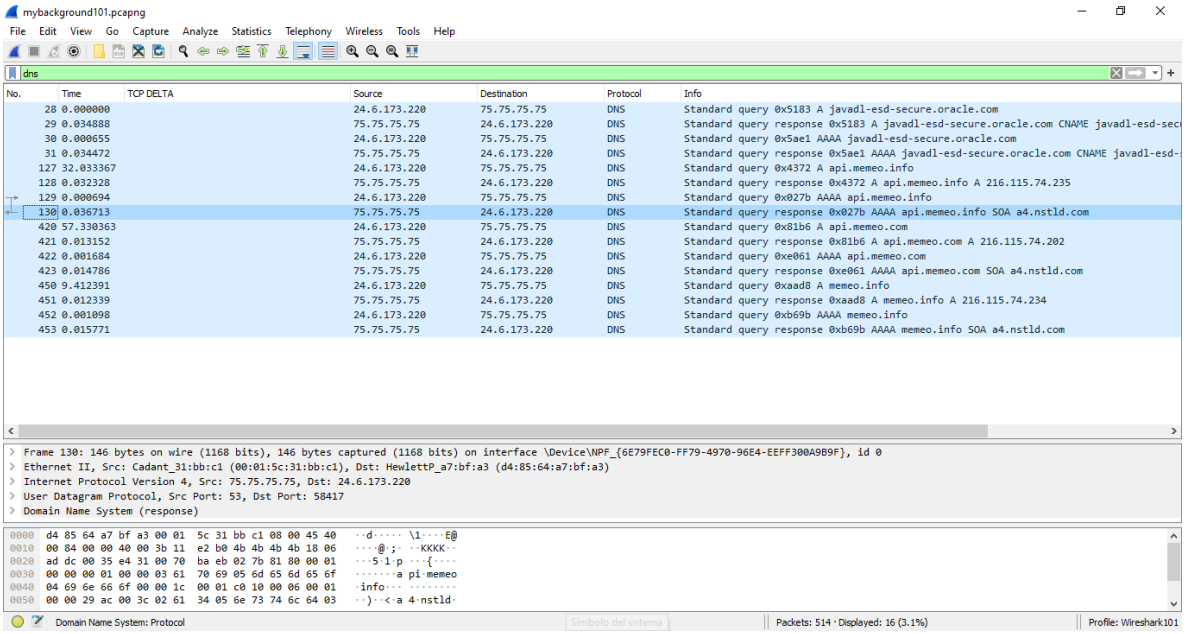
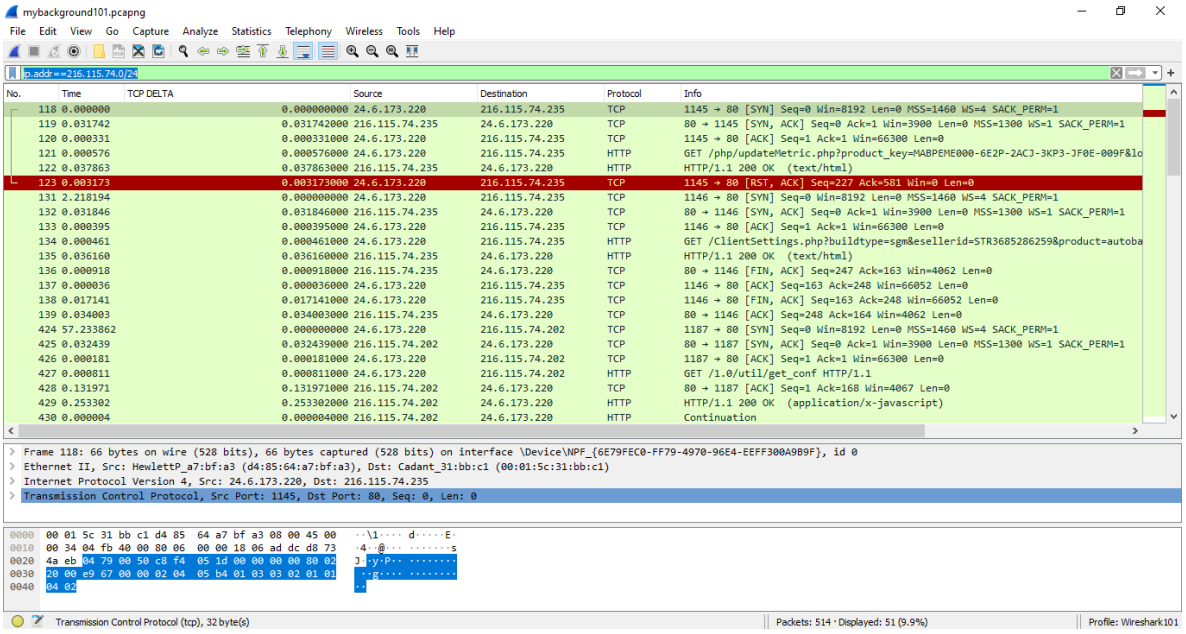
Laboratorio 17
Wireshark

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


mybackground101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time TCP DELTA Source Destination Protocol Info
28 0.000000 24.6.173.220 75.75.75.75 DNS Standard query 0x5183 A javadl-esd-secure.oracle.com
29 0.034888 75.75.75.75 24.6.173.220 DNS Standard query response 0x5183 A javadl-esd-secure.oracle.com CNAME javadl-esd-sec
30 0.000655 24.6.173.220 75.75.75.75 DNS Standard query 0x5ae1 AAAA javadl-esd-secure.oracle.com
31 0.034472 75.75.75.75 24.6.173.220 DNS Standard query response 0x5ae1 AAAA javadl-esd-secure.oracle.com CNAME javadl-esd-
127 32.033367 24.6.173.220 75.75.75.75 DNS Standard query 0x4372 A api.memeo.info
128 0.032328 75.75.75.75 24.6.173.220 DNS Standard query response 0x4372 A api.memeo.info A 216.115.74.235
129 0.000694 24.6.173.220 75.75.75.75 DNS Standard query 0x027b AAAA api.memeo.info
130 0.036713 75.75.75.75 24.6.173.220 DNS Standard query response 0x027b AAAA api.memeo.info SOA a4.nstld.com
420 57.330363 24.6.173.220 75.75.75.75 DNS Standard query 0x81b6 A api.memeo.com
421 0.013152 75.75.75.75 24.6.173.220 DNS Standard query response 0x81b6 A api.memeo.com A 216.115.74.202
422 0.001684 24.6.173.220 75.75.75.75 DNS Standard query 0xe061 AAAA api.memeo.com
423 0.014786 75.75.75.75 24.6.173.220 DNS Standard query response 0xe061 AAAA api.memeo.com SOA a4.nstld.com
450 9.412391 24.6.173.220 75.75.75.75 DNS Standard query 0xaad8 A memeo.info
451 0.012339 75.75.75.75 24.6.173.220 DNS Standard query response 0xaad8 A memeo.info A 216.115.74.234
452 0.001098 24.6.173.220 75.75.75.75 DNS Standard query 0xb69b AAAA memeo.info
453 0.015771 75.75.75.75 24.6.173.220 DNS Standard query response 0xb69b AAAA memeo.info SOA a4.nstld.com
Frame 130: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}, id 0
Ethernet II, Src: Cadant_31:bb:c1 (00:01:5c:31:bb:c1), Dst: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3)
Internet Protocol Version 4, Src: 75.75.75.75, Dst: 24.6.173.220
User Datagram Protocol, Src Port: 53, Dst Port: 58417
Domain Name System (response)
0000 d4 85 64 a7 bf a3 00 01 5c 31 bb c1 08 00 45 40
0010 00 84 00 00 40 00 3b 11 e2 b0 4b 4b 4b 18 06
0020 ad dc 00 35 e4 31 00 70 ba eb 02 7b 81 80 00 01
0030 00 00 00 01 00 00 03 61 70 69 05 6d 65 6d 65 6f
0040 04 69 6e 66 6f 00 00 1c 00 01 c0 10 00 06 00 01
0050 00 00 29 ac 00 3c 02 61 34 05 6e 73 74 6c 64 03
Domain Name System: Protocol
Packets: 514 · Displayed: 16 (3.1%)
Profile: Wireshark101


mybackground101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==216.115.74.0/24
No. Time TCP DELTA Source Destination Protocol Info
118 0.000000 0.000000000 24.6.173.220 216.115.74.235 TCP 1145 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
119 0.031742 0.031742000 216.115.74.235 24.6.173.220 TCP 80 → 1145 [SYN, ACK] Seq=0 Ack=1 Win=3900 Len=0 MSS=1300 WS=1 SACK_PERM=1
120 0.000331 0.000331000 24.6.173.220 216.115.74.235 TCP 1145 → 80 [ACK] Seq=1 Ack=1 Win=66300 Len=0
121 0.000576 0.000576000 24.6.173.220 216.115.74.235 HTTP GET /php/updateMetric.php?product_key=MABPEME000-6E2P-2ACJ-3KP3-JF0E-009F&lo
122 0.037863 0.037863000 216.115.74.235 24.6.173.220 HTTP HTTP/1.1 200 OK (text/html)
123 0.003173 0.003173000 24.6.173.220 216.115.74.235 TCP 1145 → 80 [RST, ACK] Seq=227 Ack=581 Win=0 Len=0
131 2.218194 0.000000000 24.6.173.220 216.115.74.235 TCP 1146 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
132 0.031846 0.031846000 216.115.74.235 24.6.173.220 TCP 80 → 1146 [SYN, ACK] Seq=0 Ack=1 Win=3900 Len=0 MSS=1300 WS=1 SACK_PERM=1
133 0.000395 0.000395000 24.6.173.220 216.115.74.235 TCP 1146 → 80 [ACK] Seq=1 Ack=1 Win=66300 Len=0
134 0.000461 0.000461000 24.6.173.220 216.115.74.235 HTTP GET /ClientSettings.php?buildtype=sgm&esellerid=STR3685286259&product=autoba
135 0.036160 0.036160000 216.115.74.235 24.6.173.220 HTTP HTTP/1.1 200 OK (text/html)
136 0.000918 0.000918000 216.115.74.235 24.6.173.220 TCP 80 → 1146 [FIN, ACK] Seq=247 Ack=163 Win=4062 Len=0
137 0.000036 0.000036000 24.6.173.220 216.115.74.235 TCP 1146 → 80 [ACK] Seq=163 Ack=248 Win=66052 Len=0
138 0.017141 0.017141000 24.6.173.220 216.115.74.235 TCP 1146 → 80 [FIN, ACK] Seq=163 Ack=248 Win=66052 Len=0
139 0.034003 0.034003000 216.115.74.235 24.6.173.220 TCP 80 → 1146 [ACK] Seq=248 Ack=164 Win=4062 Len=0
424 57.233862 0.000000000 24.6.173.220 216.115.74.202 TCP 1187 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
425 0.032439 0.032439000 216.115.74.202 24.6.173.220 TCP 80 → 1187 [SYN, ACK] Seq=0 Ack=1 Win=3900 Len=0 MSS=1300 WS=1 SACK_PERM=1
426 0.000181 0.000181000 24.6.173.220 216.115.74.202 TCP 1187 → 80 [ACK] Seq=1 Ack=1 Win=66300 Len=0
427 0.000811 0.000811000 24.6.173.220 216.115.74.202 HTTP GET /1.0/util/get_conf HTTP/1.1
428 0.131971 0.131971000 216.115.74.202 24.6.173.220 TCP 80 → 1187 [ACK] Seq=1 Ack=168 Win=4067 Len=0
429 0.253302 0.253302000 216.115.74.202 24.6.173.220 HTTP HTTP/1.1 200 OK (application/x-javascript)
430 0.000004 0.000004000 216.115.74.202 24.6.173.220 HTTP Continuation
Frame 118: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}, id 0
Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
Internet Protocol Version 4, Src: 24.6.173.220, Dst: 216.115.74.235
Transmission Control Protocol, Src Port: 1145, Dst Port: 80, Seq: 0, Len: 0
0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00
0010 00 34 04 fb 40 00 80 06 00 00 18 06 ad dc d8 73
0020 4a eb 04 79 00 50 c8 f4 05 1d 00 00 00 00 80 02
0030 20 00 e9 67 00 00 02 04 05 b4 01 03 03 02 01 01
0040 04 02
Transmission Control Protocol (tcp), 32 byte(s)
Packets: 514 · Displayed: 51 (9.9%)
Profile: Wireshark101