Packet sniffers, also called protocol analyzers, are tools that network security technicians use for diagnosing problems in the network. On the other hand, hackers use packet sniffing for malicious purposes such as spying on a network’s traffic and gathering user passwords.

Packet sniffers are of different types. Some of them are dedicated hardware solutions whereas others are available as software applications running on standard computers. These applications use network hardware on host computer for carrying out packet capturing and injection tasks.

**How Do Packet Sniffers Work?**

Packet sniffers intercept and log network traffic visible through a wireless or wired network interface. On a wired network, the information you can capture depends on the network’s structure. Depending on the configuration of network switches, a packet sniffer can see traffic either on the entire network or a particular segment of it. On a wireless network, packet sniffers can mostly capture one channel at a time unless host computer has numerous wireless interfaces that make it possible to capture multiple channels.

Once the raw packet data is sniffed, the software analyzes it and converts it into a readable form for the person using the software. The individual reading the data can now view detailed information of two or more nodes in the network interacting with each other. This information helps network analysts to determine where the fault is, for instance, which devices did not respond to a network request.

Hackers can also misuse packet sniffing to eavesdrop on the packets and access unencrypted data. During this process, they can access critical information such as authentication tokens and passwords. They can also use sniffing for packet injection and man-in-the-middle attacks.

**Common Tools for Packet Sniffing**

There are many free and open-source tools available for packet sniffers. One such very popular tool is Wireshark, which helps you to sniff packets in the field. You can also save the information on a CAP file and analyze it later.

**How to Protect your Network from Packet Sniffing by Hackers**

To check if a malicious user is sniffing over your network, you can use a tool such as Antisniff. Similarly, you can also ensure your network security by using encryption with Transport Layer Security (TLS) or Secure Sockets Layer (SSL). The hacker will still be able to see the source and destination of the information, but the information itself will be in an encrypted gibberish format, thus rendering it illegible for the attacker.

**Final Thoughts**

Though packet sniffers are a very good tool to diagnose network issues, they can also be misused for malicious purposes. It’s important for network analysts to stay up-to-date on new sniffing tools to know how a hacker may use it on their network.