Block 7 **Rechnernetze und Verteilte Systeme**
Daniel Wujecki Technische Universität Berlin
Amro Hendawi Wintersemester 18/19
Nils Hendrischke 31. Januar 2019
Leon Marius Moll T18 G01

---

a) Wie viele Pakete umfasst der Trace?

Der Trace umfasst 15892 Pakete.

b) Wie groß sind die Pakete im Durchschnitt?

Sie sind im Durchschnitt 897,98 groß.

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

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

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

- **IPv4:** 53
- **IPv6:** 2

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

Folgende Mac Adressen sind mit Ip Adressen verknüpft:

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

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

Bei 100 Prozent.

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

Bei 98,2 Prozent.

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.

- NetBIOS Name Service
- Link-local Multicast Name Resolution
- Dropbox LAN sync Discovery Protocol
- Domain Name System

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

- IPv4
- IPv6

k) Notieren sie alle auftauchenden Protokolle der Sicherungsschicht.

ARP

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

Es fanden 195 DNS-Abfragen statt.

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

Es gab:

- 0 Pakete mit einer TTL > 200
- 15833 Pakete mit einer TTL = 128
- 6 Pakete mit einer TTL = 64

64 und 128 sind Standardwerte, die sich jedoch bei verschiedenen Systemen unterscheiden.

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

1. Wie groß ist der Ethernet-Header?

Er ist 14 groß.

2. Wie groß ist der IP-Header?

Er ist 20 Bytes groß.

3. Wie groß ist das IP-Datagram?

Er ist 193 Bytes groß.

4. Wie groß ist der TCP-Header?

Er ist 20 Bytes groß.

5. Wie groß ist das TCP-Segment?

Er ist 153 Bytes groß.

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

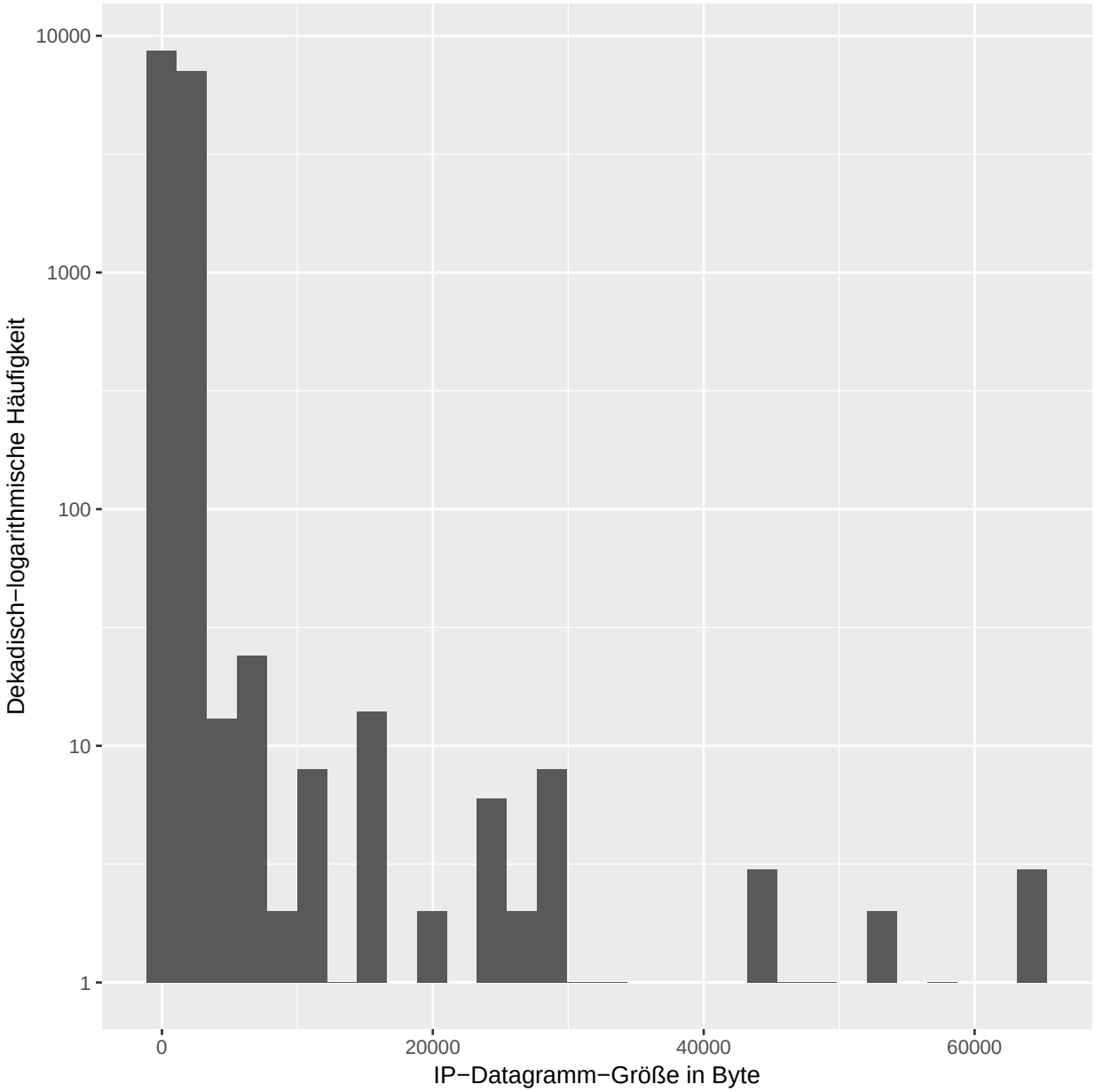

Abbildung 1: Histogram: Länge aller IP-Datagramme

Ein Großteil der IP-Datramm Pakete ist sehr kurz. Dies ist wie folgt zu erklären: Wenn man die Kommunikation in viele kleine Pakete unterteilt, ist der Schaden eines einzelnen Paketverlusts geringer als bei wenigen großen Paketen. Da zu über 98 % TCP verwendet wurde und dort die Chance des Paketverlusts erheblich höher als bei UDP ist, sind die Pakete zum Großteil kurz.

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

Die Grund der Verteilung ist der gleiche wie bei Aufgabe o) und dieser bitte zu entnehmen. Zwischen 81.166.122.238 und 172.16.254.128 wurden am meisten Bytes ausgetauscht.

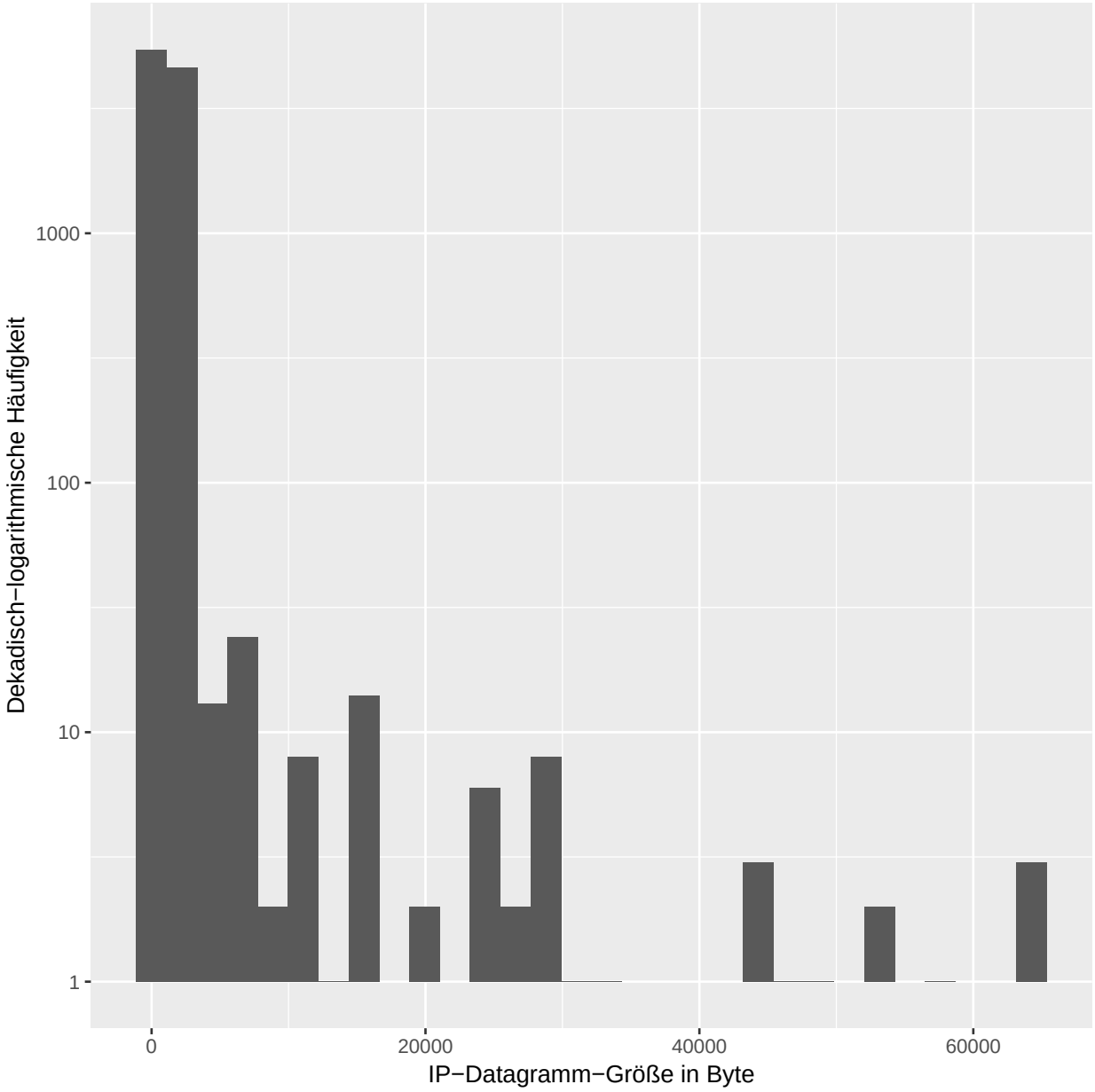

Abbildung 2: Histogram: Länge einiger IP-Datagramme

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

Zwischen 81.166.122.238 und 172.16.254.128 wurden am meisten Pakete ausgetauscht.

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

Bei 1368 Paketen bestand eine verschlüsselte Verbindung. Folgende Hosts mit folgenden IP-Adressen waren beteiligt:

- 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

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

Es wurde Chrome in der Version 41 und 40 benutzt.