Rechnernetze und Verteilte Systeme
Block 7: Aufgabe 5

Filip Twardzik
Tim Korjakow

January 28, 2018

(a) Wieviele Pakete umfasst der Trace?

Das Trace umfasst 15892 Packete.

(b) Wie groß sind die Pakete im Durchschitt?

Im Durchschnitt sind die Pakete 897.98 Bytes groß.

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Packet Lengths	15892	897.98	42	64294	0.0832	100%	1.9700	37.928
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	7565	57.92	42	79	0.0396	47.60%	1.3900	173.882
80-159	402	105.68	80	158	0.0021	2.53%	0.1700	39.236
160-319	187	237.93	161	318	0.0010	1.18%	0.1200	39.255
320-639	374	492.23	320	634	0.0020	2.35%	0.1300	51.221
640-1279	231	943.37	642	1274	0.0012	1.45%	0.0700	35.758
1280-2559	6271	1499.52	1287	1975	0.0328	39.46%	1.3100	35.192
2560-5119	782	2997.23	2604	4434	0.0041	4.92%	0.0900	178.573
5120 and greater	0	-	-	-	0.0000	0.00%	-	-

(c) Notieren Sie alle im Trace auftauchenen 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

(d) Wieviele IP-Adressen tauchen im Trace auf?

Im Trace tauchen 181 IP-Adressen auf.

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

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

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

Internet Protocol auf der Netzwerkschicht wird bei $\frac{15843}{15892} = 99.69\%$ der Pakete benutzt.

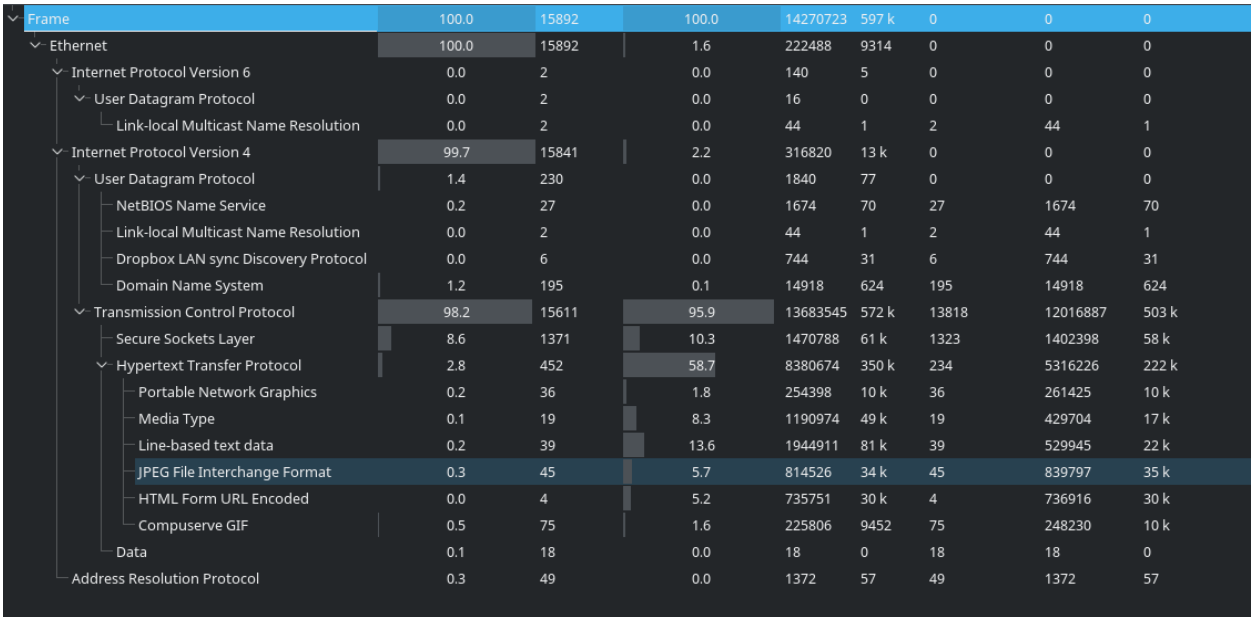
(g) Bei welchem Anteil der Pakete wird das Transmission Control Protocol (TCP) auf der Transportschicht verwendet?

Auf IPv6 werden keine Packete per TCP verschickt, bei IPv4 werden 98.2% der Packete per TCP verschickt.

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

Protokolle der Applikationsschicht die TCP benutzen:

- HTTP
- SSL



Frame	100.0	15892	100.0	14270723	597 k	0	0	0
Ethernet	100.0	15892	1.6	222488	9314	0	0	0
Internet Protocol Version 6	0.0	2	0.0	140	5	0	0	0
User Datagram Protocol	0.0	2	0.0	16	0	0	0	0
Link-local Multicast Name Resolution	0.0	2	0.0	44	1	2	44	1
Internet Protocol Version 4	99.7	15841	2.2	316820	13 k	0	0	0
User Datagram Protocol	1.4	230	0.0	1840	77	0	0	0
NetBIOS Name Service	0.2	27	0.0	1674	70	27	1674	70
Link-local Multicast Name Resolution	0.0	2	0.0	44	1	2	44	1
Dropbox LAN sync Discovery Protocol	0.0	6	0.0	744	31	6	744	31
Domain Name System	1.2	195	0.1	14918	624	195	14918	624
Transmission Control Protocol	98.2	15611	95.9	13683545	572 k	13818	12016887	503 k
Secure Sockets Layer	8.6	1371	10.3	1470788	61 k	1323	1402398	58 k
Hypertext Transfer Protocol	2.8	452	58.7	8380674	350 k	234	5316226	222 k
Portable Network Graphics	0.2	36	1.8	254398	10 k	36	261425	10 k
Media Type	0.1	19	8.3	1190974	49 k	19	429704	17 k
Line-based text data	0.2	39	13.6	1944911	81 k	39	529945	22 k
JPEG File Interchange Format	0.3	45	5.7	814526	34 k	45	839797	35 k
HTML Form URL Encoded	0.0	4	5.2	735751	30 k	4	736916	30 k
Compuserve GIF	0.5	75	1.6	225806	9452	75	248230	10 k
Data	0.1	18	0.0	18	0	18	18	0
Address Resolution Protocol	0.3	49	0.0	1372	57	49	1372	57

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

- DNS
- NBNS
- DB-LSP-DISC
- LLMNR

(j) Notieren sie alle auftauchenden Protokolle der Netzwerkschicht

Alle auftauchenden Protokolle der Netzwerkschicht:

- IPv4
- IPv6
- ARP

(k) Notieren sie alle auftauchenden Protokolle der Sicherungsschicht.

- SSL
- TLSv1.2

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

Es fanden 195 DNS-Abfragen statt.

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

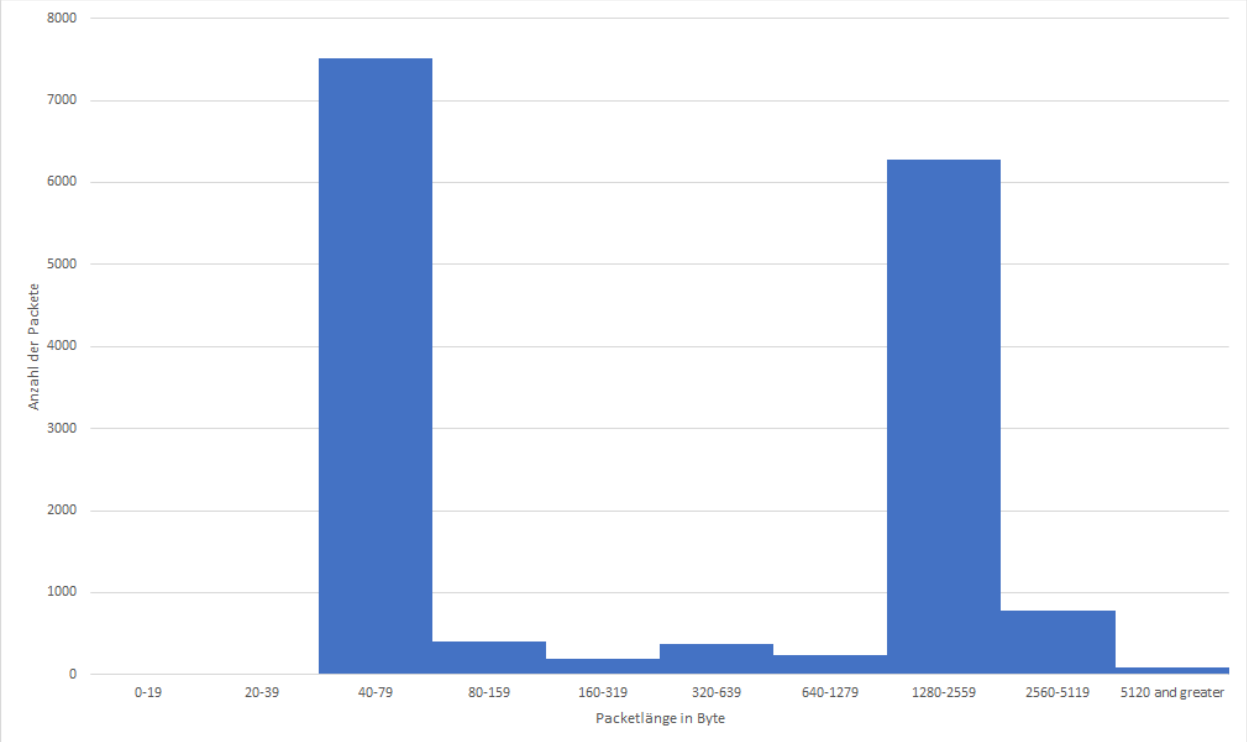
- > 200: 0
- $= 128$: 15833
- $= 64$ 6

Der TTL-Wert ist dazu da eine Überschwemmung durch nicht zustellbare Packete zu verhindern. Dabei wird standardmäßig ein Wert unter 200 gewählt, da hierbei ein Offtrade zwischen Zustellbarkeit und Netzwerklast auftritt. Die meisten Packete haben 64 or 128 als TTL-Wert, da OS-abhängig diese Werte von der Implementierung des OS-Stacks gewählt werden. Zudem kann man die Reichweite eines Packetes durch den TTL-Wert steuern. 64 entspricht dabei derselben Region und 128 demselben Kontinent, in der/dem Host/Client liegen.

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

1. Wie gross ist der Ethernet-Header?
    - 14 Bytes (frame size: 207B - total IP datagram length: 193B)
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 uber die Länge der IP-Datagramme. Interpretieren Sie das Ergebnis.

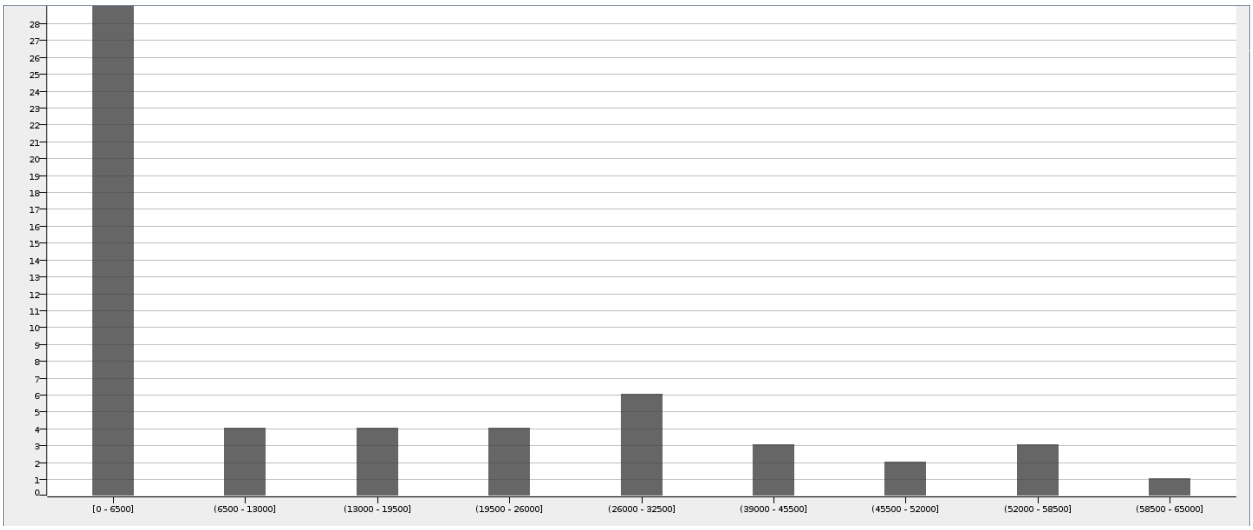


Es gibt keine IP-Datagramme, welche kürzer als 40 Byte sind, da ein IPv4 Header zwischen 20 und 60 Byte und ein IPv6 Header genau 40 Byte groß ist. Rechnet man die Größe des Payload dazu, ist man bei einem Wert größer 40.
Im Histogram lassen sich zwei klare Peaks bei 40-79 Byte pro Packet und 1280-2559 Byte

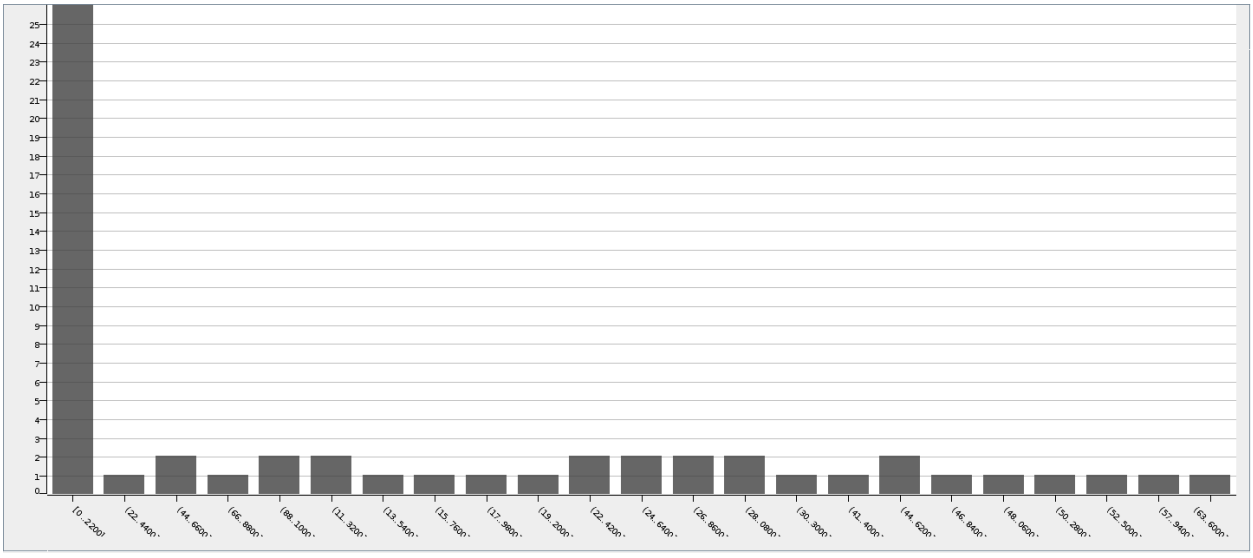
pro Packet feststellen. Dies spricht dafür, dass sowohl ein "leichtes" Protokoll als auch ein längeres Protokoll den Traffic dominieren. Das Längere ist vermutlich HTTP, da ein Großteil des Traffics im Stacktrace durch einen Browser verursacht wird. Bei genauer Analyse des Stacktraces wird ersichtlich, dass die Mehrzahl der kurzen Packete ACKs für gesendete TCP-Packete sind.

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

Die meisten Bytes werden zwischen 81.166.122.238 und 172.16.254.128 ausgetauscht. Für die Länge dieser IP-Datagramme ergibt sich folgender Histogramm:



und mehr detaillierter zweiter Histogramm:



Interpretation: Zwei Endgeräte mit den gegebenen dazugehörigen IP-Adressen schicken oft sehr viele kleine Pakete, und auf diese Weise sind zwischen ihnen die meisten BYtes ausge-

tauscht.

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

Zwischen der IP-Adresse 81.166.122.238 und der IP-Adresse 172.16.254.128 wurden am meisten Packete ausgetauscht (10124 an der Zahl).

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

Es bestanden mehrere verschlüsselte Verbindungen mit folgenden beteiligten Hosts:

```
172.16.254.128
216.58.208.227
216.58.208.238
54.227.250.135
173.194.65.94
216.58.208.196
216.58.208.237
23.205.82.104
199.16.156.21
31.13.93.3
216.58.208.225
88.221.83.67
216.58.208.226
88.221.83.80
23.192.162.171
216.58.208.206
```

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

Der user-agent header des HTTP Calls sieht wiefolgt aus:
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.115 Safari/537.36
Nach aktueller Konvention geben sich beinahe alle Browser als Mozilla 5.0 Browser aus. In diesem Falle wurde jedoch Safari/537.36 verwendet.