Using Wireshark & the Observer Platform for Complete Visibility

If you are like the average network professional, Wireshark is probably a part of your regular troubleshooting arsenal. And, why not? It's the tool by which you learned network analysis. Its flexibility in licensing, no-cost download, and familiarity, make it a logical choice to deploy to capture and analyze packets. But, what might your network team be missing, if it depends solely on Wireshark for network monitoring?

We'll look at a two-solution approach that involves using Wireshark with the Observer Platform to:

- Establish complete and effective visibility across an enterprise infrastructure
- Effectively reduce mean time to resolution (MTTR)
- Shift to proactive performance monitoring to ensure optimal user experience

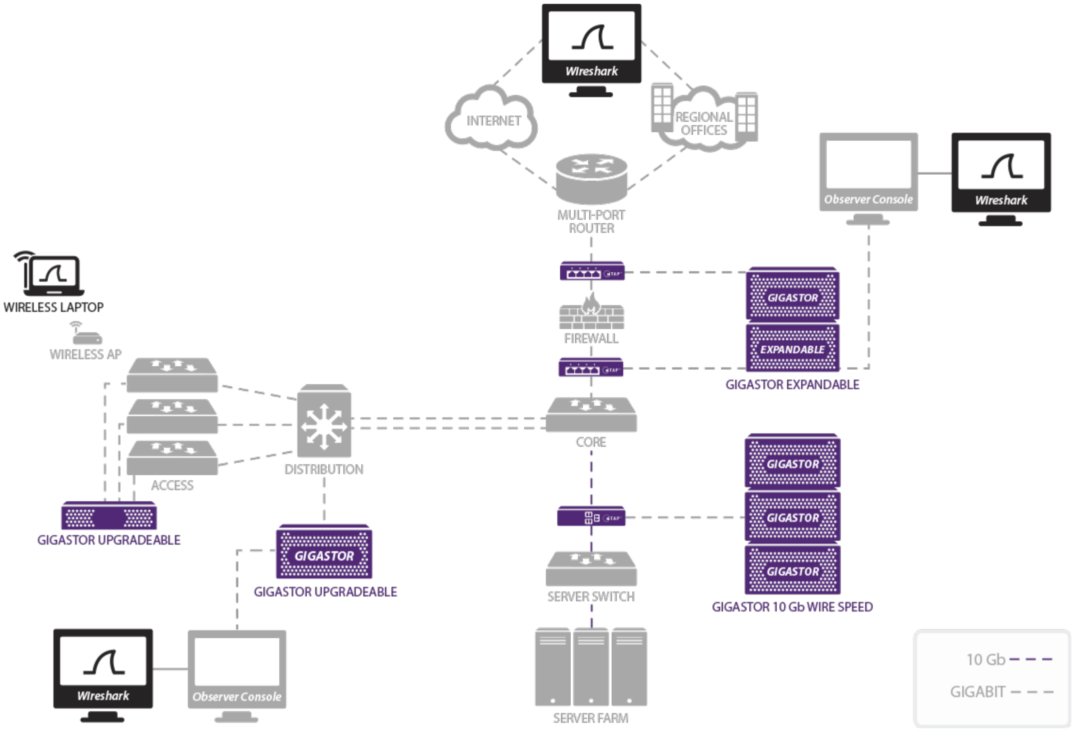
Complete Visibility

Strategically using Wireshark in conjunction with the Observer Platform allows you to achieve maximum visibility and capture all the packets.

Wireshark: Deploy Wireshark at the edge for cost-effective visibility into remote offices or on an ad-hoc basis to user stations. It's no-cost licensing makes it well-suited for these locations.

Observer Analyzer and Observer GigaStor: Monitoring multiple critical applications running on a 10 Gb or 40 Gb link in the core begs the question, "Can a software analyzer handle the load?" Realistically, the answer is no. You could attempt to apply multiple filters to reduce the amount of traffic captured. But, to effectively troubleshoot issues like contention requires all the packets. The best way to ensure availability of applications in the core is through implementing hardware analysis appliances like Observer GigaStor that can handle these speeds. Additionally, GigaStor hardware and software versions are deliberately designed for back-in-time analysis with a time-based interface for easy isolation of events around the minutes, hours, and days of interest. Having captured and retained network traffic that is immediately accessible accessible means quick reconstruction of the user experience and eliminates having to wait for the problem to reoccur.

As the following network diagram illustrates, to achieve comprehensive visibility, the Observer Platform is deployed in the core and Wireshark at the edge.

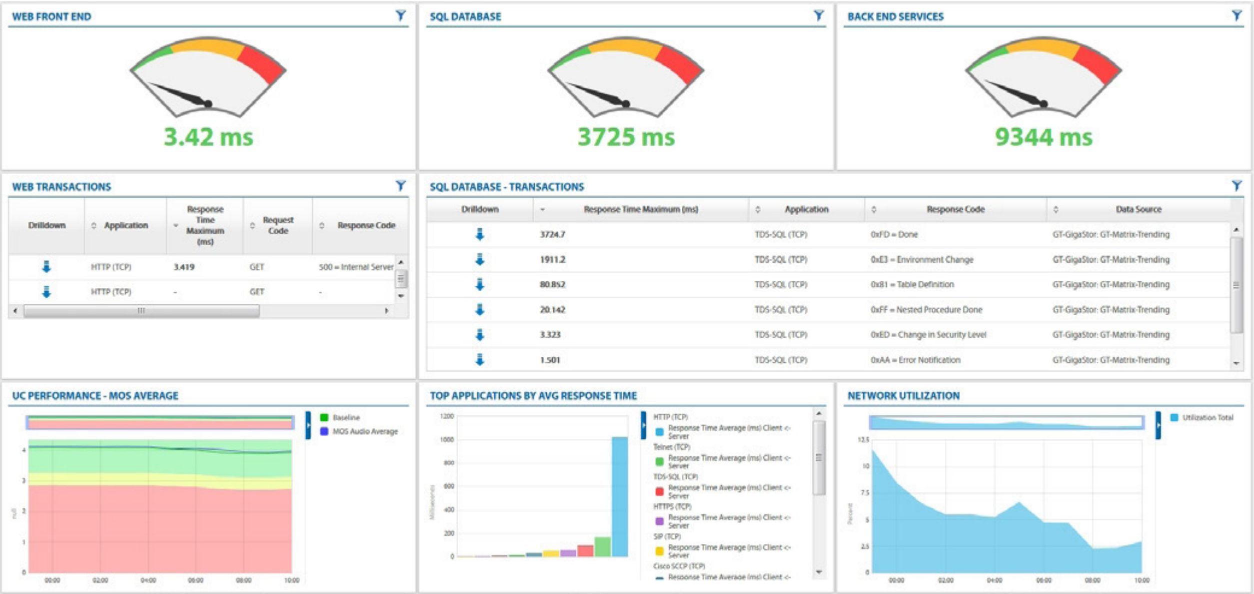


Reducing MTTR

Get to the root cause of the problem quicker by supplementing Wireshark workflows with the aggregated performance views, visualization of performance conditions, and transaction from the Observer Platform.

Wireshark: Being familiar with Wireshark means you're proficient in navigating through the interface. In cases where you prefer to use Wireshark, Analyzer and GigaStor offer easy exporting of capture files to support this.

Observer Apex: Assess the scope and severity of problems in real time with high-level aggregated views, and more appropriately scale your response to the problem. From built-in widgets, you can also get a sense of the underlying causes of poor performance, before beginning the troubleshooting process. For example, you could view the performance of individual application tiers alongside transactions and errors for indications of potential issues and navigate to the likely cause.



WEB TRANSACTIONS

Drilldown	Application	Response Time Maximum (ms)	Request Code	Response Code
⬇	HTTP (TCP)	3.419	GET	500 = Internal Server
⬇	HTTP (TCP)	-	GET	-

SQL DATABASE - TRANSACTIONS

Drilldown	Response Time Maximum (ms)	Application	Response Code	Data Source
⬇	3724.7	TDS-SQL (TCP)	0xFD = Done	GT-GigaStor: GT-Matrix-Trending
⬇	1911.2	TDS-SQL (TCP)	0xE3 = Environment Change	GT-GigaStor: GT-Matrix-Trending
⬇	80.852	TDS-SQL (TCP)	0x81 = Table Definition	GT-GigaStor: GT-Matrix-Trending
⬇	20.142	TDS-SQL (TCP)	0xFF = Nested Procedure Done	GT-GigaStor: GT-Matrix-Trending
⬇	3.323	TDS-SQL (TCP)	0xED = Change in Security Level	GT-GigaStor: GT-Matrix-Trending
⬇	1.501	TDS-SQL (TCP)	0xAA = Error Notification	GT-GigaStor: GT-Matrix-Trending

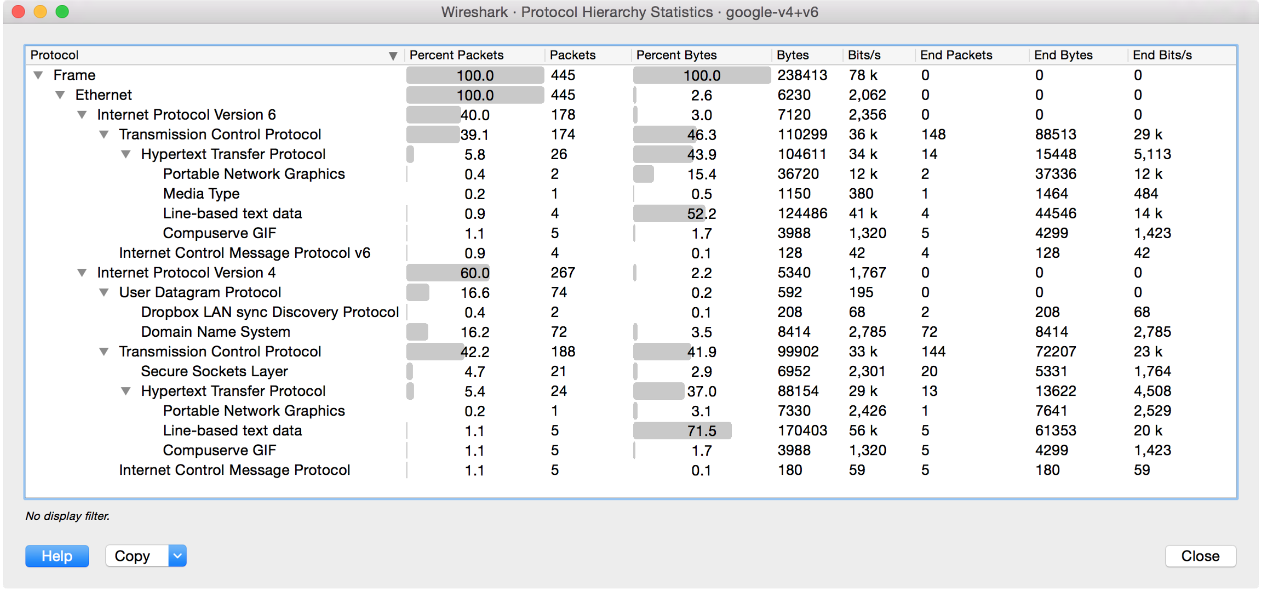
UC PERFORMANCE - MOS AVERAGE
Baseline
MOS Audio Average
4
3
2
1
0
00:00
02:00
04:00
06:00
08:00
10:00
TOP APPLICATIONS BY AVG RESPONSE TIME
1200
1000
800
600
400
200
0
Milliseconds
HTTP (TCP)
Response Time Average (ms) Client <- Server
Telnet (TCP)
Response Time Average (ms) Client <- Server
TDS-SQL (TCP)
Response Time Average (ms) Client <- Server
HTTPS (TCP)
Response Time Average (ms) Client <- Server
SIP (TCP)
Response Time Average (ms) Client <- Server
Cisco SCCP (TCP)
Response Time Average (ms) Client <-
NETWORK UTILIZATION
Utilization Total
12.5
10
7.5
5
2.5
0
Percent
00:00
02:00
04:00
06:00
08:00
10:00

Additionally, Observer Analyzer provides in-depth, transaction-level analysis on a variety of protocols complementing application protocol views in Wireshark, and bolstering your ability to pinpoint what's going wrong within the application.

Proactive Performance Monitoring

Get ahead of problems by using behavior analytics and alerts within Observer Apex to understand the normal behavior of your network and to be notified of degrading performance. Use Wireshark for snapshots of typical traffic patterns at the edge.

Wireshark: Get a sense of typical network utilization and behavior in remote offices by using Wireshark features like the Protocol Hierarchy Statistics Window. Although it's a more manual process, it's great insight.



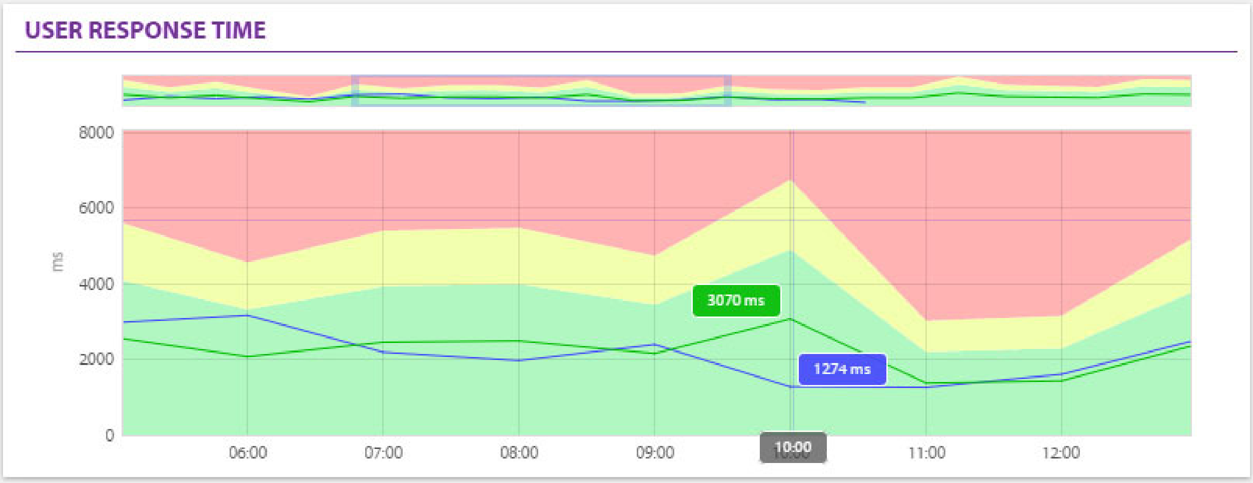
Wireshark · Protocol Hierarchy Statistics · google-v4+v6

Protocol ▼	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
▼ Frame	100.0	445	100.0	238413	78 k	0	0	0
▼ Ethernet	100.0	445	2.6	6230	2,062	0	0	0
▼ Internet Protocol Version 6	40.0	178	3.0	7120	2,356	0	0	0
▼ Transmission Control Protocol	39.1	174	46.3	110299	36 k	148	88513	29 k
▼ Hypertext Transfer Protocol	5.8	26	43.9	104611	34 k	14	15448	5,113
Portable Network Graphics	0.4	2	15.4	36720	12 k	2	37336	12 k
Media Type	0.2	1	0.5	1150	380	1	1464	484
Line-based text data	0.9	4	52.2	124486	41 k	4	44546	14 k
Compuserve GIF	1.1	5	1.7	3988	1,320	5	4299	1,423
Internet Control Message Protocol v6	0.9	4	0.1	128	42	4	128	42
▼ Internet Protocol Version 4	60.0	267	2.2	5340	1,767	0	0	0
▼ User Datagram Protocol	16.6	74	0.2	592	195	0	0	0
Dropbox LAN sync Discovery Protocol	0.4	2	0.1	208	68	2	208	68
Domain Name System	16.2	72	3.5	8414	2,785	72	8414	2,785
▼ Transmission Control Protocol	42.2	188	41.9	99902	33 k	144	72207	23 k
Secure Sockets Layer	4.7	21	2.9	6952	2,301	20	5331	1,764
▼ Hypertext Transfer Protocol	5.4	24	37.0	88154	29 k	13	13622	4,508
Portable Network Graphics	0.2	1	3.1	7330	2,426	1	7641	2,529
Line-based text data	1.1	5	71.5	170403	56 k	5	61353	20 k
Compuserve GIF	1.1	5	1.7	3988	1,320	5	4299	1,423
Internet Control Message Protocol	1.1	5	0.1	180	59	5	180	59

No display filter.

Observer Platform: Leverage trending in Analyzer or Apex's automated baselining to determine normal performance in the core. Alerts can then be configured to notify your team of performance deviations before it impacts users.

Using this two-solution approach in managing performance provides your network team with the added visibility and insight to cut troubleshooting times, reduce the number of user complaints, and proactively ensure network and application success.



Contact Us

+1 844 GO VIAVI
(+1 844 468 4284)

To reach the Viavi office nearest you,
visit viavisolutions.com/contacts.