# Converti una traccia di sniffer in file MPEG (video) visualizzabile con VLC

# Sommario

Introduzione Prerequisiti Requisiti Componenti usati Premesse Problema: Convertire una traccia dello sniffer in MPEG e visualizzarla con VLC Soluzione Converti i pacchetti in MPEG Converti traccia MPEG in un file video visualizzabile Come aprire un video MPEG con Wireshark?

# Introduzione

Questo documento descrive come convertire una traccia di sniffer contenente traffico MPEG in un video che può essere guardato con VLC.

# Prerequisiti

#### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Wireshark
- MPEG
- VLC

#### Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

#### Premesse

L'acquisizione del pacchetto in questo caso specifico è stata effettuata tra un cBR8 e un RPHY e convertita in un flusso video visualizzabile con VLC.

L'obiettivo non è solo guardare video per motivi professionali sul posto di lavoro, ma anche assistere a problemi di qualità nello streaming video, come la pixelizzazione (problemi di macroblocco o affiancamento).

# Problema: Convertire una traccia dello sniffer in MPEG e visualizzarla con VLC

Wireshark potrebbe non riconoscere automaticamente il traffico come traffico MPEG, ad esempio, se è stato registrato su un collegamento tra un CMTS (Cable Modem Termination System) e un RPD (Remote PHY Device), potrebbe decodificare il traffico come UEPI:

● ● ● Short_mpeg.pcap							
🖌 📕 🥂 🔘 🔚 🖺 🎗 🌀 🍳 🖛 🔿 🖀 🐺 🖢 🗔 🔲 🍳 🍳 🍳 🎹							
Apply a display filter .	<೫/>		- Description of the			Expression +	
No.	Time	Source	Destination	Protocol	Length Info		
	1 0.000000	10.243.192.82	18.243.192.78	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	18.243.192.78	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	18.243.192.78	UEPI	1358 UEPI-DIAG		
	7 0.082369	10.243.192.82	18.243.192.78	UEPI	1358 UEPI-DIAG		
	8 0.086907	10.243.192.82	18.243.192.78	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	18.743.197.87	18.243.192.78	LIEPT	1358 UEPT-DTAG		
▶ Frame 1: 1358 by	tes on wire (10	864 bits), 1358 bytes	captured (10864 bits)				
▶ Ethernet II, Src	: CiscoInc_11:3	6:13 (78:ba:f9:11:36:1	3), Dst: 00:27:90:0a:d	2:12 (00:27:90:0a:d2:	12)		
Internet Protoco	l Version 4, Sr	c: 10.243.192.82, Dst:	10.243.192.78				
▹ PSP Header							
0000 00 27 90 0a d	12 f2 78 ba f9 18 88 fd 73 e1	11 36 13 08 00 45 80 43 0a f3 c0 52 0a f3	.'x6E.				
0020 c0 4e 00 13 0	10 00 40 00 2c	ea 47 1f ff 10 0d cf	.N@G				
0030 3c c9 8e ac 5	of e8 74 22 4a	b4 a7 38 94 9f f2 38	<t" j80<="" td=""><td></td><td></td><td></td></t">				
0040 c3 36 f1 53 a	18 1f 8b dd b5	4b 58 c7 6b 68 1b 9e	.6.5KX.k'				
0050 79 92 10 58 0	10 3f 17 bb 6a	09 40 /1 29 31 04 01 06 b1 8c d6 c8 37 3c	yx				
0070 f3 24 3a b1 7	f 81 d0 89 2a	d2 9c e2 52 7e c8 c3	\$1 *R~				
0000 @c db c5 4e 8	10 7e 2f 76 d5	2d 63 1d ad 81 6e 79	N.~/vcny				
0090 e6 48 75 62 1	f 03 a1 12 55	a5 39 c4 a4 fd 91 86	.Hub U.9				
00a0 19 b7 8a 9d 0	N0 fc 5e ed aa	5a c6 3b 5b 02 dc f3	·····^Z.;[				
00b0 cc 90 ea c5 f	e 07 42 24 ab	4a 73 89 49 fa 23 8c	05 .Js.I.#.				
8848 99 21 d5 8b f	C Re 84 49 56	94 e7 12 93 f5 46 18	30T VF.				
00e0 66 de 2a 74 6	3 f1 47 1f ff	10 e7 9e 64 87 56 2f	f.*tGd.V/				
00f0 f0 3a 11 25 5	ia 53 9c 4a 4f	d6 18 61 9b 78 a9 d8	.:.%25.3 0a.x				
0100 Of c5 ee da a	5 ac 63 b5 b0	29 cf 3c c9 8e ac 5f	·····C· ·).<				
0110 e0 74 22 4a b	4 a7 38 94 9f	ac 30 c3 36 f1 53 a0	.t"J80.6.5.				
0120 11 00 00 05 4	0 33 67 60 60	22 26 12 22 10 20 01					
O Y Short,mpeg					Packets: 70304 - Displayed: 70304 (10	0.0%) · Load time: 0:3.56 Profile: Default	

#### Soluzione

#### Converti i pacchetti in MPEG

Passaggio 1. Selezionare un pacchetto UEPI, fare clic con il pulsante destro del mouse sull**'intestazione PSP** nella vista dei dettagli del pacchetto, quindi selezionare **Decodifica con nome.** 

Passaggio 2. In Menu corrente, scegliere UDP nell'elenco dei protocolli e fare clic su OK.

A questo punto vengono visualizzati i pacchetti UDP (Wireshark potrebbe decodificarli come qualsiasi altro protocollo UDP, a seconda del numero di porta. Se i pacchetti MPEG non vengono ancora visualizzati, procedere con il passaggio successivo).

Passaggio 3. Selezionare un pacchetto UDP, fare clic con il pulsante destro del mouse sull'intestazione del protocollo e selezionare **Decodifica con nome.** 

Passaggio 4. In Current menu selezionare MP2T nell'elenco dei protocolli e fare clic su OK

Dopodiché, vengono visualizzati i pacchetti MPEG, come mostrato nell'immagine:

● ● ● 📑 Short_mpeg.pcap							
🧉 🔳 🙋 🔇	9 🗖 🗋 🗙	🖸 ୍ ବ୍ 🍝 🍝	🕾 🐔 🛓 🗔 📄	ା ପ୍ର୍ର୍ମୁ			
Apply a display fill	tor <%/>					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 reassemb]	led 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 reassemb]	led 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 reassemb]	led 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		
licer Batancan	25 8.121268 Brotocol Sec Bort	18.743.197.87	18.243.192.78	MPEG TS	1358 NULL nacket		
<ul> <li>TSO/TEC 13818.</li> </ul>	-1 DTD-0x1fff CC-0	: 19 (19), Ost Port:	0 (0)				
<ul> <li>Header: 8x4</li> </ul>	7144418						
- TSO/TEC 12818.	-1 PTD=@v1fff CC=@						
<ul> <li>Header: 8x4</li> </ul>	7111118						
* ISO/IEC 13818-	-1 PID=0x1fff CC=0						
> Header: 8x4	71fff10						
* ISO/IEC 13818-	-1 PID=0x131 CC=6 s	kips=2					
⊨ Header: 8x4	7013116						
(MPEG2 PCR Analysis)							
▶ [Expert ]	Info (Error/Malform	ed): Detected 2 miss	ing TS frames before thi	s (last_cc:3 total sk	ips:982 discontinuity:361)]		
[TS Cont:	inuity Counter Skip	s: 2]	-	-			
[Some fro	ames dropped: 1]						
Reassembled in1 33							
v ISO/IEC 13818-1 PID=0x0 CC=5							
⊨ Header: 8x4	7488815						
[MPEG2 PCR	Analysis]						
Pointer: 0							
0000 00 27 90 0a d2 f2 78 ba f9 11 36 13 08 00 45 80 ·····x6E.							
0010 05 40 00 00 48 00 fd 73 e1 43 0a f3 c0 52 0a f3							
10020 c0 4c 00 13 00 00 40 00 30 93 47 11 f1 10 da 01 .N0.0.G							
0040 93 89 29 80 43 6f 80 19 73 31 21 44 20 40 20							
0050 d8 ae db ee 97 92 0e 9c d1 99 d9 db d7 7a 4b fdzK.							
0060 27 51 24 11 68 6d f1 63 2e 66 26 24 28 85 68 05 'Q\$.hm.c .f6\$(.h.							
0070 b1 5d b7 dd 2f 24 1d 39 a3 33 b3 b7 ae f4 97 fa .]./,5,9.3							
ered ez							
0000 9d 44 90 45 a1 b7 c5 8c b9 98 98 90 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				
00c0 3a 89 20 8	1b 43 6f 8b 19 73	31 31 21 44 2e 40 2d	:Co s11!D.@-				
Short, mpeg Packets: 70304 - Displayed: 70304 (100.0%) - Load time: 0.2.799 Profile: Default							

Per decodificare correttamente i pacchetti come MPEG, è possibile guardare questo video:

#### Converti traccia MPEG in un file video visualizzabile

Passaggio 1. Installare il plug-in LUA MPEG DUMP Wireshark, disponibile qui: mpeg\_dump.lua

Per gli utenti di MAC OS, è possibile scaricare il plugin denominato **mpeg\_packets\_dump.lua** nella pagina del link precedente e spostarlo nel percorso: /Applications/Wireshark.app/Contents/Resources/share/wireshark.

Nella stessa cartella, aggiungere la riga <dofile("mpeg\_packets\_dump.lua")> alla fine del file denominato init.lua.

Passaggio 2. A questo punto, è necessario visualizzare un nuovo elemento in Wireshark. Selezionare **Tools > Dump MPEG TS Packets**, come mostrato nell'immagine:



Selezionarlo e immettere un nome file, eventualmente un filtro se si desidera estrarre solo una parte del flusso (ad esempio un singolo PID, se il flusso contiene più elementi).





L'immagine mostra in modo mirato le porzioni video, per mostrare come questo processo sia effettivamente utile per trovare problemi di streaming video.

### Come aprire un video MPEG con Wireshark?

Come argomento collaterale, Wireshark supporta qualsiasi file video MPEG e mostra correttamente i pacchetti MPEG (ovviamente, senza alcuna intestazione IP, poiché non ne esistono nel file locale):

Acoby a display filter _ <%/>	1 * * 🖾 🔜 🖂 🐴 🖓	• II	Farression. +				
No. No. Reves	Pastination Pastanai	Leasth In	4				
6 8 001770518	Destination Protocol	Longth in	MP3T fragment of a reassembled packet]				
7 8.884534222	MPEG TS	199	MP2T fragment of a reassembled packet]				
9 8 885399935	MDEC TS	100 1	MP2T fragment of a reassembled packet]				
0 0 005045530	MOET TO	100 1	W07F fragment of a reassembled packet]				
10 0 005801333	MOED TO	100 (	MP21 fragment of a reassembled packet]				
11 0 007557037	MDEC TO	100 0	MP21 fragment of a reassembled packet]				
12 0.000/03/03/	MPEG IS	100 1	MP21 fragment of a reassembled packet]				
12 0.000312/40	MPEG IS	188	MP21 fragment of a reassembled packet)				
13 0.009000444	MPEG 15	100	Przi fragment of a reassenbled packet)				
14 0.009024140	MPEG TS	188	Program Association Table (PAT)				
15 0.010579051	MPEG TS	168	MP2T fragment of a reassembled packet]				
Erame 14: 188 butes on vice (1584 hits), 188 butes cant	MPEG TS	199	MP3T fragment of a reassembled nacket!				
> TEO/TEC 13818-1 DTD-8x8 CC-4							
w MDEC2 Program Association Table							
Table TO: Broaran Association Table (DAT) (0x00)							
able for Program Association Table (PAT) (exce)							
att - Bereput August							
.011 = Reserved: 0x00003							
0000 0001 0001 = Length: 1/							
Transport Stream ID: 0xa8a0							
11 = Reserved: 0x03							
11 101. = Version Number: 0x1d							
1 = Current/Next Indicator: Currently applica	ble						
Section Number: 0							
Last Section Number: 0							
▷ Program 8x8888a -> PID 8x8138							
▷ Program 8x888e →> PID 8x81b8							
CRC: 0x86ce7a92 [Unverified]							
v Stuffing							
Stuffing: ////////////////////////////////////							
0000 47 40 00 14 00 00 b0 11 a8 a0 fb 00 00 00 0a e1 G	e						
0010 30 00 0e e1 b0 86 ce 7a 92 ff ff ff ff ff ff ff ff e	ž						
0030 11 11 11 11 11 11 11 11 11 11 11 11 11							
0050 ** ** ** ** ** ** ** ** ** ** ** ** **							
0060 ff							
0070 ff							
0000 ff							
eege ff							
eeae ff							
😑 🍸 tovídeo		Packets: 4921	28 - Displayed: 492128 (100.0%) - Load time: 0.5.865 Profile: Default				

Ciò è estremamente utile se si desidera garantire che il file video di origine sia corretto. Se il file video originale contiene errori CC, non è una magia, c'è la possibilità di errori CC fino in fondo.

Inoltre, può essere utile nel caso in cui si possa ricevere il video solo utilizzando un dongle USB DVB-C, che cattura pacchetti MPEG e consente di memorizzare il video streaming come file. Potete quindi riaprirlo con wireshark per assicurarvi che sia corretto.