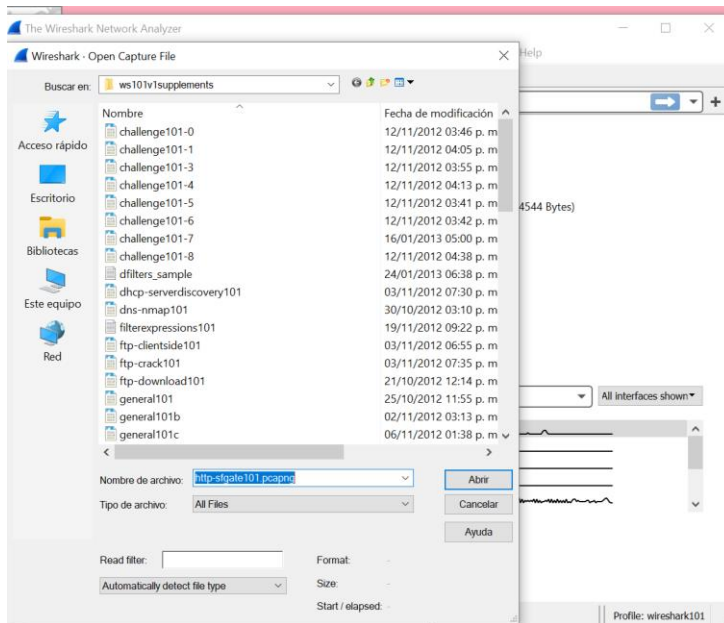
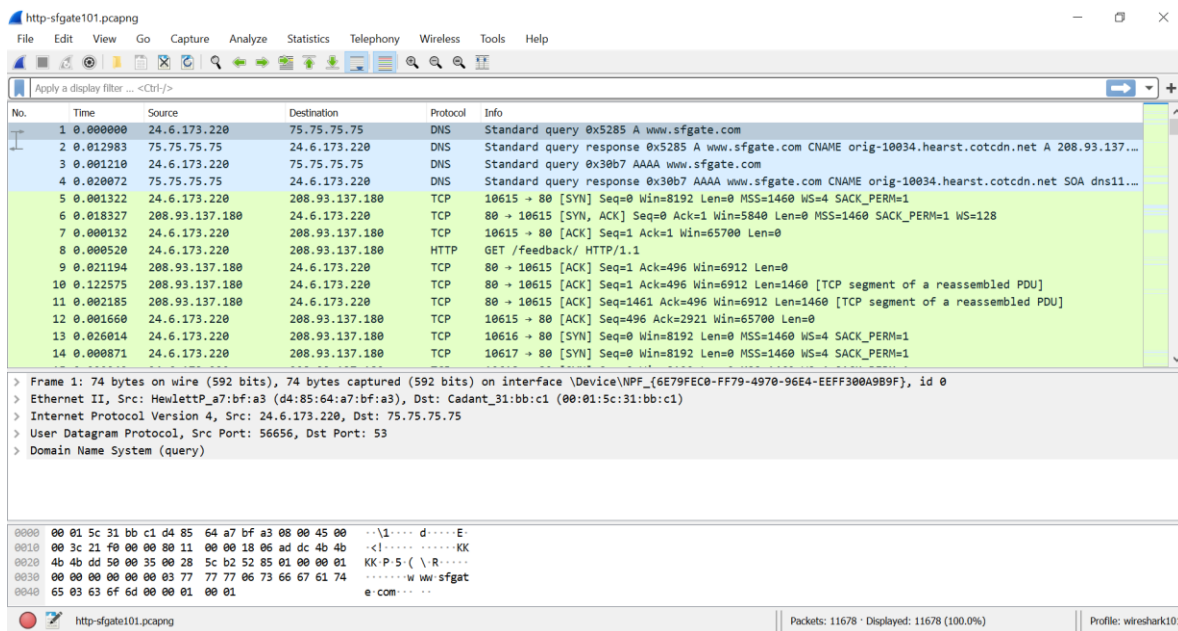


Lab 14

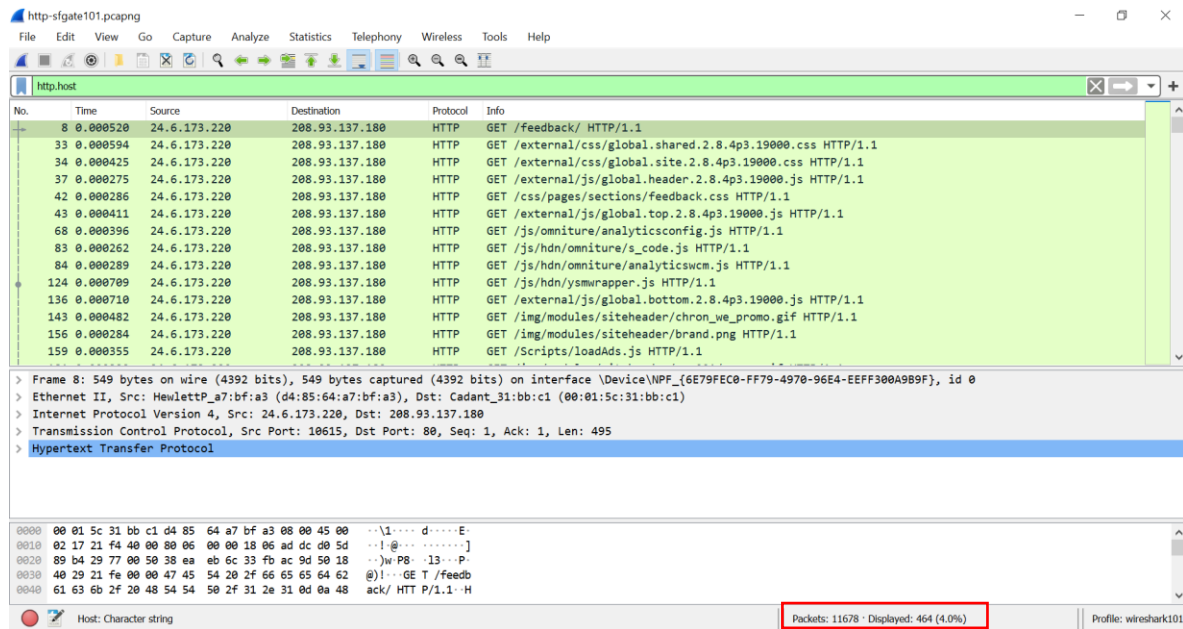
Abriremos el archivo llamado ***http-sfgate101.pcapng***



Observamos los tráficos DNS Y HTTP

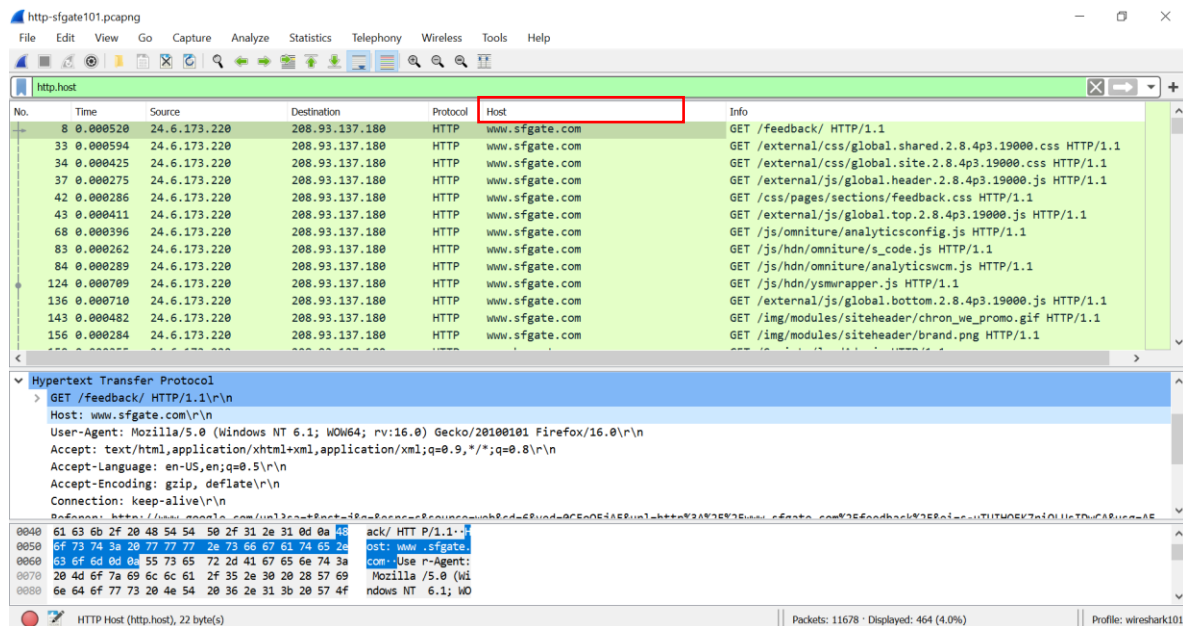


Aplicaremos un filtro escribiendo **http.host** ,veremos que se muestran 464 paquetes



The screenshot shows the Wireshark interface with a filter applied to the packet list pane: `http.host`. The packet list displays 159 packets, all of which are HTTP GET requests from 24.6.173.220 to 208.93.137.180. The packet details pane shows the structure of a selected packet, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII. The status bar at the bottom indicates that 11678 packets were captured and 464 (4.0%) are displayed.

Aplicaremos “Host” como columna



The screenshot shows the Wireshark interface with the same filter applied. A new column, `Host`, has been added to the packet list pane. The `Host` column contains the value `www.sfgate.com` for all packets. The packet details pane shows the structure of a selected packet, including the `Host` header field. The status bar at the bottom indicates that 11678 packets were captured and 464 (4.0%) are displayed.

Al aplicar el filtro veremos que ahora nos muestra 12 paquetes

http-sfgate101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.method=="POST"

No.	Time	Source	Destination	Protocol	Host	Info
859	0.000644	24.6.173.220	199.7.57.72	OCSP	ocsp.verisign.com	Request
864	0.000235	24.6.173.220	199.7.57.72	OCSP	ocsp.verisign.com	Request
865	0.000430	24.6.173.220	199.7.57.72	OCSP	ocsp.verisign.com	Request
897	0.000381	24.6.173.220	199.7.57.72	OCSP	ocsp.verisign.com	Request
898	0.000324	24.6.173.220	199.7.57.72	OCSP	ocsp.verisign.com	Request
2043	0.001817	24.6.173.220	67.192.92.227	HTTP	ad.auditudo.com	POST /adserver?u=97df6f8f08d8730261d4b44204353b4c&u=69832e95d26ae6...
3418	0.001861	24.6.173.220	208.81.191.110	HTTP	www.meebo.com	POST /cmd/cx HTTP/1.1 (application/x-www-form-urlencoded)
3419	0.000360	24.6.173.220	208.81.191.110	HTTP	www.meebo.com	POST /cmd/tc HTTP/1.1 (application/x-www-form-urlencoded)
3476	0.015034	24.6.173.220	208.81.191.110	HTTP	www.meebo.com	POST /cmd/getrotate HTTP/1.1 (application/x-www-form-urlencoded)
100...	0.000862	24.6.173.220	208.93.137.180	HTTP	extras.sfgate.com	POST /sfgate/modules/formHandlers/sfgSupportMailHandler.php HTTP/1...
104...	0.016505	24.6.173.220	208.81.191.110	HTTP	www.meebo.com	POST /cmd/cx HTTP/1.1 (application/x-www-form-urlencoded)
105...	0.000853	24.6.173.220	67.192.92.227	HTTP	ad.auditudo.com	POST /adserver?u=97df6f8f08d8730261d4b44204353b4c&u=69832e95d26ae6...

> Frame 10578: 841 bytes on wire (6728 bits), 841 bytes captured (6728 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: 67.192.92.227

> Transmission Control Protocol, Src Port: 10957, Dst Port: 80, Seq: 1, Ack: 1, Len: 787

> Hypertext Transfer Protocol

> POST /adserver?u=97df6f8f08d8730261d4b44204353b4c&u=69832e95d26ae65e69ac72002a0be78c&z=5091281=20121102085149&of=1.4&tm=15&g=1000002 HTTP/1.1\r\n

Host: ad.auditudo.com\r\n

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0\r\n

0000 31 2e 31 0d 0a 40 6f 73 74 3a 20 61 64 2e 61 25 1.1..nos t: ad.a...

0000 54 69 74 75 64 65 2a 43 6f 6d 0d 0a 55 73 65 72 auditudo.com>User

0000 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla/

0000 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 5.0 (win dows NT

0100 36 2e 31 3b 20 57 4f 57 36 34 3b 20 72 76 3a 31 6.1; NOM 64; rv:1

HTTP Host (http.host), 23 byte(s)

Packets: 11678 · Displayed: 12 (0.1%)

Profile: wireshark101

En el paquete numero 10022 veremos el mensaje del remitente

3419	0.000360	24.6.173.220	208.81.191.110	HTTP	www.meebo.com
3476	0.015034	24.6.173.220	208.81.191.110	HTTP	www.meebo.com
10022	0.000862	24.6.173.220	208.93.137.180	HTTP	extras.sfgate.com
10406	0.016505	24.6.173.220	208.81.191.110	HTTP	www.meebo.com