ▶ http Request mit curl oder wget

Erstellter Trace



en0 (tcp port 80) [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	Themis.speedport.ip	muc03s02-in-f23.1e100.net	TCP	78	54963 > http [SYN] Seq=0
2	0.024668000	muc03s02-in-f23.1e100.net	Themis.speedport.ip	TCP	74	http > 54963 [SYN, ACK]
3	0.024748000	Themis.speedport.ip	muc03s02-in-f23.1e100.net	TCP	66	54963 > http [ACK] Seq=1
4	0.024870000	Themis.speedport.ip	muc03s02-in-f23.1e100.net	HTTP	207	GET / HTTP/1.1
5	0.050458000	muc03s02-in-f23.1e100.net	Themis.speedport.ip	TCP	66	http > 54963 [ACK] Seq=1
6	0.077345000	muc03s02-in-f23.1e100.net	Themis.speedport.ip	TCP	1484	[TCP segment of a reasse
7	0.078026000	muc03s02-in-f23.1e100.net	Themis.speedport.ip	TCP	1484	[TCP segment of a reasse
8	0.078075000	Themis.speedport.ip	muc03s02-in-f23.1e100.net	TCP	66	54963 > http [ACK] Seq=1
9	0.078747000	muc03s02-in-f23.1e100.net	Themis.speedport.ip	TCP	1484	[TCP segment of a reasse
10	0.079739000	muc03s02-in-f23.1e100.net	Themis.speedport.ip	TCP	1484	[TCP segment of a reasse
11	0.079784000	Themis.speedport.ip	muc03s02-in-f23.1e100.net	TCP	66	54963 > http [ACK] Seq=1
12	0.080447000	muc03s02-in-f23.1e100.net	Themis.speedport.ip	TCP	1484	[TCP segment of a reasse

Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

- Ethernet II, Src: Avn_8c:54:fd (00:1f:3f:8c:54:fd), Dst: Apple_da:19:8c (00:23:32:da:19:8c)
- Internet Protocol Version 4, Src: muc03s02-in-f23.1e100.net (173.194.35.183), Dst: Themis.speedport.ip (192.168.2.107)
- Transmission Control Protocol, Src Port: http (80), Dst Port: 54963 (54963), Seq: 0, Ack: 1, Len: 0

0000 00 23 32 da 19 8c 00 1f 3f 8c 54 fd 08 00 45 00 .#2....?.T...E.

0010 00 3c 77 37 00 00 39 06 75 f8 ad c2 23 b7 c0 a8 .<w7..9. u...#...

0020 02 6b 00 50 d6 b3 28 76 28 fd 7e a2 38 01 a0 12 .k.P..(v (~.8...

0030 f3 b8 f6 9c 00 00 02 04 05 96 04 02 08 0a 2c c7

Frame (frame), 74 bytes | Packets: 66 Displayed: 66 Marked: 0 Dropped: 0 | Profile: Default

Wireshark GUI

ProtocolLayers.pcap [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	Themis.speedport.ip	muc03s02-in-f23.1e100.net	TCP	78	54963 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1
2	0.024668000	muc03s02-in-f23.1e100.net	Themis.speedport.ip	TCP	74	http > 54963 [SYN, ACK] Seq=0 Ack=1 Win=62392
3	0.024748000	Themis.speedport.ip	muc03s02-in-f23.1e100.net	TCP	66	54963 > http [ACK] Seq=1 Ack=1 Win=524280 Len=
4	0.024870000	Themis.speedport.ip	muc03s02-in-f23.1e100.net	HTTP	26	GET / HTTP/1.1
5	0.050458000	muc03s02-in-f23.1e100.net	Themis.speedport.ip	TCP	66	http > 54963 [ACK] Seq=1 Ack=142 Win=63488 Len=
6	0.077345000	muc03s02-in-f23.1e100.net	Themis.speedport.ip	TCP	1484	[TCP segment of a reassembled PDU]
7	0.078026000	muc03s02-in-f23.1e100.net	Themis.speedport.ip	TCP	1484	[TCP segment of a reassembled PDU]
8	0.078075000	Themis.speedport.ip	muc03s02-in-f23.1e100.net	TCP	66	54963 > http [ACK] Seq=142 Ack=2837 Win=523240
9	0.078747000	muc03s02-in-f23.1e100.net	Themis.speedport.ip	TCP	1484	[TCP segment of a reassembled PDU]
10	0.079739000	muc03s02-in-f23.1e100.net	Themis.speedport.ip	TCP	1484	[TCP segment of a reassembled PDU]
11	0.079784000	Themis.speedport.ip	muc03s02-in-f23.1e100.net	TCP	66	54963 > http [ACK] Seq=142 Ack=5673 Win=523240
12	0.080447000	muc03s02-in-f23.1e100.net	Themis.speedport.ip	TCP	1484	[TCP segment of a reassembled PDU]

Frame 4: 207 bytes on wire (1656 bits), 207 bytes captured (1656 bits) on interface 0

Ethernet II, Src: Apple_da:19:8c (00:23:32:da:19:8c), Dst: Avm_8c:54:fd (00:1f:3f:8c:54:fd)

Internet Protocol Version 4, Src: Themis.speedport.ip (192.168.2.107), Dst: muc03s02-in-f23.1e100.net (173.194.35.183)

Transmission Control Protocol, Src Port: 54963 (54963), Dst Port: http (80), Seq: 1, Ack: 1, Len: 141

Hypertext Transfer Protocol

0000 00 1f 3f 8c 54 fd 00 23 32 da 19 8c 08 00 45 00 ..?.T..# 2....E.
 0010 00 c1 73 d4 40 00 40 06 00 00 c0 a8 02 6b ad c2 ..s.@.@.k..
 0020 23 b7 d6 b3 00 50 7e a2 38 01 28 76 28 fe 80 18 #....P~. 8.(v(...
 0030 ff ff 95 40 00 01 01 08 0a 0d f2 d1 74 2c c7 ...@....t..

Internet Protocol Version 4 (... | Packets: 66 Displayed: 66 Marked: 0 Load time: 0:00.262 | Profile: Default

HTTP "GET" Paket

Wireshark "Blocks"
Bei "Frame" handelt es
sich um das gesamte
"Paket"

Inhalt eines "Paketes"
HEX und ASCII

1. Protokollschichten

- ▶ Finden Sie das HTTP “GET” Paket.
- ▶ Untersuchen Sie das Paket mit Hilfe der “Blocks” um die verwendeten Protokolle zu identifizieren.
- Hierzu kann folgendes Diagramm verwendet werden:



2. Fragmente

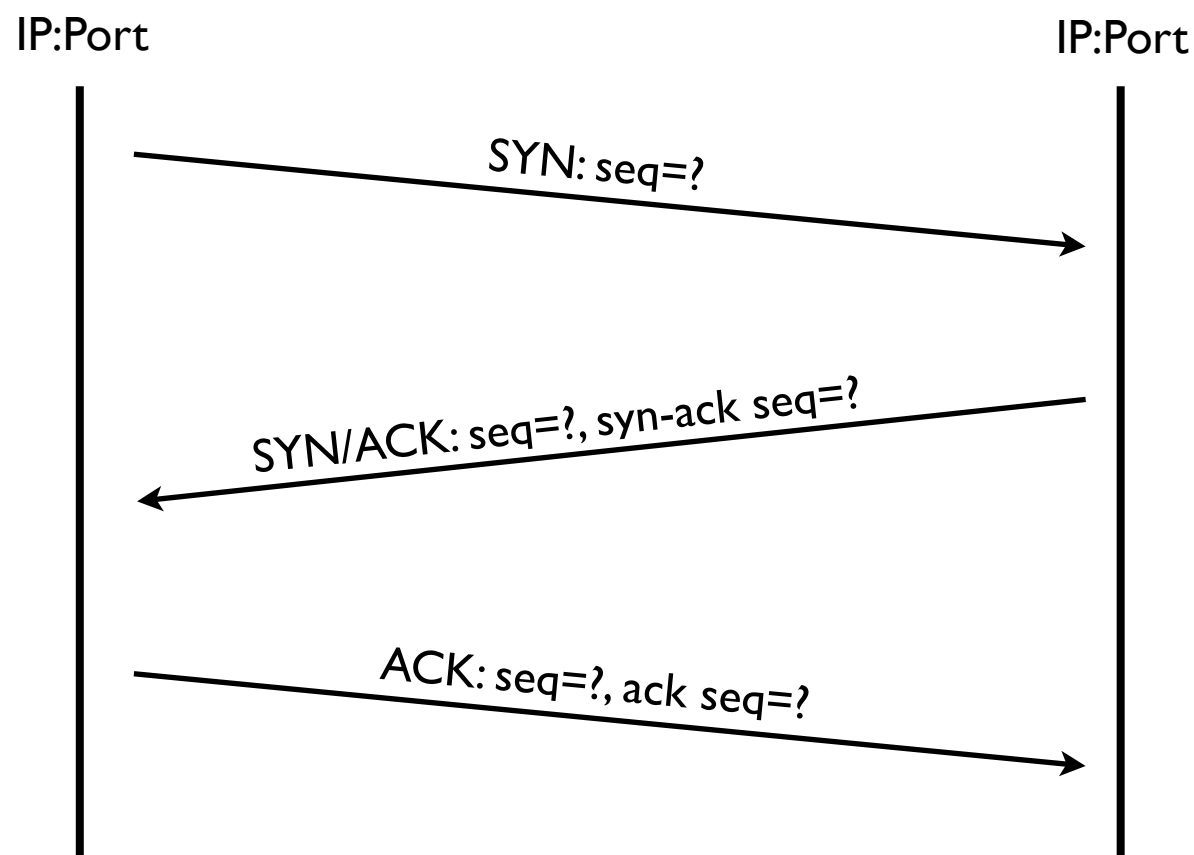
- ▶ Finden Sie das HTTP Antwort Paket (“200 OK”).
- ▶ Ist das Paket fragmentiert?
- ▶ Wenn es Fragmente gibt wie viele Fragmente sind es (Welche?)?
- ▶ Wenn es Fragmente gibt wie groß sind die Fragmente?
- ▶ Welcher Inhalt findet sich unter dem Block “Line-based text data:” im HTTP Antwort Paket (“200 OK”)

3. Protokolle

- ▶ Welche Ports (Server und Client) waren bei der Kommunikation beteiligt?
- ▶ Welche Hosts (+ deren IP Adresse) waren bei der Kommunikation beteiligt?
- ▶ Welche Netzwerkadressen (MAC-Adressen) sind beteiligt? Können diese den IP Adressen zugeordnet werden?
- ▶ Welches Transportprotokoll wurde benutzt? Woran können Sie das auf IP Ebene erkennen?
- ▶ Welches Vermittlungsprotokoll wurde benutzt? Woran können Sie das auf Ethernet Ebene erkennen?

4. TCP Verbindungsaufbau

- ▶ Finden Sie die TCP Control Segmente für den Verbindungsaufbau. Wie können Sie diese Segmente identifizieren?
- ▶ Tragen Sie die Sequenznummern Ihres Verbindungsaufbaus in das Diagramm ein.



Bemerkung: Wireshark rechnet die Angezeigten Sequenznummern relativ zu den Basis-Sequenznummern um. Die “echten” Sequenznummern können mit:

Edit->Preferences->Protocols-TCP

angezeigt werden.

Hierzu muss

“Analyse TCP sequence numbers”
und
“Relative sequence numbers”
abgewählt werden.