

The background is a dark blue gradient with a subtle pattern of white dots. Overlaid on the left side are several concentric circles and a large arc with a scale. The scale has numbers from 140 to 260 in increments of 10, with smaller tick marks between them. There are also several smaller circles and arcs, some with arrows indicating a clockwise direction.

# CAPITULO 13

UTILIZAR EL SISTEMA EXPERTO DE WIRESHARK

La información experta de Wireshark se define en los dissectores. Por ejemplo, la información del experto de TCP es mantenido en el archivo packet-tcp.c.

La información de expertos se clasifica en una de cuatro categorías:

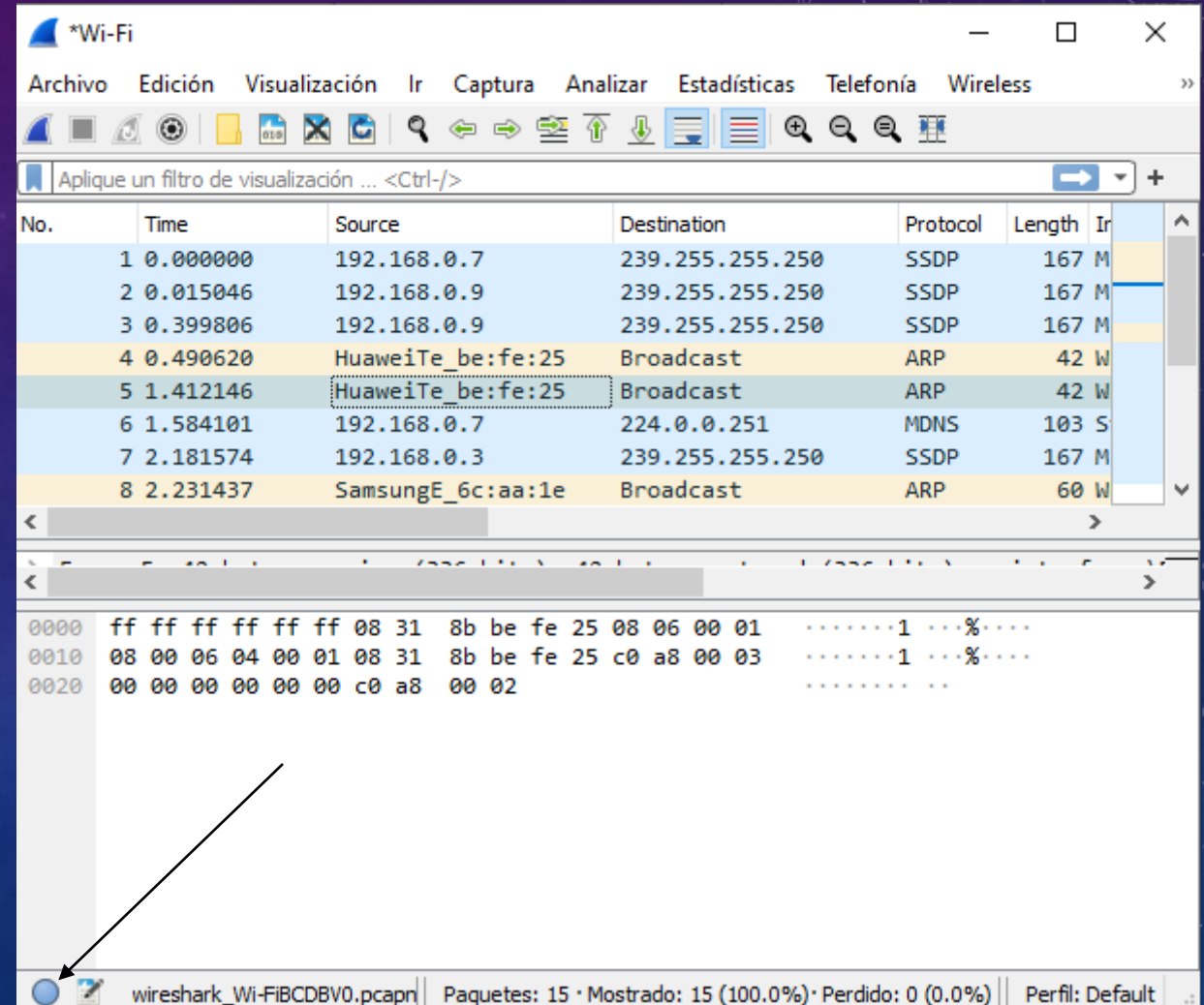
- Errores: errores de paquete o disector
- Advertencias: respuestas inusuales de la aplicación / transporte
- Notas: Respuestas inusuales de la aplicación / transporte (puede ser un proceso de recuperación de una Advertencia)
- Chats: información sobre el flujo de trabajo

Cada categoría está representada en una pestaña diferente en la ventana Información de expertos.

# INICIE LA INFORMACIÓN DE EXPERTOS RÁPIDAMENTE

El botón de información del experto está codificado por colores según el nivel más alto de la clasificación de la información de expertos enumerada.

- Errores: rojo
- Advertencias: amarillo
- Nota: cian (azul claro)
- Chats: Azul
- Comentarios: Verde
- Ninguno: gris





Gravedad	Resumen	Grupo	Protocolo	Recuento
> Warning	Failed to create decryption context: Secrets are not available	Decryption	QUIC	2
> Warning	Connection reset (RST)	Sequence	TCP	1
> Warning	DNS response retransmission. Original response in frame 84	Protocol	mDNS	15
> Warning	DNS query retransmission. Original request in frame 74	Protocol	mDNS	6
> Warning	D-SACK Sequence	Sequence	TCP	25
> Note	Duplicate ACK (#1)	Sequence	TCP	1
> Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	1
> Note	This frame is a (suspected) retransmission	Sequence	TCP	1
> Note	ACK to a TCP keep-alive segment	Sequence	TCP	16
> Note	TCP keep-alive segment	Sequence	TCP	16
> Chat	M-SEARCH * HTTP/1.1\r\n	Sequence	SSDP	167

No hay conjunto de filtro de visualización.

☐ Limitar filtro de visualización

☒ Agrupar por resumen

Buscar:

Mostrar...

Cerrar

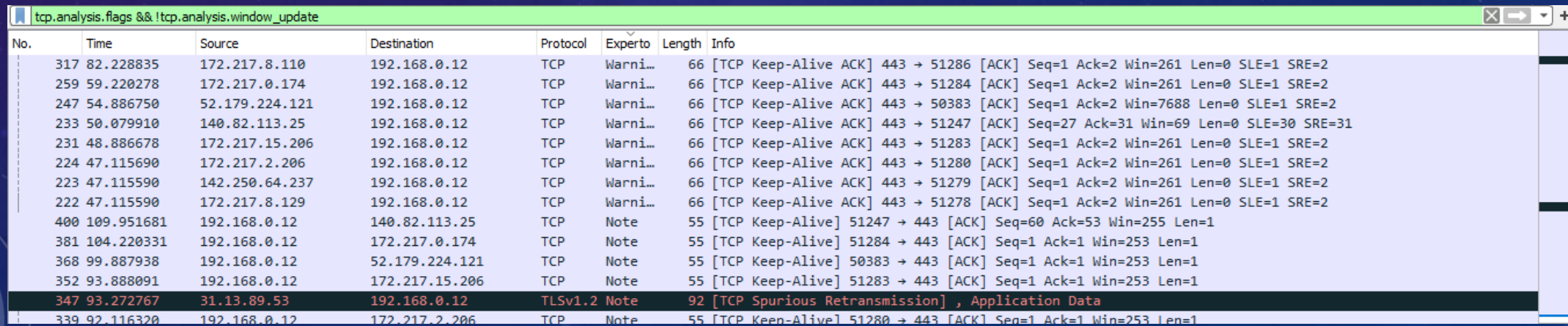
Ayuda



Gravedad	Resumen	Grupo	Protocolo	Recuento
Warning	Failed to create decryption context: Secrets are not available	Decryption	QUIC	2
149	Handshake, SCID=66d8fe0c22712502	Decryption	QUIC	
151	Protected Payload (KP0), DCID=66d8fe0c22712502	Decryption	QUIC	
Warning	Connection reset (RST)	Sequence	TCP	1
141	443 → 51274 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	Sequence	TCP	
Warning	DNS response retransmission. Original response in frame 84	Protocol	mDNS	15
Warning	DNS query retransmission. Original request in frame 74	Protocol	mDNS	6
Warning	D-SACK Sequence	Sequence	TCP	25
Note	Duplicate ACK (#1)	Sequence	TCP	1
Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	1
Note	This frame is a (suspected) retransmission	Sequence	TCP	1
Note	ACK to a TCP keep-alive segment	Sequence	TCP	16
222	[TCP Keep-Alive ACK] 443 → 51278 [ACK] Seq=1 Ack=2 Wi...	Sequence	TCP	
223	[TCP Keep-Alive ACK] 443 → 51279 [ACK] Seq=1 Ack=2 Wi...	Sequence	TCP	
224	[TCP Keep-Alive ACK] 443 → 51280 [ACK] Seq=1 Ack=2 Wi...	Sequence	TCP	
231	[TCP Keep-Alive ACK] 443 → 51283 [ACK] Seq=1 Ack=2 Wi...	Sequence	TCP	
233	[TCP Keep-Alive ACK] 443 → 51247 [ACK] Seq=27 Ack=31 ...	Sequence	TCP	
247	[TCP Keep-Alive ACK] 443 → 50383 [ACK] Seq=1 Ack=2 Wi...	Sequence	TCP	
259	[TCP Keep-Alive ACK] 443 → 51284 [ACK] Seq=1 Ack=2 Wi...	Sequence	TCP	
317	[TCP Keep-Alive ACK] 443 → 51286 [ACK] Seq=1 Ack=2 Wi...	Sequence	TCP	
336	[TCP Keep-Alive ACK] 443 → 51277 [ACK] Seq=1 Ack=2 Wi...	Sequence	TCP	
340	[TCP Keep-Alive ACK] 443 → 51278 [ACK] Seq=1 Ack=2 Wi...	Sequence	TCP	
341	[TCP Keep-Alive ACK] 443 → 51279 [ACK] Seq=1 Ack=2 Wi...	Sequence	TCP	
342	[TCP Keep-Alive ACK] 443 → 51280 [ACK] Seq=1 Ack=2 Wi...	Sequence	TCP	
354	[TCP Keep-Alive ACK] 443 → 51283 [ACK] Seq=1 Ack=2 Wi...	Sequence	TCP	
369	[TCP Keep-Alive ACK] 443 → 50383 [ACK] Seq=1 Ack=2 Wi...	Sequence	TCP	
383	[TCP Keep-Alive ACK] 443 → 51284 [ACK] Seq=1 Ack=2 Wi...	Sequence	TCP	
401	[TCP Keep-Alive ACK] 443 → 51247 [ACK] Seq=53 Ack=61 ...	Sequence	TCP	
Note	TCP keep-alive segment	Sequence	TCP	16
Chat	M-SEARCH * HTTP/1.1\r\n	Sequence	SSDP	167

# UTILIZAR EL BOTON DE FILTRO DE EXPRESION

- Botón de expresión de filtro TCP para localizar los problemas de red más comunes relacionados con TCP.
- Puede crear un filtro de visualización para examinar los paquetes que cumplen con un nivel de gravedad de información experto específico. El seguimiento proporciona ejemplos de los cuatro filtros de nivel de gravedad ("Detalles" y "Comentarios de paquetes" no se consideran un niveles de gravedad):
  - `expert.severity==error`
  - `expert.severity==warn`
  - `expert.severity==note`
  - `expert.severity==chat`



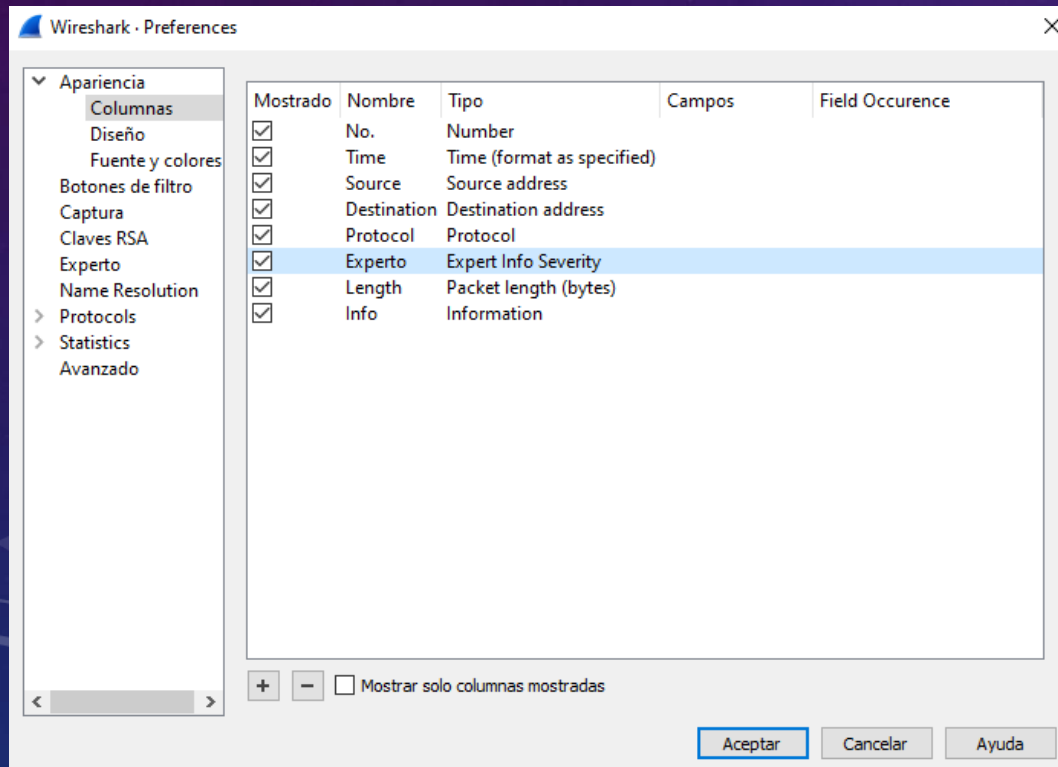
No.	Time	Source	Destination	Protocol	Experto	Length	Info
317	82.228835	172.217.8.110	192.168.0.12	TCP	Warni...	66	[TCP Keep-Alive ACK] 443 → 51286 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2
259	59.220278	172.217.0.174	192.168.0.12	TCP	Warni...	66	[TCP Keep-Alive ACK] 443 → 51284 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2
247	54.886750	52.179.224.121	192.168.0.12	TCP	Warni...	66	[TCP Keep-Alive ACK] 443 → 50383 [ACK] Seq=1 Ack=2 Win=7688 Len=0 SLE=1 SRE=2
233	50.079910	140.82.113.25	192.168.0.12	TCP	Warni...	66	[TCP Keep-Alive ACK] 443 → 51247 [ACK] Seq=27 Ack=31 Win=69 Len=0 SLE=30 SRE=31
231	48.886678	172.217.15.206	192.168.0.12	TCP	Warni...	66	[TCP Keep-Alive ACK] 443 → 51283 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2
224	47.115690	172.217.2.206	192.168.0.12	TCP	Warni...	66	[TCP Keep-Alive ACK] 443 → 51280 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2
223	47.115590	142.250.64.237	192.168.0.12	TCP	Warni...	66	[TCP Keep-Alive ACK] 443 → 51279 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2
222	47.115590	172.217.8.129	192.168.0.12	TCP	Warni...	66	[TCP Keep-Alive ACK] 443 → 51278 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2
400	109.951681	192.168.0.12	140.82.113.25	TCP	Note	55	[TCP Keep-Alive] 51247 → 443 [ACK] Seq=60 Ack=53 Win=255 Len=1
381	104.220331	192.168.0.12	172.217.0.174	TCP	Note	55	[TCP Keep-Alive] 51284 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1
368	99.887938	192.168.0.12	52.179.224.121	TCP	Note	55	[TCP Keep-Alive] 50383 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1
352	93.888091	192.168.0.12	172.217.15.206	TCP	Note	55	[TCP Keep-Alive] 51283 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1
347	93.272767	31.13.89.53	192.168.0.12	TLSv1.2	Note	92	[TCP Spurious Retransmission] , Application Data
339	92.116320	192.168.0.12	172.217.2.206	TCP	Note	55	[TCP Keep-Alive] 51280 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1

# COMPRENDER LA INFORMACIÓN EXPERTA DE TCP

- El archivo del disector de TCP, `packet-tcp.c`, enumera la información de experto de TCP al principio del archivo y el detalles de cada notificación de información de expertos más adelante en el archivo
- El sistema experto puede acelerar el proceso de localización de problemas potenciales en un archivo de seguimiento. El seguimiento
- La sección proporciona una definición de las quince notificaciones de TCP Expert definidas en el archivo `packet-tcp.c`.

# AGREGAR COLUMNA

Se encuentra disponible una columna opcional de lista de paquetes de "Severidad de información experta" que muestra la gravedad más significativa de un paquete o permanece vacía si todo parece estar bien.



Protocol	Experto	Length	Info
SSDP	Chat	325	NOTIFY
MDNS		103	Standard
SSDP	Chat	167	M-SEARCH
MDNS	Warni...	123	Standard
SSDP	Chat	167	M-SEARCH
TLSv1.2	Note	92	[TCP S
SSDP	Chat	167	M-SEARCH
TCP	Warni...	66	[TCP K
TCP	Note	55	[TCP K
TCP		54	51252
TCP		54	50336
TCP		54	51252
MDNS		119	Standard
QUIC		1392	Initial