Convert a Sniffer Trace to MPEG (Video) File Viewable With VLC

Contents

Introduction Prerequisites Requirements Components Used Background Information Problem: Convert a Sniffer Trace to MPEG and View it with VLC Solution Convert the Packets in MPEG Convert the MPEG Trace into a Viewable Video File How to Open Any MPEG Video With Wireshark?

Introduction

This document describes how to convert a sniffer trace containing MPEG traffic into a video that you can watch with VLC.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Wireshark
- MPEG
- VLC

Components Used

This document is not restricted to specific software and hardware versions.

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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The packet capture in this specific case has been taken between a cBR8 and RPHY, and converted into a video stream viewable with VLC.

The goal is to not only enjoy watching videos for professional reasons on the workplace but also witness quality issues in video stream such as pixellization (macroblocking or tiling issues).

Problem: Convert a Sniffer Trace to MPEG and View it with VLC

Wireshark might not automatically recognize the traffic as MPEG traffic, for example, if it was taken on a link between a Cable Modem Termination System (CMTS) and a Remote PHY Device (RPD), it might decode the traffic as UEPI instead:

Short_mpg.pcap					
🖌 📕 🔬 💿 🖿 🛅 🛛	🕺 🖸 🍳 🔶 💌	2 F 1 🗔 🛙	🗐 🔍 🔍 🔍 🎹		
Apply a display filter <3£/>					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 0.04/022 5 0.077740	10.243.192.82	10.243.192.78	UEPT	1358 UEPT-DIAG	
6 0.077890	18,243,192,82	10.243.192.78	UEPT	1358 UEPI-DIAG	
7 0.082369	18,243,192,82	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 0.09R878	18.743.197.87	18.243.192.78	HEPT	1358 UEPT-DIAG	
Frame 1: 1358 bytes on wire	(10864 Dits), 1358 Dytes	captured (10864 bits)			
Ethernet II, Src: Ciscoinc_I.	1136113 (78108119111136)	13), DSti 0012/19010310	2112 (0012/190103102112	,	
P Internet Protocot Version 4, PSD Header	STC: 10.245.192.02, 030	10.243.192.70			
P for neover					
0000 88 27 98 8a d2 12 78 ba	f9 11 36 13 88 88 45 88	.'			
0010 05 40 00 00 40 00 fd 73	el 43 0a f3 c0 52 0a f3	.@@s .CR			
0020 c0 4e 00 13 00 00 40 00	2e ea 47 1f ff 10 0d cf	.N@G			
0030 3c c9 8e ac 5f e8 74 22	4a b4 a7 38 94 91 12 38 b5 4b 58 c7 6b 68 1b 9c	<t" j80<="" td=""><td></td><td></td><td></td></t">			
0050 79 92 1d 58 bf c0 e8 44	95 69 4e 71 29 3f e4 61	yXD .iNg)?.a			
0050 86 6d e2 a7 40 3f 17 bb	6a 96 b1 8e d6 c0 37 3c	.m@? j7<			
0070 13 24 3a b1 7f 81 d0 89	2a d2 9c e2 52 7e c8 c3	.\$1 *R~			
0000 ec do c5 4e 80 /e 21 /6 0000 e6 48 75 62 ff 83 a1 12	05 20 03 10 a0 81 6e 79 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.;[
00b0 cc 90 ea c5 fe 07 42 24	ab 4a 73 89 49 fa 23 0c	B\$.Js.I.#.			
00c0 33 6f 15 3a 01 f8 bd db	54 b5 8c 76 b6 85 b9 e7	30. : TV			
00e0 66 de 2a 74 03 f1 47 1f	ff 18 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 0f c5 ee da a5 ac 63 b5	b0 29 cf 3c c9 0e ac 5f	·····c· ·).<			
0110 d0 74 22 4a b4 a7 38 94 0120 1f 8b dd b5 4b 58 c7 6b	97 ac 30 c3 36 f1 53 a0 60 53 9e 79 92 1d 58 bf				
11 00 00 00 10 10 00 07 00	00 00 PC 70 PE 10 00 01				
O Short_mpeg				Packets: 70304 - Displayed: 70304 (100.0	%) - Load time: 0:3.56 Profile: Default

Solution

Convert the Packets in MPEG

Step 1. Select a UEPI packet, right click on **PSP header** in the packet detail view, and click on **Decode As.**

Step 2. Under Current menu, choose UDP in the protocol list and click OK.

You now see UDP packets (Wireshark might decode it as any other UDP protocol, depending on the port number, if you still don't see MPEG packets, continue to the next step).

Step 3. Select a UDP packet, right click on the protocol header, and select Decode As.

Step 4. Under Current menu choose MP2T in the protocol list and click OK

After that, you see MPEG packets, as shown in the image:

🗧 🗧 📄 📑 Short_mpeg.pcap						
🧉 🔳 🧔 🤅	9 🗖 🗋 🕅	🖸 🤉 🔶 🏓	留子土口旧	🗐 Q Q Q 🎹		
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 reas	sembled 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 reas	isembled 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 reas	sembled 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	
A Marca Basaran	25 8.121268	18.243.192.82	18.243.192.78	MPEG TS	1358 NILL packet	
User Datagram	Protocol, Src Port	t: 19 (19), Dst Port:	0 (0)			
* 150/1EC 13818-	-1 PIDEXITT COM					
► Header: 0x4	1.070-0-1444 00-0					
* 150/1EC 13818-	-1 PID-0xittt CC-0					
F Header: 8x4 - TCO/TEC 12010	1 070-0-1444 00-0					
* 150/1EC 15818-	-1 PIDHOXITTT CCHO					
F neader: ex4	1.070-0-101.00-6	delate 3				
+ Header: Avd	7012116	sutha-s				
v (MPEG2 PCR	Analysis					
h (Expert)	Info (Ecror/Malfor	ned): Detected 2 miss	ion TS frames before th	is (last cos3 total ski	inci 002 discontinuitur 361)]	
ITS Conti	inuity Counter Ski	nedy: betterted 2 mass	ing is manes before in	is (cost_cers totot st.		
Some fro	mes drooped: 11	pp. 41				
Reassembled in	and an oppediat					
- 139/100 1301-1 120-00 00-3						
F INDEL CONTRACTOR						
Pointer: 0						
0000 08 27 98 8	a d2 f2 78 ba f9	11 36 13 88 88 45 88	.'			
0010 05 40 00 0	0 40 00 fd 73 e1	43 0a f3 c0 52 0a f3	.@@s .CR			
0020 c0 4e 00 1	3 00 00 40 00 30	93 47 1f ff 10 da 01	.N@. 0.G			
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 D4 36 18 D1 97	33 13 12 14 42 D4 82 99 d9 db d7 75 45 fd				
0050 27 51 24 1	1 68 6d f1 63 2e	66 26 24 28 85 68 85	'0\$.hm.c .f65(.h.			
0070 b1 5d b7 d	d 2f 24 1d 39 a3	33 b3 b7 ae f4 97 fa	.1/\$.9 .3			
0080 4e a2 48 2	2 d0 db e2 c6 5c	cc 4c 48 51 8b d8 8b	N.H" \.LHQ			
0090 62 bb 6f b	a 5e 48 3a 73 46	67 67 6f 5d e8 2f f4	b.o.^H:s Fggo]./.			
0000 90 44 98 4 0000 c5 76 df 7	a bc 90 74 c6 8c	90 90 90 a2 1/ a0 10 ce ce de bb d1 5f e9	v t t			
00c0 3a 89 20 8	b 43 6f 8b 19 73	31 31 21 44 2e 40 2d	:Co s11!D.@-			
0 7 thus man					Parkets: 70304 - Displayed: 70304 (100 04) -	Load time: 0.2 780 Profile: Default
- and they					carrier search - publisher search (100'0.9) -	Construction of the second of the second

In order to decode the packets correctly as MPEG, you can watch this video:

Convert the MPEG Trace into a Viewable Video File

Step 1. Install the LUA MPEG DUMP Wireshark plugin, available here: mpeg_dump.lua.

For MAC OS users, you can download the plugin named **mpeg_packets_dump.lua** at the abovelinked page, and move it in the path:

/Applications/Wireshark.app/Contents/Resources/share/wireshark.

In the same folder, append the line <dofile("mpeg_packets_dump.lua")> at the end of the file named init.lua.

Step 2. You must now see a new item in Wireshark, navigate to **Tools > Dump MPEG TS Packets**, as shown in the image:

Tools	Help
Dum	p MPEG TS Packets
Lua	►

Select it, and enter a file name, eventually a filter if you want to extract some part of the stream only (for example a single PID, if the stream contains multiple).

This creates a .ts file, which is viewable with VLC as a video stream:



This image purposely displays video tiling, to show how this process is indeed useful to find video stream problems.

How to Open Any MPEG Video With Wireshark?

As a side topic, Wireshark supports any MPEG video file and correctly shows the MPEG packets (of course, without any IP headers, since there isn't any in your local file):

	🖉 🐨 🖉 🖂	deo.ts					
	2 * 🏝 🖃 🔲	aaan					
Apply a display filter < X/>					Expression +		
No. Time Source	Destination	Protocol	Length	info			
6 0.003778518		MPEG TS	188	[MP2T fragment of a reassem	bled packet]		
7 0.004534222		MPEG TS	188	[MP2T fragment of a reassem	bled packet]		
8 0.005289925		MPEG TS	188	[MP2T fragment of a reassem	bled packet]		
9 0.006045629		MPEG TS	188	[MP2T fragment of a reassem	bled packet]		
10 0.006801333		MPEG TS	188	[MP2T fragment of a reassem	bled packet]		
11 0.007557037		MPEG TS	188	[MP2T fragment of a reassem	bled packet]		
12 0.008312740		MPEG TS	188	[MP2T fragment of a reassen	bled packet]		
13 0.009068444		MPEG TS	188	[MP2T fragment of a reassen	bled packet]		
14 0.009824148		MPEG TS	188	Program Association Table	(PAT)		
15 0.010579851		MPEG TS	188	[MP2T fragment of a reassem	bled packet]		
16 A.A11335555		MPEG TS	188	IMPOT fragment of a reassen	bled_packet1		
Frame 14: 188 bytes on wire (1504 bits), 188 bytes cap	tured (1504 bits)						
> 150/IEC 13818-1 PID=0x0 CC=4							
v 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 0x000a -> PID 0x0130							
▷ 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	Gg						
0010 30 00 0e e1 b0 86 ce 7a 92 ff ff ff ff ff ff ff	0z						
00.10							
eese ff							
0060 ff							
0070 ff							
00.0							
0050 ff							
⊘ [™] tavideo			Packets: 492	128 - Displayed: 492128 (100.0%) - Load	time: 0.5.865 Profile: Default		

This is extremely useful if you want to ensure the source video file is correct. If the source video file contains CC errors, no magic here, there is a possibility of CC errors all the way through.

Also, it can be useful in case you can only receive the video using a DVB-C USB dongle, which captures MPEG packets and allows to store the video stream as a file. You can then reopen-it with wireshark to ensure it is correct.