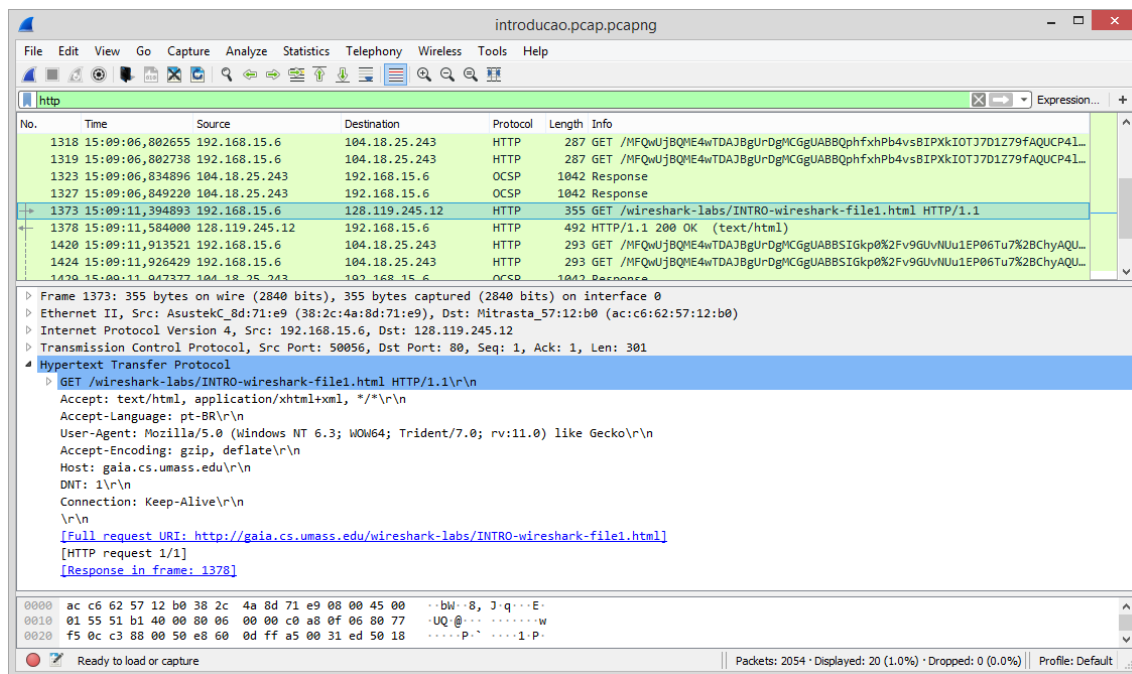


Trabalho Wireshark

Adhonay Júnior - 504656

Wireshark Lab: Iniciando

- 1) UDP, ICMPv6, TCP, IGMPv2, DNS, GQUIC, ARP, SSDP, TLSv1.2, NBNS, ICMP.
- 2) 15:09:11,394893 até 15:09:11,584000, 0.189107 segundos
- 3) IP do site gaia.cs.umass.edu : 128.119.245.12, IP da interface : 192.168.15.6
- 4)



Wireshark Lab: HTTP

1) Navegador e Servidor : HTTP 1.1

The image displays two screenshots of the Wireshark network protocol analyzer, showing an HTTP 1.1 session. The top screenshot shows a packet capture of a GET request, and the bottom screenshot shows the corresponding 200 OK response.

Top Screenshot: HTTP GET Request

The packet list shows a GET request (Frame 36) from 192.168.15.6 to 128.119.245.12. The packet details pane shows the Hypertext Transfer Protocol section with the following fields:

- GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
- [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
- Request Method: GET
- Request URI: /wireshark-labs/HTTP-wireshark-file1.html
- Request Version: HTTP/1.1
- Host: gaia.cs.umass.edu\r\n
- Connection: keep-alive\r\n
- Upgrade-Insecure-Requests: 1\r\n
- User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36\r\n
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
- Accept-Encoding: gzip, deflate\r\n
- Accept-Language: pt-BR;pt;q=0.9,en-US;q=0.8,en;q=0.7\r\n

The packet bytes pane shows the raw data of the request, including the "n: keep-alive" and "pgrade-I nsecure-Requests : 1" fields.

Bottom Screenshot: HTTP 200 OK Response

The packet list shows a 200 OK response (Frame 40) from 128.119.245.12 to 192.168.15.6. The packet details pane shows the Hypertext Transfer Protocol section with the following fields:

- HTTP/1.1 200 OK\r\n
- [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
- Response Version: HTTP/1.1
- Status Code: 200
- [Status Code Description: OK]
- Response Phrase: OK
- Date: Sat, 09 Mar 2019 21:38:24 GMT\r\n
- Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
- Last-Modified: Sat, 09 Mar 2019 06:59:01 GMT\r\n
- Etag: "80-583a3dfd4b297"\r\n
- Accept-Ranges: bytes\r\n
- Content-Length: 128\r\n
- Keep-Alive: timeout=5, max=100\r\n

The packet bytes pane shows the raw data of the response, including the "3" and "q" fields.

2) pt-BR, en-US

The screenshot shows a Wireshark capture of an HTTP transaction. The packet list on the left shows a GET request (packet 36) and a 200 OK response (packet 40). The packet details pane for packet 40 is expanded, showing the Hypertext Transfer Protocol section. The 'Accept-Language' header is highlighted with a red circle, showing 'pt-BR;q=0.9,en-US;q=0.8,en;q=0.7'. The packet bytes pane at the bottom shows the raw data of the response.

No.	Time	Source	Destination	Protocol	Length	Info
28	18:38:22,271045	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
36	18:38:25,014371	192.168.15.6	128.119.245.12	HTTP	500	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
40	18:38:25,183844	128.119.245.12	192.168.15.6	HTTP	540	HTTP/1.1 200 OK (text/html)

Packet 40 details:

- GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
- Host: gaia.cs.umass.edu\r\n
- Connection: keep-alive\r\n
- Upgrade-Insecure-Requests: 1\r\n
- User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36\r\n
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
- Accept-Encoding: gzip, deflate\r\n
- Accept-Language: pt-BR;q=0.9,en-US;q=0.8,en;q=0.7\r\n

Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

HTTP request 1/1

Response in frame: 40

3) Computador : 192.168.15.6 Servidor: 128.119.245.12

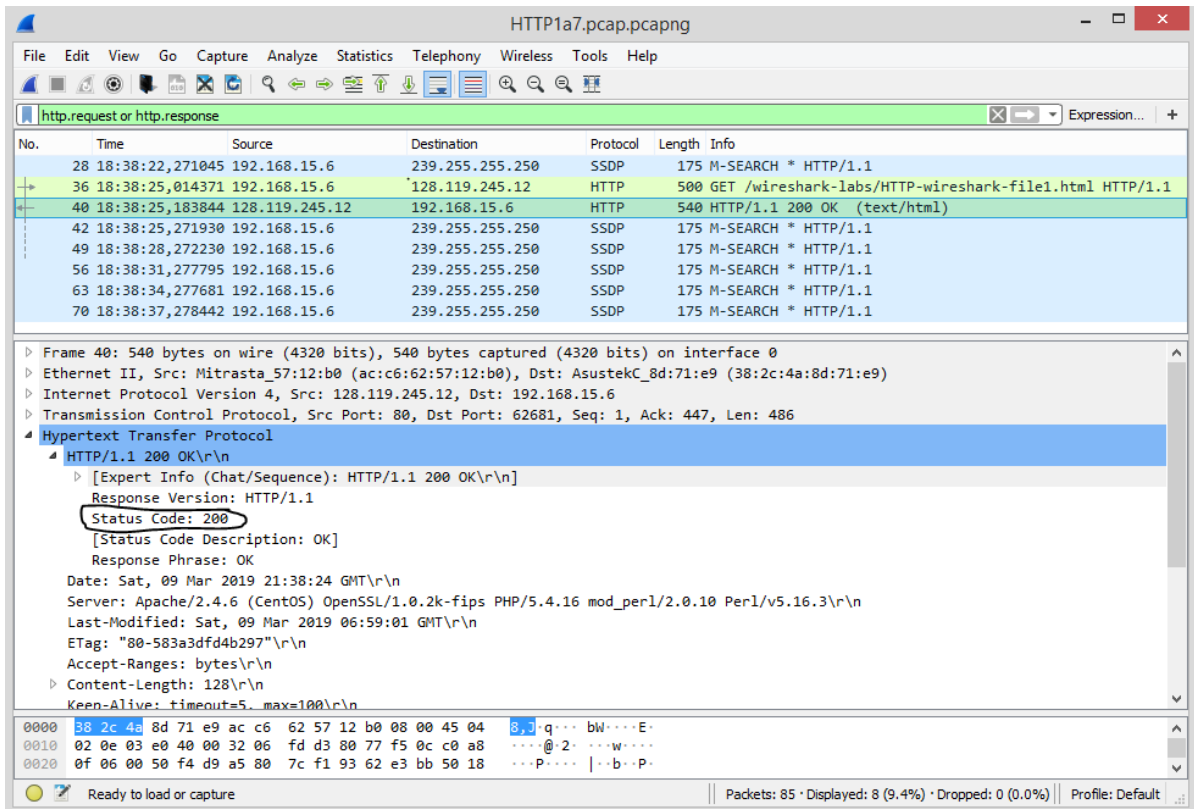
The screenshot shows a Wireshark capture of an HTTP transaction. The packet list on the left shows a GET request (packet 36) and a 200 OK response (packet 40). The packet details pane for packet 40 is expanded, showing the Hypertext Transfer Protocol section. The 'HTTP/1.1 200 OK' status line is highlighted with a red circle. The packet bytes pane at the bottom shows the raw data of the response.

No.	Time	Source	Destination	Protocol	Length	Info
28	18:38:22,271045	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
36	18:38:25,014371	192.168.15.6	128.119.245.12	HTTP	500	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
40	18:38:25,183844	128.119.245.12	192.168.15.6	HTTP	540	HTTP/1.1 200 OK (text/html)

Packet 40 details:

- HTTP/1.1 200 OK\r\n
- [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
- Response Version: HTTP/1.1
- Status Code: 200
- [Status Code Description: OK]
- Response Phrase: OK
- Date: Sat, 09 Mar 2019 21:38:24 GMT\r\n
- Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
- Last-Modified: Sat, 09 Mar 2019 06:59:01 GMT\r\n
- ETag: "80-583a3dfd4b297"\r\n
- Accept-Ranges: bytes\r\n
- Content-Length: 128\r\n
- Keep-Alive: timeout=5, max=100\r\n

4) 200 OK



The image shows a Wireshark capture of an HTTP 200 OK response. The packet list on the left shows a packet at time 18:38:25.183844 from source 128.119.245.12 to destination 192.168.15.6, protocol HTTP, length 540 bytes. The packet details pane on the right shows the Hypertext Transfer Protocol section with status code 200 OK. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
28	18:38:22,271045	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
36	18:38:25,014371	192.168.15.6	128.119.245.12	HTTP	500	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
40	18:38:25,183844	128.119.245.12	192.168.15.6	HTTP	540	HTTP/1.1 200 OK (text/html)
42	18:38:25,271930	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
49	18:38:28,272230	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
56	18:38:31,277795	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
63	18:38:34,277681	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
70	18:38:37,278442	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1

Frame 40: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0

Ethernet II, Src: Mitrasta_57:12:b0 (ac:c6:62:57:12:b0), Dst: AsustekC_8d:71:e9 (38:2c:4a:8d:71:e9)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.15.6

Transmission Control Protocol, Src Port: 80, Dst Port: 62681, Seq: 1, Ack: 447, Len: 486

Hypertext Transfer Protocol

- HTTP/1.1 200 OK\r\n
 - [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
 - Response Version: HTTP/1.1
 - Status Code: 200
 - [Status Code Description: OK]
 - Response Phrase: OK
 - Date: Sat, 09 Mar 2019 21:38:24 GMT\r\n
 - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
 - Last-Modified: Sat, 09 Mar 2019 06:59:01 GMT\r\n
 - Etag: "80-583a3dfd4b297"\r\n
 - Accept-Ranges: bytes\r\n
 - Content-Length: 128\r\n
 - Keep-Alive: timeout=5, max=100\r\n

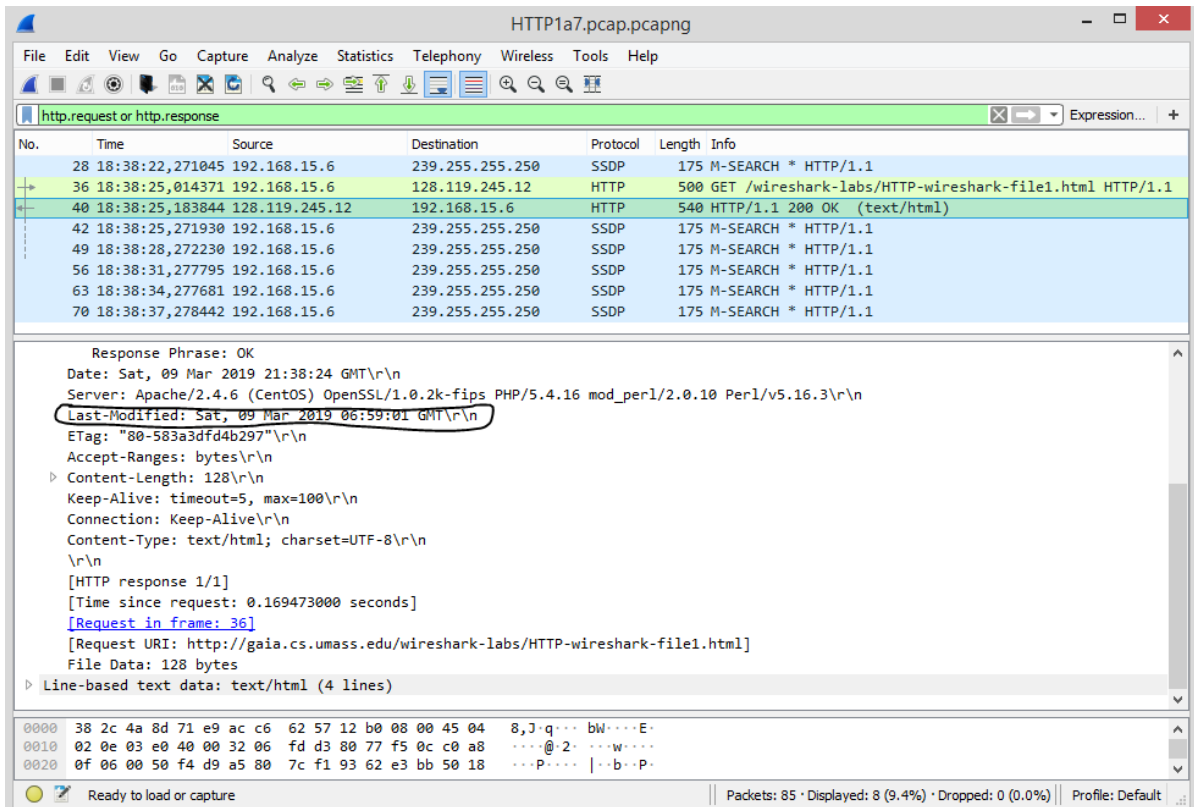
0000 38 2c 4a 8d 71 e9 ac c6 62 57 12 b0 08 00 45 04 8, J · q · · · b W · · · · E ·

0010 02 0e 03 e0 40 00 32 06 fd d3 80 77 f5 0c c0 a8 · · · · @ · 2 · · · w · · · ·

0020 0f 06 00 50 f4 d9 a5 80 7c f1 93 62 e3 bb 50 18 · · · P · · · · | · · b · P ·

Ready to load or capture | Packets: 85 · Displayed: 8 (9.4%) · Dropped: 0 (0.0%) | Profile: Default

5) 09 de Março de 2019 as 06:59:01 horas



The image shows a Wireshark capture of an HTTP 200 OK response. The packet list on the left shows a packet at time 18:38:25.183844 from source 128.119.245.12 to destination 192.168.15.6, protocol HTTP, length 540 bytes. The packet details pane on the right shows the Hypertext Transfer Protocol section with status code 200 OK. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
28	18:38:22,271045	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
36	18:38:25,014371	192.168.15.6	128.119.245.12	HTTP	500	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
40	18:38:25,183844	128.119.245.12	192.168.15.6	HTTP	540	HTTP/1.1 200 OK (text/html)
42	18:38:25,271930	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
49	18:38:28,272230	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
56	18:38:31,277795	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
63	18:38:34,277681	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
70	18:38:37,278442	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1

Response Phrase: OK

Date: Sat, 09 Mar 2019 21:38:24 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n

Last-Modified: Sat, 09 Mar 2019 06:59:01 GMT\r\n

Etag: "80-583a3dfd4b297"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 128\r\n

Keep-Alive: timeout=5, max=100\r\n

Connection: Keep-Alive\r\n

Content-Type: text/html; charset=UTF-8\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.169473000 seconds]

[Request in frame: 36]

[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]

File Data: 128 bytes

Line-based text data: text/html (4 lines)

0000 38 2c 4a 8d 71 e9 ac c6 62 57 12 b0 08 00 45 04 8, J · q · · · b W · · · · E ·

0010 02 0e 03 e0 40 00 32 06 fd d3 80 77 f5 0c c0 a8 · · · · @ · 2 · · · w · · · ·

0020 0f 06 00 50 f4 d9 a5 80 7c f1 93 62 e3 bb 50 18 · · · P · · · · | · · b · P ·

Ready to load or capture | Packets: 85 · Displayed: 8 (9.4%) · Dropped: 0 (0.0%) | Profile: Default

6) 128 Bytes

The screenshot shows a Wireshark capture of an HTTP response. The packet list pane at the top shows a packet of length 540 bytes (HTTP/1.1 200 OK (text/html)). The packet details pane shows the response structure, including the status line, headers, and the body. The body is a line-based text data (text/html) with 4 lines. The packet bytes pane shows the raw data of the response, which is 540 bytes long. The status bar at the bottom indicates that 85 packets are displayed, with 8 (9.4%) displayed and 0 (0.0%) dropped.

No.	Time	Source	Destination	Protocol	Length	Info
28	18:38:22,271045	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
36	18:38:25,014371	192.168.15.6	128.119.245.12	HTTP	500	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
40	18:38:25,183844	128.119.245.12	192.168.15.6	HTTP	540	HTTP/1.1 200 OK (text/html)
42	18:38:25,271930	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
49	18:38:28,272230	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
56	18:38:31,277795	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
63	18:38:34,277681	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
70	18:38:37,278442	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1

Response Phrase: OK
Date: Sat, 09 Mar 2019 21:38:24 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
Last-Modified: Sat, 09 Mar 2019 06:59:01 GMT\r\n
ETag: "80-583a3dfd4b297"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 128\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.169473000 seconds]
[Request in frame: 36]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
File Data: 128 bytes
Line-based text data: text/html (4 lines)

0000 38 2c 4a 8d 71 e9 ac c6 62 57 12 b0 08 00 45 04 8,J·q···bW····E·
0010 02 0e 03 e0 40 00 32 06 fd d3 80 77 f5 0c c0 a8 ····@·2····w····
0020 0f 06 00 50 f4 d9 a5 80 7c f1 93 62 e3 bb 50 18 ···P····|··b·P·

Ready to load or capture | Packets: 85 · Displayed: 8 (9.4%) · Dropped: 0 (0.0%) | Profile: Default

7) Não, não vejo nenhum cabeçalho.

The screenshot shows a Wireshark capture of an HTTP response. The packet list pane at the top shows a packet of length 500 bytes (HTTP/1.1 200 OK (text/html)). The packet details pane shows the response structure, including the status line, headers, and the body. The body is a line-based text data (text/html) with 4 lines. The packet bytes pane shows the raw data of the response, which is 500 bytes long. The status bar at the bottom indicates that 85 packets are displayed, with 8 (9.4%) displayed and 0 (0.0%) dropped.

No.	Time	Source	Destination	Protocol	Length	Info
28	18:38:22,271045	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
36	18:38:25,014371	192.168.15.6	128.119.245.12	HTTP	500	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
40	18:38:25,183844	128.119.245.12	192.168.15.6	HTTP	540	HTTP/1.1 200 OK (text/html)
42	18:38:25,271930	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
49	18:38:28,272230	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
56	18:38:31,277795	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
63	18:38:34,277681	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
70	18:38:37,278442	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1

Frame 36: 500 bytes on wire (4000 bits), 500 bytes captured (4000 bits) on interface 0
Ethernet II, Src: AsustekC_8d:71:e9 (38:2c:4a:8d:71:e9), Dst: Mitrasta_57:12:b0 (ac:c6:62:57:12:b0)
Internet Protocol Version 4, Src: 192.168.15.6, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 62681, Dst Port: 80, Seq: 1, Ack: 1, Len: 446

0000 ac c6 62 57 12 b0 38 2c 4a 8d 71 e9 08 00 45 00 ···bW····8,J·q···E·
0010 01 e6 51 cd 40 00 00 06 00 00 c0 a8 0f 06 80 77 ···Q·@··········w····
0020 f5 0c f4 d9 00 50 93 62 e1 fd a5 80 7c f1 50 18 ····P·b····|·P·
0030 01 02 47 0b 00 00 47 45 54 20 2f 77 69 72 65 73 ···G··GE T /wires
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 hark-lab s/HTTP-w
0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68 ireshark -file1.h
0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f tml HTTP /1.1·Ho
0070 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 st: gaia .cs.umas
0080 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f s.edu··C connectio
0090 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 n: keep-alive··U
00a0 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d pgrade-I nsecure-
00b0 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 Requests : 1··Use
00c0 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 r-Agent: Mozilla
00d0 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 /5.0 (Wi ndows NT
00e0 20 36 2e 33 3b 20 57 69 6e 36 34 3b 20 78 36 34 6.3; Wi n64; x64

HTTP1a7.pcap.pcapng | Packets: 85 · Displayed: 8 (9.4%) | Profile: Default

8) Não

The screenshot shows a Wireshark capture of an HTTP transaction. The packet list pane displays several packets, with packet 825 selected. The packet details pane shows the structure of the HTTP response, including the status line '200 OK (text/html)'. The packet bytes pane shows the raw data of the response, which is a 784-byte HTML document. The status bar at the bottom indicates that 12 packets are displayed out of 1284 total packets.

No.	Time	Source	Destination	Protocol	Length	Info
735	19:13:53,215633	192.168.15.6	128.119.245.12	HTTP	500	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
825	19:13:53,406184	128.119.245.12	192.168.15.6	HTTP	784	HTTP/1.1 200 OK (text/html)

9) Sim, pelo código de retorno 200 com o File Data e o texto equivalente.

The screenshot shows a Wireshark capture of an HTTP transaction, similar to the one above. The packet list pane displays several packets, with packet 825 selected. The packet details pane shows the structure of the HTTP response, including the status line '200 OK (text/html)'. The packet bytes pane shows the raw data of the response, which is a 784-byte HTML document. The status bar at the bottom indicates that 12 packets are displayed out of 1284 total packets.

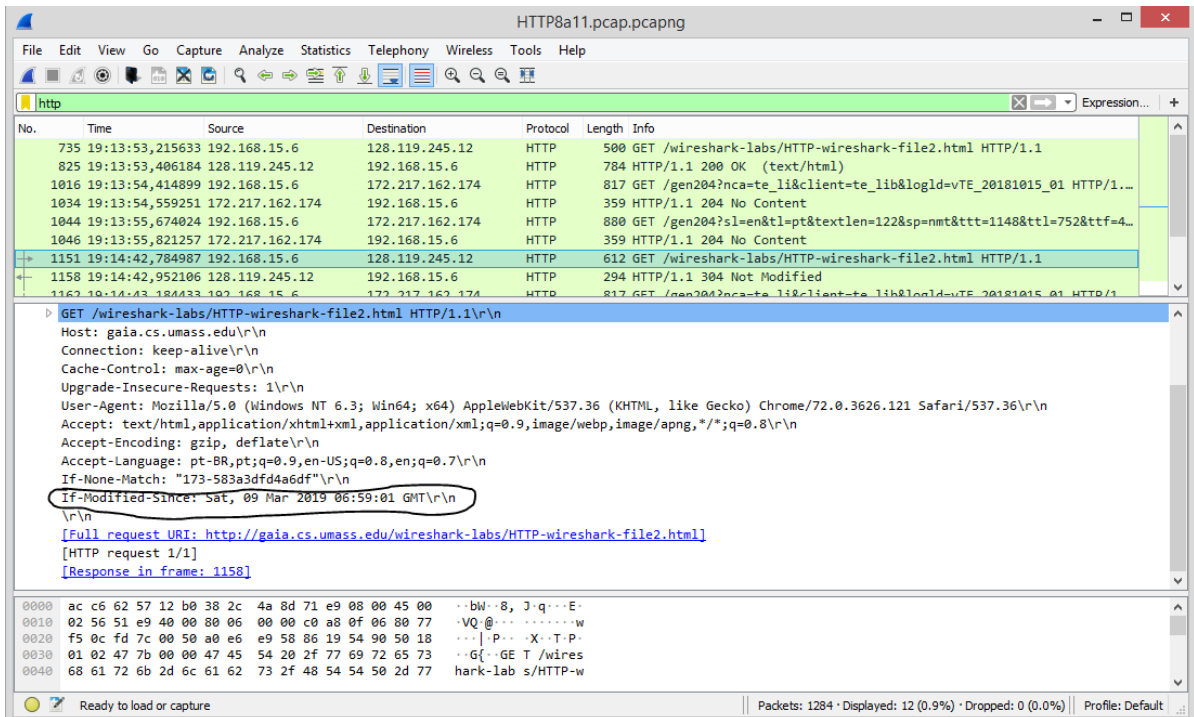
No.	Time	Source	Destination	Protocol	Length	Info
735	19:13:53,215633	192.168.15.6	128.119.245.12	HTTP	500	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
825	19:13:53,406184	128.119.245.12	192.168.15.6	HTTP	784	HTTP/1.1 200 OK (text/html)

The packet details pane for the selected packet (825) shows the following structure:

- Internet Protocol Version 4, Src: 192.168.15.6, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 64835, Dst Port: 80, Seq: 1, Ack: 1, Len: 446
- Hypertext Transfer Protocol
 - GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
 - Host: gaia.cs.umass.edu\r\n
 - Connection: keep-alive\r\n
 - Upgrade-Insecure-Requests: 1\r\n
 - User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36\r\n
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - Accept-Language: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7\r\n
 - \r\n
 - [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
 - [HTTP request 1/1]
 - [Response in frame: 825]

The packet bytes pane shows the raw data of the response, which is a 784-byte HTML document. The status bar at the bottom indicates that 12 packets are displayed out of 1284 total packets.

10) Sim, A data da última modificação do arquivo.

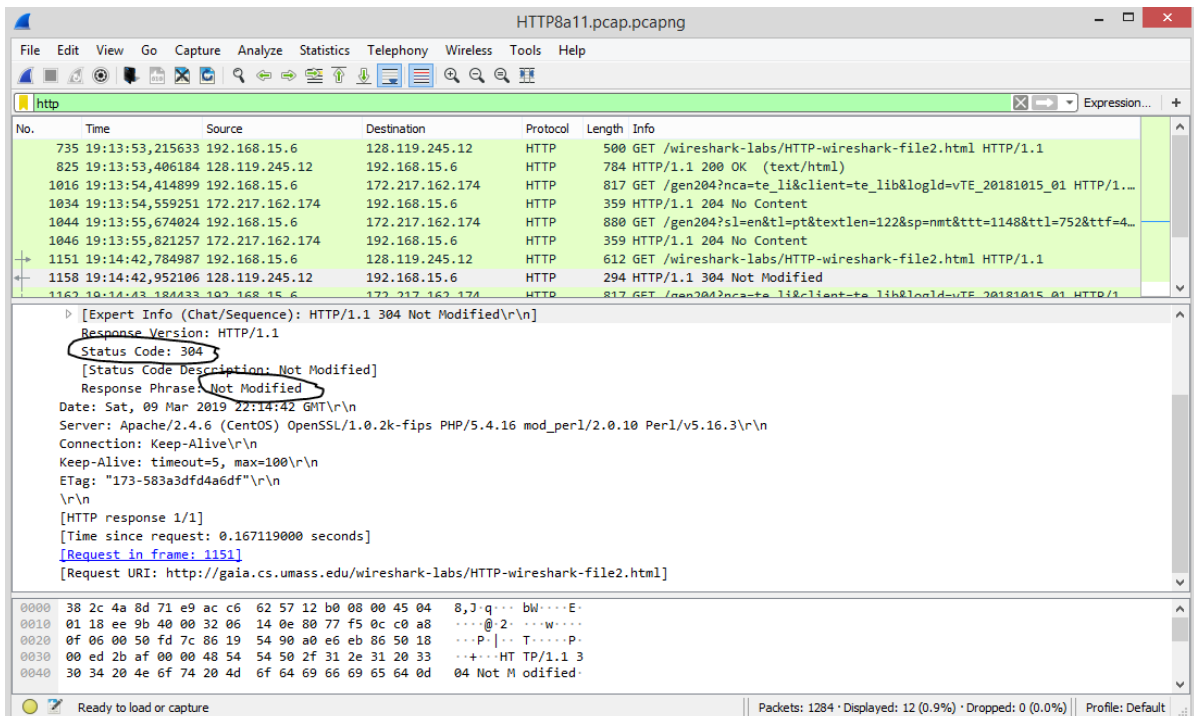


The screenshot shows a Wireshark capture of an HTTP GET request. The packet list shows a GET request for `/wireshark-labs/HTTP-wireshark-file2.html` at 11:51:19.14.42. The packet details pane shows the request headers, including `If-Modified-Since: Sat, 09 Mar 2019 06:59:01 GMT`, which is circled. The packet bytes pane shows the raw data of the request.

No.	Time	Source	Destination	Protocol	Length	Info
735	19:13:53,215633	192.168.15.6	128.119.245.12	HTTP	500	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
825	19:13:53,406184	128.119.245.12	192.168.15.6	HTTP	784	HTTP/1.1 200 OK (text/html)
1016	19:13:54,414899	192.168.15.6	172.217.162.174	HTTP	817	GET /gen204?nca=te_li&client=te_lib&logId=vTE_20181015_01 HTTP/1.1
1034	19:13:54,559251	172.217.162.174	192.168.15.6	HTTP	359	HTTP/1.1 204 No Content
1044	19:13:55,674024	192.168.15.6	172.217.162.174	HTTP	880	GET /gen204?sl=en&tl=pt&textlen=122&sp=nmt&ttt=1148&ttl=752&ttf=4... HTTP/1.1
1046	19:13:55,821257	172.217.162.174	192.168.15.6	HTTP	359	HTTP/1.1 204 No Content
1151	19:14:42,784987	192.168.15.6	128.119.245.12	HTTP	612	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1158	19:14:42,952106	128.119.245.12	192.168.15.6	HTTP	294	HTTP/1.1 304 Not Modified
1162	19:14:43,184433	192.168.15.6	172.217.162.174	HTTP	817	GET /gen204?nca=te_li&client=te_lib&logId=vTE_20181015_01 HTTP/1.1

GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7\r\n
If-None-Match: "173-583a3dfd4a6df"\r\n
If-Modified-Since: Sat, 09 Mar 2019 06:59:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 1/1]
[Response in frame: 1158]

11) 304 Not Modified. Não, devido à inclusão do campo IN-MODIFIED-SINCE na solicitação HTTP GET uma cópia completa será enviada apenas uma vez pelo servidor.



The screenshot shows a Wireshark capture of an HTTP GET request. The packet list shows a GET request for `/wireshark-labs/HTTP-wireshark-file2.html` at 11:51:19.14.42. The packet details pane shows the response headers, including `Status Code: 304`, which is circled. The packet bytes pane shows the raw data of the response.

No.	Time	Source	Destination	Protocol	Length	Info
735	19:13:53,215633	192.168.15.6	128.119.245.12	HTTP	500	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
825	19:13:53,406184	128.119.245.12	192.168.15.6	HTTP	784	HTTP/1.1 200 OK (text/html)
1016	19:13:54,414899	192.168.15.6	172.217.162.174	HTTP	817	GET /gen204?nca=te_li&client=te_lib&logId=vTE_20181015_01 HTTP/1.1
1034	19:13:54,559251	172.217.162.174	192.168.15.6	HTTP	359	HTTP/1.1 204 No Content
1044	19:13:55,674024	192.168.15.6	172.217.162.174	HTTP	880	GET /gen204?sl=en&tl=pt&textlen=122&sp=nmt&ttt=1148&ttl=752&ttf=4... HTTP/1.1
1046	19:13:55,821257	172.217.162.174	192.168.15.6	HTTP	359	HTTP/1.1 204 No Content
1151	19:14:42,784987	192.168.15.6	128.119.245.12	HTTP	612	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1158	19:14:42,952106	128.119.245.12	192.168.15.6	HTTP	294	HTTP/1.1 304 Not Modified
1162	19:14:43,184433	192.168.15.6	172.217.162.174	HTTP	817	GET /gen204?nca=te_li&client=te_lib&logId=vTE_20181015_01 HTTP/1.1

[Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
Response Version: HTTP/1.1
Status Code: 304
[Status Code Description: Not Modified]
Response Phrase: Not Modified
Date: Sat, 09 Mar 2019 22:14:42 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
Connection: Keep-Alive\r\n
Keep-Alive: timeout=5, max=100\r\n
ETag: "173-583a3dfd4a6df"\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.167119000 seconds]
[Request in frame: 1151]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

12) Uma Mensagem.

The screenshot shows a Wireshark capture of a single HTTP GET request. The packet list on the left shows packet 17 selected, which is an HTTP GET request from 192.168.15.6 to 128.119.245.12. The packet details pane on the right shows the structure of the packet: Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The packet bytes pane at the bottom shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
13	19:45:01,294695	192.168.15.6	128.119.245.12	TCP	66	50355 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
14	19:45:01,296058	192.168.15.6	128.119.245.12	TCP	66	50356 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
15	19:45:01,459224	128.119.245.12	192.168.15.6	TCP	66	80 → 50355 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM=1
16	19:45:01,459329	192.168.15.6	128.119.245.12	TCP	54	50355 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
17	19:45:01,461722	192.168.15.6	128.119.245.12	HTTP	500	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
18	19:45:01,486170	128.119.245.12	192.168.15.6	TCP	66	80 → 50356 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM=1
19	19:45:01,486274	192.168.15.6	128.119.245.12	TCP	54	50356 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
22	19:45:01,627112	128.119.245.12	192.168.15.6	TCP	60	80 → 50355 [ACK] Seq=1 Ack=447 Win=30336 Len=0
23	19:45:01,643786	128.119.245.12	192.168.15.6	TCP	1494	80 → 50355 [ACK] Seq=1 Ack=447 Win=30336 Len=1440 [TCP segment of a reassembled data stream]
24	19:45:01,643787	128.119.245.12	192.168.15.6	TCP	1494	80 → 50355 [ACK] Seq=1441 Ack=447 Win=30336 Len=1440 [TCP segment of a reassembled data stream]
25	19:45:01,643950	192.168.15.6	128.119.245.12	TCP	54	50355 → 80 [ACK] Seq=447 Ack=2881 Win=66048 Len=0
26	19:45:01,644310	128.119.245.12	192.168.15.6	TCP	1494	80 → 50355 [ACK] Seq=2881 Ack=447 Win=30336 Len=1440 [TCP segment of a reassembled data stream]
27	19:45:01,644377	192.168.15.6	128.119.245.12	TCP	54	50355 → 80 [ACK] Seq=447 Ack=4321 Win=66048 Len=0
28	19:45:01,644638	128.119.245.12	192.168.15.6	HTTP	595	HTTP/1.1 200 OK (text/html)
29	19:45:01,644702	192.168.15.6	128.119.245.12	TCP	54	50355 → 80 [ACK] Seq=447 Ack=4862 Win=65536 Len=0
381	19:45:06,648029	128.119.245.12	192.168.15.6	TCP	60	80 → 50355 [FIN, ACK] Seq=4862 Ack=447 Win=30336 Len=0
382	19:45:06,648133	192.168.15.6	128.119.245.12	TCP	54	[TCP Dup ACK 29#1] 50355 → 80 [ACK] Seq=447 Ack=4862 Win=65536 Len=0
383	19:45:06,648374	192.168.15.6	128.119.245.12	TCP	54	50355 → 80 [ACK] Seq=447 Ack=4863 Win=65536 Len=0
459	19:45:32,882319	128.119.245.12	192.168.15.6	TCP	66	[TCP Retransmission] 80 → 50356 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
460	19:45:32,882394	192.168.15.6	128.119.245.12	TCP	66	[TCP Dup ACK 19#1] 50356 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0 SLE=0 S...

Frame 17: 500 bytes on wire (4000 bits), 500 bytes captured (4000 bits) on interface 0
Ethernet II, Src: AsustekC_8d:71:e9 (38:2c:4a:8d:71:e9), Dst: Mitrasa_57:12:b0 (ac:c6:62:57:12:b0)
Internet Protocol Version 4, Src: 192.168.15.6, Dst: 128.119.245.12

01b0 70 2c 20 64 65 66 6c 61 74 65 0d 0a 41 63 63 65 p, deflate...Accept-Range: bytes
01c0 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 70 74 2d pt-Language: pt-
01d0 42 52 2c 70 74 3b 71 3d 30 2e 39 2c 65 6e 2d 55 BR;pt;q=0.9,en-U
01e0 53 3b 71 3d 30 2e 38 2c 65 6e 3b 71 3d 30 2e 37 S;q=0.8,en;q=0.7
01f0 0d 0a 0d 0a ...

HTTP Accept Language (http.accept_language), 54 bytes

Packets: 489 · Displayed: 20 (4.1%) · Dropped: 0 (0.0%) | Profile: Default

13) Quatro segmentos TCP.

The screenshot shows a Wireshark capture of a TCP retransmission and subsequent segments. The packet list on the left shows packet 28 selected, which is an HTTP 200 OK response from 128.119.245.12 to 192.168.15.6. The packet details pane on the right shows the structure of the packet: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane at the bottom shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
19	19:45:01,486274	192.168.15.6	128.119.245.12	TCP	54	50356 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
22	19:45:01,627112	128.119.245.12	192.168.15.6	TCP	60	80 → 50355 [ACK] Seq=1 Ack=447 Win=30336 Len=0
23	19:45:01,643786	128.119.245.12	192.168.15.6	TCP	1494	80 → 50355 [ACK] Seq=1 Ack=447 Win=30336 Len=1440 [TCP segment of a reassembled data stream]
24	19:45:01,643787	128.119.245.12	192.168.15.6	TCP	1494	80 → 50355 [ACK] Seq=1441 Ack=447 Win=30336 Len=1440 [TCP segment of a reassembled data stream]
25	19:45:01,643950	192.168.15.6	128.119.245.12	TCP	54	50355 → 80 [ACK] Seq=447 Ack=2881 Win=66048 Len=0
26	19:45:01,644310	128.119.245.12	192.168.15.6	TCP	1494	80 → 50355 [ACK] Seq=2881 Ack=447 Win=30336 Len=1440 [TCP segment of a reassembled data stream]
27	19:45:01,644377	192.168.15.6	128.119.245.12	TCP	54	50355 → 80 [ACK] Seq=447 Ack=4321 Win=66048 Len=0
28	19:45:01,644638	128.119.245.12	192.168.15.6	HTTP	595	HTTP/1.1 200 OK (text/html)
29	19:45:01,644702	192.168.15.6	128.119.245.12	TCP	54	50355 → 80 [ACK] Seq=447 Ack=4862 Win=65536 Len=0
381	19:45:06,648029	128.119.245.12	192.168.15.6	TCP	60	80 → 50355 [FIN, ACK] Seq=4862 Ack=447 Win=30336 Len=0
382	19:45:06,648133	192.168.15.6	128.119.245.12	TCP	54	[TCP Dup ACK 29#1] 50355 → 80 [ACK] Seq=447 Ack=4862 Win=65536 Len=0
383	19:45:06,648374	192.168.15.6	128.119.245.12	TCP	54	50355 → 80 [ACK] Seq=447 Ack=4863 Win=65536 Len=0
459	19:45:32,882319	128.119.245.12	192.168.15.6	TCP	66	[TCP Retransmission] 80 → 50356 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
460	19:45:32,882394	192.168.15.6	128.119.245.12	TCP	66	[TCP Dup ACK 19#1] 50356 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0 SLE=0 S...

Frame 28: 595 bytes on wire (4760 bits), 595 bytes captured (4760 bits) on interface 0
Ethernet II, Src: Mitrasa_57:12:b0 (ac:c6:62:57:12:b0), Dst: AsustekC_8d:71:e9 (38:2c:4a:8d:71:e9)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.15.6
Transmission Control Protocol, Src Port: 80, Dst Port: 50355, Seq: 4321, Ack: 447, Len: 541
[4 Reassembled TCP Segments (4861 bytes): #23(1440), #24(1440), #26(1440), #28(541)]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\nDate: Sat, 09 Mar 2019 22:45:01 GMT\r\nServer: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\nLast-Modified: Sat, 09 Mar 2019 06:59:01 GMT\r\nETag: "1194-583a3df4491e"\r\nAccept-Ranges: bytes\r\nContent-Length: 4500\r\n[Content length: 4500]
Keep-Alive: timeout=5, max=100\r\n\r\n0000 38 2c 4a 8d 71 e9 ac c6 62 57 12 b0 08 00 45 04 8,J q... bW...E
0010 02 45 55 ba 40 00 32 06 ab c2 80 77 f5 0c c0 a8 .EU@.2...w....
0020 0f 06 00 50 c4 b3 32 85 40 63 48 03 b1 39 50 18 ...P..2..@ch..9P
0030 00 ed 2b 38 00 00 65 64 2c 20 6e 6f 72 20 65 78 ..+8..ed , nor ex

Frame (595 bytes) Reassembled TCP (4861 bytes)

Ready to load or capture

Packets: 489 · Displayed: 20 (4.1%) · Dropped: 0 (0.0%) | Profile: Default

14) 200 OK

The screenshot shows a Wireshark capture of an HTTP 200 OK response. The packet list pane shows a sequence of TCP segments followed by an HTTP packet (No. 28). The packet details pane for the selected HTTP packet shows the following information:

- Frame 28: 595 bytes on wire (4760 bits), 595 bytes captured (4760 bits) on interface 0
- Ethernet II, Src: Mitrasa 57:12:b0 (ac:c6:62:57:12:b0), Dst: AsustekC_8d:71:e9 (38:2c:4a:8d:71:e9)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.15.6
- Transmission Control Protocol, Src Port: 80, Dst Port: 50355, Seq: 4321, Ack: 447, Len: 541
- [4 Reassembled TCP Segments (4861 bytes): #23(1440), #24(1440), #26(1440), #28(541)]
- Hypertext Transfer Protocol
 - HTTP/1.1 200 OK\r\n
 - [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
 - Response Version: HTTP/1.1
 - Status Code: 200
 - [Status Code Description: OK]
 - Response Phrase: OK
 - Date: Sat, 09 Mar 2019 22:45:01 GMT\r\n
 - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
 - Last-Modified: Sat, 09 Mar 2019 06:50:01 GMT\r\n

The packet bytes pane shows the raw data of the HTTP response, including the status line and headers.

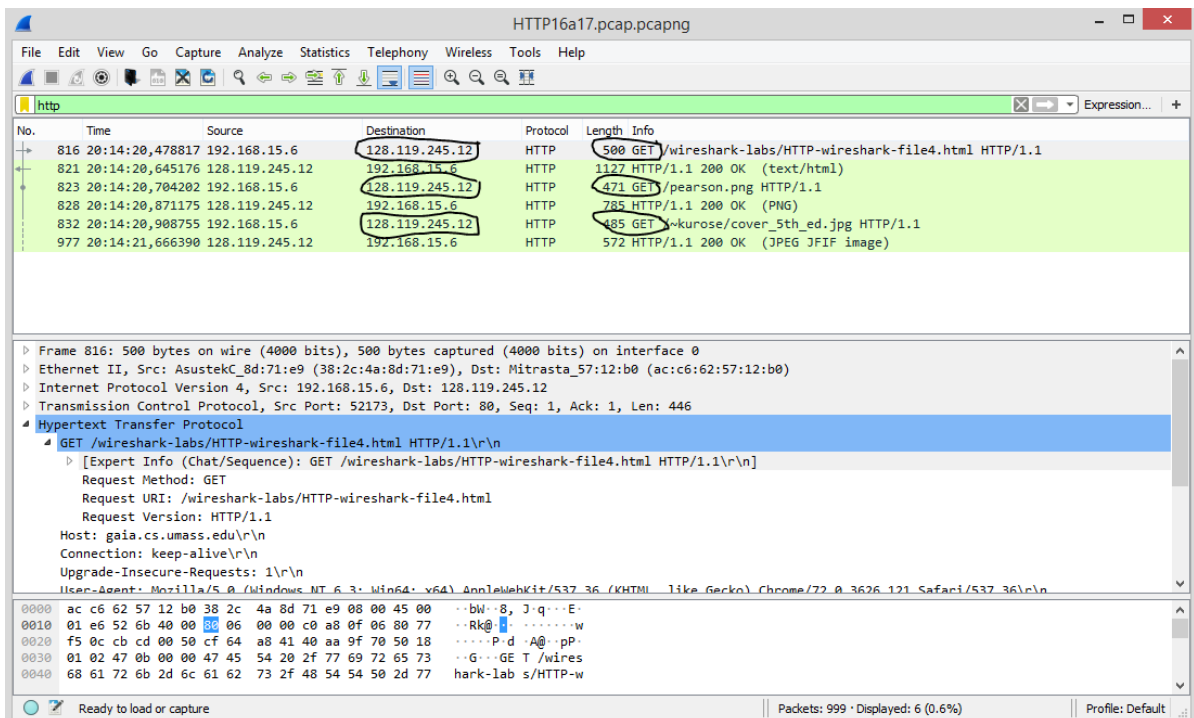
15) Não

The screenshot shows a Wireshark capture of an HTTP 200 OK response. The packet list pane shows a sequence of TCP segments followed by an HTTP packet (No. 28). The packet details pane for the selected HTTP packet shows the following information:

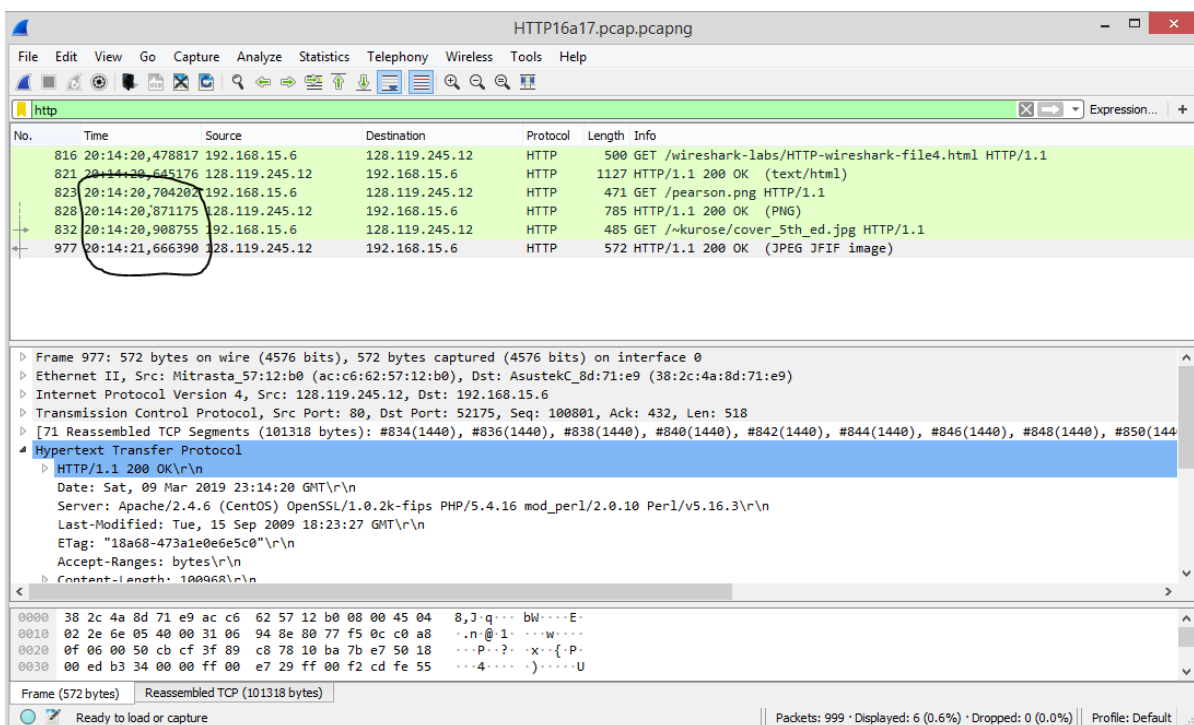
- Frame 28: 595 bytes on wire (4760 bits), 595 bytes captured (4760 bits) on interface 0
- Ethernet II, Src: Mitrasa 57:12:b0 (ac:c6:62:57:12:b0), Dst: AsustekC_8d:71:e9 (38:2c:4a:8d:71:e9)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.15.6
- Transmission Control Protocol, Src Port: 80, Dst Port: 50355, Seq: 4321, Ack: 447, Len: 541
- [4 Reassembled TCP Segments (4861 bytes): #23(1440), #24(1440), #26(1440), #28(541)]
- Hypertext Transfer Protocol
 - HTTP/1.1 200 OK\r\n
 - [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
 - Response Version: HTTP/1.1
 - Status Code: 200
 - [Status Code Description: OK]
 - Response Phrase: OK
 - Date: Sat, 09 Mar 2019 22:45:01 GMT\r\n
 - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
 - Last-Modified: Sat, 09 Mar 2019 06:50:01 GMT\r\n

The packet bytes pane shows the raw data of the HTTP response, including the status line and headers.

16) Três mensagens GET, os três possuem o mesmo ip de destino: 128.119.245.12 e os hosts: gaia.cs.umass.edu (logomarca e texto) e manic.cs.umass.edu (imagem capa do livro) .



17) Em sequência pelo tempo ser diferentes e o protocolo http 1.1 ser sequencial, o que pode ocorrer são conexões simultâneas paralelizando os request.



18) 401 Unauthorized

The screenshot shows a Wireshark capture of an HTTP 401 Unauthorized response. The packet list shows a GET request to /protected_pages/HTTP-wireshark-file5.html and a corresponding 401 response. The packet details pane shows the response structure: HTTP/1.1 401 Unauthorized, Status Code: 401, and Response Phrase: Unauthorized. The raw data pane shows the hex and ASCII representation of the response.

No.	Time	Source	Destination	Protocol	Length	Info
488	20:26:01.444843	192.168.15.6	128.119.245.12	TCP	66	52892 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
489	20:26:01.444958	192.168.15.6	128.119.245.12	TCP	66	52893 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
549	20:26:01.608886	128.119.245.12	192.168.15.6	TCP	66	80 → 52892 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_P...
550	20:26:01.608997	192.168.15.6	128.119.245.12	TCP	54	52892 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
551	20:26:01.610804	192.168.15.6	128.119.245.12	HTTP	516	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
591	20:26:01.629047	128.119.245.12	192.168.15.6	TCP	66	80 → 52893 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_P...
592	20:26:01.629134	192.168.15.6	128.119.245.12	TCP	54	52893 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
648	20:26:01.776094	128.119.245.12	192.168.15.6	TCP	60	80 → 52892 [ACK] Seq=1 Ack=463 Win=30336 Len=0
649	20:26:01.777610	128.119.245.12	192.168.15.6	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
650	20:26:01.777831	192.168.15.6	128.119.245.12	TCP	54	52892 → 80 [ACK] Seq=463 Ack=718 Win=65280 Len=0

Frame 649: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface 0
Ethernet II, Src: Mitrasta_57:12:b0 (ac:c6:62:57:12:b0), Dst: AsustekC_8d:71:e9 (38:2c:4a:8d:71:e9)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.15.6
Transmission Control Protocol, Src Port: 80, Dst Port: 52892, Seq: 1, Ack: 463, Len: 717
Hypertext Transfer Protocol
HTTP/1.1 401 Unauthorized\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
Response Version: HTTP/1.1
Status Code: 401
[Status Code Description: Unauthorized]
Response Phrase: Unauthorized
Date: Sat, 09 Mar 2019 23:26:01 GMT\r\nServer: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\nWWW-Authenticate: Basic realm="wireshark-students only"\r\n

19) O campo Authorization com o nome e senha do usuário codificados em base64.

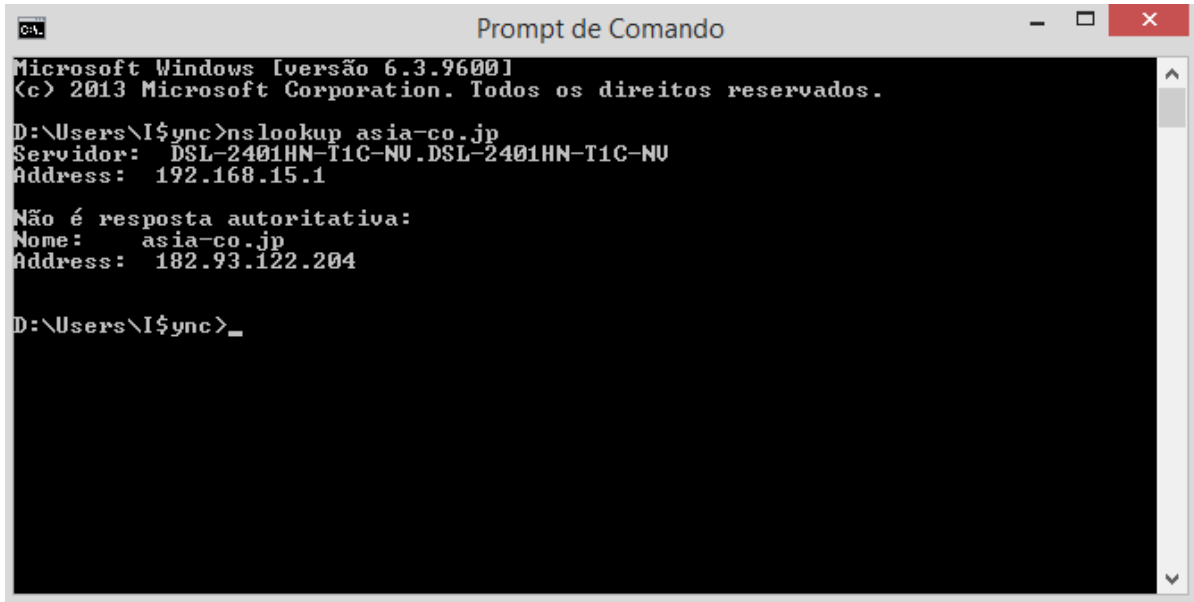
The screenshot shows a Wireshark capture of an HTTP request. The packet list shows a GET request to /protected_pages/HTTP-wireshark-file5.html. The packet details pane shows the request structure, including the Authorization header: Basic d2lyZXNoYXJFLXN0dWRLbnRzOm5ldHdvcm0=. The raw data pane shows the hex and ASCII representation of the request.

No.	Time	Source	Destination	Protocol	Length	Info
745	20:26:06.782812	192.168.15.6	128.119.245.12	TCP	54	52892 → 80 [ACK] Seq=463 Ack=719 Win=65280 Len=0
762	20:26:16.387415	192.168.15.6	128.119.245.12	TCP	54	52892 → 80 [RST, ACK] Seq=463 Ack=719 Win=0 Len=0
763	20:26:16.387642	192.168.15.6	128.119.245.12	TCP	66	52912 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
764	20:26:16.387896	192.168.15.6	128.119.245.12	TCP	54	52893 → 80 [FIN, ACK] Seq=1 Ack=1 Win=66048 Len=0
765	20:26:16.556457	128.119.245.12	192.168.15.6	TCP	66	80 → 52912 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_P...
766	20:26:16.556583	192.168.15.6	128.119.245.12	TCP	54	52912 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
767	20:26:16.559029	192.168.15.6	128.119.245.12	HTTP	575	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
769	20:26:16.573091	128.119.245.12	192.168.15.6	TCP	60	80 → 52893 [ACK] Seq=1 Ack=2 Win=29312 Len=0
770	20:26:16.573092	128.119.245.12	192.168.15.6	TCP	60	80 → 52893 [FIN, ACK] Seq=1 Ack=2 Win=29312 Len=0
771	20:26:16.573203	192.168.15.6	128.119.245.12	TCP	54	[TCP Dup ACK 592#1] 52893 → 80 [ACK] Seq=2 Ack=1 Win=66048 Len=0

Transmission Control Protocol, Src Port: 52912, Dst Port: 80, Seq: 1, Ack: 1, Len: 521
Hypertext Transfer Protocol
GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nAuthorization: Basic d2lyZXNoYXJFLXN0dWRLbnRzOm5ldHdvcm0=\r\nCredentials: wireshark-students:network\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7\r\n\r\nFull request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html

Wireshark Lab: DNS

1)



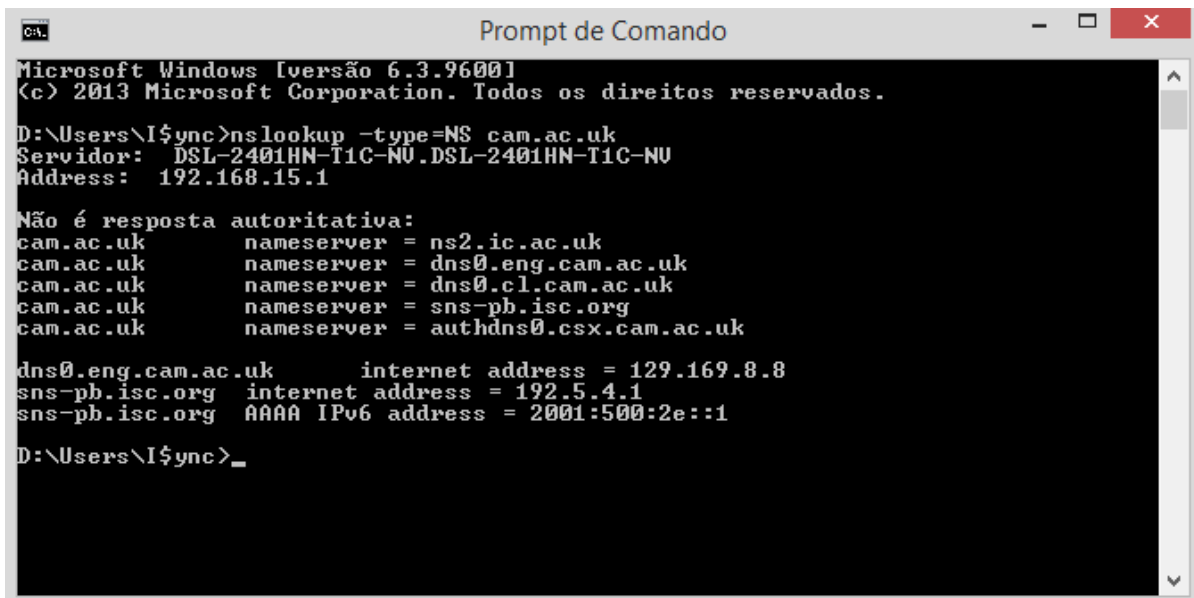
```
Microsoft Windows [versão 6.3.9600]
(c) 2013 Microsoft Corporation. Todos os direitos reservados.

D:\Users\I$ync>nslookup asia-co.jp
Servidor:  DSL-2401HN-T1C-NU.DSL-2401HN-T1C-NU
Address:  192.168.15.1

Não é resposta autoritativa:
Nome:     asia-co.jp
Address:  182.93.122.204

D:\Users\I$ync>_
```

2)



```
Microsoft Windows [versão 6.3.9600]
(c) 2013 Microsoft Corporation. Todos os direitos reservados.

D:\Users\I$ync>nslookup -type=NS cam.ac.uk
Servidor:  DSL-2401HN-T1C-NU.DSL-2401HN-T1C-NU
Address:  192.168.15.1

Não é resposta autoritativa:
cam.ac.uk      nameserver = ns2.ic.ac.uk
cam.ac.uk      nameserver = dns0.eng.cam.ac.uk
cam.ac.uk      nameserver = dns0.cl.cam.ac.uk
cam.ac.uk      nameserver = sns-ph.isc.org
cam.ac.uk      nameserver = authdns0.csx.cam.ac.uk

dns0.eng.cam.ac.uk      internet address = 129.169.8.8
sns-ph.isc.org          internet address = 192.5.4.1
sns-ph.isc.org          AAAA IPv6 address = 2001:500:2e::1

D:\Users\I$ync>_
```

3)

```
Prompt de Comando

Microsoft Windows [versão 6.3.9600]
(c) 2013 Microsoft Corporation. Todos os direitos reservados.

D:\Users\I$ync>nslookup office365.com ns2.ic.ac.uk
Servidor: ns2.ic.ac.uk
Address: 155.198.142.82

*** ns2.ic.ac.uk não encontrou office365.com: Query refused
D:\Users\I$ync>_
```

4) Enviadas com UDP.

DNS4a10.pcap.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.15.6

No.	Time	Source	Destination	Protocol	Length	Info
2	12:11:38,493293	192.168.15.6	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
3	12:11:39,307718	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
4	12:11:41,083421	192.168.15.6	192.168.15.1	DNS	74	Standard query 0x7adb A www.google.com
5	12:11:41,084395	192.168.15.1	192.168.15.6	DNS	90	Standard query response 0x7adb A www.google.com A 216.58.222.68
6	12:11:41,085773	192.168.15.6	216.58.222.68	TCP	66	49466 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7	12:11:41,090594	192.168.15.6	216.58.222.68	TCP	66	49467 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
8	12:11:41,112858	216.58.222.68	192.168.15.6	TCP	66	443 → 49466 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0 MSS=1380 SACK_PERM=1
9	12:11:41,112925	192.168.15.6	216.58.222.68	TCP	54	49466 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
10	12:11:41,114053	192.168.15.6	216.58.222.68	TCP	66	49468 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
11	12:11:41,117223	216.58.222.68	192.168.15.6	TCP	66	443 → 49467 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0 MSS=1380 SACK_PERM=1

Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: AsustekC_8d:71:e9 (38:2c:4a:8d:71:e9), Dst: Mitrasa_57:12:b0 (ac:c6:62:57:12:b0)
Internet Protocol Version 4, Src: 192.168.15.6, Dst: 192.168.15.1
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 60
Identification: 0x7496 (29846)
Flags: 0x0000
Time to live: 128
Protocol: UDP (17)
Header checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.15.6

0000 ac c6 62 57 12 b0 8d 71 e9 08 00 45 00 ..bW..S..q...E
0010 00 3c 74 96 00 00 80 11 00 00 c0 a8 0f 06 c0 a8 <.....
0020 0f 01 e9 55 00 35 00 28 9f 91 7a db 01 00 00 01 ..U-5-(...z...
0030 00 00 00 00 00 03 77 77 06 67 6f 67 6cw ww googl
0040 65 03 63 6f 6d 00 00 01 00 01 e.com....

Domain Name System (dns), 32 bytes | Packets: 3184 · Displayed: 3182 (99.9%) · Dropped: 0 (0.0%) | Profile: Default

DNS4a10.pcap.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.15.6

No.	Time	Source	Destination	Protocol	Length	Info
2	12:11:38,493293	192.168.15.6	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
3	12:11:39,307718	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
4	12:11:41,083421	192.168.15.6	192.168.15.1	DNS	74	Standard query 0x7adb A www.google.com
5	12:11:41,084395	192.168.15.1	192.168.15.6	DNS	90	Standard query response 0x7adb A www.google.com A 216.58.222.68
6	12:11:41,085773	192.168.15.6	216.58.222.68	TCP	66	49466 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7	12:11:41,090594	192.168.15.6	216.58.222.68	TCP	66	49467 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
8	12:11:41,112858	216.58.222.68	192.168.15.6	TCP	66	443 → 49466 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0 MSS=1380 SACK_PERM=1
9	12:11:41,112925	192.168.15.6	216.58.222.68	TCP	54	49466 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
10	12:11:41,114053	192.168.15.6	216.58.222.68	TCP	66	49468 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
11	12:11:41,117223	216.58.222.68	192.168.15.6	TCP	66	443 → 49467 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0 MSS=1380 SACK_PERM=1

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

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

Total Length: 76

Identification: 0x0000 (0)

Flags: 0x4000, Don't fragment

Time to live: 64

Protocol: UDP (17)

Header checksum: 0x9b49 [validation disabled]
[Header checksum status: Unverified]

Source: 192.168.15.1

Destination: 192.168.15.6

▸ User Datagram Protocol, Src Port: 53, Dst Port: 59733

▸ Domain Name System (response)

```

0010 00 4c 00 00 40 00 11 9b 49 c0 a8 0f 01 c0 a8  .L..@..I.....
0020 0f 06 00 35 e9 55 00 38 75 64 7a db 81 80 00 01  .5.U.8 udz....
0030 00 01 00 00 00 00 03 77 77 06 67 6f 6f 67 6c  .w ww.googl
0040 65 03 63 6f 6d 00 00 01 00 01 c0 0c 00 01 00 01  e.com.....
0050 00 00 00 a0 00 04 d8 3a de 44                  .D

```

Domain Name System (dns), 48 bytes

Packets: 3184 · Displayed: 3182 (99.9%) · Dropped: 0 (0.0%) · Profile: Default

5) Porta 53.

DNS4a10.pcap.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.15.6

No.	Time	Source	Destination	Protocol	Length	Info
2	12:11:38,493293	192.168.15.6	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
3	12:11:39,307718	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
4	12:11:41,083421	192.168.15.6	192.168.15.1	DNS	74	Standard query 0x7adb A www.google.com
5	12:11:41,084395	192.168.15.1	192.168.15.6	DNS	90	Standard query response 0x7adb A www.google.com A 216.58.222.68
6	12:11:41,085773	192.168.15.6	216.58.222.68	TCP	66	49466 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7	12:11:41,090594	192.168.15.6	216.58.222.68	TCP	66	49467 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
8	12:11:41,112858	216.58.222.68	192.168.15.6	TCP	66	443 → 49466 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0 MSS=1380 SACK_PERM=1
9	12:11:41,112925	192.168.15.6	216.58.222.68	TCP	54	49466 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
10	12:11:41,114053	192.168.15.6	216.58.222.68	TCP	66	49468 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
11	12:11:41,117223	216.58.222.68	192.168.15.6	TCP	66	443 → 49467 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0 MSS=1380 SACK_PERM=1

▸ Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

▸ Ethernet II, Src: AsustekC_8d:71:e9 (38:2c:4a:8d:71:e9), Dst: Mitrasta_57:12:b0 (ac:c6:62:57:12:b0)

▸ Internet Protocol Version 4, Src: 192.168.15.6, Dst: 192.168.15.1

▸ User Datagram Protocol, Src Port: 59733, Dst Port: 53

Source Port: 59733

Destination Port: 53

Length: 40

Checksum: 0x9f91 [unverified]
[Checksum Status: Unverified]

[Stream index: 1]

▸ [Timestamps]

▸ Domain Name System (query)

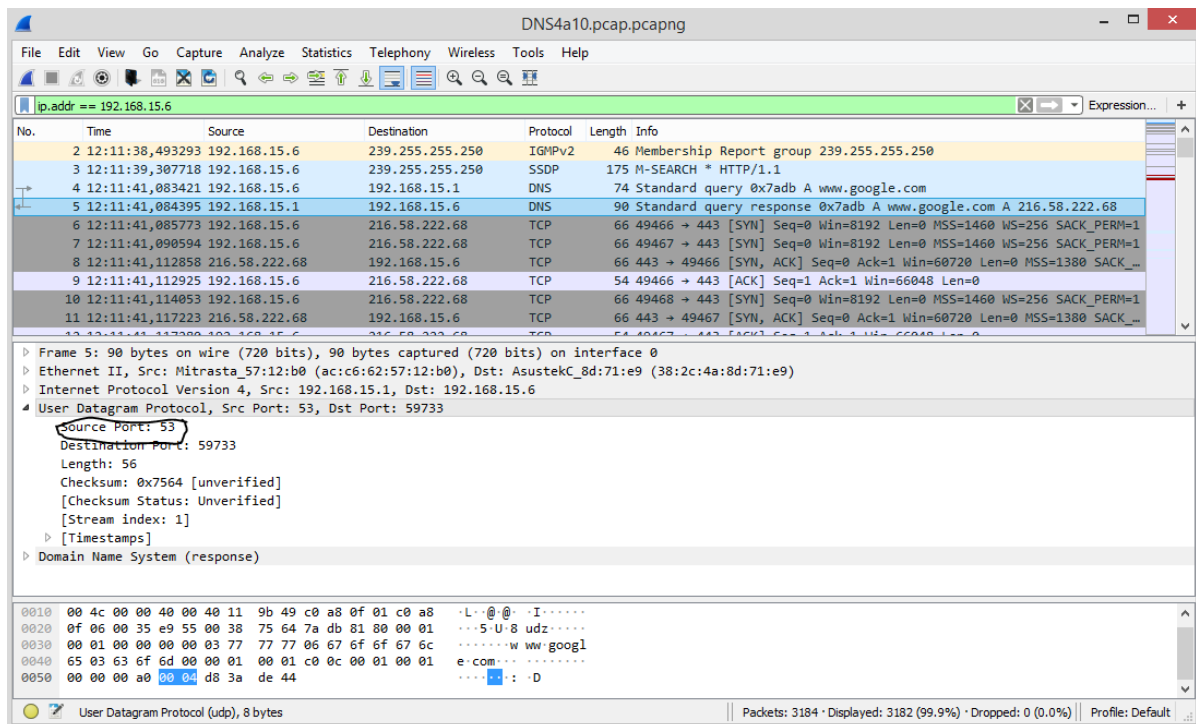
```

0000 ac c6 62 57 12 b0 38 2c 4a 8d 71 e9 08 00 45 00  .bW..8, J q...E
0010 00 3c 74 96 00 00 80 11 00 00 c0 a8 0f 06 c0 a8  .<t.....
0020 0f 01 e9 55 00 00 00 28 9f 91 7a db 01 00 00 01  .U.S.(.....
0030 00 00 00 00 00 00 03 77 77 06 67 6f 6f 67 6c  .w ww.googl
0040 65 03 63 6f 6d 00 00 01 00 01 c0 0c 00 01 00 01  e.com.....

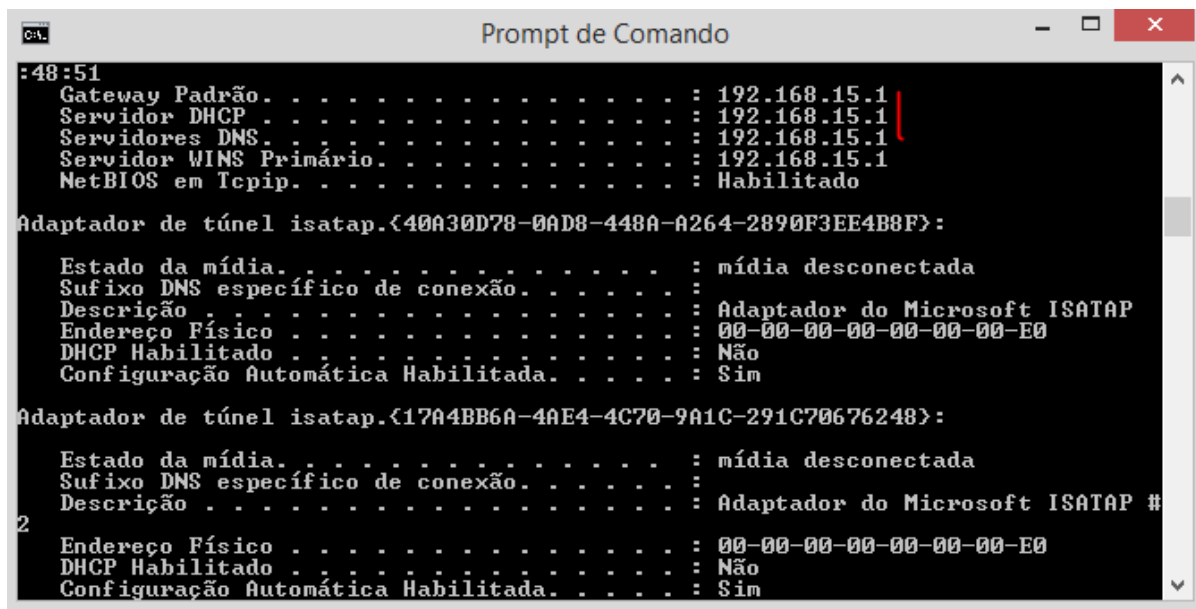
```

User Datagram Protocol (udp), 8 bytes

Packets: 3184 · Displayed: 3182 (99.9%) · Dropped: 0 (0.0%) · Profile: Default



6) 192.168.15.1, sim são os mesmos endereços.



DNS4a10.pcap.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.15.6

No.	Time	Source	Destination	Protocol	Length	Info
2	12:11:38,493293	192.168.15.6	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
3	12:11:39,307718	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
4	12:11:41,083421	192.168.15.6	192.168.15.1	DNS	74	Standard query 0x7adb A www.google.com
5	12:11:41,084395	192.168.15.1	192.168.15.6	DNS	90	Standard query response 0x7adb A www.google.com A 216.58.222.68
6	12:11:41,085773	192.168.15.6	216.58.222.68	TCP	66	49466 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7	12:11:41,090594	192.168.15.6	216.58.222.68	TCP	66	49467 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
8	12:11:41,112858	216.58.222.68	192.168.15.6	TCP	66	443 → 49466 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0 MSS=1380 SACK_PERM=1
9	12:11:41,112925	192.168.15.6	216.58.222.68	TCP	54	49466 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
10	12:11:41,114053	192.168.15.6	216.58.222.68	TCP	66	49468 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
11	12:11:41,117223	216.58.222.68	192.168.15.6	TCP	66	443 → 49467 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0 MSS=1380 SACK_PERM=1

Internet Protocol Version 4, Src: 192.168.15.6, Dst: 192.168.15.1

0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 60
 Identification: 0x7496 (29846)
 Flags: 0x0000
 Time to live: 128
 Protocol: UDP (17)
 Header checksum: 0x0000 [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.15.6
 Destination: 192.168.15.1

User Datagram Protocol, Src Port: 59733, Dst Port: 53

```

0000  ac c6 62 57 12 b0 38 2c  4a 8d 71 e9 08 00 45 00  ..bW..8, J.q...E.
0010  00 3c 74 96 00 00 80 11  00 00 c0 a8 0f 06 c0 a8  <t.....
0020  0f 01 e9 55 00 35 00 28  9f 91 7a db 01 00 00 01  ..U.5.(...z....
0030  00 00 00 00 00 00 77 77  77 77 06 6f 6f 6f 6f 6c  .....w ww googl
0040  65 03 63 6f 6d 00 00 01  00 01 00 01 00 01 00 01  e.com. ....
  
```

User Datagram Protocol (udp), 8 bytes

Packets: 3184 · Displayed: 3182 (99.9%) · Dropped: 0 (0.0%) · Profile: Default

7) Type: A, não contem.

DNS4a10.pcap.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.15.6

No.	Time	Source	Destination	Protocol	Length	Info
2	12:11:38,493293	192.168.15.6	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
3	12:11:39,307718	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
4	12:11:41,083421	192.168.15.6	192.168.15.1	DNS	74	Standard query 0x7adb A www.google.com
5	12:11:41,084395	192.168.15.1	192.168.15.6	DNS	90	Standard query response 0x7adb A www.google.com A 216.58.222.68
6	12:11:41,085773	192.168.15.6	216.58.222.68	TCP	66	49466 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7	12:11:41,090594	192.168.15.6	216.58.222.68	TCP	66	49467 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
8	12:11:41,112858	216.58.222.68	192.168.15.6	TCP	66	443 → 49466 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0 MSS=1380 SACK_PERM=1
9	12:11:41,112925	192.168.15.6	216.58.222.68	TCP	54	49466 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
10	12:11:41,114053	192.168.15.6	216.58.222.68	TCP	66	49468 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
11	12:11:41,117223	216.58.222.68	192.168.15.6	TCP	66	443 → 49467 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0 MSS=1380 SACK_PERM=1
12	12:11:41,117280	192.168.15.6	216.58.222.68	TCP	54	49467 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0

Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0

Queries

- www.google.com: type A, class IN
 - Name: www.google.com
 - [Name Length: 14]
 - [Label Count: 3]
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)

[Response In: 5]

```

0000  ac c6 62 57 12 b0 38 2c  4a 8d 71 e9 08 00 45 00  ..bW..8, J.q...E.
0010  00 3c 74 96 00 00 80 11  00 00 c0 a8 0f 06 c0 a8  <t.....
0020  0f 01 e9 55 00 35 00 28  9f 91 7a db 01 00 00 01  ..U.5.(...z....
0030  00 00 00 00 00 00 77 77  77 77 06 6f 6f 6f 6f 6c  .....w ww googl
0040  65 03 63 6f 6d 00 00 01  00 01 00 01 00 01 00 01  e.com. ....
  
```

Domain Name System (dns), 32 bytes

Packets: 3184 · Displayed: 3182 (99.9%) · Profile: Default

8) Apenas 1. Os dados de resposta do www.google.com.

Wireshark capture of a DNS response from 192.168.15.6. The packet list shows a DNS response (No. 5) from 192.168.15.1 to 192.168.15.6. The packet details pane shows the DNS response structure with a single answer for www.google.com. The packet bytes pane shows the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
2	12:11:38,493293	192.168.15.6	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
3	12:11:39,307718	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
4	12:11:41,083421	192.168.15.6	192.168.15.1	DNS	74	Standard query 0x7adb A www.google.com
5	12:11:41,084395	192.168.15.1	192.168.15.6	DNS	90	Standard query response 0x7adb A www.google.com A 216.58.222.68
6	12:11:41,085773	192.168.15.6	216.58.222.68	TCP	66	49466 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7	12:11:41,090594	192.168.15.6	216.58.222.68	TCP	66	49467 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
8	12:11:41,112858	216.58.222.68	192.168.15.6	TCP	66	443 → 49466 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0 MSS=1380 SACK...
9	12:11:41,112925	192.168.15.6	216.58.222.68	TCP	54	49466 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
10	12:11:41,114053	192.168.15.6	216.58.222.68	TCP	66	49468 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
11	12:11:41,117223	216.58.222.68	192.168.15.6	TCP	66	443 → 49467 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0 MSS=1380 SACK...

Questions: 1
 Answer RRs: 1
 Authority RRs: 0
 Additional RRs: 0

Queries

Answers

- www.google.com: type A, class IN, addr 216.58.222.68
 - Name: www.google.com
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
 - Time to live: 160
 - Data length: 4
 - Address: 216.58.222.68

0010 00 4c 00 00 40 00 40 11 9b 49 c0 a8 0f 01 c0 a8 ...L...@...I.....
 0020 0f 06 00 35 e9 55 00 38 75 64 7a db 81 80 00 01 ...5-U-8 udz.....
 0030 00 01 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6cw ww.googl
 0040 65 03 63 6f 6d 00 00 01 c0 0c 00 01 00 01 ...e.com.....
 0050 00 00 00 a0 00 04 d8 3a de 44D

9) Sim, corresponde ao endereço de “Answers”.

Wireshark capture of a TCP response from 192.168.15.6. The packet list shows a TCP response (No. 9) from 192.168.15.6 to 216.58.222.68. The packet details pane shows the TCP response structure with a single answer for www.google.com. The packet bytes pane shows the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
2	12:11:38,493293	192.168.15.6	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
3	12:11:39,307718	192.168.15.6	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
4	12:11:41,083421	192.168.15.6	192.168.15.1	DNS	74	Standard query 0x7adb A www.google.com
5	12:11:41,084395	192.168.15.1	192.168.15.6	DNS	90	Standard query response 0x7adb A www.google.com A 216.58.222.68
6	12:11:41,085773	192.168.15.6	216.58.222.68	TCP	66	49466 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7	12:11:41,090594	192.168.15.6	216.58.222.68	TCP	66	49467 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
8	12:11:41,112858	216.58.222.68	192.168.15.6	TCP	66	443 → 49466 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0 MSS=1380 SACK...
9	12:11:41,112925	192.168.15.6	216.58.222.68	TCP	54	49466 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
10	12:11:41,114053	192.168.15.6	216.58.222.68	TCP	66	49468 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
11	12:11:41,117223	216.58.222.68	192.168.15.6	TCP	66	443 → 49467 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0 MSS=1380 SACK...

0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 52
 Identification: 0x37f8 (14328)
 Flags: 0x4000, Don't fragment
 Time to live: 128
 Protocol: TCP (6)
 Header checksum: 0x0000 [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.15.6
 Destination: 216.58.222.68

Transmission Control Protocol, Src Port: 49466, Dst Port: 443, Seq: 0, Len: 0

0000 ac c6 62 57 12 b0 38 2c 4a 8d 71 e9 08 00 45 00 ...bW...8, J;q...E
 0010 00 34 37 f8 40 00 00 06 00 00 c0 a8 0f 06 d8 3a ...47 @... ..
 0020 de 44 c1 3a 01 bb bd 37 2c 7e 00 00 00 00 00 02 ...D: ...7 ~.....
 0030 20 00 06 54 00 00 02 04 05 b4 01 03 03 08 01 01 ...T.....
 0040 04 02

10) Não novas houve consultas

Wireshark capture of DNS traffic for file DNS4a10.pcap.pcapng. The filter is `ip.addr == 192.168.15.6 && dns`. The packet list shows several DNS queries and responses. Packet 4 is a query for `www.google.com`. Packet 5 is the response. Packet 556 is a query for `www.ietf.org`. Packet 568 is the response. Packet 808 is a query for `ocsdp.starfieldtech.com`. Packet 810 is the response. Packet 938 is a query for `win8.ipv6.microsoft.com`. Packet 939 is the response. The packet details for packet 4 show it's a Standard query for `www.google.com`. The packet bytes show the raw DNS data.

11) Porta 53.

Wireshark capture of DNS traffic for file DNS11a15.pcap.pcapng. The filter is `ip.addr == 192.168.15.6 && dns`. The packet list shows several DNS queries and responses. Packet 23 is a query for `PTR 1.15.168.192.in-addr.arpa`. Packet 24 is the response. Packet 25 is a query for `www.mit.edu`. Packet 26 is the response. Packet 27 is a query for `AAAA www.mit.edu`. Packet 28 is the response. The packet details for packet 25 show it's a Standard query for `www.mit.edu`. The packet bytes show the raw DNS data.

DNS11a15.pcap.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.15.6 && dns

No.	Time	Source	Destination	Protocol	Length	Info
23	13:07:46,870278	192.168.15.6	192.168.15.1	DNS	85	Standard query 0x0001 PTR 1.15.168.192.in-addr.arpa
24	13:07:46,871282	192.168.15.1	192.168.15.6	DNS	134	Standard query response 0x0001 PTR 1.15.168.192.in-addr.arpa PTR DSL-24...
25	13:07:46,877159	192.168.15.6	192.168.15.1	DNS	71	Standard query 0x0002 A www.mit.edu
26	13:07:46,927913	192.168.15.1	192.168.15.6	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey...
27	13:07:46,934365	192.168.15.6	192.168.15.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
28	13:07:46,959058	192.168.15.1	192.168.15.6	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgek...

Frame 26: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface 0

Ethernet II, Src: Mitrasta_57:12:b0 (ac:c6:62:57:12:b0), Dst: AsustekC_8d:71:e9 (38:2c:4a:8d:71:e9)

Internet Protocol Version 4, Src: 192.168.15.1, Dst: 192.168.15.6

User Datagram Protocol, Src Port: 53, Dst Port: 65080

Source Port: 53

Destination Port: 65080

Length: 126

Checksum: 0xfa05 [unverified]

[Checksum Status: Unverified]

[Stream index: 1]

[Timestamps]

Domain Name System (response)

```

0020  0f 06 00 35 fe 38 00 7e fa 05 00 02 81 80 00 01  ...5.8~ .....
0030  00 03 00 00 00 00 03 77 77 77 03 6d 69 74 03 65  ....w ww.mit.e
0040  64 75 00 00 01 00 01 c0 0c 00 05 00 01 00 00 07  du.....
0050  08 00 19 03 77 77 77 03 6d 69 74 03 65 64 75 07  ...www mit.edu
0060  65 64 67 65 6b 65 79 03 6e 65 74 00 c0 29 00 05  edgekey net...

```

Domain Name System (dns), 118 bytes

Packets: 31 • Displayed: 6 (19.4%)

Profile: Default

12) O IP esta endereçada é 192.168.15.1, endereço do modem DSL-2401HN-T1C-NV.

DNS11a15.pcap.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.15.6 && dns

No.	Time	Source	Destination	Protocol	Length	Info
23	13:07:46,870278	192.168.15.6	192.168.15.1	DNS	85	Standard query 0x0001 PTR 1.15.168.192.in-addr.arpa
24	13:07:46,871282	192.168.15.1	192.168.15.6	DNS	134	Standard query response 0x0001 PTR 1.15.168.192.in-addr.arpa PTR DSL-24...
25	13:07:46,877159	192.168.15.6	192.168.15.1	DNS	71	Standard query 0x0002 A www.mit.edu
26	13:07:46,927913	192.168.15.1	192.168.15.6	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey...
27	13:07:46,934365	192.168.15.6	192.168.15.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
28	13:07:46,959058	192.168.15.1	192.168.15.6	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgek...

Frame 25: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0

Ethernet II, Src: AsustekC_8d:71:e9 (38:2c:4a:8d:71:e9), Dst: Mitrasta_57:12:b0 (ac:c6:62:57:12:b0)

Internet Protocol Version 4, Src: 192.168.15.6, Dst: 192.168.15.1

User Datagram Protocol, Src Port: 65080, Dst Port: 53

Domain Name System (query)

```

0000  ac c6 62 57 12 b0 38 2c 4a 8d 71 e9 08 00 45 00  ...bW...8, J.q...E
0010  00 39 77 5d 00 00 80 11 00 00 c0 a8 0f 06 c0 a8  ...9w]...
0020  0f 01 fe 38 00 35 00 25 9f 8e 00 02 01 00 00 01  ...8.5.% .....
0030  00 00 00 00 00 00 03 77 77 77 03 6d 69 74 03 65  ....w ww.mit.e
0040  64 75 00 00 01 00 01  du...

```

Length (udp.length), 2 bytes

Packets: 31 • Displayed: 6 (19.4%)

Profile: Default

13) Type: A, não contem campo "answer".

The screenshot shows a Wireshark capture of a DNS query. The packet list pane displays several DNS packets. Packet 25 is selected, showing a standard query for 'www.mit.edu' type A. The packet details pane shows the query structure: Name: www.mit.edu, Type: A (Host Address), Class: IN. The packet bytes pane shows the raw data of the query.

No.	Time	Source	Destination	Protocol	Length	Info
23	13:07:46,870278	192.168.15.6	192.168.15.1	DNS	85	Standard query 0x0001 PTR 1.15.168.192.in-addr.arpa
24	13:07:46,871282	192.168.15.1	192.168.15.6	DNS	134	Standard query response 0x0001 PTR 1.15.168.192.in-addr.arpa PTR DSL-24...
25	13:07:46,877159	192.168.15.6	192.168.15.1	DNS	71	Standard query 0x0002 A www.mit.edu
26	13:07:46,927913	192.168.15.1	192.168.15.6	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey...
27	13:07:46,934365	192.168.15.6	192.168.15.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
28	13:07:46,959058	192.168.15.1	192.168.15.6	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgek...

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 www.mit.edu: type A, class IN
 Name: www.mit.edu
 [Name Length: 11]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 [Response In: 26]

0000 ac c6 62 57 12 b0 38 2c 4a 8d 71 e9 08 00 45 00 8, J:q...E-
0010 00 39 77 5d 00 00 00 11 00 00 c0 a8 0f 06 c0 a8 ...9w]...
0020 0f 01 fe 38 00 35 00 25 9f 8e 00 02 01 00 00 01 ...8:5%
0030 00 00 00 00 00 00 03 77 77 77 03 6d 69 74 03 65w ww:mit'e
0040 64 75 00 00 01 00 01 du.....

14) Existem três campos, com cada qual contendo os respectivos dados de resposta como name, type, class, time, length e cname.

The screenshot shows a Wireshark capture of a DNS response. The packet list pane displays several DNS packets. Packet 26 is selected, showing a standard query response for 'www.mit.edu' type A. The packet details pane shows the response structure: Name: www.mit.edu, Type: A, Class: IN, CNAME: www.mit.edu.edgekey.net. The packet bytes pane shows the raw data of the response.

No.	Time	Source	Destination	Protocol	Length	Info
23	13:07:46,870278	192.168.15.6	192.168.15.1	DNS	85	Standard query 0x0001 PTR 1.15.168.192.in-addr.arpa
24	13:07:46,871282	192.168.15.1	192.168.15.6	DNS	134	Standard query response 0x0001 PTR 1.15.168.192.in-addr.arpa PTR DSL-24...
25	13:07:46,877159	192.168.15.6	192.168.15.1	DNS	71	Standard query 0x0002 A www.mit.edu
26	13:07:46,927913	192.168.15.1	192.168.15.6	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey...
27	13:07:46,934365	192.168.15.6	192.168.15.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
28	13:07:46,959058	192.168.15.1	192.168.15.6	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgek...

Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0
Queries
Answers
 www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
 www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
 e9566.dscb.akamaiedge.net: type A, class IN, addr 104.78.57.24
 [Request In: 25]
 [Time: 0.050754000 seconds]

0000 38 2c 4a 8d 71 e9 ac c6 62 57 12 b0 08 00 45 00 8,J:q...bw....E-
0010 00 92 00 00 40 00 00 11 9b 03 c0 a8 0f 01 c0 a8 ...@...
0020 0f 06 00 35 fe 38 00 7e fa 05 00 02 81 80 00 01 ...5:8~
0030 00 03 00 00 00 00 03 77 77 77 03 6d 69 74 03 65w ww:mit'e
0040 64 75 00 00 01 00 01 c0 0c 00 05 00 01 00 00 07 du.....

15)

Wireshark capture of DNS traffic for file DNS11a15.pcap.pcapng. The filter is `ip.addr == 192.168.15.6 && dns`. The packet list shows several DNS queries and responses. Packet 26 is selected, showing details for a Standard query response from 192.168.15.1 to 192.168.15.6. The domain name system section shows the response for `www.mit.edu`.

No.	Time	Source	Destination	Protocol	Length	Info
23	13:07:46,870278	192.168.15.6	192.168.15.1	DNS	85	Standard query 0x0001 PTR 1.15.168.192.in-addr.arpa
24	13:07:46,871282	192.168.15.1	192.168.15.6	DNS	134	Standard query response 0x0001 PTR 1.15.168.192.in-addr.arpa PTR DSL-24...
25	13:07:46,877159	192.168.15.6	192.168.15.1	DNS	71	Standard query 0x0002 A www.mit.edu
26	13:07:46,927913	192.168.15.1	192.168.15.6	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey...
27	13:07:46,934365	192.168.15.6	192.168.15.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
28	13:07:46,959058	192.168.15.1	192.168.15.6	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgek...

Frame 26: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface 0
 Ethernet II, Src: Mitrasa_57:12:b0 (ac:c6:62:57:12:b0), Dst: AsustekC_8d:71:e9 (38:2c:4a:8d:71:e9)
 Internet Protocol Version 4, Src: 192.168.15.1, Dst: 192.168.15.6
 User Datagram Protocol, Src Port: 53, Dst Port: 65000
 Domain Name System (response)

0000 38 2c 4a 8d 71 e9 ac c6 62 57 12 b0 08 00 45 00 8, J . q . . . b W E .
 0010 00 92 00 00 40 00 00 11 9b 03 c0 a8 0f 01 c0 a8 @
 0020 0f 06 00 35 fe 38 00 7e fa 05 00 02 81 80 00 01 . . . 5 - 8 ~
 0030 00 03 00 00 00 00 03 77 77 77 03 6d 69 74 03 65 w w w . m i t . e
 0040 64 75 00 01 00 01 c0 0c 00 05 00 01 00 00 07 d u

16) O IP esta endereçada é 192.168.15.1, endereço do modem DSL-2401HN-T1C-NV.

Wireshark capture of DNS traffic for file DNS16a19.pcap.pcapng. The filter is `ip.addr == 192.168.15.6 && dns`. The packet list shows several DNS queries and responses. Packet 5 is selected, showing details for a Standard query from 192.168.15.1 to 192.168.15.6. The domain name system section shows the query for `pucminas.br`.

No.	Time	Source	Destination	Protocol	Length	Info
1	14:13:03,175237	192.168.15.6	192.168.15.1	DNS	85	Standard query 0x0001 PTR 1.15.168.192.in-addr.arpa
2	14:13:03,176316	192.168.15.1	192.168.15.6	DNS	134	Standard query response 0x0001 PTR 1.15.168.192.in-addr.arpa PTR DSL-24...
3	14:13:03,182477	192.168.15.6	192.168.15.1	DNS	71	Standard query 0x0002 NS pucminas.br
5	14:13:03,391568	192.168.15.1	192.168.15.6	DNS	235	Standard query response 0x0002 NS pucminas.br NS ns01.telmx.net.br NS ...

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 57
 Identification: 0x7a6c (31340)
 Flags: 0x0000
 Time to live: 128
 Protocol: UDP (17)
 Header checksum: 0x0000 [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.15.6
 Destination: 192.168.15.1
 User Datagram Protocol, Src Port: 51300, Dst Port: 53
 Domain Name System (query)

0000 ac c6 62 57 12 b0 38 2c 4a 8d 71 e9 08 00 45 00 . . b W . . . 8, J . q . . . E .
 0010 00 39 7a 6c 00 00 00 11 00 00 c0 a8 0f 06 c0 a8 . . 9 z 1
 0020 0f 01 c8 64 00 35 00 25 9f 8e 00 02 01 00 00 01 . . . d - 5 %
 0030 00 00 00 00 00 00 00 75 63 6d 69 6e 61 73 02 p u c m i n a s .
 0040 62 72 00 00 02 00 01 b r

17) Type: NS, não contem.

The screenshot shows a Wireshark capture of a DNS query and response. The filter is set to `ip.addr == 192.168.15.6 && dns`. The packet list shows a query (No. 3) and a response (No. 5). The packet details pane for packet 5 shows the response structure: Questions: 1, Answer RRs: 0, Authority RRs: 0, Additional RRs: 0. Under Queries, it lists the query for `pucminas.br` with type NS and class IN. The response section shows a single NS record for `pucminas.br` with type NS, class IN, and a reference to `ns01.telmx.net.br`. The packet bytes pane shows the raw data of the response.

No.	Time	Source	Destination	Protocol	Length	Info
1	14:13:03.175237	192.168.15.6	192.168.15.1	DNS	85	Standard query 0x0001 PTR 1.15.168.192.in-addr.arpa
2	14:13:03.176316	192.168.15.1	192.168.15.6	DNS	134	Standard query response 0x0001 PTR 1.15.168.192.in-addr.arpa PTR DSL-24...
3	14:13:03.182477	192.168.15.6	192.168.15.1	DNS	71	Standard query 0x0002 NS pucminas.br
5	14:13:03.391568	192.168.15.1	192.168.15.6	DNS	235	Standard query response 0x0002 NS pucminas.br NS ns01.telmx.net.br NS ...

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0

Queries

- pucminas.br: type NS, class IN
Name: pucminas.br
[Name Length: 11]
[Label Count: 2]
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
[Response In: 5]

0000 ac c6 62 57 12 b0 38 2c 4a 8d 71 e9 08 00 45 00 ..bW..8, J.q...E.
0010 00 39 7a 6c 00 00 80 11 00 00 c0 a8 0f 06 c0 a8 ..9z1...
0020 0f 01 c8 64 00 35 00 25 9f 8e 00 02 01 00 00 01d.5%
0030 00 00 00 00 00 00 08 70 75 63 6d 69 6e 61 73 02p ucminas.
0040 62 72 00 00 02 00 01 br.....

Destination Hardware Address (eth.dst), 6 bytes | Packets: 22 · Displayed: 4 (18.2%) · Dropped: 0 (0.0%) | Profile: Default

18) ns.pucminas.br, não oferece os IPS dos servidores DNS.

The screenshot shows a Wireshark capture of a DNS query and response. The filter is set to `ip.addr == 192.168.15.6 && dns`. The packet list shows a query (No. 3) and a response (No. 5). The packet details pane for packet 5 shows the response structure: Authority RRs: 0, Additional RRs: 2. Under Answers, it lists five NS records for `pucminas.br` with type NS, class IN, and references to `ns01.telmx.net.br`, `dns02.redeinfovias.net.br`, `ns.embratel.net.br`, `ns2.telbrax.net.br`, and `ns.pucminas.br`. The packet bytes pane shows the raw data of the response.

No.	Time	Source	Destination	Protocol	Length	Info
1	14:13:03.175237	192.168.15.6	192.168.15.1	DNS	85	Standard query 0x0001 PTR 1.15.168.192.in-addr.arpa
2	14:13:03.176316	192.168.15.1	192.168.15.6	DNS	134	Standard query response 0x0001 PTR 1.15.168.192.in-addr.arpa PTR DSL-24...
3	14:13:03.182477	192.168.15.6	192.168.15.1	DNS	71	Standard query 0x0002 NS pucminas.br
5	14:13:03.391568	192.168.15.1	192.168.15.6	DNS	235	Standard query response 0x0002 NS pucminas.br NS ns01.telmx.net.br NS ...

Authority RRs: 0
Additional RRs: 2

Queries

Answers

- pucminas.br: type NS, class IN, ns ns01.telmx.net.br
- pucminas.br: type NS, class IN, ns dns02.redeinfovias.net.br
- pucminas.br: type NS, class IN, ns ns.embratel.net.br
- pucminas.br: type NS, class IN, ns ns2.telbrax.net.br
- pucminas.br: type NS, class IN, ns ns.pucminas.br

Additional records
[Request In: 3]
[Time: 0.209091000 seconds]

0000 38 2c 4a 8d 71 e9 ac c6 62 57 12 b0 08 00 45 00 8,J.q...bW...E.
0010 00 dd 00 00 00 40 11 9a b8 c0 a8 0f 01 c0 a8 ...@.@...
0020 0f 06 00 35 c8 64 00 c9 42 3d 00 02 81 80 00 01 ...5.d..B=
0030 00 05 00 00 00 02 08 70 75 63 6d 69 6e 61 73 02p ucminas.
0040 62 72 00 00 02 00 01 c0 0c 00 02 00 01 00 00 00 br.....

Destination Hardware Address (eth.dst), 6 bytes | Packets: 22 · Displayed: 4 (18.2%) · Dropped: 0 (0.0%) | Profile: Default

19)

Wireshark capture of DNS traffic for file DNS16a19.pcap.pcapng. The packet list shows four packets:

No.	Time	Source	Destination	Protocol	Length	Info
1	14:13:03.175237	192.168.15.6	192.168.15.1	DNS	85	Standard query 0x0001 PTR 1.15.168.192.in-addr.arpa
2	14:13:03.176316	192.168.15.1	192.168.15.6	DNS	134	Standard query response 0x0001 PTR 1.15.168.192.in-addr.arpa PTR DSL-24...
3	14:13:03.182477	192.168.15.6	192.168.15.1	DNS	71	Standard query 0x0002 NS pucminas.br
5	14:13:03.391568	192.168.15.1	192.168.15.6	DNS	235	Standard query response 0x0002 NS pucminas.br NS ns01.telmex.net.br NS ...

The selected packet (No. 5) is expanded to show details of the Domain Name System response, including the source IP 192.168.15.1 and destination 192.168.15.6. The packet bytes pane shows the raw data in hexadecimal and ASCII.

20) O IP esta endereçada é 192.168.15.1, endereço do modem DSL-2401HN-T1C-NV.

Wireshark capture of DNS traffic for file DNS20a23.pcap.pcapng. The packet list shows five packets:

No.	Time	Source	Destination	Protocol	Length	Info
4	14:32:21.410898	192.168.15.6	192.168.15.1	DNS	85	Standard query 0x0001 PTR 1.15.168.192.in-addr.arpa
5	14:32:21.411855	192.168.15.1	192.168.15.6	DNS	134	Standard query response 0x0001 PTR 1.15.168.192.in-addr.arpa PTR DSL-24...
6	14:32:21.418009	192.168.15.6	192.168.15.1	DNS	74	Standard query 0x0002 A www.aiit.or.kr
7	14:32:21.799907	192.168.15.1	192.168.15.6	DNS	90	Standard query response 0x0002 A www.aiit.or.kr A 58.229.6.225
8	14:32:21.806409	192.168.15.6	192.168.15.1	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
9	14:32:22.162412	192.168.15.1	192.168.15.6	DNS	128	Standard query response 0x0003 AAAA www.aiit.or.kr SOA ns9.dnszi.com

The selected packet (No. 8) is expanded to show details of the Domain Name System response, including the source IP 192.168.15.1 and destination 192.168.15.6. The packet bytes pane shows the raw data in hexadecimal and ASCII.

21) Type: A, não contem.

The screenshot shows a Wireshark capture of DNS traffic. The filter is set to `ip.addr == 192.168.15.6 && dns`. The packet list shows several DNS messages. The packet details pane is expanded to show the query for `www.aiit.or.kr` with type A, class IN. The packet bytes pane shows the raw data of the query.

No.	Time	Source	Destination	Protocol	Length	Info
4	14:32:21,410898	192.168.15.6	192.168.15.1	DNS	85	Standard query 0x0001 PTR 1.15.168.192.in-addr.arpa
5	14:32:21,411855	192.168.15.1	192.168.15.6	DNS	134	Standard query response 0x0001 PTR 1.15.168.192.in-addr.arpa PTR DSL-24...
6	14:32:21,418009	192.168.15.6	192.168.15.1	DNS	74	Standard query 0x0002 A www.aiit.or.kr
7	14:32:21,799907	192.168.15.1	192.168.15.6	DNS	90	Standard query response 0x0002 A www.aiit.or.kr A 58.229.6.225
8	14:32:21,806409	192.168.15.6	192.168.15.1	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
9	14:32:22,162412	192.168.15.1	192.168.15.6	DNS	128	Standard query response 0x0003 AAAA www.aiit.or.kr SOA ns9.dnszi.com

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 www.aiit.or.kr: type A, class IN
 Name: www.aiit.or.kr
 [Name Length: 14]
 [Label Count: 4]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 [Response In: 7]

Domain Name System (dns), 32 bytes

22) Apenas 1, do nome até o endereço de resposta de www.aiit.or.kr

The screenshot shows a Wireshark capture of DNS traffic. The filter is set to `ip.addr == 192.168.15.6 && dns`. The packet list shows several DNS messages. The packet details pane is expanded to show the query for `www.aiit.or.kr` with type A, class IN, and the response address 58.229.6.225. The packet bytes pane shows the raw data of the query.

No.	Time	Source	Destination	Protocol	Length	Info
4	14:32:21,410898	192.168.15.6	192.168.15.1	DNS	85	Standard query 0x0001 PTR 1.15.168.192.in-addr.arpa
5	14:32:21,411855	192.168.15.1	192.168.15.6	DNS	134	Standard query response 0x0001 PTR 1.15.168.192.in-addr.arpa PTR DSL-24...
6	14:32:21,418009	192.168.15.6	192.168.15.1	DNS	74	Standard query 0x0002 A www.aiit.or.kr
7	14:32:21,799907	192.168.15.1	192.168.15.6	DNS	90	Standard query response 0x0002 A www.aiit.or.kr A 58.229.6.225
8	14:32:21,806409	192.168.15.6	192.168.15.1	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
9	14:32:22,162412	192.168.15.1	192.168.15.6	DNS	128	Standard query response 0x0003 AAAA www.aiit.or.kr SOA ns9.dnszi.com

Additional RRs: 0
Queries
 www.aiit.or.kr: type A, class IN, addr 58.229.6.225
 Name: www.aiit.or.kr
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 7200
 Data length: 4
 Address: 58.229.6.225
 [Request In: 6]
 [Time: 0.381898000 seconds]

Domain Name System (dns), 48 bytes

23)

DNS20a23.pcap.pcapng

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

ip.addr == 192.168.15.6 && dns

Expression...

No.	Time	Source	Destination	Protocol	Length	Info
4	14:32:21,410898	192.168.15.6	192.168.15.1	DNS	85	Standard query 0x0001 PTR 1.15.168.192.in-addr.arpa
5	14:32:21,411855	192.168.15.1	192.168.15.6	DNS	134	Standard query response 0x0001 PTR 1.15.168.192.in-addr.arpa PTR DSL-24...
6	14:32:21,418009	192.168.15.6	192.168.15.1	DNS	74	Standard query 0x0002 A www.aiit.or.kr
7	14:32:21,799907	192.168.15.1	192.168.15.6	DNS	90	Standard query response 0x0002 A www.aiit.or.kr A 58.229.6.225
8	14:32:21,806409	192.168.15.6	192.168.15.1	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
9	14:32:22,162412	192.168.15.1	192.168.15.6	DNS	128	Standard query response 0x0003 AAAA www.aiit.or.kr SOA ns9.dnszi.com

▶ Frame 7: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0

▶ Ethernet II, Src: Mitrasta_57:12:b0 (ac:c6:62:57:12:b0), Dst: AsustekC_8d:71:e9 (38:2c:4a:8d:71:e9)

▶ Internet Protocol Version 4, Src: 192.168.15.1, Dst: 192.168.15.6

▶ User Datagram Protocol, Src Port: 53, Dst Port: 53723

▶ Domain Name System (response)

0010 00 4c 00 00 40 00 40 11 9b 49 c0 a8 0f 01 c0 a8 .L..@...I.....

0020 0f 06 00 35 d1 db 00 38 ad fc 00 02 81 80 00 01 ...5...8.....

0030 00 01 00 00 00 00 03 77 77 77 04 61 69 69 74 02w ww.aiit.

0040 6f 72 02 6b 72 00 00 01 00 01 c0 0c 00 01 00 01 or.kr.....

0050 00 00 1c 20 00 04 3a e5 06 e1 ...:..

Domain Name System (dns), 48 bytes

Packets: 17 · Displayed: 6 (35.3%) · Dropped: 0 (0.0%) | Profile: Default