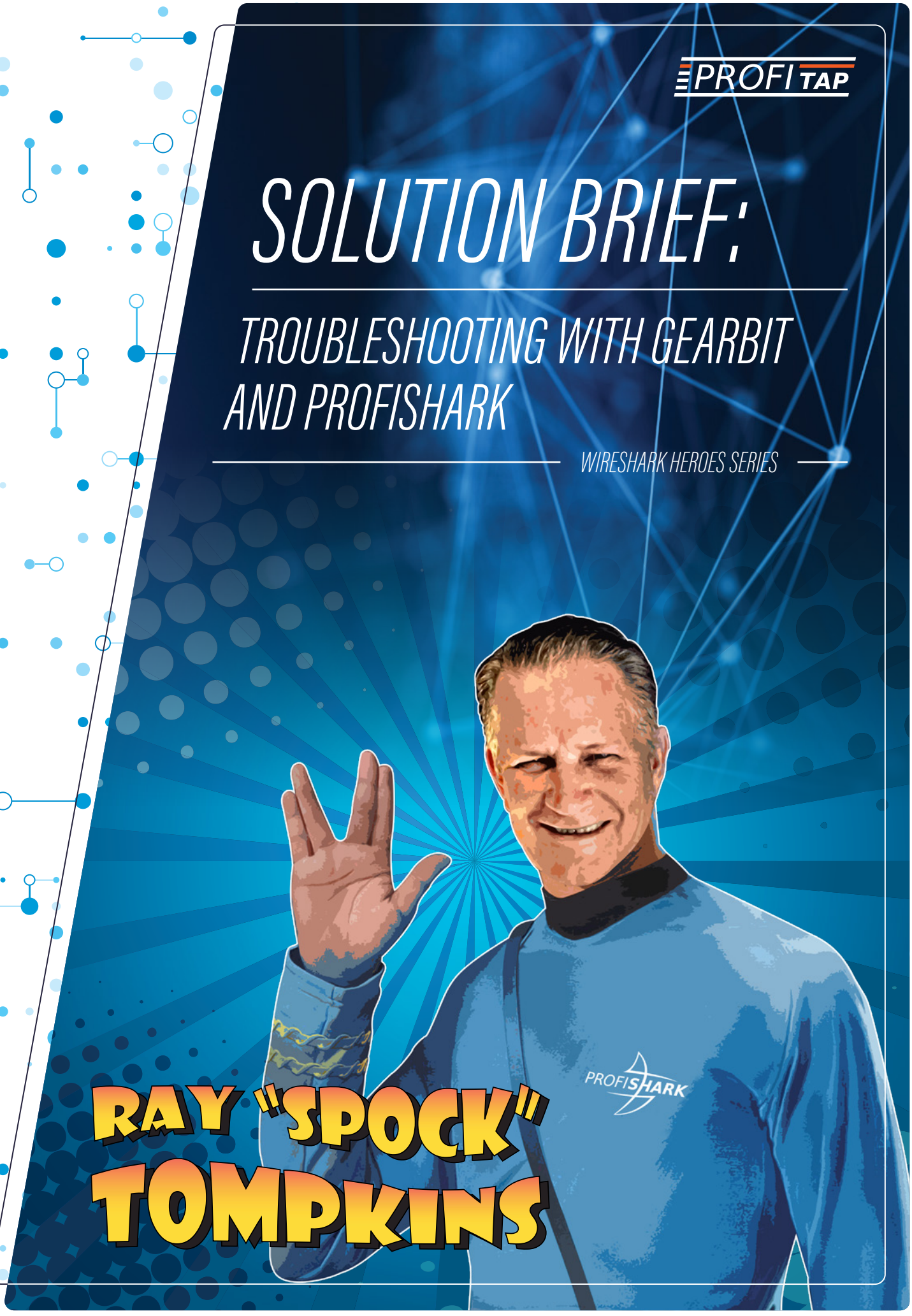
PROFITAP

SOLUTION BRIEF:

TROUBLESHOOTING WITH GEARBIT AND PROFISHARK

WIRESHARK HEROES SERIES



RAY TOMPKINS

NETWORK ANALYST & FOUNDER GEARBIT

In 2006 Ray founded Gearbit, Austin TX. He has managed global enterprise networks for companies including, Lucent, HP-Compaq and JP Morgan Chase. His success is credited for establishing leadership teams that focused on corporate communication business applications.

WWW.GEARBIT.COM

ISSUE HUNTING

I'm ashamed to admit it but this one caused issues for several weeks.

OK, months.

Slow response time, slow connecting to the network, and slow telnet sessions to the switch.

I'll get to more of the problem and solution in a moment, but first let me mention what I was thinking: I keep a pretty extensive 'Tool Kit' that enables me to get to the problem and I'm always looking to improve it.

My concern with some issues when going after the problem is, will I be able to capture everything, and have the details in the packet trace be complete, having enough to identify the issue, or will setting up a SPAN cause issues? Setting up a SPAN would cause the switch to be under stress, adding to the problem. Not that common, but in this case the switch is already under stress, so a SPAN might have a negative impact.

Adding the ProfiShark 10G tap (see Figure 1:1 ProfiShark 10G) into my kit helped save the day.

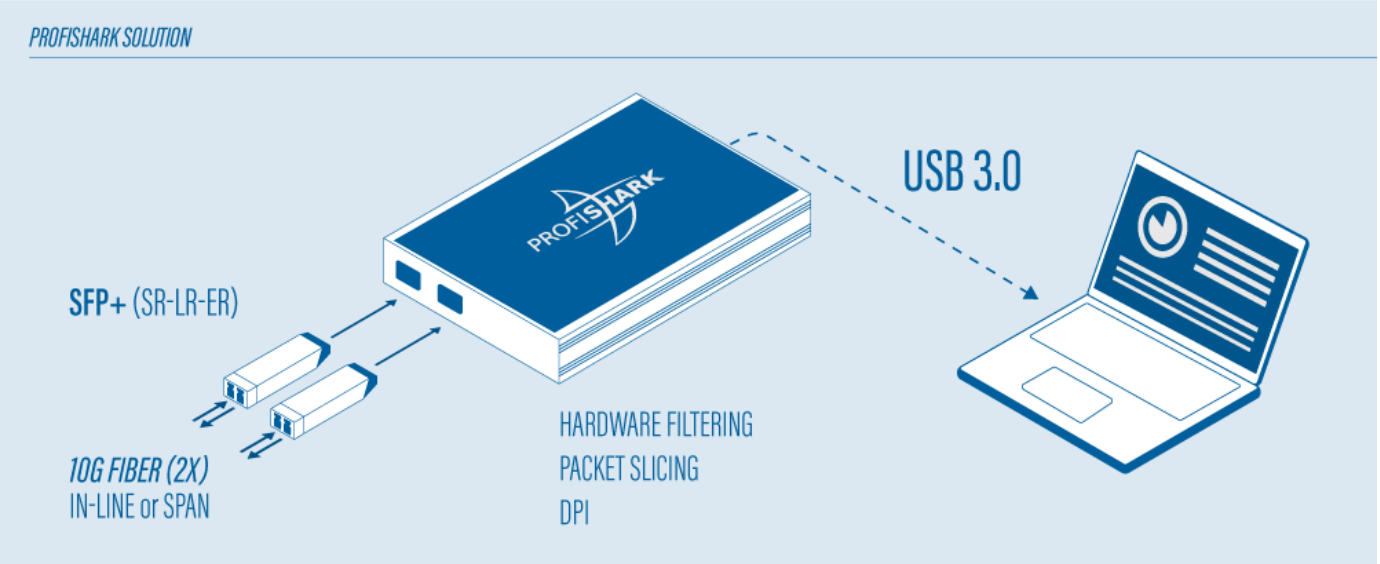


Figure 1:1 ProfiShark 10G

This problem was so severe I was really concerned about the effects of a SPAN port on an already overloaded switch. With the ProfiShark 10G I could tap into the 10 Gig switch-to-switch connections, allowing me to take the packet captures as needed, without affecting other the other network components or critical links.

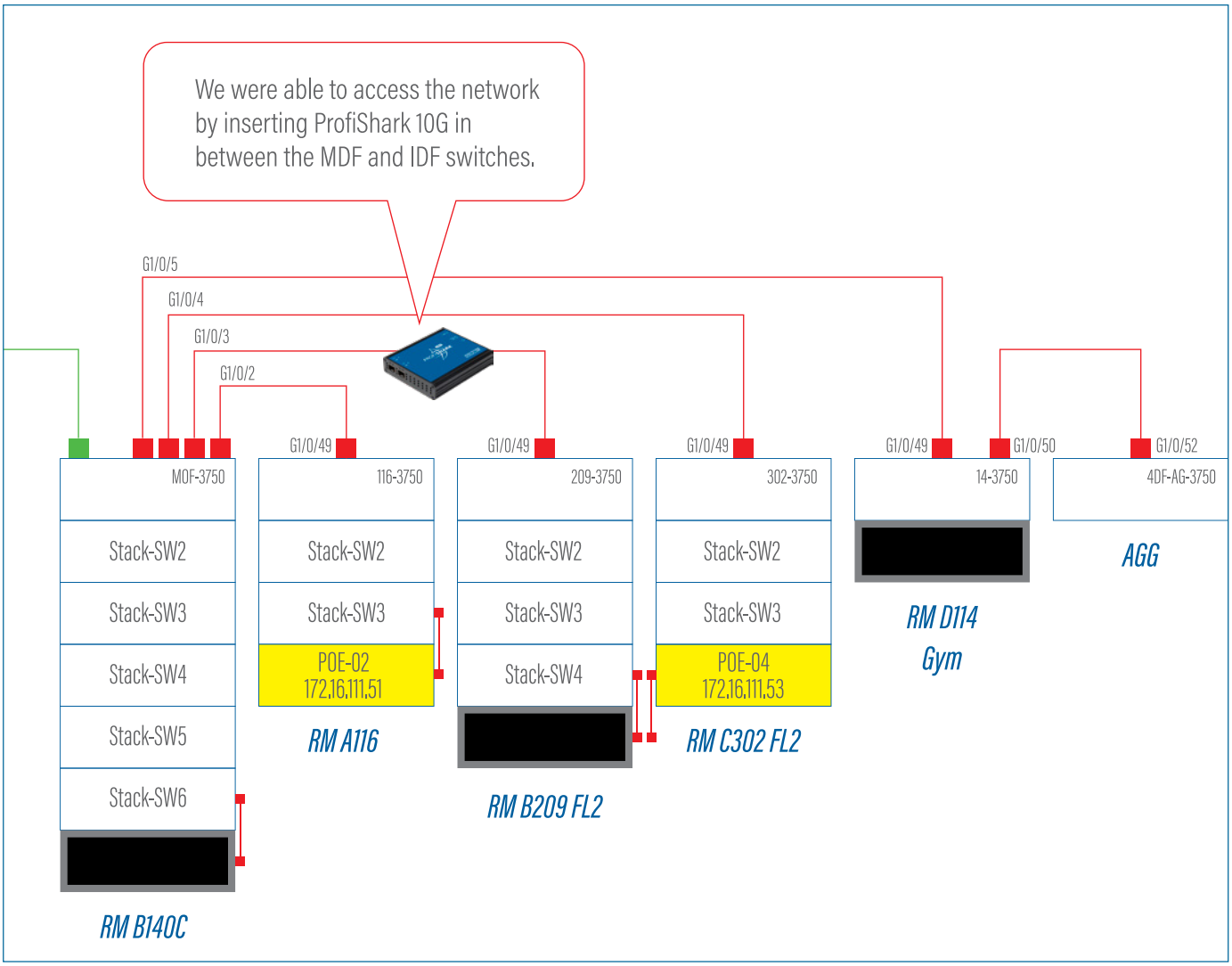


Figure 1:2 Network Switch Layout and ProfiShark Location

PROBLEM: This one caught me by surprise. Symptoms were intermittent, and would come and go throughout the day, not show up for days and then reappear. When the problems showed up you would hear complaints of slow response time, high ping times, even the telnet access to the Cisco switches were sluggish. I had looked at it for weeks past doing some of the normal troubleshoot methods from the Cisco switch, but this never really identified the issue. I also took a couple of trace files from a PC attached to the network, but this also yielded no results.

GATHER INFORMATION: We knew the problem was at this campus, mainly determined by the high ping times. That allowed us to concentrate on a stack of switches that supported that location. Getting as close to the problem as possible is always best. .

A first look at the trace didn't seem to indicate a problem, (see Figure 1:3 Packet Trace of Malware PC without MAC Column). I was confused, Wireshark was masking the problem. Or should I say the way I had Wireshark configured was masking the issue. With my normal methods of network analysis I don't normally look at the MAC addresses that often, and I had gotten complacent about it, not having a MAC address column visible in Wireshark.

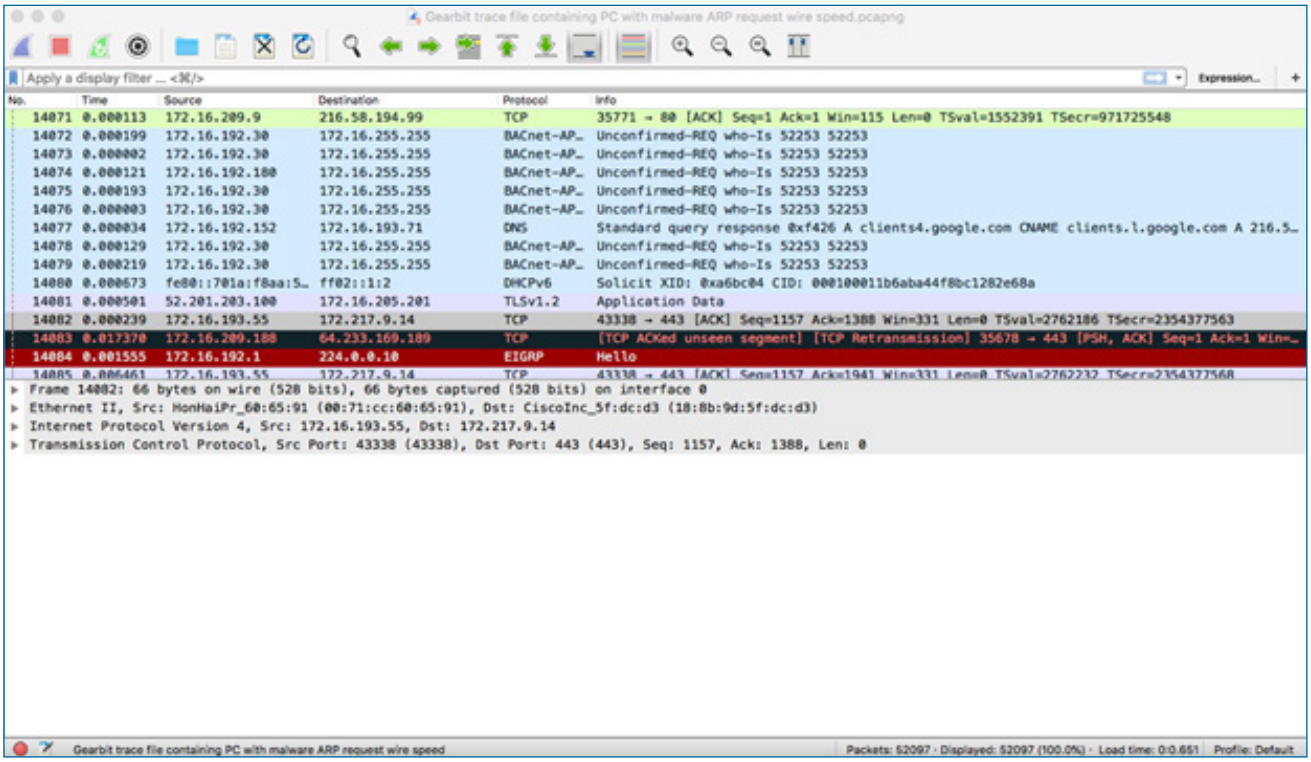


Figure 1:3 Packet Trace of Malware PC without MAC Column

PACKET TRACE: ARPs were transmitted at sub millisecond .000001 wire speed, also taking on the IP address of the default gateway. The MAC address was a little confusing: f4:8e:38:87:2c:ea. The leading byte was f4 taking in the bridge within the pc. Interesting, but the rest of the Mac was identical to the original Mac of the NIC card.

DISSECTING THE PACKET TRACE: Well, the trace files show the intensity in which this PC was just hammering the network. Even though the utilization wasn't close to 100%, the delta time they are being sent out at .000001 rate, and that is really spewing out packets. Not quite wire speed, but getting close to it. If you see a device sending broadcast packets out at a rate of .000001 per packet that's fast, I mean really fast.

Think about the network effects for a second. Everything within that broadcast dome will see that packet. And not only that, that device will have to process it, make the decision what to do with it. In this case most devices will just drop the packet. Also, the network devices, switches and routers will also have to process these packets.

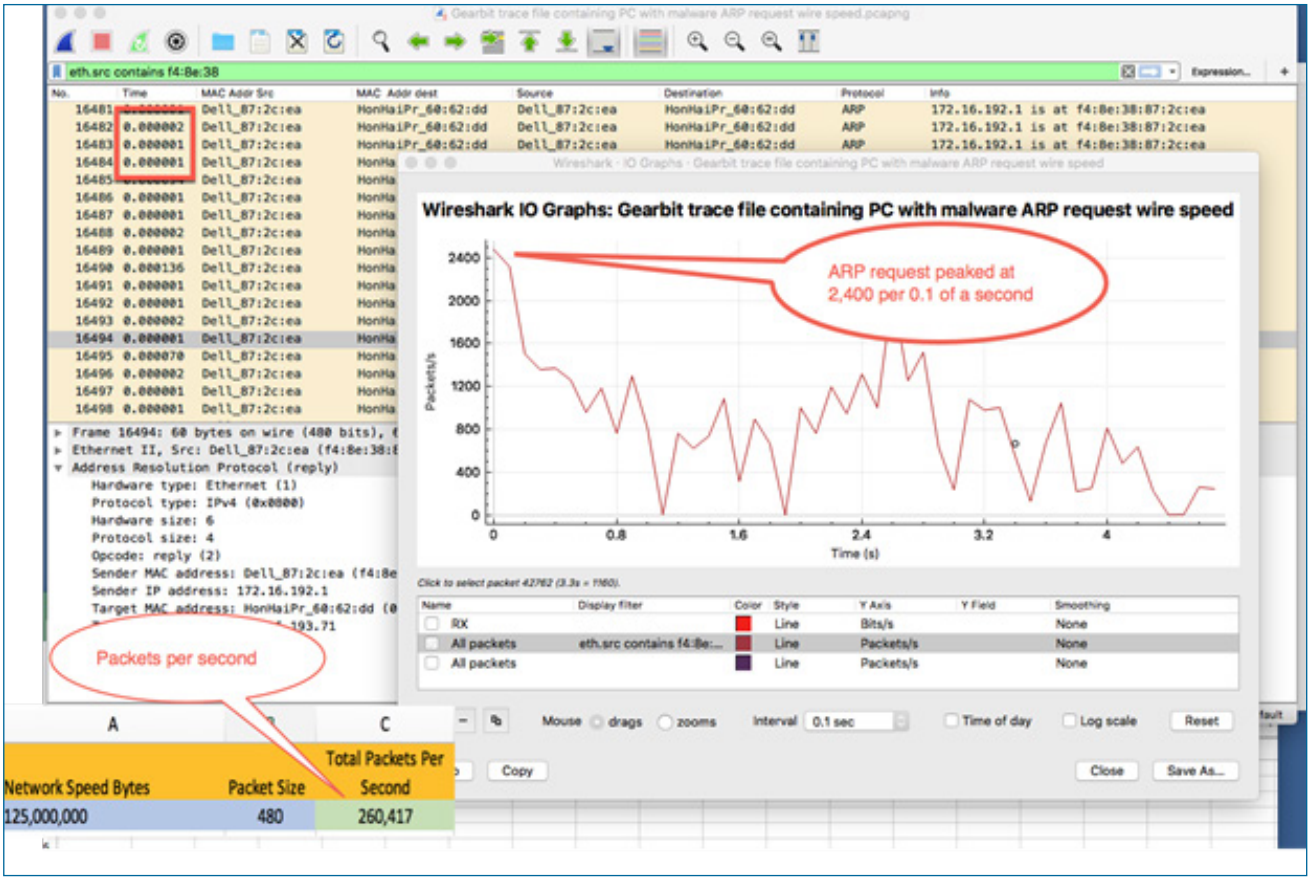


Figure 1:4 Packet Trace of Malware PC

CLEAN UP: How do you know you've solved the issue? Collecting all the facts and completing the analysis is always key: calculations show 260,417 packets per second on a 1Gb connection with a packet size of 480 bits.
With this kind of volume, all devices in the broadcast domain get very busy looking at all those packets, creating the conditions that everyone was reporting. This way you can be convinced that you've uncovered the "needle in the haystack" and act accordingly.

PROFISHARK OVERVIEW

PROFISHARK 1G

PROFISHARK 10G

The ProfiShark 1G and 10G can capture any traffic, frames of any size and type, in-line or SPAN, for analysis and monitoring with Wireshark, or any major software analyzer. The included ProfiShark Manager software provides additional information, statistics, and configuration and capture options.

PROFISHARK 1G+

PROFISHARK 10G+

The ProfiShark 1G+ and 10G+'s GPS/GLONASS function can tag packets with accurate UTC timestamps. The ProfiShark 1G+ and 10G+ can also receive or generate a PPS signal, enabling accurate timestamp synchronization in various topologies.

PROFISHARK 100M

The ProfiShark 100M is designed for the capture of 10/100M Ethernet traffic. It is the perfect tool for troubleshooting Real-Time Industrial Ethernet protocols. As an all-in-one network TAP in a pocket-sized box, this portable traffic capture device gives you all the flexibility and ease of use you require for the monitoring of industrial networks.

- USB powered, no adapter required
- Lightweight and portable
- Hardware aggregation
- SPAN and In-Line modes
- 8 ns hardware timestamping
- Capture any type of frames
- Low level error and bandwidth monitoring
- Hardware filtering, deep packet inspection
- CRC error capture
- Packet slicing
- Non-intrusive, fail-safe monitoring
- Real time statistics
- Direct capture to disk
- Very low CPU usage
- Quick setup and easy to use
- Invisible to the network

COMPATIBILITY

- Wireshark
- ClearSight
- OmniPeek
- Packetyzer
- OptiView
- NetSpector
- NetDecoder
- Ethertest

And many more...

PROFISHARK LONG-TERM TRAFFIC CAPTURE SETUP

Long-term Traffic Capture

ProfiShark long-term capture solution is designed with flexibility in mind. Combined with a NAS for storage tailored to your specific needs, the long-term capture feature makes it easy to catch intermittent problems in the act.

IT ALL STARTS WITH VISIBILITY

PROFITAP

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

Profitap

@Profitap

profitap-international