1. Network traffic analysis using tcpdump

1.1 How many packets does the trace contain?

32616

tcpdump -n -r hw1.pcap | wc -l

1.2 How many ARP packets and how many UDP packets?

11304

tcpdump -n -r hw1.pcap | grep 'ARP' | wc -l

1.3 How many packets were exchanged between 91.189.90.41 and 192.168.0.200?

19

tcpdump -n -r hw1.pcap | grep '91.189.90.41' | grep '192.168.0.200' | wc -l

1.4 Print the unique source IP addresses found in the trace.

0.0.0.0

1.234.31.20

122.154.101.54

130.75.16.5

159.148.96.184

169.254.56.55

192.168.0.1

192.168.0.10

192.168.0.11

192.168.0.12

192.168.0.2

192.168.0.200

192.168.0.3

192.168.0.5

192.168.0.6

192.168.0.7

194.168.4.100

216.137.63.121

216.137.63.137

46.51.197.88

46.51.197.89

62.252.170.81

62.252.170.91

87.230.23.162

87.98.246.8

91.189.88.33

91.189.89.88

91.189.90.40

91.189.90.41

91.189.91.14

91.189.91.15

91.189.92.190

92.240.68.152

tcpdump -n -r hw1.pcap ip | cut -d " " -f 3 | cut -d "." -f 1-4 | sort | uniq

1.5 Print the unique 'private network' (according to RFC1918) source IP

addresses found in the trace.

192.168.0.1

192.168.0.10

192.168.0.11

192.168.0.12

192.168.0.2

192.168.0.200

192.168.0.3

192.168.0.5

192.168.0.6

192.168.0.7

tcpdump -n -r hw1.pcap ip and \(src net 172.16.0.0/20 or src net 10.0.0.0/8 or src net 192.168.0.0/16\) | cut -d " " -f 3 | cut -d "." -f 1-4 | sort | uniq

1.6 Print the unique destination IP addresses found in the trace.

192.168.0.12

192.168.0.200

192.168.0.255

tcpdump -n -r hw1.pcap ip and \(dst net 172.16.0.0/20 or dst net 10.0.0.0/8 or dst net 192.168.0.0/16\) | cut -d " " -f 5 | cut -d "." -f 1-4 | sort | uniq

1.7 What are the top-5 TCP and top-5 UDP destination ports?

TCP:

(occurrence / port)

727 80

697 54634

346 49836

61 47110

36 40341

tcpdump -n -r hw1.pcap tcp| cut -d " " -f 5 | cut -d "." -f 5 | sort | uniq -c | sort -r | head -5

UDP:

(occurrence / port)

1925 137

1516 5355

13178 1900

840 5353

399 138

tcpdump -n -r hw1.pcap udp| cut -d " " -f 5 | cut -d "." -f 5 | sort | uniq -c | sort -r | head -5

1.8 How many TCP packets have the SYN flag set?

75

tcpdump -n -r hw1.pcap 'tcp[tcpflags] & tcp-syn != 0' | wc -l

1.9 How many TCP connection attempts were made?

37

tcpdump -n -r hw1.pcap 'tcp[tcpflags] == tcp-syn' | wc -l

1.10 Towards which ports were TCP connection attempts made? How many attempts

per port?

(attempts | destination port)

1 443

1 465

2 9100

33 80

tcpdump -n -r hw1.pcap 'tcp[tcpflags] == tcp-syn' | cut -d " " -f 5 | cut -d "." -f 5 | sort | uniq -c | sort

1.11 How many HTTP GET requests were made? Print the URLs of all HTTP requests

for JPG files.

94 HTTP GET requests were made.

tcpdump -n -r hw1.pcap 'tcp[((tcp[12:1] & 0xf0) >> 2):4] = 0x47455420'|wc -l

URLs:

http://pic.leech.it/i/f166c/479246b0asttas.jpg

/i/f166c/479246b0asttas.jpg

http://ecx.images-amazon.com/images/I/41oZ1XsiOAL.\_SL500\_AA300\_.jpg

http://www.nature.com/news/2009/090527/images/459492a-i1.0.jpg

/news/2009/090527/images/459492a-i1.0.jpg

tcpdump -n -r hw1.pcap 'tcp[((tcp[12:1] & 0xf0) >> 2):4] = 0x47455420'| grep '.jpg' | grep -Eo "HTTP: GET .+ " | cut -d " " -f 3

1.12 When (date and time) was the first and last packet of the trace sent?

first:

2013-01-12 11:37:42.871346

tcpdump -tttt -nr hw1.pcap | head -n 1 | cut -d " " -f 1-2

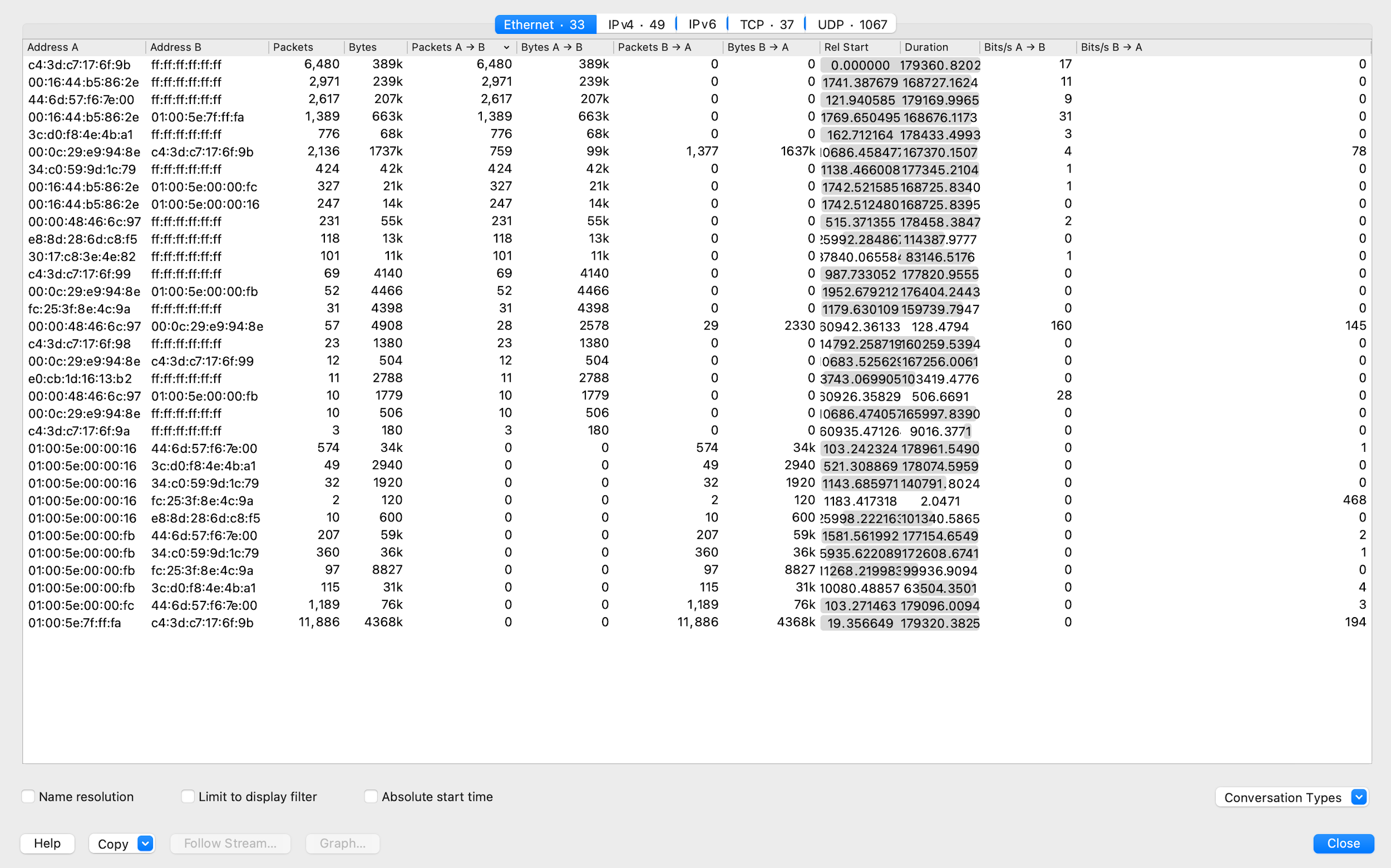
last:

2013-01-14 13:27:03.691498

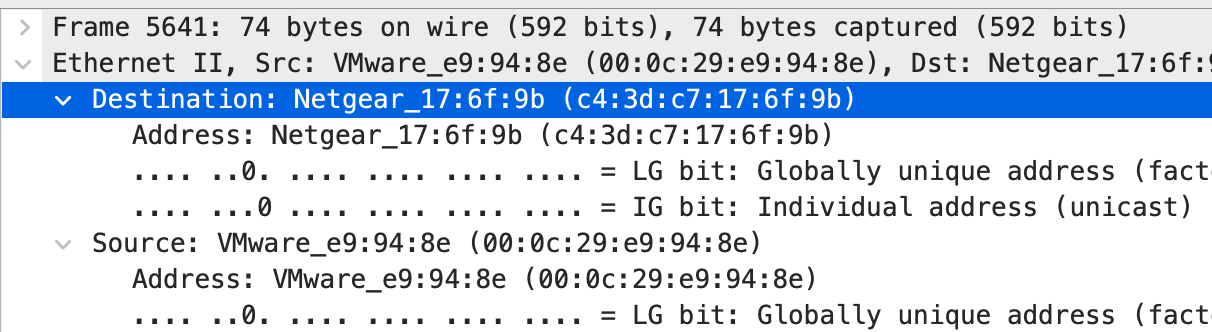
tcpdump -tttt -nr hw1.pcap | tail -n 1 | cut -d " " -f 1-2

1.13 What is the brand of the device that sent most of the packets? What is its

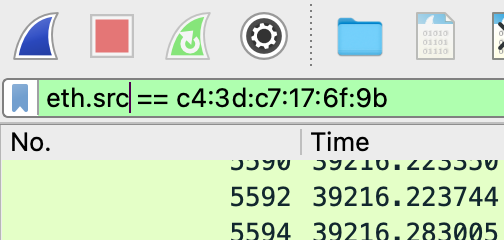
IP address?



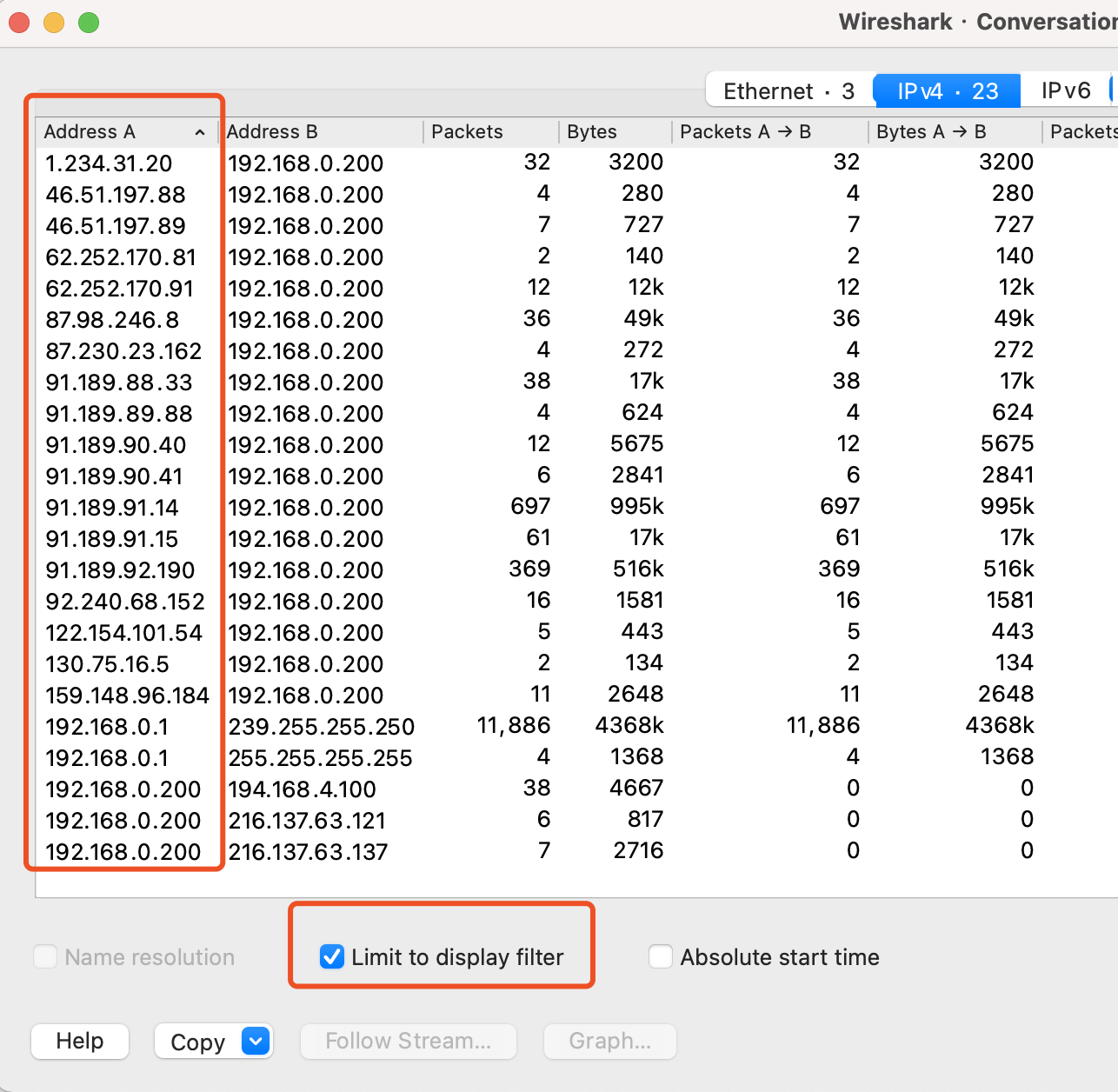
From the result of wireshark’s conversations analysis, we know the device of mac address c4:3d:c7:17:6f:9b sent the most packets, from one packet’s ethernet analysis in Wireshark, we know it is from brand Netgear\_17:6f:9b.



Now we limit the result by filter:



Then check the related conversations analysis again, below are the IPs of this device:



1.14 Report the distribution of Ethernet packet sizes (how many packets of size

X exist in the trace, for all values of X in the trace).

(number of packets | length)

2759 length 363

2759 length 353

2759 length 289

2749 length 298

1740 length 50

11280 length 46

1034 length 1448

887 length 22

748 length 0

375 length 24

325 length 300

283 length 201

232 length 21

180 length 68

164 length 442

164 length 433

162 length 497

161 length 513

158 length 485

155 length 499

146 length 133

88 length 352

88 length 344

87 length 350

87 length 348

86 length 320

86 length 296

86 length 276

85 length 356

85 length 284

62 length 125

60 length 123

53 length 207

40 length 991

39 length 177

30 length 189

24 length 28

22 length 656

22 length 180

16 length 179

14 length 265

13 length 624

11 length 486

10 length 514

10 length 500

10 length 498

10 length 443

10 length 434

10 length 266

9 length 182

8 length 774

8 length 280

8 length 26

7 length 308

7 length 262

6 length 992

6 length 544

6 length 27

6 length 267

6 length 264

6 length 198

5 length 775

5 length 562

5 length 547

5 length 263

5 length 100

4 length 993

4 length 548

4 length 288

4 length 279

4 length 23

4 length 20

4 length 188

4 length 178

3 length 431

3 length 232

3 length 203

3 length 183

3 length 181

3 length 167

3 length 14

2 length 638

2 length 570

2 length 564

2 length 558

2 length 555

2 length 549

2 length 546

2 length 545

2 length 541

2 length 532

2 length 527

2 length 484

2 length 480

2 length 436

2 length 412

2 length 317

2 length 278

2 length 255

2 length 244

2 length 243

2 length 239

2 length 228

2 length 202

2 length 200

2 length 199

2 length 195

2 length 191

2 length 170

2 length 163

2 length 1146

1 length 913

1 length 886

1 length 860

1 length 694

1 length 686

1 length 680

1 length 664

1 length 628

1 length 613

1 length 612

1 length 574

1 length 56

1 length 542

1 length 535

1 length 530

1 length 526

1 length 522

1 length 502

1 length 482

1 length 478

1 length 469

1 length 452

1 length 440

1 length 418

1 length 416

1 length 413

1 length 380

1 length 367

1 length 366

1 length 362

1 length 351

1 length 346

1 length 330

1 length 323

1 length 306

1 length 302

1 length 281

1 length 254

1 length 252

1 length 251

1 length 249

1 length 246

1 length 242

1 length 240

1 length 157

1 length 141

1 length 1403

1 length 129

1 length 1152

1 length 112

1 length 1113

1 length 111

1 length 1104

1 length 1096

1 length 105

1 length 1036

tcpdump -nr hw1.pcap | grep -Eo "length \d+" | sort | uniq -c | sort -r