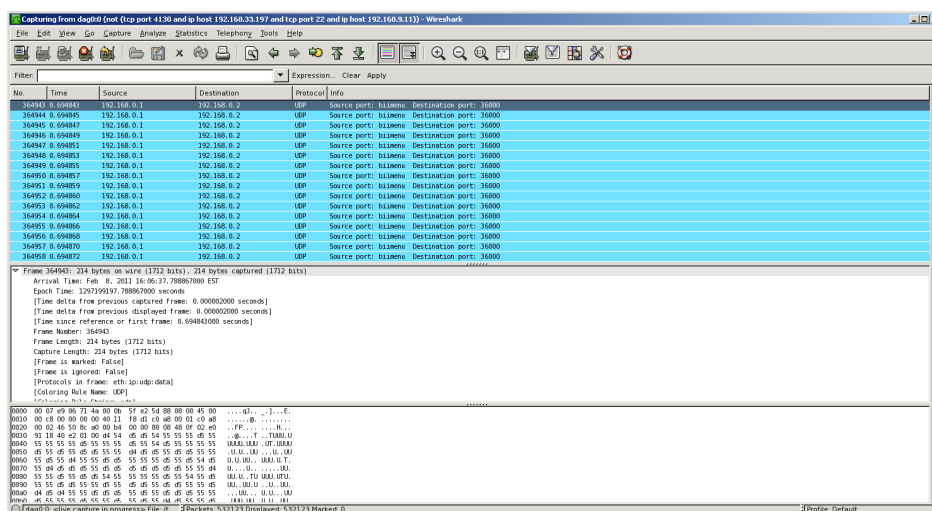




Wireshark



Wireshark® is a network protocol analyser that allows you to capture and interactively browse network traffic. It has a rich and powerful feature set and is one of the most popular tools of its kind. Network professionals, security experts, developers, and educators around the globe use Wireshark regularly as a key application in their suite of monitoring tools.

Freely available as open source software, Wireshark is released under the GNU General Public License version 2. The application is developed and maintained thanks to the contributions of a global team of protocol experts.

Wireshark “understands” the structure of different networking protocols. It is able to display the encapsulation and the fields, along with their meanings, of different packets specified by different networking protocols.

Wireshark’s most powerful feature is its vast array of display filters (over 105,000). These filters allow you to drill down to the precise traffic you want to see and are the basis of many of Wireshark’s other features, such as the colouring rules.

Wireshark uses PCAP to capture packets, and as such can only capture packets on the types of networks that PCAP supports.

WHAT IS NETWORK ANALYTICS?

Network Analytics is a specific technique that enables an analyst to use a protocol analyser to drill down into the packets captured from a network to troubleshoot network problems, examine security problems or to debug protocol implementations.

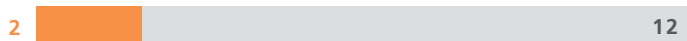
KEY FEATURES

- Data can be captured via an EndaceProbe™ or EndaceSensor™
- Captured network data can be browsed via a GUI or via a command-line utility
- Data display can be refined by using a display filter
- Plug-ins can be created for analysing new protocols
- Wireshark native trace file format is the libpcap format supported by libpcap and WinPcap

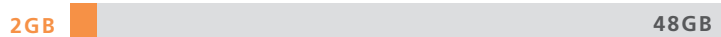


PERFORMANCE INDICATORS

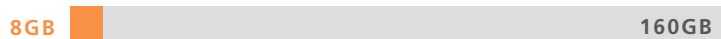
PROCESSING CORES



MEMORY



STORAGE



* Guidelines based on simulated usage in Endace Application Dock Lab environment testing conducted on an EndaceProbe 7000

KEY

- Used capacity on EndaceProbe
- Available capacity on EndaceProbe

APPLICATION DOCK LAB ENVIRONMENT

The Endace Application Dock Lab environment is designed to simulate a real-world deployment of the Application Dock Partner's applications on EndaceProbes. The typical architecture for a deployment in the Endace Application Dock Lab environment consists of the following three nodes:

- Agent – the partner's agent application is used in the collection of the network traffic
- Server – the partner's server application is used to display, report and analyse traffic collected by the Agent application for a set purpose
- Traffic Replay – the Traffic Replay server replays a captured file containing network traffic, simulating live network traffic.

Testing methods may differ and are dependent on the Endace Application Dock partner's application requirements.



Wireshark is developed and maintained thanks to the contributions of a global team of protocol experts. Wireshark is freely available as open source software and is released under the GNU General Public License version 2.

www.wireshark.org

APPLICATION DOCK PARTNER PROGRAMME

To ensure a predictable customer experience, Endace has established the Application Dock Programme. The programme provides application vendors with a structured method for testing and validating the performance of particular applications in the Application Dock environment. Deploying applications into the Application Dock environment offers organisations a number of important and valuable benefits, including:

- Improved application performance
- Reduction in hardware
- Improved workflow
- Improved flexibility and agility

For more information about the Endace Application Dock Partner Programme, please visit endace.com.

For more information on Endace products visit: endace.com
For enquiries email: enquiries@endace.com

Note: All trademarks referred to are the property of their respective owners.