

UNIVERSIDAD DE LOS ANDES
DEPARTAMENTO DE INGENIERIA DE
SISTEMAS Y COMPUTACIÓN



LABORATORIO: ANÁLISIS DE PROTOCOLOS DE LA
CAPA DE APLICACIÓN

ISIS 3204 – INFRAESTRUCTURA DE
COMUNICACIONES

Nathalia Quiroga

Grupo 10

Andres charry 202214507

Miguel florez 202317266

Manuel prieto 202226947

Contenido

8. PRUEBAS DE CONECTIVIDAD USANDO WIRESHARK Y CMD.....	3
8.1 Prueba ping.....	3
8.2 Análisis de tráfico del Servicio DNS	4
WEB_IP	4
WEB.....	5
8.3 Análisis de tráfico del Servicio HTTP	7
8.4 Análisis de tráfico del Servicio FTP	7
8.5 Análisis de tráfico del Servicio Web	9
8.6 Análisis de tráfico del Servicio Web	13
8.7 Análisis TCP.....	13
8.8 Análisis del protocolo VoIP.....	16
8.9 Análisis del protocolo RTMP.....	25
Topología de red:	27

8. PRUEBAS DE CONECTIVIDAD USANDO WIRESHARK Y CMD.

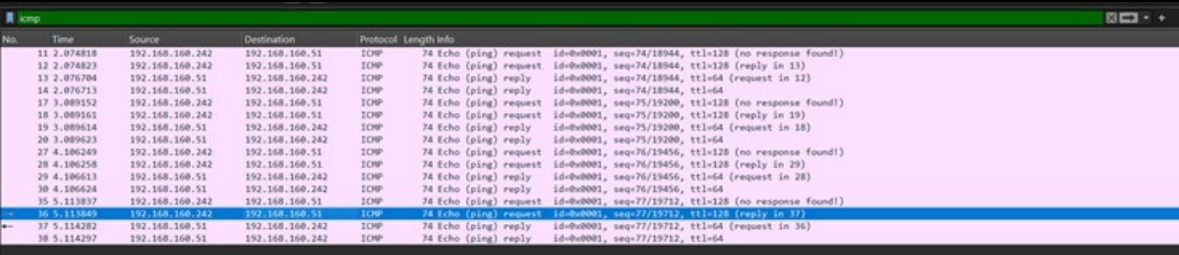
8.1 Prueba ping

DNS	
Dirección IP de origen request	192.168.160.242
Dirección IP de destino request	192.168.160.53
Dirección IP de origen reply	192.168.160.53
Dirección IP de destino reply	192.168.160.242
Dirección MAC del equipo Cliente	b8:1e:a4:bb:2e:8f
Dirección MAC del equipo Servidor	00:0c:29:37:de:17

No.	Time	Source	Destination	Protocol	Length	Info
29	1.935517	192.168.160.242	192.168.160.53	ICMP	74	Echo (ping) request id=0x0001, seq=70/17920, ttl=128 (no response found!)
30	1.935540	192.168.160.242	192.168.160.53	ICMP	74	Echo (ping) request id=0x0001, seq=70/17920, ttl=128 (reply in 31)
31	1.936929	192.168.160.53	192.168.160.242	ICMP	74	Echo (ping) reply id=0x0001, seq=70/17920, ttl=64 (request in 30)
32	1.936934	192.168.160.53	192.168.160.242	ICMP	74	Echo (ping) reply id=0x0001, seq=70/17920, ttl=64
47	2.939674	192.168.160.242	192.168.160.53	ICMP	74	Echo (ping) request id=0x0001, seq=71/18176, ttl=128 (no response found!)
48	2.939686	192.168.160.242	192.168.160.53	ICMP	74	Echo (ping) request id=0x0001, seq=71/18176, ttl=128 (reply in 49)
49	2.940167	192.168.160.53	192.168.160.242	ICMP	74	Echo (ping) reply id=0x0001, seq=71/18176, ttl=64 (request in 48)
50	2.940176	192.168.160.53	192.168.160.242	ICMP	74	Echo (ping) reply id=0x0001, seq=71/18176, ttl=64
59	3.952409	192.168.160.242	192.168.160.53	ICMP	74	Echo (ping) request id=0x0001, seq=72/18432, ttl=128 (no response found!)
60	3.952423	192.168.160.242	192.168.160.53	ICMP	74	Echo (ping) request id=0x0001, seq=72/18432, ttl=128 (reply in 61)
61	3.952838	192.168.160.53	192.168.160.242	ICMP	74	Echo (ping) reply id=0x0001, seq=72/18432, ttl=64 (request in 60)
62	3.952845	192.168.160.53	192.168.160.242	ICMP	74	Echo (ping) reply id=0x0001, seq=72/18432, ttl=64
73	4.965128	192.168.160.242	192.168.160.53	ICMP	74	Echo (ping) request id=0x0001, seq=73/18688, ttl=128 (no response found!)
74	4.965137	192.168.160.242	192.168.160.53	ICMP	74	Echo (ping) request id=0x0001, seq=73/18688, ttl=128 (reply in 75)
75	4.965591	192.168.160.53	192.168.160.242	ICMP	74	Echo (ping) reply id=0x0001, seq=73/18688, ttl=64 (request in 74)
76	4.965601	192.168.160.53	192.168.160.242	ICMP	74	Echo (ping) reply id=0x0001, seq=73/18688, ttl=64

En la imagen se observa la captura en Wireshark de los paquetes ICMP generados durante la prueba de conectividad (ping) entre el cliente y el servidor DNS. Se distinguen claramente los mensajes Echo request enviados desde la IP 192.168.160.242 (cliente) hacia la IP 192.168.160.53 (servidor), así como las respuestas Echo reply en sentido inverso. Esto evidencia la correcta conectividad a nivel de red entre ambos dispositivos. Además, la prueba permite identificar los parámetros solicitados en el informe, tales como direcciones IP y MAC de origen y destino.

FTP	
Dirección IP de origen request	192.168.160.242
Dirección IP de destino request	192.168.160.51
Dirección IP de origen reply	192.168.160.51
Dirección IP de destino reply	192.168.160.242
Dirección MAC del equipo Cliente	b8:1e:a4:bb:2e:8f
Dirección MAC del equipo Servidor	00:0c:29:71:ce:b2

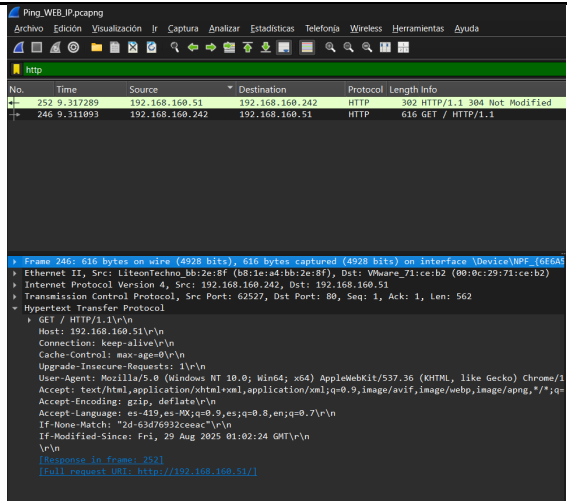


En esta captura se muestra el tráfico ICMP entre el cliente (192.168.160.242) y el servidor FTP (192.168.160.51). Los paquetes de *request* y *reply* evidencian que existe comunicación directa, verificando que el servidor FTP está disponible y accesible dentro de la red configurada.

8.2 Análisis de tráfico del Servicio DNS

WEB_IP

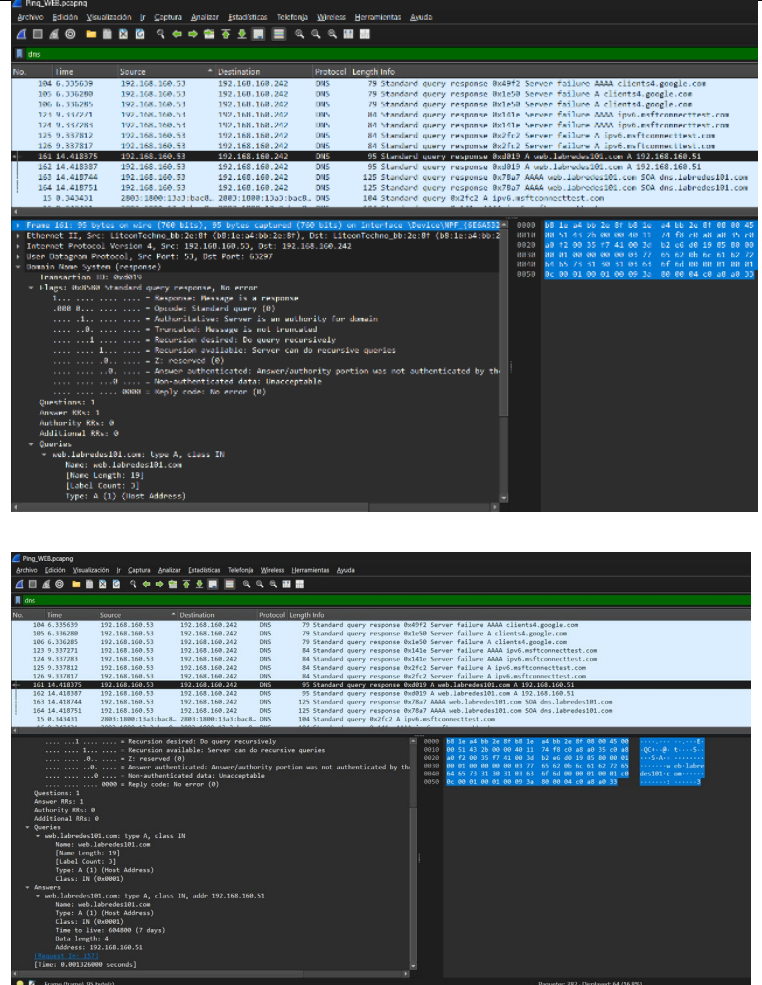
WEB	
Protocolo	DNS – UDP - HTTP
Información de la capa de aplicación	

	
Puertos	53, 53250, 63297
Dirección IP de origen request	192.168.160.242
Dirección IP de destino request	192.168.160.51
Dirección IP de origen reply	192.168.160.51
Dirección IP de destino reply	192.168.160.242
Dirección MAC del equipo Cliente	b8:1e:a4:bb:2e:8f
Dirección MAC del equipo Servidor	00:0c:29:71:ce:b2

La captura muestra las consultas DNS realizadas por el cliente (192.168.160.242) al servidor (192.168.160.51) para resolver la dirección del servicio web. Se observan paquetes de petición (request) y respuesta (reply) sobre UDP, junto con el uso de puertos característicos como el 53. Esta evidencia confirma que el servidor DNS responde correctamente, permitiendo que el acceso al servicio web se realice tanto por IP como por nombre de dominio.

WEB

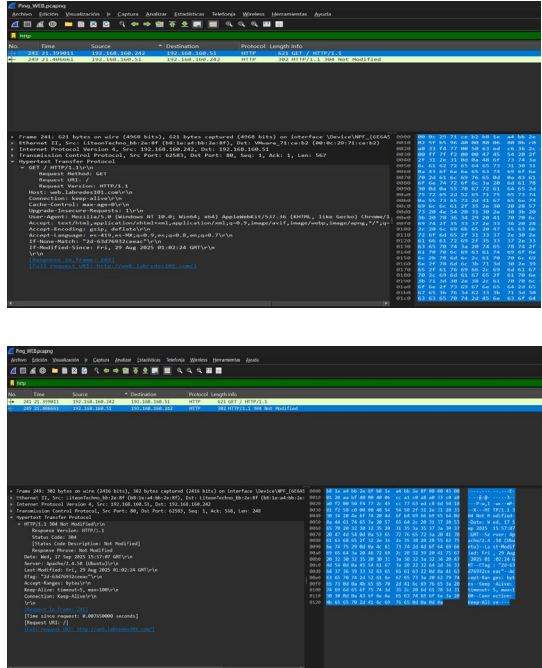
DNS	
Protocolo	DNS - UDP
Información de la capa de aplicación	

	
Puertos	53, 53250, 63297
Dirección IP de origen request	192.168.160.242
Dirección IP de destino request	192.168.160.51
Dirección IP de origen reply	192.168.160.51
Dirección IP de destino reply	192.168.160.242
Dirección MAC del equipo Cliente	b8:1e:a4:bb:2e:8f
Dirección MAC del equipo Servidor	00:0c:29:71:ce:b2

La captura evidencia los paquetes intercambiados entre el cliente (192.168.160.242) y el servidor (192.168.160.51) durante la resolución del nombre del servicio web y la posterior comunicación. Se observan consultas enviadas desde el cliente y sus respectivas respuestas por parte del servidor, utilizando el protocolo UDP con puerto destino 53 y puertos efímeros de origen (53250, 63297).

En el detalle del paquete se aprecia la traducción del dominio configurado a la dirección IP correspondiente, junto con los encabezados propios de la capa de aplicación.

8.3 Análisis de tráfico del Servicio HTTP

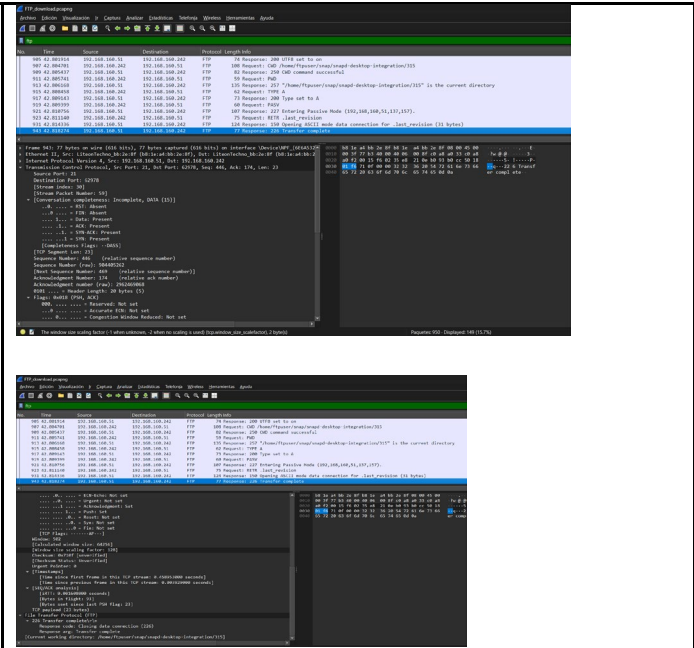
HTTP	
Protocolo	HTTP - TCP
Información de la capa de aplicación	 <p>The image displays two Wireshark packet captures. The top capture shows an HTTP GET request from 192.168.160.242 to 192.168.160.51 on port 80. The bottom capture shows the corresponding 304 Not Modified response from the server. Both captures include detailed packet analysis and hex/ASCII data views.</p>
Puertos	80, 62583

Las captura muestran la interacción entre el cliente (192.168.160.242) y el servidor (192.168.160.51) mediante el protocolo HTTP sobre TCP. Se observa una petición HTTP GET generada por el cliente hacia el recurso alojado en el servidor, y la correspondiente respuesta del servidor con el código 304 Not Modified, que indica que el contenido solicitado no ha cambiado desde la última consulta.

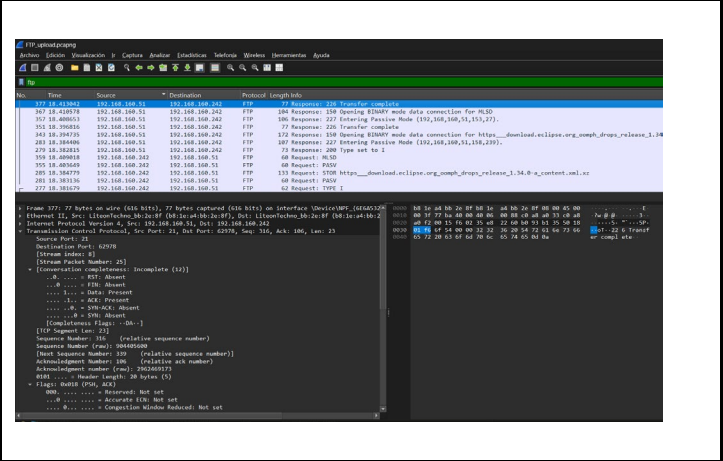
En la capa de aplicación se aprecian los encabezados HTTP intercambiados, incluyendo detalles como el agente de usuario, los tipos de contenido admitidos y la información de control de caché.

8.4 Análisis de tráfico del Servicio FTP

FTP Download	
Protocolo	FTP – TCP - DNS
Información de la capa de aplicación	

	
Puertos	21, 62978

Las captura evidencia la comunicación establecida entre el cliente (192.168.160.242) y el servidor (192.168.160.51) utilizando el protocolo FTP sobre TCP. Se observan los comandos enviados por el cliente (PWD, TYPE I, PASV, RETR) y las respuestas del servidor que habilitan la transferencia de datos. En la capa de aplicación se aprecia el intercambio propio del protocolo FTP, donde el puerto 21 se emplea para el canal de control, mientras que el cliente utiliza un puerto efímero (62978) para la conexión.

FTP Upload	
Protocolo	FTP – TCP - DNS
Información de la capa de aplicación	

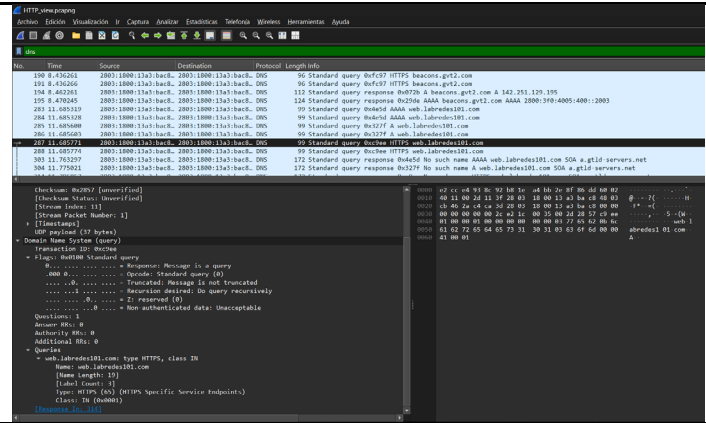
Puertos	21, 62978

La captura muestra el proceso de transferencia de archivos desde el cliente (192.168.160.242) hacia el servidor (192.168.160.51) utilizando el protocolo FTP sobre TCP. En la capa de aplicación se distinguen comandos como TYPE I, PASV y STOR, a través de los cuales el cliente solicita la subida de un archivo al directorio asignado. El canal de control se establece sobre el puerto estándar 21, mientras que el puerto efímero 62978 del cliente es usado para la conexión.

8.5 Análisis de tráfico del Servicio Web

HTTP

Protocolo	UDP - DNS
Información de la capa de aplicación	

	
Puertos	53, 57884

Las captura evidencia el intercambio de paquetes entre el cliente (192.168.160.242) y el servidor (192.168.160.51) durante el proceso de resolución de nombres previo al acceso HTTP. Se observan solicitudes DNS query enviadas desde el cliente hacia el servidor para obtener la dirección IP correspondiente al dominio web.labredes101.com, y las respectivas DNS response con la resolución exitosa. El tráfico utiliza el protocolo UDP, con puerto destino 53 en el servidor y un puerto efímero de origen (57884) en el cliente.

616 GET HTTP	
Protocolo	HTTP - TCP
Información de la capa de aplicación	

	<div><div>TP_view.pcapng</div><div><div>File</div><div>Edición</div><div>Visualización</div><div>Ir</div><div>Captura</div><div>Analizar</div><div>Estadísticas</div><div>Telefonía</div><div>Wireless</div><div>Herramientas</div><div>Ayuda</div></div><div><div></div><div><div>Filter</div><div>Packet List</div><div>Packet Details</div><div>Packet Bytes</div></div><table><thead><tr><th>No.</th><th>Time</th><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr></thead><tbody><tr><td>137</td><td>7.978884</td><td>192.168.160.242</td><td>192.168.160.51</td><td>HTTP</td><td>616</td><td>GET / HTTP/1.1</td></tr><tr><td>145</td><td>7.986319</td><td>192.168.160.51</td><td>192.168.160.242</td><td>HTTP</td><td>302</td><td>HTTP/1.1 304 Not Modified</td></tr><tr><td>232</td><td>9.193014</td><td>192.168.160.242</td><td>192.168.160.51</td><td>HTTP</td><td>616</td><td>GET / HTTP/1.1</td></tr><tr><td>234</td><td>9.197125</td><td>192.168.160.51</td><td>192.168.160.242</td><td>HTTP</td><td>301</td><td>HTTP/1.1 304 Not Modified</td></tr><tr><td>337</td><td>11.790887</td><td>192.168.160.242</td><td>192.168.160.51</td><td>HTTP</td><td>621</td><td>GET / HTTP/1.1</td></tr><tr><td>345</td><td>11.794083</td><td>192.168.160.51</td><td>192.168.160.242</td><td>HTTP</td><td>302</td><td>HTTP/1.1 304 Not Modified</td></tr></tbody></table><div><p>Packet 137: 616 bytes on wire (4928 bits), 616 bytes captured (4928 bits) on interface \Device\NPF{...} Ethernet II, Src: LiteonTechno_bb:2e:8f (b8:1e:a4:bb:2e:8f), Dst: VMware_71:ce:b2 (00:0c:29:71:ce:b2), Internet Protocol Version 4, Src: 192.168.160.242, Dst: 192.168.160.51</p><p>Transmission Control Protocol, Src Port: 63175, Dst Port: 80, Seq: 1, Ack: 1, Len: 562</p><p>Source Port: 63175</p><p>Destination Port: 80</p><p>[Stream index: 5]</p><p>[Stream Packet Number: 7]</p><p>[Conversation completeness: Complete, WITH_DATA (31)]</p><p>...0. = RST: Absent</p><p>...1. = FIN: Present</p><p>.... 1... = Data: Present</p><p>.... .1.. = ACK: Present</p><p>.... ..1. = SYN-ACK: Present</p><p>.... ...1 = SYN: Present</p><p>[Completeness Flags: -FDASS]</p><p>[TCP Segment Len: 562]</p><p>Sequence Number: 1 (relative sequence number)</p><p>Sequence Number (raw): 1863387283</p><p>[Next Sequence Number: 563 (relative sequence number)]</p><p>Acknowledgment Number: 1 (relative ack number)</p><p>Acknowledgment number (raw): 1450367222</p><p>0101 = Header Length: 20 bytes (5)</p><p>Flags: 0x018 (PSH, ACK)</p><p>000. = Reserved: Not set</p><p>...0 = Accurate ECN: Not set</p><p>.... 0... = Congestion Window Reduced: Not set</p></div></div></div>	No.	Time	Source	Destination	Protocol	Length	Info	137	7.978884	192.168.160.242	192.168.160.51	HTTP	616	GET / HTTP/1.1	145	7.986319	192.168.160.51	192.168.160.242	HTTP	302	HTTP/1.1 304 Not Modified	232	9.193014	192.168.160.242	192.168.160.51	HTTP	616	GET / HTTP/1.1	234	9.197125	192.168.160.51	192.168.160.242	HTTP	301	HTTP/1.1 304 Not Modified	337	11.790887	192.168.160.242	192.168.160.51	HTTP	621	GET / HTTP/1.1	345	11.794083	192.168.160.51	192.168.160.242	HTTP	302	HTTP/1.1 304 Not Modified
No.	Time	Source	Destination	Protocol	Length	Info																																												
137	7.978884	192.168.160.242	192.168.160.51	HTTP	616	GET / HTTP/1.1																																												
145	7.986319	192.168.160.51	192.168.160.242	HTTP	302	HTTP/1.1 304 Not Modified																																												
232	9.193014	192.168.160.242	192.168.160.51	HTTP	616	GET / HTTP/1.1																																												
234	9.197125	192.168.160.51	192.168.160.242	HTTP	301	HTTP/1.1 304 Not Modified																																												
337	11.790887	192.168.160.242	192.168.160.51	HTTP	621	GET / HTTP/1.1																																												
345	11.794083	192.168.160.51	192.168.160.242	HTTP	302	HTTP/1.1 304 Not Modified																																												
Puertos	80, 63175																																																	

La captura evidencia la comunicación entre el cliente (192.168.160.242) y el servidor web (192.168.160.51) mediante el protocolo HTTP sobre TCP. Se observan varias solicitudes HTTP GET realizadas por el cliente, y las correspondientes respuestas del servidor con el código 304 Not Modified, indicando que los recursos solicitados no han cambiado desde la última consulta. En la capa de aplicación se reflejan los encabezados HTTP propios de la interacción cliente-servidor, mientras que en la capa de transporte se aprecia el uso del puerto estándar 80 en el servidor y el puerto efímero 63175 en el cliente.

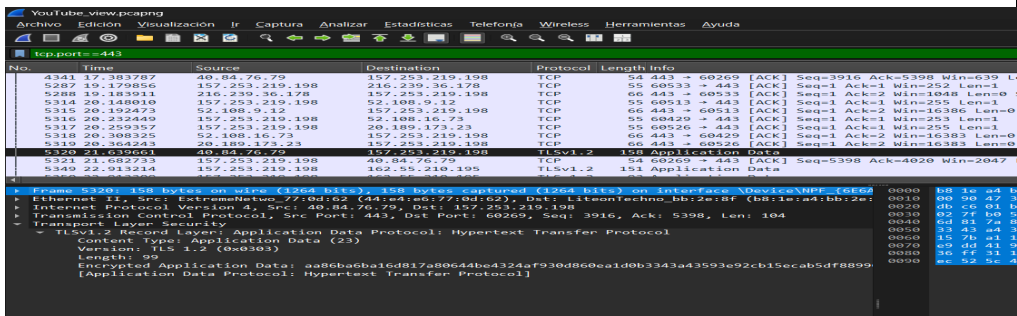
302 HTTP	
Protocolo	HTTP - TCP
Información de la capa de aplicación	 <p>The image displays two screenshots of a Wireshark packet capture. The top screenshot shows the packet list and details for an HTTP 302 Found response. The packet list shows a GET request from 192.168.160.242 to 192.168.160.51, followed by a 302 Found response from 192.168.160.51 to 192.168.160.242. The packet details show the response status code 302 and the 'Location' header pointing to http://192.168.160.51/.</p> <p>The bottom screenshot shows the packet list and details for the same HTTP 302 Found response. The packet list shows a GET request from 192.168.160.242 to 192.168.160.51, followed by a 302 Found response from 192.168.160.51 to 192.168.160.242. The packet details show the response status code 302 and the 'Location' header pointing to http://192.168.160.51/.</p>
Puertos	80, 63175

En la captura se aprecia la respuesta HTTP/1.1 302 Found, enviada desde el servidor (192.168.160.51) hacia el cliente (192.168.160.242). Esta respuesta indica una redirección temporal, lo que significa que el recurso solicitado en la petición previa (HTTP GET) se encuentra disponible en una ubicación diferente.

El tráfico viaja sobre TCP, utilizando el puerto estándar 80 en el servidor y el puerto efímero 63175 en el cliente.

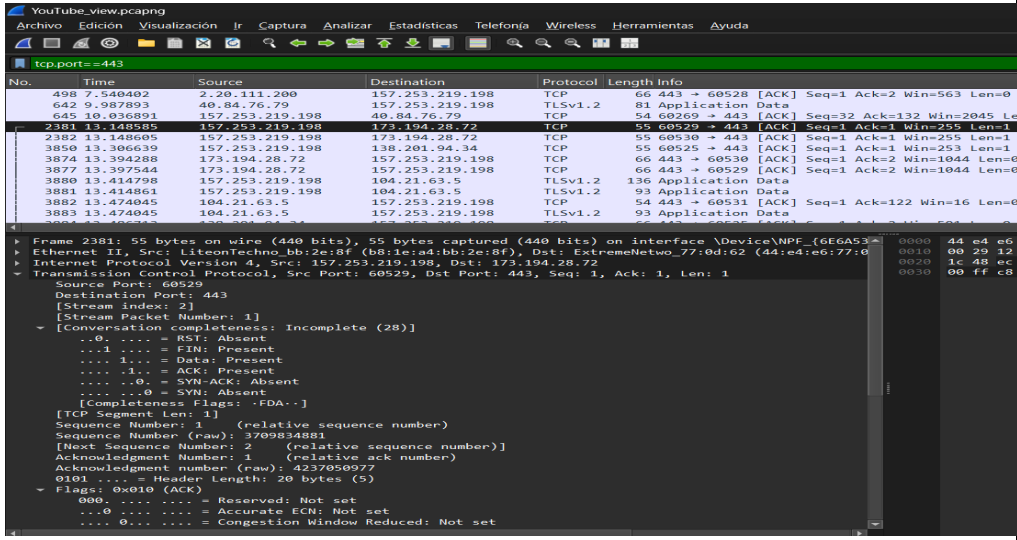
8.6 Análisis de tráfico del Servicio Web

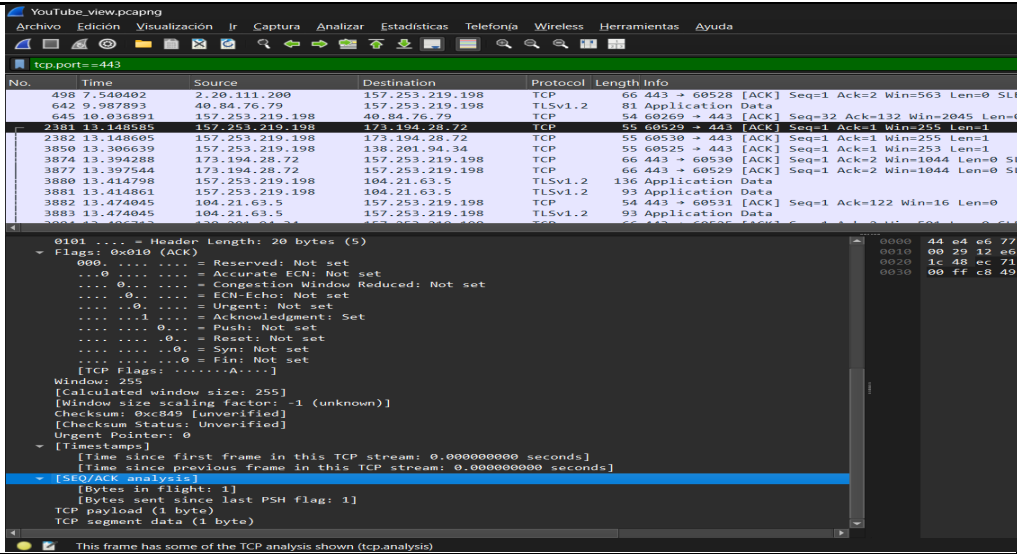
Youtube

TLS	
Protocolo	TLS - TCP
Información de la capa de aplicación	
Puertos	443, 60269

En la captura se observa el tráfico generado por el servicio web de YouTube, donde el cliente (192.168.219.198) establece una conexión con el servidor (157.55.219.198) a través del protocolo TLSv1.2. El servidor utiliza el puerto estándar 443 (HTTPS), mientras que el cliente emplea el puerto efímero 60269. Los segmentos muestran la negociación y transmisión de datos cifrados en la capa de aplicación

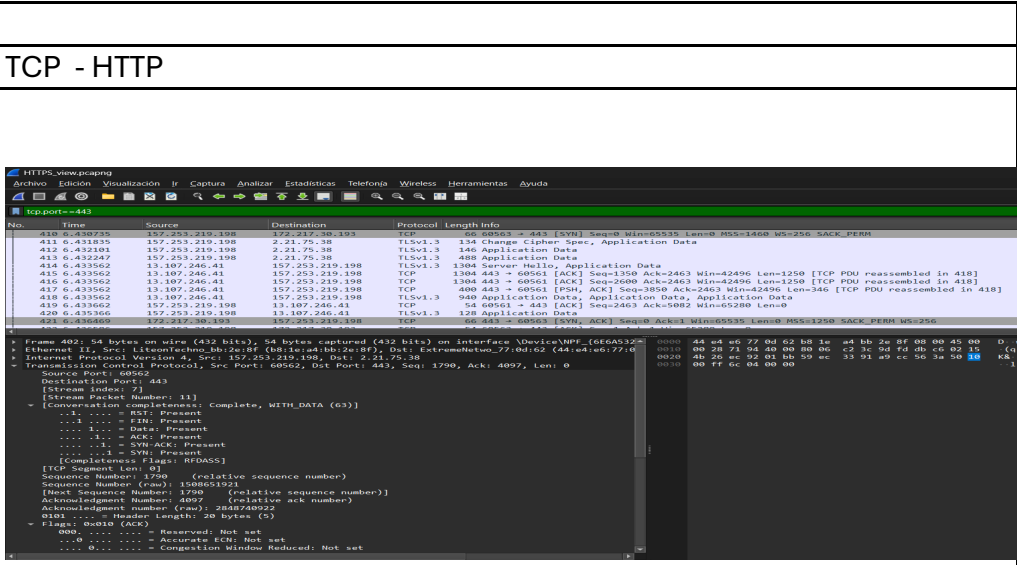
8.7 Análisis TCP

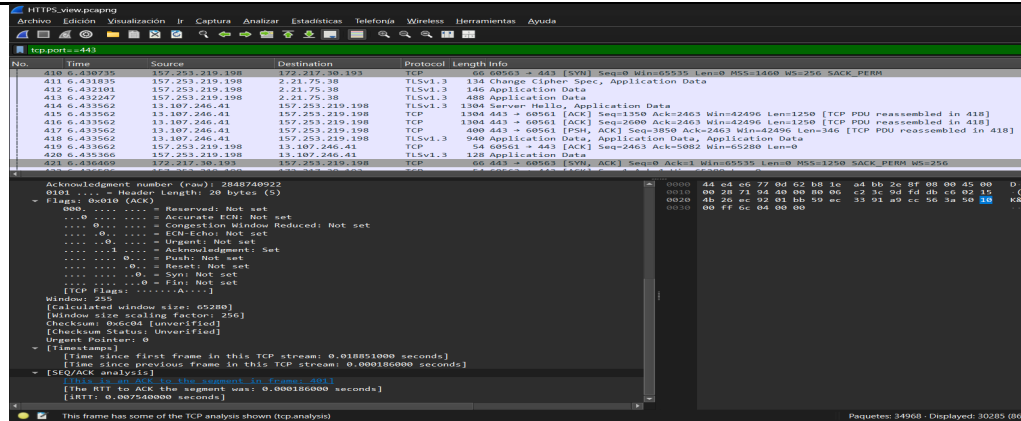
TCP	
Protocolo	TCP - HTTP
Información de la capa de aplicación	

	
Puertos	443, 60529

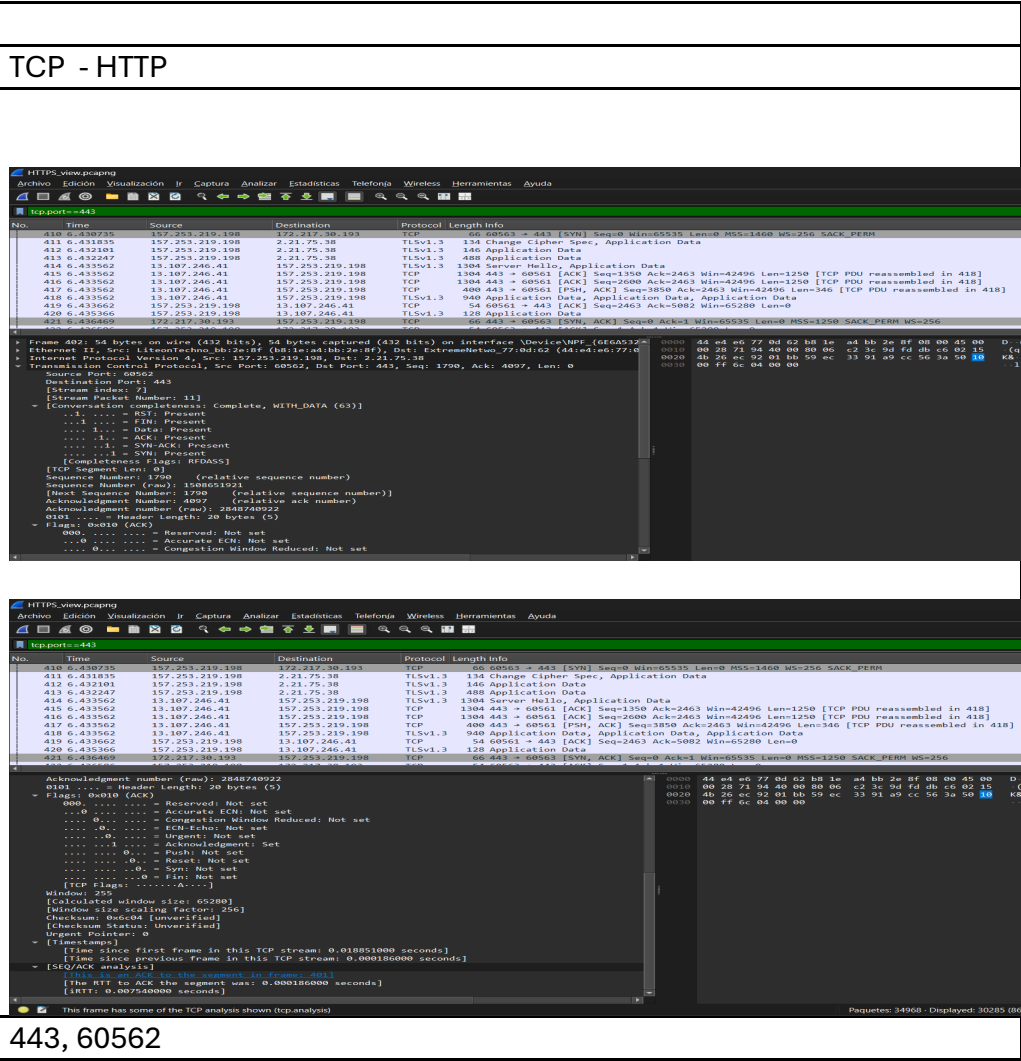
En la captura se observa el establecimiento de una sesión TCP entre el cliente (192.168.219.198) y el servidor (157.55.219.198). El servidor utiliza el puerto estándar 443, mientras que el cliente emplea el puerto efímero 60529. Los segmentos muestran confirmaciones ACK que garantizan la entrega ordenada de los datos y mantienen activa la conexión.

HTTPS view

TCP	
Protocolo	TCP - HTTP
Información de la capa de aplicación	

	
Puertos	443, 60562

En la captura se observa la comunicación entre el cliente (192.168.219.198) y el servidor (157.240.28.219) donde TCP (puerto origen 60559, puerto destino 443) establece el canal confiable de transporte. Sobre este canal, la capa de aplicación ejecuta HTTP, pero los mensajes no aparecen en texto claro, ya que son encapsulados y cifrados por TLS v1.3

TCP	
Protocolo	TCP - HTTP
Información de la capa de aplicación	
Puertos	443, 60562

En la captura se observa el intercambio de tráfico seguro entre el cliente (192.168.219.198) y el servidor (157.240.28.243) a través de TLSv1.3. El servidor utiliza el puerto estándar 443, mientras que el cliente emplea el puerto efímero 60562. En la capa de aplicación se identifican mensajes de tipo Change Cipher Spec y bloques de Application Data, que corresponden a información HTTP cifrada mediante TLS. Posteriormente, los segmentos ACK garantizan la entrega confiable de los datos dentro de la sesión.

[illegible]

8.8 Análisis del protocolo VoIP

Voip

RTP																																																																																																			
Protocolo	RTP - UDP																																																																																																		
Información de la capa de aplicación	<div><div>VoIP_view.pcapng</div><div>ArchivoEdiciónVisualizaciónIrCapturaAnalizarEstadísticasTelefoníaWirelessHerramientasAyuda</div><div><div><div>rtptime</div></div><table><tr><th>No.</th><th>Time</th><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr><tr><td>2003</td><td>19.309978</td><td>192.168.160.242</td><td>192.168.160.52</td><td>RTP</td><td>214</td><td>PT=ITU-T G.711 PC</td></tr><tr><td>2002</td><td>19.309956</td><td>192.168.160.242</td><td>192.168.160.52</td><td>RTP</td><td>214</td><td>PT=ITU-T G.711 PC</td></tr><tr><td>117</td><td>8.209194</td><td>192.168.160.242</td><td>192.168.160.52</td><td>RTP</td><td>214</td><td>PT=ITU-T G.711 PC</td></tr><tr><td>116</td><td>8.209172</td><td>192.168.160.242</td><td>192.168.160.52</td><td>RTP</td><td>214</td><td>PT=ITU-T G.711 PC</td></tr><tr><td>107</td><td>8.169225</td><td>192.168.160.242</td><td>192.168.160.52</td><td>RTP</td><td>214</td><td>PT=ITU-T G.711 PC</td></tr><tr><td>106</td><td>8.169216</td><td>192.168.160.242</td><td>192.168.160.52</td><td>RTP</td><td>214</td><td>PT=ITU-T G.711 PC</td></tr><tr><td>105</td><td>8.098435</td><td>192.168.160.242</td><td>192.168.160.52</td><td>RTP</td><td>55</td><td>PT=Unassigned, SS</td></tr><tr><td>104</td><td>8.098426</td><td>192.168.160.242</td><td>192.168.160.52</td><td>RTP</td><td>55</td><td>PT=Unassigned, SS</td></tr><tr><td>118</td><td>8.214526</td><td>192.168.160.106</td><td>192.168.160.26</td><td>RTP</td><td>55</td><td>PT=Unassigned, SS</td></tr><tr><td>1990</td><td>19.275501</td><td>192.168.160.106</td><td>192.168.160.242</td><td>ICMP</td><td>242</td><td>Destination unrea</td></tr><tr><td>1987</td><td>19.254728</td><td>192.168.160.106</td><td>192.168.160.242</td><td>ICMP</td><td>242</td><td>Destination unrea</td></tr><tr><td>1984</td><td>19.231501</td><td>192.168.160.106</td><td>192.168.160.242</td><td>ICMP</td><td>242</td><td>Destination unrea</td></tr><tr><td>1981</td><td>19.233666</td><td>192.168.160.106</td><td>192.168.160.242</td><td>ICMP</td><td>242</td><td>Destination unrea</td></tr></table><div><div>Frame 107: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface \Device</div><div>Ethernet II, Src: LiteonTechno_bb:2e:8f (b8:1e:a4:bb:2e:8f), Dst: VMware_d8:d9:34 (00:0c:29:d</div><div>Internet Protocol Version 4, Src: 192.168.160.242, Dst: 192.168.160.52</div><div>User Datagram Protocol, Src Port: 63253, Dst Port: 13402</div><div>Source Port: 63253</div><div>Destination Port: 13402</div><div>Length: 180</div><div>Checksum: 0x473b [unverified]</div><div>[Checksum Status: Unverified]</div><div>[Stream index: 64]</div><div>[Stream Packet Number: 4]</div><div>[Timestamps]</div><div>UDP payload (172 bytes)</div><div>Real-Time Transport Protocol</div><div>[Stream setup by SDP (Frame 81)]</div><div>10.. = Version: RFC 1889 Version (2)</div><div>..0. = Padding: False</div><div>.... 0000 = Extension: False</div><div>.... 0000 = Contributing source identifiers count: 0</div><div>1... .. = Marker: True</div><div>Payload type: ITU-T G.711 PCMU (0)</div><div>Sequence number: 53016</div><div>[Extended sequence number: 53016]</div><div>Timestamp: 2546679317</div><div>[Extended timestamp: 2546679317]</div><div>Synchronization Source identifier: 0x8816b1e9 (2283188713)</div><div>Payload [...]: ff</div></div></div></div>	No.	Time	Source	Destination	Protocol	Length	Info	2003	19.309978	192.168.160.242	192.168.160.52	RTP	214	PT=ITU-T G.711 PC	2002	19.309956	192.168.160.242	192.168.160.52	RTP	214	PT=ITU-T G.711 PC	117	8.209194	192.168.160.242	192.168.160.52	RTP	214	PT=ITU-T G.711 PC	116	8.209172	192.168.160.242	192.168.160.52	RTP	214	PT=ITU-T G.711 PC	107	8.169225	192.168.160.242	192.168.160.52	RTP	214	PT=ITU-T G.711 PC	106	8.169216	192.168.160.242	192.168.160.52	RTP	214	PT=ITU-T G.711 PC	105	8.098435	192.168.160.242	192.168.160.52	RTP	55	PT=Unassigned, SS	104	8.098426	192.168.160.242	192.168.160.52	RTP	55	PT=Unassigned, SS	118	8.214526	192.168.160.106	192.168.160.26	RTP	55	PT=Unassigned, SS	1990	19.275501	192.168.160.106	192.168.160.242	ICMP	242	Destination unrea	1987	19.254728	192.168.160.106	192.168.160.242	ICMP	242	Destination unrea	1984	19.231501	192.168.160.106	192.168.160.242	ICMP	242	Destination unrea	1981	19.233666	192.168.160.106	192.168.160.242	ICMP	242	Destination unrea
No.	Time	Source	Destination	Protocol	Length	Info																																																																																													
2003	19.309978	192.168.160.242	192.168.160.52	RTP	214	PT=ITU-T G.711 PC																																																																																													
2002	19.309956	192.168.160.242	192.168.160.52	RTP	214	PT=ITU-T G.711 PC																																																																																													
117	8.209194	192.168.160.242	192.168.160.52	RTP	214	PT=ITU-T G.711 PC																																																																																													
116	8.209172	192.168.160.242	192.168.160.52	RTP	214	PT=ITU-T G.711 PC																																																																																													
107	8.169225	192.168.160.242	192.168.160.52	RTP	214	PT=ITU-T G.711 PC																																																																																													
106	8.169216	192.168.160.242	192.168.160.52	RTP	214	PT=ITU-T G.711 PC																																																																																													
105	8.098435	192.168.160.242	192.168.160.52	RTP	55	PT=Unassigned, SS																																																																																													
104	8.098426	192.168.160.242	192.168.160.52	RTP	55	PT=Unassigned, SS																																																																																													
118	8.214526	192.168.160.106	192.168.160.26	RTP	55	PT=Unassigned, SS																																																																																													
1990	19.275501	192.168.160.106	192.168.160.242	ICMP	242	Destination unrea																																																																																													
1987	19.254728	192.168.160.106	192.168.160.242	ICMP	242	Destination unrea																																																																																													
1984	19.231501	192.168.160.106	192.168.160.242	ICMP	242	Destination unrea																																																																																													
1981	19.233666	192.168.160.106	192.168.160.242	ICMP	242	Destination unrea																																																																																													
Puertos	63253, 13402																																																																																																		

SIP	
Protocolo	SIP - UDP
Información de la capa de aplicación	

VoIP_view.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

sip

No.	Time	Source	Destination	Protocol	Length	Info
1994	19.286742	192.168.160.52	192.168.160.242	SIP/SDP	993	Request: INVITE sip:1001@192.
266	9.208376	192.168.160.52	192.168.160.242	SIP	696	Status: 200 OK (REGISTER) (1
265	9.208368	192.168.160.52	192.168.160.242	SIP	696	Status: 200 OK (REGISTER) (1
248	9.099768	192.168.160.52	192.168.160.242	SIP	637	Status: 401 Unauthorized
247	9.099758	192.168.160.52	192.168.160.242	SIP	637	Status: 401 Unauthorized
122	8.217892	192.168.160.52	192.168.160.242	SIP	529	Request: ACK sip:1001@192.168
121	8.217855	192.168.160.52	192.168.160.242	SIP	529	Request: ACK sip:1001@192.168
115	8.194013	192.168.160.52	192.168.160.242	SIP/SDP	970	Request: INVITE sip:1001@192.
114	8.193986	192.168.160.52	192.168.160.242	SIP/SDP	970	Request: INVITE sip:1001@192.
111	8.176835	192.168.160.52	192.168.160.242	SIP	529	Request: ACK sip:1001@192.168
110	8.176822	192.168.160.52	192.168.160.242	SIP	529	Request: ACK sip:1001@192.168
82	6.043222	192.168.160.52	192.168.160.242	SIP/SDP	1058	Request: INVITE sip:1001@192.

Frame 121: 529 bytes on wire (4232 bits), 529 bytes captured (4232 bits) on interface \Device\NPF_{6E6...}

Ethernet II, Src: LiteonTechno_bb:2e:8f (b8:1e:a4:bb:2e:8f), Dst: LiteonTechno_bb:2e:8f (b8:1e:a4:bb:2e:8f)

Internet Protocol Version 4, Src: 192.168.160.52, Dst: 192.168.160.242

User Datagram Protocol, Src Port: 5060, Dst Port: 55200

- Source Port: 5060
- Destination Port: 55200
- Length: 495
- Checksum: 0x5f41 [unverified]
- [Checksum Status: Unverified]
- [Stream index: 17]
- [Stream Packet Number: 15]
- [Timestamps]
- UDP payload (487 bytes)

Session Initiation Protocol (ACK)

- Request-Line: ACK sip:1001@192.168.160.242:55200 SIP/2.0
- Method: ACK
- Request-URI: sip:1001@192.168.160.242:55200
 - Request-URI User Part: 1001
 - Request-URI Host Part: 192.168.160.242
 - Request-URI Host Port: 55200
- [Resent Packet: False]
- [Request Frame: 114]
- [Response Time (ms): 23]
- Message Header
 - Via: SIP/2.0/UDP 192.168.160.52:5060;branch=z9hG4bK2ee3b923;rport
 - Transport: UDP
 - Sent-by Address: 192.168.160.52

VoIP_view.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

sip

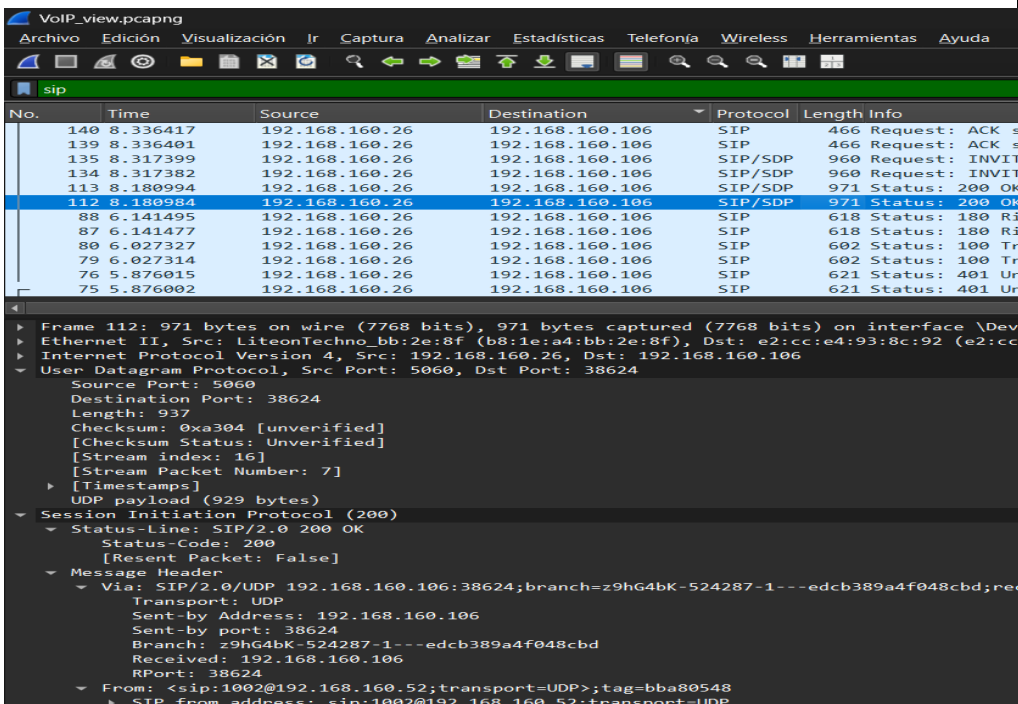
No.	Time	Source	Destination	Protocol	Length	Info
1994	19.286742	192.168.160.52	192.168.160.242	SIP/SDP	993	Request: INVITE
266	9.208376	192.168.160.52	192.168.160.242	SIP	696	Status: 200 OK (
265	9.208368	192.168.160.52	192.168.160.242	SIP	696	Status: 200 OK (
248	9.099768	192.168.160.52	192.168.160.242	SIP	637	Status: 401 Unau
247	9.099758	192.168.160.52	192.168.160.242	SIP	637	Status: 401 Unau
122	8.217892	192.168.160.52	192.168.160.242	SIP	529	Request: ACK sip
121	8.217855	192.168.160.52	192.168.160.242	SIP	529	Request: ACK sip
115	8.194013	192.168.160.52	192.168.160.242	SIP/SDP	970	Request: INVITE
114	8.193986	192.168.160.52	192.168.160.242	SIP/SDP	970	Request: INVITE
111	8.176835	192.168.160.52	192.168.160.242	SIP	529	Request: ACK sip
110	8.176822	192.168.160.52	192.168.160.242	SIP	529	Request: ACK sip
82	6.043222	192.168.160.52	192.168.160.242	SIP/SDP	1058	Request: INVITE
81	6.043218	192.168.160.52	192.168.160.242	SIP/SDP	1058	Request: INVITE

```

Via: SIP/2.0/UDP 192.168.160.52:5060;branch=z9hG4bK2ee3b923;rport
    Transport: UDP
    Sent-by Address: 192.168.160.52
    Sent-by port: 5060
    Branch: z9hG4bK2ee3b923
    RPort: rport
    Max-Forwards: 70
From: "Usuario 1002" <sip:1002@192.168.160.52>;tag=as038d46e6
    SIP from display info: "Usuario 1002"
    SIP from address: sip:1002@192.168.160.52
    SIP from tag: as038d46e6
To: <sip:1001@192.168.160.242:55200;rinstance=de23cc5cd8700bcd;transport=UDP>;tag=4d395201
    SIP to address: sip:1001@192.168.160.242:55200;rinstance=de23cc5cd8700bcd;transport=
        SIP to address User Part: 1001
        SIP to address Host Part: 192.168.160.242
        SIP to address Host Port: 55200
        SIP To URI parameter: rinstance=de23cc5cd8700bcd
        SIP To URI parameter: transport=UDP
        SIP to tag: 4d395201
Contact: <sip:1002@192.168.160.52:5060>
    Contact URI: sip:1002@192.168.160.52:5060
        Contact URI User Part: 1002
        Contact URI Host Part: 192.168.160.52
        Contact URI Host Port: 5060
Call-ID: 194eb1c65c140e8a38b7729a6ad91fa2@192.168.160.52:5060
[Generated Call-ID: 194eb1c65c140e8a38b7729a6ad91fa2@192.168.160.52:5060]
CSeq: 103 ACK
  
```

	<div><div>VolP_view.pcapng</div><div>ArchivoEdiciónVisualizaciónIrCapturaAnalizarEstadísticasTelefoníaWirelessHerramientasAyuda</div><div></div><div>sip</div><table><thead><tr><th>No.</th><th>Time</th><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr></thead><tbody><tr><td>1994</td><td>19.286742</td><td>192.168.160.52</td><td>192.168.160.242</td><td>SIP/SDP</td><td>993</td><td>Request: INVITE sip:1002@192.168.160.52</td></tr><tr><td>266</td><td>9.208376</td><td>192.168.160.52</td><td>192.168.160.242</td><td>SIP</td><td>696</td><td>Status: 200 OK (Reason: SIP/2.0)</td></tr><tr><td>265</td><td>9.208368</td><td>192.168.160.52</td><td>192.168.160.242</td><td>SIP</td><td>696</td><td>Status: 200 OK (Reason: SIP/2.0)</td></tr><tr><td>248</td><td>9.099768</td><td>192.168.160.52</td><td>192.168.160.242</td><td>SIP</td><td>637</td><td>Status: 401 Unauthorized</td></tr><tr><td>247</td><td>9.099758</td><td>192.168.160.52</td><td>192.168.160.242</td><td>SIP</td><td>637</td><td>Status: 401 Unauthorized</td></tr><tr><td>122</td><td>8.217892</td><td>192.168.160.52</td><td>192.168.160.242</td><td>SIP</td><td>529</td><td>Request: ACK sip:1002@192.168.160.52</td></tr><tr><td>121</td><td>8.217855</td><td>192.168.160.52</td><td>192.168.160.242</td><td>SIP</td><td>529</td><td>Request: ACK sip:1002@192.168.160.52</td></tr><tr><td>115</td><td>8.194013</td><td>192.168.160.52</td><td>192.168.160.242</td><td>SIP/SDP</td><td>970</td><td>Request: INVITE sip:1002@192.168.160.52</td></tr><tr><td>114</td><td>8.193986</td><td>192.168.160.52</td><td>192.168.160.242</td><td>SIP/SDP</td><td>970</td><td>Request: INVITE sip:1002@192.168.160.52</td></tr><tr><td>111</td><td>8.176835</td><td>192.168.160.52</td><td>192.168.160.242</td><td>SIP</td><td>529</td><td>Request: ACK sip:1002@192.168.160.52</td></tr><tr><td>110</td><td>8.176822</td><td>192.168.160.52</td><td>192.168.160.242</td><td>SIP</td><td>529</td><td>Request: ACK sip:1002@192.168.160.52</td></tr><tr><td>82</td><td>6.043222</td><td>192.168.160.52</td><td>192.168.160.242</td><td>SIP/SDP</td><td>1058</td><td>Request: INVITE sip:1002@192.168.160.52</td></tr></tbody></table><div><div>Branch: z9hG4bK2ee3b923</div><div>RPort: rport</div><div>Max-Forwards: 70</div><div>From: "Usuario 1002" <sip:1002@192.168.160.52>;tag=as038d46e6</div><div>SIP from display info: "Usuario 1002"</div><div>SIP from address: sip:1002@192.168.160.52</div><div>SIP from tag: as038d46e6</div><div>To: <sip:1001@192.168.160.242:55200;rinstance=de23cc5cd8700bcd;transport=UDP>;tag=4d395201</div><div>SIP to address: sip:1001@192.168.160.242:55200;rinstance=de23cc5cd8700bcd;transport=UDP</div><div>SIP to address User Part: 1001</div><div>SIP to address Host Part: 192.168.160.242</div><div>SIP to address Host Port: 55200</div><div>SIP To URI parameter: rinstance=de23cc5cd8700bcd</div><div>SIP To URI parameter: transport=UDP</div><div>SIP to tag: 4d395201</div><div>Contact: <sip:1002@192.168.160.52:5060></div><div>Contact URI: sip:1002@192.168.160.52:5060</div><div>Contact URI User Part: 1002</div><div>Contact URI Host Part: 192.168.160.52</div><div>Contact URI Host Port: 5060</div><div>Call-ID: 194eb1c65c140e8a38b7729a6ad91fa2@192.168.160.52:5060</div><div>[Generated Call-ID: 194eb1c65c140e8a38b7729a6ad91fa2@192.168.160.52:5060]</div><div>CSeq: 103 ACK</div><div>Sequence Number: 103</div><div>Method: ACK</div><div>User-Agent: Asterisk PBX 20.6.0~dfsg+~cs6.13.40431414-2build5</div><div>Content-Length: 0</div></div></div>	No.	Time	Source	Destination	Protocol	Length	Info	1994	19.286742	192.168.160.52	192.168.160.242	SIP/SDP	993	Request: INVITE sip:1002@192.168.160.52	266	9.208376	192.168.160.52	192.168.160.242	SIP	696	Status: 200 OK (Reason: SIP/2.0)	265	9.208368	192.168.160.52	192.168.160.242	SIP	696	Status: 200 OK (Reason: SIP/2.0)	248	9.099768	192.168.160.52	192.168.160.242	SIP	637	Status: 401 Unauthorized	247	9.099758	192.168.160.52	192.168.160.242	SIP	637	Status: 401 Unauthorized	122	8.217892	192.168.160.52	192.168.160.242	SIP	529	Request: ACK sip:1002@192.168.160.52	121	8.217855	192.168.160.52	192.168.160.242	SIP	529	Request: ACK sip:1002@192.168.160.52	115	8.194013	192.168.160.52	192.168.160.242	SIP/SDP	970	Request: INVITE sip:1002@192.168.160.52	114	8.193986	192.168.160.52	192.168.160.242	SIP/SDP	970	Request: INVITE sip:1002@192.168.160.52	111	8.176835	192.168.160.52	192.168.160.242	SIP	529	Request: ACK sip:1002@192.168.160.52	110	8.176822	192.168.160.52	192.168.160.242	SIP	529	Request: ACK sip:1002@192.168.160.52	82	6.043222	192.168.160.52	192.168.160.242	SIP/SDP	1058	Request: INVITE sip:1002@192.168.160.52
No.	Time	Source	Destination	Protocol	Length	Info																																																																																						
1994	19.286742	192.168.160.52	192.168.160.242	SIP/SDP	993	Request: INVITE sip:1002@192.168.160.52																																																																																						
266	9.208376	192.168.160.52	192.168.160.242	SIP	696	Status: 200 OK (Reason: SIP/2.0)																																																																																						
265	9.208368	192.168.160.52	192.168.160.242	SIP	696	Status: 200 OK (Reason: SIP/2.0)																																																																																						
248	9.099768	192.168.160.52	192.168.160.242	SIP	637	Status: 401 Unauthorized																																																																																						
247	9.099758	192.168.160.52	192.168.160.242	SIP	637	Status: 401 Unauthorized																																																																																						
122	8.217892	192.168.160.52	192.168.160.242	SIP	529	Request: ACK sip:1002@192.168.160.52																																																																																						
121	8.217855	192.168.160.52	192.168.160.242	SIP	529	Request: ACK sip:1002@192.168.160.52																																																																																						
115	8.194013	192.168.160.52	192.168.160.242	SIP/SDP	970	Request: INVITE sip:1002@192.168.160.52																																																																																						
114	8.193986	192.168.160.52	192.168.160.242	SIP/SDP	970	Request: INVITE sip:1002@192.168.160.52																																																																																						
111	8.176835	192.168.160.52	192.168.160.242	SIP	529	Request: ACK sip:1002@192.168.160.52																																																																																						
110	8.176822	192.168.160.52	192.168.160.242	SIP	529	Request: ACK sip:1002@192.168.160.52																																																																																						
82	6.043222	192.168.160.52	192.168.160.242	SIP/SDP	1058	Request: INVITE sip:1002@192.168.160.52																																																																																						
Puertos	5060, 552000																																																																																											

La captura muestra el intercambio de mensajes del Session Initiation Protocol (SIP) entre el cliente (192.168.160.242) y el servidor (192.168.160.52). El servidor utiliza el puerto estándar 5060, mientras que el cliente se conecta desde el puerto efímero 55200, ambos sobre el protocolo de transporte UDP. A diferencia de TCP, aquí no existe confirmación de entrega a nivel de transporte, por lo que la confiabilidad depende de los mecanismos propios de la aplicación.

SIP /SDP																																																																																												
Protocolo	SIP - UDP																																																																																											
Información de la capa de aplicación	 <p>The screenshot displays a Wireshark capture of network traffic. The top pane shows a list of packets, with packet 112 (SIP/SDP) selected. The middle pane shows the details of this packet, including the User Datagram Protocol (UDP) and Session Initiation Protocol (SIP) headers. The SIP message is a 200 OK response.</p> <table><tr><th>No.</th><th>Time</th><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr><tr><td>140</td><td>8.336417</td><td>192.168.160.26</td><td>192.168.160.106</td><td>SIP</td><td>466</td><td>Request: ACK s</td></tr><tr><td>139</td><td>8.336401</td><td>192.168.160.26</td><td>192.168.160.106</td><td>SIP</td><td>466</td><td>Request: ACK s</td></tr><tr><td>135</td><td>8.317399</td><td>192.168.160.26</td><td>192.168.160.106</td><td>SIP/SDP</td><td>960</td><td>Request: INVIT</td></tr><tr><td>134</td><td>8.317382</td><td>192.168.160.26</td><td>192.168.160.106</td><td>SIP/SDP</td><td>960</td><td>Request: INVIT</td></tr><tr><td>113</td><td>8.180994</td><td>192.168.160.26</td><td>192.168.160.106</td><td>SIP/SDP</td><td>971</td><td>Status: 200 OK</td></tr><tr><td>112</td><td>8.180984</td><td>192.168.160.26</td><td>192.168.160.106</td><td>SIP/SDP</td><td>971</td><td>Status: 200 OK</td></tr><tr><td>88</td><td>6.141495</td><td>192.168.160.26</td><td>192.168.160.106</td><td>SIP</td><td>618</td><td>Status: 180 R</td></tr><tr><td>87</td><td>6.141477</td><td>192.168.160.26</td><td>192.168.160.106</td><td>SIP</td><td>618</td><td>Status: 180 R</td></tr><tr><td>80</td><td>6.027327</td><td>192.168.160.26</td><td>192.168.160.106</td><td>SIP</td><td>602</td><td>Status: 100 Tr</td></tr><tr><td>79</td><td>6.027314</td><td>192.168.160.26</td><td>192.168.160.106</td><td>SIP</td><td>602</td><td>Status: 100 Tr</td></tr><tr><td>76</td><td>5.876015</td><td>192.168.160.26</td><td>192.168.160.106</td><td>SIP</td><td>621</td><td>Status: 401 Ur</td></tr><tr><td>75</td><td>5.876002</td><td>192.168.160.26</td><td>192.168.160.106</td><td>SIP</td><td>621</td><td>Status: 401 Ur</td></tr></table> <p>Frame 112: 971 bytes on wire (7768 bits), 971 bytes captured (7768 bits) on interface \Dev Ethernet II, Src: LiteonTechno_bb:2e:8f (b8:1e:a4:bb:2e:8f), Dst: e2:cc:e4:93:8c:92 (e2:cc Internet Protocol Version 4, Src: 192.168.160.26, Dst: 192.168.160.106 User Datagram Protocol, Src Port: 5060, Dst Port: 38624 Source Port: 5060 Destination Port: 38624 Length: 937 Checksum: 0xa304 [unverified] [Checksum Status: Unverified] [Stream index: 16] [Stream Packet Number: 7] [Timestamps] UDP payload (929 bytes) Session Initiation Protocol (200) Status-Line: SIP/2.0 200 OK Status-Code: 200 [Resent Packet: False] Message Header Via: SIP/2.0/UDP 192.168.160.106:38624;branch=z9hG4bK-524287-1---edcb389a4f048cbd;re Transport: UDP Sent-by Address: 192.168.160.106 Sent-by port: 38624 Branch: z9hG4bK-524287-1---edcb389a4f048cbd Received: 192.168.160.106 RPort: 38624 From: <sip:1002@192.168.160.52;transport=UDP>;tag=bba80548 SIP from address: sip:1002@192.168.160.52;transport=UDP</p>	No.	Time	Source	Destination	Protocol	Length	Info	140	8.336417	192.168.160.26	192.168.160.106	SIP	466	Request: ACK s	139	8.336401	192.168.160.26	192.168.160.106	SIP	466	Request: ACK s	135	8.317399	192.168.160.26	192.168.160.106	SIP/SDP	960	Request: INVIT	134	8.317382	192.168.160.26	192.168.160.106	SIP/SDP	960	Request: INVIT	113	8.180994	192.168.160.26	192.168.160.106	SIP/SDP	971	Status: 200 OK	112	8.180984	192.168.160.26	192.168.160.106	SIP/SDP	971	Status: 200 OK	88	6.141495	192.168.160.26	192.168.160.106	SIP	618	Status: 180 R	87	6.141477	192.168.160.26	192.168.160.106	SIP	618	Status: 180 R	80	6.027327	192.168.160.26	192.168.160.106	SIP	602	Status: 100 Tr	79	6.027314	192.168.160.26	192.168.160.106	SIP	602	Status: 100 Tr	76	5.876015	192.168.160.26	192.168.160.106	SIP	621	Status: 401 Ur	75	5.876002	192.168.160.26	192.168.160.106	SIP	621	Status: 401 Ur
No.	Time	Source	Destination	Protocol	Length	Info																																																																																						
140	8.336417	192.168.160.26	192.168.160.106	SIP	466	Request: ACK s																																																																																						
139	8.336401	192.168.160.26	192.168.160.106	SIP	466	Request: ACK s																																																																																						
135	8.317399	192.168.160.26	192.168.160.106	SIP/SDP	960	Request: INVIT																																																																																						
134	8.317382	192.168.160.26	192.168.160.106	SIP/SDP	960	Request: INVIT																																																																																						
113	8.180994	192.168.160.26	192.168.160.106	SIP/SDP	971	Status: 200 OK																																																																																						
112	8.180984	192.168.160.26	192.168.160.106	SIP/SDP	971	Status: 200 OK																																																																																						
88	6.141495	192.168.160.26	192.168.160.106	SIP	618	Status: 180 R																																																																																						
87	6.141477	192.168.160.26	192.168.160.106	SIP	618	Status: 180 R																																																																																						
80	6.027327	192.168.160.26	192.168.160.106	SIP	602	Status: 100 Tr																																																																																						
79	6.027314	192.168.160.26	192.168.160.106	SIP	602	Status: 100 Tr																																																																																						
76	5.876015	192.168.160.26	192.168.160.106	SIP	621	Status: 401 Ur																																																																																						
75	5.876002	192.168.160.26	192.168.160.106	SIP	621	Status: 401 Ur																																																																																						

VoIP_view.pcapng
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

sip

No.	Time	Source	Destination	Protocol	Length	Info
140	8.336417	192.168.160.26	192.168.160.106	SIP	466	Request: ACK sip:10
139	8.336401	192.168.160.26	192.168.160.106	SIP	466	Request: ACK sip:10
135	8.317399	192.168.160.26	192.168.160.106	SIP/SDP	960	Request: INVITE sip
134	8.317382	192.168.160.26	192.168.160.106	SIP/SDP	960	Request: INVITE sip
113	8.180994	192.168.160.26	192.168.160.106	SIP/SDP	971	Status: 200 OK (INV
112	8.180984	192.168.160.26	192.168.160.106	SIP/SDP	971	Status: 200 OK (INV
88	6.141495	192.168.160.26	192.168.160.106	SIP	618	Status: 180 Ringing
87	6.141477	192.168.160.26	192.168.160.106	SIP	618	Status: 180 Ringing
80	6.027327	192.168.160.26	192.168.160.106	SIP	602	Status: 100 Trying
79	6.027314	192.168.160.26	192.168.160.106	SIP	602	Status: 100 Trying
76	5.876015	192.168.160.26	192.168.160.106	SIP	621	Status: 401 Unauthc
75	5.876002	192.168.160.26	192.168.160.106	SIP	621	Status: 401 Unauthc

RPort: 38624

- From: <sip:1002@192.168.160.52;transport=UDP>;tag=bba80548
 - SIP from address: sip:1002@192.168.160.52;transport=UDP
 - SIP from tag: bba80548
- To: <sip:1001@192.168.160.52>;tag=as485450be
 - SIP to address: sip:1001@192.168.160.52
 - SIP to address User Part: 1001
 - SIP to address Host Part: 192.168.160.52
 - SIP to tag: as485450be
- Call-ID: y1mx9gzpKZieleb9NUA6jA..
- [Generated Call-ID: y1mx9gzpKZieleb9NUA6jA..]
- CSeq: 2 INVITE
 - Sequence Number: 2
 - Method: INVITE
- Server: Asterisk PBX 20.6.0~dfsg+~cs6.13.40431414-2build5
- Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH, MESSAGE
- Supported: replaces, timer
- Session-Expires: 1800;refresher=uas
- Contact: <sip:1001@192.168.160.26:5060>
 - Contact URI: sip:1001@192.168.160.26:5060
 - Contact URI User Part: 1001
 - Contact URI Host Part: 192.168.160.26
 - Contact URI Host Port: 5060
- Content-Type: application/sdp
- Require: timer
- Content-Length: 309
- Message Body

Bytes 284-318: Call-ID (sip.Call-ID)

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Capture, Analyze, Statistics, Telephone, Wireless, and Help. The toolbar contains various icons for file operations, network analysis, and search. The packet list pane shows a list of captured packets, with packet 112 selected. The packet details pane shows the structure of the selected packet, including Session Description Protocol (SDP) information. The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
140	8.336417	192.168.160.26	192.168.160.106	SIP	466	Request: ACK sip
139	8.336401	192.168.160.26	192.168.160.106	SIP	466	Request: ACK sip
135	8.317399	192.168.160.26	192.168.160.106	SIP/SDP	960	Request: INVITE
134	8.317382	192.168.160.26	192.168.160.106	SIP/SDP	960	Request: INVITE
113	8.180994	192.168.160.26	192.168.160.106	SIP/SDP	971	Status: 200 OK
112	8.180984	192.168.160.26	192.168.160.106	SIP/SDP	971	Status: 200 OK
88	6.141495	192.168.160.26	192.168.160.106	SIP	618	Status: 180 Ring
87	6.141477	192.168.160.26	192.168.160.106	SIP	618	Status: 180 Ring
80	6.027327	192.168.160.26	192.168.160.106	SIP	602	Status: 100 Tryi
79	6.027314	192.168.160.26	192.168.160.106	SIP	602	Status: 100 Tryi
76	5.876015	192.168.160.26	192.168.160.106	SIP	621	Status: 401 Unau
75	5.876002	192.168.160.26	192.168.160.106	SIP	621	Status: 401 Unau

Content-Length: 309

Message Body

Session Description Protocol

Session Description Protocol Version (v): 0

Owner/Creator, Session Id (o): root 1992404056 1992404056 IN IP4 192.168.160.26

Owner Username: root

Session ID: 1992404056

Session Version: 1992404056

Owner Network Type: IN

Owner Address Type: IP4

Owner Address: 192.168.160.26

Session Name (s): Asterisk PBX 20.6.0~dfsg+~cs6.13.40431414-2build5

Connection Information (c): IN IP4 192.168.160.26

Connection Network Type: IN

Connection Address Type: IP4

Connection Address: 192.168.160.26

Time Description, active time (t): 0 0

Session Start Time: 0

Session Stop Time: 0

Media Description, name and address (m): audio 18322 RTP/AVP 0 8 101

Media Type: audio

Media Port: 18322

Media Protocol: RTP/AVP

Media Format: ITU-T G.711 PCMU

Media Format: ITU-T G.711 PCMA

Media Format: DynamicRTP-Type-101

Media Attribute (a): rtpmap:0 PCMU/8000

	<div><div><div>VolP_view.pcapng</div><div>ArchivoEdiciónVisualizaciónIrCapturaAnalizarEstadísticasTelefoníaWirelessHerramientasAyuda</div><div><div><div><div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div></div></div></div></div></div>
--	---

En la captura se observa el intercambio de mensajes SIP/SDP entre el cliente (192.168.160.26) y el servidor (192.168.160.106). El servidor utiliza el puerto estándar 5060, mientras que el cliente se conecta desde el puerto efímero 38624, ambos sobre UDP como protocolo de transporte.

En la capa de aplicación se aprecia un mensaje 200 OK (INVITE), que confirma la aceptación de la sesión iniciada previamente. Este mensaje incluye un cuerpo con Session Description Protocol (SDP), encargado de transportar los parámetros de la sesión multimedia: códec de audio soportado, direcciones IP de origen/destino y puertos donde se establecerá posteriormente el flujo de voz mediante RTP.

8.9 Análisis del protocolo RTMP

RTMP						
Protocolos	RTMP - TCP					
	No.	Time	Source	Destination	Protocol	Length Info
	7024	15.405199	192.168.160.54	192.168.160.166	TCP	1514 [TCP Retransmission]
	7025	15.405212	192.168.160.54	192.168.160.166	RTMP	1514 Unknown (0x0)
Información de la capa de aplicación	<div>> Frame 7025: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{...}</div> <div>> Ethernet II, Src: Intel_34:d5:0a (f4:26:79:34:d5:0a), Dst: Intel_34:d5:0a (f4:26:79:34:d5:0a)</div> <div>> Internet Protocol Version 4, Src: 192.168.160.54, Dst: 192.168.160.166</div> <div>> Transmission Control Protocol, Src Port: 1935, Dst Port: 60616, Seq: 2922050, Ack: 17, Len: 1460</div> <div>> Real Time Messaging Protocol (Unknown (0x0))<div>RTMP Header<div>11.. = Format: 3</div><div>..10 0101 = Chunk Stream ID: 37</div><div>Timestamp: 0 (calculated)</div></div>RTMP Body</div>					
Puertos	1935, 60616					

En la captura se observa tráfico correspondiente al Real-Time Messaging Protocol (RTMP), utilizado principalmente para la transmisión en tiempo real de audio, video y datos en aplicaciones de streaming. La comunicación se establece sobre el protocolo de transporte TCP, lo que garantiza la entrega confiable y ordenada de los paquetes. En los encabezados se distinguen las direcciones IP de origen y destino, junto con los puertos utilizados para mantener la sesión activa. En la capa de aplicación, RTMP organiza los mensajes en fragmentos que se envían de forma continua a través de la conexión TCP.

8.7 Análisis del protocolo RTMP

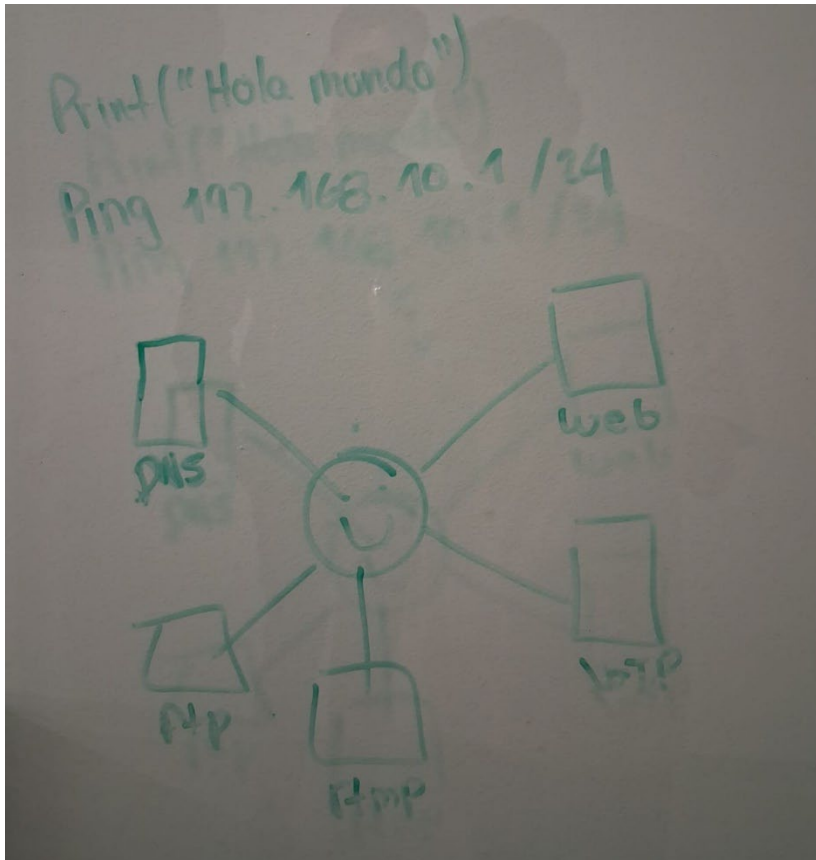
TCP

TCP						
Protocolo	TCP					
	No.	Time	Source	Destination	Protocol	Length Info
	7024	15.405199	192.168.160.54	192.168.160.166	TCP	1514 [TCP Retransmission] 1935 → 60616 [ACK] Seq=2920590 Ack=17 Win=572 Len=1460
Información de la capa de						

aplicación	<ul style="list-style-type: none"> ▼ Transmission Control Protocol, Src Port: 1935, Dst Port: 60616, Seq: 2920590, Ack: 17, Len: 1460 <ul style="list-style-type: none"> Source Port: 1935 Destination Port: 60616 [Stream index: 10] [Stream Packet Number: 6958] > [Conversation completeness: Incomplete (12)] [TCP Segment Len: 1460] Sequence Number: 2920590 (relative sequence number) Sequence Number (raw): 901663263 [Next Sequence Number: 2922050 (relative sequence number)] Acknowledgment Number: 17 (relative ack number) Acknowledgment number (raw): 1753205443 0101 = Header Length: 20 bytes (5) > Flags: 0x010 (ACK) Window: 572 [Calculated window size: 572] [Window size scaling factor: -1 (unknown)] Checksum: 0xfd5d [unverified] [Checksum Status: Unverified] Urgent Pointer: 0 ▼ [Timestamps] <ul style="list-style-type: none"> [Time since first frame in this TCP stream: 8.805040000 seconds] [Time since previous frame in this TCP stream: 0.000001000 seconds] ▼ [SEQ/ACK analysis] <ul style="list-style-type: none"> [Bytes in flight: 1460] [Bytes sent since last PSH flag: 2920] > [TCP Analysis Flags] TCP payload (1460 bytes) Retransmitted TCP segment data (1460 bytes)
Puertos	1935, 60616

En las imágenes se observa que el protocolo RTMP se transporta sobre TCP, destacándose los puertos involucrados en la comunicación, como el 1935 (puerto estándar utilizado por RTMP) y un puerto efímero asignado por el cliente, en este caso 60616. Esta relación refleja el modelo cliente-servidor: el servidor escucha en el puerto 1935 para recibir las conexiones entrantes, mientras que el cliente emplea un puerto dinámico para iniciar y mantener la sesión. El uso de TCP asegura que los fragmentos de audio, video y metadatos transmitidos por RTMP lleguen de forma ordenada, íntegra y sin pérdidas, lo cual es esencial para la reproducción en tiempo real

Topología de red:



En este laboratorio, las máquinas virtuales fueron configuradas en modo Bridge, lo que significa que cada VM se comporta como un dispositivo independiente dentro de la red local. Todas ellas obtienen direcciones IP del mismo rango que el host físico (por ejemplo 192.168.10.51), permitiendo la comunicación directa sin necesidad de traducción de direcciones.

La topología de red fue explicada en clase por el monitor, quien realizó un esquema en el tablero para ilustrar la conexión entre los diferentes servicios. En dicho esquema, cada servidor está conectado a un nodo central que representa el switch o punto de interconexión de la red, formando así una topología en estrella.

En esta configuración se desplegaron servidores con diferentes roles: DNS, FTP, HTTP (Web) y SMTP, lo que permite simular un entorno de red completo. Gracias al modo Bridge, todas las máquinas virtuales pueden comunicarse entre sí y con el host físico de manera transparente.