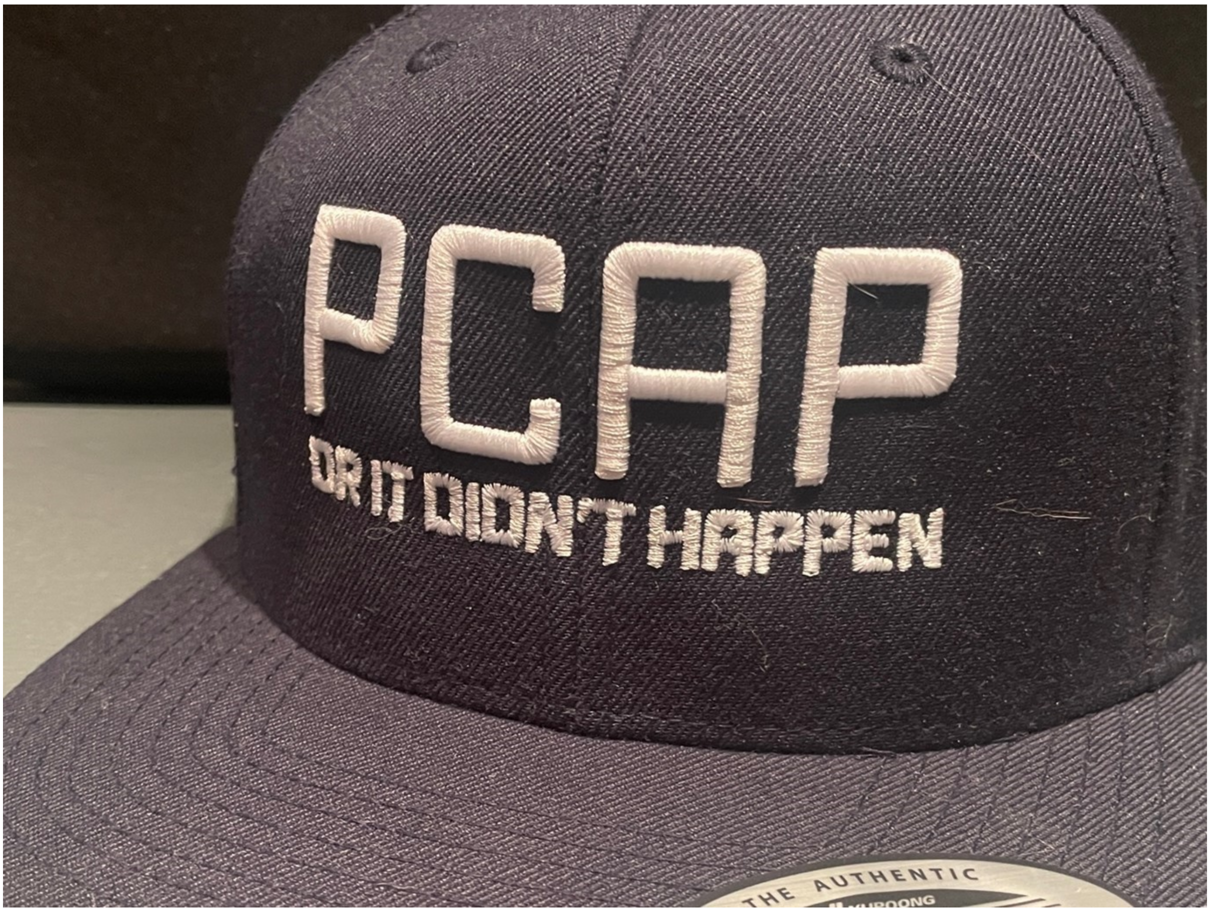
Haapakangas, V. (2023) Did you know that packets are everywhere? TAMK International. 22.2.2023.

URL: https://blogs.tuni.fi/tamk-international/international-event/did-you-know-that-packets-are-everywhere/

Did you know that packets are everywhere?

22.2.2023



Pcap means captured network packets.

In daily life you give and receive packers all the time. Even while reading this blog, your computer is sending out numerous packets, requests, to the server and receiving even more packets, replies, from the server.

These packets are quite important, right? Luckily it is possible to capture these packets from the network. Captured packets are called pcaps or trace-files.

Packet analysis is important

Packet analysis is the process of examining captured packets. This can be done for a variety of purposes, including troubleshooting, security, and performance monitoring, to improve services and data transportation technologies etc.

One of the main reasons why packet analysis is important, is that it allows network administrators and engineers to understand what is happening in their networks. By examining packets of data, they can see which devices are communicating with each other, what protocols are being used, and how much traffic is being transmitted. This information is critical for identifying problems, optimising network performance, and ensuring the security of the network.

Packet analysis is also useful for identifying and troubleshooting problems on a network and in network services. For example, if a device is experiencing connectivity issues, packet analysis can help to determine the cause of the problem. It can also be used to detect and diagnose issues such as latency, jitter, and packet loss, which can all impact the performance of a network services.

In addition to previous uses, packet analysis is also important from a security point of view. By examining packets, security professionals can identify and monitor potential threats, such as malware or cyber attacks. This allows them to take appropriate measures to protect the network and its users.

How is packet analysis done?

Packet analysis can be accomplished using a variety of tools. These tools collect and process network traffic, and provide detailed information about each packet, including the source and destination IP addresses, port numbers, packet size, and the protocol used.

One of the most famous packet analysers is a program called Wireshark. Wireshark enables you to see what's happening on your network at a microscopic level. Wireshark development thrives thanks to the volunteer contributions of networking experts around the globe and is the continuation of a project started by **Gerald Combs** in 1998. [1]

Gerald Combs at Sharkfest22 Europe event.

Sharkfest [2] is an event for Wireshark users and developers, and it is held annually in the United States, Europe, and Asia. The Sharkfest22 Europe was held in Estoril, Portugal. This time I got to participate as a speaker when my proposal “Learning Bluetooth Low Energy with Wireshark” was accepted as presentation. In general, presentations at Sharkfest are of highly technical and quite in-depth analysis of packets. My presentation was more pedagogical, and its main goal was to share thoughts about the use of Wireshark as an aid for studying various communication protocols. The presentation was well accepted, and it was great to be able to have a speech in such a high-level conference to people for whom analysing packets is a matter of the heart.

In summary, packet analysis is a crucial tool and skill for many professionals who, with their own contribution, improve the opportunities for all of us to operate in a digitised world.

Text: Ville Haapakangas, Senior Lecturer in Industrial Engineering and a Wireshark enthusiast

Pictures: Ville Haapakangas

References:

[1] Wireshark: https://www.wireshark.org/

[2] Sharkfest: https://sharkfesteurope.wireshark.org/about