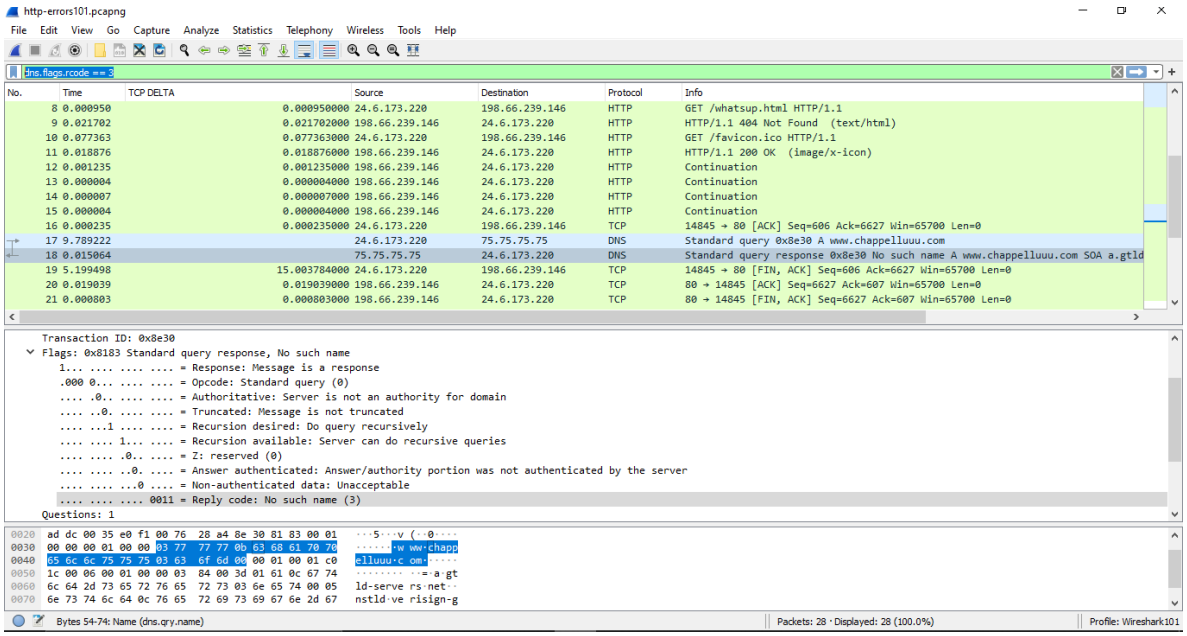
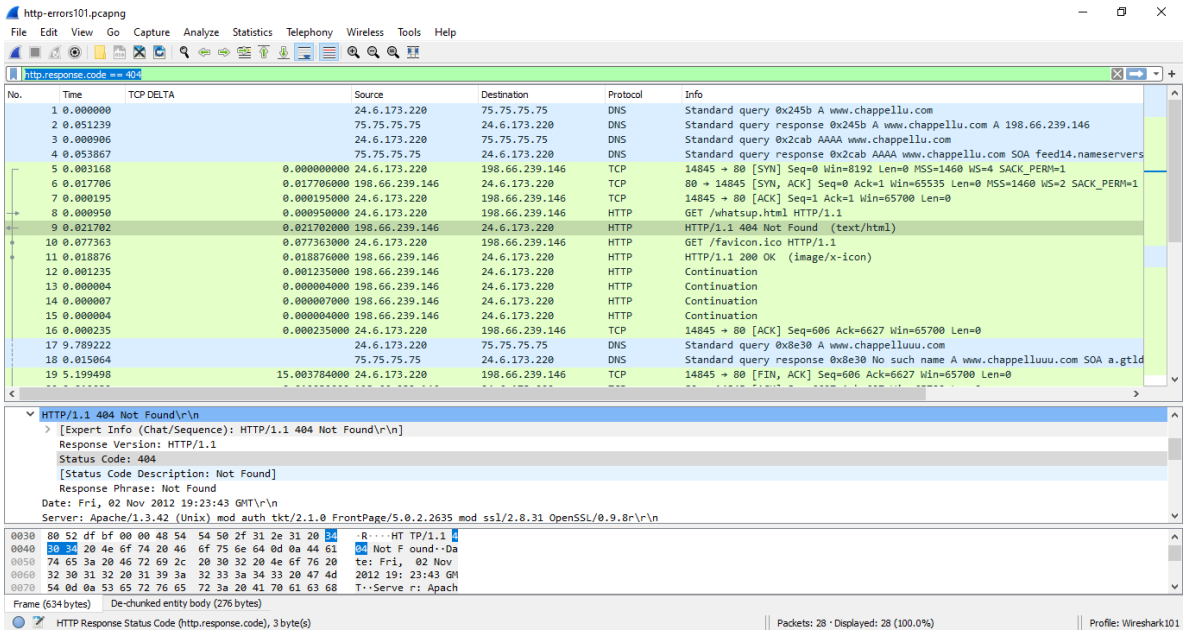
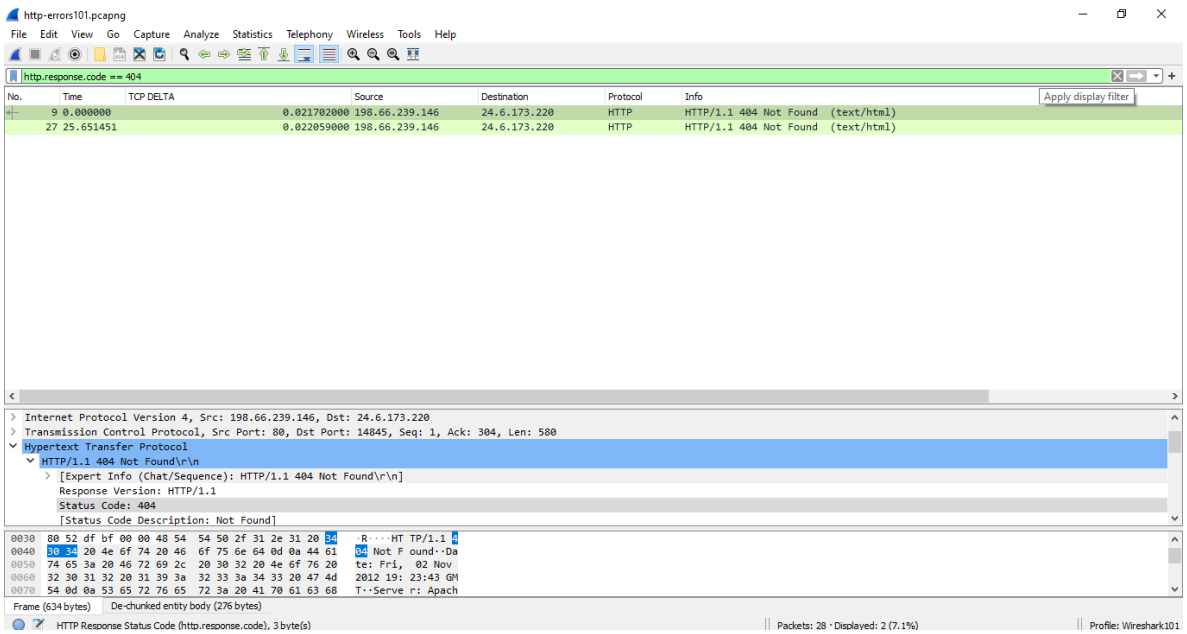
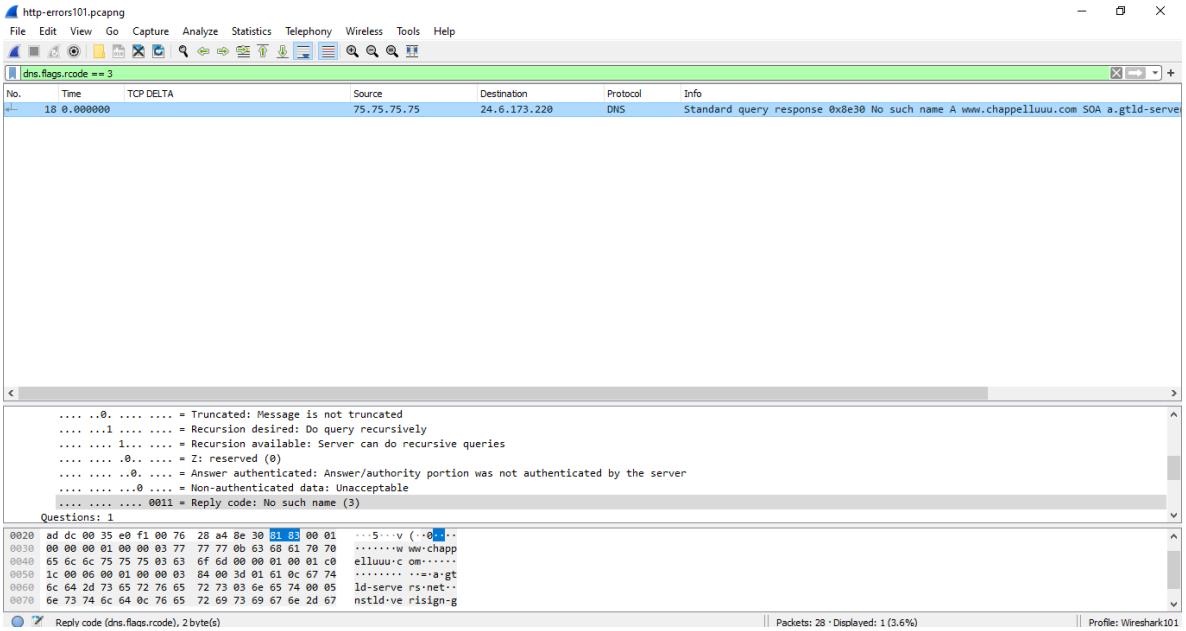
Laboratorio 18
Wireshark

Wilmer Rodríguez Jiménez
Fundamentos de telecomunicaciones
Prof: Ismael Jimenez Sanchez
Periodo Ago – Dic


http-errors101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns.flags.rcode == 3
No. Time TCP DELTA Source Destination Protocol Info
8 0.000950 0.000950000 24.6.173.220 198.66.239.146 HTTP GET /whatsup.html HTTP/1.1
9 0.021702 0.021702000 198.66.239.146 24.6.173.220 HTTP HTTP/1.1 404 Not Found (text/html)
10 0.077363 0.077363000 24.6.173.220 198.66.239.146 HTTP GET /favicon.ico HTTP/1.1
11 0.018876 0.018876000 198.66.239.146 24.6.173.220 HTTP HTTP/1.1 200 OK (image/x-icon)
12 0.001235 0.001235000 198.66.239.146 24.6.173.220 HTTP Continuation
13 0.000004 0.000004000 198.66.239.146 24.6.173.220 HTTP Continuation
14 0.000007 0.000007000 198.66.239.146 24.6.173.220 HTTP Continuation
15 0.000004 0.000004000 198.66.239.146 24.6.173.220 HTTP Continuation
16 0.000235 0.000235000 24.6.173.220 198.66.239.146 TCP 14845 → 80 [ACK] Seq=606 Ack=6627 Win=65700 Len=0
17 9.789222 24.6.173.220 75.75.75.75 DNS Standard query 0x8e30 A www.chappelluuu.com
18 0.015064 75.75.75.75 24.6.173.220 DNS Standard query response 0x8e30 No such name A www.chappelluuu.com SOA a.gtld
19 5.199498 15.003784000 24.6.173.220 198.66.239.146 TCP 14845 → 80 [FIN, ACK] Seq=606 Ack=6627 Win=65700 Len=0
20 0.019039 0.019039000 198.66.239.146 24.6.173.220 TCP 80 → 14845 [ACK] Seq=6627 Ack=607 Win=65700 Len=0
21 0.000803 0.000803000 198.66.239.146 24.6.173.220 TCP 80 → 14845 [FIN, ACK] Seq=6627 Ack=607 Win=65700 Len=0
Transaction ID: 0x8e30
Flags: 0x8183 Standard query response, No such name
1... .... = Response: Message is a response
.000 0... .... = Opcode: Standard query (0)
.... .0.. .... = Authoritative: Server is not an authority for domain
.... ..0. .... = Truncated: Message is not truncated
....1 .... = Recursion desired: Do query recursively
.... 1... .... = Recursion available: Server can do recursive queries
.... .0.. .... = Z: reserved (0)
....0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 .... = Non-authenticated data: Unacceptable
.... 0011 = Reply code: No such name (3)
Questions: 1
0020 ad dc 00 35 e0 f1 00 76 28 a4 8e 30 81 83 00 01 ···5···v (··0····
0030 00 00 00 01 00 00 03 77 77 77 0b 63 68 61 70 70 ·······w ww·chapp
0040 65 6c 6c 75 75 75 03 63 6f 6d 00 00 01 00 01 c0 elluuu·c om·····
0050 1c 00 06 00 01 00 00 03 84 00 3d 01 61 0c 67 74 ······ ··=·a·gt
0060 6c 64 2d 73 65 72 76 65 72 73 03 6e 65 74 00 05 ld-serve rs·net··
0070 6e 73 74 6c 64 0c 76 65 72 69 73 69 67 6e 2d 67 nstld·ve risign-g
Bytes 54-74: Name (dns.qry.name)
Packets: 28 · Displayed: 28 (100.0%)
Profile: Wireshark101


http-errors101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.response.code == 404
No. Time TCP DELTA Source Destination Protocol Info
1 0.000000 24.6.173.220 75.75.75.75 DNS Standard query 0x245b A www.chappellu.com
2 0.051239 75.75.75.75 24.6.173.220 DNS Standard query response 0x245b A www.chappellu.com A 198.66.239.146
3 0.000906 24.6.173.220 75.75.75.75 DNS Standard query 0x2cab AAAA www.chappellu.com
4 0.053867 75.75.75.75 24.6.173.220 DNS Standard query response 0x2cab AAAA www.chappellu.com SOA feed14.nameservers
5 0.003168 0.000000000 24.6.173.220 198.66.239.146 TCP 14845 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
6 0.017706 0.017706000 198.66.239.146 24.6.173.220 TCP 80 → 14845 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=2 SACK_PERM=1
7 0.000195 0.000195000 24.6.173.220 198.66.239.146 TCP 14845 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
8 0.000950 0.000950000 24.6.173.220 198.66.239.146 HTTP GET /whatsup.html HTTP/1.1
9 0.021702 0.021702000 198.66.239.146 24.6.173.220 HTTP HTTP/1.1 404 Not Found (text/html)
10 0.077363 0.077363000 24.6.173.220 198.66.239.146 HTTP GET /favicon.ico HTTP/1.1
11 0.018876 0.018876000 198.66.239.146 24.6.173.220 HTTP HTTP/1.1 200 OK (image/x-icon)
12 0.001235 0.001235000 198.66.239.146 24.6.173.220 HTTP Continuation
13 0.000004 0.000004000 198.66.239.146 24.6.173.220 HTTP Continuation
14 0.000007 0.000007000 198.66.239.146 24.6.173.220 HTTP Continuation
15 0.000004 0.000004000 198.66.239.146 24.6.173.220 HTTP Continuation
16 0.000235 0.000235000 24.6.173.220 198.66.239.146 TCP 14845 → 80 [ACK] Seq=606 Ack=6627 Win=65700 Len=0
17 9.789222 24.6.173.220 75.75.75.75 DNS Standard query 0x8e30 A www.chappelluuu.com
18 0.015064 75.75.75.75 24.6.173.220 DNS Standard query response 0x8e30 No such name A www.chappelluuu.com SOA a.gtld
19 5.199498 15.003784000 24.6.173.220 198.66.239.146 TCP 14845 → 80 [FIN, ACK] Seq=606 Ack=6627 Win=65700 Len=0
HTTP/1.1 404 Not Found\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found\r\n]
Response Version: HTTP/1.1
Status Code: 404
[Status Code Description: Not Found]
Response Phrase: Not Found
Date: Fri, 02 Nov 2012 19:23:43 GMT\r\n
Server: Apache/1.3.42 (Unix) mod_auth_tkt/2.1.0 FrontPage/5.0.2.2635 mod_ssl/2.8.31 OpenSSL/0.9.8r\r\n
0030 80 52 df bf 00 00 48 54 54 50 2f 31 2e 31 20 34 ·R····HT TP/1.1 4
0040 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0d 0a 44 61 04 Not F ound··Da
0050 74 65 3a 20 46 72 69 2c 20 30 32 20 4e 6f 76 20 te: Fri, 02 Nov
0060 32 30 31 32 20 31 39 3a 32 33 3a 34 33 20 47 4d 2012 19: 23:43 GM
0070 54 0d 0a 53 65 72 76 65 72 3a 20 41 70 61 63 68 T··Serve r: Apach
Frame (634 bytes)
De-chunked entity body (276 bytes)
HTTP Response Status Code (http.response.code), 3 byte(s)
Packets: 28 · Displayed: 28 (100.0%)
Profile: Wireshark101


http-errors101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.response.code == 404
Apply display filter
No. Time TCP DELTA Source Destination Protocol Info
9 0.000000 0.021702000 198.66.239.146 24.6.173.220 HTTP HTTP/1.1 404 Not Found (text/html)
27 25.651451 0.022059000 198.66.239.146 24.6.173.220 HTTP HTTP/1.1 404 Not Found (text/html)
Internet Protocol Version 4, Src: 198.66.239.146, Dst: 24.6.173.220
Transmission Control Protocol, Src Port: 80, Dst Port: 14845, Seq: 1, Ack: 304, Len: 580
Hypertext Transfer Protocol
HTTP/1.1 404 Not Found\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found\r\n]
Response Version: HTTP/1.1
Status Code: 404
[Status Code Description: Not Found]
0030 80 52 df bf 00 00 48 54 54 50 2f 31 2e 31 20 34 ·R····HT TP/1.1 4
0040 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0d 0a 44 61 04 Not F ound··Da
0050 74 65 3a 20 46 72 69 2c 20 30 32 20 4e 6f 76 20 te: Fri, 02 Nov
0060 32 30 31 32 20 31 39 3a 32 33 3a 34 33 20 47 4d 2012 19: 23:43 GM
0070 54 0d 0a 53 65 72 76 65 72 3a 20 41 70 61 63 68 T··Serve r: Apach
Frame (634 bytes)
De-chunked entity body (276 bytes)
HTTP Response Status Code (http.response.code), 3 byte(s)
Packets: 28 · Displayed: 2 (7.1%)
Profile: Wireshark101


http-errors101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns.flags.rcode == 3
No. Time TCP DELTA Source Destination Protocol Info
18 0.000000 75.75.75.75 24.6.173.220 DNS Standard query response 0x8e30 No such name A www.chappelluuu.com SOA a.gtld-serve
.... ..0. .... = Truncated: Message is not truncated
....1 .... = Recursion desired: Do query recursively
.... 1... .... = Recursion available: Server can do recursive queries
.... .0.. .... = Z: reserved (0)
....0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 .... = Non-authenticated data: Unacceptable
.... 0011 = Reply code: No such name (3)
Questions: 1
0020 ad dc 00 35 e0 f1 00 76 28 a4 8e 30 81 83 00 01
0030 00 00 00 01 00 00 03 77 77 77 0b 63 68 61 70 70
0040 65 6c 6c 75 75 75 03 63 6f 6d 00 00 01 00 01 c0
0050 1c 00 06 00 01 00 00 03 84 00 3d 01 61 0c 67 74
0060 6c 64 2d 73 65 72 76 65 72 73 03 6e 65 74 00 05
0070 6e 73 74 6c 64 0c 76 65 72 69 73 69 67 6e 2d 67
Reply code (dns.flags.rcode), 2 byte(s)
Packets: 28 · Displayed: 1 (3.6%)
Profile: Wireshark101