

Instituto Tecnológico de Cancún

Fundamentos de Telecomunicaciones

**Lab17 - Filter on Traffic to or from
Online Backup Subnets**

Prof. Ismael Jiménez Sánchez

**Alumno(a). Laury del Rosario Mex
Martin**

Ciclo 2020-B

Paso 1: Aplicaremos el filtro **dns** y notaremos la IP de *api.memeeo.info* y *api.memeeo.com* que tiene como comienzo **216.115.74**, y veremos que solo hay 16 paquetes

The screenshot shows the Wireshark interface with the filter 'dns' applied. The packet list displays 16 DNS-related packets. The packet details pane shows the structure of a DNS Standard query response from 216.115.74.235 to 24.6.173.220.

No.	Time	TCP Delta	Source	Destination	Protocol	Host	Info
29	0.034888		24.6.173.220	75.75.75.75	DNS		Standard query 0x5183 A javadl-esd-secure.oracle.com
30	0.000655		24.6.173.220	75.75.75.75	DNS		Standard query response 0x5183 A javadl-esd-secure.oracle.com CNAME javadl-esd-secure.oracle.com.edgekey.net CN...
31	0.034472		75.75.75.75	24.6.173.220	DNS		Standard query 0x5ae1 AAAA javadl-esd-secure.oracle.com
127	0.192225		24.6.173.220	75.75.75.75	DNS		Standard query response 0x4372 A api.memeeo.info
128	0.032328		75.75.75.75	24.6.173.220	DNS		Standard query response 0x4372 A api.memeeo.info A 216.115.74.235
129	0.000694		24.6.173.220	75.75.75.75	DNS		Standard query 0x827b AAAA api.memeeo.info
130	0.036713		75.75.75.75	24.6.173.220	DNS		Standard query response 0x827b AAAA api.memeeo.info SOA a4.nstld.com
420	0.989049		24.6.173.220	75.75.75.75	DNS		Standard query 0x81b6 A api.memeeo.com
421	0.013152		75.75.75.75	24.6.173.220	DNS		Standard query response 0x81b6 A api.memeeo.com A 216.115.74.202
422	0.001684		24.6.173.220	75.75.75.75	DNS		Standard query 0xe061 AAAA api.memeeo.com
423	0.014786		75.75.75.75	24.6.173.220	DNS		Standard query response 0xe061 AAAA api.memeeo.com SOA a4.nstld.com
450	0.011033		24.6.173.220	75.75.75.75	DNS		Standard query 0xaad8 A memeeo.info
451	0.012339		75.75.75.75	24.6.173.220	DNS		Standard query response 0xaad8 A memeeo.info A 216.115.74.234
452	0.001098		24.6.173.220	75.75.75.75	DNS		Standard query 0xb69b AAAA memeeo.info
453	0.015771		75.75.75.75	24.6.173.220	DNS		Standard query response 0xb69b AAAA memeeo.info SOA a4.nstld.com

Domain Name System (response)

Paquetes: 514 · Mostrado: 16 (3.1%)

Paso 2: Aplicamos el filtro **ip.addr==216.115.74.0/24** y veremos que hay en total 51 paquetes.}

The screenshot shows the Wireshark interface with the filter 'ip.addr==216.115.74.0/24' applied. The packet list displays 51 packets, including TCP, HTTP, and DNS traffic. The packet details pane shows the structure of a TCP Reset (RST) packet from 216.115.74.235 to 24.6.173.220.

No.	Time	TCP Delta	Source	Destination	Protocol	Host	Info
118	2.312784		0.000000000	24.6.173.220	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	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	TCP		1145 → 80 [ACK] Seq=1 Ack=1 Win=66300 Len=0
121	0.000576		0.000576000	24.6.173.220	HTTP	www.mem...	GET /php/updateMetric.php?product_key=HABPEME000-6E2P-2AC3-3KP3-JF8E-009F&locale=en-US&num_jobs=1&eselle...
122	0.037863		0.037863000	216.115.74.235	HTTP		HTTP/1.1 200 OK (text/html)
123	0.003172		0.003172000	24.6.173.220	TCP		1145 → 80 [RST, ACK] Seq=227 Ack=581 Win=0 Len=0
131	0.000299		0.000000000	24.6.173.220	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	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	TCP		1146 → 80 [ACK] Seq=1 Ack=1 Win=66300 Len=0
134	0.000461		0.000461000	24.6.173.220	HTTP	api.mem...	GET /clientSettings.php?buildtype=sgm&esellerid=STR3685286259&product=autobackuppro&productleveltype=PRE-
135	0.036160		0.036160000	216.115.74.235	HTTP		HTTP/1.1 200 OK (text/html)
136	0.000918		0.000918000	216.115.74.235	TCP		80 → 1146 [FIN, ACK] Seq=247 Ack=163 Win=4062 Len=0
137	0.000036		0.000036000	24.6.173.220	TCP		1146 → 80 [ACK] Seq=163 Ack=248 Win=66052 Len=0
138	0.017141		0.017141000	24.6.173.220	TCP		1146 → 80 [FIN, ACK] Seq=163 Ack=248 Win=66052 Len=0
139	0.034003		0.034003000	216.115.74.235	TCP		80 → 1146 [ACK] Seq=248 Ack=164 Win=4062 Len=0
424	0.001136		0.000000000	24.6.173.220	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	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	TCP		1187 → 80 [ACK] Seq=1 Ack=1 Win=66300 Len=0
427	0.000811		0.000811000	24.6.173.220	HTTP	api.mem...	GET /1.0/util/get_conf HTTP/1.1
428	0.131971		0.131971000	216.115.74.202	TCP		80 → 1187 [ACK] Seq=1 Ack=168 Win=4067 Len=0
429	0.253302		0.253302000	216.115.74.202	HTTP		HTTP/1.1 200 OK (application/x-javascript)
430	0.000004		0.000004000	216.115.74.202	HTTP		Continuation
431	0.000757		0.000757000	24.6.173.220	TCP		1187 → 80 [ACK] Seq=168 Ack=1461 Win=66300 Len=0
432	0.000863		0.000863000	216.115.74.202	HTTP		Continuation
433	0.000004		0.000004000	216.115.74.202	TCP		80 → 1187 [FIN, ACK] Seq=2300 Ack=168 Win=4067 Len=0
434	0.000443		0.000443000	24.6.173.220	TCP		1187 → 80 [ACK] Seq=168 Ack=2301 Win=65460 Len=0
435	0.000090		0.000090000	24.6.173.220	TCP		1187 → 80 [FIN, ACK] Seq=168 Ack=2301 Win=65460 Len=0
436	0.031720		0.031720000	216.115.74.202	TCP		80 → 1187 [ACK] Seq=2301 Ack=169 Win=4067 Len=0
437	0.197193		0.000000000	24.6.173.220	TCP		1188 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1

Transmission Control Protocol, Src Port: 1145, Dst Port: 80, Seq: 0, Len: 0

Paquetes: 514 · Mostrado: 51 (9.9%)