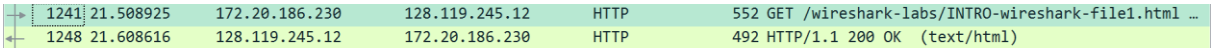
Aufgabe 3:

1. Nennen sie mindestens fünf Protokolle, welche Wireshark erkannt hat:

ARP, UDP, TCP, HTTP, NBNS

2. Wie lange hat es vom Senden des HTTP Requests bis zum Erhalt der HTTP Response gedauert?



21.608616s – 21.508925s = 0.099691s = 99ms

3. Was ist die Internet-Adresse ihres Rechners? Was ist die Ethernet-Adresse (MAC-Adresse, physikalische Adresse) ihres Rechners? Welches ist die Ziel-MAC-Adresse, zu der ihr Rechner Pakete sendet? Vergleichen Sie die Ziel-MAC-Adresse für verschiedene Ziel-IP-Adressen. Welchem Netzknoten können Sie die Ziel-MAC-Adresse zuordnen?

172.20.186.230,

Src: 98:22:ef:7e:90:d7

Dst: 00:a6:ca:f4:9b:4d

ip Adresse unterscheidet sich, MAC-Adresse allerdings nicht.

(Man kann die MAC-Adresse Cicso zuordnen)

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

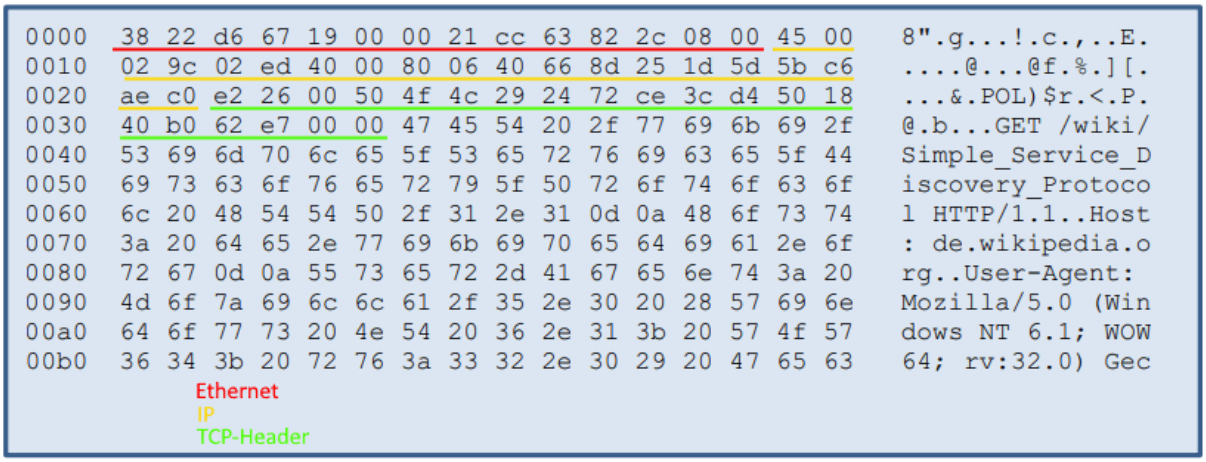
OCSP, XML

OCSP = Anwendungsschicht

XML = Presentation Layer

Aufgabe 4:

1:



2:

Ziel MAC-Adresse 38 22 d6 67 19 00,

Quell-Macadresse: 00 21 cc 63 82 2c

3:

Ziel IP: 5b c6 ae c0

Quell IP: 8d 25 1d 5d

4:

Ziel Port: 00 50

Quell Port: e2 26

Aufgabe 5:

Frage 1 : tcp.port == 80

Frage 2: Nein, wir erhalten sowohl HTTP als auch TCP Pakete.

Frage 3: Filtert nach HTTP Paketen, die nicht über den udp.port 1900 laufen.

Frage 4: ip.dst==ip.src

Aufgabe6:

1.

Upstream:

Befehl: tcp.port==443 && ip.dst==128.65.210.180 && ip.src==192.168.178.70

Pakete: 152

Downstream:

Befehl: tcp.port==443 && ip.dst==192.168.178.70 && ip.src==128.65.210.180

Pakete: 127

2.

In Wireshark unter Verbindungen und dann auf TCP und nach der Verbindung zwischen

IP: 192.168.178.70 und IP: 128.65.210.180 suchen.

Bytes über Uplink: 22 K

Bytes über Downlink: 181 K

3.

Filter für Anzeige auf: tcp.port==443 && ip.dst==192.168.178.70 ändern.

Unter Verbindungen auf IPv4 und nach Anzeigefilter einschränken.

Dann wird die Anzahl der IP-Addressen angezeigt die meine IP als Ziel hatten.

Anzahl IPs: 57

4. Gleiche Vorgehensweise wie in Aufgabe 3 nur diesmal auf TCP statt auf IPv4.

Hier werden Daten von IP+Port: 443 auf meiner IP auf unterschiedlichen Ports empfangen.

Anzahl TCP Sockets: 70

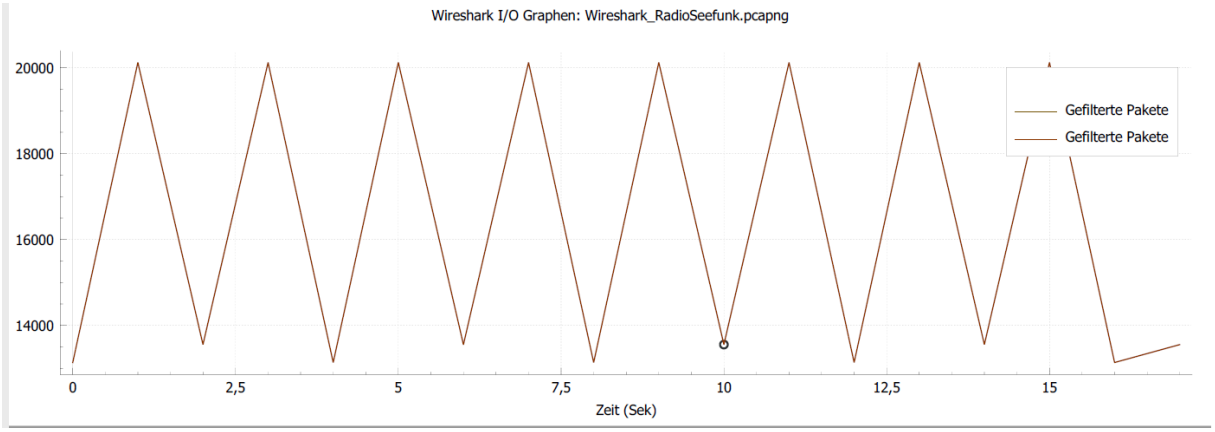
Aufgabe 7:

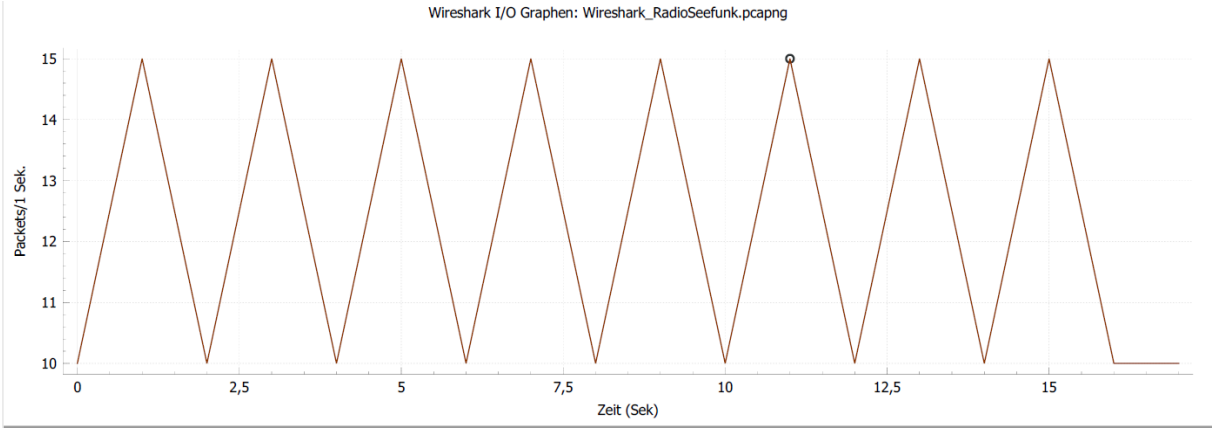
Downlink: Es werden zwischen 10 und 15 Paketen übertragen.

Die Paketanzahl verläuft im 2 Sekunden Rhythmus zwischen 10 und 15 Bits

-> 1s = 15 Packets ----> 2s = 10 Packets ----> 3s = 15 Packets ----> 4s = 10 Packets

Hierbei werden zwischen 13000 und 20000 Bytes übertragen.





Uplink: Es werden zwischen 2 bis 6 Paketen auf dem Uplink übertragen.

Wenn man die übertragenen Bytes auf dem Uplink mit der Anzahl an Paketen vergleicht, sieht man,

dass die Kurven parallel verlaufen.