

### 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?

→	1241	21.508925	172.20.186.230	128.119.245.12	HTTP	552 GET /wireshark-labs/INTRO-wireshark-file1.html ...
←	1248	21.608616	128.119.245.12	172.20.186.230	HTTP	492 HTTP/1.1 200 OK (text/html)

$21.608616s - 21.508925s = 0.099691s = 99ms$

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 Cisco 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:

0000	38	22	d6	67	19	00	00	21	cc	63	82	2c	08	00	45	00	8".g...!.c.,...E.
0010	02	9c	02	ed	40	00	80	06	40	66	8d	25	1d	5d	5b	c6	....@...@f.%.]
0020	ae	c0	e2	26	00	50	4f	4c	29	24	72	ce	3c	d4	50	18	...&.POL)\$r.<.P.
0030	40	b0	62	e7	00	00	47	45	54	20	2f	77	69	6b	69	2f	@.b...GET /wiki/
0040	53	69	6d	70	6c	65	5f	53	65	72	76	69	63	65	5f	44	Simple_Service_D
0050	69	73	63	6f	76	65	72	79	5f	50	72	6f	74	6f	63	6f	iscovery_Protoco
0060	6c	20	48	54	54	50	2f	31	2e	31	0d	0a	48	6f	73	74	l HTTP/1.1..Host
0070	3a	20	64	65	2e	77	69	6b	69	70	65	64	69	61	2e	6f	: de.wikipedia.o
0080	72	67	0d	0a	55	73	65	72	2d	41	67	65	6e	74	3a	20	rg..User-Agent:
0090	4d	6f	7a	69	6c	6c	61	2f	35	2e	30	20	28	57	69	6e	Mozilla/5.0 (Win
00a0	64	6f	77	73	20	4e	54	20	36	2e	31	3b	20	57	4f	57	dows NT 6.1; WOW
00b0	36	34	3b	20	72	76	3a	33	32	2e	30	29	20	47	65	63	64; rv:32.0) Gec

Ethernet  
IP  
TCP-Header

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-Adressen 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

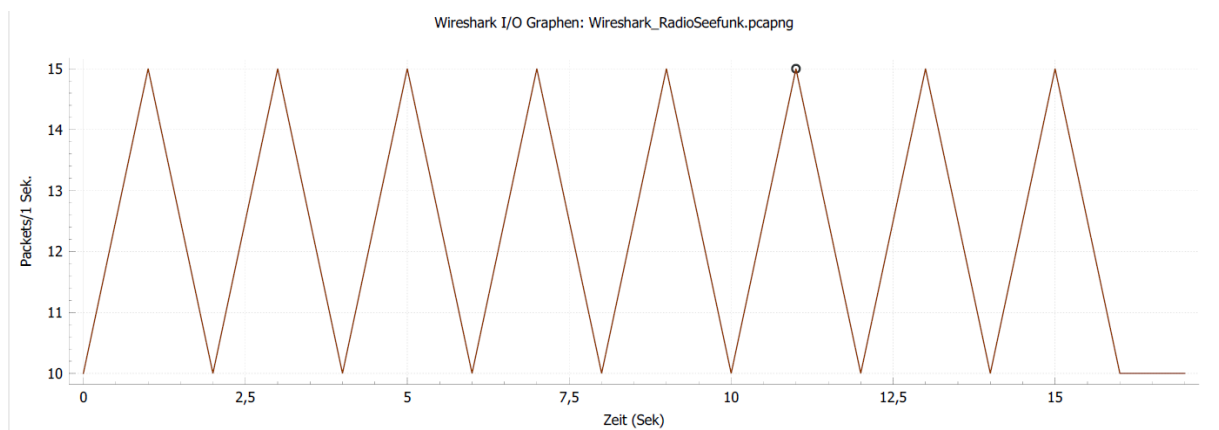
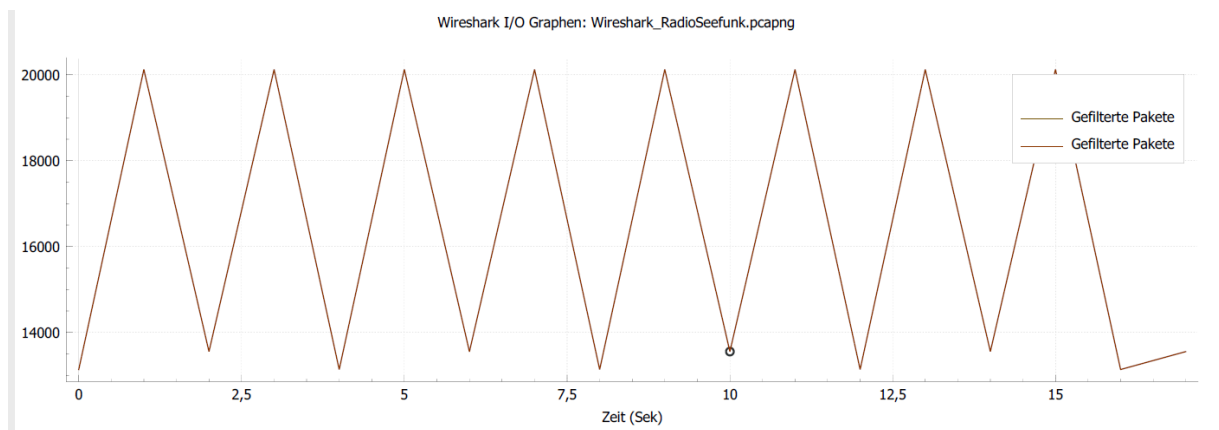
## Aufgabe 7:

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.

