a) Wie viele Pakete umfasst der Trace?

15892

b) Wie groß sind die Pakete im Durchschnitt?

897.98 Bytes

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

Es gibt 6 MAC-Adressen:

00:0c:29:b6:b5:48
00:50:56:c0:00:08
00:50:56:f3:f2:f6
01:00:5e:00:00:fc
33:33:00:01:00:03
ff:ff:ff:ff:ff:ff

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

Es gibt 53 IPv4 und 2 IPv6 Adressen.

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

MAC - IP
00:0c:29:b6:b5:48 - 172.16.254.128
00:50:56:f3:f2:f6 - 172.16.254.2

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

15841 IPv4 + 2 IPv6 = 15843 IP
15843 IP / 15892 Packets = 99,7%
Das IP Protocol wird bei 99,7% Pakete verwendet.

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

15611 TCP / 15892 Packets = 98,2%
Das TCP Protocol wird bei 98,2% Pakete verwendet.

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

TLSv1.2
HTTP
Data "protocol" - Ein Protokoll, das Wireshark entweder nicht (mehr) unterstuetzt oder nicht erkennt.

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

NBNS (Netbios Name Service)
LLMNR (Link-local Multicast Name Resolution)
DNS
DB-LSP-DISC (Dropbox LAN sync Discovery Protocol)

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

Internet Protocol Version 6, Internet Protocol Version 4, Address Resolution Protocol

k) Notieren sie alle auftauchenden Protokolle der Sicherungsschicht.

Ethernet

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

Es gab 97 DNS Abfragen.

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 Erklarung¨ fur¨ die gefundene Verteilung zu finden.

genau 64 - 6
genau 128 - 15833
größer als 200 - 0

By convention 64 is the TTL if both communicating parties are located in the same region, whereas 128 in the same continent. The server must be located in the same continent, thus TTL is set to 128. There doesn’t seem to be any direct intercontinental communication, so there aren’t any packets with TTL>200 to be found.

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

1. Wie groß ist der Ethernet-Header?

14 Bytes

2. Wie groß ist der IP-Header?

20 Bytes

3. Wie groß ist das IP-Datagram?

193 Bytes

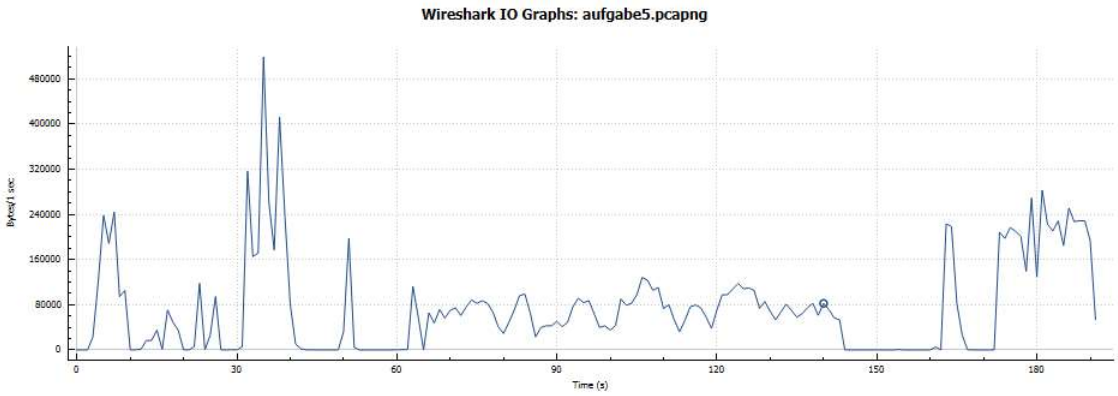
4. Wie groß ist der TCP-Header?

20 Bytes

5. Wie groß ist das TCP-Segment?

153 Bytes

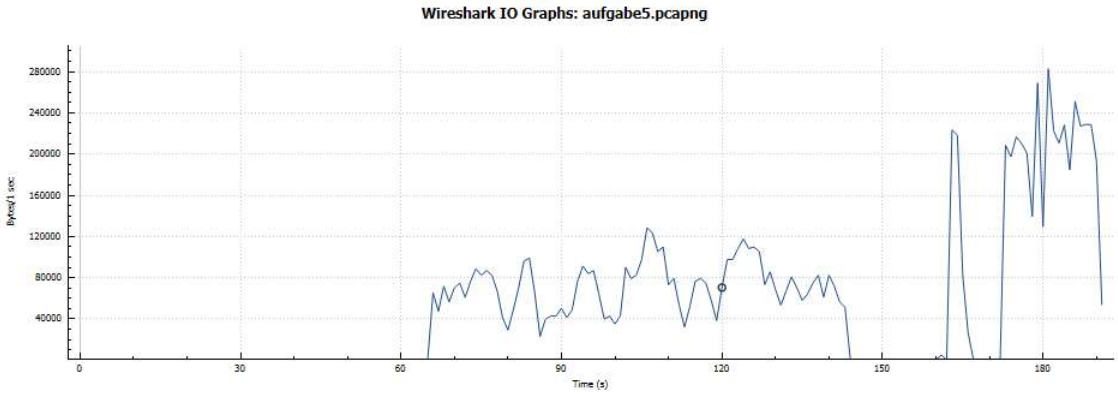
o) Erstellen Sie ein Histogramm über die Lange der IP-Datagramme. Interpretieren Sie das Ergebnis.



Die meisten Pakete sind unter 100 Bytes groß. Die absolute Mehrheit wird zwischen der ninja-game.org Website und einer lokalen Adresse ausgetauscht. Bei online Spielen ist die Geschwindigkeit wichtig und somit werden viele kleine Pakete ausgetauscht. Es werden aber auch viele Pakete der Größe ~1500 zwischen den Adressen ausgetauscht. Außerdem gibt es noch viel Pakete mit einer Größe von ~1500 Bytes, die von gstaticadssl.l.google.com geschickt werden. Also sind dies sehr wahrscheinlich Suchergebnisse

p) Zwischen welchen IP-Adressen werden die meisten Bytes ausgetauscht? Erstellen Sie ein Histogramm über die Lange¨ dieser IP-Datagramme. Interpretieren Sie das Ergebnis.

Zwischen 81.166.122.238 (ninja-game.org) und 172.16.254.128 die meisten Bytes [insgesamt über 10 MBytes] ausgetauscht wurden. Bei online Spielen ist die Geschwindigkeit und kleine Latenz wichtig (um z.B. die in-game Position der Spieler, Game Zustand zu vermitteln) und somit werden sehr viele kleine Pakete ausgetauscht.



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

Zwischen 81.166.122.238 und 172.16.254.128 die meisten Pakete aufgetaucht wurden.
172.16.254.128 - IP address of device in local network

r) Bestand eine verschlüsselte Verbindung? Notieren Sie ggf. die beteiligten Hosts.

Ja, folgende Hosts haben das Protokoll TLSv1.2 benutzt:
23.192.162.171
23.205.82.104
31.13.93.3
54.227.250.135
88.221.83.67
88.221.83.80
172.16.254.128
173.194.65.94
199.16.156.21
216.58.208.196
216.58.208.206
216.58.208.225
216.58.208.226
216.58.208.227
216.58.208.237
216.58.208.238

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

Zu sehen sind:
Chrome 41 on Windows 7
Chrome 40 on Mac OS X (Yosemite)