Convertir une trace de renifleur en fichier MPEG (vidéo) consultable avec VLC

Contenu

Introduction Conditions préalables Conditions requises Components Used Informations générales Problème : Convertir un Sniffer Trace en MPEG et le visualiser avec VLC Solution Convertir les paquets en MPEG Convertir les paquets en MPEG Convertir le suivi MPEG en fichier vidéo visible Comment ouvrir une vidéo MPEG avec Wireshark ?

Introduction

Ce document décrit comment convertir une trace de renifleur contenant du trafic MPEG en une vidéo que vous pouvez regarder avec VLC.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Wireshark
- MPEG
- VLC

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

La capture de paquets dans ce cas spécifique a été prise entre un cBR8 et RPHY, et convertie en flux vidéo visible avec VLC.

L'objectif est non seulement de profiter de regarder des vidéos pour des raisons professionnelles sur le lieu de travail, mais aussi d'être témoin de problèmes de qualité dans les flux vidéo tels que la pixellisation (problèmes de macroblocage ou de carrelage).

Problème : Convertir un Sniffer Trace en MPEG et le visualiser avec VLC

Wireshark peut ne pas reconnaître automatiquement le trafic en tant que trafic MPEG, par exemple, s'il a été pris sur une liaison entre un système CMTS (Cable Modem Termination System) et un périphérique PHY distant (RPD), il peut décoder le trafic en tant qu'UEPI à la place :

Short_mpeg.pcap							
🧉 📕 🙋 💿) 🗖 🗋 関	🖸 🤉 🗰 🔿	월 🗿 🛓 🛄 🛛	📃 Q Q Q 🤅	Π.		
Apply a display filte	r <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		
. France 1, 1360 b	11 0.09R878	18.243.192.82	18.243.192.78	LIEPT	1358 UEPT-DTAG		
▶ Frame 1: 1358 D	sytes on wire (18	864 Dits), 1358 Dytes	captured (10864 bits)	12.12 100.22.00.0	(2)		
Ethernet II, Sr	ci ciscoinc_iiis	6113 (781bait9111136)	13), DSti 0012/1901031	d2112 (001271901031d2)	(12)		
Internet Protoc	ot version 4, 5r	c: 10.243.192.82, DSC	: 10.243.192.76				
P Far neuvei							
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 0e ac	51 e8 74 22 4a	b4 a7 38 94 91 12 38	<t" j80<="" td=""><td></td><td></td><td></td></t">				
0040 C3 36 T1 53	a0 17 80 00 05	40 58 C7 60 60 10 9e	.0.5KX.K				
0050 79 92 10 30 0050 86 6d e2 a7	48 3f 17 bb 6a	96 b1 8e d6 c8 37 3c					
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 e6 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 5e ed aa	5a c6 3b 5b 82 dc f3	·····^Z.;[
0000 cc 90 ca c5	Te 07 42 24 ab	4a 73 89 49 1a 23 8c	BS .JS.I.#.				
eede 99 21 d5 8b	fc 0e 84 49 56	94 e7 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 d8	.:.%25.3 0a.x				
0100 Of c5 ee da	a5 ac 63 b5 b0	29 cf 3c c9 8e ac 5f	·····C· ·).<				
0110 00 74 22 40	b4 a7 38 94 9f	ac 30 c3 36 f1 53 a0	.t"J80.6.5.				
0120 11 00 00 05	40 30 67 00 68	22 26 12 27 10 28 01					
O 7 Short_mpeg					Packets: 70304 - Displayed: 70304 (10	0.0%) - Load time: 0:3.56 Profile: Default	

Solution

Convertir les paquets en MPEG

Étape 1. Sélectionnez un paquet UEPI, cliquez avec le bouton droit sur l'**en-tête PSP** dans la vue des détails du paquet, puis cliquez sur **Décoder sous.**

Étape 2. Sous menu actuel, sélectionnez UDP dans la liste des protocoles et cliquez sur OK.

Vous voyez maintenant des paquets UDP (Wireshark peut les décoder comme n'importe quel autre protocole UDP, selon le numéro de port, si vous ne voyez toujours pas de paquets MPEG, passez à l'étape suivante).

Étape 3. Sélectionnez un paquet UDP, cliquez avec le bouton droit de la souris sur l'en-tête du

protocole, puis sélectionnez décoder sous.

Étape 4. Sous Current menu, choisissez MP2T dans la liste des protocoles et cliquez sur OK.

Après cela, les paquets MPEG s'affichent, comme le montre l'image :

Short_mpeg.pcap							
4 1 2 0	9 🗖 🗋 🕅	🖸 🤉 🗰 👄	雪子 土口市	🗐 Q Q Q 🎹			
Apply a display fi	ter <%/>		- Internet - Internet			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 R.121268	18.243.192.82	18.243.192.78	MPEG TS	1358 NULL packet		
> User Datagram	Protocol, Src Port	t: 19 (19), Dst Port:	0 (0)				
TSO/IEC 13818	-1 PID=0x1fff CC=0						
▶ Header: 8x4	171fff10						
# ISO/IEC 13818	-1 PID=0x1fff CC=0						
⊨ Header: 8x4	171fff10						
v ISO/IEC 13818	-1 PID=0x1fff CC=0						
▹ Header: 0x4	171fff10						
ISO/IEC 13818	-1 PID=0x131 CC=6 :	skips=2					
⊨ Header: 8x4	47013116						
(MPEG2 PCR)	Analysis]						
⊨ [Expert	Info (Error/Malfor	ned): Detected 2 miss:	ing TS frames before th	is (last_cc:3 total ski	ps:902 discontinuity:361)]		
[TS Cont	inuity Counter Ski	ps: 2]					
[Some fr	ames dropped: 1]						
Reassembled in: 33							
TS0/IEC 13818	-1 PID=@x@ CC=5						
⊨ Header: 8x4	17488815						
[MPEG2 PCR	Analysis]						
Pointer: 0							
0000 00 27 90 0	a d2 f2 78 ba f9	11 36 13 88 88 45 88	.'x6E.				
0010 05 40 00 0	90 40 00 fd 73 e1	43 0a 13 c0 52 0a 13	.@@s .CR				
0030 6c 57 6d	7 4b c9 87 4c 68	cc ec ed eb bd 25 fe	IWE K. N h				
93 a8 92 88 b4 36 f8 b1 97 33 13 12 14 42 b4 42							
0050 d8 ae db e	e 97 92 0e 9c d1	99 d9 db d7 7a 4b fd	zK.				
0050 27 51 24 1	11 68 6d f1 63 2e	66 26 24 28 85 68 85	'Q\$.hm.c .f6\$(.h.				
0070 b1 5d b7 d	10 21 24 10 39 a3	33 D3 D7 ac 14 97 Ta	.]/\$.9 .3				
0000 62 bb 6f	a 5e 48 3a 73 46	67 67 6f 5d c8 2f f4	b.o. His Foool.				
00a0 9d 44 90 4	45 a1 b7 c5 8c b9	98 98 98 a2 17 a8 16	.D.E				
00b0 c5 76 df 7	74 bc 90 74 e6 8c	ce ce de bb d1 5f e9	.v.tt				
00c0 3a 89 20 8	3b 43 6f 8b 19 73	31 31 21 44 2e 40 2d	:Co s11!D.@-				
O 7 Short_mper	2				Packets: 70304 - Displayed: 7030	4 (100.0%) · Load time: 0.2.799 Profile: Default	

Afin de décoder correctement les paquets en MPEG, vous pouvez regarder cette vidéo :

Convertir le suivi MPEG en fichier vidéo visible

Étape 1. Installez le plug-in LUA MPEG DUMP Wireshark, disponible ici : mpeg_dump.lua.

Pour les utilisateurs du système d'exploitation MAC, vous pouvez télécharger le plug-in **mpeg_packets_dump.lua** sur la page ci-dessus, et le déplacer dans le chemin : /**Applications/Wireshark.app/Contents/Resources/share/wireshark.**

Dans le même dossier, ajoutez la ligne <dofile(*« mpeg_packets_dump.lua »*)> à la fin du fichier nommé init.lua.

Étape 2. Vous devez maintenant voir un nouvel élément dans Wireshark, naviguez jusqu'à **Tools > Dump MPEG TS Packets**, comme illustré dans l'image :



Sélectionnez-le et entrez un nom de fichier, éventuellement un filtre si vous voulez extraire une partie du flux uniquement (par exemple un PID unique, si le flux contient plusieurs).



Ceci crée un fichier .ts, qui peut être visualisé avec VLC en tant que flux vidéo :

Cette image affiche intentionnellement le carrelage vidéo, pour montrer comment ce processus est en effet utile pour trouver des problèmes de flux vidéo.

Comment ouvrir une vidéo MPEG avec Wireshark ?

Comme sujet secondaire, Wireshark prend en charge n'importe quel fichier vidéo MPEG et affiche correctement les paquets MPEG (bien sûr, sans en-têtes IP, puisqu'il n'y en a pas dans votre fichier local) :

•••	i tovideo.ts							
📶 🔳 🧷 🔘 🖿 🗋 🕅 🖄 🖉 🤇 🗣 👄 💆 ች 🛓 🛽	ରୁ 🔲 ପ୍ରୁ ପ୍ରୁ 🎹 👘							
Apply a display filter <%/>		Expression +						
No. Time Source Destination	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 8.886845629	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 Association Table (PAT)						
15 0.010579851	MPEG TS	188 [MP2T fragment of a reassembled packet]						
16.0.011225555	MDEG TS	188 [MP2T fragment of a reassembled packet]						
Frame 14: 188 bytes on wire (1504 bits), 188 bytes captured (1504 bit	(\$)							
▷ 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: @xa8a@								
11 = Reserved: 0x03								
11 101. = Version Number: 0x1d								
1 = Current/Next Indicator: Currently applicable								
Section Number: 0								
Last Section Number: 0								
▷ Program 8x8088a -> PID 8x8138								
▶ Program 8x8000c → PID 8x81b8								
CRC: 0x86ce7a92 [Unverified]								
v Stuffing								
Stuffing: ####################################								
0000 47 40 00 14 00 00 b0 11 a8 a0 fb 00 00 00 0a c1 G0								
0010 30 00 0e e1 b0 86 ce 7a 92 ff ff ff ff ff ff ff ffz								
00.50								
0050 ff								
eese ff								
0070 ff								
eese ff								
0050 ff								
0 7 mideo	Pari	ate: 492128 - Displayer: 492128 (100 0%) - Loss time: 0.5 865 Dealer: Default						

Cela est extrêmement utile si vous voulez vous assurer que le fichier vidéo source est correct. Si le fichier vidéo source contient des erreurs CC, pas de magie ici, il y a une possibilité d'erreurs CC tout au long du chemin.

En outre, il peut être utile dans le cas où vous ne pouvez recevoir la vidéo qu'à l'aide d'un dongle USB DVB-C, qui capture les paquets MPEG et permet de stocker le flux vidéo sous forme de fichier. Vous pouvez ensuite le rouvrir avec wireshark pour vous assurer qu'il est correct.