# Konvertieren eines Sniffer Trace in eine mit VLC sichtbare MPEG (Video)-Datei

### Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Problem: Konvertieren eines Sniffer Trace in MPEG und Anzeigen mit VLC Lösung Konvertieren der Pakete in MPEG Konvertieren der MPEG-Trace in eine sichtbare Videodatei Öffnen von MPEG-Video mit Wireshark

# Einführung

In diesem Dokument wird beschrieben, wie eine Sniffer-Trace, die MPEG-Datenverkehr enthält, in ein Video konvertiert wird, das Sie mit VLC ansehen können.

### Voraussetzungen

#### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Wireshark
- MPEG
- VLC

#### Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

### Hintergrundinformationen

Die Paketerfassung in diesem speziellen Fall wurde zwischen cBR8 und RPHY durchgeführt und in einen Video-Stream konvertiert, der mit VLC angezeigt werden kann.

Ziel ist es, nicht nur Videos aus beruflichen Gründen anzusehen, sondern auch Qualitätsprobleme im Video-Stream wie Pixellization (Makroblockierung oder Tiling-Probleme) zu beobachten.

# Problem: Konvertieren eines Sniffer Trace in MPEG und Anzeigen mit VLC

Wireshark erkennt den Datenverkehr möglicherweise nicht automatisch als MPEG-Datenverkehr. Wenn er beispielsweise an einer Verbindung zwischen einem Cable Modem Termination System (CMTS) und einem Remote PHY Device (RPD) aufgenommen wurde, kann er den Datenverkehr stattdessen als UEPI decodieren:

Image: Construction       Protocol       Length info         Image: Constrelevel<	
Image: Constraint of the second sec	
No.         Time         Source         Destination         Protocol         Length         Info           1         0.000000         10.243.192.82         10.243.192.78         UEPI         1358         UEPI-0IAG           2         0.009388         10.243.192.82         10.243.192.78         UEPI         1358         UEPI-0IAG           3         0.047005         10.243.192.82         10.243.192.78         UEPI         1358         UEPI-0IAG           4         0.047022         10.243.192.78         UEPI         1358         UEPI-0IAG           5         0.077748         10.243.192.78         UEPI         1358         UEPI-0IAG           6         0.077789         10.243.192.82         10.243.192.78         UEPI         1358         UEPI-0IAG           6         0.077890         10.243.192.82         10.243.192.78         UEPI         1358         UEPI-0IAG           7         0.082369         10.243.192.82         10.243.192.78         UEPI         1358         UEPI-0IAG           7         0.082369         10.243.192.82         10.243.192.78         UEPI         1358         UEPI-0IAG           7         0.082369         10.243.192.02         10.243.192.78         UEPI	n +
1         0.000000         10.243.192.82         10.243.192.78         UEPI         1358         UEPI-DIAG           2         0.000388         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         0.047005         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         0.07789         10.243.192.82         10.243.192.78         UEPI         1358         UEPI-DIAG           7         0.082369         10.243.192.02         10.243.192.78         UEPI         1358         UEPI-DIAG	
2         0.009388         10.243.192.82         10.243.192.78         UEPI         1358         UEPI-DIAG           3         0.047065         10.243.192.82         10.243.192.78         UEPI         1358         UEPI-DIAG           4         0.047022         10.243.192.78         UEPI         1358         UEPI-DIAG           5         0.077748         10.243.192.78         UEPI         1358         UEPI-DIAG           6         0.077890         10.243.192.78         UEPI         1358         UEPI-DIAG           7         0.082369         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	
3       0.047005       10.243.192.02       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         7       0.082369       10.243.192.62       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           7         0.082369         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           7         0.082369         10.243.192.62         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 10.243.192.62 10.243.192.78 UEPI 1358 UEPI-DIAG	
7 0.082369 10.243.192.82 10.243.192.78 UEPI 1358 UEPI-DIAG	
8 A AREAST 10 242 102 02 10 242 102 20 UEDT 1200 UEDT 1200	
6 6.600967 16.243.192.62 16.243.192.76 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 A.AGRR7R 10.243.192.82 10.243.192.78 IIFPT 1358 IIFPT_DTAG	
▶ Frame 1: 1358 bytes on wire (10864 bits), 1358 bytes captured (10864 bits)	
Ethernet II, Src: CiscoInc_11:36:13 (78:ba:f9:11:36:13), Dst: 00:27:90:0a:d2:f2 (00:27:90:0a:d2:f2)	
Internet Protocol Version 4, Src: 10.243.192.82, Dst: 10.243.192.78	
▶ PSP Header	
0000 00 27 90 0a d2 f2 78 ba f9 11 36 13 08 00 45 80 .'x6E.	
0010 05 40 00 04 00 fd 73 e1 43 0a f3 c0 52 0a f3 .0Qs. CR	
0020 c0 4e 00 13 00 00 40 00 2e ea 47 1f ff 10 0d cf .N@G	
0030 3c c9 0e ac 5f e0 74 22 4a b4 a7 38 94 9f f2 30 <, t" J.B0	
0040 C3 30 T1 33 40 17 80 00 D3 40 38 C7 60 60 10 90 0555555 MAK K .	
0000 75 52 40 50 01 00 00 40 50 50 40 71 25 51 04 01 91.0.0.0 100000000000000000000000000	
0070 13 24 3a b1 7f 81 d0 89 2a d2 9c e2 52 7e c8 c3 .51	
0000 @c db c5 4e 80 7e 2f 76 d5 2d 63 1d ad 81 6e 79N.~/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 02 dc f3^Z.;[	
0000 cc 90 ea c5 fe 07 42 24 ab 4a 73 89 49 fa 23 0c85 .Js.I.#.	
00c0 33 0T 15 38 01 78 00 0D 54 05 86 76 00 05 09 07 30 T. V	
0000 00 de 2a 74 03 f1 47 11 ff 10 29 96 40 75 62 ft ft.t. d. V	
00f0 f0 3a 11 25 5a 53 9c 4a 4f d6 18 61 9b 78 a9 d0 425.3 0a.x.	
0100 0f c5 ee da a5 ac 63 b5 b0 29 cf 3c c9 0e ac 5fc).<	
0110 e0 74 22 4a b4 a7 38 94 9f ac 30 c3 36 f1 53 a0 .t"J80.6.5.	
0120 1f 8b dd b5 4b 58 c7 6b 60 53 9e 79 92 1d 58 bfKX.k 'S.yX.	
O 7 Short,mpeg Packets: 70304 - Displayed: 70304 (100.0%) - Load time: 0:3.56 Prof	e: Default

# Lösung

#### Konvertieren der Pakete in MPEG

Schritt 1: Wählen Sie ein UEPI-Paket aus, klicken Sie mit der rechten Maustaste in der Paketdetailansicht auf den **PSP-Header**, und klicken Sie auf **Decode As**.

Schritt 2: Wählen Sie im Menü Aktuell in der Protokollliste die Option UDP aus, und klicken Sie auf OK.

Sie sehen jetzt UDP-Pakete (Wireshark kann es als jedes andere UDP-Protokoll dekodieren, abhängig von der Portnummer, wenn Sie immer noch keine MPEG-Pakete sehen, fahren Sie mit dem nächsten Schritt fort).

Schritt 3: Wählen Sie ein UDP-Paket aus, klicken Sie mit der rechten Maustaste auf den Protokoll-Header, und wählen Sie **Decode As** aus.

Schritt 4: Wählen Sie im aktuellen Menü MP2T in der Protokollliste aus, und klicken Sie auf OK.

Danach werden MPEG-Pakete angezeigt, wie im Bild gezeigt:

• • • A Short_mpeg.pcap								
🛋 🔳 🙇 (	۱ 🗀 📄	🖉 🤉 🔶 🏓	2 7 ± 🗔 🗏	ା ପ୍ର୍ସ୍ 🏾	-			
Apply a display fi	iter <%/>				🖬 - 🗋	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 packs	et]		
	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 packs	at] 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 packs	at]		
	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			
Harry Datasara	25 8.121268	18.243.192.82	18.243.192.78	MPEG TS	1358 NILL packet			
User Datagram TEO/TEC 13919	Protocol, Src Port	: 19 (19), Dst Port:	0 (0)					
+ 150/100 13010	17144410							
- TCO/TEC 13010	-1 DTD-0-1444 CC-0							
+ 150/1EC 15616	17144410							
► Header: UX4/11T12								
<ul> <li>Header: 8x</li> </ul>	47144410							
P INGOUTS WAYATTAY * TSA/TET 13018-1 DTD=04131 (C=6 skins=2								
⊨ Header: 0x	47013116	napa-s						
V [MPEG2 PCR Analysis]								
Expert Info (Error/Malformed): Detected 2 missing TS frames before this (last cc:3 total skips:902 discontinuity:361)]								
ITS Continuity Counter Skips: 2]								
[Some frames dropped: 1]								
Reassembled in 1 33								
v ISO/IEC 13818-1 PID=0x0 CC=5								
▶ Header: 0x47400015								
[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 40 00 fd 73 el	43 0a f3 c0 52 0a f3	.@@s .CR					
0020 C0 40 00	13 00 00 40 00 30 17 Ab c0 87 Ac 68	93 47 11 11 10 0a 01	IN. K N h					
0040 93 a8 92	88 b4 36 f8 b1 97	33 13 12 14 42 b4 82						
0050 d8 ae db	ee 97 92 8e 9c d1	99 d9 db d7 7a 4b fd	zK.					
0060 27 51 24	11 68 6d f1 63 2e	56 26 24 28 85 68 85	'Q\$.hm.c .f&\$(.h.					
0070 b1 5d b7	dd 2f 24 1d 39 a3	33 b3 b7 ac f4 97 fa	.]/\$.9 .3					
0000 4e az 48	22 d0 db e2 c6 5c	CC 4C 48 51 80 88 80	N.H" \.LHQ					
00b0 c5 76 df	74 bc 90 74 e6 8c	ce ce de bb d1 5f e9	.v.tt					
00c0 3a 89 20 1	8b 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								

Um die Pakete korrekt als MPEG zu dekodieren, können Sie dieses Video ansehen:

#### Konvertieren der MPEG-Trace in eine sichtbare Videodatei

Schritt 1: Installieren Sie das LUA MPEG DUMP Wireshark-Plugin, das Sie hier finden: <u>mpeg\_dump.lua.</u>

Für MAC-OS-Benutzer können Sie das Plug-In **mpeg\_packages\_dump.lua** auf der oben verlinkten Seite herunterladen und in den Pfad verschieben: /Applications/Wireshark.app/Contents/Resources/share/wireshark

Fügen Sie im gleichen Ordner die Zeile <dofile("mpeg\_packages\_dump.lua")> am Ende der Datei init.lua an.

Schritt 2: Sie müssen jetzt ein neues Element in Wireshark sehen, und navigieren Sie zu **Extras > Dump MPEG TS Packets**, wie im Bild gezeigt:



Wählen Sie diese Option aus, und geben Sie einen Dateinamen ein, und schließlich einen Filter, wenn Sie nur einen Teil des Streams extrahieren möchten (z. B. eine einzelne PID, wenn der Stream mehrere enthält).

Dadurch wird eine .ts-Datei erstellt, die mit VLC als Video-Stream angezeigt werden kann:



Dieses Bild zeigt absichtlich Videoflimmern, um zu zeigen, wie dieser Prozess tatsächlich nützlich ist, um Probleme mit Video-Streams zu finden.

## Öffnen von MPEG-Video mit Wireshark

Als Nebenthema unterstützt Wireshark jede MPEG-Videodatei und zeigt die MPEG-Pakete korrekt an (natürlich ohne IP-Header, da in Ihrer lokalen Datei keine vorhanden sind):

	🗵 🖃 બંબ બ	16	Formation +					
R Apply a display man Set/2	in the second	Li conte la de	Copressioner 1					
No. Time Source Destination	on Protocol	Length into	third eaches!					
0 0.003//0510	MPEG IS	188 (MP2) fragment of a reasse	moted packet]					
7 0.004334222	HPEG IS	166 (HP21 fragment of a reasse	mbled packet]					
8 0.005289925	MPEG IS	188 (MP21 fragment of a reasse	mbled packet)					
9 0.000045029	MPEG TS	188 (MP21 fragment of a reasse	mbled packet]					
10 0.000001333	MPEG TS	100 [MP21 fragment of a reasse	mbled packet]					
11 0.007557037	MPEG TS	188 (MP2T fragment of a reasse	mbled packet]					
12 0.008312740	MPEG TS	188 [MP2T fragment of a reasse	mbled packet]					
13 0.009068444	MPEG TS	188 [MP2T fragment of a reasse	mbled packet]					
14 0.009824148	MPEG TS	188 Program Association Table	(PAT)					
15 0.010579851	MPEG TS	188 [MP2T fragment of a reasse	mbled packet]					
16. 0.011225555	MPEG TS	188 IMP2T fragment of a reasse	mbled_nacket1					
Frame 14: 100 bytes on wire (1504 bits), 100 bytes captured (15 troated 1500 bytes on wire (1504 bits), 100 bytes captured (15	HO4 DIUS/							
P 150/100 13010-1 Plonexe Conq								
V MPEGZ Program Association Table								
Table 101 Program Association Table (PAT) (0000)								
1 III = 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 0x000a -> PID 0x0130								
▷ Program 8x888e -> PID 8x81b8								
CRC: 0x86ce7a92 [Unverified]								
v Stuffing								
Stuffing: ffffffffffffffffffffffffffffffffffff								
0000 47 40 00 14 00 00 b0 11 a8 a0 fb 00 00 00 0a e1 Gg								
0010 30 00 0e e1 b0 86 ce 7a 92 ff ff ff ff ff ff ff ffz								
0020 ff								
0050 ff								
0050 ff								
0070 ff								
0000 ff								
0000 ff								
coac if								
U tovideo		Packets: 492128 - Displayed: 492128 (100.0%) - Los	ad time: 0.5.865 Profile: Default					

Dies ist besonders nützlich, wenn Sie sicherstellen möchten, dass die Quellvideodatei korrekt ist. Wenn die Quell-Videodatei CC-Fehler enthält, gibt es hier keine Magie, es besteht die Möglichkeit, dass CC-Fehler durchgängig auftreten.

Es kann auch nützlich sein, wenn Sie nur das Video mit einem DVB-C USB Dongle empfangen können, der MPEG-Pakete erfasst und es ermöglicht, den Video-Stream als Datei zu speichern. Sie können es dann mit Wireshark erneut öffnen, um sicherzustellen, dass es korrekt ist.