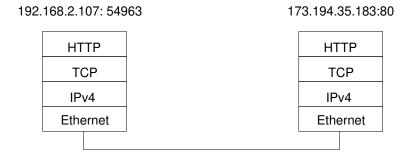
Lösung Wireshark Übung: Trace Analyse

1. Protokollschichten

Das "HTTP GET" Paket kann mit dem Display-Filter: http.request == TRUE gefunden werden. Folgende Protokolle können für die einzelnen Schichten identifiziert werden:



2. Fragmente

Das HTTP Antwortpaket kann mit dem Display-Filter: http.response == TRUE gefunden werden.

• Zu sehen sind die TCP Segmente welche der MSS (Maximum Segment Size), in Abhängigkeit zur MTU (Maximum Transfer Unit) entsprechen. Da als Sicherungsschichtprotokoll Ethernet eingesetzt wurde ist die MTU 1500 bytes. Die entsprechende MSS wird im ersten TCP SYN Paket (Options Feld) für die Verbindung gesetzt. Im vorliegenden Fall 1460 bytes (1500 – 20(IP Header) – 20(TCP Header)) In vielen Fällen wird allerdings eine etwas kleinere Segmentgröße verwendet:

```
1484\ bytes\ on\ wire \Rightarrow -26bytes\ (Ethernet\ Header)

1458\ bytes - 20\ (IP\ Header)

1438\ bytes - 20\ (TCP\ Header)

1418\ bytes \Rightarrow HTTP\ payload
```

```
▶ Frame 9: 1484 bytes on wire (11872 bits), 1484 bytes captured (11872 bits) on interface 0
▶ Ethernet II, Src: Avm_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: 173.194.35.183 (173.194.35.183), Dst: 192.168.2.107 (192.168.2.107)
▶ Transmission Control Protocol, Src Port: http (80), Dst Port: 54963 (54963), Seq: 2837, Ack: 142, Len: 1418
```

- Insgesamt handelt es sich um 9 Segmente.
- Unter "Line Based text data" wird der Payload des HTTP Protokolls angezeigt.

3. Protokolle

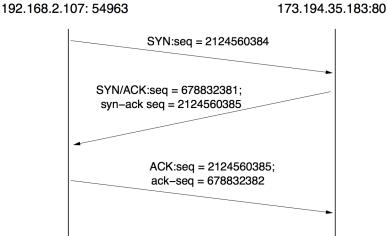
```
IP's und Port's im HTTP Request (#4): Source/Client: 192.168.2.107: 54963 Destination/Server: 173.194.35.183: 80 IP's und Port's im HTTP Reply (#17): Source/Server: 173.194.35.183: 80 Destination/Client: 192.168.2.107: 54963
```

Folgende MAC Adressen waren beteiligt: 00:23:32:da:19:8c und 00:1f:3f:8c:54:fd. Es lässt sich lediglich die IP Adresse des Clients (192.168.2.107) der MAC Adresse 00:23:32:da:19:8c zuorden die Mac Adresse 00:1f:3f:8c:54:fd ist die des lokalen NAT

Gateways (MAC/Schicht 2/Ethernet Adressierung ist lediglich lokal!) Als Vermittlungsprotokoll wurde TCP verwendet, dies wird im IP Header im Feld "Protocol" angezeigt (Demultiplexing Key) Als Netzwerkprotokoll wurde IPv4 verwendet, dies wird im Ethernet Header im Feld "Type" angezeigt (Demultiplexing Key)

4. TCP Verbindungsaufbau

Die Control Segmente befinden sich in den Frames: $\#1, \ \#2, \ und \ \#3$ zu erkennen am felenden Payload und an den TCP Header Flags SYN, SYN-ACK und ACK



3