3. Fragen

Nachdem wir einen ersten Einblick in WireShark gewonnen haben, ein paar Fragen:

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

TCP, HTTP, UDP, SSDP, DNS

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

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

0,116sec

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?

SRC-IP: 172.20.139.227

SRC-MAC: 90:0f:0c:ba:77:2b

DEST-MAC: 00:a6:ca:f4:9b:4d 🡪 HTWG-WLAN-Router

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?

Frame 4862: LinkLayer

Ethernet II: LinkLayer

IPv4: NetworkLayer

TCP: TransportLayer

HTTP: ApplicationLayer

Ein Bild, das Text, Screenshot, Schrift, Zahl enthält.

Automatisch generierte Beschreibung

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

Orange: Ethernet

Türkis: IP

Braun: TCP

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

Quell: 00:21:cc:63:82:2c

Ziel: 38:22:d6:67:19:00

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

Quell: 8d.25.1d.5d

Ziel: 5b.c6.ae.c0

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

Quell: e226

Ziel: 0050

Fragen:

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 das Ergebnis ist das gleiche, wenn keine HTTP-Requests über andere Protokolle (wie UDP) empfangen/gesendet werden

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

Gibt alle http-Anfragen aus, die nicht über Port 1900 laufen.

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

Adresse haben?

ip.dst == 172.20.139.227