

VISIT WWW.PROFITAP.COM



### MEGUMI TAKESHITA

#### ,IKERIRI NETWORK SERVICE CO.,LTD.

Megumi Takeshita, known as Packet Otaku, runs a packet analysis company after having worked as a network analyst at BayNetworks and Nortel Networks for many years. Ikeriri Network Service is a reseller of Riverbed, Metageek, Profitap and other packet capture products in Japan. Megumi has written more than 10 books about packet analysis and deep inspection using Wireshark in Japanese.

WWW.IKERIRI.NE.I

### CONTENT

Importance of hardware capturing	2
ProfiShark series products	2
ProfiShark 1G/1G+ hands on	2
Long term traffic capture	4
Long term capture solution hands on	4

## IMPORTANCE OF HARDWARE CAPTURING

There are many troubles and security problems in today's internet. However, it is difficult to determine the source of these problems by commands and log files alone. This is why packet based analysis is the good way to analyze the issue. Another option is using flow based technologies, but they are not the best. For example: sampling based analysis (iFlow, sFlow, etc.) loses a part of actual traffic. Especially, small packets with short timing, like 64 bytes frames tend to be omitted by sampling. These are TCP SYN, TCP FIN, TCP ACK without data, small ICMP ping, and so on.



So non-sampling capturing is important to analyze the traffic. But an ordinary NIC like the e1000 (Intel Pro 1000) is not good at capturing line rate speeds. So if you use typical Windows PC and capture 64 bytes frames, 140Mbps is the actual rate, because ordinal NIC is controlled by mainly software to create trace file. So CPU usage and packet drop rate is rising at over-140Mbps traffic. You may capture over 90% if the average frame size is about 1500bytes, but you can capture full packets at 430Mbps when the frame size is 200 byte.



Another problem is the time. If you use Wireshark to capture packets in Windows environments, Wireshark doesn't create any time stamps itself, but simply gets them. A capture driver (such as WinPcap, NPcap, libpcap) sets the time and the accuracy depends on Windows time system call. The precision is different from the environment, but it is not by nanosecond, but a couple of microseconds or

Wireshark timestamp accuracy

https://osqa-ask.wireshark.org/questions/2010/wireshark-timestamp-accuracy

Synchronization of time in many different systems may cause the trace file problems with the timestamping. So capturing packets with good time accuracy is very important for analysis.

So we need hardware-based capture device. The hardware-based capture device is a kind of capture driver accelerator; it has their own memory and FPGA for capturing and processing MAC. also, it creates a trace file directly and communicates with the PC. ProfiShark providea a non-sampling, full-capturing solution. This type of hardware-based capture devices is essential in enterprise networks, such as a backbone network crammed with tons of packets with frames sizes ranging from 64bytes to jumbo frame.

### PROFISHARK SERIES

I am a reseller of Profitap as well as an eager fan of ProfiShark series. The ProfiShark series is one of the best hardware capture solutions in the world. Since 2014, I've made use of the ProfiShark series in daily troubleshooting and investigation. And Ikeriri Network Series also resells the series of ProfiShark for the Japanese market.



ProfiShark series consists of the ProfiShark 100M, ProfiShark 1G, ProfiShark 1G+, ProfiShark 10G and ProfiShark 10G+. They all use common USB3 interface but capture interfaces and GPS/PPS function are different per model.



MODEL	PROFISHARK 100M	PROFISHARK 1G	PROFISHARK 1G+	PROFISHARK 10G	PROFISHARK 10G+
Capture int.		2 x RJ-45		2 x S	)FP+
PC Interface		USB3 ( direct (	capture to disk support ]	) *power supply	
Other interface	5VDC(opt)	5VDC(opt)	5VDC(opt) 2xSMA female (GPS/PPS)	5VDC(opt)	5VDC(opt) 2xSMA female (GPS/PPS)
Mayor function	Ideal for both regular Ethernet and Real-Time Industrial Internet	Full-duplex wirespeed capture SPAN and In-Line modes Hardware timestamping (+model:GPS timestamping) Low level error monitoring PoE support		Full-duplex SPAN and In Hardware ti (+model:GPS t Low level err Hardware filterir	fiber capture -Line modes mestamping imestamping ) or monitoring ng packet slicing
Direct Capture		Compatible w	ith all Intel based Synolo	ogy NAS system	

Many hardware capture device are a kind of specialized NIC card, This means we need to create our own Packet Capture Device, set up OS and determine the settings and customize for reliable and stable capturing. Sometimes it takes a lot of time to set up a capture PC. We need to attach the NIC and configure many detail settings of the OS service and applications.

ProfiShark is a USB3 device, not the NIC style device, so it is not connected with PC deeply and independent from the capture PC. This saves a lot of time and cost to use. We just connect ProfiShark with USB3 interface.

ProfiShark has two interface types (RJ-45 or SFP+), these interfaces can be used as two different capture interfaces (with hardware aggregation) and also as one port for the uplink and the other for the downlink (a.k.a. In-Line modes).

USB3 bandwidth is 5Gbps, which is enough for wirespeed capturing with ProfiShark1G/1G+. The USB3 interface is also used for power supply. So a bundled USB3 cable is the only thing you need to start capturing.

As Mentioned before, time accuracy in packet capturing is one of the problems in enterprise analysis, because the precision depends on capture driver and OS environment with ordinal NIC.

ProfiShark provides 8ns hardware timestamping (all models) and 16ns precision with GPS through SMA connector for GPS/PPS (Plus models).

### PROFISHARK 1G/1G+ HANDS ON

To use the ProfiShark for the first time, we need to install the driver. You can use the USB drive bundled with ProfiShark or get the newest driver and tools from the Profitap website. In this case we install driver on Windows10 pro (64bit).

#### STEP 1: LOCATING INSTALLATION FILES

Open USB key>Windows->Profishark\_1.2.18.exe ( I recommend with administrator privilege )

USBKEY Profishark 1G - 0015			U	BKEY Profishark 1G - 0015 → Windows			
	名前 ^	更新日時	_	A		2 m . 1 m	
		2018/05/28 20:11		名前	更新目時	裡題	サイズ
7	📙 Linux	2018/05/28 20:11		🐷 Drofishark 1218 eve	2015/12/23 13:40	マゴリケーション	72.0
Я	📙 Windows	2018/05/28 20:11	1	Fronshark_hetrolexe	2010/10/2010/40	7777 747	10,0
*	🗃 Installation.txt	2014/11/26 13:21		ProfiShark_Wireshark_1.12.x-dissector_1	2015/05/13 11:25	ZIP ファイル	
*	📩 ProfiShark 1G Manual v2.3.pdf	2015/11/27 15:43	٢				

Figure 3-1: ProfiShark USB Key

### STEP 2: PROFISHARK MANAGER INSTALLATION

/ ProfiShark Manager - Instal	IShield Wizard $ imes$	EE Windows セキュリティ	×
<u>ح</u>	Welcome to the InstallShield Wizard for ProfiShark Manager	このデバイス ソフトウェアをインストールしますか? を前: Cypress ユニバーカル シリアル バス ユントローラー デ 用 行力: Cypress Semiconductor Corporation	
	The InstallShield(R) Wizard will install ProfiShark Manager on your computer. To continue, click Next.		ストールしない(N) 17を利断する方法
2	WARNING: This program is protected by copyright law and international treaties.	□□ Windows 2年3リディ × このデバイス ソフトウェアをイソストールしますか? 電影: Pochtap ネットワーク アダプター 発行力: Com Carlt	
	<back next=""> Cancel</back>	○ "Com Cait' からのソフトウェアを素に虚構す 3(A) インストール0 インストール4000 ① 復興する執行元からのドライバーソフトウェアのみモインストールしてください。安全にインストールできか行くス ソフトウスアモを損用するカム	

Figure 3-2: ProfiShark Manager

Figure 3-3: Driver installs warning

Click next to install ProfiShark Manager (management program for the ProfiShark Series)

#### ▶ Note: You need to click "install" button in device driver install warning screen.

Please disconne	ect your Profishark device	×
Please disconn	nect your Profishark device	
Note : If you sk	kip this step, vou will not be able to use vou Pro	ofiShark device until the computer is rest
		Skin
		JKIP

Note: If you have already connected ProfiShark, you need to disconnect ProfiShark and connect again to proceed

#### STEP 3: LAUNCHING THE MANAGER

				INVADANDO I	- Parm
and the log	Peolants Capiture				
RADIES CIRCUIS	191.4				
Own-MI		Tatel	East C/D	Perinter	
	VMI (white				ALL DESCRIPTION OF THE PARTY OF
Cas A	0.04				ALC: N. M.
	68 × 1020				A
Cas B	2102				A An Advantation 10
	Toldbybe				1
	Prind Income	•	•		
	104				Acres Acres
	68 - 1020				L
	> 802				Argenter Charles A Concerne X
	Part B				
		Tahl	Face (7.0	Percentary	
	Validated are				ALC: NOT THE OWNER OF THE OWNER OWNER OF THE OWNER
	104				A R M H R
	64 - 1020				A
	1981				S
	Tuicket				an o the second states
	Broad and particular		*		
	6.64				Ann Ann
	68 = 1020				6
	1 8181				Angewhalt-Dags A CRC arrist \$
	7 Plant				

Course: Danks in Contract (Contract Contract Con
Netline Kafeynet De Anne State
Tawar Julian Dawar Mauji Franan Capita Rawar
Dever Pauli Fornae Calus Rund
Capture Konset
Capitas Pontol
Disease transmission in a capital in the capital in
E ree cació

Launch ProfiShark Manager and click Features tab, check the message "ProfiShark 1G or 1G+ connected". In this dialog, you can flash the firmware too.

### STEP 4: TIMESTAMPING SETTINGS

Ó

 $\bigcirc$ 

If you want to use hardware timestamping, check "Enable timestamps in live capture" under the Capture Format group in the Features tab. And you also set "Transmit CRC Errors", "Keep CRC32" and other settings in this screen.

Capture Format	
Enable timestamps in live capture	🗌 Disable Port A
Iransmit CRC Errors	🗌 Disable Port B
Keep CRC32	Packet Slicing

Figure 3-6: Capture Format group in Features tab

#### STEP 5: CONNECTING THE PROFISHARK



We use in-line mode with fail safe, connect upstream link and downstream link to each RJ-45 port (port A and port B)

Figure 3-7: in-line mode with fail safe connection

### STEP 6: STARTING THE CAPTURE

The ProfiShark 1G is recognized as a network adapter. To avoid any useless management packet, I recommend checking off all protocols of network in ProfiShark adapter.





Figure 3-8: Adapter option and properties of ProfiShark NIC adapter

ProfiShark has 2 types of Capture Driver, ProfiShark Live Capture Driver and ProfiShark Direct Capture Driver. The difference is as follows, I recommend using Direct Capture Driver for stability, but if you want to use ProfiShark to capture live to the interface of Wireshark, ProfiShark Live Capture Driver is the right option.

PROFISHARK NIC CAPTURE DRIVER	PROFISHARK DIRECT CAPTURE DRIVER
Start capturing using Wireshark, tshark, dumpcap and other application as usual	Start capturing using Capture tab of ProfiShark Manager
<b>キャプチャ</b> …このフィルタを利用: VMware Network Adapter VMnet8 <u></u> Npcap Loopback Adapter <u></u> VMware Network Adapter VMnet1 <u></u> Wi-Fi 6 <u></u> <u>{</u> <u>1-サネット</u> <u></u>	
ProfiShark NIC Capture Driver	ProfiShark Direct Capture Driver
<ul> <li>Network Driver (NDIS)</li> </ul>	• Trace file (pcapng/pcap) in SSD/HDD
• Capture Driver (WinPcap etc.)	• Wireshark
<ul> <li>● Wireshark</li> </ul>	

Now open the Capture tab in ProfiShark Manager. Click Browse button to set Output Capture File, and choose Capture file format from PCAP-NG, PCAP Nanosecond and ERF, set Maximum Capture File Size (MB), Number of files to use, and other settings. Push "Start Capture" button to capture packets!

ProfiShark Manager - 1.2.18	
Counters Charts Log Features Capture	
Output Capture File : C¥Users¥megumi]KERIRWDesktop¥fullcapture.pcapng Capture file format : PCAP-NG ~ Maximum Capture File Size (MB) : 100 Number of files to use : 200 □ Loop	Browse Start Capture
Buffer size : 5	\$0.00 MB
Stop when buffer is full	
Written to File : 0 Bytes Current Buffer Usage : 0 Bytes Dropped : 0 Bytes	

Figure 3-9: Capture tab in ProfiShark Manager

#### STEP 7: STATISTICS

 $\cap$ 



When you capture using ProfiShark Direct Capture Driver, you can check dynamic statistics in Charts tab and configure log information in Log tab.

Now we got non-sampling, full-capture trace files!

Note: Profitap also provides dissector plugin of Wireshark (Windows (x64/x86) / Linux) so you can copy unzipped profishark.dll into global plugin folder of Wireshark.

- [ profishark-dissector-linux.zip
- 📔 profishark-dissector-windows.zip



Figure 3-10: Charts tab in ProfiShark Manager

# LONG TERM TRAFFIC CAPTURE

Sometimes, we cannot find the key of the problem from just a small trace file. For example, we may find the trends of traffic and discover traffic anomaly from many trace files for a month. Sometimes we need to look for the security problem from huge forensics trace files. Long term traffic capture is important for troubleshooting and security investigation in these situations.

However, bringing a packet analysis PC into enterprise network is not an option. A PC (Windows or Linux) has a lot of vulnerabilities such as OS security, many interfaces such as Wi-Fi, Wired and USB, and application problems. So using a ProfiShark with PC in customer's network is difficult, because security cannot be guaranteed.

Another problem is stability and reliability for long-term traffic capture. Using the Wireshark GUI is not suitable for long-term capturing, but tshark CLI application has many functions. Using dumpcap command is one of the good ways.

For example, if you want to capture and create hourly file which name is "test\_xxxxx\_yyyymmddhhmmss.pcapng" (xxxxx: sequence number y:year m:month d:day h:hour m:minute s:second) for a month (720 files ) then stop capturing. The command is below.

#### dumpcap -i 1 -s 400 -b duration:3600 -a files:720 -w test.pcapng

NOTE -i: interface index, -s: snaplen (bytes), -b multiple file option (duration: seconds by each file), -a autostop option, -w write file path

But using PC is not the best way for long term traffic capture, because we need to change storage such as SSD/HDD. And waking up troubleshooting PC for a month without crash and reboot is difficult. Do you think it works?

That's why Profitap has a nice solution, ProfiShark supports all Intel based Synology NAS systems! We can capture, create and transfer trace files to NAS without PC. The NAS has a huge storage as well as fault tolerance such as RAID.

A NAS is much stable than a PC and you do not need a lot of time and money to build capture system for long-term analysis. The only thing you have do is just connecting a USB3 cable from ProfiShark to an Intel based Synology NAS system.





Figure 4-1: connecting a NAS to the ProfiShark

Off course you can utilize full function of ProfiShark, use ringbuffer or normal capture mode, and split capture to different files based on time and size. And more, ProfiShark with NAS solution has good statistics screens with pie charts and histograms for long term traffic

Figure 4-2: ProfiShark with NAS solution

## LONG TERM CAPTURE SOLUTION HANDS ON

Let's start the hands-on of longterm capture solution. There is a ProfiShark 1G connected with a Synology NAS. All configurations are done in the WebUI of NAS.

Note: we use demo site of ProfiShark NAS solution.

### STEP 1: LOGIN

Login into Synology NAS via WebUI, then click top-left menu button to access ProfiShark icon. It appears ProfiShark window.



			Profis	hark	7 -
Capture status					Kandwidth unopr
evice status: Corn	exted Profishar8-334	5 (d) (0) 29 9d ec al)			Part A
aptara status: Stops	and				200
tai lact.ret. 01-6	*1				25
rispond by software O but	ri.				()
Bat rober Brouches			Packets court		
					Notes Data
<ul> <li>Device Configuration</li> </ul>					+8000
inimeports Sking: 1					2000
					Lacco
Capture configuration					Port A packets size Port 8 packets si
lotare direttory 2015	ure Select director	Con start			
Prine buffer			E - 1718		
asimum files 200	0				
admonstile size (in MS) 100		Est size on disk 197,54.0	bottes		
avenum Ne duration: 00	* : 00 * :	00 ¥			110.30% 100.31%
\$ 188969C6					
	POTATION	NAM	Port & total	PORt 6 /8	
byset.	1.47 Chiften	12.16.9/bytes/e	1.47 Objtes	12 16 Whytwo/a	
Valid Fackots	7,089,374	63,735/5	7,892,374	63,735,%	
Invalid Packets	0	6/4		0/4	
Include with pick < 6.4	6	6/9		0/9	
facility with size between 64 a .	7,889,374	63,735/5	2,889,824	63,7965	
Package with size > 1518		6/4		0/4	
Dollasiona	0	6/5		0/5	
ORC errors		6/6		0,4	
atter	4	6/8		2.4	

Figure 5-2: ProfiShark window

#### STEP 2: CAPTURE STATUS

Check Capture status in ProfiShark window. This time "Connected Profishark-1Gv5" is shown in Device status, and we can check capture status, total captured bytes, and so on. You can also control capturing by pushing the 'Start capture' and 'Stop capture' buttons. And if you want to set specified inline ports and Slicing, you can set in Device Configuration section.

▲ Capture status				
Device status: Connected Profishark-16v5				
Capture status: Stopped				
Total captured: 0 bytes				
Dropped by software: 0 bytes				
Start capture Stop capture				
∧ Device Configuration				
Inline ports Slicing :	1			

#### STEP 3: LONG-TERM CAPTURE SETTINGS

Ο

You can set long term capture settings in Capture configuration section. You can set the path of trace files in Capture directory. If you want to overwrite the oldest file, please check the checkbox for Ring buffer. You can set Maximum files, Maximum file size (in MB) and Maximum file duration. In this case we need to capture and create hourly trace files for a month in /capture directory. We set as below.

∧ Capture configuration					
Capture directory:	/capture Select director	У			
Ring buffer					
Maximum files:	720				
Maximum file size (in MB):	2000	Est. size on disk : 1.37 Tbytes			
Maximum file duration:	01 🕶 : 00 🕶 :	00 💌 Est. duration : 30d 0h 0m 0s			

Figure 5-4: Capture configuration section

#### STEP 4: LONG-TERM CAPTURE STATISTICS

You can also check dynamic statistics in Statics section as well as bar and pie chart in right window. The statistics tables are consists of Bytes, Valid Packets, Packets with size < 64, Packets with size between 64 and 1518, Packets with size > 1518, Collisions, CRC errors and Jabber by Port A total, Port A/s, Port B total and Port B/s. If you want to reset counters, just push the 'Reset statistics' button.

	Port A total	Port A /s	Port B total	Port B /s
Bytes	17.66 Gbytes	12.17 Mbytes/s	17.66 Gbytes	12.17 Mbytes/s
Valid Packets	94,816,138	63,797/s	94,816,138	63,797/s
Invalid Packets	1	0/s	2	0/s
Packets with size < 64	0	0/s	0	0/s
Packets with size between 64 a	94,816,138	63,797/s	94,816,138	63,797/s
Packets with size > 1518	0	0/s	0	0/s
Collisions	0	0/s	0	0/s
CRC errors	1	0/s	2	0/s
Jabber	0	0/s	0	0/s

Figure 5-5: Statistics section and Graph



### CONCLUSION

Profitap's ProfiShark series are the best hardware based packet capture solution in the world. We do not need a powerful and customized Desktop PC; we just bring a laptop to start non-sampling and full-capturing. In case of long term capturing, ProfiShark solutions with a Synology NAS provide enterprise monitoring at an incredible price!



# IT ALL STARTS WITH VISIBILITY

### **EPROFITAP**

Profitap develops a wide range of state-of-the-art and user-friendly network monitoring tools for both SMEs and the enterprise sector. Our wide range of highdensity network TAPs, field service troubleshooters and network packet brokers are extremely performant, providing complete visibility and access to your network, 24/7.

We've been creating monitoring solutions for network analysis and traffic acquisition for more than 33 years. Therefore, we are experts in our field and our award-winning ProfiShark® 1G stands to prove it. This lightweight, advanced and portable network TAP is one the most innovative products on the market.

With more than 1,000 clients from 55 countries, PROFITAP has become a must-have solution for many important businesses, many of which are among Fortune 500 companies.

#### PROFITAP HQ B.V. HIGH TECH CAMPUS 9 5656 AE EINDHOVEN THE NETHERLANDS

sales@profitap.com www.profitap.com

Profitap

@Profitap

profitap-international

Copyright Profitap, 04/2018, v1.0

in