

# REVIEW:

## A LOOK AT A PORTABLE USB3 NETWORK TAP

WIRESHARK HEROES SERIES

**JASPER**  
**"MACGYVER"**  
**BONGERTZ**





## JASPER BONGERTZ

TECHNICAL CONSULTANT FOR AIRBUS  
DEFENCE

*Jasper Bongertz is a Senior Technical Consultant for Airbus Defence and Space CyberSecurity. He started working freelance in 1992 when he began studying computer science at the Technical University of Aachen, eventually moving to Airbus to focus on IT security, Incident Response and Network Forensics. He runs a blog about network analysis topics at [blog.packet-foo.com](http://blog.packet-foo.com) and can be found on Twitter at [@packetjay](https://twitter.com/packetjay).*

### EXPERTISE:

- Network Forensics
- Incident Response
- CERT operations
- Network Security Monitoring (NSM/IDS/IPS)
- Network Troubleshooting and Analysis
- Network Attack Mitigation Strategies

[BLOG.PACKET-FOO.COM](http://BLOG.PACKET-FOO.COM)

## INTRODUCTION

A while ago I wrote a post for LoveMyTool about how I managed to power my Garland Gigabit TAP with a USB cable, which got me into a discussion about the Profitap USB3 device on LinkedIn. I had used 100Mbit USB2 Profitap devices before and had some issues with it on Linux, so I was a bit skeptical towards the new ProfiShark 1G as well. In the end, the nice people at Profitap offered to send me a sample to see how it performed, and I am always happy to get my hands on interesting capture solutions to see how they perform.



The ProfiShark 1G is a pretty small and portable aggregation TAP, which means that it combines receive and transmit (RX/TX) of a link into a single stream of packets which is then captured by the analyzer. Other than all the TAPs I own it is unique in the way it transports the network frames to the PC, because instead of RJ54 based network cards it uses a USB3 connection. While this may seem odd it has a couple of advantages (as long as the PC has a USB3 port, which should be pretty common by now). There are also a few minor disadvantages, if you want to call them that.

# ADVANTAGES

## *Supports Wireshark and other tools*

The ProfiShark 1G appears as a capture card in Wireshark/tshark/dumpcap as soon as you installed the ProfiShark driver and restarted the NPF driver to have it detect the new device (either by rebooting or doing a “net stop npf” and “net start npf”). The latest driver installer version will do this automatically, while the one I had didn't yet.

## *USB 3 powered*

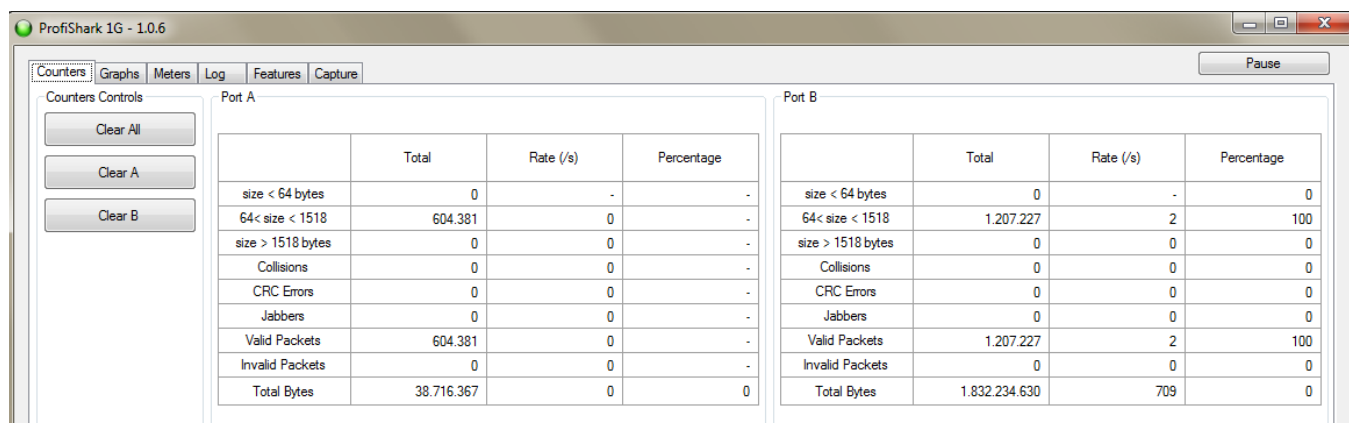
The USB3 port powers the TAP without the need of an additional power source during the capture, so you don't need to find a power socket for an additional power supply. This is pretty useful when you're using a laptop and don't have additional power sockets available (and boy, do we all have been in that kind of situation at customer sites)

## *Lossless Full Duplex Link aggregation*

USB3 has a total throughput of up to 5 GBit/s, so it has no trouble transporting the combined 2Gbit/s of a fully utilized duplex Gigabit link to the analyzer without dropping frames due to overload, which an aggregation TAP normally can't achieve over a single RJ45 connector. In all my tests the TAP did not drop a single frame, no matter how much load I put on the link.

## *USB utility*

The ProfiShark 1G comes with a USB utility that allows seeing the status and configuring the TAP in an easy way.



	Total	Rate (/s)	Percentage
size < 64 bytes	0	-	-
64 < size < 1518	604.381	0	-
size > 1518 bytes	0	0	-
Collisions	0	0	-
CRC Errors	0	0	-
Jabbers	0	0	-
Valid Packets	604.381	0	-
Invalid Packets	0	0	-
Total Bytes	38.716.367	0	0

	Total	Rate (/s)	Percentage
size < 64 bytes	0	-	0
64 < size < 1518	1.207.227	2	100
size > 1518 bytes	0	0	0
Collisions	0	0	0
CRC Errors	0	0	0
Jabbers	0	0	0
Valid Packets	1.207.227	2	100
Invalid Packets	0	0	0
Total Bytes	1.832.234.630	709	0

While I don't care about most of the status displays they may help at one point or another, but I could live without them. More interesting are the capture options you can set, which I'll explain in greater detail later in this post. The utility can also be used to capture packets directly, writing either PCAP, PCAPng or ERF files.



# DISADVANTAGES

## *RJ45 and SFP based professional capture devices*

You can't use this TAP with capture devices that are purely RJ45 or GBic/SFP based. You'll need a device with an USB3 port for this TAP to work as intended. So if you're using a professional capture or security appliance equipped with expensive FPGA based network capture cards this TAP is not for you.

## *External power*

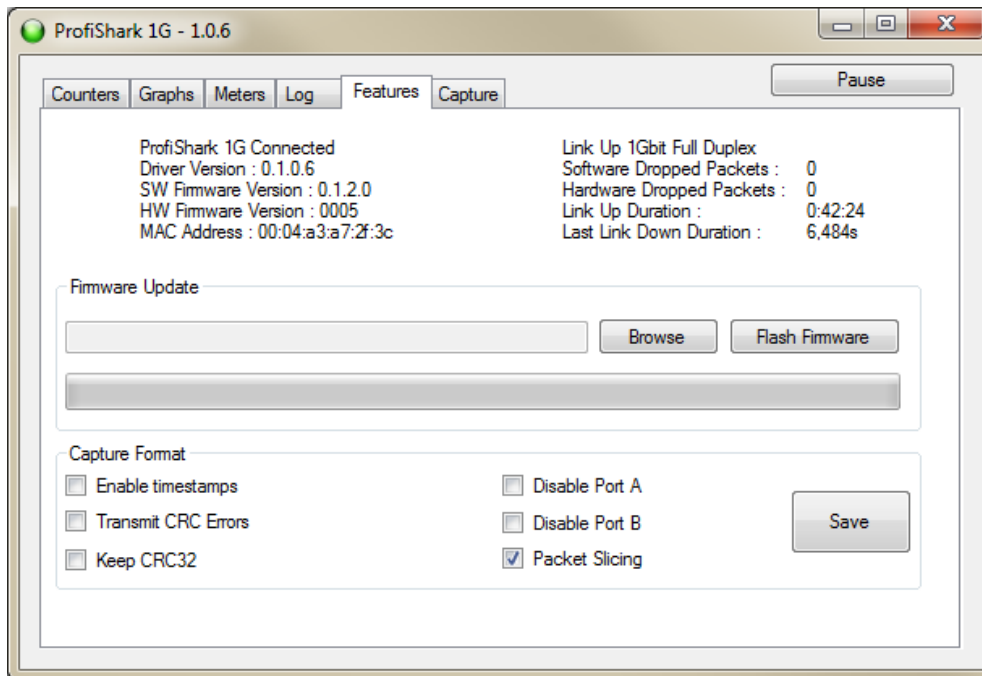
I already mentioned that one of the advantages of the TAP is that it draws power from USB3. The problem with that occurred to me during a real world capture job I used the ProfiShark in. Imagine you're capturing in a cold, noisy data center. You bring the laptop, insert the ProfiShark into the link, and start capturing. So far so good. Now, you need to take a look at the packets after you ran some tests that should have reproduced the problem. Most likely you don't want to do that standing in a data center row, with the laptop in your hands – instead, you'd go somewhere quiet (and with big monitors to see as much as you can). Which means that the TAP will lose power as soon as you disconnect it. That is no problem as it will do a layer 1 fallback, but it can interrupt the link for a short moment, and again when you plug it back in.



The engineers have thought of that though, and provide an optional 5v connector to power the TAP without being connected to USB – but you need to have an additional power supply for that. At least in my box there wasn't one. It's not really a big thing, but something to consider in data center capture situations – most people do not like link down synchronizations happening too many times in data centers ;-)

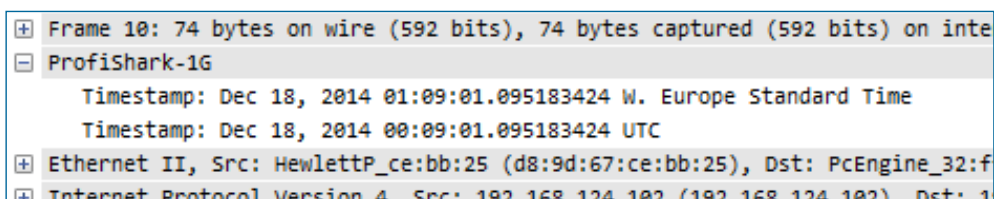
# THE USB UTILITY

While it's nice to have the graphs and counters in the USB utility, its real value is in the capture options it can configure on the ProfiShark as well as the ability to write capture files without having to start dumpcap or Wireshark first. It also allows updating the Firmware.



## Enable Timestamps

When enabling timestamp, the TAP adds an additional timestamp record trailing the Ethernet frame, which Wireshark can decode as soon as you install the ProfiShark DLL into the plugins directory of Wireshark. This will give you a time-stamp resolution of 8 nanoseconds instead of the normal PC milli- to microseconds.



If you don't install the plugin Wireshark will decode the bytes as VSS monitoring timestamps, which results in funny values.

## Transmit CRC Errors

With this setting the ProfiShark will accept and transfer broken frames to the capture PC, so you can record physical problems that way. I tried but could not pick up any such frames, which speaks for the quality of my networks I guess.

## Keep CRC32

As most of you know, normal PC captures do not keep the Ethernet FCS (a CRC32 checksum), which is why we almost never see the FCS in a capture. With this option the FCS is provided by the tap, so you can finally capture full frames of 1518 bytes and check the FCS. I had a little problem with this, but it was fixed in a new firmware sent to me on short notice (which allowed me to test the firmware upgrade procedure, which worked without any problems).

## Disable Port A / Display Port B

When either Port is disabled you'll not receive packets seen on that port. The communication on the link itself is not disturbed, but the capture will only see on side of the conversations. I have no idea why anybody would want to do this, but there is probably some reason for this setting. BTW, disabling both ports does in fact get you an empty capture file... :-)

## Packet Slicing

Now this may be an interesting setting, as it limits the packets to a hard coded size of 128 bytes and cuts away the rest. Many "intelligent" TAPs offer a feature like that to reduce the load on the capture device. The big problem with this is that the analyzer only sees 128 bytes and doesn't know how big the frame really was. This is exactly what happens if you choose to use Wireshark to capture like this, resulting in the problems we seen in the next screenshot:

No.	If ID	Source	Destination	Protocol	Info	Length	Delta Time
176	0	10.129.1.21	10.129.1.17	TCP	2777→55792 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1	66	0.000000000
177	0	10.129.1.17	10.129.1.21	TCP	55792→2777 [SYN, ACK] Seq=0 Ack=1 Win=17920 Len=0 MSS=8960 SACK_PERM=1 WS=128	66	0.000002000
178	0	10.129.1.21	10.129.1.17	TCP	2777→55792 [ACK] Seq=1 Ack=1 Win=262140 Len=0	60	0.000002000
180	0	10.129.1.17	10.129.1.21	FTP-DATA	FTP Data: 74 bytes	128	0.030000000
181	0	10.129.1.17	10.129.1.21	FTP-DATA	[TCP Previous segment not captured] FTP Data: 74 bytes	128	0.000003000
182	0	10.129.1.17	10.129.1.21	FTP-DATA	[TCP Previous segment not captured] FTP Data: 74 bytes	128	0.000001000
183	0	10.129.1.17	10.129.1.21	FTP-DATA	[TCP Previous segment not captured] FTP Data: 74 bytes	128	0.000002000
184	0	10.129.1.17	10.129.1.21	FTP-DATA	[TCP Previous segment not captured] FTP Data: 74 bytes	128	0.000001000
185	0	10.129.1.17	10.129.1.21	FTP-DATA	[TCP Previous segment not captured] FTP Data: 74 bytes	128	0.000001000
186	0	10.129.1.17	10.129.1.21	FTP-DATA	[TCP Previous segment not captured] FTP Data: 74 bytes	128	0.000002000
187	0	10.129.1.17	10.129.1.21	FTP-DATA	[TCP Previous segment not captured] FTP Data: 74 bytes	128	0.000001000
188	0	10.129.1.17	10.129.1.21	FTP-DATA	[TCP Previous segment not captured] FTP Data: 74 bytes	128	0.000001000
189	0	10.129.1.17	10.129.1.21	FTP-DATA	[TCP Previous segment not captured] FTP Data: 74 bytes	128	0.000002000
190	0	10.129.1.21	10.129.1.17	TCP	[TCP ACKED unseen segment] 2777→55792 [ACK] Seq=1 Ack=2921 Win=262140 Len=0	60	0.000001000
191	0	10.129.1.21	10.129.1.17	TCP	2777→55792 [ACK] Seq=1 Ack=5841 Win=262140 Len=0	60	0.000002000
192	0	10.129.1.17	10.129.1.21	FTP-DATA	[TCP Previous segment not captured] FTP Data: 74 bytes	128	0.000001000
193	0	10.129.1.17	10.129.1.21	FTP-DATA	[TCP Previous segment not captured] FTP Data: 74 bytes	128	0.000001000
194	0	10.129.1.17	10.129.1.21	FTP-DATA	[TCP Previous segment not captured] FTP Data: 74 bytes	128	0.000001000
195	0	10.129.1.17	10.129.1.21	FTP-DATA	[TCP Previous segment not captured] FTP Data: 74 bytes	128	0.000002000
196	0	10.129.1.21	10.129.1.17	TCP	2777→55792 [ACK] Seq=1 Ack=8761 Win=262140 Len=0	60	0.000001000

At first it seems like the TAP or the laptop dropped a ton of packets, but that's not the case. If you look at the packets you'll see the problem (I hope):

+	Frame 180: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on
+	Ethernet II, Src: IcpElect_bf:10:78 (00:08:0b:bf:10:78), Dst: HewlettP_ce:b
+	Internet Protocol Version 4, Src: 10.129.1.17 (10.129.1.17), Dst: 10.129.1.
-	Transmission Control Protocol, Src Port: 55792 (55792), Dst Port: 2777 (277
	Source Port: 55792 (55792)
	Destination Port: 2777 (2777)
	[Stream index: 3]
	[TCP Segment Len: 74]
	Sequence number: 1 (relative sequence number)
	[Next sequence number: 75 (relative sequence number)]
	Acknowledgment number: 1 (relative ack number)
	Header Length: 20 bytes
+	.... 0000 0001 0000 = Flags: 0x010 (ACK)
	Window size value: 140
	[Calculated window size: 17920]
	[Window size scaling factor: 128]
+	Checksum: 0x0676 [validation disabled]
	Urgent pointer: 0
+	[SEQ/ACK analysis]
	FTP Data (74 bytes data)

In frame 180, the "Next expected sequence number" is 75, because the frame only seems to carry 74 bytes of payload (while it truth it had been 1460 bytes, which would mean that the next sequence is 1461). So when the next frame is analyzed, Wireshark thinks that there is a gap:

```

+ Frame 181: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on
+ Ethernet II, Src: IcpElect_bf:10:78 (00:08:9b:bf:10:78), Dst: HewlettP_ce:
+ Internet Protocol Version 4, Src: 10.129.1.17 (10.129.1.17), Dst: 10.129.1.
- Transmission Control Protocol, Src Port: 55792 (55792), Dst Port: 2777 (27
  Source Port: 55792 (55792)
  Destination Port: 2777 (2777)
  [Stream index: 3]
  [TCP Segment Len: 74]
  Sequence number: 1461 (relative sequence number)
  [Next sequence number: 1535 (relative sequence number)]
  Acknowledgment number: 1 (relative ack number)
  Header Length: 20 bytes
+ .... 0000 0001 0000 = Flags: 0x010 (ACK)
  Window size value: 140
  [Calculated window size: 17920]
  [Window size scaling factor: 128]
+ Checksum: 0x50c3 [validation disabled]
  Urgent pointer: 0
+ [SEQ/ACK analysis]
  FTP Data (74 bytes data)

```

This is caused by the hard slicing at 128 bytes, and can't be helped because the TAP has no way of telling Wireshark the real wire size. But fortunately there's a workaround if you need this kind of feature: if you use the ProfiShark USB utility to capture the packets, it will write the wire size to the ERF or PCAPng headers (which didn't work at first, but the firmware update I mentioned fixed that, too). Problem solved.

## FINAL WORDS

The ProfiShark 1G is an interesting device for laptop captures, because it is small and works with just an USB3 port while doing aggregation without packet drops. It's not a TAP you want to put into your network permanently though, and I don't think that's what it was designed for anyway. If you need TAPs to put in once and stay you are probably better off with a RJ45 based TAP. Other than that, it's a useful TAP to carry in your laptop bag.

# IT ALL STARTS WITH VISIBILITY



Profitap develops and manufactures network monitoring solutions that drive network visibility and analytics on all traffic across physical and virtual infrastructures. All these solutions are designed with the security, forensics, deep packet capture, and network & application performance monitoring sectors in mind.

Profitap's network visibility solutions provide reliable and secure traffic access, help optimize and manage data flow and assist in capturing and analyzing network data of interest. With a portfolio of high-end network packet brokers, the most diverse TAP portfolio on the market, and award-winning ProfiShark® 1G and IOTA®, Profitap sets new standards in an industry where the definition of excellence is constantly being challenged.

With more than 1,000 clients, many of which are among Fortune 500 companies, from 60 countries, Profitap has become a must-have partner to achieve reliable network visibility and analytics.

PROFITAP HQ B.V.  
HIGH TECH CAMPUS 84  
5656AG EINDHOVEN  
THE NETHERLANDS

[sales@profitap.com](mailto:sales@profitap.com)  
[www.profitap.com](http://www.profitap.com)



Profitap



@Profitap



profitap-international