First Encounters with the ProfiShark-10G

Contents

Introduction

I've been using a ProfiShark-10G, a new packet capture Tap from the ProfiTap folks, to tackle a sticky problem. In a future posting, I will describe the problem and what I learned from it. In the meantime, here is a first look at the ProfiShark-10G.

The ProfiShark line consists of small boxes -- small enough to stuff into your laptop bag -- which attach via USB to your computer and deliver in-line hardware-based packet capture across a range of media types.

Their use model enhances our common work-flow. As an operational IT professional, I typically receive tickets saying something like "The network is slow". So I visit the end-user to see what is happening, and of course I want a packet trace. Historically, I have inserted an ancient Ethernet mini-hub + my laptop, or installed Wireshark on the end-user's PC, or set-up a SPAN port and captured using my laptop ... all these approaches take time and make the analysis more difficult, for numerous reasons.[1] The last thing I need when analyzing traces is additional complexity combined with doubt over whether I am actually seeing all the frames, ordered accurately, with realistic time stamps.

By contrast, pulling the ProfiShark from my laptop bag and inserting it in-line with the end-user PC and its wall jack allows me to eliminate these confounding factors.

In this document, I use Windows and Wireshark. In addition, the ProfiShark line of Taps also ship with Linux drivers and support for a range of commercial analyzers (OmniPeek, OptiView, many others).

Background

The ProfiTap folks focus on in-line packet capture, via various products. The ProfiShark product line currently consists of (4) devices:

ProfiShark 1G
ProfiShark 1G+
ProfiShark 10G
ProfiShark 10G+

Briefly, the 1G supports in-line 10/100/1000BaseT capture, while the 10G device sports 10G capture via SFP+ ports. Naturally, you must provide the SFP+ transceivers. In this way, the ProfiShark supports each 10G flavor of Ethernet, minus 10GBaseT.[2]

[1] See Jasper Bongertz's Network Capture Playbook series at http://blog.packet-foo.com for a detailed discussion of the challenges involved, leading to the conclusion that the in-line Tap is the tool-of-choice for those of us analyzing client / server packet traces.

[2] ProfiTap is exploring what it would take to support 10GBaseT. Apparently, the power draw of 10GBaseT is substantial and acts as an early challenge to manufacturers wanting to support 10GBaseT in their Taps. For

The '+' models include GPS modules, for accurate time-syncing with a global time source.

First Encounters with a ProfiShark

Looks Like Another NIC

The ProfiTap 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.

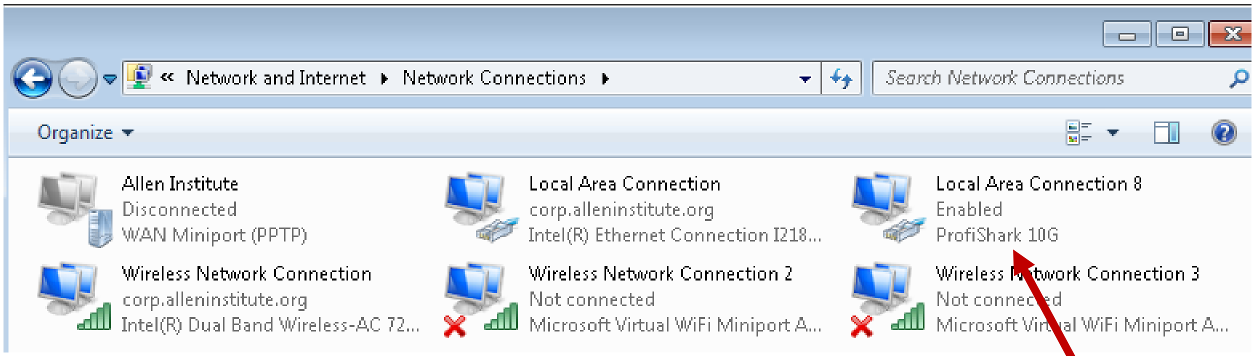
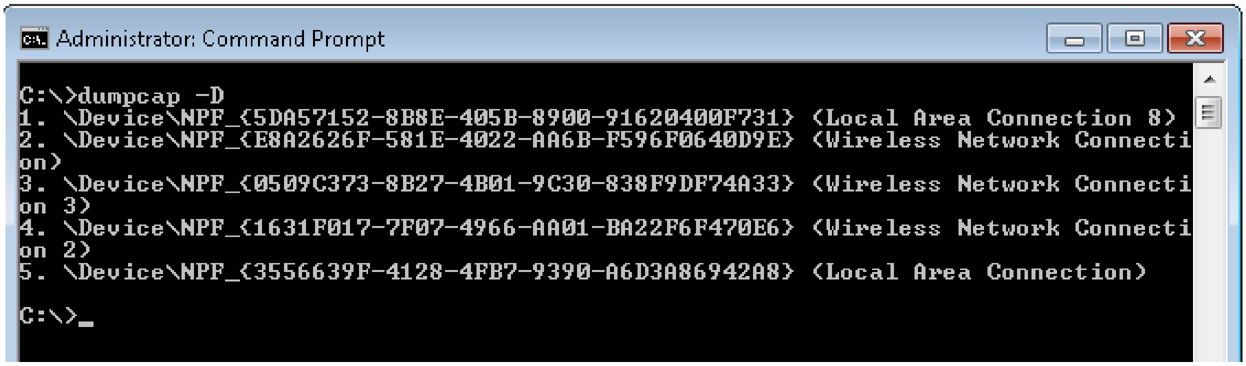

« Network and Internet ▸ Network Connections ▸
Search Network Connections
Organize ▾
Allen Institute
Disconnected
WAN Miniport (PPTP)
Local Area Connection
corp.alleninstitute.org
Intel(R) Ethernet Connection I218...
Local Area Connection 8
Enabled
ProfiShark 10G
Wireless Network Connection
corp.alleninstitute.org
Intel(R) Dual Band Wireless-AC 72...
Wireless Network Connection 2
Not connected
Microsoft Virtual WiFi Miniport A...
Wireless Network Connection 3
Not connected
Microsoft Virtual WiFi Miniport A...

Figure 1: Just Another NIC

ProfiTap-10G

Dumpcap sees it as just another NIC, Local Area Connection 8 in this example.



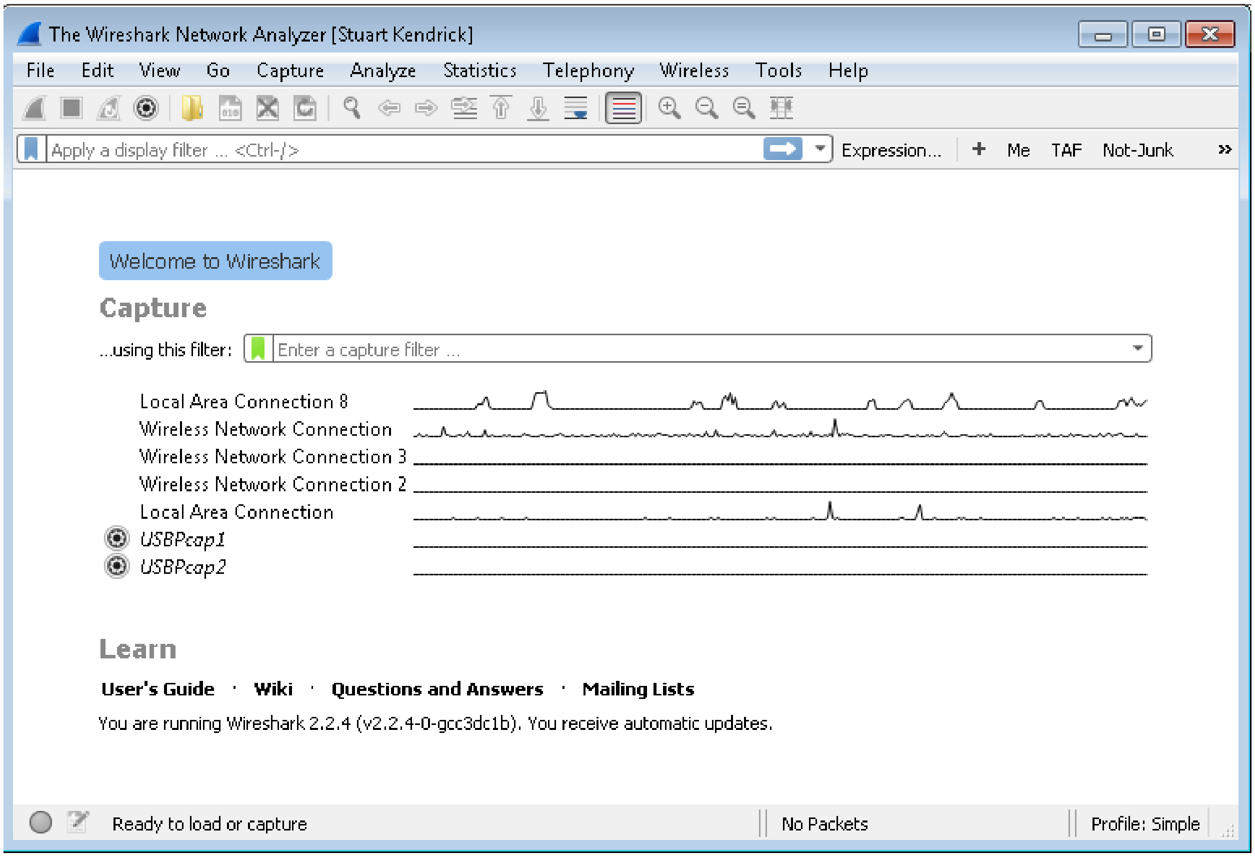
```
C:\>dumpcap -D
1. \Device\NPF_{5DA57152-8B8E-405B-8900-91620400F731} (Local Area Connection 8)
2. \Device\NPF_{E8A2626F-581E-4022-AA6B-F596F0640D9E} (Wireless Network Connecti
on)
3. \Device\NPF_{0509C373-8B27-4B01-9C30-838F9DF74A33} (Wireless Network Connecti
on 3)
4. \Device\NPF_{1631F017-7F07-4966-AA01-BA22F6F470E6} (Wireless Network Connecti
on 2)
5. \Device\NPF_{3556639F-4128-4FB7-9390-A6D3A86942A8} (Local Area Connection)

C:\>_
```

Figure 2: Dumpcap NIC List

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

example, 10GBaseT power draw exceeds what the SFP+ specification provides, which is why we don't see 10GBaseT SFP+ transceivers.

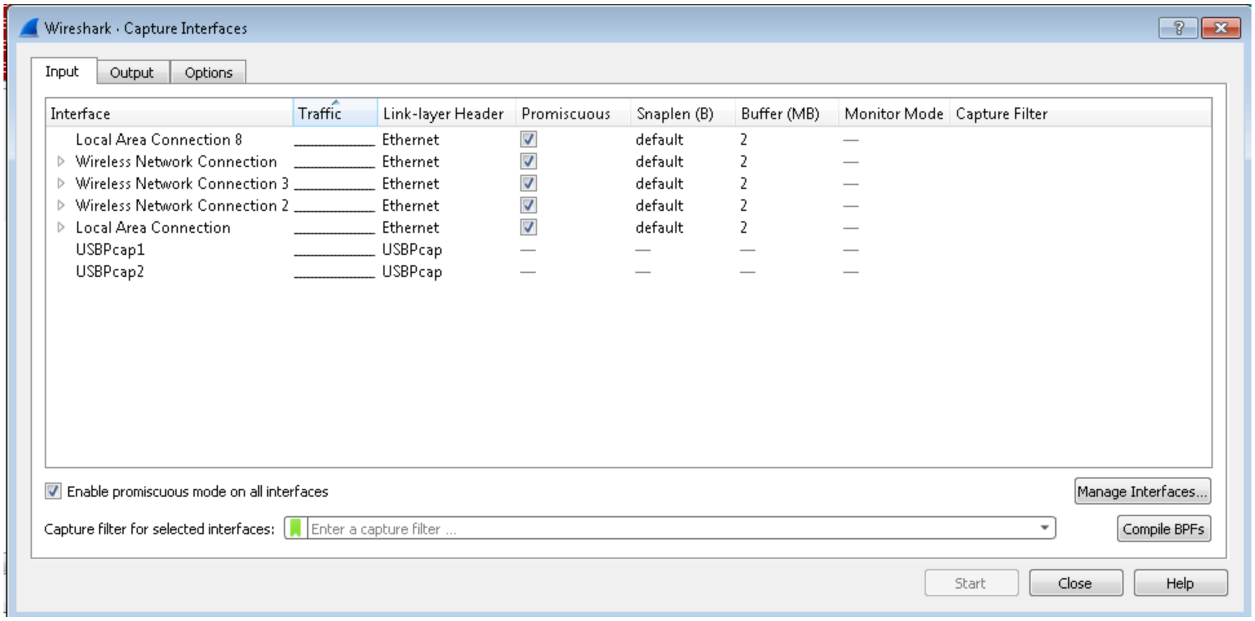

The Wireshark Network Analyzer [Stuart Kendrick]
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression... + Me TAF Not-Junk »
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

Local Area Connection 8
Wireless Network Connection
Wireless Network Connection 3
Wireless Network Connection 2
Local Area Connection
USBPcap1
USBPcap2

You are running Wireshark 2.2.4 (v2.2.4-0-gcc3dc1b). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Simple

Figure 3: Wireshark Start Capture List



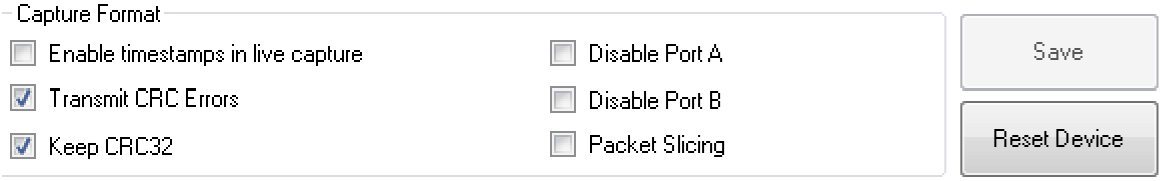
Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (B)	Buffer (MB)	Monitor Mode	Capture Filter
Local Area Connection 8		Ethernet	☑	default	2	—	
Wireless Network Connection		Ethernet	☑	default	2	—	
Wireless Network Connection 3		Ethernet	☑	default	2	—	
Wireless Network Connection 2		Ethernet	☑	default	2	—	
Local Area Connection		Ethernet	☑	default	2	—	
USBPcap1		USBPcap	—	—	—	—	
USBPcap2		USBPcap	—	—	—	—	

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter ...

Figure 4: Wireshark Interface List

The Tap ships with a supporting application *(ProfiShark Manager)* which allows you to configure its in-line functionality.



Capture Format

☐ Enable timestamps in live capture
☑ Transmit CRC Errors
☑ Keep CRC32
☐ Disable Port A
☐ Disable Port B
☐ Packet Slicing

Figure 5: ProfiShark-10G Capture Format Options

1. *Enable timestamps in live capture* invokes the Tap's on-board clock to deliver timestamps with 8ns resolution.
2. *Transmit CRC Errors* instructs the Tap to forward Ethernet frames whose CRC trailers do not correctly summarize the frame's contents. This allows us to choose whether or not to keep damaged frames.
3. *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. This allows us to choose whether or not we want to examine the Ethernet CRC.
4. *Disable Port A/B* allows you to capture in a single direction -- useful if you want to verify the direction from which a given frame or conversation is arriving.
5. *Packet Slicing* currently slices frames to 128 bytes, to allow you to conserve IO and disk space. ProfiTap plans to offer more granular control in a future software release.

Items #2 & #3 above are classic features of hardware-based capture engines. In contrast, most analyzers, running on commodity NICs using commodity drivers, can perform neither of these: run Wireshark on your average Windows or Linux box, and you'll discover that the NIC discards frames with CRC errors before Wireshark (more precisely, before winpcap / libpcap) receives it. Similarly, the average NIC strips the CRC from the frame before passing it to winpcap / libpcap.

This is not a line-rate capture solution -- the Tap must forward frames across the USB 3.1 port (Generation 1: 5 Gb/s) and your laptop must then write those frames to disk. ProfiTap has measured ~3.2 Gb/s capture rate, using their *ProfiShark Manager* software.

You can capture using your favorite analyzer -- Wireshark, for example. However, you can also capture using the *ProfiShark Manager* software (Windows or Linux) written by ProfiTap, which uses a custom IO driver to improve write performance to local storage, thus allowing your host laptop to capture more frames per second than Wireshark (libpcap / winpcap) by itself can typically manage.

Deploying

Here is what the ProfiShark looks like in action. I have inserted the ProfiShark in-line with an uplink off a Catalyst 2960X Switch Stack supporting a particular IDF in my building. A little hard to see in this photo, but the blue OM4 jumper plugged into *6s-1-esx-5* (center right -- look for the yellow label) actually runs down to the ProfiShark sitting on the floor of this IDF. This

Switch Stack consists of (8) Catalyst 2960X supporting the access-layer for this IDF, with redundant 10GBaseSR uplinks (plugged into Te1/0/1 and Te5/0/1) to a Distribution Layer (Nexus 9000, not shown) living in the building's MDF.[3]

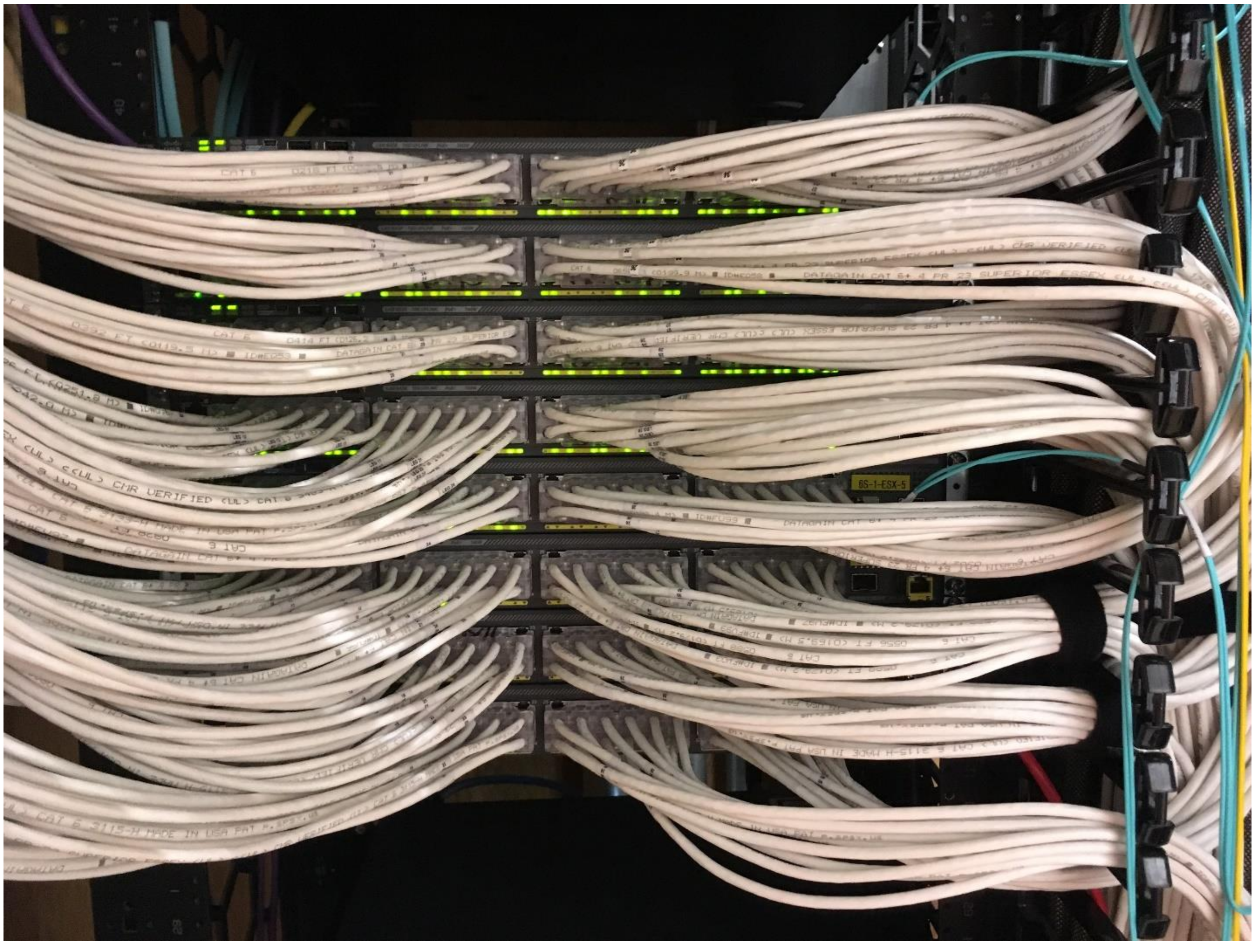


Figure 6: Catalyst 2960X Stack

Here is the ProfiShark 10G itself, plugged into my laptop, both sitting on the floor of an IDF.

[3] The SwitchPack Cat6 assemblies which plug into the Ethernet ports are an *AFL HyperScale* product which allow us to more effectively manage the physical layer in dense IDFs like this one: each (12) cable assembly terminates in a single connector, greatly simplifying the task of inserting / removing Cat6 cables. See http://www.networkcomputing.com/data-centers/cable-management-tackling-tangles/1944964207 for a photo essay introduction to high-density cable management, or http://www.skendric.com/philosophy/uptime/physical-layer/Designing-IDFs-to-Reduce-Operational-Cost.pdf for a detailed description. Both illustrate the use of SwitchPacks.

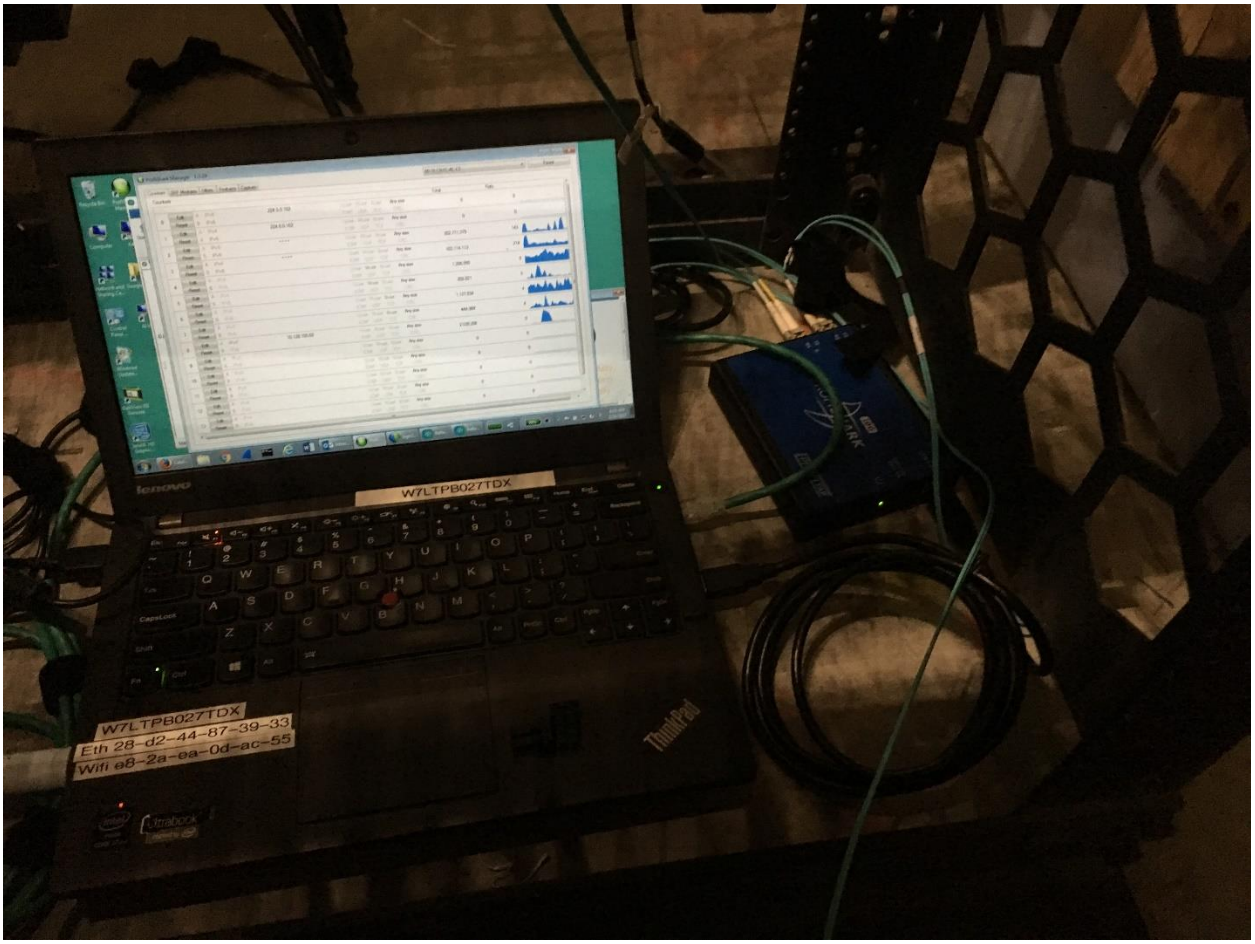


Figure 7: Laptop powering ProfiShark-10G

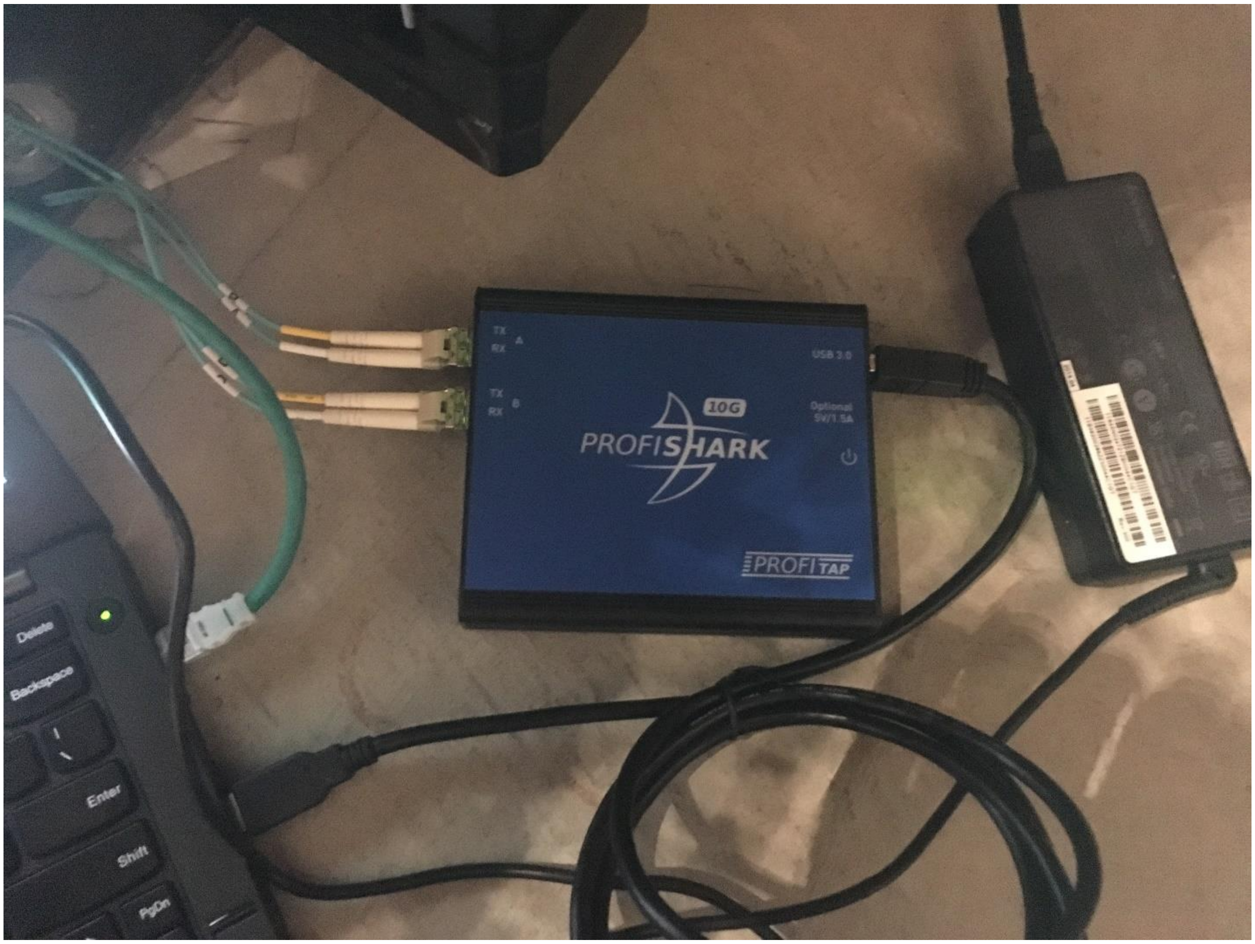


Figure 8: Focus on ProfiShark-10G

One of those blue OM4 jumpers runs to Te5/0/1 on *6s-1-esx-5*, while the other runs to the structured glass leading to the MDF: the right-hand jumper in the top left of the following photo. The black USB cable connects the ProfiShark to my laptop, while the green cable is a vanilla Cat6 cable providing commodity Ethernet to the laptop (not necessary for this story, but then again, it gives me RDP access to the laptop, so convenient for my use case, as I sometimes want to capture remotely, rather than while squatting on the floor of the IDF).

Notice that the ProfiShark is powered by the laptop -- remove the laptop, and link drops on the 10GBaseSR pathway traversing the ProfiShark. The ProfiShark can be powered by a separate AC/DC power adapter (not shown); I use this when I want to temporarily remove my laptop to use it elsewhere but want to sustain the link through the ProfiShark. Without the laptop, I can no longer capture of course -- ProfiShark capture is managed either by Wireshark or the *ProfiShark Manager* application.

Interestingly, though, even without the laptop, the ProfiShark Tap continues to track statistics, which show up in the several Counters screens available through the *ProfiShark Manager* application -- reconnect the laptop, and the accumulated statistics again become visible -- see the Counters section later in this document for detail.

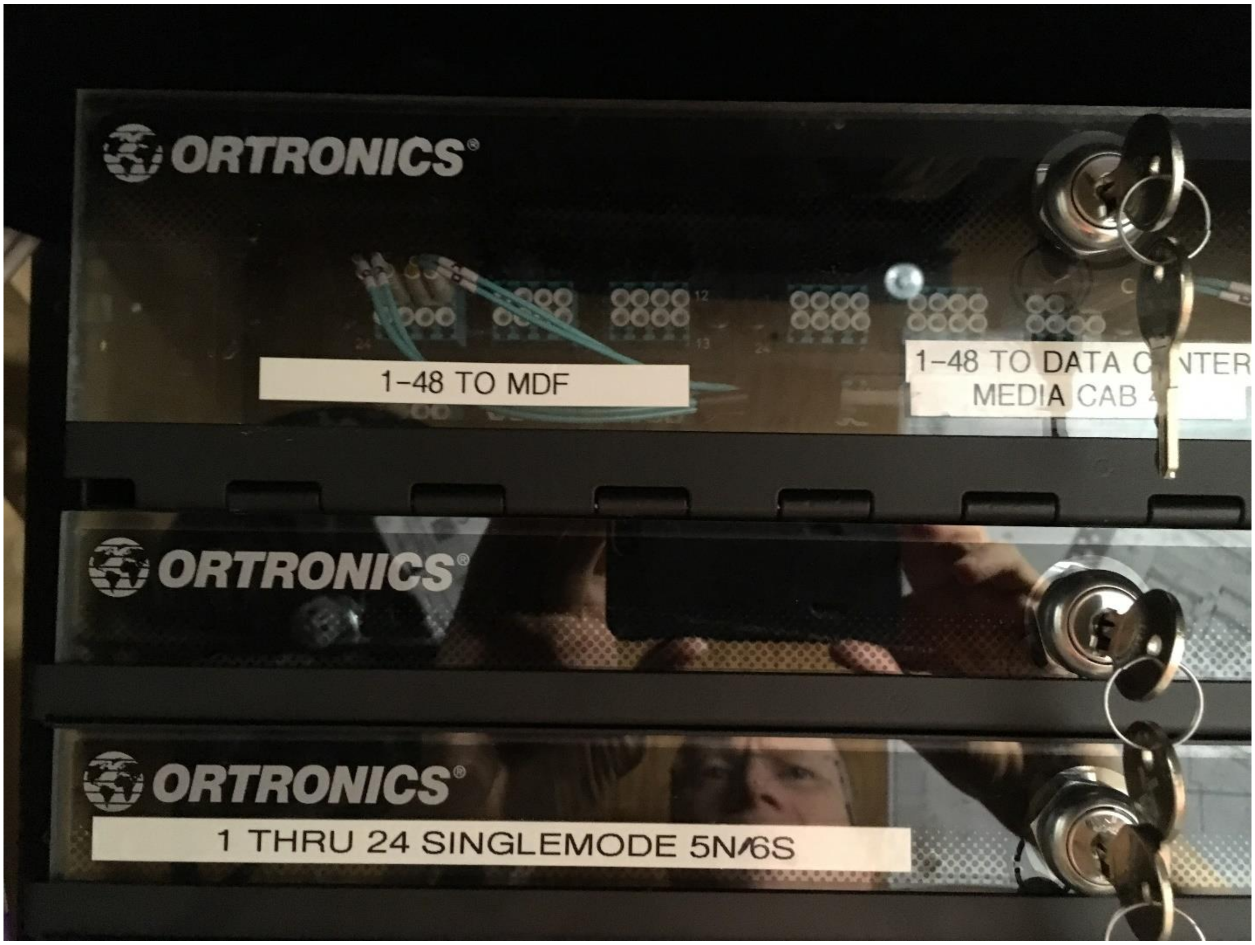
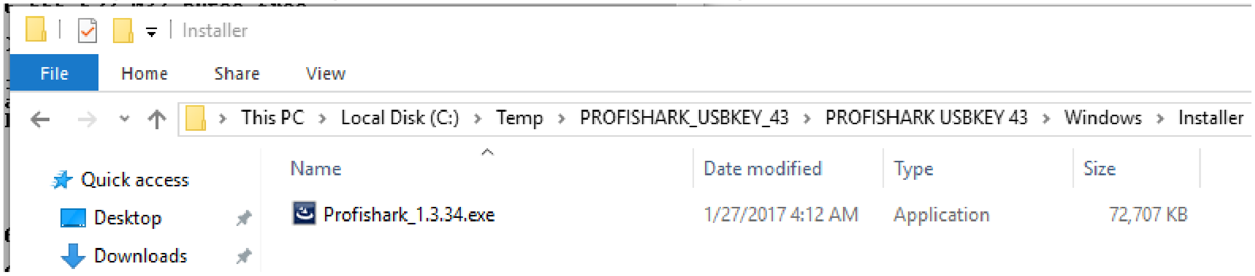


Figure 9: Structured Glass Cabling to MDF

Software Installation

Installing the software begins with the usual Installer program.



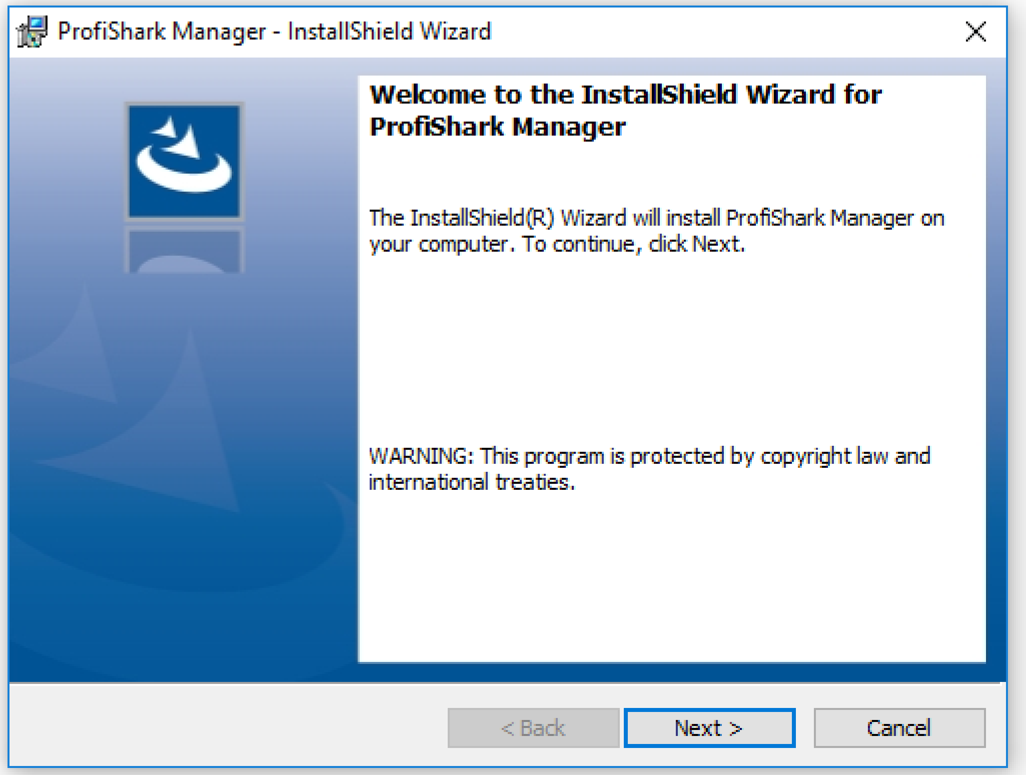
This PC › Local Disk (C:) › Temp › PROFISHARK_USBKEY_43 › PROFISHARK USBKEY 43 › Windows › Installer

Name	Date modified	Type	Size
Profishark_1.3.34.exe	1/27/2017 4:12 AM	Application	72,707 KB

Figure 10: Windows Installer

And the resulting InstallShield Wizard.

Once that finishes, installation progresses as usual.


ProfiShark Manager - InstallShield Wizard

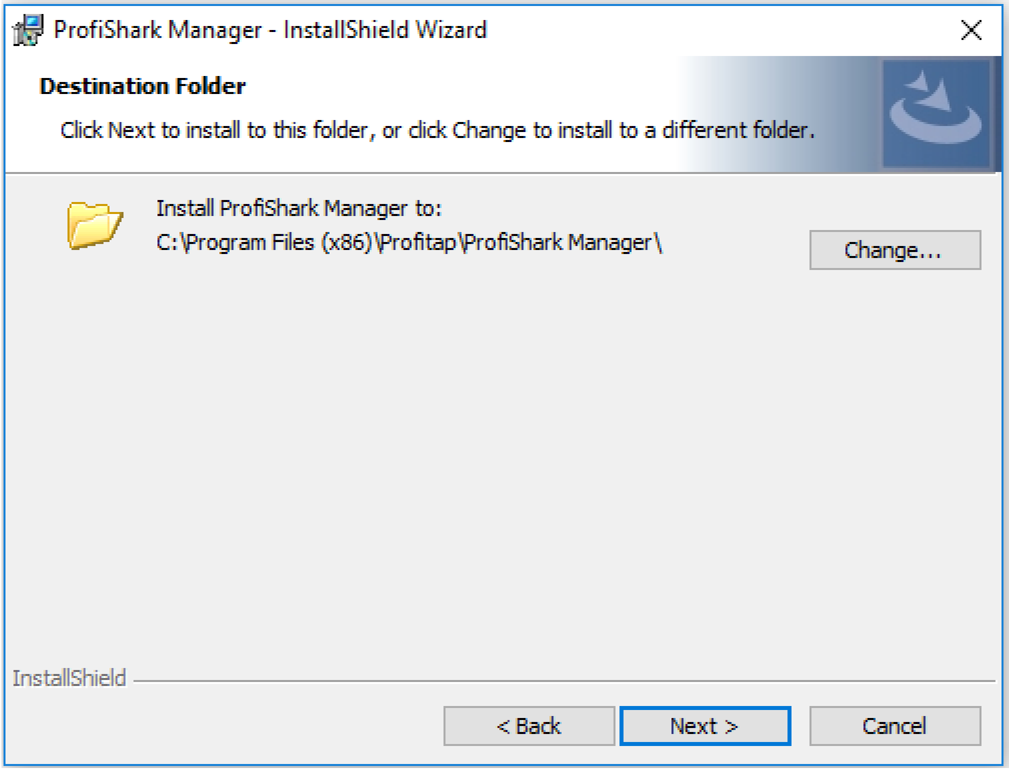
Welcome to the InstallShield Wizard for ProfiShark Manager

The InstallShield(R) Wizard will install ProfiShark Manager on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

Figure 11: InstallShield Wizard

The Installer progresses in the usual way:

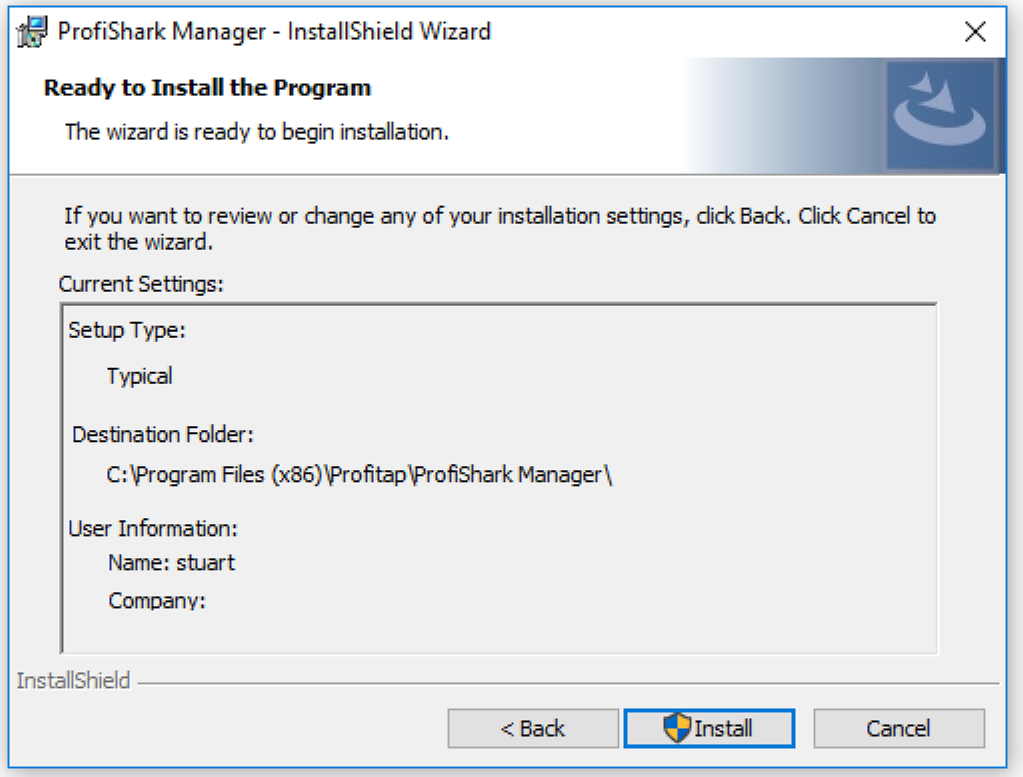


Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install ProfiShark Manager to:
C:\Program Files (x86)\Profitap\ProfiShark Manager\

Figure 12: InstallShield Wizard Destination



Ready to Install the Program

The wizard is ready to begin installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

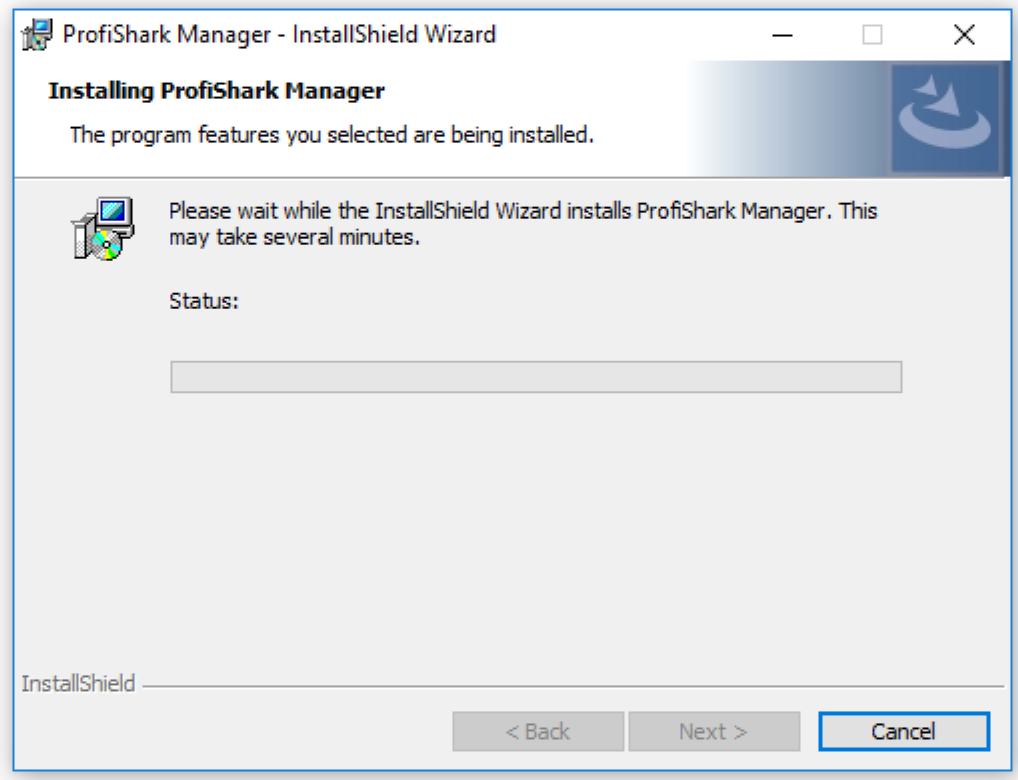
Current Settings:

Setup Type:
Typical

Destination Folder:
C:\Program Files (x86)\Profitap\ProfiShark Manager\

User Information:
Name: stuart
Company:

Figure 13: InstallShield Wizard Ready to Begin



ProfiShark Manager - InstallShield Wizard

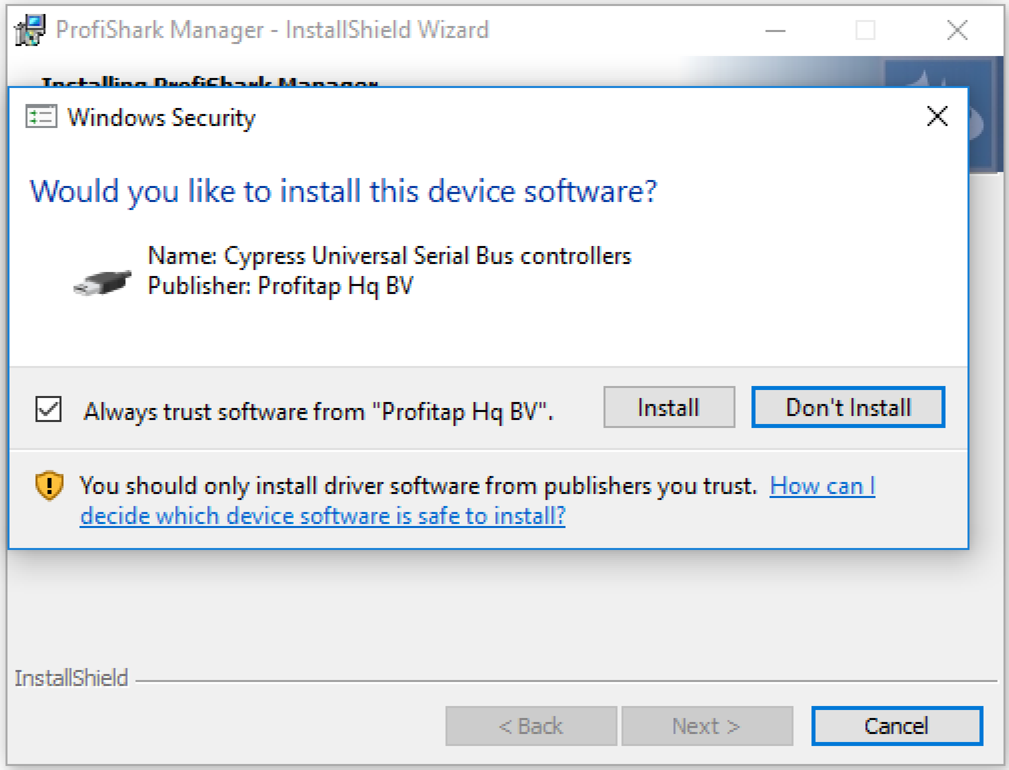
Installing ProfiShark Manager

The program features you selected are being installed.

Please wait while the InstallShield Wizard installs ProfiShark Manager. This may take several minutes.

Status:

Figure 14: Validating Install


ProfiShark Manager - InstallShield Wizard
Installing ProfiShark Manager
Windows Security
Install
Don't Install
InstallShield
< Back
Next >
Cancel

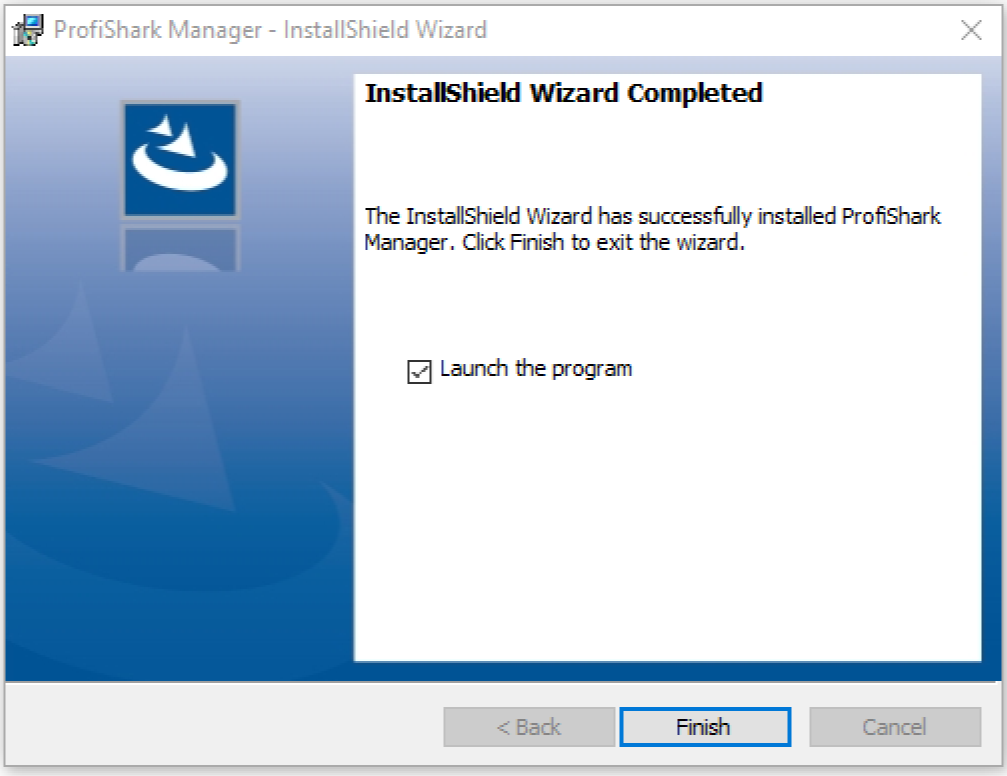
Would you like to install this device software?

Name: Cypress Universal Serial Bus controllers
Publisher: Profitap Hq BV

☑ Always trust software from "Profitap Hq BV".

You should only install driver software from publishers you trust. How can I decide which device software is safe to install?

Figure 15: Install USB Driver



InstallShield Wizard Completed

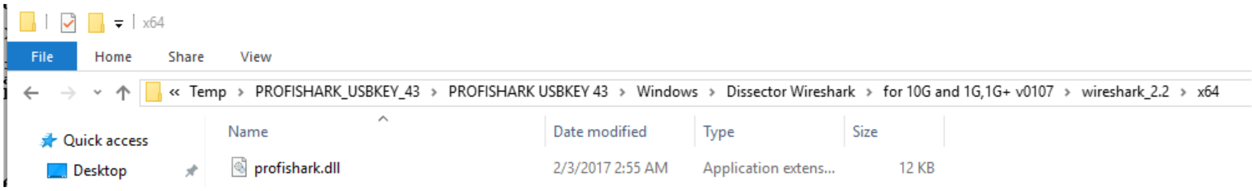
The InstallShield Wizard has successfully installed ProfiShark Manager. Click Finish to exit the wizard.

☑ Launch the program

Figure 16: Launch the program

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

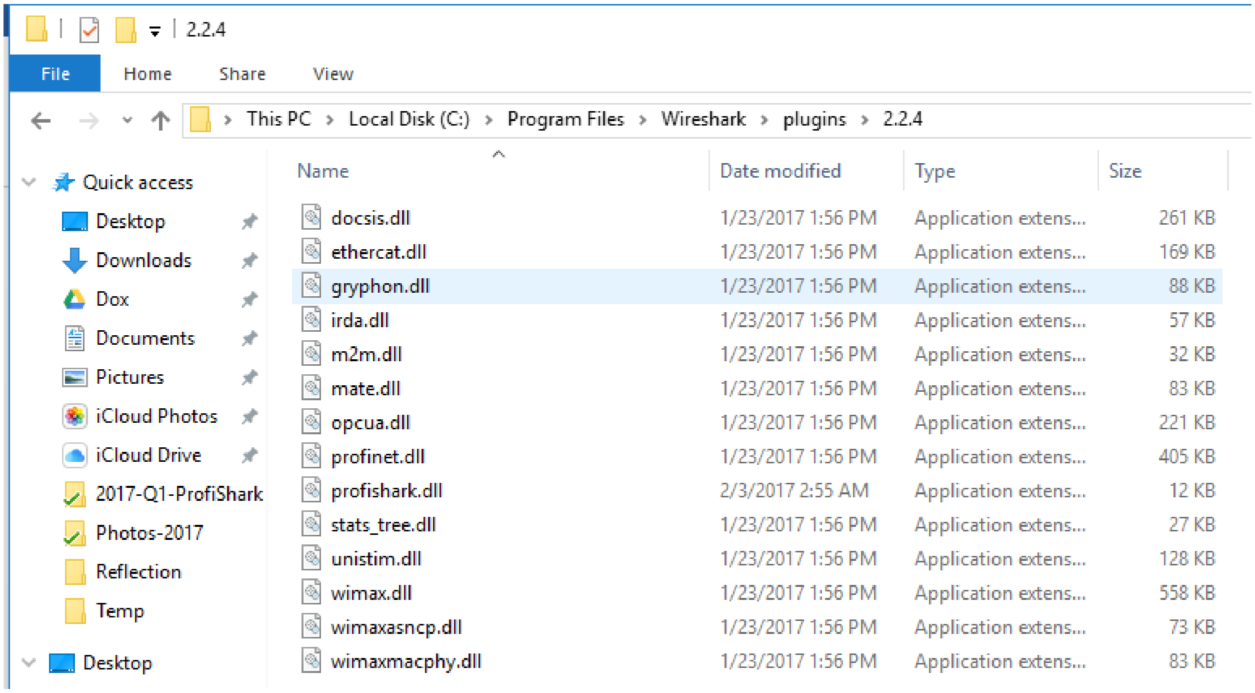
Finally, manually copy the dissector *profishark_1g.dll* into your Wireshark plugins folder.



« Temp › PROFISHARK_USBKEY_43 › PROFISHARK USBKEY 43 › Windows › Dissector Wireshark › for 10G and 1G,1G+ v0107 › wireshark_2.2 › x64

Name	Date modified	Type	Size
profishark.dll	2/3/2017 2:55 AM	Application extens...	12 KB

Figure 17: Copy Wireshark Dissector

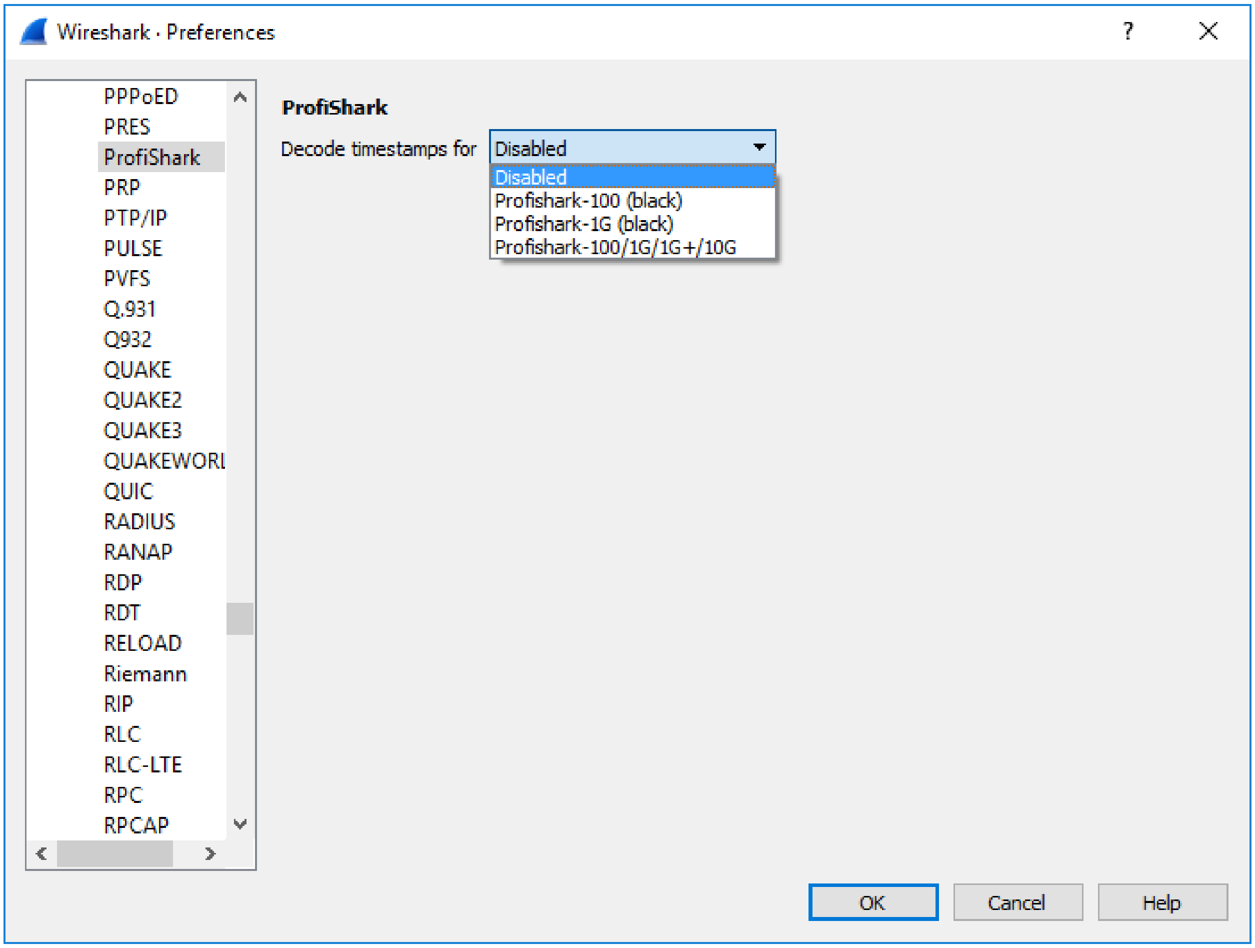


This PC › Local Disk (C:) › Program Files › Wireshark › plugins › 2.2.4

Name	Date modified	Type	Size
docsis.dll	1/23/2017 1:56 PM	Application extens...	261 KB
ethercat.dll	1/23/2017 1:56 PM	Application extens...	169 KB
gryphon.dll	1/23/2017 1:56 PM	Application extens...	88 KB
irda.dll	1/23/2017 1:56 PM	Application extens...	57 KB
m2m.dll	1/23/2017 1:56 PM	Application extens...	32 KB
mate.dll	1/23/2017 1:56 PM	Application extens...	83 KB
opcua.dll	1/23/2017 1:56 PM	Application extens...	221 KB
profinet.dll	1/23/2017 1:56 PM	Application extens...	405 KB
profishark.dll	2/3/2017 2:55 AM	Application extens...	12 KB
stats_tree.dll	1/23/2017 1:56 PM	Application extens...	27 KB
unistim.dll	1/23/2017 1:56 PM	Application extens...	128 KB
wimax.dll	1/23/2017 1:56 PM	Application extens...	558 KB
wimaxasncp.dll	1/23/2017 1:56 PM	Application extens...	73 KB
wimaxmacphy.dll	1/23/2017 1:56 PM	Application extens...	83 KB

Figure 18: To Wireshark Plugins Folder

Copying *profishark.dll* into place adds the ProfiShark protocol to the Preferences... Protocols... list and allows you to enable or disable hardware time-stamp decoding.

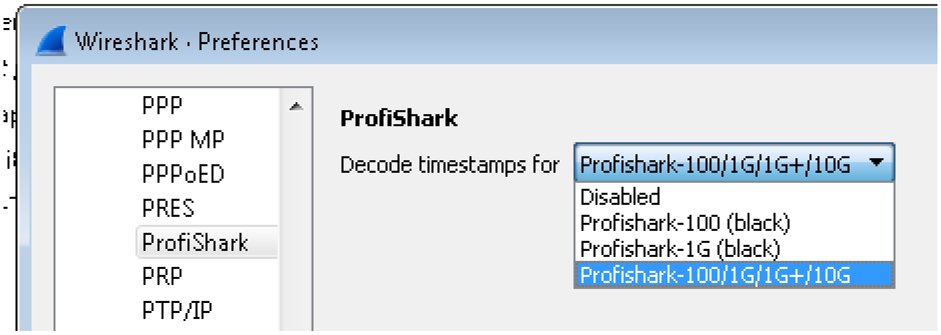


ProfiShark

Decode timestamps for: Disabled

Figure 19: ProfiShark Timestamp Decoding in Wireshark

Enable *Decode timestamps for* to instruct Wireshark to decode the timestamps which ProfiShark adds to pcaps. [Naturally, if the pcap you are analyzing does not contain ProfiShark-added timestamps, then this choice has no effect.]



ProfiShark

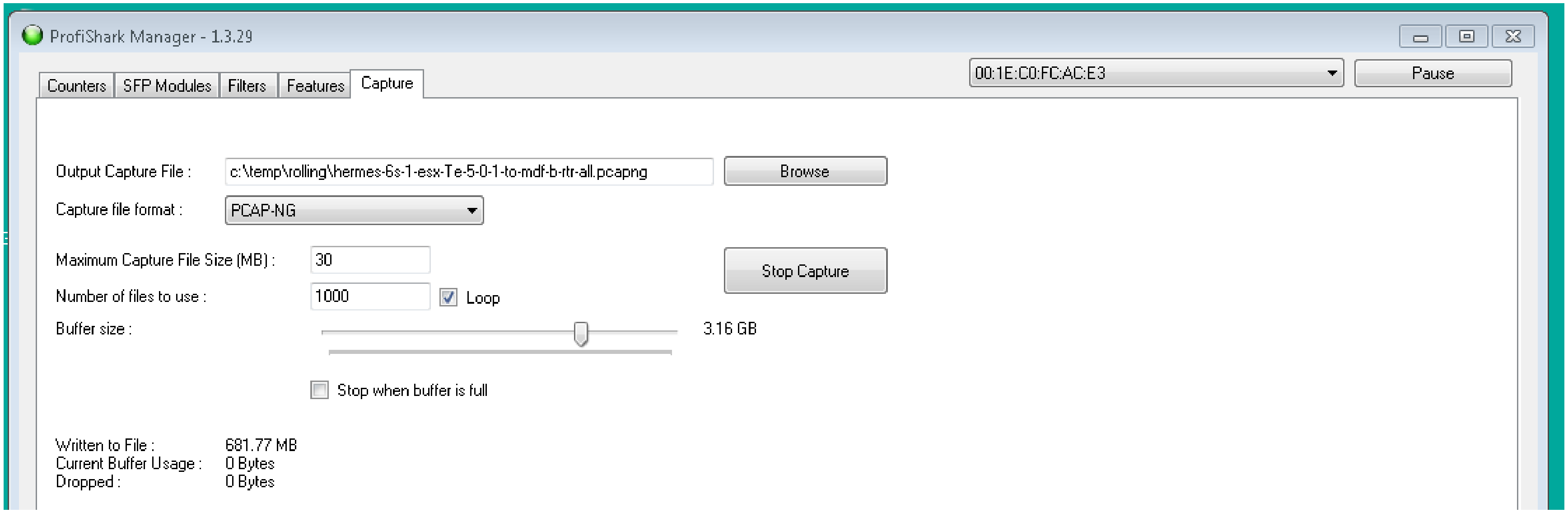
Decode timestamps for: Profishark-100/1G/1G+/10G

Figure 20: Enable *Decode timestamps for*

Capturing Using ProfiManager

At this point, you can open Wireshark (or one of the many other supported analysis programs) and capture using this newly-visible ProfiShark NIC. However, for the purposes of this document, I will focus on the functionality provided by the included ProfiManager application.

Opening the newly-installed ProfiManager application allows us to talk directly to the Tap. Here, I skip ahead to the Capture Tab.



00:1E:C0:FC:AC:E3

Output Capture File : c:\temp\rolling\hermes-6s-1-esx-Te-5-0-1-to-mdf-b-rtr-all.pcapng

Capture file format : PCAP-NG

Maximum Capture File Size (MB) : 30

Number of files to use : 1000 ☑ Loop

Buffer size : 3.16 GB

☐ Stop when buffer is full

Written to File : 681.77 MB
Current Buffer Usage : 0 Bytes
Dropped : 0 Bytes

Figure 21: ProfiManager Capture Tab

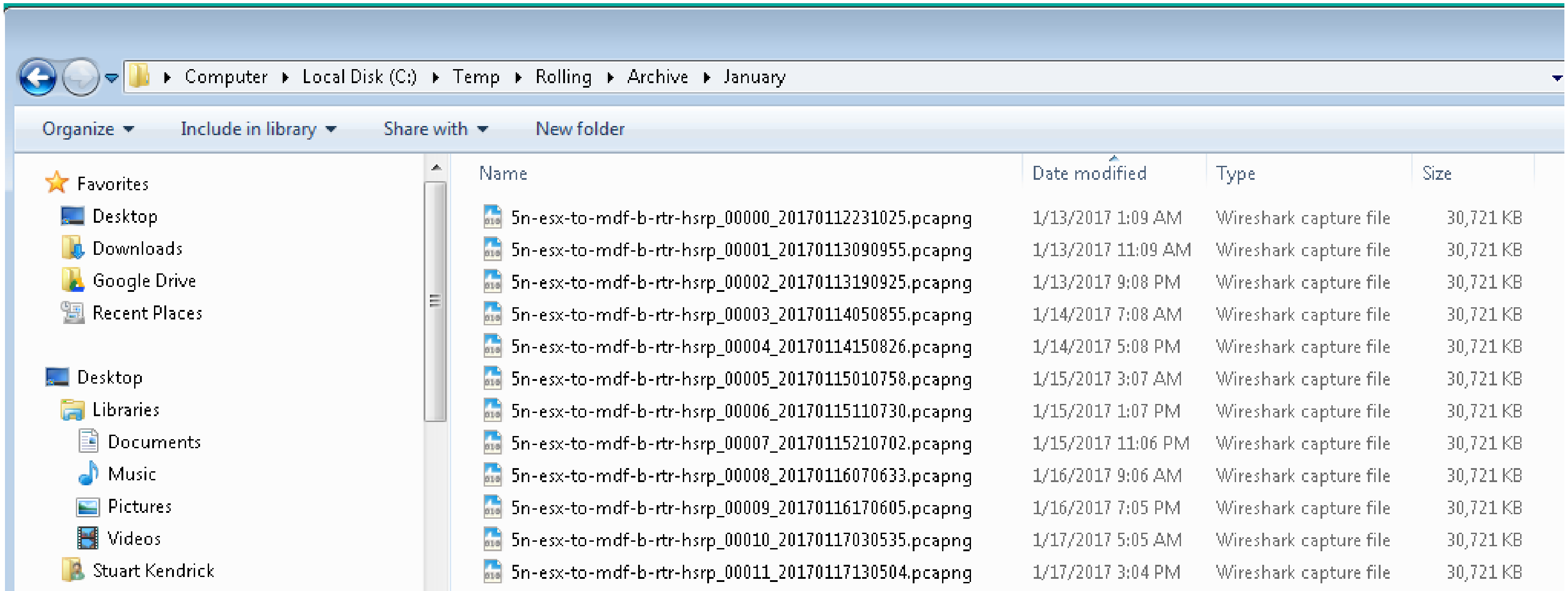
Notice how ProfiShark Manager keeps track of Dropped frames -- tells you if the packet stream is over-running your capture pipeline (USB 3.1 plus your laptop's storage).

In the screen shot above, I have configured ProfiManager to capture:

- 1000 files of 30MB each
- Consume no more than 3.16GB of disk space

- Loop (aka ring-buffer), i.e. the 1001st file will overwrite file 1

The resulting directory will look something like the following:



Name	Date modified	Type	Size
5n-esx-to-mdf-b-rtr-hsrp_00000_20170112231025.pcapng	1/13/2017 1:09 AM	Wireshark capture file	30,721 KB
5n-esx-to-mdf-b-rtr-hsrp_00001_20170113090955.pcapng	1/13/2017 11:09 AM	Wireshark capture file	30,721 KB
5n-esx-to-mdf-b-rtr-hsrp_00002_20170113190925.pcapng	1/13/2017 9:08 PM	Wireshark capture file	30,721 KB
5n-esx-to-mdf-b-rtr-hsrp_00003_20170114050855.pcapng	1/14/2017 7:08 AM	Wireshark capture file	30,721 KB
5n-esx-to-mdf-b-rtr-hsrp_00004_20170114150826.pcapng	1/14/2017 5:08 PM	Wireshark capture file	30,721 KB
5n-esx-to-mdf-b-rtr-hsrp_00005_20170115010758.pcapng	1/15/2017 3:07 AM	Wireshark capture file	30,721 KB
5n-esx-to-mdf-b-rtr-hsrp_00006_20170115110730.pcapng	1/15/2017 1:07 PM	Wireshark capture file	30,721 KB
5n-esx-to-mdf-b-rtr-hsrp_00007_20170115210702.pcapng	1/15/2017 11:06 PM	Wireshark capture file	30,721 KB
5n-esx-to-mdf-b-rtr-hsrp_00008_20170116070633.pcapng	1/16/2017 9:06 AM	Wireshark capture file	30,721 KB
5n-esx-to-mdf-b-rtr-hsrp_00009_20170116170605.pcapng	1/16/2017 7:05 PM	Wireshark capture file	30,721 KB
5n-esx-to-mdf-b-rtr-hsrp_00010_20170117030535.pcapng	1/17/2017 5:05 AM	Wireshark capture file	30,721 KB
5n-esx-to-mdf-b-rtr-hsrp_00011_20170117130504.pcapng	1/17/2017 3:04 PM	Wireshark capture file	30,721 KB

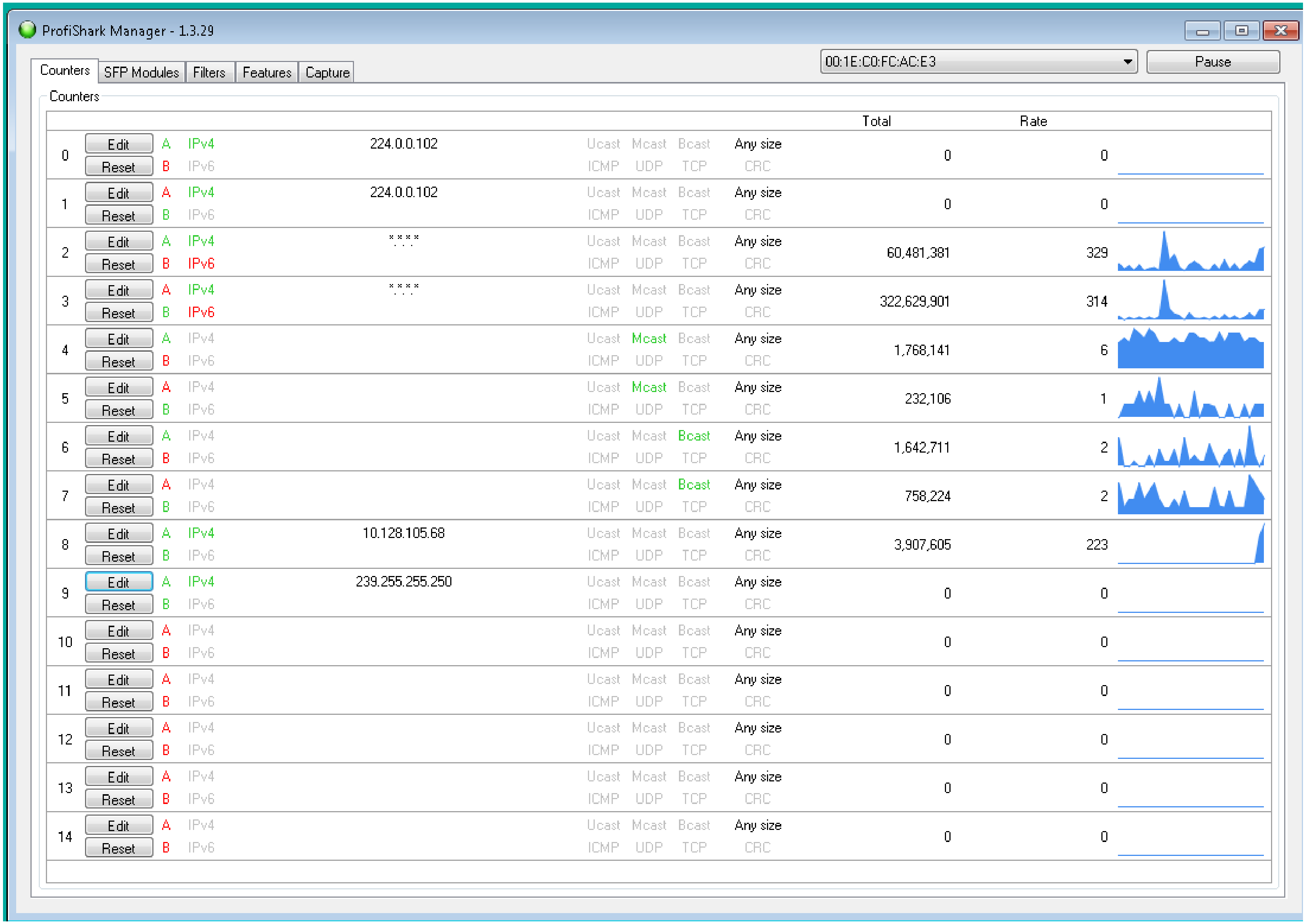
Figure 22: Looping Capture

So that's how you capture in-line.

Neat Features

Counters

The opening tab in ProfiShark Manager offers a new capability (new in that this Tab isn't available on the 1G line of ProfiSharks). This tab is called Counters.



00:1E:C0:FC:AC:E3

Counters

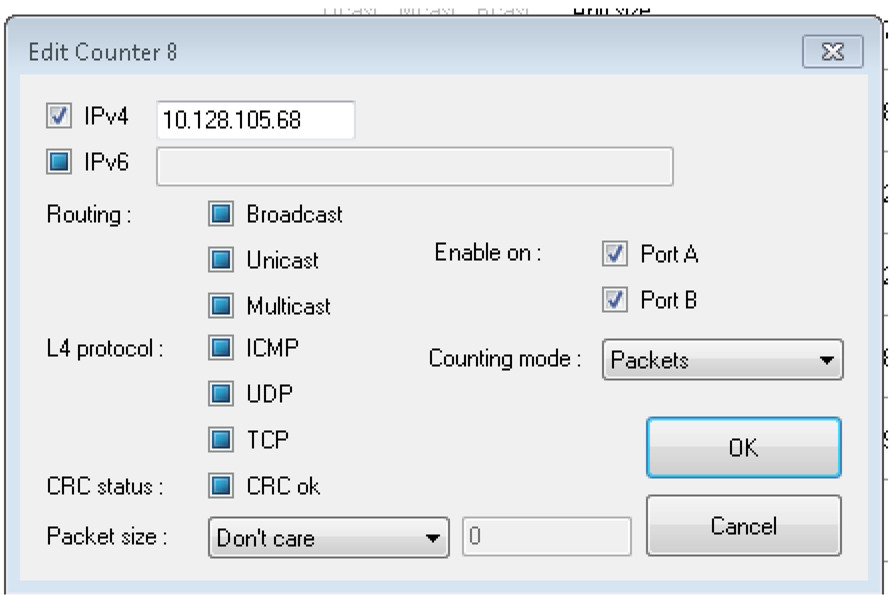
							Total	Rate
0	Edit Reset	A B	IPv4 IPv6	224.0.0.102	Ucast Mcast Bcast ICMP UDP TCP	Any size CRC	0	0
1	Edit Reset	A B	IPv4 IPv6	224.0.0.102	Ucast Mcast Bcast ICMP UDP TCP	Any size CRC	0	0
2	Edit Reset	A B	IPv4 IPv6	*.*.*.*	Ucast Mcast Bcast ICMP UDP TCP	Any size CRC	60,481,381	329
3	Edit Reset	A B	IPv4 IPv6	*.*.*.*	Ucast Mcast Bcast ICMP UDP TCP	Any size CRC	322,629,901	314
4	Edit Reset	A B	IPv4 IPv6		Ucast Mcast Bcast ICMP UDP TCP	Any size CRC	1,768,141	6
5	Edit Reset	A B	IPv4 IPv6		Ucast Mcast Bcast ICMP UDP TCP	Any size CRC	232,106	1
6	Edit Reset	A B	IPv4 IPv6		Ucast Mcast Bcast ICMP UDP TCP	Any size CRC	1,642,711	2
7	Edit Reset	A B	IPv4 IPv6		Ucast Mcast Bcast ICMP UDP TCP	Any size CRC	758,224	2
8	Edit Reset	A B	IPv4 IPv6	10.128.105.68	Ucast Mcast Bcast ICMP UDP TCP	Any size CRC	3,907,605	223
9	Edit Reset	A B	IPv4 IPv6	239.255.255.250	Ucast Mcast Bcast ICMP UDP TCP	Any size CRC	0	0
10	Edit Reset	A B	IPv4 IPv6		Ucast Mcast Bcast ICMP UDP TCP	Any size CRC	0	0
11	Edit Reset	A B	IPv4 IPv6		Ucast Mcast Bcast ICMP UDP TCP	Any size CRC	0	0
12	Edit Reset	A B	IPv4 IPv6		Ucast Mcast Bcast ICMP UDP TCP	Any size CRC	0	0
13	Edit Reset	A B	IPv4 IPv6		Ucast Mcast Bcast ICMP UDP TCP	Any size CRC	0	0
14	Edit Reset	A B	IPv4 IPv6		Ucast Mcast Bcast ICMP UDP TCP	Any size CRC	0	0

Figure 23: Counters Tab

Recall that Port A captures frames Transmitted from the upstream Nexus 9000, arriving into this Catalyst 2960X Stack, while Port B captures frames transmitted from the Catalyst 2960X Stack toward the upstream Nexus 9000.

Counter 0: Count all frames with a source or destination address of 224.0.0.102 which arrive via Port A.
Counter 1: Count all frames with a source or destination address of 224.0.0.102 which arrive via Port B.
Counter 2: All IPv4 frames arriving via Port A.
Counter 3: All IPv4 frames arriving via Port B.
Counter 4: All Multicast frames arriving via Port A.
Counter 5: All Multicast frames arriving via Port B.
Counter 6: All Broadcast frames arriving via Port A.
Counter 7: All Broadcast frames arriving via Port B.
Counter 8: All Unicast frames arriving via both Ports with a source or destination address of 10.128.105.68.
Counter 9: All Multicast frames arriving via both Ports with a source or destination address of 239.255.255.250

The Edit button allows one to create the Counter using filter options which look like this.



Edit Counter 8

☑ IPv4 10.128.105.68

▣ IPv6

Routing : ▣ Broadcast ▣ Unicast ▣ Multicast

Enable on : ☑ Port A ☑ Port B

L4 protocol : ▣ ICMP ▣ UDP ▣ TCP

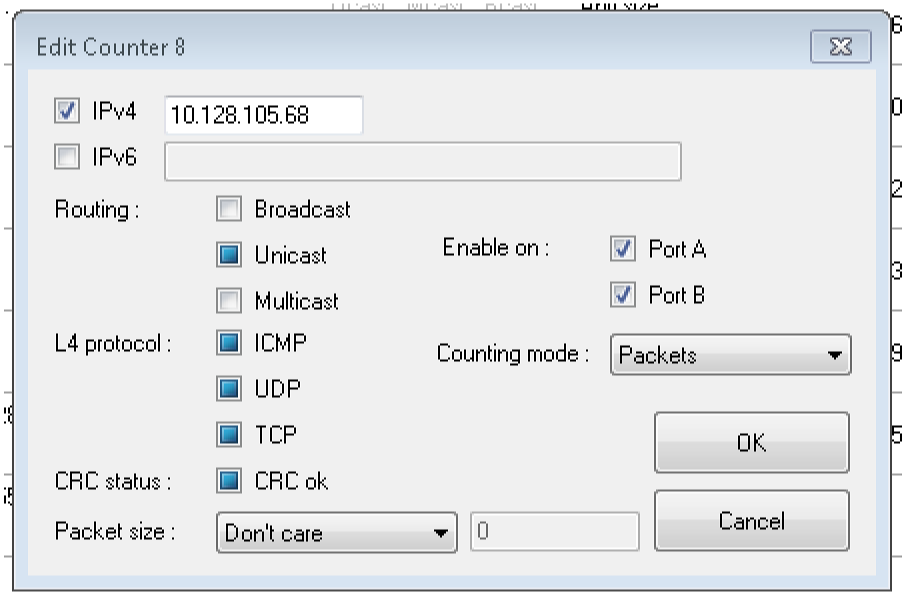
Counting mode : Packets

CRC status : ▣ CRC ok

Packet size : Don't care 0

Figure 24: Editing Counter 8 Example 1

In the example above, the Counter tracks frames arriving on either channel (Port A or Port B) with a source or destination address of 10.128.105.68. The blue square in each of the other checkboxes translates into "Don't care", i.e. the Counter will include the frame in its counting regardless of whether the frame is Broadcast / Unicast / Multicast or ICMP / UDP / TCP, etc.



Edit Counter 8

☑ IPv4 10.128.105.68

□ IPv6

Routing : □ Broadcast ■ Unicast □ Multicast

Enable on : ☑ Port A ☑ Port B

L4 protocol : ■ ICMP ■ UDP ■ TCP

Counting mode : Packets

CRC status : ■ CRC ok

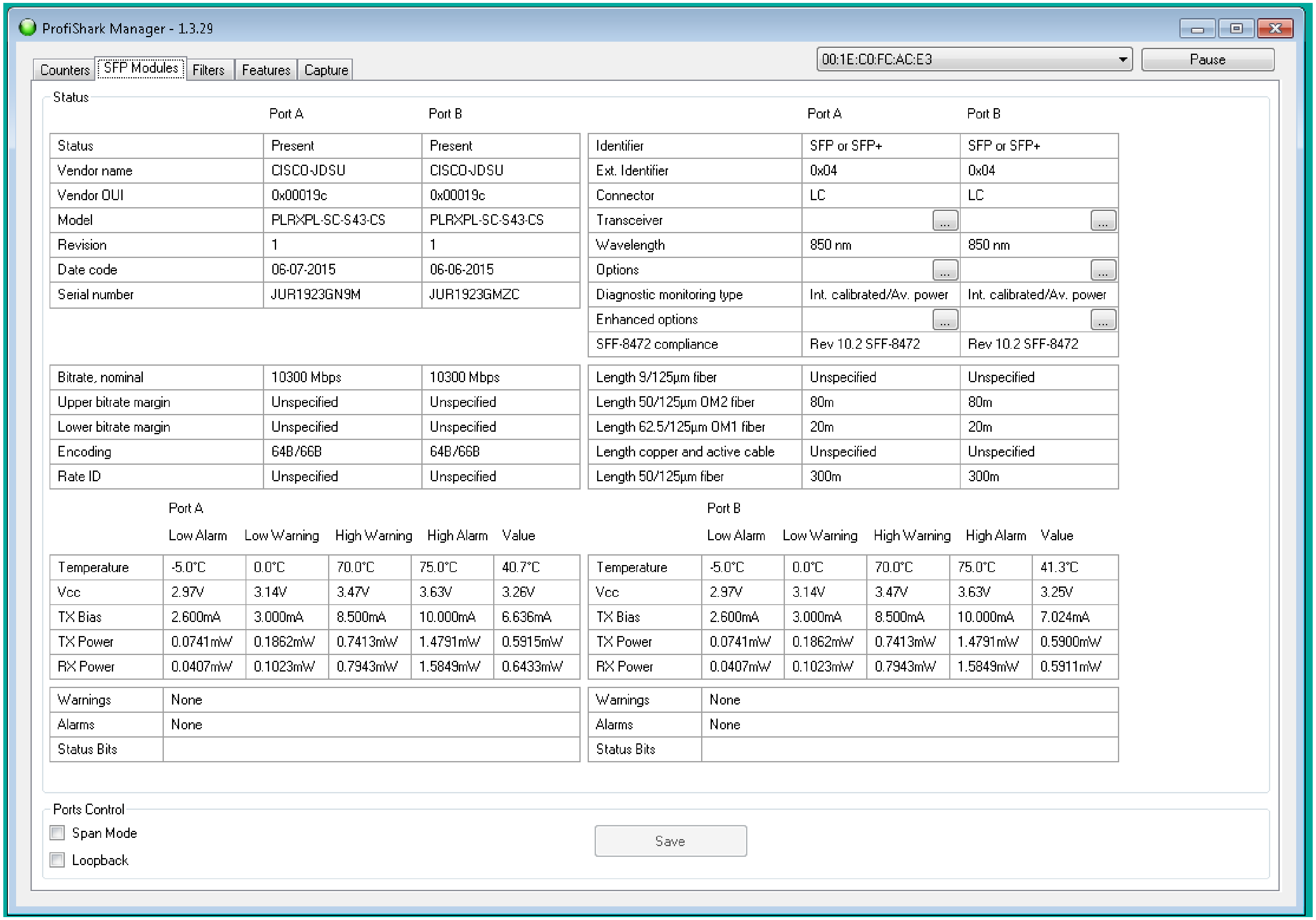
Packet size : Don't care 0

Figure 25: Editing Counter 8 Example 2

In the above screenshot, I have excluded Broadcast and Multicast frames from counting (in addition, I have excluded IPv6 frames ... but I don't believe they would be counted anyway, as the IPv4 "10.128.105.68" criterion would have excluded them).

SFP Modules

ProfiShark Manager offers the most thorough view into SFP+ hardware of any interface I've ever seen. Here is the initial screen:



	Port A	Port B
Status	Present	Present
Vendor name	CISCO-JDSU	CISCO-JDSU
Vendor OUI	0x00019c	0x00019c
Model	PLRXPL-SC-S43-CS	PLRXPL-SC-S43-CS
Revision	1	1
Date code	06-07-2015	06-06-2015
Serial number	JUR1923GN9M	JUR1923GMZC

	Port A	Port B
Identifier	SFP or SFP+	SFP or SFP+
Ext. Identifier	0x04	0x04
Connector	LC	LC
Transceiver	...	...
Wavelength	850 nm	850 nm
Options	...	...
Diagnostic monitoring type	Int. calibrated/Av. power	Int. calibrated/Av. power
Enhanced options	...	...
SFF-8472 compliance	Rev 10.2 SFF-8472	Rev 10.2 SFF-8472

Bitrate, nominal	10300 Mbps	10300 Mbps
Upper bitrate margin	Unspecified	Unspecified
Lower bitrate margin	Unspecified	Unspecified
Encoding	64B/66B	64B/66B
Rate ID	Unspecified	Unspecified

Length 9/125µm fiber	Unspecified	Unspecified
Length 50/125µm OM2 fiber	80m	80m
Length 62.5/125µm OM1 fiber	20m	20m
Length copper and active cable	Unspecified	Unspecified
Length 50/125µm fiber	300m	300m

	Port A				
	Low Alarm	Low Warning	High Warning	High Alarm	Value
Temperature	-5.0°C	0.0°C	70.0°C	75.0°C	40.7°C
Vcc	2.97V	3.14V	3.47V	3.63V	3.26V
TX Bias	2.600mA	3.000mA	8.500mA	10.000mA	6.636mA
TX Power	0.0741mW	0.1862mW	0.7413mW	1.4791mW	0.5915mW
RX Power	0.0407mW	0.1023mW	0.7943mW	1.5849mW	0.6433mW

	Port B				
	Low Alarm	Low Warning	High Warning	High Alarm	Value
Temperature	-5.0°C	0.0°C	70.0°C	75.0°C	41.3°C
Vcc	2.97V	3.14V	3.47V	3.63V	3.25V
TX Bias	2.600mA	3.000mA	8.500mA	10.000mA	7.024mA
TX Power	0.0741mW	0.1862mW	0.7413mW	1.4791mW	0.5900mW
RX Power	0.0407mW	0.1023mW	0.7943mW	1.5849mW	0.5911mW

Warnings	None
Alarms	None
Status Bits	

Warnings	None
Alarms	None
Status Bits	

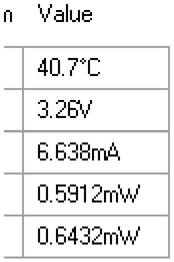
Ports Control

☐ Span Mode

☐ Loopback

Figure 26: SFP+ Hardware Overview

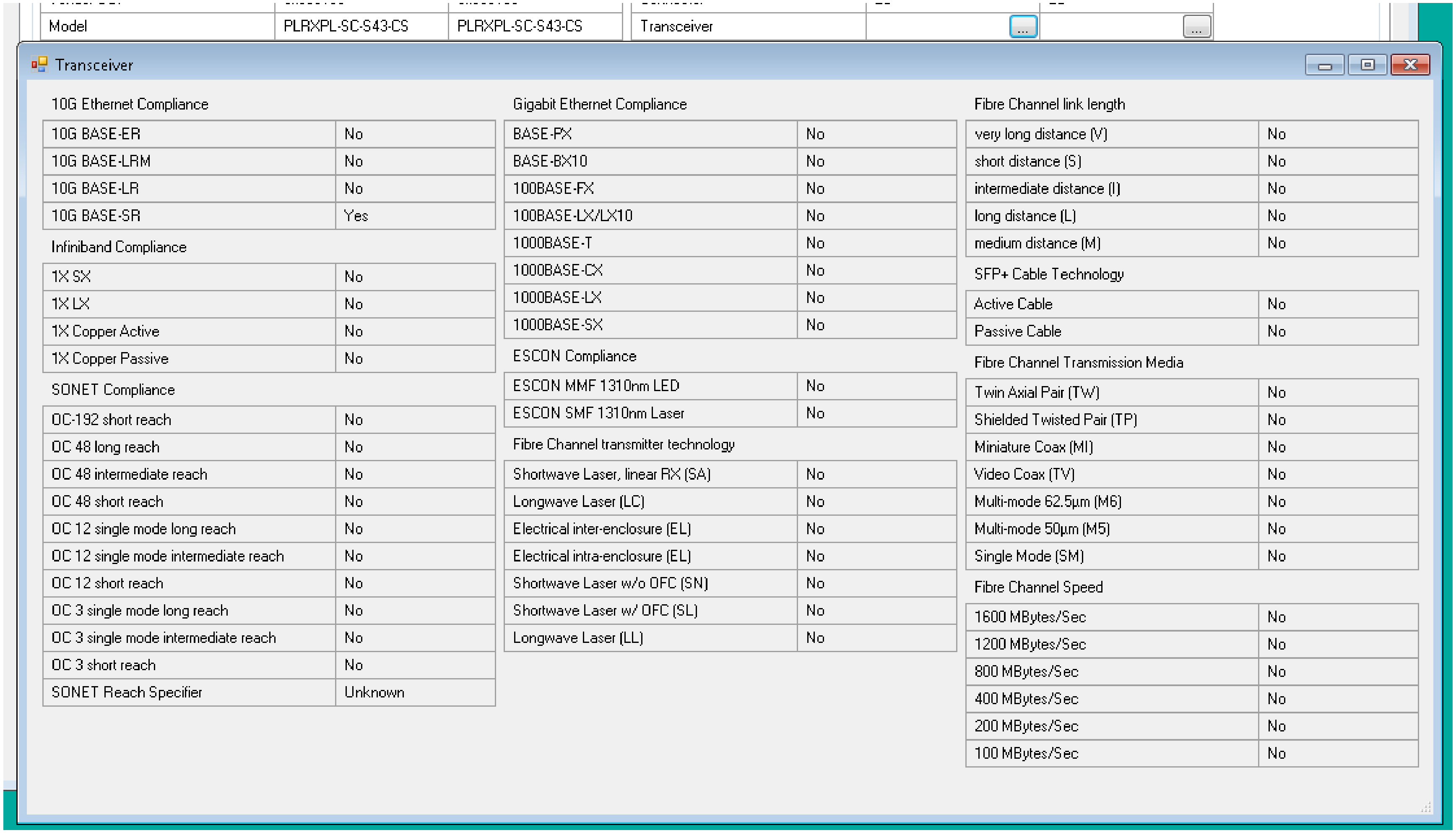
Note that the Values for Temperature, Vcc, TX Bias, TX Power, and RX Power are dynamic -- changing in real-time.



n	Value
	40.7°C
	3.26V
	6.638mA
	0.5912mW
	0.6432mW

Figure 27: SFP+ Dynamic Monitoring

Clicking on the Transceiver button produces the following view:



Model	PLRXPL-SC-S43-CS	PLRXPL-SC-S43-CS	Transceiver	...	...

Transceiver

10G Ethernet Compliance

10G BASE-ER	No
10G BASE-LRM	No
10G BASE-LR	No
10G BASE-SR	Yes

Infiniband Compliance

1X SX	No
1X LX	No
1X Copper Active	No
1X Copper Passive	No

SONET Compliance

OC-192 short reach	No
OC 48 long reach	No
OC 48 intermediate reach	No
OC 48 short reach	No
OC 12 single mode long reach	No
OC 12 single mode intermediate reach	No
OC 12 short reach	No
OC 3 single mode long reach	No
OC 3 single mode intermediate reach	No
OC 3 short reach	No
SONET Reach Specifier	Unknown

Gigabit Ethernet Compliance

BASE-PX	No
BASE-BX10	No
100BASE-FX	No
100BASE-LX/LX10	No
1000BASE-T	No
1000BASE-CX	No
1000BASE-LX	No
1000BASE-SX	No

ESCON Compliance

ESCON MMF 1310nm LED	No
ESCON SMF 1310nm Laser	No

Fibre Channel transmitter technology

Shortwave Laser, linear RX (SA)	No
Longwave Laser (LC)	No
Electrical inter-enclosure (EL)	No
Electrical intra-enclosure (EL)	No
Shortwave Laser w/o OFC (SN)	No
Shortwave Laser w/ OFC (SL)	No
Longwave Laser (LL)	No

Fibre Channel link length

very long distance (V)	No
short distance (S)	No
intermediate distance (I)	No
long distance (L)	No
medium distance (M)	No

SFP+ Cable Technology

Active Cable	No
Passive Cable	No

Fibre Channel Transmission Media

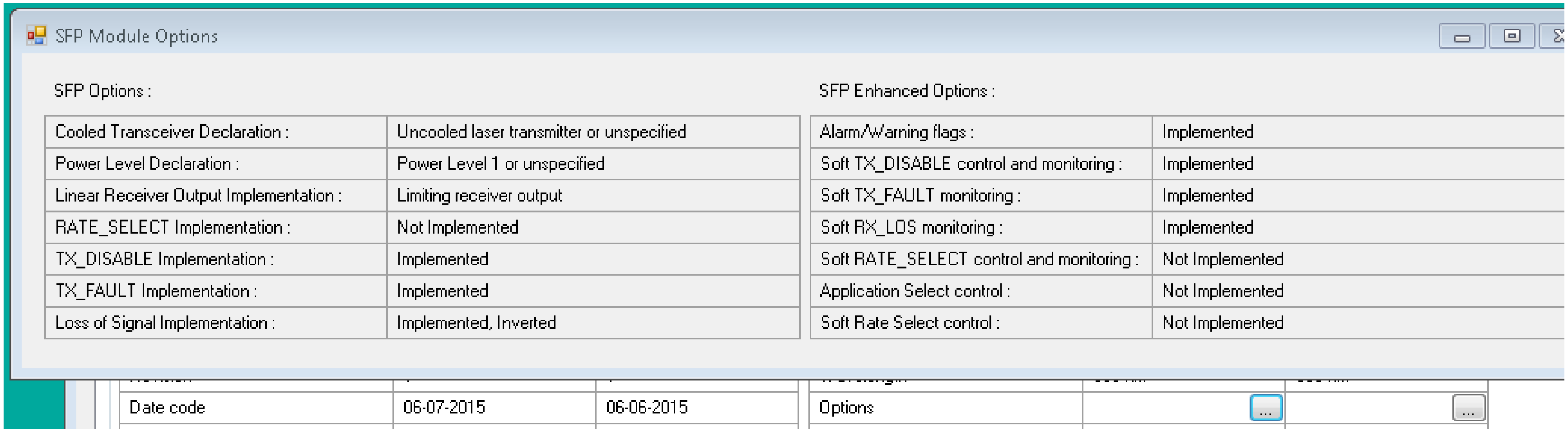
Twin Axial Pair (TW)	No
Shielded Twisted Pair (TP)	No
Miniature Coax (MI)	No
Video Coax (TV)	No
Multi-mode 62.5µm (M6)	No
Multi-mode 50µm (M5)	No
Single Mode (SM)	No

Fibre Channel Speed

1600 MBytes/Sec	No
1200 MBytes/Sec	No
800 MBytes/Sec	No
400 MBytes/Sec	No
200 MBytes/Sec	No
100 MBytes/Sec	No

Figure 28: SFP+ Transceiver Details

Clicking on the Options... button produces this:



SFP Options :

Cooled Transceiver Declaration :	Uncooled laser transmitter or unspecified
Power Level Declaration :	Power Level 1 or unspecified
Linear Receiver Output Implementation :	Limiting receiver output
RATE_SELECT Implementation :	Not Implemented
TX_DISABLE Implementation :	Implemented
TX_FAULT Implementation :	Implemented
Loss of Signal Implementation :	Implemented, Inverted

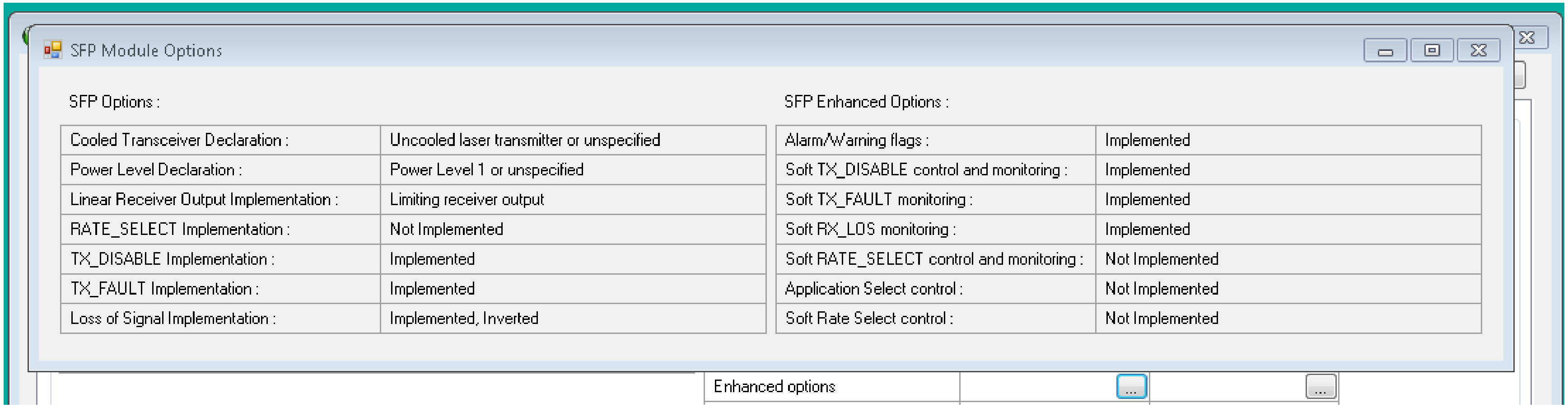
SFP Enhanced Options :

Alarm/Warning flags :	Implemented
Soft TX_DISABLE control and monitoring :	Implemented
Soft TX_FAULT monitoring :	Implemented
Soft RX_LOS monitoring :	Implemented
Soft RATE_SELECT control and monitoring :	Not Implemented
Application Select control :	Not Implemented
Soft Rate Select control :	Not Implemented

Date code	06-07-2015	06-06-2015	Options	...	...

Figure 29: SFP+ Options

And clicking on the Enhanced options... button produces this:



SFP Options :

Cooled Transceiver Declaration :	Uncooled laser transmitter or unspecified
Power Level Declaration :	Power Level 1 or unspecified
Linear Receiver Output Implementation :	Limiting receiver output
RATE_SELECT Implementation :	Not Implemented
TX_DISABLE Implementation :	Implemented
TX_FAULT Implementation :	Implemented
Loss of Signal Implementation :	Implemented, Inverted

SFP Enhanced Options :

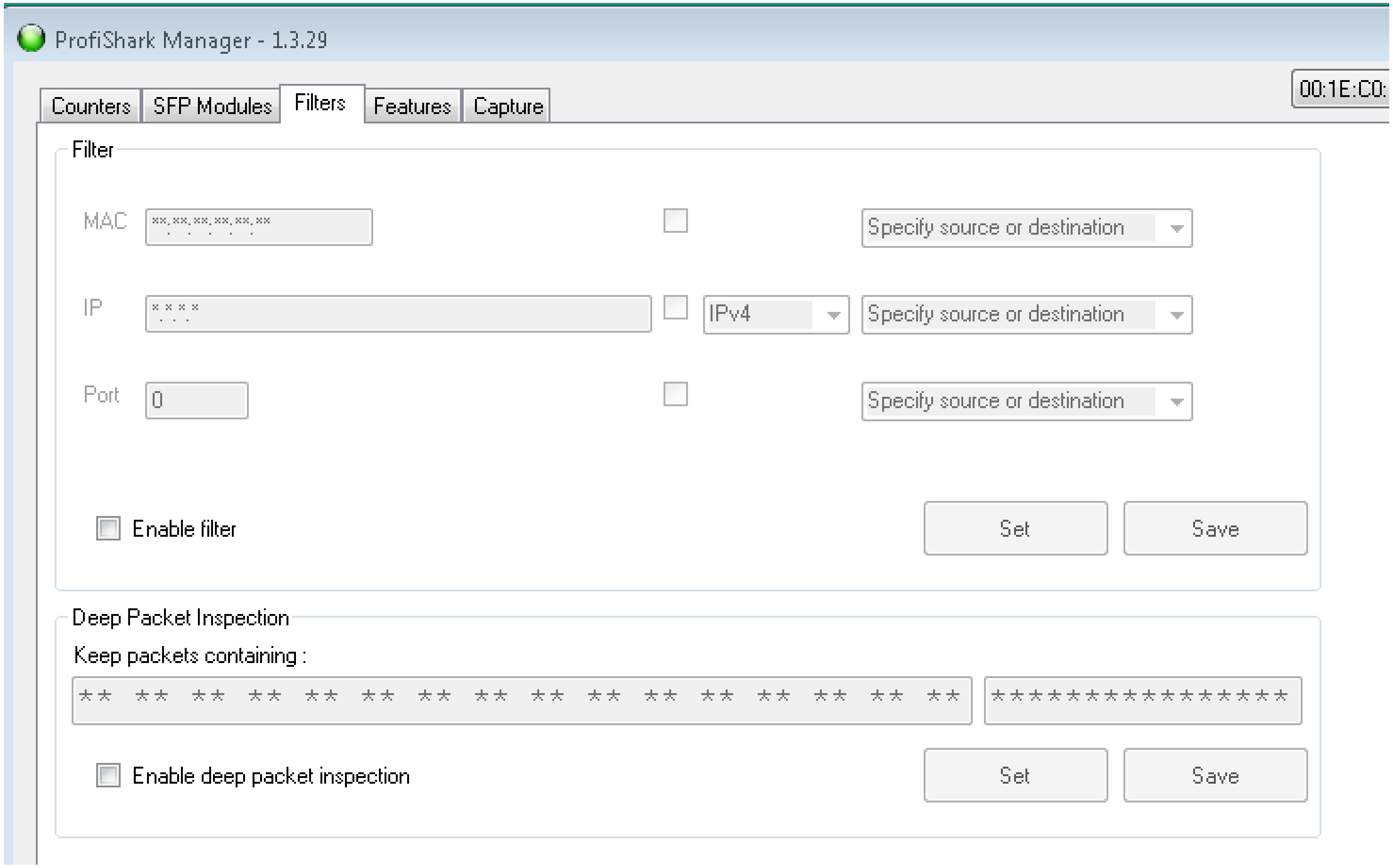
Alarm/Warning flags :	Implemented
Soft TX_DISABLE control and monitoring :	Implemented
Soft TX_FAULT monitoring :	Implemented
Soft RX_LOS monitoring :	Implemented
Soft RATE_SELECT control and monitoring :	Not Implemented
Application Select control :	Not Implemented
Soft Rate Select control :	Not Implemented

Enhanced options	...	...

Figure 30: SFP+ Enhanced Options

Filters

The next ProfiShark Manager tab is Filters, which offers the usual MAC and IP-based filter options, along with TCP / UDP Port filtering. In addition, this Tap supports free text filtering, called *Deep Packet Inspection*, which allows you to capture frames which match any string whatsoever.



Filter

MAC **:**:**:**:**:** ☐ Specify source or destination

IP *.*.*.* ☐ IPv4 Specify source or destination

Port 0 ☐ Specify source or destination

☐ Enable filter

Deep Packet Inspection

Keep packets containing :

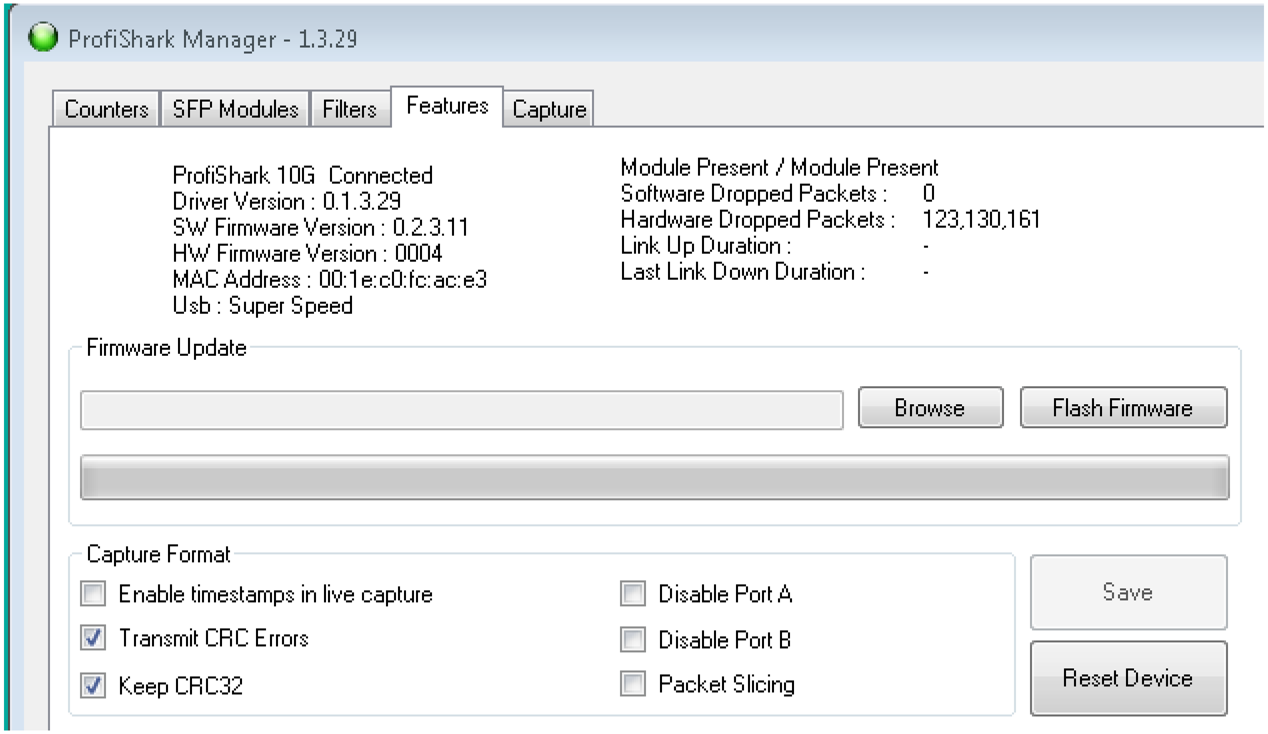
** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ****************

☐ Enable deep packet inspection

Figure 31: Filters

Features

The Features tab provides a miscellaneous collection of information & functions, including the firmware update facility and ways to control the options around capture.



ProfiShark 10G Connected
Driver Version : 0.1.3.29
SW Firmware Version : 0.2.3.11
HW Firmware Version : 0004
MAC Address : 00:1e:c0:fc:ac:e3
Usb : Super Speed

Module Present / Module Present
Software Dropped Packets : 0
Hardware Dropped Packets : 123,130,161
Link Up Duration : -
Last Link Down Duration : -

□ Enable timestamps in live capture
☑ Transmit CRC Errors
☑ Keep CRC32
□ Disable Port A
□ Disable Port B
□ Packet Slicing

Figure 32: Features

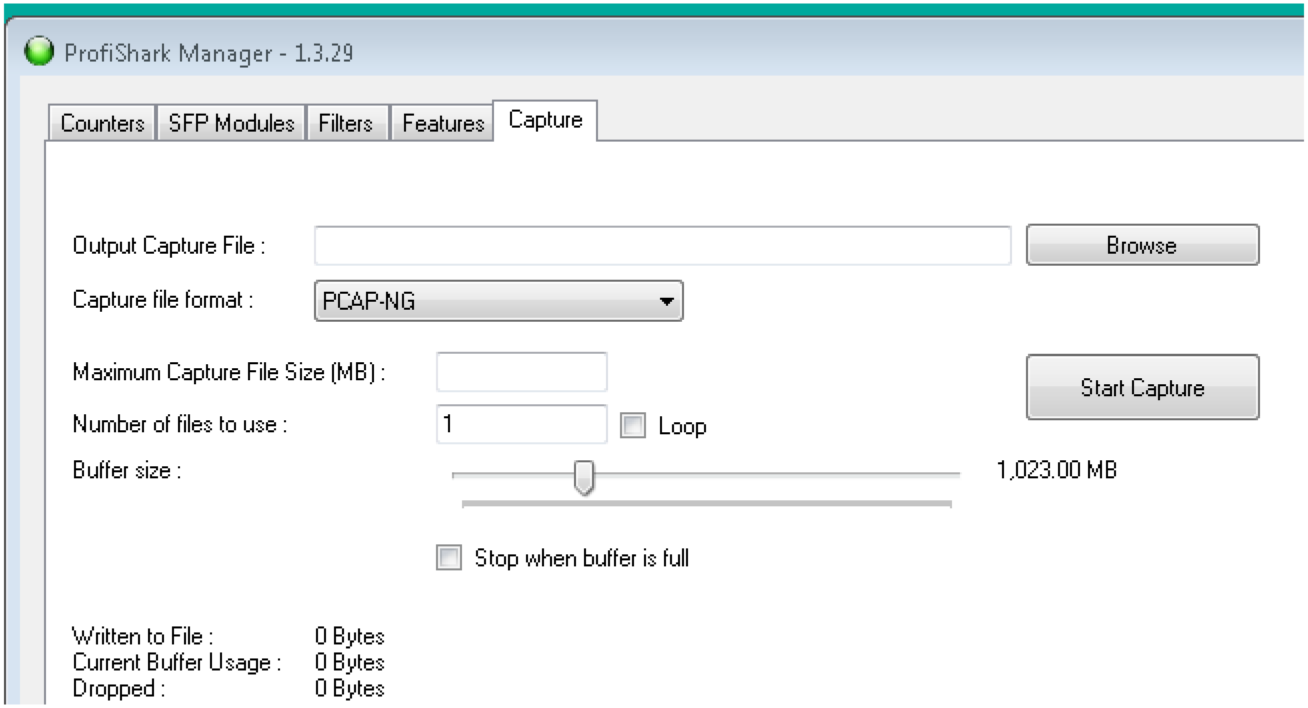
1. *Enable timestamps in live capture* invokes the Tap's on-board clock to deliver timestamps with 8ns resolution.
2. *Transmit CRC Errors* instructs the Tap to forward Ethernet frames whose CRC trailers do not correctly summarize the frame's contents. This allows us to choose whether or not to keep damaged frames.
3. *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. This allows us to choose whether or not we want to examine the Ethernet CRC.
4. *Disable Port A/B* allows you to capture in a single direction -- useful if you want to verify the direction from which a given frame or conversation is arriving.

5. *Packet Slicing* currently slices frames to 128 bytes, to allow you to conserve IO and disk space. ProfiTap plans to offer more granular control in a future software release.

Recall that your average Wireshark experience cannot see CRC Errors, as the typical NIC drops such frames before analyzers like Wireshark ever see them. Ditto with the Ethernet CRC32 -- the average NIC strips this before forwarding the frame deeper into your laptop, where libpcap / winpcap picks it up.

Capture

And here is another view of the Capture tab, a more detailed view of which we saw earlier in this document.



Output Capture File :

Capture file format : PCAP-NG

Maximum Capture File Size (MB) :

Number of files to use : 1 ☐ Loop

Buffer size : 1,023.00 MB

☐ Stop when buffer is full

Written to File : 0 Bytes
Current Buffer Usage : 0 Bytes
Dropped : 0 Bytes

Figure 33: Capture

Summary

As of this writing, the ProfiTap-10G (and 1G) offer 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. This collection of Taps also offer the added bonus of portability -- since it fits into my laptop bag, I am more likely to have it with me when I run into situation wanting packet capture. In addition, the bundled ProfiShark Manager application offers various ways to summarize statistics and to log events on the capture stream, offering quick insights into the traffic stream, prior to your cracking open a pcap to dig deeper.