First Encounters with the ProfiTap-1G

Contents

Introduction
Overview
Hardware
Installation7
Talking to the ProfiTap-1G14
Counters
Graphs
Meters
Log
Features
Capture
Live Capture: Capturing and Decoding Using Your Analyzer
Enable Capture Formats and Enable ProfiShark-1G Dissector
Enable Capture Formats and Disable ProfiShark-1G Dissector
Disable Capture Formats and Enable ProfiShark-1G Dissector
Summarize Interactions
My Two Bits
Direct Capture
Link-Local Frames
LACP
Bad Ethernet Frame Check Sequence
Summary

Figure 1: Just Another NIC	3
Figure 2: Dumpcap NIC List	3
Figure 3: Wireshark Start Capture List	4
Figure 4: Wireshark Interface List	4
Figure 5: ProfiTap-1G Capture Format options	5
Figure 6: Focus on ProfiTap-1G	6
Figure 7: Laptop plus ProfiTap-1G	7
Figure 8: Windows Installer	8
Figure 9: Install Visual C++	8
Figure 10: InstallShield Wizard	9
Figure 11: Validating Install	10
Figure 12: Install Network Driver	10
Figure 13: Files in Use	11
Figure 14: Finished	12
Figure 15: Copy the Dissector into Place	13
Figure 16: Counters	14
Figure 17: Graphs	16
Figure 18: Meters	17
Figure 19: Log	18
Figure 20: Features	19
Figure 21: Capture	20
Figure 22: Capture Interfaces	21
Figure 23: Capture Format	21
Figure 24: ProfiShark-1G Dissector	22
Figure 25: ProfiShark-1G Dissector in Action	23
Figure 26: Eight Bytes of Timestamp	23
Figure 27: Correctly dissect Ethernet CRC	24
Figure 28: Incorrectly dissect Ethernet CRC	24
Figure 29: VSS-Monitoring Dissector	25
Figure 30: Don't Do This	26
Figure 31: Capture Parameters vs Dissector Status	27
Figure 32: LACP Hellos	30
Figure 33: Drill Down on Host LACP Frame	31
Figure 34: Drill Down on Switch LACP Frame	32
Figure 35: Bad Frame Check Sequence	34

Introduction

I recently had a chance to try out a ProfiTap-1G, a new packet capture Tap from the ProfiTap folks. Here is a record of my experience. I document this experience using Windows and Wireshark. In addition, this Tap also ships with Linux drivers and support for a range of commercial analyzers (OmniPeek, OptiView, many others).

Overview

The ProfiTap-1G is a hand-held device with two Ethernet ports and one USB port. As with any Tap, we insert it in-line with the Host-of-Interest (where some problem is occurring), and then the Tap forwards all traffic traversing it to our analyzer.

The Tap appears as just another NIC on your computer.



Dumpcap sees it as just another NIC.

Administrator: Cmd	
C:\Temp>dumpcap -D 1. \Device\NPF_{@AB5D447-7604-4493-B9A0-3F7421FDF625 2. \Device\NPF_{C3C70196-8A6C-43C3-9DE8-1D4FE123C54A 3. \Device\NPF_{52E99398-7685-44AE-AD97-E80C38C44D95 4. \Device\NPF_{90CD5F4C-6878-422D-AA27-22B35575B276 on> C:\Temp>	<pre>> (Built-in Ethernet) > (Local Area Connection 3) > (ProfiShark) > (Wireless Network Connecti</pre>

Figure 2: Dumpcap NIC List

Once inside Wireshark, the Tap continues to appear as just another NIC.

WIRESHARK	The World's Most Popular Net Version 1.12.3 (v1.12.3-0-gbb3e9a0 fr
	Capture
Interface List Live list of the capture interface (counts incoming packets) Start	15
Choose one or more interfaces	to capture from, then Start
Local Area Connection 3	
ProfiShark	=
Wireless Network Connection	n 🔫
Start a capture with detailed op	ntions



Wireshark: Capture Interfaces	Appendix, Con-	-	-		
Device	Description	IP	Packets	Packets/s	
🔲 🔊 Built-in Ethernet	Intel(R) 82567LM Gigabit Network Connection	none	73	5	Details
🔲 🔊 Local Area Connection 3	Intel(R) Advanced NetworkiS) NDIS Intermediate Driver	10.0.150.1	59	3	D etails
📝 🝺 ProfiShark	ProfiShark 1G	none	76	3	Details
🔲 🗊 Wireless Network Connection	Microsoft	10.254.0.9	3	0	Details
<u>H</u> elp	<u>Start</u> Stop		<u>O</u> ptions		<u>C</u> lose

Figure 4: Wireshark Interface List

The Tap ships with a supporting application which allows you to configure its in-line functionality.



Figure 5: ProfiTap-1G Capture Format options

- *Enable timestamps* invokes the Tap's on-board clock to deliver timestamps with 8ns resolution.
- *Transmit CRC Errors* instructs the Tap to forward Ethernet frames whose CRC trailers do not correctly summarize the frame's contents.
- *Keep CRC32* instructs the Tap to retain the trailing 4 byte CRC on the Ethernet, as the Tap forwards the frame across its USB port and down to our analyzer.

The Tap itself can capture at line-rate, and its USB 3.0 port can easily accommodate the theoretical Gigabit Ethernet maximum of 2Gb/s (1Gb/s transmit plus 1Gb/s receive). Whether your analyzer can actually swallow 2Gb/s of frames arriving across its USB port depends, of course, on the IO capabilities of your analyzer.

Hardware

Here is what the ProfiTap-1G looks like in action. I am using my laptop not only as the Host-of-Interest but also as the analyzer.



Figure 6: Focus on ProfiTap-1G

USB cable to my laptop



Installation

Installing the software begins with the usual Installer program.

← → Computer → Loca	al Disk (D:) → Install → Network-Toys → ProfiTag	p		- ↓	1
Organize 🔻 🖬 Open 🛛 Burr	New folder			:== :==	,
Pictures	Name	Date modified	Туре	Size	
Videos 🔝 stuart	ProfiShark-1G_1.0.10.exe	2/5/2015 5:22 AM	Application	73,787 KB	

Figure 8: Windows Installer

And the resulting InstallShield Wizard.

ProfiShark	1G - InstallShield Wizard
<mark>ع</mark> ۳	rofiShark 1G requires the following items to be installed on your computer. Click Install b begin installing these requirements.
Status	Requirement
Pending	Microsoft Visual C++ 2012 Redistributable Package (x64)
Pending	Microsoft Visual C++ 2012 Redistributable Package (x86)
	Install Cancel

Figure 9: Install Visual C++

Once that finishes, installation progresses as usual.



Figure 10: InstallShield Wizard

The Installer progresses in the usual way:

🛃 ProfiShar	rk 1G - InstallShield Wizard
Destinati Click Nex	on Folder At to install to this folder, or click Change to install to a different folder.
Ø	Install ProfiShark 1G to: C:\Program Files (x86)\Profitap\ProfiShark 1G\ Change
InstallShield –	
	< Back Next > Cancel

First Encounter with the ProfiTap-1G Stuart Kendrick

🛃 ProfiShar	k 1G - InstallShield Wizard
Installing The prog	ProfiShark 1G gram features you selected are being installed.
17	Please wait while the InstallShield Wizard installs ProfiShark 1G. This may take several minutes.
	Status: Validating install
InstallShield -	
	< Back Next > Cancel

Figure 11: Validating Install



Figure 12: Install Network Driver

If you see one of these File in Use dialogue boxes, I recommend selecting the "Do not close applications. (A reboot will be required.)", as I ran into trouble taking the "Automatically close and attempt to restart applications" approach (I had to re-install the affected applications in order to restore functionality).

ProfiShark 1G - InstallShield Wizard
Files in Use Some files that need to be updated are currently in use.
The following applications are using files that need to be updated by this setup. AVG Firewall AVG User Interface AVG User Interface AVG WatchDog AVGIDSAgent
Automatically dose and attempt to restart applications. Do not dose applications. (A reboot will be required.) InstallShield OK Cancel

Figure 13: Files in Use

ProfiShark 1G - InstallShield	Wizard
	InstallShield Wizard Completed
	The InstallShield Wizard has successfully installed ProfiShark 1G. Click Finish to exit the wizard.
	✓ Launch the program
	< Back Finish Cancel

Figure 14: Finished

At this point, reboot, to allow the install to finish.

Finally, manually copy the ProfiShark-1G dissector *profishark_1g.dll* into your Wireshark plugins folder.

ganize 🔻 Include in library	•	Share with 🔻 🛛 Burn New folder			
鳻 Box Sync 🥣	•	Name	Date modified	Туре	Size
🔓 Contacts		locsis.dll	1/7/2015 12:47 PM	Application extens	209 KB
hesktop		sthercat.dll	1/7/2015 12:48 PM	Application extens	109 KB
Downloads		🥘 gryphon.dll	1/7/2015 12:48 PM	Application extens	72 KB
Pavorites		🚳 irda.dll	1/7/2015 12:48 PM	Application extens	42 KB
InstallAnywhere		🚳 m2m.dll	1/7/2015 12:48 PM	Application extens	19 KB
My Documents		🚳 mate.dll	1/7/2015 12:48 PM	Application extens	87 KB
My Music		🚳 opcua.dll	1/7/2015 12:48 PM	Application extens	182 KB
My Dictures		🚳 profinet.dll	1/7/2015 12:48 PM	Application extens	367 KB
My Videos	_	profishark_1g.dll	8/12/2014 5:47 PM	Application extens	11 KB
Saved Games	=	stats_tree.dll	1/7/2015 12:48 PM	Application extens	12 KB
Searches		unistim.dll	1/7/2015 12:48 PM	Application extens	113 KB
Tracing		🚳 wimax.dll	1/7/2015 12:48 PM	Application extens	505 KB
		🔌 wimaxasncp.dll	1/7/2015 12:48 PM	Application extens	61 KB
Network	-	🚳 wimaxmacphy.dll	1/7/2015 12:48 PM	Application extens	69 KB

Figure 15: Copy the Dissector into Place

Copying *profishark_1g.dll* into place adds the ProfiShark-1G protocol to the Preferences... Protocols... list



We'll come back to the utility of this dissector later. In the meantime, make sure that this box is unchecked; otherwise, Wireshark will attempt to apply it to your traces and will incorrectly dissect many protocols as a result (unless the trace you are analyzing was captured using the ProfiShark-1G; see below for details).

Talking to the ProfiTap-1G

Opening the newly-installed ProfiShark-1G application allows us to talk directly to the Tap.

Counters

The opening screen tabulates basic traffic statistics.

ProfiShark 1G - 1.0.10 Counters Graphs Meters Li	og Features Captur	re						Pause
Counters Controls	Port A				Port B			
Clear All								
Clear A		Total	Rate (/s)	Percentage		Total	Rate (/s)	Percentage
	size < 64 bytes	0	-	0	size < 64 bytes	0	-	0
Clear B	64< size < 1518	884,627	12	100	64< size < 1518	446,233	12	100
	size > 1518 bytes	0	0	0	size > 1518 bytes	0	0	0
	Collisions	0	0	0	Collisions	0	0	0
	CRC Errors	0	0	0	CRC Errors	0	0	0
	Jabbers	1	0	0	Jabbers	0	0	0
	Valid Packets	884,627	12	100	Valid Packets	446,233	12	100
	Invalid Packets	1	0	0	Invalid Packets	0	0	0
	Total Bytes	1,244,309,	3,383	0.01	Total Bytes	29,385,760	996	0

Figure 16: Counters

Recall that because a Tap sits in-line with traffic, it can capture frames which Ethernet NIC drivers generally filter out, like Collisions, CRC Errors, and Jabbers.

Graphs

The next tab allows for semi-real-time display of the statistics visible in the Counters tab.



Figure 17: Graphs

Meters

The third tab uses an automobile dashboard metaphor to display utilization.



Figure 18: Meters

Log

The next tab allows us to record utilization events.

First Encounter with the ProfiTap-1G Stuart Kendrick

17

Created: 2015-02-07 Updated: 2015-02-22

ProfiShark 1G - 1.0.10		- • ×
Counters Graphs Meters	Log Features Capture	Pause
- Log Controls	2/7/2015 11:07:17 AM : Port A Bandwidth usage > 5% ((10.00047%)
Clear Log	2/7/2015 11:07:19 AM : Port A Bandwidth usage > 5% (2/7/2015 11:07:20 AM : Port A Bandwidth usage > 5% ((10.00709%) (10.00121%)
Port A	2/7/2015 11:07:21 AM : Port A Bandwidth usage > 5% (2/7/2015 11:07:22 AM : Port A Bandwidth usage > 5% ((9.822953%)
Bandwidth Usage >	2/7/2015 11:07:26 AM : Port A Bandwidth usage > 5% ((10.0003%)
5.00 🚖	2/7/2015 11:07:28 AM : Port A Bandwidth usage > 5% (2/7/2015 11:07:28 AM : Port A Bandwidth usage > 5% (2/7/2015 11:07:29 AM : Port A Bandwidth usage > 5% ((10.00034%) (10.00117%) (10.00051%)
CRC Error % >	2/7/2015 11:07:30 AM : Port A Bandwidth usage > 5% (2/7/2015 11:07:30 AM : Port A Bandwidth usage > 5% (2/7/2015 11:07:31 AM : Det A Bandwidth usage > 5% ((10.00119%)
1.00 🚖	2/7/2015 11:07:31 AM : Port A Bandwidth usage > 5% (2/7/2015 11:07:32 AM : Port A Bandwidth usage > 5% ((10.00118%)
Port B	2/7/2015 11:07:34 AM : Port A Bandwidth usage > 5% (2/7/2015 11:07:34 AM : Port A Bandwidth usage > 5% (2/7/2015 11:07:34 AM : Port A Bandwidth usage > 5% ((10.00014%) (10.00091%)
Bandwidth Usage >	2/7/2015 11:07:38 AM : Port A Bandwidth usage > 5% (2/7/2015 11:07:39 AM : Port A Bandwidth usage > 5% ((10.00188%) (10.00113%)
5.00	2/7/2015 11:07:41 AM : Port A Bandwidth usage > 5% (2/7/2015 11:07:41 AM : Port A Bandwidth usage > 5% ((10.00036%) (10.00115%)
CRC Error % >	2/7/2015 11:07:42 AM : Port A Bandwidth usage > 5% 2/7/2015 11:07:43 AM : Port A Bandwidth usage > 5%	(10.00123%)
1.00	2/7/2015 11:07:44 AM : Port A Bandwidth usage > 5% 2/7/2015 11:07:45 AM : Port A Bandwidth usage > 5%	(10.01266%) (10.00199%)
	2/7/2015 11:07:50 AM : Port A Bandwidth usage > 5% 2/7/2015 11:07:50 AM : Port A Bandwidth usage > 5%	(10.00149%) (8.647278%)
	2///2015 11:07:52 AM : Port A Bandwidth usage > 5% (2/7/2015 11:07:52 AM : Port A Bandwidth usage > 5% ((9.559908%) (9.559908%)
	2///2015 11:07:53 AM : Port A Bandwidth usage > 5% (2/7/2015 11:07:53 AM : Port A Bandwidth usage > 5% ((9.949832%) (10.00093%)
	2/7/2015 11:07:54 AM : Port A Bandwidth usage > 5% (2/7/2015 11:07:55 AM : Port A Bandwidth usage > 5% ((9.930365%) (9.96991%)
	2///2015 11:07:56 AM : Port A Bandwidth usage > 5% (2/7/2015 11:07:57 AM : Port A Bandwidth usage > 5% ((9.990382%) (10.00186%)
		-

Figure 19: Log

Features

This tab offers a configuration information about the Tap. Notice that here we have access to the Capture Format choices: *Enable timestamps* (8ns resolution), *Transmit CRC Errors*, and retaining the Ethernet CRC trailer (*Keep CRC32*).

🥥 ProfiShark 1G - 1.0.10			
Counters Graphs Meters Log Features	Capture		Pause
ProfiShark 1G Connected Driver Version : 0.1.0.10 SW Firmware Version : 0.1.2.0 HW Firmware Version : 0006 MAC Address : 00:04:a3:a7:2f:16	Link Up 1Gbit Full Duplex Software Dropped Packets : Hardware Dropped Packets : Link Up Duration : Last Link Down Duration :	0 0 1:20:09 3.695s	
Firmware Update			
	Browse	Hash Himware	
Capture Format			
Enable timestamps	Disable Port A		
Transmit CRC Errors	Disable Port B		
Keep CRC32	Packet Slicing	Save	
Span Mode			

Figure 20: Features

Capture

The last tab allows us to use this application's built-in capture capabilities -- this application bypasses much of the Windows networking stack, capturing frames as they flow across the USB port, dropping them into RAM cache, and from their spooling them First Encounter with the ProfiTap-1G 19 Created: 2015-02-07 Stuart Kendrick Updated: 2015-02-22

off to disk. The ProfiShark application can achieve line-rate capture using this technique, and if storage IO is sufficiently fast, can save those frames to storage without drops, even at line-rate.

The GUI offers the usual options for a ring-buffer (Loop), size and number of saved files, plus tweaking the RAM cache.

O ProfiShark 1G - 1.0.10			
Counters Graphs Meters Log	Features Capture	Pause	
Output Capture File :		Browse	
Maximum Capture File Size (MB) :		Start Capture	
Number of files to use :	1 Loop		
Buffer size :		311.00 MB	
	Stop when buffer is full		
Written to File : 0 Bytes			
Dropped : 0 Bytes			
			_)

Figure 21: Capture

Live Capture: Capturing and Decoding Using Your Analyzer

We can use the provided ProfiShark application to capture frames, but we can also use any of a number of 3rd party software packages to perform the capture -- the ProfiTap folks call this *Live Capture* mode. To your favorite software analyzer, the Tap looks like any other NIC; I illustrate this using Wireshark:

4	Wireshark: Capture Interfaces					
	Device	Description	IP	Packets	Packets/s	;
	🔲 😥 Built-in Ethernet	Intel(R) 82567LM Gigabit Network Connection	none	73	5	<u>D</u> etails
	🔲 😥 Local Area Connection 3	Intel(R) Advanced NetworkiS) NDIS Intermediate Driver	10.0.150.1	. 59	3	Details
	🔽 🔊 ProfiShark	ProfiShark 1G	none	76	3	Details
	🔲 🔊 Wireless Network Connection	Microsoft	10.254.0.9	3	0	Details
	<u>H</u> elp	<u>Start</u> Stop		<u>O</u> ptions		<u>C</u> lose

Figure 22: Capture Interfaces

But we must now pay attention to the Capture Format boxes which are checked on the Feature tab

Capture Format								
Enable timestamps								
Iransmit CRC Errors								
Keep CRC32								
Figure 23. Conture Format								
rigure 25. Capture Format								

and how they interact with whether or not the ProfiShark-1G dissector is enabled.

Recall that adding the *profishark_1g.dll* dissector adds a ProfiShark-1G item to the list of protocols visible via Preferences... Protocol...

<u> </u>	Vireshark: Preferences	- Profile: Simple	 -		
	T NEW	•			
	ProfiShark-1G			Enable ProfiShark 1G decoding	
	PRP			Enable Prononante 10 accounty	
	PULSE				
Fig	ure 24: Profis	Shark-1G Dissector			

The interaction between Capture Format and ProfiShark-1G makes sense once we understand how the ProfiTap transmits hardware timestamp information. It does so by encoding the timestamp into eight (8) bytes and appending these eight bytes to the frame, as it transmits the frame across the USB port to the analyzer.

Enable Capture Formats and Enable ProfiShark-1G Dissector

If the ProfiShark-1G dissector is enabled, then Wireshark correctly interprets those eight bytes, using them to populate any Time columns and also displaying the timestamp as a 'protocol' -- notice the ProfiShark-1G 'frame' located in front of the Ethernet II frame.

📕 d	umpca	ap-with-	all-ha	rdware-fe	atures	enable	ed.pca	apng	[Stuart	Kendri	ick]	[Wiresh	ark 1.12.	3 (v1.12	2.3 -0- 9	gbb3e	9a0 fr
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>G</u> o	<u>C</u> apture	<u>A</u> na	lyze	<u>S</u> tatist	tics T	elepho	n <u>y T</u>	ools	<u>I</u> nterna	als <u>H</u> el	р			
0	0	(.	Ø		×	Z	Q	\	🗼 🏟	• 🐨	垫			e e	0	++	¥.
Fi	lter:											-	Expres	sion	Clea	ar	Арр
No.	Tim	e		Bytes	Source	e			Dest	inatio	n					Prot	ocol
	4 0.3	102989	9704	89	10.0	.150	.1		10.	0.0.	1					DNS	5
	5 0.0	000626	5266	89	10.0	.150	.1		10.	0.0.	1					DNS	5
	6 0.	002071	L678	89	10.0	.150	.1		10.	0.0.	1					DNS	5
	7 0.	00463	5930	89	10.0).150	.1		10.	0.0.	1					DNS	5
۰.																	
+ F	rame	7:8	9 byt	tes on	wire	(71	2 bi	ts),	89 b	ytes	caj	ptured	(712	bits) on	inte	erfa
P	rofi	shark	-1G							-							
	Tim	estam	p: Fe	eb 3,	2015	05:	27:4	5.58	72324	10 P	acit	fic St	andar	d Tim	e		

Timestamp: Feb 3, 2015 13:27:45.587232410 UTC

- Internet Protocol Version 4, Src: 10.0.150.1 (10.0.150.1), Dst: 10.0.0.1 (10.
- Domain Name System (query)

Figure 25: ProfiShark-1G Dissector in Action

Here we can see the eight bytes of timestamp appended to the frame:

No.	Time	Bytes Source	Destination	Protocol	Info						
	4 0.102989704	89 10.0.150.1	10.0.0.1	DNS	Standard query	0xbe81	TXT	config.	nos-avg.	cz	
	5 0.000626266	89 10.0.150.1	10.0.0.1	DNS	Standard query	0xbe81	TXT	config.	nos-avg.	cz	
	6 0.002071678	89 10.0.150.1	10.0.0.1	DNS	Standard query	0xbe81	TXT	config.	nos-avg.	cz	
	7 0.004635930	89 10.0.150.1	10.0.0.1	DNS	Standard query	0xbe81	TXT	config.	nos-avg.	cz	
•											
÷F	rame 7: 89 byt	es on wire (712 bits:), 89 bytes captured (712 bits) on interface 0	0	000 d4	8c b	5 21 bf	f9 00 26	5 b9 9f 73 5h	08 00 45 00
- F	ProfiShark-1G				0	010 00	31 2	7 dc 00	00 80 11	. 68 d0 0a 00	0 96 01 0a 00
	Timestamp: Fe	eb 3, 2015 05:27:45.	587232410 Pacific Star	dard Time	0	020 00	00 0	0 00 00	00 06 63	6f 6e 66 69	9 67 07 6e 6f
	Timestamp: Fe	b 3, 2015 13:27:45.	587232410 UTC		Ő	040 73	2d 6	1 76 67	02 63 7a	00 00 10 00	0 01 38 55 76
+ E	Ethernet II, Sr	c: DellInc_9f:73:5b	(00:26:b9:9f:73:5b), E	st: Cisco_21:bf:f9 (d4:8c:b	5:21:bf:f9) 0	050 f6	54 d	0 cc d1	96 54 do	: f4	
+ 1	Internet Protoc	ol Version 4, Src: 1	0.0.150.1 (10.0.150.1)	, Dst: 10.0.0.1 (10.0.0.1)							
÷ι	Jser Datagram F	rotocol, Src Port: 5	0113 (50113), Dst Port	: 53 (53)							
+ [Domain Name Sys	tem (query)									

Figure 26: Eight Bytes of Timestamp

First Encounter with the ProfiTap-1G 23 Stuart Kendrick Created: 2015-02-07 Updated: 2015-02-22 Furthermore, with those eight bytes accounted for, Wireshark's heuristics have a better chance of accurately dissecting the Ethernet CRC, which consists of the four (4) bytes which just prior to the newly-added eight byte timestamp.



Figure 27: Correctly dissect Ethernet CRC

Enable Capture Formats and Disable ProfiShark-1G Dissector

However, if we disable the ProfiShark-1G dissector, then Wireshark interprets that last four bytes of the frame as an Ethernet CRC and then stumbles from there. Notice here that the ProfiShark-1G frame has vanished and that Wireshark incorrectly believes that the last four bytes consist of the Ethernet CRC.

🚄 d	umpca	p-with	-all-ha	ardwar	e-feat	ures-e	nableo	l.pcapn	g [St	tuart	Kend	rick]	[Wire	shark	1.12.3	(v1.1	2.3-0- <u>c</u>	bb3e	9a0 fr	om m	aster-1	.12)]																						
<u>F</u> ile	<u>E</u> dit	Viev	<u> <u>G</u>o</u>	<u>C</u> apt	ure	<u>A</u> naly:	ze <u>S</u> t	atistics	Tel	ephor	n <u>y</u>]	<u>T</u> ools	Inte	rnals	<u>H</u> elp																													
0	0	()	l 🖉			X (2	Q 🔅	•	- 🍛	Ŧ	⊉			Ð	Q		1	X	¥ !	8 %		<u>d</u>																					
Fi	lter:										_			▼ Đ	press	on	Clea	r	Арр	ly	Save	2	Me	2	ΤA	١F	Not	-Junk	тср	Rese	:													
No.	Tim 7 0.0	e 00463	5930	Byt	es S 891	ource 0.0.	150.	1		Desti 10.	inatio 0.0	on .1						Prot DNS	ocol 5		lı S	nfo Stan	ıdard	que	ry ()xbe	81	тхт	conf	ig.	nos-	-avg.	cz	[ЕТНЕ	RNE	TF	RAME	сн	ЕСК	SEQ	UENCE	INC	DRREC	:т]
	8 0.0	00738	5076		89 1	0.0.	150.	1		10.	0.0	.1						DNS	5		5	stan	idar d	que	ery ()xbe	81	TXT	conf	fig.	nos-	-avg.	cz	ETHE]	ERNE	ΤF	RAME	E CH	ECK	SEQ	UENCE	INC	DRREC	T]
1	9 0.0	00001	7464	1	.95 1	$\frac{0.0.}{0.0}$	$\frac{0.1}{0.1}$			10.	0.1	50.1						DNS	5			Stan	idar d	que	ry r	resp	onse		0081		T [[THEF	INET	FRAM		HEC	K SE		NCE	INC				
-	.0 0.1	71195	9207		ד נפ.	0.0.	0.1			10.	0.1	JO. 1						DNa	2			stan	iuai u	que	ну і	esp	UIIS	2 0.0	160T	1.	1 [1	THE		FRAM		HEC	K DE	QUE	NCE	THC	UKKEC	<u>'</u>]		
•										_			1	1																														
+ F - E +	rame ther Des Sou Typ Tra	7:8 net tina rce: e: II iler	39 by 11, 2 10n: Dell 2 (0x 385	rtes cis Inc_ 0800 576f	on w Dell co_2 9f:7) 654d	ire Inc_ 1:bf 3:5b 0ccd	(712 9f:7 :f9 (00 1	bits 3:5b (d4:8 :26:b), 8 (00: :b5):9f	9 by 26:1 5:21 5:73	/tes 99:9 :bf: :5b)	5 cap 9 <mark>f:7</mark> :f9))	otur 3:5b	ed ()), D:	712 st:	oits <mark>Cisc</mark>) on 0_21:	int bf:	erfa f9 (ce 0 d4:8	c:b5	:21:	bf:f	9)	00 00 00 00 00	00 10 20 30 40 50	d4 00 00 73 f6	8c b 3f 2 01 c 00 0 2d 6 54 d	5 21 7 dc 3 c1 0 00 1 76 0 cc	bf 00 00 67 d1	f9 00 35 00 02 96	00 2 80 1 00 2 06 6 63 7 54 d	6 b 1 6 b 7 3 6 a 0 c f	9 9f 8 d0 0 4a 6 6e 0 00	73 0a be 66 10	5b 00 81 69 00	08 96 01 67 01	00 4 01 0 00 0 07 6 38 5	15 0 0a 0 00 0 5e 6 55 7	0 0 1 f 6	.?'. s-avo	& 5.+ c .cz	s[h pJ onfi	E. g.no .8UV
+ I + U + D	Fra nter ser omai	me cl net l Data n Nar	neck Proto gram ne Sy	sequ col Prot stem	ence Vers ocol (qu	: Ox ion , Sr ery)	9654 4, 5 c Po	dcf4 rc: 10 rt: 50	[ind).0.)113	150. (50	2Ct, .1 (0113	, sho (10.(3), [ould).15 Ost	be 0.1) Port	Dxac Ds 53	085f t: 1 (53	3a] 0.0.()).1	(10.	0.0.:	1)																							

Figure 28: Incorrectly dissect Ethernet CRC

First Encounter with the ProfiTap-1G 24 Stuart Kendrick
 0000
 d4
 8c
 b5
 21
 bf
 f9
 00
 26
 b9
 9f
 73
 5b
 08
 00
 45
 00

 0010
 00
 3f
 27
 dc
 00
 08
 11
 68
 d0
 0a
 00
 96
 01
 0a
 00

0020 00 01 c3 c1 00 35 00 2b 70 4a be 81 01 00 00 01

0030 00 00 00 00 00 00 06 63 6f 6e 66 69 67 07 6e 6f

0040 73 2d 61 76 67 02 63 7a 00 00 10 00 01 38 0050 16 54 d0 cc d1 96 54 dc f4 Interestingly enough, if we capture with Hardware Timestamps enabled, Keep CRC32 disabled, but forget to enable the ProfiShark-1G dissector, another dissector, the VSS-Monitoring dissector, will kick in and correctly decode the timestamp, though displaying the result in a different location than the one chosen by the ProfiShark-1G dissector.

🚄 dumpcap-with-timestamps-enabled.pcapng [Stuart Kendrick] [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephony <u>I</u> ools <u>I</u> nternals <u>H</u> elp	
◉ ◉ ∡ ■ ፈ ⊨ 🗎 X 2 < ⇔ ⇔ २ 7 ½ 🗐 🗐 0 < 0 1 1 ₩ ⊠ 🚳 % 🕱 🚽	
Filter: Expression Clear Apply Save Me	TAF Not-Junk TCP Reset
No. Time Bytes Source Destination Protocol	Info
4 0.014853000 535 10.0.0.1 10.0.150.1 DNS	Standard query response 0x4980 SRV 100 10 443 fe-self002.
۲ m	
Frame 4: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface 0 E Ethernet II, Src: cisco_21:bf:f9 (d4:8c:b5:21:bf:f9), D5: DellInc_9f:73:5b (00:26:b9:9f:73:5b) Internet Protocol version 4, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.150.1 (10.0.150.1) U user Datagram Protocol, Src Port: 53 (53), Dst Port: 52444 (52444) Domain Name System (response) VSS-Monitoring ethernet trailer, Timestamp: 04:50:27.428233704 Time Stamp: Feb 3, 2015 04:50:27.428233704 Pacific Standard Time Clock Source: NTP (1)	$ \begin{array}{c c c c c c c c c c c c c c c c c c c $

Figure 29: VSS-Monitoring Dissector

Disable Capture Formats and Enable ProfiShark-1G Dissector

Conversely, if we capture without Hardware Timestamps but leave the ProfiShark-1G dissector enabled, then we also confuse Wireshark: we are telling Wireshark "Interpret the last eight bytes as a nanosecond timestamp" ... when in fact, the last eight bytes of the frame do not contain a timestamp; rather they contain, in the example below, the last eight bytes of a TCP frame.



Figure 30: Don't Do This

Summarize Interactions

I summarize what happens based on various combinations in the following table. Basically, if we enable the Hardware Timestamping feature on the ProfiTap, then we want to analyze that trace with the ProfiShark dissector enabled. Otherwise, we want to make sure that the ProfiShark dissector is disabled. The ProfiShark-1G dissector conceptually has nothing to do with Ethernet CRC dissection, but it does get tangled up in the issue, because Wireshark's heuristics around correctly identifying an Ethernet CRC become confused if the ProfiShark dissector does not kick in.

ProfiShark Capture Parameters	ProfiShark-1G Dissector Status	Result
Timestamps & Keep CRC32 Enabled	Enabled	Accurate Wireshark dissection
Timestamps & Keep CRC32 Enabled	Disabled	Mangled Wireshark dissection
Timestamps Enabled	Enabled	Accurate Wireshark dissection
Timestamps Enabled	Disabled	Mostly accurate Wireshark dissection ¹
KeepCRC32 Enabled	Enabled	Accurate Wireshark dissection
KeepCRC32 Enabled	Disabled	Accurate Wireshark dissection
Timestamps & Keep CRC32 Disabled	Enabled	Mangled Wireshark dissection
Timestamps & Keep CRC32 Disabled	Disabled	Accurate Wireshark dissection

Figure 31: Capture Parameters vs Dissector Status

In other words, checking the *Enable timestamps* box in ProfiShark-1G tells ProfiShark-1G to append a timestamp to the frames it forwards across the USB cable to the virtual ProfiShark-1G NIC, where Wireshark is capturing. ProfiShark-1G does it this way because Wireshark, relying on Winpcap / libpcap, does not record the time when it receives the frame with any particular accuracy -- to take advantage of the Tap's 8ns timestamp resolution, the Tap has to communicate the timestamp using some other mechanism, and the mechanism the ProfiTap folks chose was to modify the forwarded frames themselves, by pasting the timestamp onto the end of the frame. To correctly interpret these appended bytes as a timestamp, Wireshark must invoke a dissector which looks for this timestamp.

My Two Bits

I kept forgetting that I had enabled the ProfiShark-1G dissector and then trying to analyze pcaps captured using some other mechanism, which leads to incorrect dissection. At the moment, I've disabled the ProfiShark-1G dissector and always use Direct Capture mode, see next section.

Direct Capture

The subtleties of the ProfiShark-1G dissector evaporate when we use *Direct Capture* mode, i.e. when we use the Capture tab inside ProfiShark Manager. When we do this, ProfiShark-1G owns the creation of the timestamp, which it inserts into the appropriate

¹ Wireshark incorrectly applies the VSS-Monitoring dissector. This dissector correctly decodes the timestamp as a nanosecond timestamp but inaccurately claims that the time source for the stamp comes from NTP.

First Encounter with the ProfiTap-1G27Created: 2015-02-07Stuart KendrickUpdated: 2015-02-22

location in whichever format you have chosen (.erf, .pcap, or .pcapng being the three file formats which ProfiShark-1G supports). No appended timestamp and thus no need for a dedicated dissector.

Here, I've unchecked the *Enable timestamps* box -- now the frames forwarded across the USB port no longer contain the appended hardware-generated timestamp, though the files created by Direct Capture still retain 8ns resolution timestamps.

Counters Graphs Meters Log Features C	apture
ProfiShark 1G Connected Driver Version : 0.1.0.10 SW Firmware Version : 0.1.2.0 HW Firmware Version : 0006 MAC Address : 00:04:a3:a7:2f:16	Link Up 1Gbit Full Duplex Software Dropped Packets : 0 Hardware Dropped Packets : 0 Link Up Duration : 0:23:28 Last Link Down Duration : 7.839s
Firmware Update	Browse Flash Firmware
Firmware Update	Browse Flash Firmware
Firmware Update Capture Format Finable timestamps	Browse Flash Firmware Disable Port A
Firmware Update Capture Format Enable timestamps Transmit CRC Errors	Browse Flash Firmware Disable Port A Disable Port B

Link-Local Frames

So what does a Tap do for us, as protocol analysts? Well, it allows us to view *link-local* frames, frames which, for example, the SPAN / Port-Mirroring function of an Ethernet switch would not forward to us.

LACP

Here is an example of LACP Hellos being exchanged between a host and a switch:

First Encounter with the ProfiTap-1G Stuart Kendrick 30

Created: 2015-02-07 Updated: 2015-02-22 Focusing on the LACP frame inside Frame #2, transmitted by the host:

```
⊕ Frame 2: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface 0
ProfiShark-1G
Ethernet II, Src: DellInc_9f:73:5b (00:26:b9:9f:73:5b), Dst: slow-Protocols (01:80:c2:00:00:02)
Link Aggregation Control Protocol
   Slow Protocols subtype: LACP (0x01)
   LACP Version Number: 0x01
   Actor Information: 0x01
   Actor Information Length: 0x14
   Actor System Priority: 65535
   Actor System: DellInc_9f:73:5b (00:26:b9:9f:73:5b)
   Actor Key: 17
   Actor Port Priority: 255
   Actor Port: 1
 Actor State: 0x3d (Activity, Aggregation, Synchronization, Collecting, Distributing)
    Reserved: 000000
   Partner Information: 0x02
   Partner Information Length: 0x14
   Partner System Priority: 32768
   Partner System: HewlettP_7d:b7:10 (f0:92:1c:7d:b7:10)
   Partner Key: 10
   Partner Port Priority: 32768
   Partner Port: 5
 B Partner State: 0x3f (Activity, Timeout, Aggregation, Synchronization, Collecting, Distributing)
    Reserved: 000000
   Collector Information: 0x03
   Collector Information Length: 0x10
   Collector Max Delay: 0
    Reserved: 00000000000000000000000000
   Terminator Information: 0x00
   Terminator Length: 0x00
```

Figure 33: Drill Down on Host LACP Frame

And here's the LACP Hello from the switch:

```
    Herame 3: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface 0

Profishark-1G

    ⊞ Ethernet II, Src: HewlettP_7d:b7:15 (f0:92:1c:7d:b7:15), Dst: slow-Protocols (01:80:c2:00:00:02)

Link Aggregation Control Protocol
   Slow Protocols subtype: LACP (0x01)
   LACP Version Number: 0x01
   Actor Information: 0x01
   Actor Information Length: 0x14
   Actor System Priority: 32768
   Actor System: HewlettP_7d:b7:10 (f0:92:1c:7d:b7:10)
   Actor Key: 10
   Actor Port Priority: 32768
   Actor Port: 5
 Actor State: 0x3f (Activity, Timeout, Aggregation, Synchronization, Collecting, Distributing)
   Reserved: 000000
   Partner Information: 0x02
   Partner Information Length: 0x14
   Partner System Priority: 65535
   Partner System: DellInc_9f:73:5b (00:26:b9:9f:73:5b)
   Partner Key: 17
   Partner Port Priority: 255
   Partner Port: 1
 B Partner State: 0x3d (Activity, Aggregation, Synchronization, Collecting, Distributing)
   Reserved: 000000
   Collector Information: 0x03
   Collector Information Length: 0x10
   Collector Max Delay: 0
   Terminator Information: 0x00
   Terminator Length: 0x00
```

Figure 34: Drill Down on Switch LACP Frame

If we were to Port-Mirror port 1 or port 5 on this Ethernet switch, we would not see these LACP frames.

Bad Ethernet Frame Check Sequence

Similarly, frames in which bits have been flipped, in this case due to a bad cable, are normally discarded by the first Ethernet chipset that sees them (perhaps on your switch, perhaps on your analyzer's NIC)², because the originally calculated Ethernet FCS does not match the FCS which the receiving NIC calculates, and modern NICs, by default, discard such frames. The ProfiTap, being specialized hardware, can be instructed to capture them, as seen here. A typical analyzer would not capture Frame 1218 and you the analyst would then be puzzled as to why the new Frame 1218 (1219 in the display below) arrived ~.1487s after the previous one: you would not, a priori, know why the conversation contained such a large delay, but would have to infer what happened from further analysis.

 ² The average NIC driver in a typical PC does not let you override this behavior; even checking 'Promiscuous mode' doesn't help -- your NIC will drop frames which fail the CRC check, long before Winpcap / libpcap see them.

 First Encounter with the ProfiTap-1G
 33
 Created: 2015-02-07

 Stuart Kendrick
 Updated: 2015-02-22

CRC-Errors-Bad-Cable_00000_20150215162513.pcapng [Stuart Kendrick] [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
<u>File E</u> dit <u>V</u> iew <u>Go</u> <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephony <u>I</u> ools <u>I</u> nternals <u>H</u> elp
▣ ◎ ◢ ■ ◢ □ 🖞 ೫ 🛃 ੧, 수 🔿 🗛 🛧 🖢 □ 🕞 ❶, ੨, 액, 🗹 ₩, ⊠ 🥵 ※ ໘
Filter: tcp Expression Clear Apply Save Me TAF Not-Junk TCP Reset
No Time Piter Source Detination Protocol Info
1213 0,422012224 70 10,0.150,1 46,255,41.2 TCP 7943-443 [SYN] Seg=0 win=8192 Len=0 MSS=1428 WS=4 SACK PERM=1
1214 0.148460474 70 46.255.41.2 10.0.150.1 TCP 443-7943 [SYN, ACK] seq=0 Ack=1 win=14600 Len=0 MSS=1370 SACK_PERM=1 WS=51
1215 0.000124248 64 10.0.150.1 46.255.41.2 TCP 7943-443 [ACK] seq=1 Ack=1 win=65760 Len=0
1216 0.000364664 182 10.0.150.1 46.255.41.2 TLSv1 Client Hello [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
1218 0.040424665 182 10.0.150.1 46.255.41.2 TCP [TCP Retransmission] 7943-443 [PSH, ACK] Seq=1 Ack=1 Win=65760 Len=124
1219 0.148790738 64 46.255.41.2 10.0.150.1 TCP 443-7943 [ACK] seq=1 Ack=125 win=14848 Len=0
1220 0.001067168 1428 46.255.41.2 10.0.150.1 TLSv1 Server Hello
1221 0.000324376 1044 46.255.41.2 10.0.150.1 TLSv1 Ignored Unknown Record
1222 0.000099424 64 10.0.150.1 46.255.41.2 TCP 7943-443 [ACK] Seq=125 ACK=2357 Win=65760 Len=0
1223 0.000590056 3/2 10.0.150.1 40.255.41.2 TLSVI Chient Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1224 0.155101752 312 40.255.41.2 10.0.150.1 ILSVI New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
1225 0.0012112113 99 10.0.100.1 40.235.41.2 ILSVI Application bata
1222 0.000053108 110 10.0.100.1 40.253.41.2 11.5VL Approximation Data
1228 0.000090320 64 10 0 150 1 46 255 41 2 TCP 7943-443 EEN ACK Seq=565 Ack=2611 win=65504 Len=0
1229 0.146667763 70 46.255.41.2 10.0.150.1 TCP 443-7943 [ACK] Seq=2611 ACK=480 Win=15872 Len=0 SI E=565 SRE=566
1230 0.000061216 70 46.255.41.2 10.0.150.1 TCP 443-7943 [ACK] seq=2611 ACk=538 Win=15872 Len=0 SLE=565 SRE=566
· · · · · · · · · · · · · · · · · · ·
■ Frame 1216: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits) on interface 0
Enternet II, src: DellInc_MT://sbb (00:20:D9:9T://sbb), Dst: Cisco_21:DT:T9 (04:8C:D5:21:DT:T9)
Bestington: Cisco_ff2;sb, (0,26;b6)(ff2;sb)
Type: TP (0/0800)
Figure check sequence: 0xf18a3cc9 [incorrect_should be 0x0dcd9b67]
Internet Protocol Version 4, Src: 10.0.150.1 (10.0.150.1), Dst: 46.255.41.2 (46.255.41.2)
Transmission Control Protocol, Src Port: 7943 (7943), Dst Port: 443 (443), Seq: 1, Ack: 1, Len: 124
Source Port: 7943 (7943)
Destination Port: 443 (443)
[Stream index: 82]
[TCP Segment Len: 124]
Sequence number: 1 (relative sequence number)
[Next sequence number: 125 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Header Length: 20 bytes
[Calculated window size: 65760]
[window size scaling factor: 4]
Checksum: 0xe969 [incorrect, should be 0xe968 (maybe caused by "TCP checksum offload"?)]
Urgent pointer: 0
∃ [SEQ/ACK analysis]
⊕ [Timestamps]
B Secure Sockets Layer
● Y Frame (frame), 182 bytes Packets: 29049 · Displayed: 8885 (30.6%) · Load time: 0:00.425

Figure 35: Bad Frame Check Sequence

First Encounter with the ProfiTap-1G 34 Stuart Kendrick Created: 2015-02-07 Updated: 2015-02-22

Summary

As of this writing, the ProfiTap-1G offers the cheapest way I know of to capture in-line -- in one package, it provides an in-line capture engine, leveraging the USB port on your PC, rather than requiring a specialized capture engine to be installed in your PC. As an added bonus, you can choose to continue using your existing analyzer software to capture. Or, you can use the included capture application, which additionally offers various ways to summarize statistics and log events on the capture stream.