WireShark Aufgabe

Aufgabe 1 & 2

➔ Einleitung

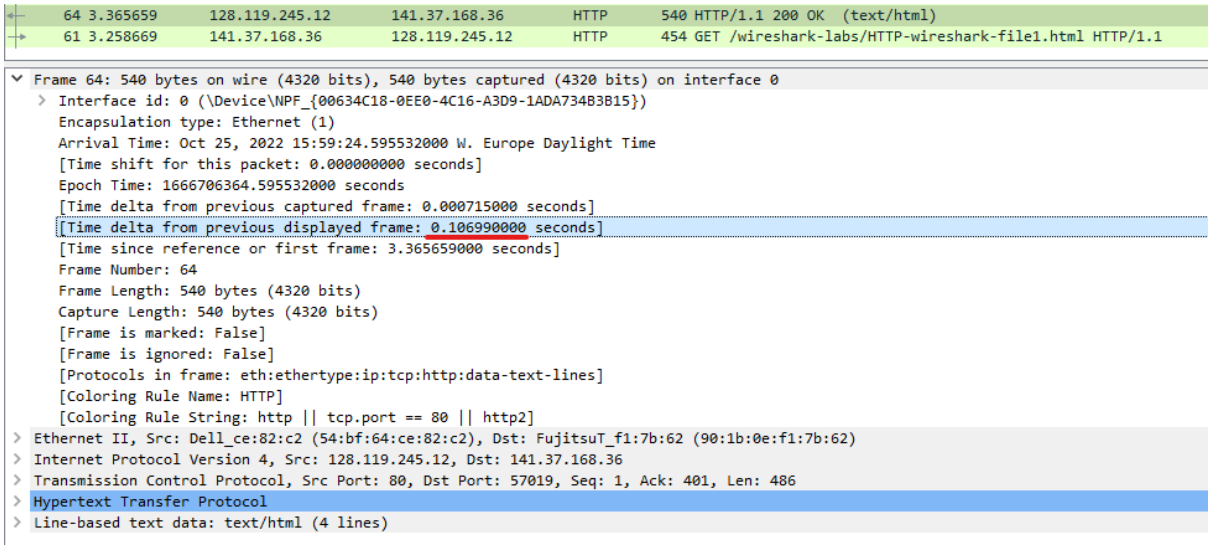
Aufgabe 3

1. Nennen Sie mindestens 5 Protokolle, die WireShark erkannt hat.

1. HHTP
2. TCP
3. DNS
4. TLS
5. ARP

2. Wie lange hat es vom Senden des HTTP Requests (hWp://gaia.cs.umass.edu/wireshark-labs/

INTRO-wireshark-file1.html) bis zum Erhalt der HTTP Response gedauert?

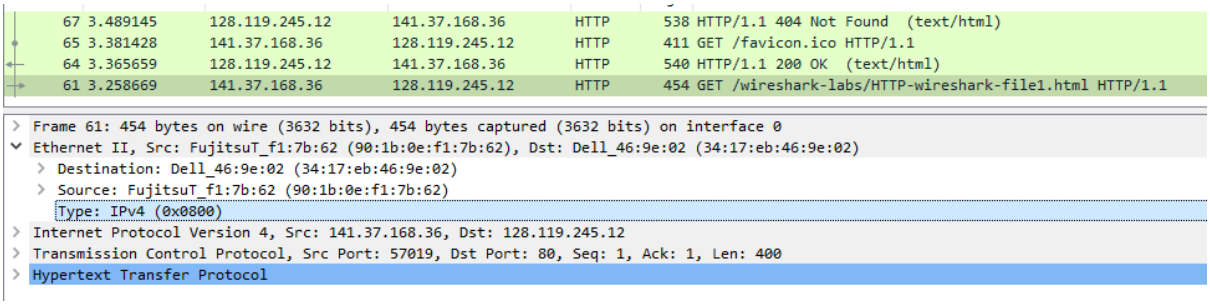


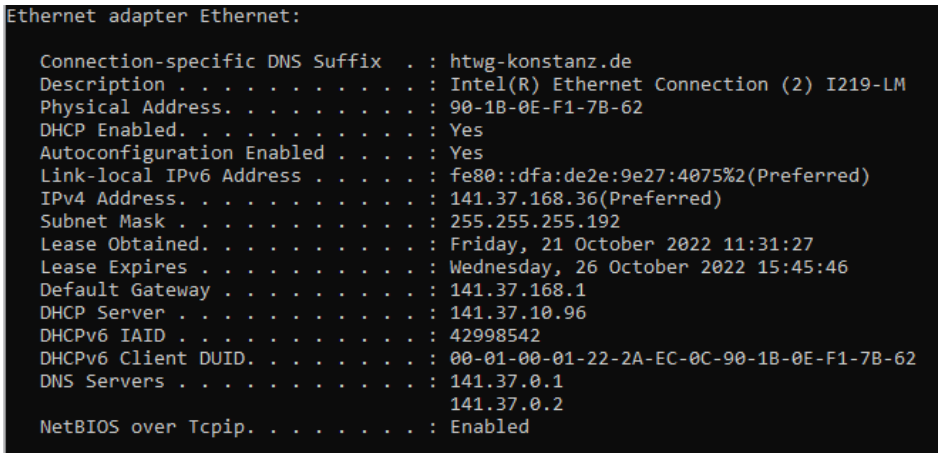
3. Was ist die Internet-Adresse ihres Rechners?
=> 141.37.168.36

Was ist die Ethernet-Adresse (MAC-Adresse,physikalische Adresse) ihres Rechners?
=> 90:1B:0E:F1:7B:62

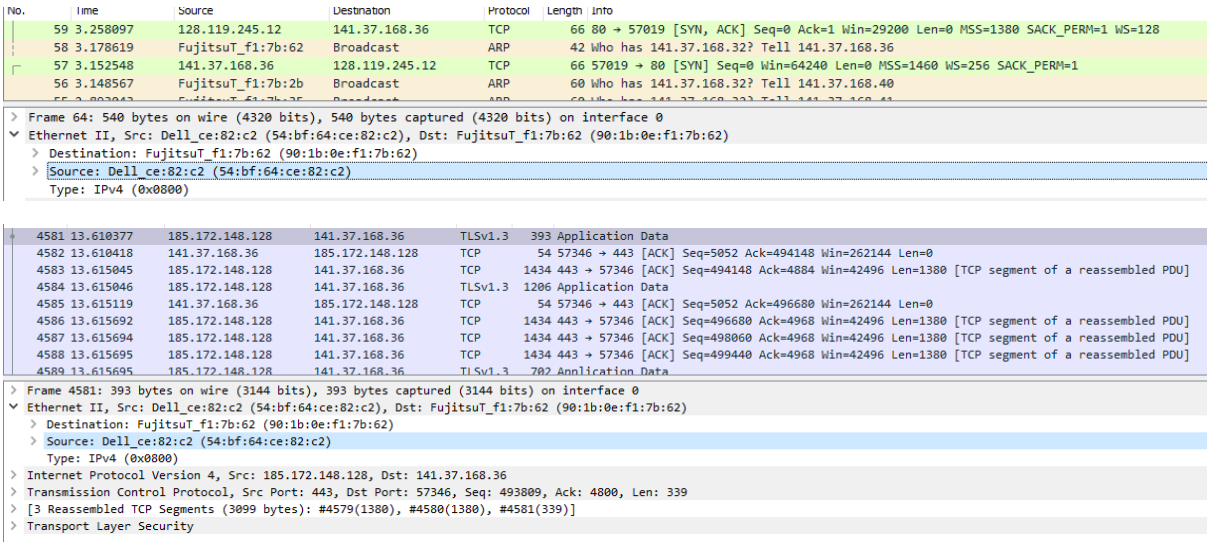
Welches ist die Ziel-MAC-Adresse, zu der ihr Rechner Pakete sendet?

⇨ 34:17:EB:46:9E:02



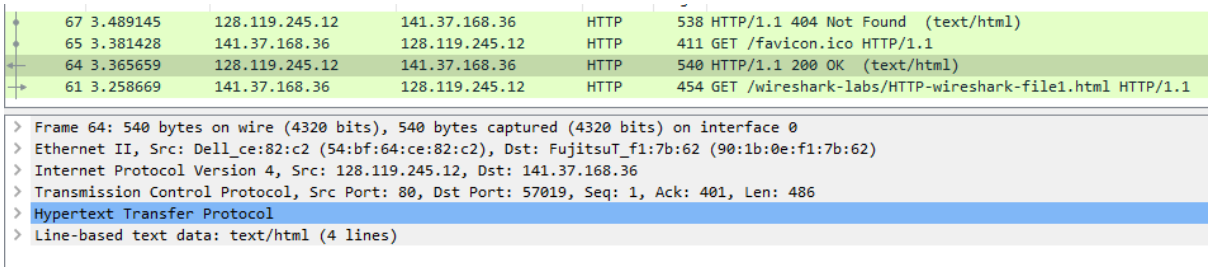


Vergleichen Sie die Ziel-MAC-Adresse für verschiedene Ziel-IP-Adressen.
Welchem Netzknoten können Sie die Ziel-MAC-Adresse zuordnen?



⇨ Netzknoten: Dell_ce (siehe Bilder)

4. Betrachten Sie ein HTTP Paket. Welche weiteren Protokolle werden genutzt, um ein http Paket zu übertragen? Welchen Schichten des TCP/IP-Schichtenmodells können Sie die Pakete zuordnen?



- ⇨ TCP = Transportschicht [Application Layer]
- ⇨ IP = Netzwerkschicht [Network Layer]
- ⇨ Ethernet = Zugriffsschicht [Access Layer]

Aufgabe 4:

1. Markieren Sie im obigen Paket Ethernet, IP und TCP Header

2. Was sind die Quell- und Ziel-MAC-Adressen Adressen des dargestellten Pakets?

   => Ziel: 38-22-D6-67-19-00

   => Quelle: 00-21-CC-63-82-2C

3. Was sind die Quell- und Ziel-IP-Adressen des dargestellten Pakets?

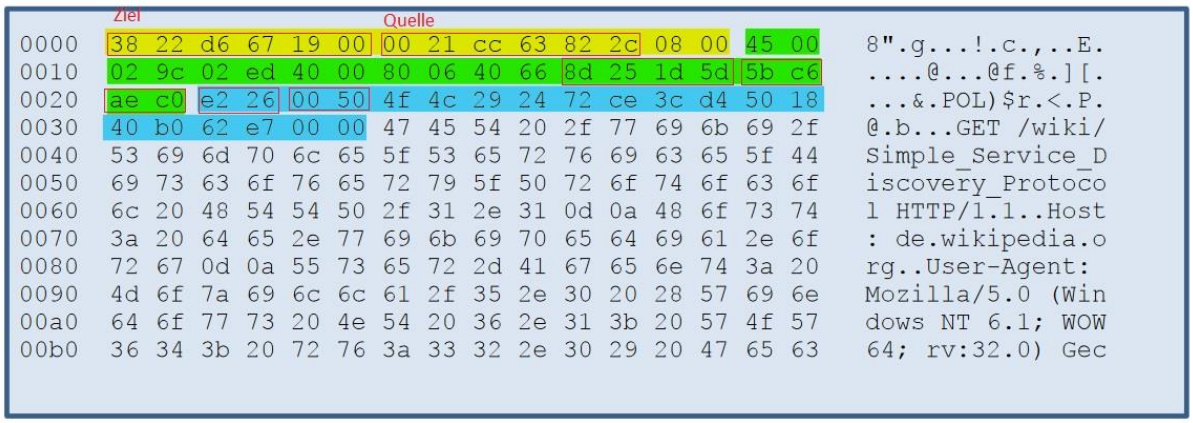
   => Ziel: 5B C6 AE C0 [91.198.174.192]

   => Quelle: 8D 25 1D 5D [141.37.29.93]

4. Was sind die verwendeten TCP-Ports des dargestellten Pakets?

   => Ziel: 00 50 [Port 80]

   => Quelle: E2 26 [Port 57.894]



Aufgabe 5

1. Wie lautet der Filter, mit dem Sie über den TCP Port http Verkehr filtern können?

   => **tcp.port == 80 && http**

2. Erhalten Sie das gleiche Ergebnis wie bei dem Filter HTTP? Erklären Sie ihre Erkenntnis

   => Ja da Port 80 den HTTP Port darstellt

3. Was bewirkt der Filter: http && !(udp.port==1900)

   => Es werden lediglich http Anfragen gefiltert die nicht über den UDP port 1900 laufen

   > => „UDP port 1900 besorgt einen unzuverlässigen Dienst und Datagramme können ohne Meldung verdoppelt, unzulässig kommen oder verschwinden. UDP port 1900 denkt, dass die Fehlernachprüfung und -korrektion nicht erforderlich ist oder in dieser Anwendung nicht vollgezogen wird, um das Overhead dieser Bearbeitung auf dem Netzwerkschnittstellniveau zu vermeiden“ [Quelle: https://de.adminsub.net/tcp-udp-port-finder/1900]

4. Welcher Filter bewirkt, dass nur Pakete angezeigt, werden, die ihre eigene IP-Adresse als Ziel-Adresse haben?

   => **ip.dst == 141.37.168.36** (bzw. ip.dst == xxx.xxx.xxx.xxx wobei x = eigene IP)