17. tétel How to use **Wireshark ( network analysis tool)** to capture, filter and inspect packets

I am an IT engineer and work for a multinational company which deals with the network security risk assessment. I have heard that you aren’t familiar with the network traffic analysis so I would like to present you **Wireshark, the network packet analyser**. You could think of it as a measuring device used to examine what’s going on inside a network cable. In the past, such tools were either very expensive, proprietary, or both.

**Network traffic analysis** is primarily done to get in-depth insight into what type of traffic/network packets or data is flowing through a network. Typically, network traffic analysis is done through a **network monitoring** or network bandwidth monitoring software/application. Here are some examples **people use** Wireshark for: network administrators use it to *troubleshoot network problems;* network security engineers to *examine security problems;* developers to *debug protocol implementations* and others to *learn network protocol* internals.

**Wireshark** is a network analysis tool which **captures packets** in real time and **display them** in human-readable format. It includes filters, color-coding and other features. You can use Wireshark to **inspect** a suspicious program’s network traffic, **analyse** the traffic flow on your network or **troubleshoot** network problems.

The following are **some of the many features** Wireshark provides:

* **Capture live packet data from a network interface.** Wireshark can capture traffic from many different network media types - and despite its name - including wireless LAN as well. After downloading and installing Wireshark, you can **launch** it and double-click the name of a network interface under Capture to **start capturing packets** on that interface.
* **Display packets with very detailed protocol information.**
* **Filter packets on many criteria**. If you’re trying to **inspect something specific**, such as the traffic, a program sends when phoning home, it helps to close down all other applications using the network so you **can narrow down the traffic**.
* **Search for packets on many criteria.**

## **Colorize packet display based on filters.** Colour Coding: You’ll probably see packets **highlighted** in a variety of different colours. Wireshark uses colours to help you identify the types of traffic at a glance. You can also customize and modify the colouring rules.

* **Open files containing packet data.**

## **Create various statistics.**

* **Import files from many other capture programs**. Wireshark can open packets captured from a large number of other capture programs.
* **Export some or all packets in a number of capture file formats.**
* **Save packet data captured**. You can also save your own captures in Wireshark and open them later. Click File > Save to save your captured packets.
* **Available for UNIX and Windows.**

Wireshark is an **open source software** project. You can freely use Wireshark on any number of computers you like, without worrying about license keys or fees. Wireshark is perhaps one of the best open source packet analysers available today.

Here are some things **Wireshark** doe**s not** provide:

* Wireshark isn’t an intrusion detection system. It will **not warn you when someone does strange things on your network** that he/she isn’t allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on.
* Wireshark will **not manipulate things on the network**, it will only "measure" things from it. Wireshark doesn’t send packets on the network or do other active things.

You can **download Wireshark for Windows** or **Mac OS X** from its official website. If you are using Linux or another Unix-like system, you will probably find Wireshark in its package repositories.

Wireshark is an extremely **powerful tool**. Professionals use it to debug network protocol implementations, examine security problems and inspect network protocol internals.