PECB

*When Recognition Matters*


# THE COMPARISON OF PROGRAMS FOR NETWORK MONITORING

Imagine a working environment comprised of a number of switches, routers, some terminals and file servers. Network performance decreased during last days and the reason is unknown. There is no Intrusion Detection System IDS that can alarm or inform for attacks or malfunctioning of the network. Slowdowns in the network performance, connectivity loss or shutting down of terminals within the network for unknown reasons, are among the other problems.

Reasons for all these can be different, such as poor configuration of network architecture, or use of unrequired routing protocols, etc. However the continually increase of network security threats can also be one of the most frequent reasons for this network condition. Different attacks by bad guys who can put web server out-of-service through Denial of Service (DoS) attack, sending traffic with a poisoned ARP in an attempt to discover hosts, or by simply infecting ports with malware to form part of an alien network or botnet, etc.

What can be done in such cases? Taking care of the network by having information regarding the source address of the attack would be one of the possibilities. This can be done by constantly monitoring the computer networks for slow or failing components and notifying the network administrator via email, SMS or other alarms in case of outages. This kind of policy is part of network maintenance and network management.

However, to protect and analyze traffic in network it is very important to have different software/programs that are designed to control, analyze and filter packets that carry our very important data. In general these programs will help us to:

1. identify and analyze network security threats associated with security gateways;
2. define network security requirements for security gateways based on threat analysis;
3. use techniques for design and implementation to address the threats and control aspects associated with typical network scenarios; and
4. address issues associated with implementing, operating, monitoring and reviewing network security gateway controls.

A search on the Internet will reveal many network analyzers available. Some network analyzers provide basic functions, such as packet sniffing that makes them ideal for simple tasks. Others give you all the necessary tools and functions to finish the work in the best possible way.

# WIRESHARK

Wireshark is an open-source network sniffer and packet analyzer designed by Gerald Combs. Its main aim is to analyze the traffic and to resolve network problems. This network packet analyzer will try to capture network packets and to display that packet data as detailed as possible.
The following are some of the other important aspects of Wireshark:

•Available for UNIX and Windows.
•Capture live packet data from a network interface.
•Display packets with very detailed protocol information.
•Open and Save packet data captured.
•Import and Export packet data between programs.
•Filter packets on many criteria.
•Search for packets on many criteria.
•Colorize packet display based on filters.
•Create various statistics, etc.

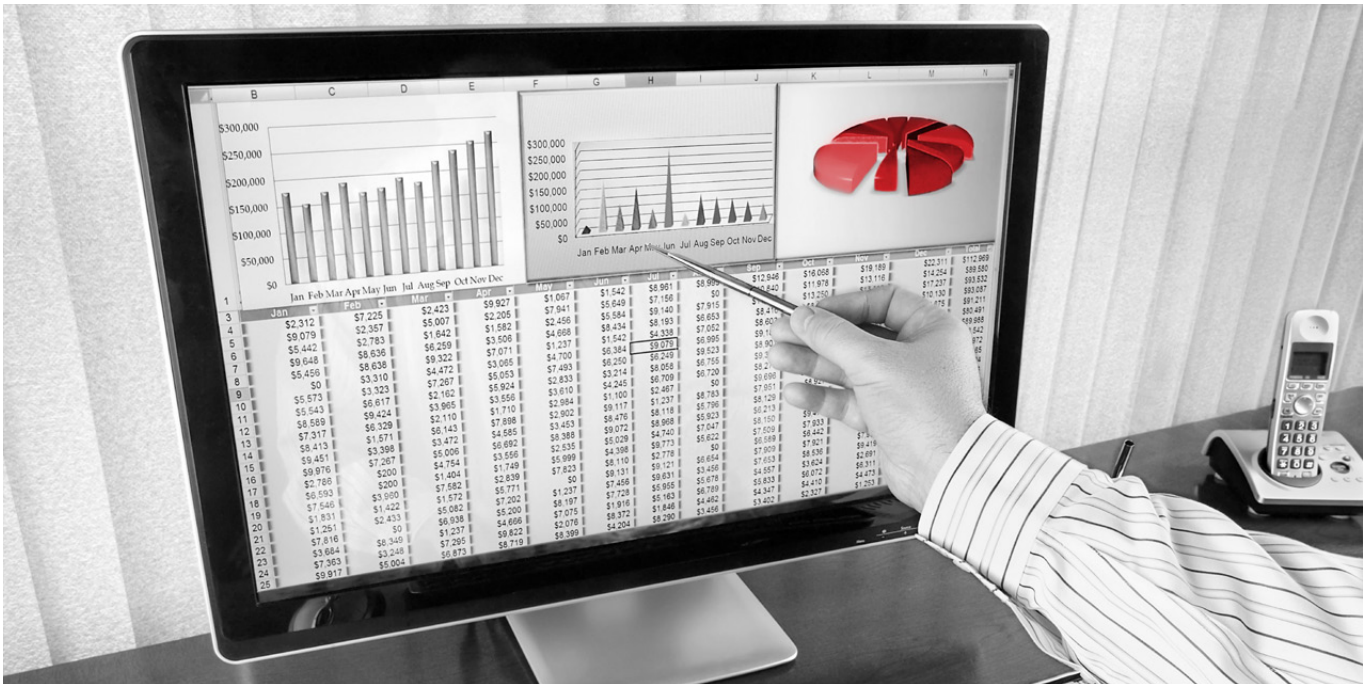
Wireshark offers various benefits that make it attractive for daily use. It is attractive for daily users as well as for experts for analyzing packets since it offers various opportunities for everyone.

Supported protocols –Wireshark is distinguished for a number of protocols, it supports more than 1100, starting from simple ones such as IP and DHCP up to those more advanced and proprietary such as Apple Talk and Bit Torrent.

User-friendliness –Wireshark interface is one of the easiest methods for analyzing any packet. It is based on GUI, with very clear written context menus. It also offers various opportunities designed for an easier use. It also provides several features designed to enhance usability, such as protocol-based color coding and detailed graphical representations of raw data. The Wireshark GUI is great for those who are just entering in the world of packet analysis.

Cost -Since it is open source, Wireshark's pricing cannot be beaten: Wireshark is released as free software. Wireshark can be downloaded and used for different purposes, personal or commercial.

Program support – When you deal with free software like Wireshark you may not have official support, which is why the open source community often relies on its user base to provide support. Luckily for us, the Wireshark community is one of the most active of many open source project.
Operating system support Wireshark supports all major operating systems like Windows, Mac OS X, and Linux-based platforms.



## MICROSOFT NETWORK MONITOR

Network Monitor is another tool that is used to collect information from network packets that travel during communication. One of the main functions of Network Monitor is the use for network trouble-shooting tasks.

This is possible because the data that are collected from different packets contain:

•the source address of the computer that sent a frame onto a network
•the destination address of the computer that received the frame
•the protocols used to send the frame
•the data, or portion of the message being sent, etc.

The main function of Microsoft Network Monitor is to collect information using a process known as capturing. What should be considered is:

•where to take and start capture,
•how to gather documentation and use a cheat sheet,
•how to customize what information should be captured,
•how to customize the user interface,
•how to make sense of the captured data,
•how to get more information out of the data that's captured, and
•how to view specific frames in an XML format and in a window by themselves.

## COLASOFT CAPSA

The network analyzers Colasoft Capsa is perfect in that way that it helps network specialists to improve network performance, enhance network security and troubleshoot network problems. Capsa is a portable network analyzer for both LAN and WLAN which has real-time packet capturing, 24 hours a day network monitoring, in-depth packet decoding, advanced protocol analysis and automatic expert diagnosis. It provides a high-level and comprehensive visibility to the entire network, helps network engineers pinpoint fast and resolve different application problems, and therefore advance the experience of the user and guarantee a productive network environment.
Capsa is a great network tool which helps to lower IT cost, improve network security and enhance customer service. The reason that it can capture packets in real time, do automatic network events diagnosis, decode and analyze accurate protocol, combine powerful filters and information statistic of global network.

Some of the Colasoft Capsa features are:

•Capture real-time and save data transmitted over local networks, including wired network and wireless network like 802.11a/b/g/n;
•Identify and analyze above 300 network protocols, as well as network applications based on the protocols;
•Monitor network bandwidth and usage by capturing data packets transmitted over the network and providing summary and decoding information about these packets;
•View network statistics with one view allowing easy capture and interpretation of network usage data;
•Monitor Internet, e-mail and instant messaging traffic;
•Diagnose and pinpoint network problems quickly by detecting and locating ominous hosts;
•Detect the details, including traffic, IP address, and MAC, of each host on the network, allowing for easy identification of each host and the traffic that passes through each;
•Visualize the entire network that shows the connections and traffic between each host.

## CONCLUSION

As a conclusion, we can say that Wireshark comes with countless functions that help us analyze multiple network problems; not only those caused by poor configuration or device failures, but also a wide range of external and internal. It is a good idea to make the network administrators aware of the importance of using this type of tool, as it is a key utility to help find the source of some problems that would take a great deal of time to discover by other means, with the repercussion that comes with it in terms of availability and information confidentiality taking precedence over the rest of your services.

Using filters through which we can purge and perform more rigorous analysis of traffic, as well as other Wireshark functions *(Follow TCPStream, Expert Info, etc.)*. Lastly, we have seen how to use graphs to interpret the benefits and efficiency of our network in Wireshark. Wireshark, apart from being one of the best protocol analyzers today, is an excellent source of knowledge for any network or communications enthusiast.

In the other hand Microsoft Network Monitor is a very useful tool that allows network administrator to keep track of what is being sent across the network on the lowest level. The tool provides functionality to explore what packets are being sent across the network and where they are being sent from. This is the main idea to detect spoofing actions in network. That is the reason why we can say that Network Monitor monitors a network for threats from the outside, and monitors the network for problems caused by overloaded and/or crashed servers, network connections or other devices. Its best point is the fact that divides packet by applications in a familiar sight that we can see in a frame pane, and have very useful way of telling the conversation between the end hosts in Network Conversations pane.

Colasoft Capsa Network Analyzer offers various improvements that make it pleasant to work with and easy for anyone to find the information needed. Its functions such as the Diagnosis, Matrix and Reports surely make it unique and can be invaluable for anyone who troubleshoots network errors. Every person that has very elementary knowledge for network in general, can give an opinion, form a formulary, or give a report using Colasoft towards network and its performance. This is the reason why Colasoft is preferred by lots of companies.

Rreze Halili is the Security, Continuity, Recovery (SCR) Product Manager at PECB. She is in charge of developing and maintaining training courses related to SCR. If you have any questions, please do not hesitate to contact: scr@pecb.com.

For further information, please visit http://www.pecb.com/site/renderPage?param=139