Praktische Aufgaben – Block 7

a) Wie viele Pakete umfasst der Trace?

- 15892

b) Wie groß sind die Pakete im Durchschnitt?

- 898 Byte

c) Notieren Sie alle im Trace auftauchenden MAC-Adressen.

- 00:07:7d:0a:75:6f
- 00:07:b4:00:00:02
- 00:22:0d:ea:68:00
- 01:00:5e:00:00:fb
- 01:00:5e:7f:ff:fa
- 33:33:00:00:00:fb
- 48:bf:6b:e1:63:22
- a0:cf:5b:3d:d2:bc
- c8:9c:1d:4d:01:00

d) Wie viele IP-Adressen tauchen im Trace auf?

- 53(IP4) + 2(IP6) = 55

e) Einige der auftauchenden MAC-Adressen sind mit IP-Adressen verknüpft. Notieren sie diese Verknüpfungen.

- 141.23.210.146 -> 48:bf:6b:e1:63:22
- 141.23.192.1 -> 00:07:b4:00:00:02

f) Bei welchem Anteil der Pakete wird das Internet Protocol(IP) auf der Vermittlungs/Netzwerkschicht (ISO/OSI Modell) verwendet?

- 0,3 %

g) Bei welchem Anteil der Pakete wird das Transmission Control Protocol (TCP) auf der Transportschicht verwendet?

- 98,2 %

h) Notieren Sie alle Protokolle der Applikationsschicht die TCP nutzen.

- HTTP

i) Notieren Sie alle Protokolle der Applikationsschicht die das User Datagram Protocol(UDP)nutzen.

- Dropbox Lan sync Discovery Protocol

j) Notieren sie alle auftauchenden Protokolle der Vermittlungs/Netzwerkschicht.

- IPv4, IPv6, ARP

k) Notieren sie alle auftauchenden Protokolle der Sicherungsschicht.

- Ethernet

l) Wie viele Domain Name System (DNS)-Abfragen fanden statt?

- 97

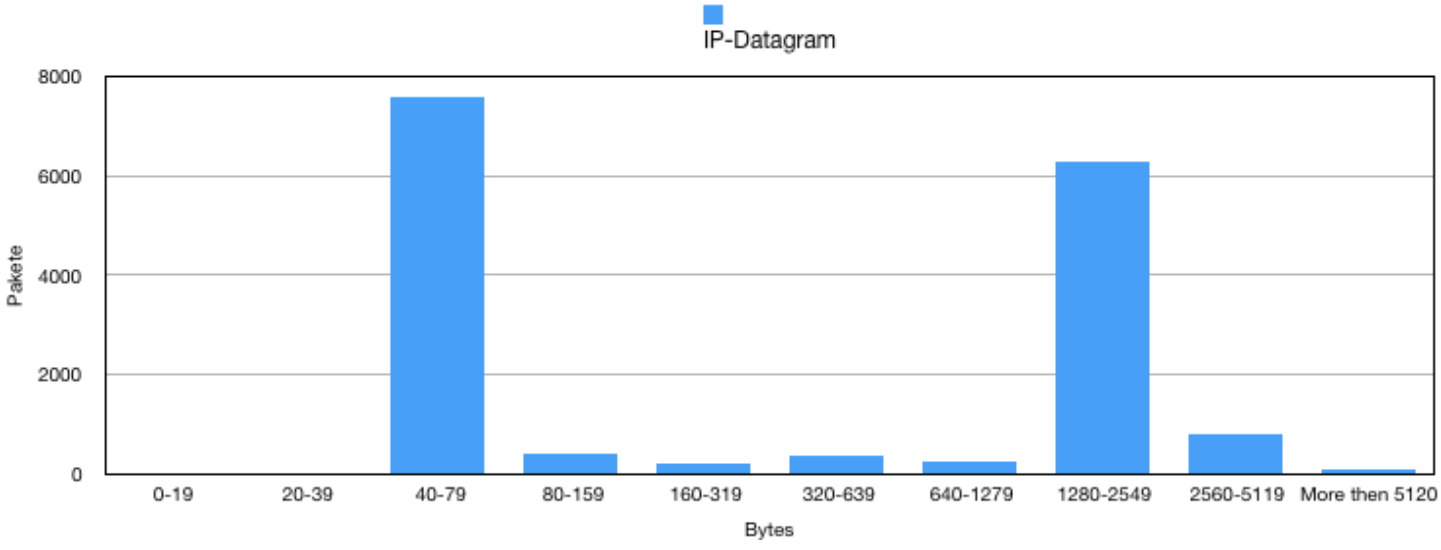
m) Wie viele IP-Pakete haben einen “Time-To-Live” (TTL) Wert größer als 200, mit genau 128 und mit genau 64? Versuchen sie, eine Erklärung für die gefundene Verteilung zu finden.

- 6 bei ttl 64
- 0 bei ttl 200
- 15884 bei 128

n) Untersuchen Sie das 16. Paket im Trace genauer:

1. Wie groß ist der Ethernet-Header?
    - 1518 bytes
2. Wie groß ist der IP-Header?
    - 20 bytes
3. Wie groß ist das IP-Datagram?
    - 173 bytes
4. Wie groß ist der TCP-Header?
    - 20 bytes
5. Wie groß ist das TCP-Segment?
    - 153 bytes

o) Erstellen Sie ein Histogramm über die Länge der IP-Datagramme. Interpretieren Sie das Ergebnis.



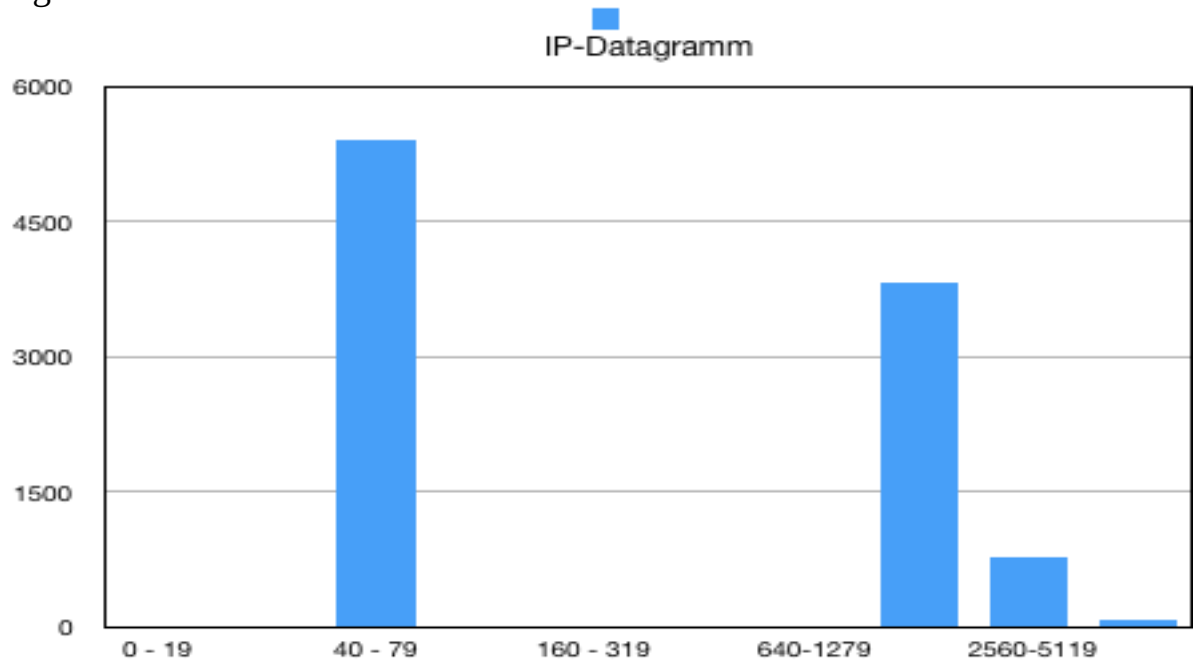
Aus dem Histogramm kann man gut sehen, dass die meisten Pakete die Lenge zwischen 40-70 Bytes haben. Diese kleinen Pakete entsprechen der minimalen Lenge, um die Protokolle zu transportieren und sind für die Koordination zuständig. Das erklärt, warum es keine Pakete kleiner als 40 Bytes gibt.

Eine zweitgrößte Spalte ist für den tatsächlichen Datentransport zuständig und entspricht der durchschnittlichen Lenge der meisten Pakete.

p) Zwischen welchen IP-Adressen werden die meisten Bytes ausgetauscht?

- zwischen 81.66.122.238 und 172.16.254.128

Erstellen Sie ein Histogramm über die Länge dieser IP-Datagramme. Interpretieren Sie das Ergebnis.



Das Histogramm zeigt, dass die meisten Pakete 40-70 Bytes erhalten, diese sind für die Koordination zuständig und bestehen meistens z.B aus ACK oder SYN. Große Pakete, die über 1230 Bytes bestehen, sind für den tatsächlichen Datentransport zuständig.

q) Zwischen welchen IP-Adressen werden die meisten Pakete ausgetauscht?

- Adresse A: 81.166.122.238
- Adresse B: 172.16.254.128
- Packets A -> B: 7554
- Packets B -> A: 2570
- Packets insgesamt: 10124

r) Bestand eine verschlüsselte Verbindung? Notieren Sie ggf. die beteiligten Hosts.
Gefiltert nach ssl (Secure Sockets Layer):
Wir: 172.16.254.128 von jedem Host bestand eine Verbindung zu uns

- Host 1: 216.58.208.227
- Host 2: 54.227.250.135
- Host 3: 173.194.65.94
- Host 4: 216.58.208.196
- Host 5: 199.16.156.21
- Host 6: 216.58.208.206
- Host 7: 216.58.208.225
- Host 8: 216.58.208.226
- Host 9: 216.58.208.237
- Host 10: 216.58.208.238
- Host 11: 23.192.162.171
- Host 12: 23.205.82.104
- Host 13: 31.13.93.3
- Host 14: 88.221.83.67
- Host 15: 88.221.83.80

s) Wurde ein Web-Browser benutzt? Wenn ja, welche?
Google Chrome