Converter um rastreamento de farejador em arquivo MPEG (Vídeo) visualizável com VLC

Contents

Introduction Prerequisites Requirements Componentes Utilizados Informações de Apoio Problema: Converta um rastreamento de farejador em MPEG e visualize-o com VLC Solução Converter os pacotes em MPEG Converta o rastreamento MPEG em um arquivo de vídeo visualizável Como abrir gualguer vídeo MPEG com o Wireshark?

Introduction

Este documento descreve como converter um rastreamento de farejador contendo tráfego MPEG em um vídeo que você pode assistir com VLC.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Wireshark
- MPEG
- VLC

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A captura de pacotes neste caso específico foi realizada entre um cBR8 e RPHY e convertida em um fluxo de vídeo visualizável com VLC.

O objetivo é não apenas assistir vídeos por motivos profissionais no local de trabalho, mas também testemunhar problemas de qualidade no fluxo de vídeo, como pixelização (macrobloqueio ou problemas de temporização).

Problema: Converta um rastreamento de farejador em MPEG e visualize-o com VLC

O Wireshark pode não reconhecer automaticamente o tráfego como tráfego MPEG, por exemplo, se ele foi tomado em um link entre um CMTS (Cable Modem Termination System) e um RPD (Remote PHY Device), ele pode decodificar o tráfego como UEPI em vez disso:

• • •			📮 Short_m	peg.pcap		
🧉 🔳 🧷 💿		🕹 🤉 🔶 🔊	2 ¥ ± 🗔 🗐	0,0,0,	11	
Apply a display filter	<೫/>					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	
	11 0.098878	18.243.192.82	18.243.192.78	HEPT	1358 UEPT-0146	
▶ Frame 1: 1358 byt	es on wire (188	64 Dits), 1358 Dytes (captured (10864 bits)		(2)	
Ethernet II, Srci	C1sc01nc_11136	113 (781ba11911113611	s), DSTI 0012/19010a102112	(6615)1361691051	(12)	
Internet Protocol	version 4, Src	: 10.243.192.82, Dst:	10.243.192.78			
► PSP header						
0000 00 27 90 0a d2	2 f2 78 ba f9 1	11 36 13 88 88 45 88	.'x6E.			
0010 05 40 00 00 40	0 00 fd 73 el 4	43 0a f3 c0 52 0a f3	.@@s .CR			
0020 c0 4e 00 13 00	0 00 40 00 2c o	ea 47 1f ff 10 0d cf	.N@G			
0030 3c c9 0e ac 51	f e8 74 22 4a t	b4 a7 38 94 91 12 30	<t" j80<="" td=""><td></td><td></td><td></td></t">			
0040 C3 36 T1 53 at	0 17 80 00 D5 4	40 58 C/ 60 60 10 9e	.0.5KX.K			
0050 86 6d e2 a7 44	8 3f 17 bb 6a 9	96 b1 8e d6 c8 37 3c	.m@? 1			
0070 13 24 3a b1 71	f 81 d0 89 2a d	d2 9c e2 52 7e c8 c3	.\$1 *R~			
0080 @c db c5 4e 86	0 7e 2f 76 d5 2	2d 63 1d ad 81 6e 79	N.~/vcny			
0090 e6 48 75 62 ft	f 03 a1 12 55 a	a5 39 c4 a4 fd 91 86	.Hub U.9			
00a0 19 b7 8a 9d 00	8 fc 5e ed aa 5	5a c6 3b 5b 02 dc f3	·····^Z.;[
0000 CC 90 68 C5 TC	0 0/ 42 24 ab 4	48 73 89 49 T8 23 8C	30.1 7 4			
00d0 99 21 d5 8b fe	c 8e 84 49 56 9	94 c7 12 93 f5 46 18	.!I VF.			
00e0 66 de 2a 74 0	3 f1 47 1f ff 1	10 e7 9e 64 87 56 2f	f.*tGd.V/			
00f0 f0 3a 11 25 5a	a 53 9c 4a 4f d	d6 18 61 9b 78 a9 d8	.:.%25.3 0a.x			
0100 Of c5 ee da a5	5 ac 63 b5 b0 2	29 cf 3c c9 0e ac 5f	·····C· ·).<			
0110 e0 74 22 4a b4	4 a7 38 94 9f a	ac 30 c3 36 f1 53 a0	.t"J80.6.5.			
0120 11 00 00 05 40	0 30 67 60 68 5	22 46 14 45 10 26 01				
○ 🎢 Short_mpeg					Packets: 70304 - Displayed: 70304 (100.0%)	Load time: 0:3.56 Profile: Default

Solução

Converter os pacotes em MPEG

Etapa 1. Selecione um pacote UEPI, clique com o botão direito do mouse no **cabeçalho PSP** na exibição de detalhes do pacote e clique em **Decodificar como**.

Etapa 2. No menu Atual, escolha UDP na lista de protocolos e clique em OK.

Agora você vê pacotes UDP (o Wireshark pode decodificá-los como qualquer outro protocolo UDP, dependendo do número da porta, se você ainda não vir pacotes MPEG, continue na próxima etapa).

Etapa 3. Selecione um pacote UDP, clique com o botão direito no cabeçalho do protocolo e

selecione Decodificar como.

Etapa 4. No menu Atual, escolha MP2T na lista de protocolos e clique em OK

Depois disso, você verá pacotes MPEG, como mostrado na imagem:

Short_mpeg.pcap							
1 1 0 0		0 9 + +	2 7 4 DU	a a a T			
Apply a display filt	ter <%/>					Expression +	
No.	Time	Source	Destination	Protocol	Length Info		
	15 0.108201	10.243.192.82	10.243.192.78	MPEG TS	1358 [MP2T fragment of a	reassembled 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	reassembled 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	reassembled 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 nacket		
User Datagram	Protocol, Src Port	t: 19 (19), Dst Port:	e (e)				
TSO/IEC 13818- TSO/IEC 13818-	-1 PID=0x1fff CC=0						
⊨ Header: 0x4	71fff10						
# ISO/IEC 13818-	-1 PID=0x1fff CC=0						
⊨ Header: 0x4	71fff10						
TSO/IEC 13818- 150/IEC 13818-	-1 PID=0x1fff CC=0						
▶ Header: 0x4	71fff10						
ISO/IEC 13818-	-1 PID=0x131 CC=6 s	skips=2					
⊨ Header: 0x4	7013116						
V [MPEG2 PCR]	Analysis]						
▷ [Expert]	Info (Error/Malforn	ned): Detected 2 miss:	ing TS frames before th	is (last_cc:3 total ski	ps:902 discontinuity:361)]		
[TS Cont]	inuity Counter Skip	ps: 2]					
[Some frames dropped: 1]							
Reassembled in: 33							
v ISO/IEC 13818-1 PID=0x0 CC=5							
▶ Header: 0x47480015							
[MPEG2 PCR Analysis]							
Pointer: 0							
0000 00 27 90 0	a d2 f2 78 ba f9	11 36 13 88 88 45 88					
0010 03 40 00 0	3 00 00 40 00 30	43 68 13 C0 52 68 13 93 47 1f ff 18 da 81	N				
0030 6c 57 6d f	7 4b c9 87 4e 68	cc ec ed eb bd 25 fe	Wm.KN h				
0040 93 a8 92 0	8 b4 36 f8 b1 97	33 13 12 14 42 b4 02	63B				
0050 d8 ae db e	e 97 92 8e 9c d1	99 d9 db d7 7a 4b fd	2К.				
0050 27 51 24 1 0070 b1 5d b7 d	1 68 6d f1 63 2e	66 26 24 28 85 68 85	'Q\$.hm.c .fas(.h.				
0000 4e a2 48 2	2 d8 db e2 c6 5c	cc 4c 48 51 8b d8 8b	N.H" \.LHO				
0090 62 bb 6f b	a 5e 48 3a 73 46	67 67 6f 5d c8 2f f4	b.o. H:s Fggo]./.				
00a0 9d 44 90 4	5 a1 b7 c5 8c b9	98 98 98 a2 17 a0 16	.D.E				
00b0 c5 76 df 7	4 bc 90 74 e6 8c	ce ce de bb d1 5f e9	.v.tt.				
0000 3a 89 28 8	0 43 67 80 19 73	31 31 21 44 Ze 40 2d	:Co s11:D.@-				
O 7 Short_mpeg					Packets: 70304 - Displayed: 70304 (10	0.0%) · Load time: 0.2.799 Profile: Default	

Para decodificar os pacotes corretamente como MPEG, você pode assistir a este vídeo:

Converta o rastreamento MPEG em um arquivo de vídeo visualizável

Etapa 1. Instale o plugin LUA MPEG DUMP Wireshark, disponível aqui: mpeg_dump.lua.

Para usuários do MAC OS, você pode fazer o download do plug-in chamado mpeg_packets_dump.lua na página vinculada acima e movê-lo no caminho: /Applications/Wireshark.app/Contents/Resources/share/wireshark.

Na mesma pasta, anexe a linha <dofile("mpeg_packets_dump.lua")> no final do arquivo denominado init.lua.

Etapa 2. Agora você deve ver um novo item no Wireshark, navegue para **Ferramentas > Descarregar pacotes TS MPEG**, como mostrado na imagem:



Selecione-o e insira um nome de arquivo, eventualmente um filtro se quiser extrair alguma parte do fluxo somente (por exemplo, um único PID, se o fluxo contiver vários).



Isso cria um arquivo .ts, que pode ser visto com VLC como um fluxo de vídeo:

Essa imagem exibe propositalmente o tiling do vídeo, para mostrar como esse processo é realmente útil para encontrar problemas de fluxo de vídeo.

Como abrir qualquer vídeo MPEG com o Wireshark?

Como tópico secundário, o Wireshark suporta qualquer arquivo de vídeo MPEG e mostra corretamente os pacotes MPEG (claro, sem cabeçalhos de IP, já que não há nenhum em seu arquivo 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 dxddde -> PID dxd1bd							
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				

Isso é extremamente útil se você quiser garantir que o arquivo de vídeo de origem esteja correto. Se o arquivo de vídeo de origem contiver erros CC, nenhuma mágica aqui, há uma possibilidade de erros CC por todo o caminho.

Além disso, pode ser útil caso você só possa receber o vídeo usando um dongle USB DVB-C, que captura pacotes MPEG e permite armazenar o fluxo de vídeo como um arquivo. Você pode reabri-lo com o Wireshark para garantir que ele esteja correto.