PROFI TAP

REVIEW:

PROFISHARK LONG TERM CAPTURE

VISIT WWW.PROFITAP.COM

MEGUMI TAKESHITA

SYSTEMS ENGINEER AT ALLEN INSTITUTE

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, Dualcomm, 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

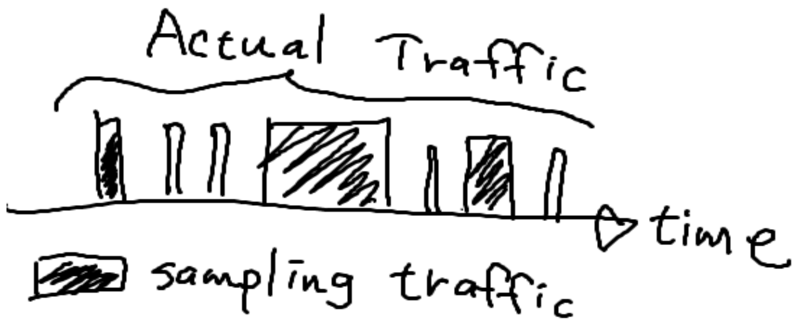
EXPERTISE:

WWW.IKERIRI.NE.JP

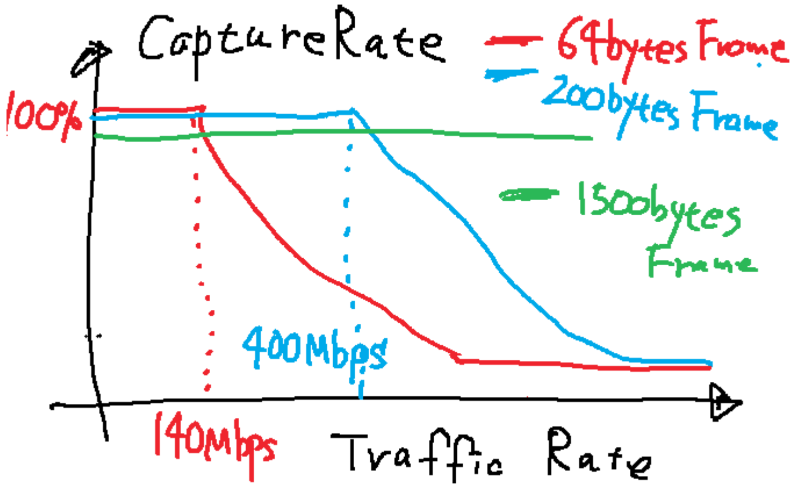
CONTENT

IMPORTANCE OF HARDWARE CAPTURING

There are many troubles and security problems in today's internet. But it is difficult to determine the conclusion by commands and log files. So packet based analysis is the good way to analyze the issue. But flow based technologies are not the best. For example sampling based analysis (iFlow, sFlow, etc.) loses a part of actual traffic. Especially, small packets uses short time, so 64 bytes frames are tends to omit by sampling. They 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 ordinal NIC like e1000 (Intel Pro 1000) is not good at full-capturing. 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, Capture driver (such as WinPcap, NPcap, libpcap) set 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

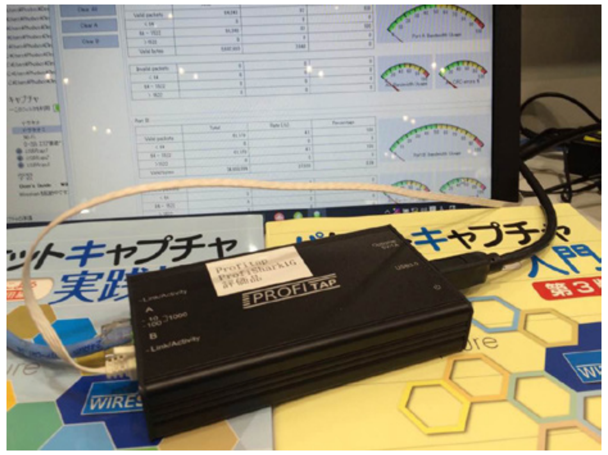
Wireshark timestamp accuracy
https://osqa-ask.wireshark.org/questions/2010/wireshark-timestamp-accuracy

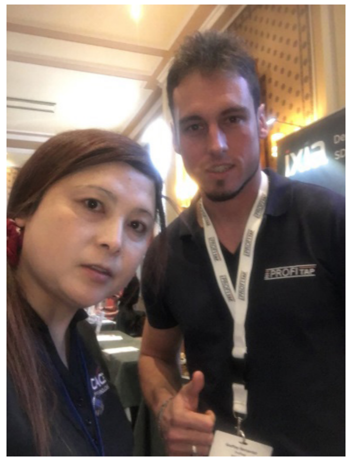
And synchronization of time in many systems may cause the trace file problem of time. So capturing packet with good time accuracy is also important for analysis.

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. And it creates trace file directly and communicate with PC. ProfiShark can provide non-sampling, full-capturing solution. Hardware-based capture device is essential in enterprise network, such as backbone network crammed with tons of packets those sizes is 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 are one of the best hardware capture solution in the world. I make use of old package version of ProfiShark since 2014 in daily troubleshooting, investigation. And ikeriri also resells the series of ProfiShark for Japanese customer.





ProfiShark series consists of ProfiShark1G, ProfiShark1G+, ProfiShark10G, ProfiShark10G+. They use common USB3 interface but capture interfaces and GPS/PPS function are different.

MODEL	PROFISHARK 1G	PROFISHARK 1G+	PROFISHARK 10G	PROFISHARK 10G+
Capture int.	2 x RJ-45		2 x SFP+	
PC Interface	USB3 (direct capture to disk support) *power supply			
Other interface	5VDC(opt)	5VDC(opt) 2xSMA female (GPS/PPS)	5VDC(opt)	5VDC(opt) 2xSMA female (GPS/PPS)
Mayor function	Full-duplex wirespeed capture SPAN and In-Line modes Hardware timestamping (+model:GPS timestamping) Low level error monitoring PoE support		Full-duplex fiber capture SPAN and In-Line modes Hardware timestamping (+model:GPS timestamping) Low level error monitoring Hardware filtering packet slicing	
Direct Capture	Compatible with all Intel based Synology NAS system			

Many hardware capture device is a kind of specialized NIC card, so we need to create our own Packet Capture Device, we set up OS and harden the settings and customize for reliable and stable capturing. Sometimes it takes a lot of time to set up capture PC. We need to attach the NIC and configure many detail settings of OS service and applications. But ProfiShark is USB3 device, not the NIC style. So it is not connected with PC deeply and is dependent from capture PC. It saves a lot of time and cost to use. We just connect ProfiShark with USB3 interface.

ProfiShark has 2 interface (RJ-45/SFP+), these interface can be used as 2 different capture interface (with hardware aggregation) and also as one is from the uplink and the other to the downlink (a.k.a. In-Line modes).

USB3 bandwidth is 5Gbps so it is enough for wirespeed capturing with ProfiShark1G/1G+ and USB3 interface is also used for power supply. So you need just a bundled USB3 cable to start capturing.

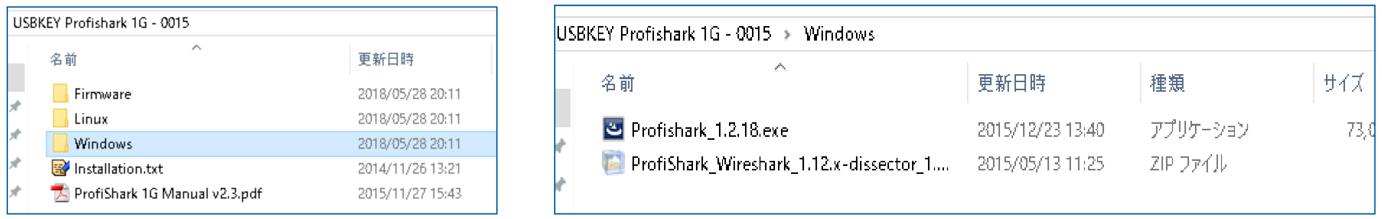
Time accuracy in packet capturing is one of the problems in enterprise analysis. And the precision depends on capture driver and OS environment with ordinal NIC. ProfiShark provides 8ns hardware timestamp (all model) and 16ns precision with GPS with SMA connector for GPS/PPS (Plus model).

PROFISHARK 1G/1G+ HANDS ON

At first we need to install the driver, you can use the USB drive bundled with ProfiShark or get the newest driver and tools from Profitap website. Now we try to install driver on Windows10 pro (64bit).

STEP 1

Open USB key>Windows->Profishark_1.2.18.exe (I recommend with administrator privilege)



USBKEY Profishark 1G - 0015

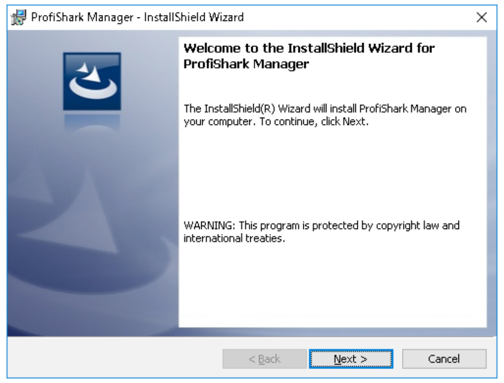
名前	更新日時
Firmware	2018/05/28 20:11
Linux	2018/05/28 20:11
Windows	2018/05/28 20:11
Installation.txt	2014/11/26 13:21
ProfiShark 1G Manual v2.3.pdf	2015/11/27 15:43

USBKEY Profishark 1G - 0015 › Windows

名前	更新日時	種類	サイズ
Profishark_1.2.18.exe	2015/12/23 13:40	アプリケーション	73,(
ProfiShark_Wireshark_1.12.x-dissector_1....	2015/05/13 11:25	ZIP ファイル	

Figure 3-1: ProfiShark USB Key

STEP 2



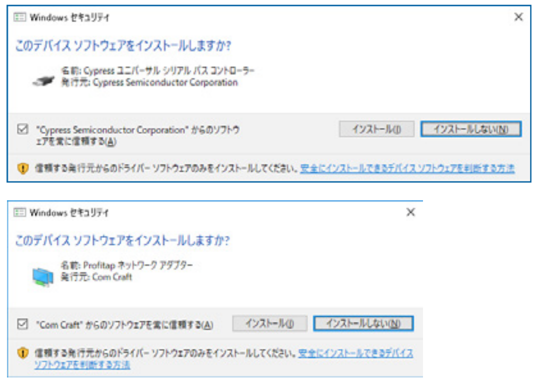
ProfiShark Manager - InstallShield Wizard

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 3-2: ProfiShark Manager



Windows セキュリティ

このデバイス ソフトウェアをインストールしますか?

名前: Cypress ユニバーサル シリアル バス コントローラー
発行元: Cypress Semiconductor Corporation

☑ "Cypress Semiconductor Corporation" からのソフトウェアを常に信頼する(A)

信頼する発行元からのドライバー ソフトウェアのみをインストールしてください。安全にインストールできるデバイス ソフトウェアを判断する方法

Windows セキュリティ

このデバイス ソフトウェアをインストールしますか?

名前: Profitap ネットワーク アダプター
発行元: Com Craft

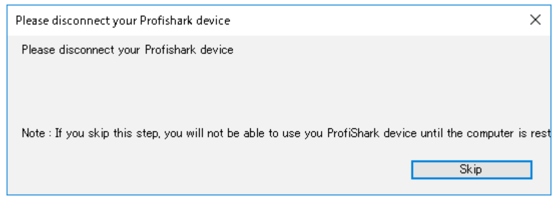
☑ "Com Craft" からのソフトウェアを常に信頼する(A)

信頼する発行元からのドライバー ソフトウェアのみをインストールしてください。安全にインストールできるデバイス ソフトウェアを判断する方法

Figure 3-3: Driver installs warning

Click next sometimes to install ProfiShark Manager (management program)

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



Please disconnect your Profishark device

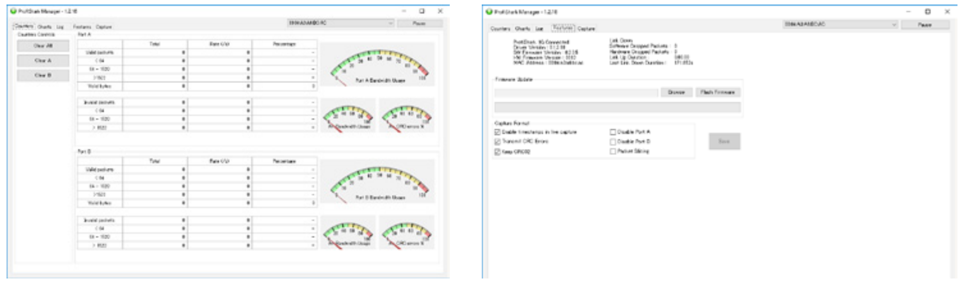
Please disconnect your Profishark device

Note : If you skip this step, you will not be able to use you ProfiShark device until the computer is rest

Figure 3-4: Warning dialog

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

STEP 3

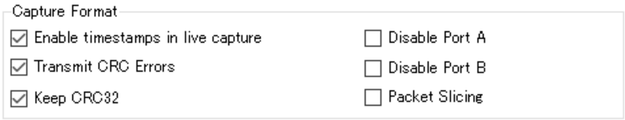


Launch ProfiShark Manager and click Features tab, check the message "ProfiShark 1G or 1G+ connected". In this dialog, you can flash the firmware too.

Figure 3-5: ProfiShark Manager Dialog

STEP 4

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

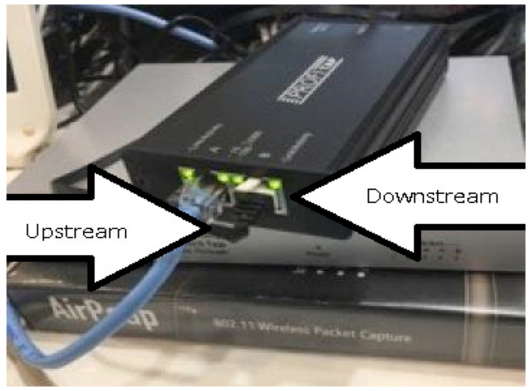


Capture Format

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

Figure 3-6: Capture Format group in Features tab

STEP 5

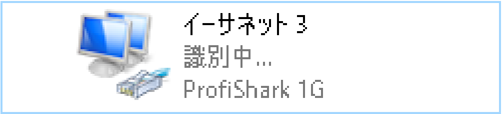


We use in-line mode with fail safe, connect upstream link and downstream link to each RJ-45 port (port A and port B)

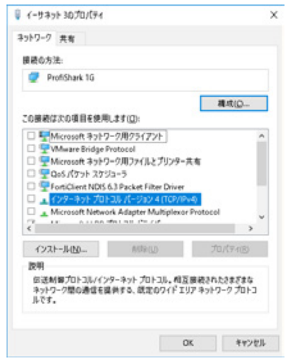
Figure 3-7: in-line mode with fail safe connection

STEP 6

You can see ProfiShark 1G adapter as one of network adapter, to avoid any useless management packet, I recommend checking off all protocols of network in ProfiShark adapter.



イーサネット 3
識別中...
ProfiShark 1G



イーサネット 3のプロパティ

ネットワーク　共有

接続の方法:
ProfiShark 1G
構成(C)...

この接続は次の項目を使用します(O):
☐ Microsoft ネットワーク用クライアント
☐ VMware Bridge Protocol
☐ Microsoft ネットワーク用ファイルとプリンター共有
☐ QoS パケット スケジューラ
☐ FortiClient NDIS 6.3 Packet Filter Driver
☐ インターネット プロトコル バージョン 4 (TCP/IPv4)
☐ Microsoft Network Adapter Multiplexor Protocol

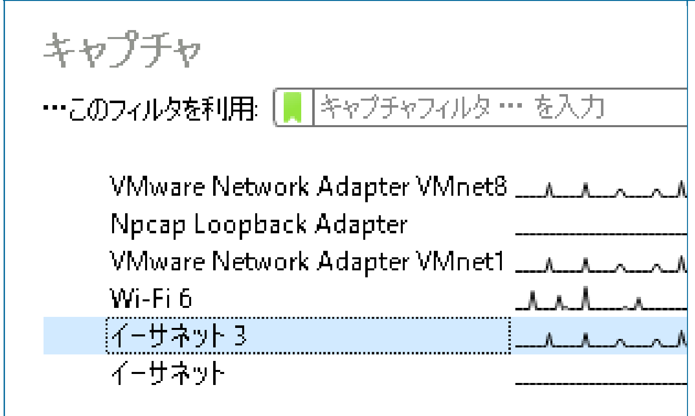
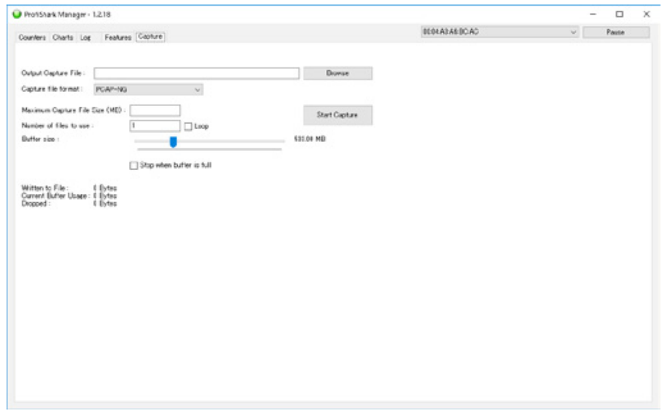
インストール(N)...　削除(U)　プロパティ(R)

説明
伝送制御プロトコル/インターネット プロトコル。相互接続されたさまざまなネットワーク間の通信を提供する、既定のワイド エリア ネットワーク プロトコルです。

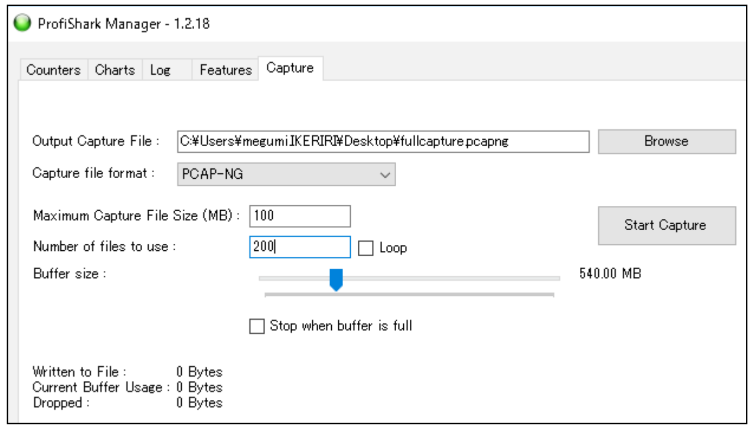
OK　キャンセル

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

ProfiShark has 2 types of Capture Driver, ProfiShark NIC Capture Driver and ProfiShark Direct Capture Driver. The difference is as follows, I recommend using Direct Capture Driver for stabilities, but if you want to use ProfiShark as one of capture interface of Wireshark interactively, ProfiShark NIC Capture Driver is the good way.

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
 キャプチャ …このフィルタを利用: キャプチャフィルタ … を入力 VMware Network Adapter VMnet8 Npcap Loopback Adapter VMware Network Adapter VMnet1 Wi-Fi 6 イーサネット 3 イーサネット	 ProfiShark Manager - 1.2.18 Counters　Charts　Log　Features　Capture 00:04:A3:A6:BC:AC　Pause Output Capture File :　Browse Capture file format :　PCAP-NG Maximum Capture File Size (MB) :　Start Capture Number of files to use :　1　☐ Loop Buffer size :　531.00 MB ☐ Stop when buffer is full Written to File :　0 Bytes Current Buffer Usage :　0 Bytes Dropped :　0 Bytes
ProfiShark NIC Capture Driver ⊙ Network Driver (NDIS) ⊙ Capture Driver (WinPcap etc.) ⊙ Wireshark	ProfiShark Direct Capture Driver ⊙ Trace file (pcapng/pcap) in SSD/HDD ⊙ Wireshark

This time open 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¥megumiIKERIRI¥Desktop¥fullcapture.pcapng　Browse
Capture file format :　PCAP-NG

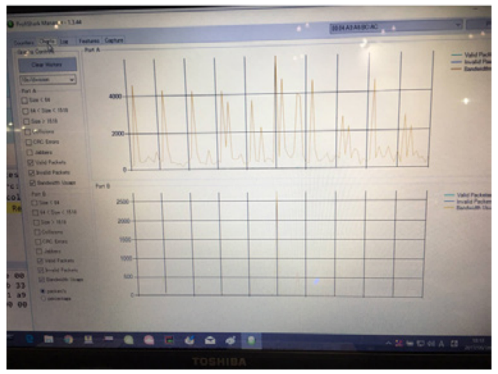
Maximum Capture File Size (MB) :　100　Start Capture
Number of files to use :　200　☐ Loop
Buffer size :　540.00 MB

☐ 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



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
profishark.dll

Figure 3-10: Charts tab in ProfiShark Manager

LONG TERM TRAFFIC CAPTURE

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.

But it is not welcome to bring packet analysis PC into enterprise network. PC (Windows or Linux) has a lot of vulnerabilities such as OS security hall, many interfaces such as Wi-Fi, Wired and USB, and application problems. So using ProfiShark with PC in customer's network is difficult for security reason.

Another problem is stability and reliability for long term traffic capture. Using Wireshark GUI is not suitable for long term capturing. But tshark CLI application has many functions. So 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?

In that case 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 a fault tolerance such as RAID.

And NAS is much stable than PC and you do not need a lot of time and cost to build capture PC for long term analysis. Only things you do is just connecting USB3 cable from ProfiShark to Intel based Synology NAS system.

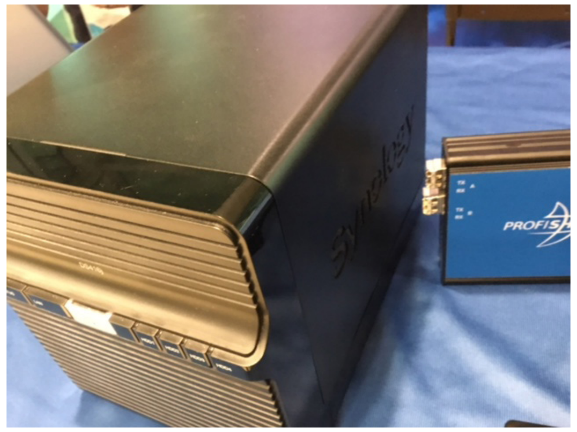


Figure 4-1: connecting a NAS to the ProfiShark

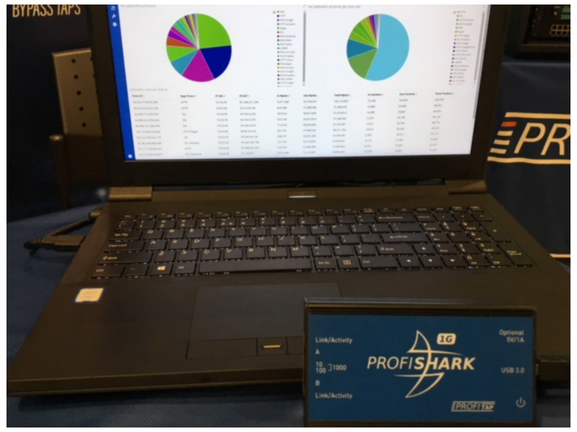


Figure 4-2: ProfiShark with NAS solution

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

LONG TERM CAPTURE SOLUTION HANDS ON

Let's start hands on of long term capture solution. There are a ProfiShark 1G connected with a Synology NAS. All configurations are done by WebUI of NAS. Note: we use demo site of ProfiShark NAS solution.

STEP 1

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

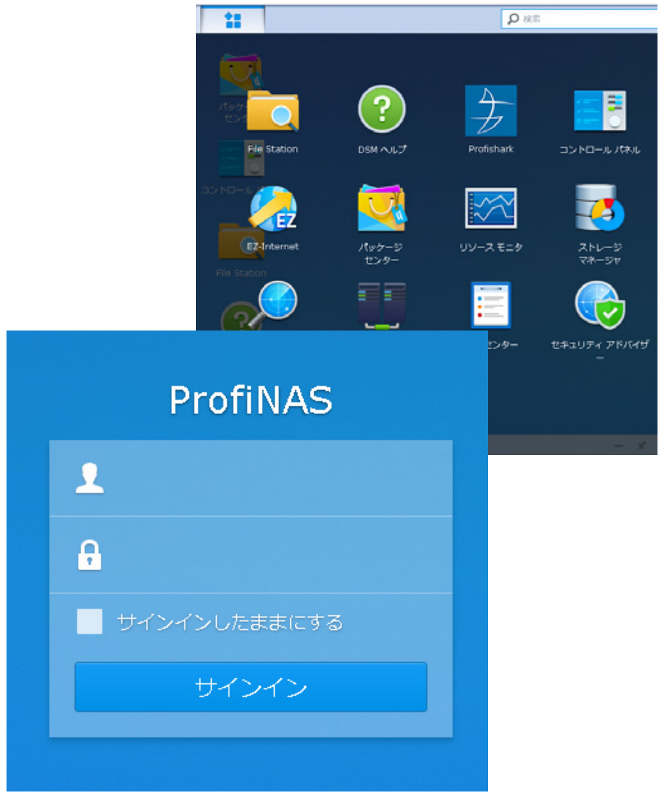


Figure 5-1: Synology NAS WebUI

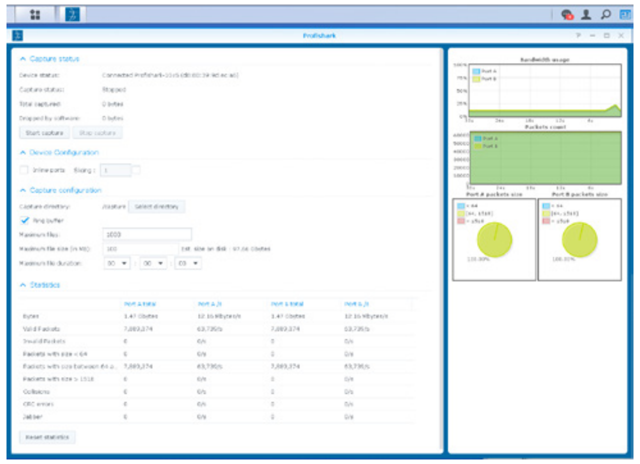
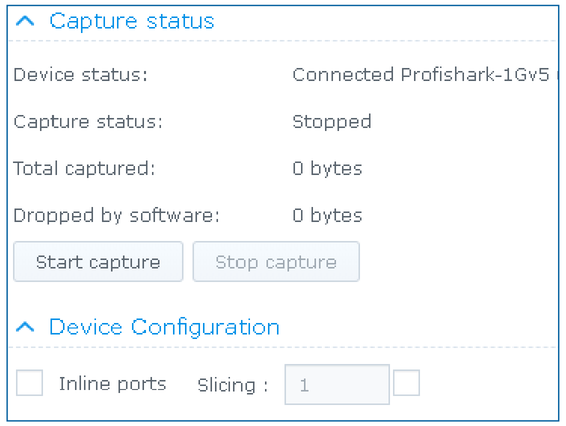


Figure 5-2: ProfiShark window

STEP 2

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 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-1Gv5

Capture status: Stopped

Total captured: 0 bytes

Dropped by software: 0 bytes

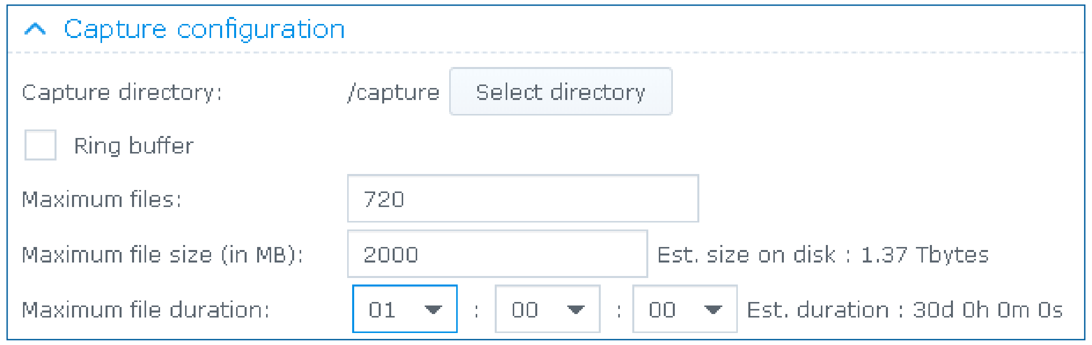
Device Configuration

□ Inline ports Slicing : 1 □

Figure 5-3: Capture status and Device Configuration section

STEP 3

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 Ring buffer checkbox. 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

□ Ring buffer

Maximum files: 720

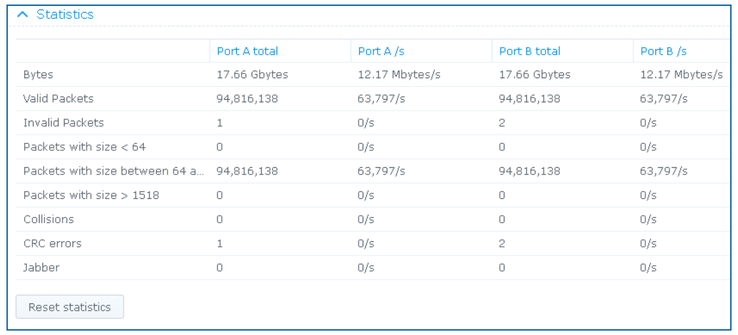
Maximum file size (in MB): 2000 Est. size on disk : 1.37 Tbytes

Maximum file duration: 01 : 00 : 00 Est. duration : 30d 0h 0m 0s

Figure 5-4: Capture configuration section

STEP 4

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 a "Reset statistics" button.



Statistics

	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

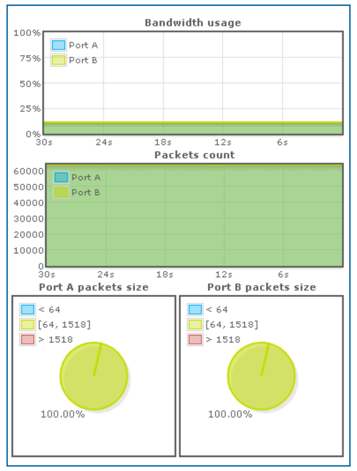


Figure 5-5: Statistics section and Graph

CONCLUSION

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

IT ALL STARTS WITH VISIBILITY

PROFI TAP

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 high-density 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

f Profitap

@Profitap

in profitap-international