Convertir un rastro de sabueso en un archivo MPEG (vídeo) visible con VLC

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Antecedentes Problema: Convertir un rastro de sabueso a MPEG y verlo con VLC Solución Convertir los paquetes en MPEG Convertir el seguimiento MPEG en un archivo de vídeo visible ¿Cómo se abre un vídeo MPEG con Wireshark?

Introducción

Este documento describe cómo convertir un rastro de sabueso que contiene tráfico MPEG en un video que puede ver con VLC.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Wireshark
- MPEG
- VLC

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La captura de paquetes en este caso específico se ha tomado entre un cBR8 y RPHY, y se ha convertido en una transmisión de video visible con VLC.

El objetivo es no solo disfrutar viendo videos por razones profesionales en el lugar de trabajo, sino también presenciar problemas de calidad en la transmisión de videos como pixellization (macroblocking o tiling).

Problema: Convertir un rastro de sabueso a MPEG y verlo con VLC

Es posible que Wireshark no reconozca automáticamente el tráfico como tráfico MPEG, por ejemplo, si se tomara en un enlace entre un sistema de terminación de cablemódem (CMTS) y un dispositivo PHY remoto (RPD), podría decodificar el tráfico como UEPI en su lugar:

• • •			📑 Sho	rt_mpeg.pcap		
🧉 🔳 🙋 💿	📄 🗋 🕅	👟 🌪 🖸	曾 承 土 🗔 🎼	j Q Q Q j	*	
Apply a display filter			- During - Du			Expression +
No.	Time	Source	Destination	Protocol	Length Info	
	1 0.000000	10.243.192.82	10.243.192.78	UEPI	1358 UEPI-DIAG	
	2 0.009388	10.243.192.82	10.243.192.78	UEPI	1358 UEPI-DIAG	
	3 0.047005	10.243.192.82	10.243.192.78	UEPI	1358 UEPI-DIAG	
	4 0.047022	10.243.192.82	10.243.192.78	UEPI	1358 UEPI-DIAG	
	5 0.077748	10.243.192.82	10.243.192.78	UEPI	1358 UEPI-DIAG	
	6 0.077890	10.243.192.82	10.243.192.78	UEPI	1358 UEPI-DIAG	
	7 0.082369	10.243.192.82	10.243.192.78	UEPI	1358 UEPI-DIAG	
	8 0.086907	10.243.192.82	10.243.192.78	UEPI	1358 UEPI-DIAG	
	9 0.091919	10.243.192.82	10.243.192.78	UEPI	1358 UEPI-DIAG	
	10 0.094112	10.243.192.82	10.243.192.78	UEPI	1358 UEPI-DIAG	
. France 1, 1350 h.	11 0.09R878	18.743.197.87	18.243.192.78	HEPT	1358 UEPT-DTAG	
Frane 1: 1358 0	ytes on wire (ier	504 DIts/, 1338 Dytes	Captured (10864 DIts)		(2)	
Ethernet II, Sro	c: Ciscoinc_ii:st	0:13 (/0:00:19:11:30:1	10 242 102 70	2112 (0012/1901031021	(2)	
Internet Protoco	ot version 4, 5re	c: 10.243.192.82, DSt:	10.243.192.70			
P Far neaver						
0000 00 27 90 0a	d2 f2 78 ba f9	11 36 13 88 88 45 88	.'x6E.			
0010 05 40 00 00	40 00 fd 73 e1	43 0a f3 c0 52 0a f3	.@@s .CR			
0020 c0 4e 00 13	00 00 40 00 2c	ea 47 1f ff 10 0d cf	.N@G			
0030 3c c9 8e ac	5f e0 74 22 4a	b4 a7 38 94 91 12 30	<t" j80<="" td=""><td></td><td></td><td></td></t">			
0040 C3 36 T1 53 0050 79 92 1d 58	a0 11 80 00 05	40 58 C7 60 66 10 9e 69 4e 71 29 3f e4 61	V. X. D. (No)2.a			
0050 86 6d e2 a7	48 3f 17 bb 6a	96 b1 8e d6 c8 37 3c	.m0? 17<			
0070 f3 24 3a b1	7f 81 d0 89 2a	d2 9c e2 52 7e c8 c3	.\$1 *R~			
0000 @c db c5 4e	80 7e 2f 76 d5	2d 63 1d ad 81 6e 79	N.~/vcny			
0090 c6 48 75 62	ff 03 a1 12 55	a5 39 c4 a4 fd 91 86	.Hub U.9			
00a0 19 b7 8a 9d	00 fc Se ed aa	5a c6 3b 5b 82 dc f3				
0000 CC 90 68 C5	81 f8 bd db 54	4a 73 89 49 1a 23 6C b5 8c 76 b6 85 b9 e7	30 T			
00d0 99 21 d5 8b	fc 0e 84 49 56	94 c7 12 93 f5 46 18	.!I VF.			
00e0 66 de 2a 74	03 f1 47 1f ff	10 e7 9e 64 87 56 2f	f.*tGd.V/			
00f0 f0 3a 11 25	5a 53 9c 4a 4f	d6 18 61 9b 78 a9 d0	.:.%25.3 0a.x			
0100 0f c5 ee da	a5 ac 63 b5 b0	29 cf 3c c9 8e ac 5f	·····C· ·).<			
0120 1f 8b dd b5	4b 58 c7 6b 68	ac 30 C3 30 T1 53 80 53 9e 79 92 1d 58 bf				
O Short_mpeg					Packets: 70304 - Displayed: 70304 (100	1.0%) · Load time: 0:3.56 Profile: Default

Solución

Convertir los paquetes en MPEG

Paso 1. Seleccione un paquete UEPI, haga clic con el botón derecho en el **encabezado PSP** en la vista de detalles del paquete y haga clic en **Decodificar como.**

Paso 2. En el menú Actual, elija UDP en la lista de protocolos y haga clic en Aceptar.

Ahora verá los paquetes UDP (Wireshark podría descodificarlos como cualquier otro protocolo UDP, dependiendo del número de puerto, si aún no ve los paquetes MPEG, continúe con el siguiente paso).

Paso 3. Seleccione un paquete UDP, haga clic con el botón derecho en el encabezado del

protocolo y seleccione Decodificar como.

Paso 4. En el menú Actual elija MP2T en la lista de protocolos y haga clic en Aceptar

Después de eso, verá los paquetes MPEG, como se muestra en la imagen:

Short mpeq.pcap							
4 1 2 0		C 9 👄 👄	9 7 4 DU	= Q Q Q T			
Apply a display filte						Expression. +	
No	Time	Source	Destination	Brotocol	Length Info		
190.	15 0.108201	18,243,192,82	10.243.192.78	MPEG TS	1358 [MP2T fragment of a re-	assembled packet]	
	16 0.108540	10,243,192,82	10,243,192,78	MPEG TS	1358 NULL packet		
	17 0,112934	10,243,192,82	10,243,192,78	MPEG TS	1358 NULL packet		
	18 0.115269	10.243.192.82	10.243.192.78	MPEG TS	1358 [MP2T fragment of a re-	assembled packet] Program _	
	19 0.115706	10.243.192.82	10.243.192.78	MPEG TS	1358 NULL packet		
	20 0.116250	10.243.192.82	10.243.192.78	MPEG TS	1358 NULL packet		
	21 0.117028	10.243.192.82	10.243.192.78	MPEG TS	1358 NULL packet		
	22 0.117624	10.243.192.82	10.243.192.78	MPEG TS	1358 [MP2T fragment of a re-	assembled packet]	
	23 0.119800	10.243.192.82	10.243.192.78	MPEG TS	1358 NULL packet		
	24 0.120631	10.243.192.82	10.243.192.78	MPEG TS	1358 NULL packet		
	25 A.121268	18.243.192.82	18.243.192.78	MPEG TS	1358 NILL packet		
> User Datagram I	Protocol, Src Por	t: 19 (19), Dst Port:	0 (0)				
v ISO/IEC 13818-	1 PID=0×1fff CC=0						
⊨ Header: 0x47	71fff10						
V ISO/IEC 13818-3	1 PID=0x1fff CC=0						
⊨ Header: 0x47	71fff10						
TSO/IEC 13818-3	1 PID=0x1fff CC=0						
▶ Header: 0x47	71fff10						
ISO/IEC 13818-	1 PID=0×131 CC=6	skips=2					
▶ Header: 0x47013116							
V (MPEG2 PCR A	Analysis]						
> (Expert 1	nto (Error/Mattor	med): Detected 2 missi	ing 15 frames before t	his (last_cc:3 total ski	ps:902 discontinuity:361)]		
[T5 Continuity Counter Skips: 2]							
[Some Trames Gropped: 1]							
Measure Lean 1 and Annual A							
* 150/1EC 13818-1 *10-808 CC=S							
► Incader: Ux4740015							
Introve type Analysis)							
0000 00 27 00 00	42 f2 78 ha f9	11 36 13 88 88 45 88	1. X. 6. F.				
0010 05 40 00 00	0 40 00 fd 73 e1	43 0a f3 c0 52 0a f3	.@@s .CR				
0020 c0 4e 00 13	3 00 00 40 00 30	93 47 1f ff 10 da 01	.N@. 0.G				
0030 6c 57 6d f7	7 4b c9 87 4e 68	cc ec ed eb bd 25 fe	Wm.KN h%.				
0040 93 a8 92 08	8 b4 36 f8 b1 97	33 13 12 14 42 64 82	····.63B				
0050 d8 ae d0 ee	1 68 64 f1 63 2e	99 09 00 07 78 40 T0 66 26 24 28 85 68 85	'04. hm. c . f65(. h.				
0070 b1 5d b7 dd	1 2f 24 1d 39 a3	33 b3 b7 ac f4 97 fa	.1/5.9 .3				
0080 4e a2 48 22	2 d0 db e2 c6 5c	cc 4c 48 51 0b d0 0b	N.H" \.LHQ				
0090 62 bb 6f ba	a 5e 48 3a 73 46	67 67 6f 5d e8 2f f4	b.o.^H:s Fggo]./.				
0000 90 44 90 45	b a1 b7 c5 8c b9	98 98 98 98 az 17 að 16	.D.E				
00c0 3a 89 28 8b	43 6f 8b 19 73	31 31 21 44 2e 48 2d	:Co s11!D.@-				
0.7							
Short_mpeg					Packets: 70304 · Displayed: 70304 (100.0%)	 Load time: 0.2.799 Profile: Default 	

Para decodificar los paquetes correctamente como MPEG, puede ver este video:

Convertir el seguimiento MPEG en un archivo de vídeo visible

Paso 1. Instale el complemento LUA MPEG DUMP Wireshark, disponible aquí: mpeg_dump.lua.

Para los usuarios de MAC OS, puede descargar el complemento denominado **mpeg_packets_dump.lua** en la página enlazada arriba y moverlo en la trayectoria: /Applications/Wireshark.app/Contents/Resources/share/wireshark.

En la misma carpeta, añada la línea <dofile("mpeg_packets_dump.lua")> al final del archivo denominado init.lua.

Paso 2. Ahora debe ver un nuevo elemento en Wireshark, navegue hasta **Herramientas > Volcar** paquetes MPEG TS, como se muestra en la imagen:



Selecciónelo e introduzca un nombre de archivo y, finalmente, un filtro si desea extraer alguna parte de la secuencia solamente (por ejemplo, un PID único, si la secuencia contiene varios).



Esto crea un archivo .ts, que se puede ver con VLC como flujo de vídeo:

Esta imagen muestra el mosaico de vídeo a propósito para mostrar cómo este proceso es realmente útil para encontrar problemas de transmisión de vídeo.

¿Cómo se abre un vídeo MPEG con Wireshark?

Como tema secundario, Wireshark admite cualquier archivo de vídeo MPEG y muestra correctamente los paquetes MPEG (por supuesto, sin encabezados IP, ya que no hay ninguno en el archivo local):

•••	L tovideo.ts						
🏾 🗖 🔍 🔍 🚞 🗋 🗶 🖉 🔍 🗢 🔿 💆	🗿 🛓 🗔 🔲 🍳 ସ୍ ସ୍	11					
Apply a display filter <%/>			Expression +				
No. Time Source De	stination Protocol	Length Info					
6 0.003778518	MPEG TS	188 (MP2T fragment of	a reassembled packet]				
7 0.004534222	MPEG TS	188 (MP2T fragment of	a reassembled packet]				
8 0.005289925	MPEG TS	188 [MP2T fragment of	a reassembled packet]				
9 0.006045629	MPEG TS	188 [MP2T fragment of	a reassembled packet]				
10 0.006801333	MPEG TS	188 [MP2T fragment of	a reassembled packet]				
11 0.007557037	MPEG TS	188 [MP2T fragment of	a reassembled packet]				
12 0.008312740	MPEG TS	188 (MP2T fragment of	a reassembled packet]				
13 0.009068444	MPEG TS	188 (MP2T fragment of	a reassembled packet]				
14 0.009824148	MPEG TS	188 Program Associati	on Table (PAT)				
15 0.010579851	MPEG TS	188 [MP2T fragment of	a reassembled packet]				
16. 0.011335555	MPEG TS	188 IMP2T fragment of	a reassembled nacket]				
Frame 14: 188 bytes on wire (1504 bits), 188 bytes captured	(1504 bits)						
▷ ISO/IEC 13818-1 PID=0x0 CC=4							
w MPEG2 Program Association Table							
Table ID: Program Association Table (PAT) (0x00)							
1 = Syntax indicator: 1							
.011 = Reserved: 0x0003							
0000 0001 0001 = Length: 17							
Transport Stream ID: 0xa8a0							
11 = Reserved: 0x03							
11 101. = Version Number: 0x1d							
1 = Current/Next Indicator: Currently applicable							
Section Number: 0							
Last Section Number: 0							
> Program 0x000s -> PID 0x0130							
> Program 0x000c -> PID 0x01c0							
CRC: Av86ce2a02 [Unverified]							
v Stuffing							
Stuffing: ####################################							
0000 47 40 00 14 00 00 b0 11 a8 a0 fb 00 00 00 0a c1 Gg							
0010 30 00 0e e1 b0 86 ce 7a 92 ff ff ff ff ff ff ff ff							
0020 ff							
aasa fe							
0060 11 11 11 11 11 11 11 11 11 11 11 11 11							
8878 ff							
080 ff							
0000 11 11 11 11 11 11 11 11 11 11 11 11							
0 Z milan		Packets: 402128 - Displayed: 402128 (1	00.0%) - Load time: 0.5.865 Profile: Default				

Esto es extremadamente útil si desea asegurarse de que el archivo de vídeo de origen es correcto. Si el archivo de video de origen contiene errores CC, no hay magia aquí, hay una posibilidad de errores CC todo el camino.

Además, puede ser útil en caso de que sólo pueda recibir el vídeo mediante un dispositivo de seguridad USB DVB-C, que captura paquetes MPEG y permite almacenar la secuencia de vídeo como un archivo. A continuación, puede reabrirlo con Wireshark para asegurarse de que es correcto.