

**Instituto Tecnológico de Cancún**

**Ingeniería en Sistemas Computacionales**

**Fundamentos de Telecomunicaciones**

**Lab18 - Filter on DNS Name Errors or  
HTTP 404 Responses**

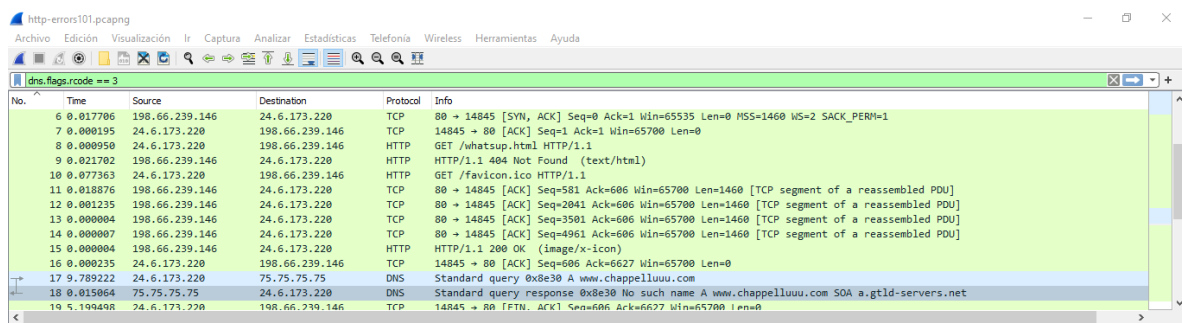
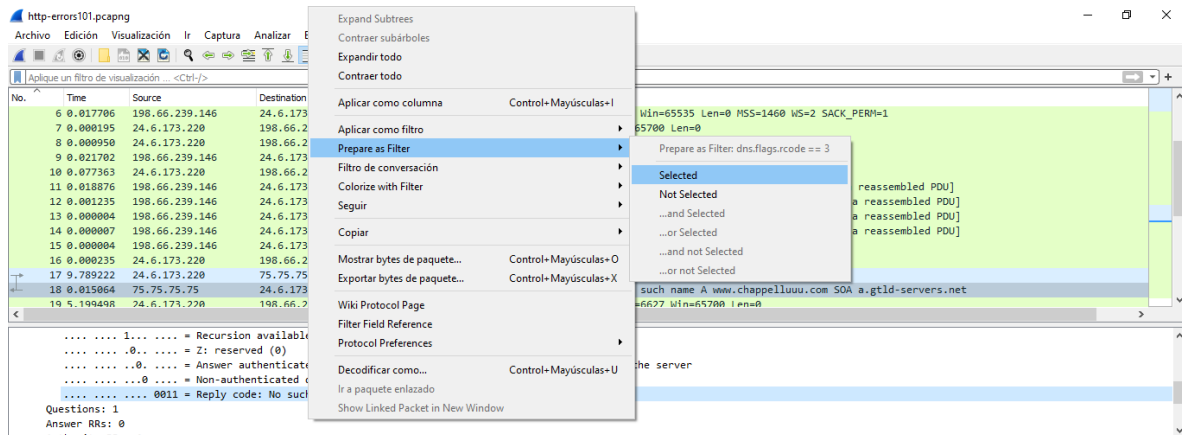
**Docente: Ing. Ismael Jiménez Sánchez**

**Alumno: Uc Uc César Enrique**

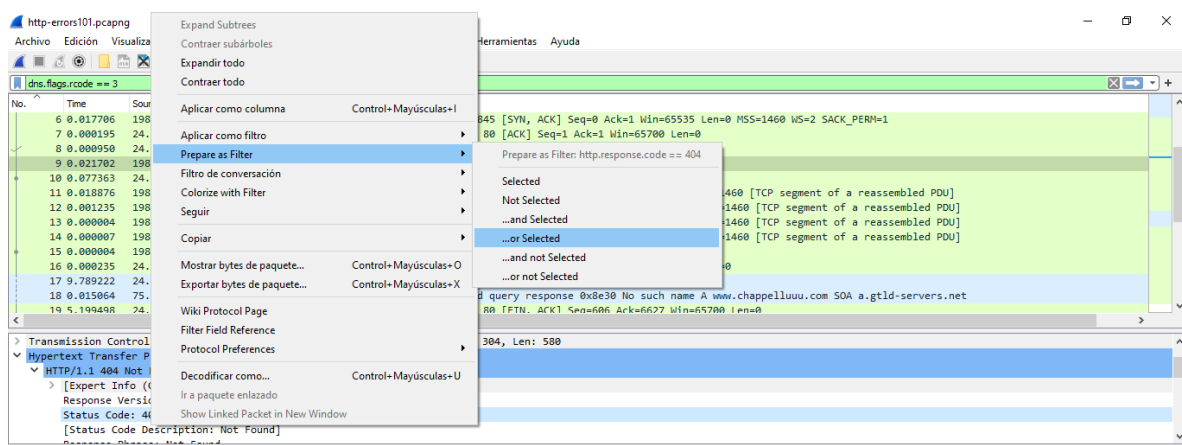
## Lab18 - Filter on DNS Name Errors or HTTP 404 Responses

### 1 Abrimos el archivo http-errors101.pcapng

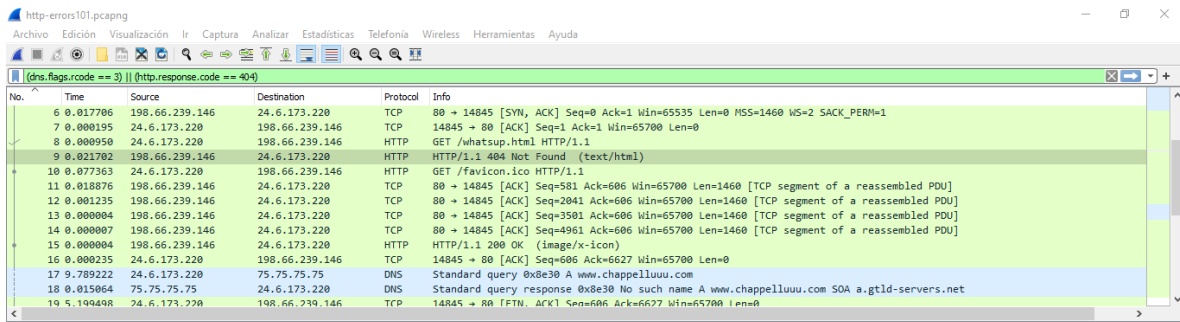
### 2 En el paquete 18 en el panel de detalles, en la parte de Reply code: no such name(3) le damos click derecho Prepare a Filter>Select



### 3 Seleccionamos el paquete 9, expandimos la sección HTTP, click derecho en Status code: 404 > Prepare a Filter > ... or selected



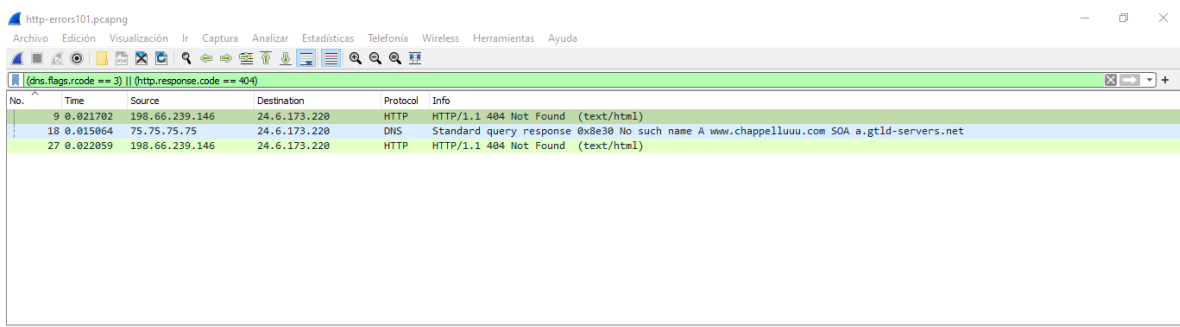
El área de filtro deberá aparecer (dns.flags.rcode == 3) || (http.response.code == 404)



Wireshark packet capture showing various network traffic. The filter is (dns.flags.rcode == 3) || (http.response.code == 404). The table below shows the captured packets:

No.	Time	Source	Destination	Protocol	Info
6	0.017706	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	24.6.173.220	198.66.239.146	TCP	14845 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
8	0.000950	24.6.173.220	198.66.239.146	HTTP	GET /whatsup.html HTTP/1.1
9	0.021702	198.66.239.146	24.6.173.220	HTTP	HTTP/1.1 404 Not Found (text/html)
10	0.077363	24.6.173.220	198.66.239.146	HTTP	GET /favicon.ico HTTP/1.1
11	0.018876	198.66.239.146	24.6.173.220	TCP	80 → 14845 [ACK] Seq=581 Ack=606 Win=65700 Len=1460 [TCP segment of a reassembled PDU]
12	0.001235	198.66.239.146	24.6.173.220	TCP	80 → 14845 [ACK] Seq=2041 Ack=606 Win=65700 Len=1460 [TCP segment of a reassembled PDU]
13	0.000004	198.66.239.146	24.6.173.220	TCP	80 → 14845 [ACK] Seq=3501 Ack=606 Win=65700 Len=1460 [TCP segment of a reassembled PDU]
14	0.000007	198.66.239.146	24.6.173.220	TCP	80 → 14845 [ACK] Seq=4961 Ack=606 Win=65700 Len=1460 [TCP segment of a reassembled PDU]
15	0.000004	198.66.239.146	24.6.173.220	HTTP	HTTP/1.1 200 OK (image/x-icon)
16	0.000235	24.6.173.220	198.66.239.146	TCP	14845 → 80 [ACK] Seq=606 Ack=6627 Win=65700 Len=0
17	0.789222	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-servers.net
19	0.194498	24.6.173.220	198.66.239.146	TCP	14845 → 80 [FIN, ACK] Seq=606 Ack=6627 Win=65700 Len=0

#### 4. Lo aplicamos y solo aparecerán 3 paquetes



Wireshark packet capture showing only the filtered packets. The filter is (dns.flags.rcode == 3) || (http.response.code == 404). The table below shows the captured packets:

No.	Time	Source	Destination	Protocol	Info
9	0.021702	198.66.239.146	24.6.173.220	HTTP	HTTP/1.1 404 Not Found (text/html)
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-servers.net
27	0.022059	198.66.239.146	24.6.173.220	HTTP	HTTP/1.1 404 Not Found (text/html)