

Bil 452 – Ödev 5 NAT
Fatih Furkan Has
141101024

1-)

NAT_home_side.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl>F

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.100	10.119.240.64	SNMP	120	GetRequest 1.3.6.1.2.1.45.3.2.1.5.1.1.3.6.1.2.1.25.3.5.1.2.1
2	1.124997	192.168.1.100	68.87.71.230	DNS	91	Standard query 0xa9a9 A safebrowsing.clients.google.com
3	1.138265	68.87.71.230	192.168.1.100	DNS	211	Standard query response 0xa9a9 A safebrowsing.clients.google.com CNAME clients.1.google.com A 74.125.91.113 A 74.125.91.139 A 74.125.91.111 A 74.125.91.113
4	1.140302	192.168.1.100	74.125.91.113	TCP	66	4330 -> 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
5	1.207818	74.125.91.113	192.168.1.100	TCP	66	80 -> 4330 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM=1 WS=64
6	1.207873	192.168.1.100	74.125.91.113	TCP	54	4330 -> 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
7	1.208040	192.168.1.100	74.125.91.113	TCP	1035	4330 -> 80 [PSH, ACK] Seq=1 Ack=1 Win=260176 Len=981
8	1.259370	Cisco-Li_45:1f:1b	HonHaiPr_0d:ca:8f	ARP	60	Who has 192.168.1.100? Tell 192.168.1.1
9	1.259387	HonHaiPr_0d:ca:8f	Cisco-Li_45:1f:1b	ARP	42	192.168.1.100 is at 00:22:08:0d:ca:8f
10	1.269675	74.125.91.113	192.168.1.100	TCP	60	80 -> 4330 [ACK] Seq=1 Ack=982 Win=7744 Len=0
11	1.274062	74.125.91.113	192.168.1.100	TCP	853	80 -> 4330 [PSH, ACK] Seq=1 Ack=982 Win=7744 Len=799
12	1.474508	192.168.1.100	74.125.91.113	TCP	54	4330 -> 80 [ACK] Seq=982 Ack=800 Win=259376 Len=0
13	1.528648	74.125.91.113	192.168.1.100	TCP	853	[TCP Spurious Retransmission] 80 -> 4330 [PSH, ACK] Seq=1 Ack=982 Win=7744 Len=799
14	1.528672	192.168.1.100	74.125.91.113	TCP	54	[TCP Dup ACK 12x] 4330 -> 80 [ACK] Seq=982 Ack=800 Win=259376 Len=0
15	1.529354	192.168.1.100	68.87.71.230	DNS	89	Standard query 0x1773 A safebrowsing-cache.google.com
16	1.549501	68.87.71.230	192.168.1.100	DNS	140	Standard query response 0x1773 A safebrowsing-cache.google.com CNAME safebrowsing.cache.1.google.com A 74.125.106.31
17	1.550220	192.168.1.100	74.125.106.31	TCP	66	4331 -> 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
18	1.572197	74.125.106.31	192.168.1.100	TCP	66	80 -> 4331 [SYN, ACK] Seq=0 Ack=1 Win=5640 Len=0 MSS=1460 SACK_PERM=1 WS=64
19	1.572228	192.168.1.100	74.125.106.31	TCP	54	4331 -> 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
20	1.572315	192.168.1.100	74.125.106.31	TCP	767	4331 -> 80 [PSH, ACK] Seq=1 Ack=1 Win=260176 Len=713
21	1.601242	74.125.106.31	192.168.1.100	TCP	60	80 -> 4331 [ACK] Seq=1 Ack=714 Win=7296 Len=0

Frame 1: 120 bytes on wire (960 bits), 120 bytes captured (960 bits)

- Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:08:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:0b:45:1f:1b)
- Internet Protocol Version 4, Src: 192.168.1.100, Dst: 10.119.240.64
- User Datagram Protocol, Src Port: 1028, Dst Port: 161
- Simple Network Management Protocol

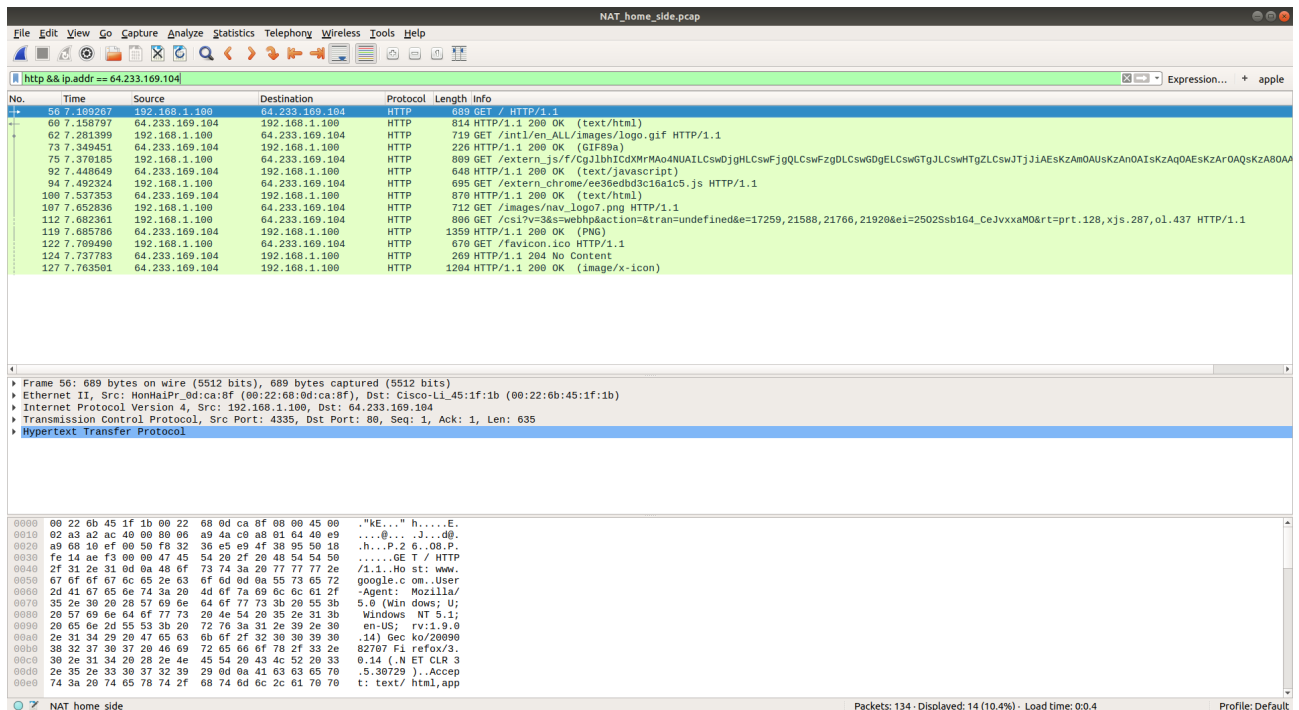
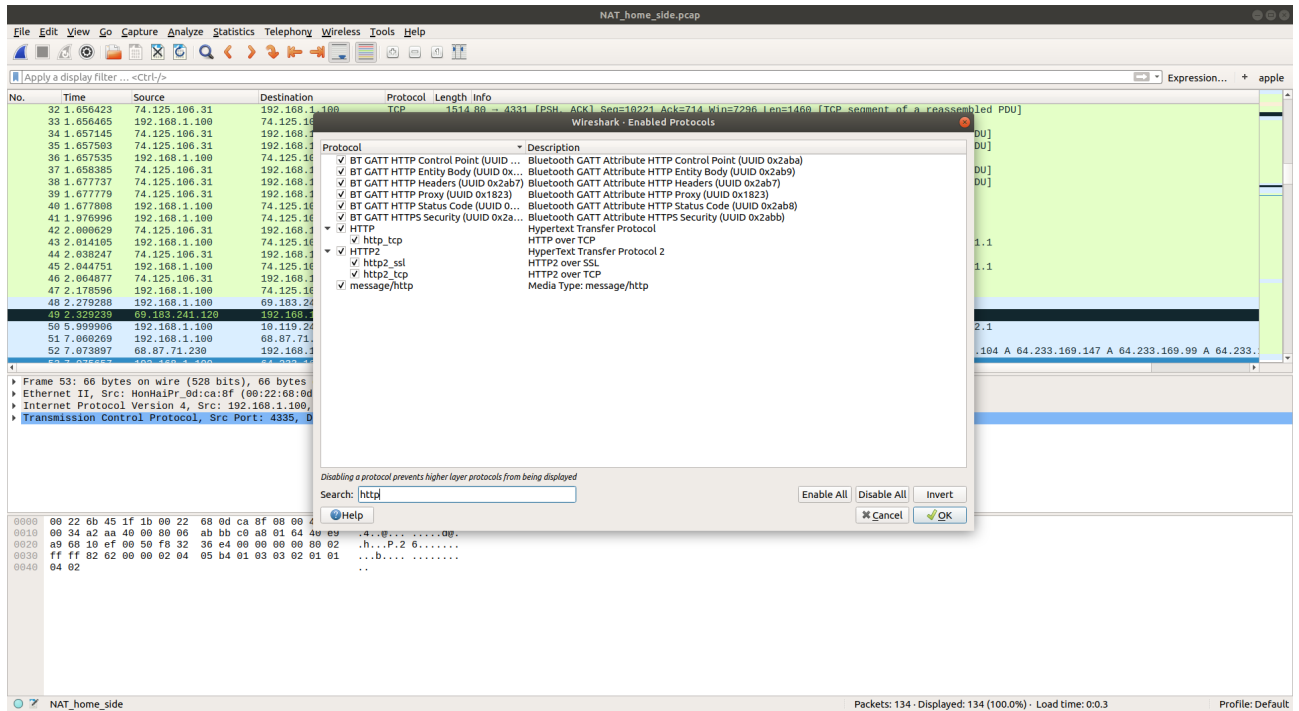
```
0000  00 22 0b 45 1f 1b 00 22  68 0d ca 8f 00 00 45 00  .".kE... h....E.
0010  00 6a a2 62 00 00 00 11  db 5c c0 a8 01 64 0a 77  .j.b....\...d.w
0020  f0 40 04 04 00 a1 00 56  00 36 30 4c 02 01 00 04  .@....V .60L...
0030  00 70 75 62 6c 69 63 a0  3f 02 02 29 51 02 01 00  .public. 7..)Q...
0040  02 01 00 30 33 30 0f 06  0b 2b 06 01 02 01 19 03  ..030..+.....
0050  02 01 05 01 05 00 30 0f  06 0b 2b 06 01 02 01 19  .....0..*.....
0060  03 05 01 01 01 05 00 30  0f 06 0b 2b 06 01 02 01  .....0..*+....
0070  19 03 05 01 02 01 05 00  .....
```

NAT_home_side Packets: 134 - Displayed: 134 (100.0%) - Load time: 0:0.3 Profile: Default

İstemcinin IP adresi: 192.168.1.100

2-)

http && ip.addr == 64.233.169.104 bu şekilde filtrelediğimde herhangi bir sonuca ulaşamadım ancak daha sonra Wireshark'ın enabled protocols kısmından http protokolünü aktif edince bu filtreleme işleminden sonuç alabildim.



3-)

Wireshark packet capture analysis of NAT_home_side.pcap. The packet list shows a GET request from 192.168.1.100 to 64.233.169.104 on port 88. The packet details pane shows the full structure of the Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol layers. The packet bytes pane shows the raw hex and ASCII data.

Epoch Time: 1253479387.378487888 seconds

- [Time delta from previous captured frame: 0.000214000 seconds]
- [Time delta from previous displayed frame: 0.000214000 seconds]
- [Time since reference or first frame: 7.109267000 seconds]

Frame Number: 56

Frame Length: 689 bytes (5512 bits)

Capture Length: 689 bytes (5512 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp:http]

[Coloring Rule Name: HTTP]

[Coloring Rule String: http || tcp.port == 80 || http2]

Ethernet II, Src: NonHapiPr_0d:ca:8f (00:22:08:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)

Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total length: 675

Identification: 0xa2ac (41644)

Flags: 0x02 (Don't Fragment)

Fragment offset: 0

Time to live: 128

Protocol: TCP (6)

Header checksum: 0xa9da (validation disabled)

[Header checksum status: Unverified]

Source: 192.168.1.100

Destination: 64.233.169.104

[Source GeoIP: Unknown]

[Destination GeoIP: United States, AS15169 Google LLC, United States, AS15169 Google LLC, 34.054401, -118.244003]

Transmission Control Protocol, Src Port: 4335, Dst Port: 88, Seq: 1, Ack: 1, Len: 635

Hypertext Transfer Protocol

0000 00 22 0b 45 1f 1b 00 22 68 0d ca 8f 08 00 45 00 . "kE..." h....E.

0010 02 a3 a2 ac 40 00 00 06 a9 da c0 a8 01 64 40 e9@... J...@.

0020 a9 08 10 ef 00 50 f8 32 36 e5 e9 4f 38 95 50 18 .h...P.2 6.08.P.

0030 fe 14 ae f3 00 00 47 45 54 20 2f 20 48 54 54 50GE T / HTTP

0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 72 e /i...Host: www.

0050 67 6f 6f 67 6c 65 2e 63 6f 6d 0d 0a 55 75 65 72 google.com>User

0060 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla/

Time relative to time reference or first frame (frame.time_relative)

Packets: 134 - Displayed: 134 (100.0%) - Load time: 0:0.6

Profile: Default

Source IP: 192.168.1.100
Source Port: 4335
Destination IP: 64.233.169.104
Destination Port: 88

4-)

Packet details view for packet 60 (HTTP GET) from 64.233.169.104 to 192.168.1.100. The packet is an HTTP GET request for /text/html. The TCP layer shows a sequence number of 2861 and an acknowledgment number of 636. The packet bytes pane shows the raw data of the HTTP request.

Time: 7.158797000 seconds
Source IP: 64.233.169.104
Source Port: 80
Destination IP: 192.168.1.100
Destination Port: 4335

Time: 7.158797000 seconds
Source IP: 64.233.169.104
Source Port: 80
Destination IP: 192.168.1.100
Destination Port: 4335

5-)

SYN

The image shows a Wireshark packet capture titled "NAT_home_side.pcap". The packet list pane at the top shows several packets. Packet 53, at time 7.075657, is a TCP SYN packet from source 192.168.1.100 to destination 64.233.169.104 on port 80. This packet is highlighted with a red box. The packet details pane below shows the structure of this packet, with several fields also highlighted by red boxes: "Frame Number: 53", "Header checksum status: Unverified", "Source: 192.168.1.100", "Destination: 64.233.169.104", and "Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0". The packet bytes pane at the bottom shows the raw data of the packet. A large text overlay "Get request'ten önceki SYN" is positioned over the packet details pane.

Epoch Time: 1253479387.344792000 seconds
[Time delta from previous captured frame: 0.001760000 seconds]
[Time delta from previous displayed frame: 0.001760000 seconds]
[Time since reference or first frame: 7.075657000 seconds]
Frame Number: 53
Frame Length: 60 bytes (528 bits)
Capture Length: 66 bytes (528 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:08:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:0b:45:1f:1b)
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 52
Identification: 0xa2aa (41642)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 120
Protocol: TCP (6)
Header checksum: 0xabbb (validation disabled)
[Header checksum status: Unverified]
Source: 192.168.1.100
Destination: 64.233.169.104
[Source GeoIP: Unknown]
[Destination GeoIP: United States, AS15109 Google LLC, United States, AS15109 Google LLC, 34.854481, -110.244003]
Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0
0000 00 22 0b 45 1f 1b 00 22 08 0d ca 8f 08 00 45 00 ..KE... h.....E.
0010 00 34 a2 aa 00 00 00 00 ab bb c0 a0 01 04 40 e9 ..4..@... ..00.
0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00P..2 6.....
0030 ff ff 82 62 00 00 02 04 05 b4 01 03 03 02 01 01 ...b.....
0040 04 02 ..

Time: 7.075657000 seconds

Source IP: 192.168.1.100

Source IP: 4335

Destination IP: 64.233.169.104

Destination Port: 80

SYN ACK

The image shows a Wireshark packet capture window titled "NAT_home_side.pcap". The packet list on the left shows several packets, with packet 54 selected. The packet details pane on the right shows the following information:

- Frame Number: 54
- Frame Length: 66 bytes (528 bits)
- Capture Length: 66 bytes (528 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: eth:ethertype:ip:tcp]
- [Coloring Rule Name: HTTP]
- [Coloring Rule String: http || tcp.port == 80 || http2]
- Ethernet II, Src: Ciscoc-Li_45:1f:1b (08:22:0b:45:1f:1b), Dst: HonHaiPr_0d:ca:8f (08:22:68:0d:ca:8f)
- Internet Protocol Version 4, Src: 64.233.169.104, Dst: 192.168.1.100
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
 - Total Length: 52
 - Identification: 0xf61a (63002)
 - Flags: 0x00
 - Fragment offset: 0
 - Time to live: 50
 - Protocol: TCP (6)
 - Header checksum: 0xe62b [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 64.233.169.104
 - Destination: 192.168.1.100
 - [Source GeoIP: United States, AS15169 Google LLC, United States, AS15169 Google LLC, 34.054401, -118.244003]
 - [Destination GeoIP: Unknown]
- Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 0, Ack: 1, Len: 0

The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII:

```
0000 08 22 08 0d ca 8f 08 22 6b 45 1f 1b 08 00 45 20  "h..." KE...E
0010 00 34 f6 1a 00 00 32 00 e6 2b 40 e9 a9 08 c9 a8  .A...2..+H.h..
0020 01 64 00 50 10 ef e9 4f 38 94 f8 32 36 e5 00 12  .d.P...0 8..26...
0030 16 58 4a 2f 00 00 02 04 05 96 01 01 04 02 01 03  .XJ/.....
0040 03 06                                     **
```

Time: 7.108986000 seconds
Source IP: 64.233.169.104
Source Port: 80
Destination IP: 192.168.1.100
Destination Port: 4335

6-)

Time: 6.069168000 seconds
Source IP: 71.192.34.104
Source Port: 4335
Destination IP: 64.233.169.104
Destination Port: 80

3. soruyla karşılaştırdığımızda sadece Source IP değişmiştir.

7-)

Home Side

Wireshark capture of NAT traffic from Home Side. The packet list shows an HTTP GET request from 192.168.1.100 to 64.233.169.104. The packet details pane shows the IP header, ICMP, and TCP segments. The packet bytes pane shows the raw data.

Frame 56: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits) on Ethernet II, Src: HonHaiPr-0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li-45:1f:1b (08:2d:6b:45:1f:1b)

Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total length: 675
Identification: 0xa2ac (41644)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0xa94a [validation disabled]
Header checksum status: Unverified
Source: 192.168.1.100
Destination: 64.233.169.104
[Source GeoIP: Unknown]
[Destination GeoIP: United States, AS15169 Google LLC, United States, AS15169 Google LLC, 34.054401, -118.244003]
Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
Hypertext Transfer Protocol

0000 00 2d 6b 45 1f 1b 00 22 68 0d ca 8f 08 00 15 00 .".KE..." h.....
0010 02 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..P.....
0020 a9 03 10 ef 00 50 f8 32 36 e5 e9 4f 38 95 50 18P.2 6..08.P..
0030 fe 14 ae f3 00 00 47 45 54 20 2f 20 48 54 54 50GE T / HTTP
0040 2f 31 2e 31 0d 0e 40 6f 73 74 3a 20 77 77 77 2e /1.1..Ho st: www..
0050 67 6f 67 67 6c 65 2e 63 6f 6d 00 0a 55 73 65 72 google.c om..User
0060 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla/
0070 35 2e 30 20 28 57 69 6e 64 6f 77 73 3b 20 55 3b 5.0 (Win dows; U;
Packets: 134 - Displayed: 134 (100.0%) - Load time: 0:0.7 Profile: Default

ISP Side:

Wireshark capture of NAT traffic from ISP Side. The packet list shows an HTTP GET request from 71.192.34.104 to 64.233.169.104. The packet details pane shows the IP header, ICMP, and TCP segments. The packet bytes pane shows the raw data.

Frame 85: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits) on Ethernet II, Src: Dell-4f:36:23 (00:08:74:4f:36:23), Dst: Cisco bf:6c:01 (00:0e:d6:bf:6c:01)

Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total length: 675
Identification: 0xa2ac (41644)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 127
Protocol: TCP (6)
Header checksum: 0x022f [validation disabled]
Header checksum status: Unverified
Source: 71.192.34.104
Destination: 64.233.169.104
[Source GeoIP: United States, Florence, MA, AS7922 Comcast Cable Communications, LLC, United States, Florence, MA, AS7922 Comcast Cable Communications, LLC, 42.329399, -72.693901]
[Destination GeoIP: United States, AS15169 Google LLC, United States, AS15169 Google LLC, 34.054401, -118.244003]
Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
Hypertext Transfer Protocol

0000 00 0e d6 bf 6c 01 00 08 74 4f 36 23 08 00 15 001...t06#...
0010 02 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..P.....
0020 a9 03 10 ef 00 50 f8 32 36 e5 e9 4f 38 95 50 18P.2 6..08.P..
0030 fe 14 ae f3 00 00 47 45 54 20 2f 20 48 54 54 50GE T / HTTP
0040 2f 31 2e 31 0d 0e 40 6f 73 74 3a 20 77 77 77 2e /1.1..Ho st: www..
0050 67 6f 67 67 6c 65 2e 63 6f 6d 00 0a 55 73 65 72 google.c om..User

Packets: 210 - Displayed: 210 (100.0%) - Load time: 0:0.8 Profile: Default

Sadece checksum değişmiştir bunun sebebi de Source IP'nin değişmiş olmasıdır. Cihazların internete bağlanabilmesi için NAT, IP dönüşümü yapmaktadır. Burada da IP değiştiği için checksum değişmiştir.

8-)

Home Side

Wireshark capture of NAT traffic from Home Side. The packet list shows a reassembled TCP segment (Seq=636, Win=7040) and an HTTP GET request. The packet details pane shows the IP header (Source: 64.233.169.104, Destination: 192.168.1.100) and the HTTP request line (GET /intl/en_ALL/images/logo.gif HTTP/1.1). The packet bytes pane shows the raw data of the reassembled TCP segment.

ISP Side:

Wireshark capture of NAT traffic from ISP Side. The packet list shows a reassembled TCP segment (Seq=636, Win=7040) and an HTTP GET request. The packet details pane shows the IP header (Source: 64.233.169.104, Destination: 71.192.34.104) and the HTTP request line (GET /intl/en_ALL/images/logo.gif HTTP/1.1). The packet bytes pane shows the raw data of the reassembled TCP segment.

Time: 6.117570000 seconds

Source IP: 64.233.169.104

Source Port: 80

Destination IP: 71.192.34.104

Destination Port: 4335

Time to live ve header checksum değışmiştir.

9-)

Home Side

Time: 7.415726000 seconds
Source IP: 64.233.169.104
Destination IP: 192.168.1.100
Time to live değişmiştir (5. soruda 128 idi)

ISP Side

Time: 6.067775000 seconds
Source IP: 64.233.169.104
Destination IP: 71.192.34.104
Identification, Time to live (58 idi), Destination IP değişmiştir.

10-)

WAN (Outside) LAN (Local) IP Port IP Port 71.192.34.104 4335 192.168.1.100 4335

WAN		LAN	
IP	Port	IP	Port
71.192.34.104	4335	192.168.1.100	4335