Nennen sie mindestens fünf Protokolle, welche Wireshark erkannt hat:

ARP, UDP, TCP, HTTP, NBNS

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

27,157000ms

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.

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?

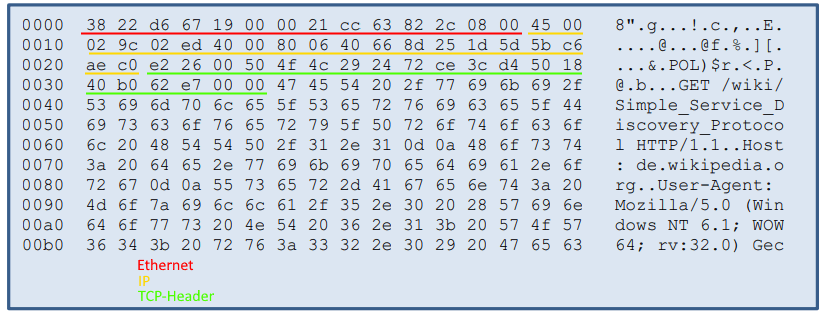
OCSP, XML

OCSP = Vermittlungsschicht

XML = Datenschicht

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:

Frage 4: Filtert nach HTTP Paketen, die nicht über den udp.port 1900 laufen.

Frage 5: ip.dst==ip.src

Aufgabe 6:

1. Downstream Pakete: 129 Upstream Pakete: 23