# Fragen:

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

UDP: User Data Protocol, Schicht4(Transport)  
ARP: Address Resolution Protocol  
SSDP: Simple Service Discovery Protocol  
TLS: Transport Layer Security  
NBNS: NetBIOS Name Service  
TCP: Transmission Control Protocol

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

Time Send: 2.31997

Response: 2.423962

Differenz: 0.103965

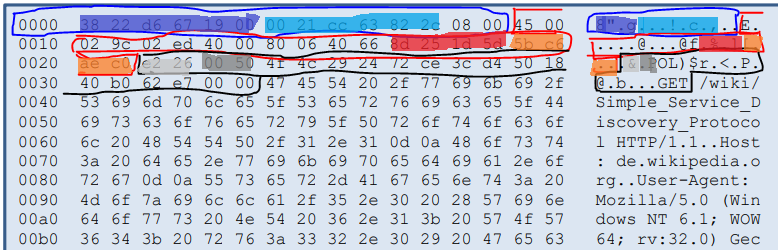
Ipv4: 141.37.168.36

Ipv6: fe80::dfa:de2e:9e27:4075%2

SrcMac: 90:1b:0e:f1:7b:62  
DstMac: 34:17:eb:46:9e:02

Die Ziel-Mac-Addresse ist immer dieselbe, vermutlich gehört diese Addresse nur zum Gateway der HTWG.

1. Weitere Protokolle wären:   
   - TCP: Schicht 4 (Transport Layer)  
   - IP: Schicht 3 (Network Layer)  
   - Ethernet: Schicht 1/2 (Network Access Layer)



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

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

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

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

1. 1. Der TCP-Filter für den HTTP-Verkehr lautet: http && tcp.port == 80

2. Ja wir erhalten das gleiche Ergebnis, weil HTTP immer über Port 80 läuft

3. Dieser Filter bewirkt, dass alle HTTP-Ergebnisse abgesehen von den UPD.Port 1900 angezeigt werden. Dieser UDP-Port sollte über das Internet nicht erreichbar sein, weil darüber Geräte konfiguriert werden können.

4. ip.dst == 141.37.168.36

1. 1. Insgesammt: 408, Downstream: 217, Upstream: 112 Pakete

2. Down: 209681, Up: 32014

3. Wir haben insgesammt von 27 Addressen Daten empfangen

4. Wir haben über 20 Sockets Daten empfangen