1.1 How many packets does the trace contain?

**Command** => tcpdump -n -r hw1.pcap | wc -l

**Result** : 32664

1.2 How many ARP packets and how many UDP packets?

**ARP:** Command => tcpdump -n -r hw1.pcap arp | wc -l

**Result** : 11304

**UDP:** Command => tcpdump -n -r hw1.pcap udp | wc -l

**Result** : 18382

1.3 How many packets were exchanged between 192.168.0.200 and 91.189.90.40?  
 tcpdump -n -r hw1.pcap | grep "192.168.0.200" | grep "91.189.90.40" | wc -l

**Result** : 32

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

**Command** => tcpdump -n -r hw1.pcap | grep -v "ARP" | awk '{print $3}' | awk -F. '{print $1"."$2"."$3"."$4}' | sort -n | uniq

**Result** : 33

0.0.0.0

1.234.31.20

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

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

1.5 Print the unique private network (according to RFC1918) source IP  
 addresses found in the trace.

**Command** :

tcpdump -n -r hw1.pcap | grep "IP" | awk '{print $3}' | awk -F. '{ if($1==172 && $2 >= 16 && $2 <= 31)print " "$1"."$2"."$3"."$4; else if($1 == 192 || $1 == 10)print " "$1"."$2"."$3"."$4}' | sort -n | uniq -c

**Result** :

11890 192.168.0.1

164 192.168.0.10

3424 192.168.0.11

263 192.168.0.12

5 192.168.0.2

838 192.168.0.200

2684 192.168.0.3

104 192.168.0.5

10 192.168.0.6

387 192.168.0.7

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

**Command** => tcpdump -n -r hw1.pcap | grep -v "ARP" | awk '{print $5}' | awk -F. '{print $1"."$2"."$3"."$4}' | awk -F: '{print $1}' | sort -n | uniq | less

**Result** : 31

1.234.31.20

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

122.154.101.54

130.75.16.5

159.148.96.184

169.254.255.255

192.168.0.12

192.168.0.200

192.168.0.255

194.168.4.100

216.137.63.121

216.137.63.137

224.0.0.22

224.0.0.251

224.0.0.252

224.0.0.253

239.255.255.250

255.255.255.255

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

**Top-5 UDP port**

**Command :**

tcpdump -n -r hw1.pcap 'udp'| awk '{print $5}' | awk -F. '{print $5}' | awk -F: '{print $1}' |sort | uniq -c | sort -n -r | head -n 5 | awk '{print $2}'

**Result** :

**Port**

1900

137

5355

5353

138

**Top-5 TCP port**

**Command**:

tcpdump -n -r hw1.pcap tcp | awk '{print $5}'| awk -F. '{print $5}' | awk -F: '{print $1}' |sort -n | uniq -c | sort -n -r | head -n 5| awk '{print $2}'

**Result** :

80

54634

49836

47110

40341

1.8 How many TCP packets have the SYN flag set?

**Command** :

tcpdump -n -r hw1.pcap -i xl0 'tcp[13] & 2 == 2' | wc -l

**Result** : 75

1.9 How many TCP connection attempts were made?

**Command** :

**Total number of connection attempt should be equal to the number of Syn request.**

tcpdump -n -r hw1.pcap -i xl0 'tcp[13]==2' | wc -l

**Result** : 37

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

**Command** :

tcpdump -n -r hw1.pcap -i xl0 'tcp[13]==2' | awk '{print $5}' | awk -F. '{print $5}' | awk -F: '{print $1}'| sort -n | uniq -c | sort -n

Count : Port

1 443

1 465

2 9100

33 80

1.11 How many HTTP GET requests were made? Print the URLs of all HTTP requests  
 for JPG files.

**GET Request**

**Command:**

tcpdump -n -r hw1.pcap tcp | grep -i "HTTP: GET" | wc -l

**Result:**

94

**JPG Image Urls**

**Command:**

tcpdump -n -r hw1.pcap tcp | grep -i "HTTP: GET" | awk -F"GET" '{print $2}' | grep -i ".jpg" | awk -F'HTTP' '{print $1}'

**Result:**

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

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

**Command** :

**Min** => sudo tcpdump -n -r hw1.pcap -tttt | awk '{print $1 " "$2}' | sort -n | head -n 1

**Result**=> **2013-01-12 12:37:42.871346**

**Command** :

**Max** => sudo tcpdump -n -r hw1.pcap -tttt | awk '{print $1 " "$2}' | sort -n -r| head -n 1

**Result**=> **2013-01-14 14:27:03.691498**

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

**Command** :

tcpdump -n -r hw1.pcap -e | awk '{if($6 =="ARP" )print $2" "$12; else print $2" "$10;}' | awk -F. '{print $1"."$2"."$3"."$4}' | sort -n -k 1| uniq -c | sort -n -r | head -n 1

**Result** :

**Count Mac IP**

11890 c4:3d:c7:17:6f:9b 192.168.0.1

**Brand** **Netgear** [C4-3D-C7-00-00-00 - C4-3D-C7-FF-FF-FF] Mac range

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).

**Command** :

tcpdump -n -r hw1.pcap -e | awk '{print $9}' | awk -F: '{print $1}'| sort -n | uniq -c

**Result** :

24 42

1 54

12190 60

13 62

232 63

887 64

4 65

1046 66

8 68

6 69

3 70

1 72

87 74

8 75

6 76

2 77

4 79

54 81

52 82

43 84

4 85

14 87

5 88

4 89

13 90

341 91

1740 92

2 93

2 94

2 95

2 105

4 106

10 107

180 110

2 111

28 119

121 120

4 124

7 125

15 127

2 129

11 142

1 144

7 149

10 154

1 156

60 165

62 167

12 168

4 170

1 171

146 175

4 177

1 178

2 184

1 195

17 202

1 207

2 208

39 219

2 220

1 223

2 229

36 231

3 233

2 236

279 243

4 244

16 245

22 246

3 247

9 248

56 249

2 252

4 254

2 255

2 257

2 261

6 264

2 265

2 266

4 267

2 268

3 269

6 282

9 284

2 288

2 294

3 298

15 302

2 305

1 306

12 307

1 308

2 309

2 310

1 312

24 315

1 317

86 318

1 320

2 321

4 322

85 326

7 328

5 329

10 330

2773 331

10 332

6 333

1 335

88 338

2749 340

326 342

3 344

4 345

4 346

1 347

6 350

86 362

1 372

1 374

2 383

88 386

1 389

87 390

87 392

86 394

2759 395

1 396

85 398

2758 405

1 412

1 417

2 418

1 428

1 429

1 432

1 433

1 446

33 460

164 475

10 476

2 478

1 479

1 482

165 484

10 485

13 489

3 497

2 502

1 506

1 518

158 527

10 528

1 535

162 539

10 540

155 541

10 542

1 544

2 546

1 548

2 550

17 551

1 552

161 555

10 556

1 568

1 588

2 590

1 592

2 593

1 596

2 598

1 601

32 602

2 607

1 608

6 610

2 611

2 612

5 613

2 614

2 615

2 621

2 624

5 628

2 630

2 636

1 640

12 666

1 678

1 679

1 690

1 694

22 698

2 704

1 730

1 746

1 752

1 760

8 816

5 817

1 926

1 952

1 979

40 1033

6 1034

4 1035

1 1102

1 1162

1 1170

1 1179

2 1212

1 1218

1 1469

1034 1514