

Davi Ventura Cardoso Perdigão - 82148

1- 192.168.1.100

```
▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: Dell_58:98:2a (00:21:7
  Sender IP address: 169.254.247.145
  Target MAC address: 00:00:00_00:00:00 (00:
  Target IP address: 192.168.1.101
```

2-

The image shows a Wireshark capture of network traffic from a file named NAT_home_side.pcap. The filter applied is http && ip.addr == 64.233.169.104. The packet list shows several HTTP requests from source 192.168.1.100 to destination 64.233.169.104. The selected packet (No. 56) is an HTTP GET request for / HTTP/1.1. The packet details pane shows the structure of the frame, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The packet bytes pane displays the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
56	7.109267	192.168.1.100	64.233.169.104	HTTP	689	GET / HTTP/1.1
60	7.158797	64.233.169.104	192.168.1.100	HTTP	814	HTTP/1.1 200 OK (tex
62	7.281399	192.168.1.100	64.233.169.104	HTTP	719	GET /intl/en_ALL/imag
73	7.349451	64.233.169.104	192.168.1.100	HTTP	226	HTTP/1.1 200 OK (GIF
75	7.370185	192.168.1.100	64.233.169.104	HTTP	809	GET /extern_js/f/CgJl
92	7.448649	64.233.169.104	192.168.1.100	HTTP	648	HTTP/1.1 200 OK (tex
94	7.492324	192.168.1.100	64.233.169.104	HTTP	695	GET /extern_chrome/ee
100	7.537353	64.233.169.104	192.168.1.100	HTTP	870	HTTP/1.1 200 OK (tex
107	7.652836	192.168.1.100	64.233.169.104	HTTP	712	GET /images/nav_logo7
112	7.682361	192.168.1.100	64.233.169.104	HTTP	806	GET /csi?v=3&s=webhp&
119	7.685786	64.233.169.104	192.168.1.100	HTTP	1359	HTTP/1.1 200 OK (PNG

Packet 56 details:

- Frame 56: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits) on interface
- Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: 192.168.1.100
- Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104
- Transmission Control Protocol, Src Port: 4335, Dst Port: 80
- Hypertext Transfer Protocol

Packet bytes:

```
0000 00 22 6b 45 1f 1b 00 22 68 0d ca 8f 08 00 4
0010 02 a3 a2 ac 40 00 80 06 a9 4a c0 a8 01 64 4
0020 a9 68 10 ef 00 50 f8 32 36 e5 e9 4f 38 95 5
0030 fe 14 ae f3 00 00 47 45 54 20 2f 20 48 54 5
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 7
0050 67 6f 6f 67 6c 65 2e 63 6f 6d 0d 0a 55 73 6
0060 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 6
0070 35 2e 30 20 28 57 69 6e 64 6f 77 73 3b 20 5
0080 20 57 69 6e 64 6f 77 73 20 4e 54 20 35 2e 3
0090 20 65 6e 2d 55 53 3b 20 72 76 3a 31 2e 39 2
00a0 2e 31 34 29 20 47 65 63 6b 6f 2f 32 30 30 3
00b0 38 32 37 30 37 20 46 69 72 65 66 6f 78 2f 3
00c0 30 2e 31 34 20 28 2e 4e 45 54 20 43 4c 52 2
00d0 2e 35 2e 33 30 37 32 39 29 0d 0a 41 63 63 6
```

3 -

IP ORIGEM: 192.168.1.1000

IP DESTINO: 64.233.169.104

PORTA ORIGEM: 4335

PORTA DESTINO: 80

```

Transmission Control Protocol, Src Port: 4335
  Source Port: 4335
  Destination Port: 80
  [Stream index: 2]
  [Conversation completeness: Incomplete,
  [TCP Segment Len: 635]
  Sequence Number: 1 (relative sequence
  Sequence Number (raw): 4164040421
  [Next Sequence Number: 636 (relative
  Acknowledgment Number: 1 (relative ac
  Acknowledgment number (raw): 3914283157
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
  Window: 65044
  [Calculated window size: 260176]
  [Window size scaling factor: 4]
  Checksum: 0x386d [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  [Timestamp]

```

4 -

```
✓ [ ] Reassembled TCP segments (3020 bytes).  
✓ Hypertext Transfer Protocol  
  > HTTP/1.1 200 OK\r\n  
    Date: Sun, 20 Sep 2009 20:43:07 GMT\r\n    Expires: -1\r\n    Cache-Control: private, max-age=0\r\n    Content-Type: text/html; charset=UTF-8\r\n    Content-Encoding: gzip\r\n    Server: gws\r\n  > Content-Length: 3417\r\n    \r\n    [HTTP response 1/5]  
    [Time since request: 0.048402000 seconds]  
    \[Request in frame: 85\]  
    \[Next request in frame: 93\]  
    \[Next response in frame: 103\]  
    [Request URI: http://www.google.com/]  
    Content-encoded entity body (gzip): 3417  
    File Data: 8468 bytes
```

5 -

SYN

IP DE ORIGEM 192.168.1.100

IP DE DESTINO: 64.233.169.104

PORTA ORIGEM: 4335

PORTA DESTINO: 80

ACK:

IP DE ORIGEM: 64.233.169.104

IP DE DESTINO: 192.168.1.100

PORTA ORIGEM: 80

PORTA DESTINO: 4335

6-

IP DE ORIGEM: 71.192.34.104

IP DE DESTINO: 64.233.169.104

PORTA ORIGEM: 4335

PORTA DESTINO: 80

TIME: 6.069

7 -

NAT_ISP_side.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
94	6.273849	64.233.169.104	71.192.34.104	TCP	309	80 → 4335 [PSH, ACK]
145	6.643434	64.233.169.104	71.192.34.104	TCP	309	80 → 4335 [PSH, ACK]
159	6.721914	64.233.169.104	71.192.34.104	TCP	312	80 → 4338 [PSH, ACK]
170	7.189872	73.160.28.1	255.255.255.255	DHCP	342	DHCP ACK - Trans
44	0.996890	74.125.106.31	71.192.34.104	HTTP	526	HTTP/1.1 200 OK (app
121	6.407366	64.233.169.104	71.192.34.104	HTTP	648	HTTP/1.1 200 OK (tex
38	0.636388	74.125.106.31	71.192.34.104	HTTP	651	HTTP/1.1 200 OK (app
154	6.669397	71.192.34.104	64.233.169.104	HTTP	670	GET /favicon.ico HTTP
85	6.069168	71.192.34.104	64.233.169.104	HTTP	689	GET / HTTP/1.1
125	6.452270	71.192.34.104	64.233.169.104	HTTP	695	GET /extern_chrome/ee
135	6.533219	71.192.34.104	74.125.91.113	HTTP	709	GET /generate_204 HTTP

> Frame 85: 689 bytes on wire (5512 bits), 689 by
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36
> Internet Protocol Version 4, Src: 71.192.34.104
✓ Transmission Control Protocol, Src Port: 4335,
Source Port: 4335
Destination Port: 80
[Stream index: 2]
[Conversation completeness: Incomplete, DATA
[TCP Segment Len: 635]
Sequence Number: 1 (relative sequence num
Sequence Number (raw): 4164040421
[Next Sequence Number: 636 (relative sequ

0020 a9 68 10 ef 00 50 f8 32 36 e5 e9 4f 38 95 5
0030 fe 14 38 6d 00 00 47 45 54 20 2f 20 48 54 5
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 7
0050 67 6f 6f 67 6c 65 2e 63 6f 6d 0d 0a 55 73 6
0060 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 6
0070 35 2e 30 20 28 57 69 6e 64 6f 77 73 3b 20 5
0080 20 57 69 6e 64 6f 77 73 20 4e 54 20 35 2e 3
0090 20 65 6e 2d 55 53 3b 20 72 76 3a 31 2e 39 2
00a0 2e 31 34 29 20 47 65 63 6b 6f 2f 32 30 30 3
00b0 38 32 37 30 37 20 46 69 72 65 66 6f 78 2f 3
00c0 30 2e 31 34 20 28 2e 4e 45 54 20 43 4c 52 2
00d0 2e 35 2e 33 30 37 32 39 29 0d 0a 41 63 63 6
00e0 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 7
00f0 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2

O Campo checksum mudou, ele é usado para verificar a integridade dos dados do pacote IP na transmissão.

NAT_home_side.pcap							
No.	Time	Source	Destination	Protocol	Length	Info	
113	7.684575	64.233.169.104	192.168.1.100	TCP	309	80 → 4335 [PSH, ACK]	
126	7.762993	64.233.169.104	192.168.1.100	TCP	312	80 → 4338 [PSH, ACK]	
44	2.038247	64.233.169.104	192.168.1.100	HTTP	526	HTTP/1.1 200 OK (app)	
92	7.448649	64.233.169.104	192.168.1.100	HTTP	648	HTTP/1.1 200 OK (tex)	
39	1.677779	74.125.106.31	192.168.1.100	HTTP	651	HTTP/1.1 200 OK (app)	
122	7.709490	192.168.1.100	64.233.169.104	HTTP	670	GET /favicon.ico HTTP	
56	7.100267	192.168.1.100	64.233.169.104	HTTP	689	GET / HTTP/1.1	
94	7.492324	192.168.1.100	64.233.169.104	HTTP	695	GET /extern_chrome/ee	
104	7.573305	192.168.1.100	74.125.91.113	HTTP	709	GET /generate_204 HTT	
107	7.652836	192.168.1.100	64.233.169.104	HTTP	712	GET /images/nav_logo7	
62	7.281399	192.168.1.100	64.233.169.104	HTTP	719	GET /intl/en_ALL/imag	

0101 = Header Length: 20 bytes (5)	0000 00 22 6b 45 1f 11 00 22 68 0d ca 8f 08 00 4
> Flags: 0x018 (PSH, ACK)	0010 02 a3 a2 ac 40 00 00 06 a9 4a c0 a8 01 64 4
Window: 65044	0020 a9 68 10 ef 00 50 f8 32 36 e5 e9 4f 38 95 1
[Calculated window size: 260176]	0030 fc 14 ae f3 00 00 47 45 54 20 2f 20 48 54 4
[Window size scaling factor: 4]	0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 7
Checksum: 0xaeaf [unverified]	0050 67 6f 6f 67 6c 65 2e 63 6f 6d 0a 55 73 6
[Checksum Status: Unverified]	0060 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 6
Urgent Pointer: 0	0070 35 2e 30 20 28 57 69 6e 64 6f 77 73 3b 20 1
> [Timestamps]	0080 20 57 69 6e 64 6f 77 73 20 4e 54 20 35 2e 1
> [SEQ/ACK analysis]	0090 20 65 6e 2d 55 53 30 20 72 76 3a 31 2e 39 2
> TCP payload (635 bytes)	00a0 2e 31 34 29 20 47 65 63 6b 6f 2f 32 30 30 1
> Hypertext Transfer Protocol	00b0 38 32 37 30 37 20 46 69 67 65 66 6f 78 2f 2
	00c0 30 2e 31 34 20 28 2e 4e 45 54 20 43 4c 52 2
	00d0 2e 35 2e 33 30 37 32 39 29 0d 0a 41 63 63 6

Acknowledgment Number: 1 (relative ack num	0010 02 a3 a2 ac 40 00 7f 06 02 2f 47 c0 22 68 4
Acknowledgment number (raw): 3914283157	0020 a9 68 10 ef 00 50 f8 32 36 e5 e9 4f 38 95 1
0101 = Header Length: 20 bytes (5)	0030 fe 14 30 6d 00 00 47 45 54 20 2f 20 48 54 4
> Flags: 0x018 (PSH, ACK)	0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 7
Window: 65044	0050 67 6f 6f 67 6c 65 2e 63 6f 6d 0a 55 73 6
[Calculated window size: 260176]	0060 35 2e 30 20 28 57 69 6e 64 6f 77 73 3b 20 1
[Window size scaling factor: 4]	0070 20 57 69 6e 64 6f 77 73 20 4e 54 20 35 2e 1
Checksum: 0x386d [unverified]	0080 20 65 6e 2d 55 53 30 20 72 76 3a 31 2e 39 2
[Checksum Status: Unverified]	0090 2e 31 34 29 20 47 65 63 6b 6f 2f 32 30 30 1
Urgent Pointer: 0	00a0 38 32 37 30 37 20 46 69 67 72 65 66 6f 78 2f 2
> [Timestamps]	00b0 30 2e 31 34 20 28 2e 4e 45 54 20 43 4c 52 2
> [SEQ/ACK analysis]	00c0 2e 35 2e 33 30 37 32 39 29 0d 0a 41 63 63 6
	00d0 74 3a 20 74 65 78 2f 68 74 6d 6c 2c 61 6

8 -

IP DE ORIGEM: 74.125.91.113

IP DE DESTINO: 71.192.34.104

PORTA ORIGEM: 80

PORTA DESTINO: 4330

As portas permanecem com os mesmos valores.

O ip de origem,destino mudou em relação ao do arquivo NAT_home_side

NAT_home_side.pcap							
No.	Time	Source	Destination	Protocol	Length	Info	
1	0.000000	192.168.1.100	10.119.240.64	SNMP	120	get-request 1.3.6.1.2	
2	1.124897	192.168.1.100	68.87.71.230	DNS	91	Standard query 0xa9a9	
3	1.138265	68.87.71.230	192.168.1.100	DNS	211	Standard query respon	
4	1.140302	192.168.1.100	74.125.91.113	TCP	66	4330 → 80 [SYN] Seq=0	
5	1.207818	74.125.91.113	192.168.1.100	TCP	66	80 → 4330 [SYN, ACK]	
6	1.207873	192.168.1.100	74.125.91.113	TCP	54	4330 → 80 [ACK] Seq=1	
7	1.208040	192.168.1.100	74.125.91.113	HTTP	1035	POST /safebrowsing/d	
8	1.259370	Cisco-Li_45:1f:1b	HonHaiPr_0d:ca:8f	ARP	60	who has 192.168.1.100	
9	1.259387	HonHaiPr_0d:ca:8f	Cisco-Li_45:1f:1b	ARP	42	192.168.1.100 is at 0	
10	1.269675	74.125.91.113	192.168.1.100	TCP	60	80 → 4330 [ACK] Seq=1	
11	1.274062	74.125.91.113	192.168.1.100	HTTP	853	HTTP/1.1 200 OK (app)	

> Frame 11: 853 bytes on wire (6824 bits), 853 by	0000 00 22 68 0d ca 8f 00 22 6b 45 1f 1b 00 00 4
> Ethernet II, Src: Cisco-Li_45:1f:1b (00:22:6b:4	0010 03 47 63 53 00 00 33 06 b9 43 4a 7d 5b 71 4
> Internet Protocol Version 4, Src: 74.125.91.113	0020 01 64 00 50 10 ea a1 83 00 24 38 ca bc d5 1
> Transmission Control Protocol, Src Port: 80, Ds	0030 00 79 a7 ff 00 00 4a 53 54 50 2f 31 2e 31 2
Source Port: 80	0040 30 20 20 4f 4b 0d 0a 43 6f 6e 74 65 20 74 4
Destination Port: 4330	0050 79 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6
[Stream index: 0]	0060 2f 76 6e 64 2e 67 6f 6f 67 6c 65 2e 73 61 6
[Conversation completeness: Incomplete, DATA	0070 62 72 6f 77 73 69 6e 67 2d 75 70 64 61 74 6
[TCP Segment Len: 799]	0080 0a 44 61 74 65 3a 20 53 75 6e 2c 20 32 30 3
Sequence Number: 1 (relative sequence num	0090 65 70 20 32 30 30 39 20 32 30 3a 33 33 3a 3
Sequence Number (raw): 2709749796	00a0 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 4
[Next Sequence Number: 800 (relative sequ	00b0 75 6e 6b 65 64 20 55 70 64 61 74 65 20 53 6
	00c0 67 65 72 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 6
	00d0 67 74 68 3a 20 36 33 33 0d 0a 0d 0a 6d 3a 2

> Frame 9: 853 bytes on wire (6824 bits), 853 byt	0010 03 47 63 53 00 00 34 06 10 28 4a 7d 5b 71 4
> Ethernet II, Src: Cisco_bf:6c:01 (00:0e:0d:bf:6	0020 22 68 00 50 10 ea a1 83 80 24 38 ca bc d5 1
> Internet Protocol Version 4, Src: 74.125.91.113	0030 00 79 ff e3 00 00 48 54 54 50 2f 31 2e 31 2
> Transmission Control Protocol, Src Port: 80, Ds	0040 30 30 20 4f 4b 0d 0a 43 6f 6e 74 65 6e 74 4
Source Port: 80	0050 79 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6
Destination Port: 4330	0060 2f 76 6e 64 2e 67 6f 6f 67 6c 65 2e 73 61 6
[Stream index: 0]	0070 62 72 6f 77 73 69 6e 67 2d 75 70 64 61 74 6
[Conversation completeness: Incomplete, DATA	0080 0a 44 61 74 65 3a 20 53 75 6e 2c 20 32 30 3
[TCP Segment Len: 799]	0090 65 70 20 32 30 30 39 20 32 30 3a 33 33 3a 3
Sequence Number: 1 (relative sequence num	00a0 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 4
Sequence Number (raw): 2709749796	00b0 75 6e 6b 65 64 20 55 70 64 61 74 65 20 53 6
[Next Sequence Number: 800 (relative sequ	00c0 76 65 72 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 6
	00d0 67 74 68 3a 20 36 33 33 0d 0a 0d 0a 6d 3a 2
	00e0 33 76 34 59 42 63 6c 50 75 44 67 65 65 49 1

```
Header Checksum: 0x4941 [validation disabled]
[Header checksum status: Unverified]
Source Address: 71.192.34.104
Destination Address: 74.125.91.113
Transmission Control Protocol, Src Port: 4330
  Source Port: 4330
  Destination Port: 80
  [Stream index: 0]
  [Conversation completeness: Incomplete,
  [TCP Segment Len: 0]
  Sequence Number: 0      (relative sequence number)
  Sequence Number (raw): 952809727
  [Next Sequence Number: 1      (relative sequence number)
  Acknowledgment Number: 0
  Acknowledgment number (raw): 0
  1000 .... = Header Length: 32 bytes (8)
> Flags: 0x002 (SYN)
Window: 65535
```