Application-Centric Analysis Helps Maximize the Value of Wireshark®

The 'cost' of freeware

Protocol analysis has long been viewed as the last line of defense when it comes to resolving nagging network and application issues. But while almost every network engineer has a copy of Wireshark® on their laptop, and the dissection of packet traces is something that everyone would like to be able to do, very few have truly acquired this skill. Tools like Wireshark are readily available to anyone who takes the time to download them. However only a small fraction of network professionals are successful in using Wireshark to isolate the network problem and formulate a resolution. In spite of the good intentions of the network operations staff to save the organization money on the cost of tools, the hidden expense in terms of the excessive time spent to resolve problems and the corresponding lost productivity can be staggering.

Table of contents

FLUKE networks

The challenge in using freely available protocol analyzers is that they are usually very good with displaying the packets, but they do not summarize and analyze the network traffic in a way that will reduce the time it takes to resolve the network problem. Instead, the expectation is that the person using the analyzer knows what they are looking for and are merely looking for a way to filter and display the information. This is rarely the case.

It is important to first discuss how protocol analysis has developed over the years. 25 years ago all protocol analysis was performed by capturing bits on WAN circuits and manually decoding those bits into data blocks. 20 years ago the protocol analyzers were available to apply decodes to the capture data, to reduce the time it took to analyze the network traffic. Over the last 20 years, we have seen the addition of expert analysis to assist in the identification of problems such as TCP retransmissions and other basic problems. While the addition of this expert analysis has helped, much of the analysis still depends on the abilities of the analyst interpreting the trace file.

In recent years, we have seen the technology move toward application-centric analysis of network traffic. Instead of focusing on the lower layers of the OSI model, such as the Network and Transport Layers, the focus has been put on the Application Layer. This move up the protocol stack reduces the time it takes to isolate a specific problem. It does however require that the analyzer used to troubleshoot the problem be able to analyze the traffic at the Application Layer.

Taking an Application Centric approach to protocol analysis changes the workflow from that used with a traditional protocol analyzer such as Wireshark.

The traditional protocol analyzer requires that we start at the bottom of the protocol stack and start working our way up to the top, in hopes that we will eventually determine the cause of the application problem. But does lower layer problems really affect application performance?

With the Application Centric approach, we start with alerts based on a flow-based summary of automated application layer decodes and work our way down into the details that will help identify the root cause of the problem.

In this whitepaper, we'll compare 6 key protocol analysis features looking at Wireshark® and the Fluke Networks ClearSight Analyzer, and how the two can be used together to maximize the value of each, and make the network support staff more efficient when troubleshooting performance problems:

- Packet Level vs Application Level Visibility
- Expert Analysis of Application Traffic
- Reassembly of Application Data
- Data Flow Ladder Diagram
- Combined Data Flows
- Report of Application Layer Traffic
- Conclusion

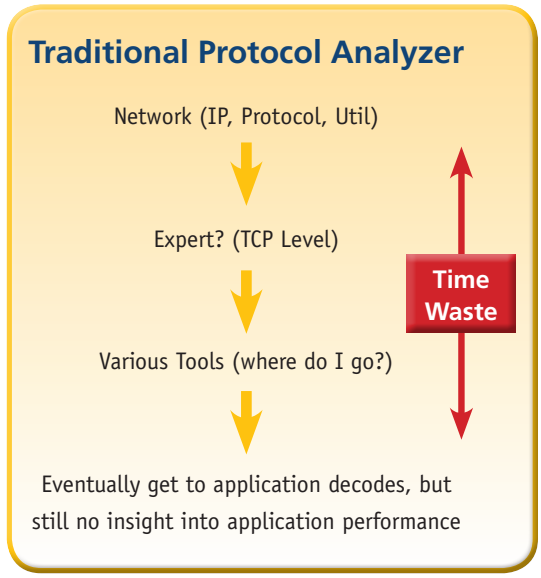

Figure 1

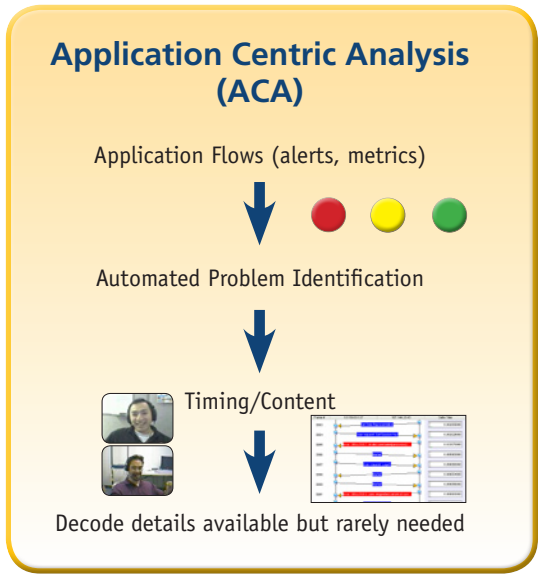

Figure 2

Packet Level vs Application Level Visibility

Wireshark® provides many benefits when it comes to troubleshooting network problems. It is freely available and can be quickly downloaded from the Internet at anytime, so an entire department can be equipped with a packet capture tool. While it does provide an effective means to capture and view packets traversing the network, when we stop a trace, we are presented with the screen below:

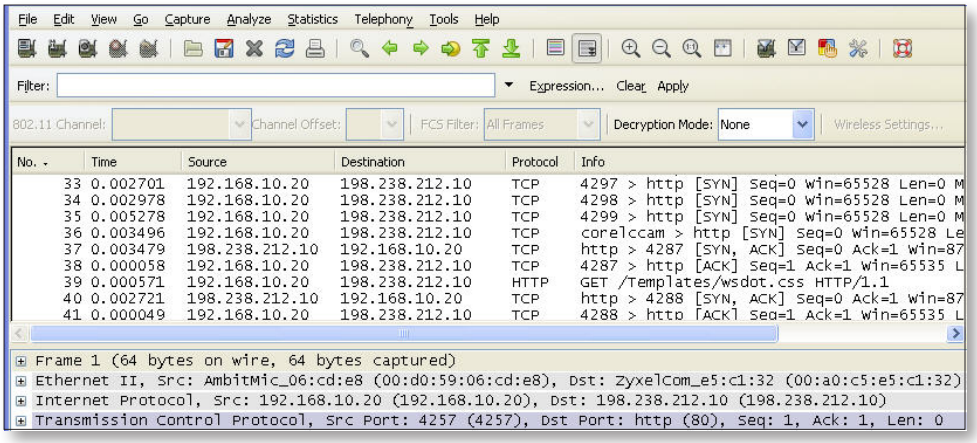

Figure 3

This screen shows us the packets and their detailed decodes, but it does not provide us with a high level view of the traffic. This analysis is left up to the person using the analyzer and their success depends on their understanding of the protocol operation.

In contrast, when we open or capture a trace with the ClearSight Analyzer, we are presented with a summary screen showing the protocols present in the capture. For each one of these protocols, we can quickly see the number of servers, data flows, problems and issues. In addition, we can see the amount of bandwidth each one of these protocols is using within the trace. This information allows us to quickly zero in on problems, without having to dig through thousands of packets.

In addition to the ability to see which protocols are present and the related issues, we can apply a filter based on any of the protocols simply by pushing a single button. This eliminates the need to remember complex filter commands.

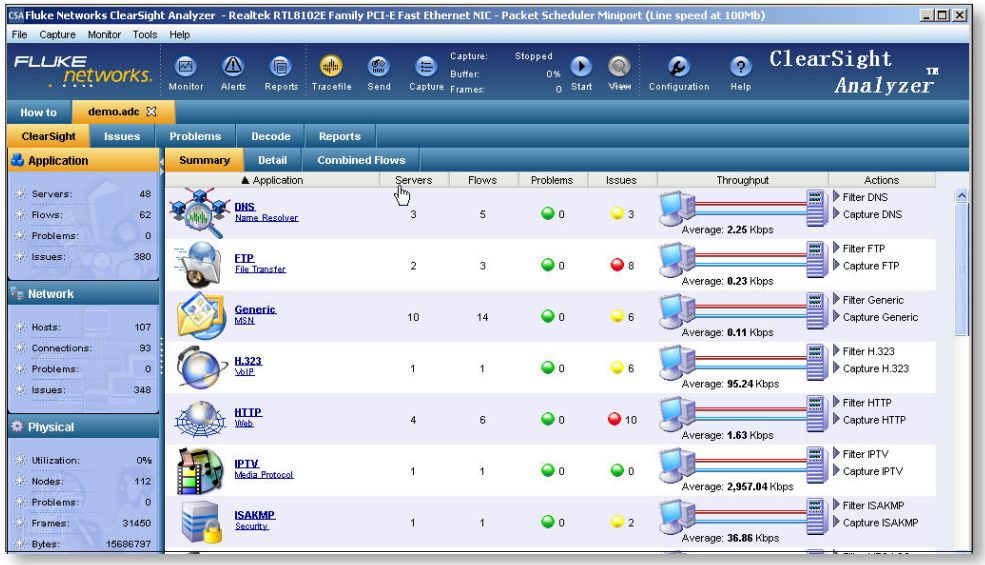

Figure 4

Expert Analysis of Application Traffic

The goal with any network problem is to reduce the time to resolution. When it comes to network and application troubleshooting, expert analysis of the traffic is key to finding the problem as quickly as possible. The Wireshark analyzer does provide some analysis of the packets. This analysis, however, is performed from the transport layer down. If we are trying to troubleshoot an application layer problem, this expert analysis will be of little help.

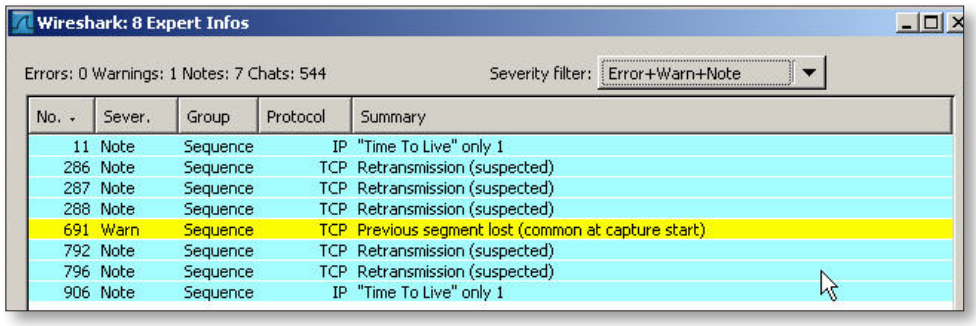

Figure 5

The ClearSight Analyzer performs expert analysis on each one of the layers in the Open System Interconnection (OSI) Model including the application layer. Any issues found within the trace are displayed as red dots next to the application on the summary screen of the analyzer. By clicking on the application, each one of the data flows within the application are displayed. The individual flows containing the issues will have red dots next to them.

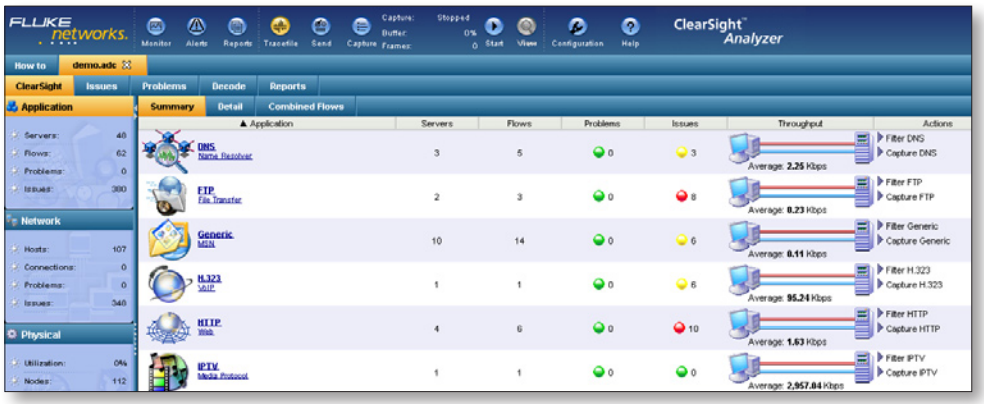

Figure 6

This visual indication of issues makes it easier and less time consuming to identify those parts of the application flows that are contributing to the slowdown or failure. It is also possible to view all of the issues within the capture. Each one of these issues contains information about the source, destination, protocol, and a description of the issue. As with the data flows, colored dots next to each issue indicate the severity of the problems, so that the critical issues can be investigated first.

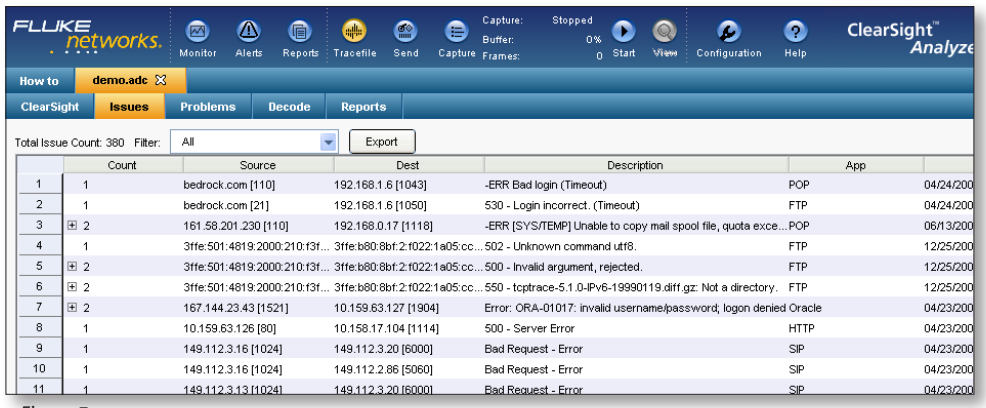

Figure 7

Reassembly of Application Data

In some cases, when troubleshooting application problems it is useful to reassemble the application data in order to determine the cause of the problem. The Wireshark analyzer provides the "Follow TCP Stream" feature that will apply a filter based on a IP address and TCP port combination. The data portion of these packets will then be reassembled and displayed in a window such as the one below.

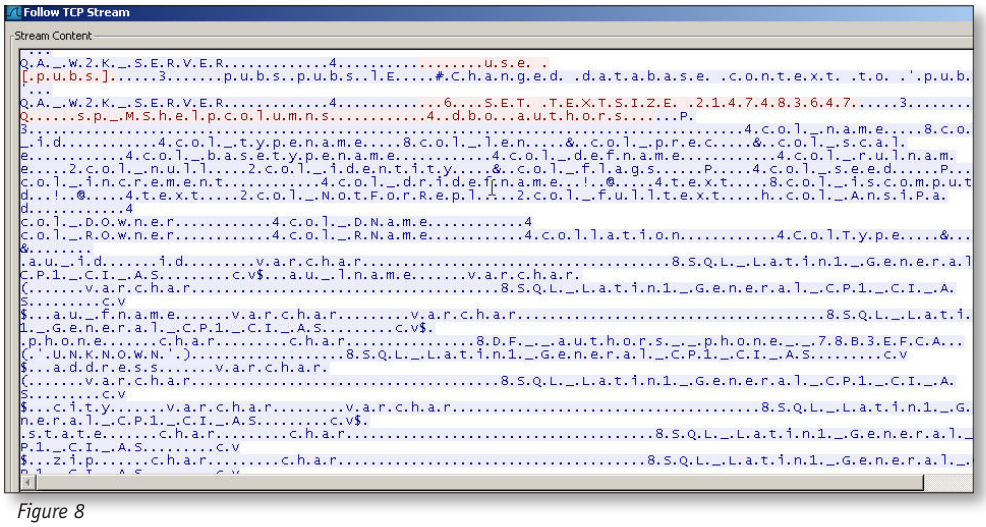

Figure 8

This window accurately displays the data contained within the packets. However, it does not display this data in a way that helps us resolve problems when it comes to protocols such as SQL. The data contained above is from a SQL transaction. It is possible to pick out some of the information, but it is difficult to determine which part of this is the return data and which is the SQL call.

When using the ClearSight Analyzer, each one of the SQL calls is broken out as a separate data flow. This allows us to clearly see the SQL call as it was sent to the SQL server.

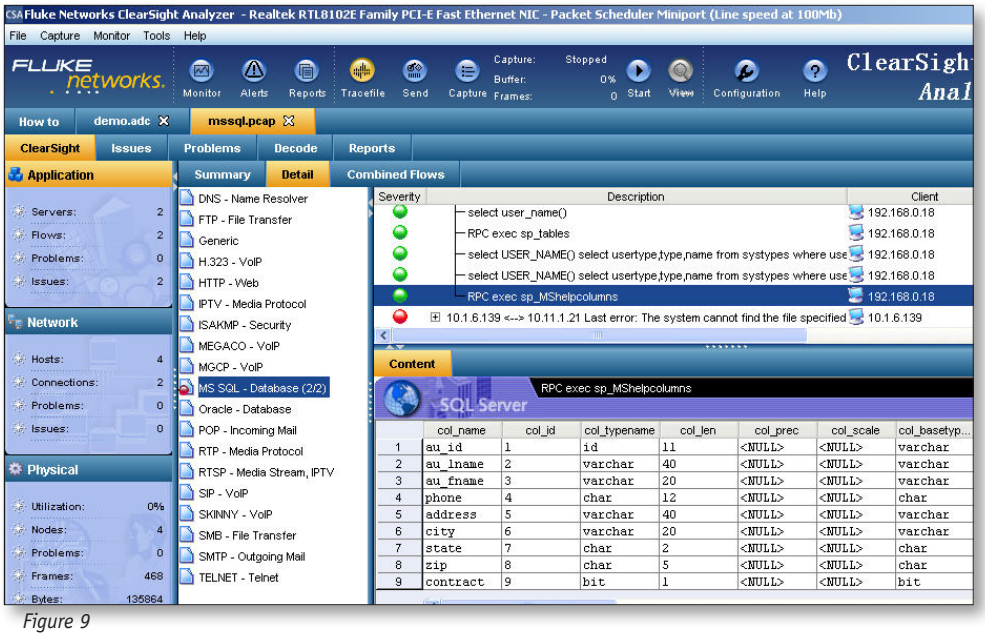

Figure 9

By clicking on a flow, the ClearSight Analyzer will reassemble the return data for the call and display it in a way that can be easily understood and analyzed. There is no need to dig through cryptic data dumps looking for values.

Through this single view, we can look at the delta time between each one of the application packets. By looking for large delta times between the packets, we are able to quickly identify when the application is being slowed down.

Data Flow Ladder Diagrams

It is said that a picture is worth a thousand words. When analyzing applications, a picture can be worth thousands of minutes of analysis time! Being able to view the flow of data in a graphical format, instead of looking at a series of individual packets, allows the analyst to quickly find delays and errors. Both Wireshark® and the ClearSight Analyzer provide the ability to display the data flows in a graphical manner. The key difference between the two analyzer is the way they display these flows. To illustrate this, we have selected the same data flows from the same trace file.

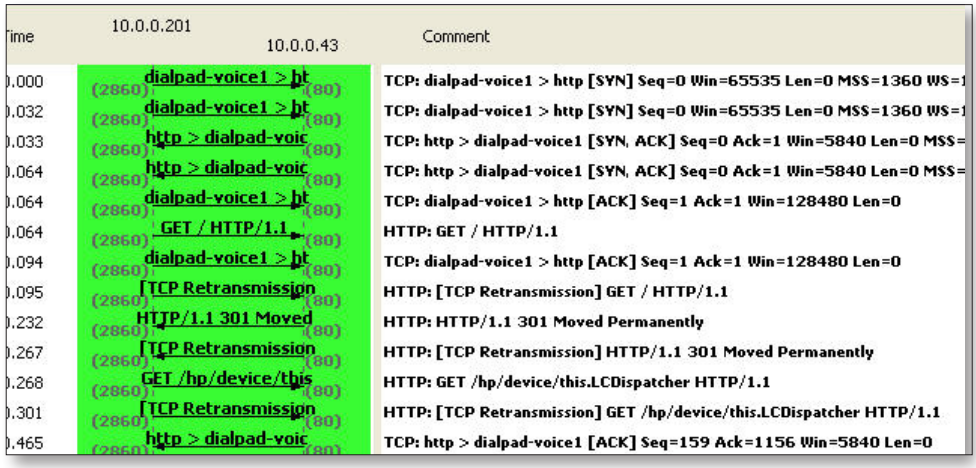

Figure 10

Above is the data flow as shown with Wireshark®. This flow diagram does give us some idea of the flow of the traffic between the client and the server. From an analysis standpoint, we are interested in the TCP connection setup, the HTTP request, and the HTTP response. The time it takes to perform these tasks will help us determine if this flow is contributing to the overall application delay. Wireshark® shows us this, in addition to all of the TCP frames going back and forth between the client and the server. This excess information makes it difficult to focus in on the transactions related to the application delays. The time value shown on the left is displayed as the number of seconds since the start of the trace. In order to determine the location of the delays, we must calculate the time between packets manually.

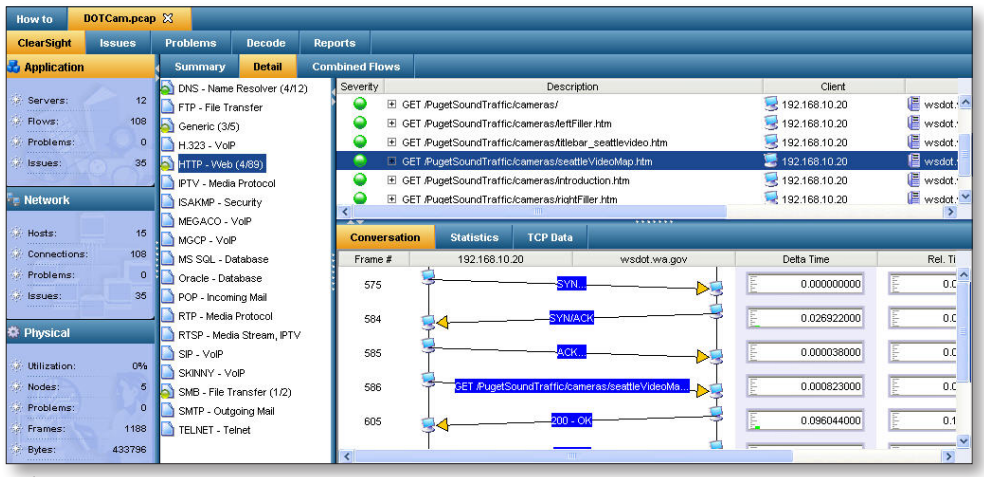

Figure 11

The ClearSight Analyzer displays those packets required to perform application-centric analysis and hides those that are not necessary to perform this analysis. In the example above, the ClearSight Analyzer displays the packets associated with the establishment of the TCP connection. The delta time between these packets give us an idea of the roundtrip time between the client and the server. Instead of showing all of the packets involved in the transaction, we see the request sent by the client (frame 586) and the reply sent by the server (frame 605). The delta time between these frames gives us an idea of the time required by the server to respond to this request. By condensing the flow down to the key frames, it is easy to display the entire transaction on a single screen. To display this same transaction within Wireshark® requires multiple screens, making it difficult to quickly determine the time between the start and the end of the transaction.

Combined Data Flows

One of the challenges encountered with troubleshooting applications is determining whether the problem is a network related problem, or whether it is a server related problem. Capturing on both ends of the connection and combining the data flows is one method of quickly answering this question. This is a case where Wireshark and the ClearSight Analyzer can be combined to provide a comprehensive analysis solution.

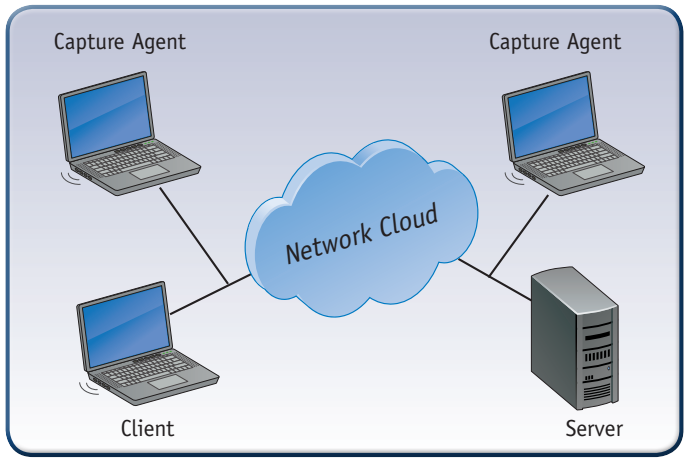

Figure 12

Wireshark can be used to capture the packets on both sides of the connection between the client and the server. Once these captures have been completed, it is necessary to combine them into one single view for analysis. While the Mergecap utility is available as part of the Wireshark installation, it does not provide a means to synchronize the timing between the two traces. The resulting merged trace file will contain all of the packets, but will not provide the useful information necessary to troubleshoot the application.

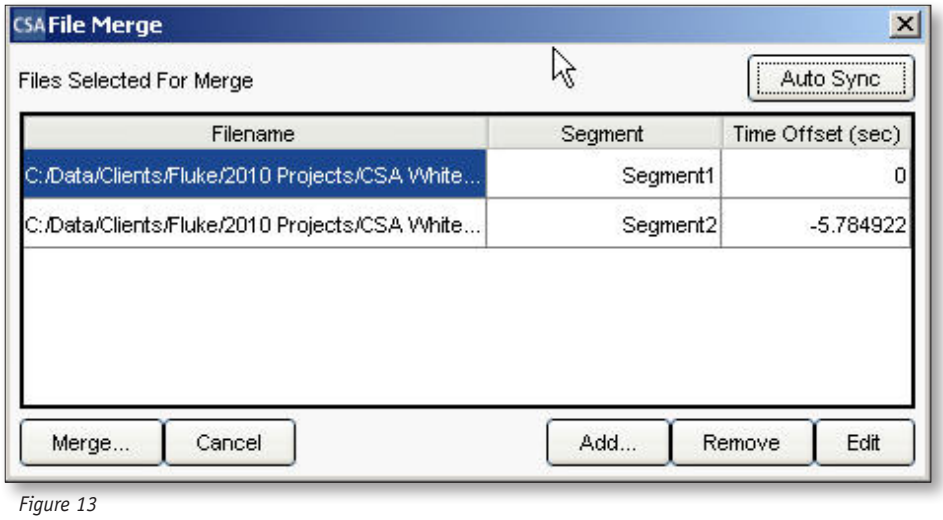

Figure 13

The ClearSight merge utility will not only merge the two trace files, but synchronize them so that they can be combined into a single view that will illustrate the amount of time spent traversing the network verse the amount of time spent by the server responding to the request.

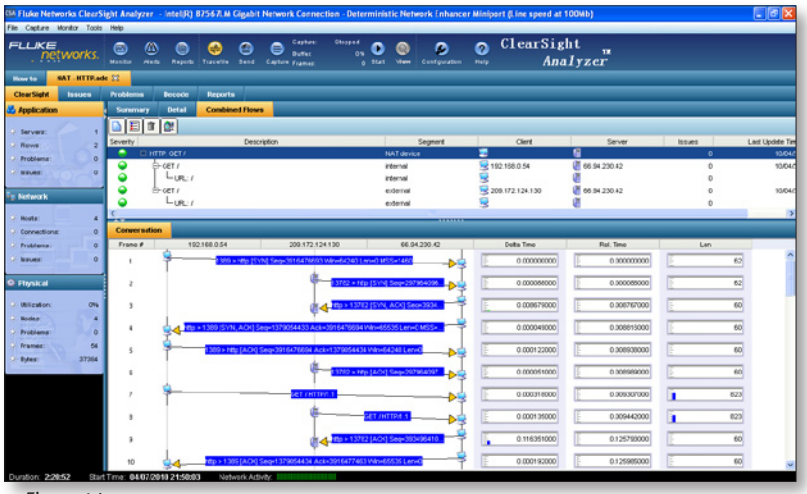

Figure 14

The combined flow diagram above is an example of a case where Wireshark was used to capture the packets on both sides of the WAN connection. The ClearSight merge utility was used to synchronize the two traces and merge them into a single trace file. The Delta Time column to the right of the ladder diagram indicates the amount of time between each of the frames. Using this time, we can determine how long it took for a single frame to traverse the WAN.

Performance Matrix

	Flow 1	Flow 2
Throughput(Kbps)	50.219	49.876
Network Time(sec)	0.032227	0.031132
Client Time(sec)	1.188474	2.806010
Server Time(sec)	12.296878	10.686421
TCP Connection(sec)	0.064454	0.062265
First Byte Downloading(sec)	0.266802	0.200721
Min Client Window Size(KB)	63586	63586
Max Client Window Size(KB)	65535	65535
Min Server Window Size(KB)	5450	5450
Max Server Window Size(KB)	5840	5840
Retry	0	1
Out of Sequence Count	0	1
Packet Loss	0	0
TCP Turns	56	52

Figure 15

The Performance Matrix within ClearSight can then be used to summarize the response times. This allows us to determine exactly how much time was taken by each component.

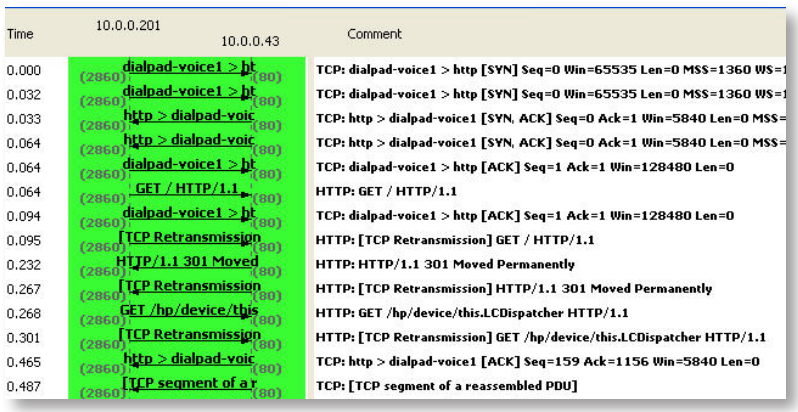

Figure 16

By comparison, this is the ladder diagram we get when using Wireshark to view the same trace. While it does show the frames going back and forth, it is difficult to determine which delays are related to the server and which are related to the network.

Report of Application Traffic

At the conclusion of the analysis, it is important to be able to report on the application traffic seen in the captured files. Once the problem has been isolated, it may be necessary to share these findings with other groups within the same organization or with the application vendor. Other than printing out the raw packets, the Wireshark analyzer does not provide a reporting feature.

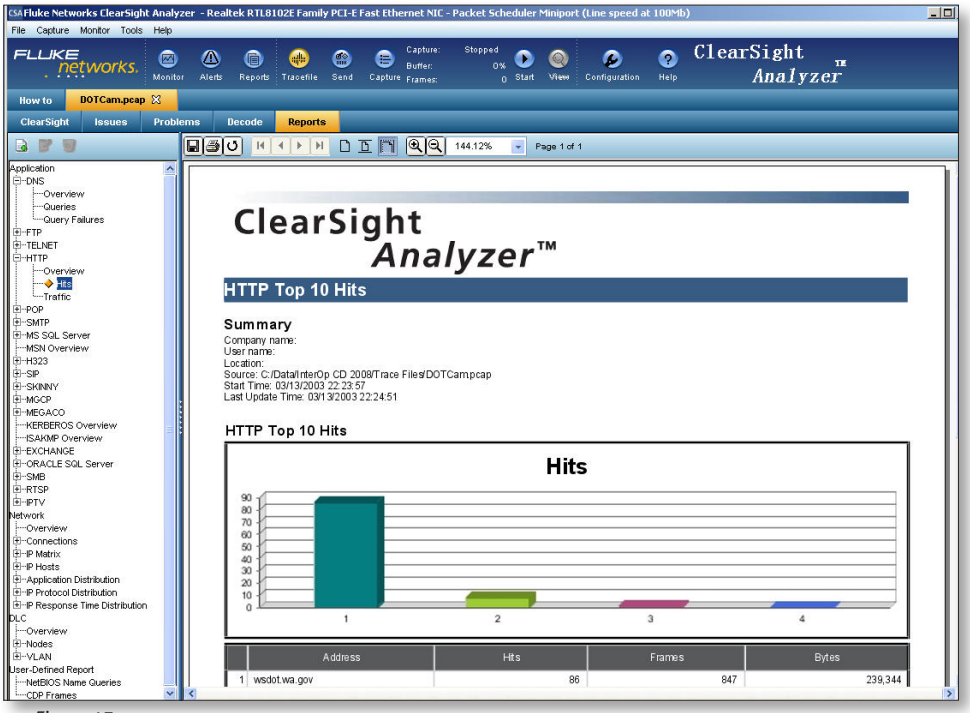

Figure 17

The ClearSight Analyzer does provide a comprehensive report generator. Reports can be generated on the overall network traffic, individual protocols or applications such as Voice Over IP.

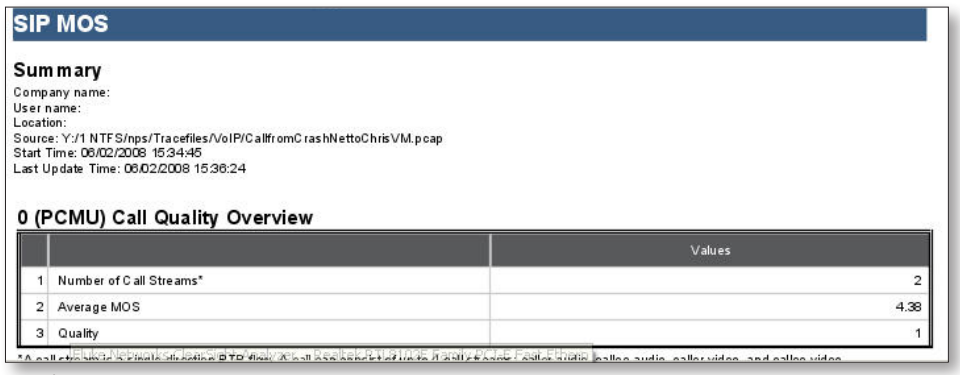

Figure 18

In the case of Voice over IP, the ClearSight Analyzer will analyze each VoIP call and calculate a Mean Opinion Score (MOS). The MOS provides an indication of the quality of the call. Using the SIP report within the ClearSight Analyzer, we can produce a summary report showing the total number of calls captured and the distribution of MOS values for those calls. This type of reporting saves many hours of analysis and report generation work on the part of the network engineer. If the quality of the voice traffic is in question, a capture can be taken and a report generated quickly to show whether there is a measurable problem or whether the issue may reside somewhere other than the network.

Analyzer Feature Summary

Analysis Feature	Wireshark	ClearSight
Combined Data Flows	❍	●
Application Layer Ladder Diagram	❍	●
Application Layer Overview	❍	●
Detailed Packet Decode	●	●
Reassembly of SQL Queries	❍	●
Expert Analysis	❍	●
Detailed Reports	❍	●
Server Response Time Summary	❍	●
Summary	Free, but costs associated with time to actually solve the problem	Pays for itself through time saved with analysis, increased productivity and job satisfaction of network support staff

Figure 19

Conclusion

Getting to the root cause of application problems quickly is key to reducing the impact they have on business operations. While traditional protocol analyzers, such as Wireshark are useful for capturing packets and performing basic analysis on the lower layers such as IP and TCP, they fail to provide the view into the application layer. Using a product such as Fluke Networks' ClearSight Analyzer allows the analyst to take a top down approach to resolving the application problem.

Combining these two protocol analyzers is a cost-effective means to solving tough performance problems. An entire department and remote staff can be freely equipped with Wireshark for capture and basic packet viewing, and application-centric analysis can be done with one or more instances of ClearSight Analyzer. For problems that span central and remote sites, the staff can capture packets on both ends of the network using Wireshark, then use ClearSight Analyzer to synchronize the timing between the two traces and merge them into a single trace file. Through the use of ladder diagrams, expert analysis, and summary reports, the ClearSight Analyzer can help the analyst to quickly identify the root cause of the problem.

For more information visit the Application-centric Analysis Resource Center at **www.flukenetworks.com/app-centric**
Contact Fluke Networks: Phone **800-283-5853** or **Email: info@flukenetworks.com**.

For a free trial to see how ClearSight can reveal answers in Wireshark traces, go to **www.flukenetworks.com/csatrial**

Fluke Networks
P.O. Box 777, Everett, WA USA 98206-0777

Fluke Networks operates in more than 50 countries worldwide. To find your local office contact details, go to **www.flukenetworks.com/contact**.