What is Packet Sniffer?

Hackers can use Sniffer to eavesdrop on unencrypted data and see the information exchanged between the two. To better understand Packet Sniffer, as well as Packet Sniffer's operation mechanism, you can refer to the following article of Network Administration.

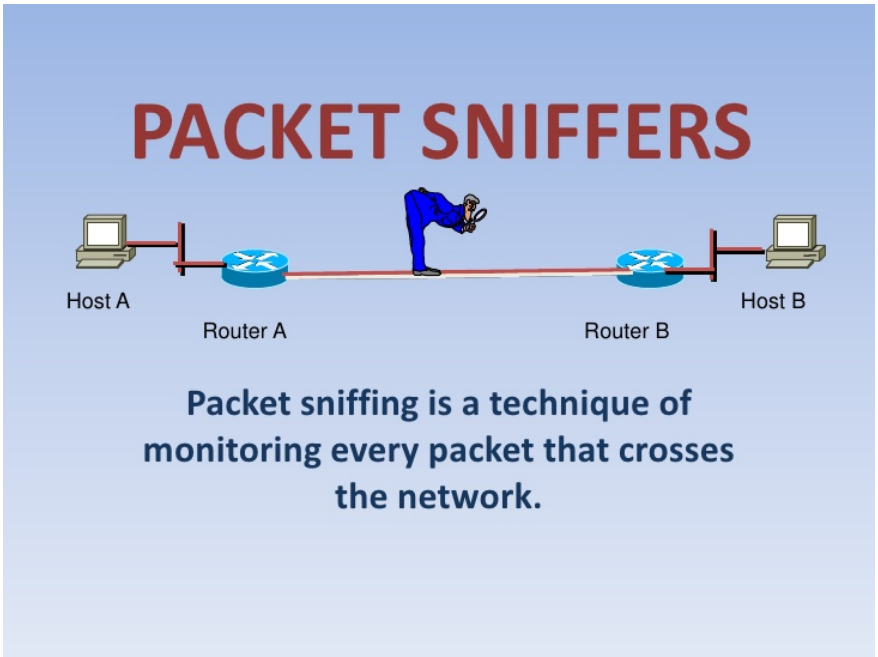
Packet Sniffer or **Protocol Analyzer** are tools used to diagnose and detect network problems and related problems. Hackers use Packet Sniffer for the purpose of eavesdropping on unencrypted data and viewing information exchanged between the two.

Learn about Packet Sniffer

1. What is Packet Sniffer?

Packet Sniffer or Protocol Analyzer are tools used to diagnose and detect network problems and related problems. Packet Sniffers is used by hackers for purposes such as monitoring Network Traffic secrets and collecting user password information.

Some Packet Sniffer are used by technicians for the purpose of resolving hardware while other Packet Sniffer software applications run on standard user computers, using network hardware. provided on the server to perform packet blocking and putting data in.



2. How does Packet Sniffers work?

Packet Sniffer works by blocking Network Traffic, you can see it through a wired or wireless network that Packet Sniffer software accesses on the server.

For wired networks, blocking Network Traffic depends on the network structure. A Packet Sniffer can view all Network Traffic or only view one segment, depending on how the Nework Switch is configured, location .

With wireless networks, Packet Sniffer can only block one channel at a time unless your computer has multiple wireless interfaces that allow multiple channels to be blocked.

After the raw data packet is blocked, Packet Sniffer software will analyze and display the message to the user.

Data analysts can see the "conversation" details that occur between two or more network nodes.

Technicians can use this information to identify errors, such as determining which devices do not meet the network requirements.

Hackers can use Sniffer to eavesdrop on unencrypted data and see the information exchanged between the two. In addition, they can collect information such as passwords and password verification. Hackers can also block capture packets (Capture packets), and attack packets on your system.

3. Software, tools used in Packet Sniffing

Each IT administrator must continually maintain network performance because it is one of the most important resources for the organization. Administrators cannot let the network stop working, even for a few minutes, as this can cause great losses for the company.

At the same time, managing a network with a fixed size is not easy. This is why tools like packet sniffer are always helpful in identifying and troubleshooting quickly. The main task of packet sniffer is to check if packets

are sent, received and transmitted correctly in the network. During the test, packet sniffer can also diagnose various network related problems.

All tools and packet sniffer software will analyze each packet's header and payload. After that, the packages will be categorized and analyzed.

Because packet sniffing is widely used as an effective form of network troubleshooting, there are currently many options available for review.

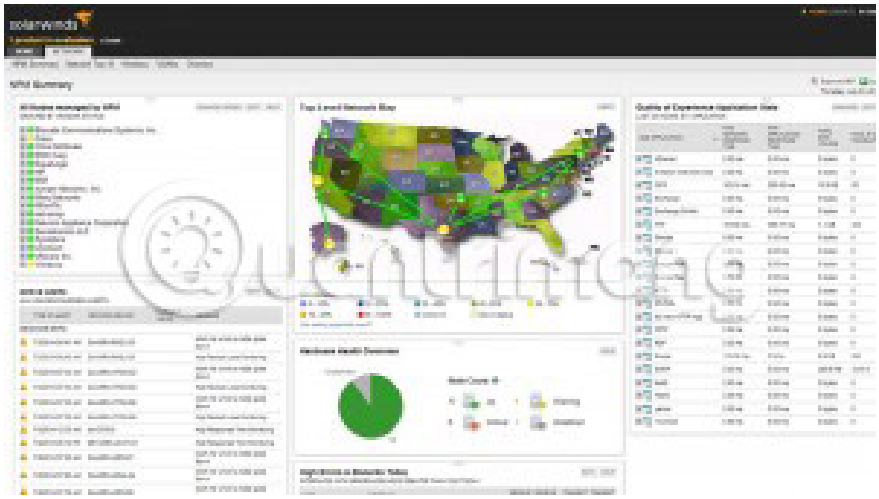
Both Network Engineer (engineers) and Hackers like free tools, which is why open source (open source) software and free Sniffer software applications are selected and used tools. in Packet Sniffing.

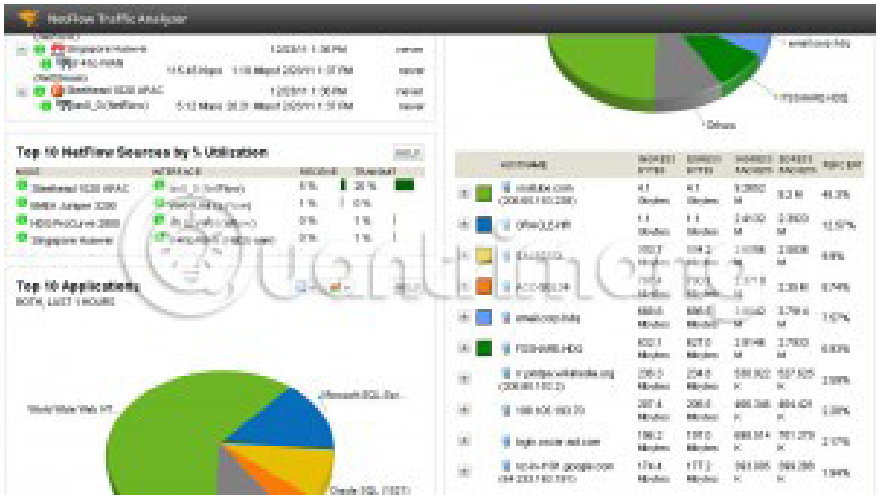
One of the popular open source is: **Wireshark** (formerly known as **Ethereal**).

You can refer to the steps to use Wireshark to analyze data packets in the network here.

Also, you have the following options:

Solarwinds Bandwidth Analyzer 2-Pack





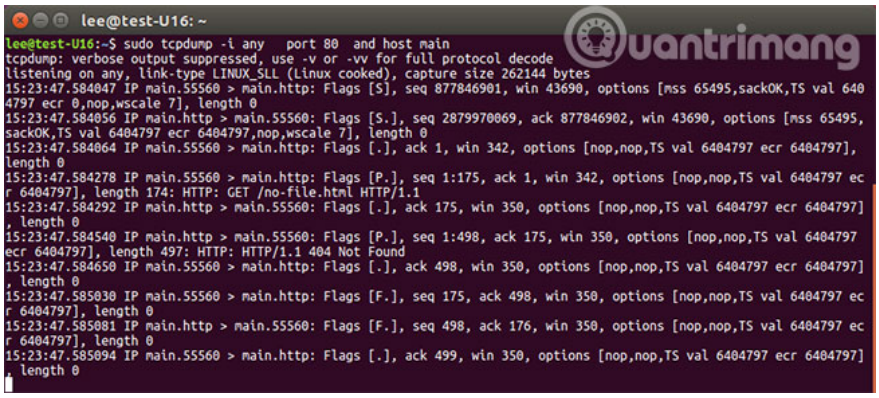
The Solarwinds Bandwidth Analyzer tool is really a two-in-one tool: You have Solarwinds Bandwidth Analyzer (Network Performance Monitor) for error handling, availability and performance monitoring for networks of all sizes, as well as Netflow Traffic Analyzer uses traffic technology to analyze network bandwidth performance and traffic patterns. Both applications are integrated in Solarwinds Bandwidth Analyzer.

Network Performance Monitor displays the response time, availability and performance of network devices, as well as detects, diagnoses and resolves performance issues through dashboards, alerts and reports. The tool also displays network performance statistics in real time through dynamic network maps.

The **Netflow Analyzer** tool comes with identifying users, applications and protocols consuming their bandwidth, highlighting their IP addresses and displaying detailed traffic data minute by minute. It also analyzes Cisco NetFlow, Juniper J-Flow, IPFIX, sFlow, Huawei NetStream and other traffic data.

Tcpdump.org

TCPDump is a common packet sniffer that runs in the command line.This tool displays TCP / IP packets transmitted over the Internet, so you will know how many packets are transmitted and received, and based on this information, you will be able to identify any problems that occur. in the network.



During the time before Ethereal appeared (this tool is still in use today), TCPDump is the defacto standard for packet sniffing. It doesn't have a nice user interface like Wireshark's and integrated logic to decode application flows, but is still an option for many network administrators. This is a standard that has been tested and used since the late 80s. It can capture and record packages with very few system resources (that's why it's popular among many people). TCPDump was originally designed for UNIX systems and is usually installed by default.

Some important features of TCPDump include:

1. Export information describing packages on the network interface using boolean expressions, to read and understand quickly.
2. Provides the option of writing a package to a file for later analysis or reading from a saved file.
3. Create a comprehensive report after capturing (capturing) packages.This report contains information such as the number of packages received and processed, packets received by filters, packets removed by kernel, descriptions and timestamp.
4. Provides the option to export the package buffer to an output file.
5. The various options of TCPDump allow you to customize the output according to your needs.
6. Works well on most Unix-like operating systems like Linux, Solaris, BSD, Android and AIX.

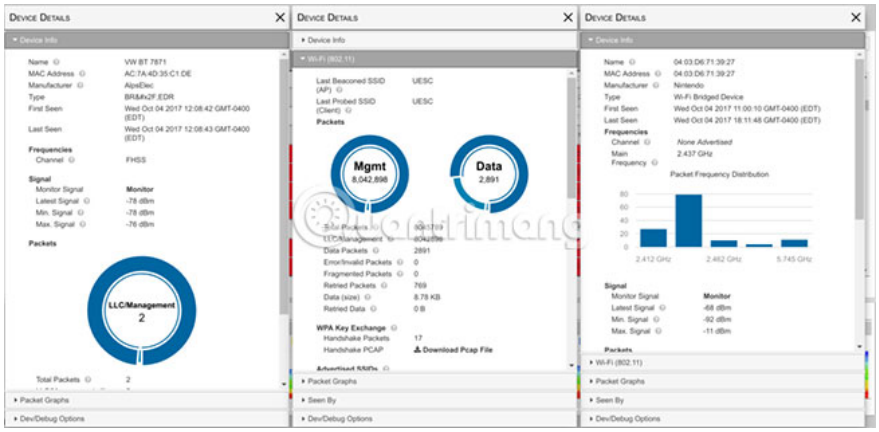
7. TCPdump can be used specifically to block and display contact information for a specific user or computer.
8. In networks with large traffic, users have the option to limit the number of packages captured by the capture tool.This feature makes the output more readable.
9. There are options to drop or add privileges to individual users who want to run TCPDump.

TCPDump is an open-source, free to use tool.

Download TCPDump.

Kismetwireless.net

Kismet is a wireless network, sniffer and intrusion detection system, operating primarily on WiFi.Besides, Kismet can also be expanded to other network types through a plug-in.



In the past decade, wireless networks are an extremely important part of most business networks. Now, people use wireless networks for laptops, mobile phones and tablets. As the importance of offices in these devices increases, the role of wireless networks becomes more pronounced. Packet sniffing on wireless networks has some difficulties with supported adapters and that's when Kismet shines. Kismet is designed for Packet wireless sniffing and supports any wireless network adapter that uses raw monitoring mode. In addition to 802.11 monitoring, it has plugin support for decoding.

Some outstanding features of Kismet include:

1. Support for sniffing 802.11 features
2. Providing PCAP logging is compatible with other packet sniffing tools such as Wireshark and TCPDump.
3. Follow the client / server structure model.
4. There is a plug-in structure, so you can extend the functionality of the core features.
5. Provides the option to export packages to many other tools via an intuitive interface.Exporting these packages can be done in real time.
6. Provides support for other network protocols such as 802.11a, 802.11b, 802.11g and 802.11n.

Kismet is available for free.

Download Kismet.

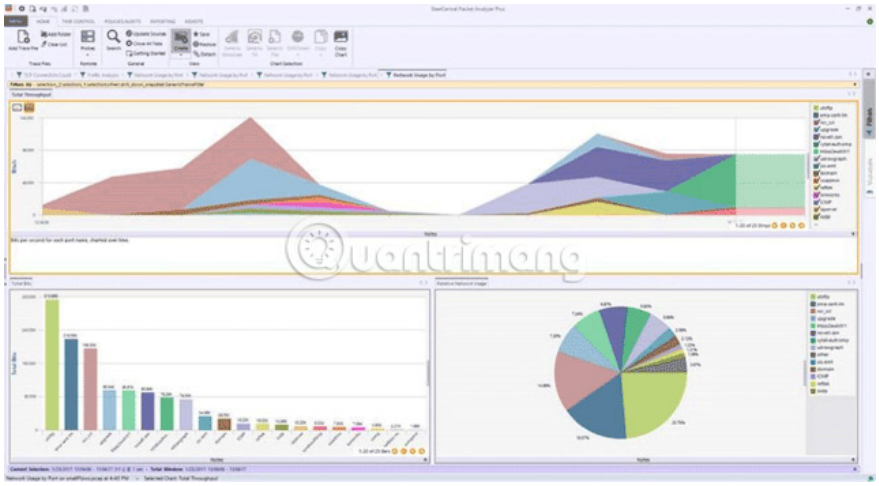
EtherApe

Like Wireshark, EtherApe is an open source free software designed to test network packets. Instead of displaying lots of information in text format, EtherApe aims to represent the captured packets visually, as well as a variety of connections and data streams. EtherApe supports viewing network packets in real time, but can also check the standard formats of existing packages. This provides the admin with another useful tool in troubleshooting network problems.

Link to reference: **http://etherape.sourceforge.net/**

SteelCentral Packet Analyzer

SteelCentral Packet Analyzer is a packet sniffer network from a company named Riverbed.



This tool comes with a variety of powerful features, making IT administrators' jobs easier to breathe:

1. You can easily separate traffic by drag and drop, as well as drill down to multiple levels for interface elements.
2. Comes with a collection of many analytical perspectives.
3. You can configure triggers and alarms to detect abnormal behavior.
4. Scan through millions of packets for prediction and analysis.
5. Allows you to merge and analyze multiple tracking files at the same time, to get a clearer view of network behavior.
6. Accurately identify problems online, in many different cases.
7. Support hundreds of views and charts to analyze network traffic.
8. Charts can be customized or imported / exported in many formats.
9. Custom reports include all-class conversations, IP fragmentation analysis, DHCP address assignments, TCP top talk tools and unicast, multicast and broadcast traffic details.
10. Has an intuitive graphical user interface.
11. Fully integrated with WireShark.

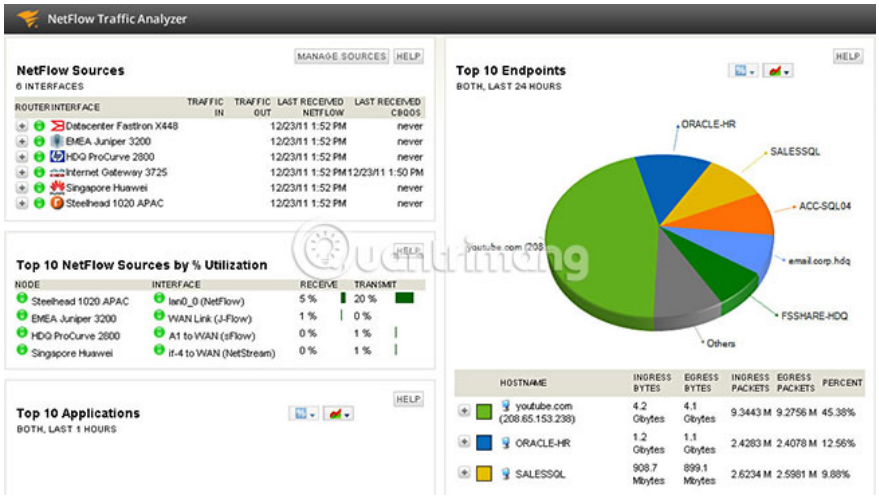
Option:

SteelCentral Packet Analyzer has three versions: SteelCentral packet Analyzer Pro, SteelCentral Packet Analyzer and SteelCentral packet Analyzer Personal. The difference between these three versions is:

Features SteelCentral packet Analyzer Pro SteelCentral Packet Analyzer SteelCentral Packet Personal Edition Works with SteelCentral AppResponse 11 Yes No No Works with SteelCentral Netshark No No Works with trace files (event log files) Yes Yes Yes Works with SteelHead and SteelFusion No Yes No Analyze packages and drill down into Wireshark Yes Yes Yes Quick analysis of capture multi-TB files Yes Yes Yes Indexing Microflow for quick analysis Yes Yes Yes Rich analysis perspective for troubleshooting visual Yes Yes Yes VoIP Decoding Yes Yes Yes FIX Decoding, financial transactions, databases, CIF and ICA protocols Yes Yes No Package sequence diagram Yes Yes No Is there any specific SteelCentral transactions? transactional Analyzer Yes Yes No Multi-segment analysis Yes Yes No View editor No Yes No AirPcap No Yes No

SolarWinds Packet Analysis Bundle

SolarWinds Packet Analysis Bundle network analysis to identify problems quickly. This is an extremely perfect tool, providing a lot of data based on network connections and can assist in handling those issues accurately, quickly and efficiently.



Here are some things SolarWinds Packet Analysis Bundle can do for businesses:

1. Determine if there is a problem with the network or application, and then find out the corresponding troubleshooting method.
2. Identify mutations in data flow and volume, as this may be due to potential security breaches.
3. Continuous scanning of more than 1,200 applications online, so you can better understand your network traffic.
4. Provides a quick view of network traffic at any time.
5. Comes with advanced reporting tools to help you better understand your traffic.
6. Provide insightful information on traffic patterns.
7. Keep track of many different metrics such as response time, data volume, transactions, etc.
8. Classify traffic into different categories based on traffic type, volume and risk level. Such classification makes the analysis process easier.

SolarWinds Packet Analysis Bundle is part of a comprehensive network performance monitor.

Download a 30-day FREE trial of SolarWinds Packet Analysis Bundle .

These are just a few of the packet sniffer available to users. There are still many other options out there. When evaluating packet sniffer, it is important to understand the specific circumstances that you are trying to solve. In most situations, most free tools work well or even better than any paid software. Try some new software and maybe you will find your favorite tool!

4. How to protect network and network system data from Hackers using Sniffer?

If a technician, administrator or you want to see if anyone is using the Sniffer tool on your network, you can use the tool called **Antisniff** to check.

Antisniff can detect if a network interface on your network is put into **Promiscuous** mode **.**

Another way to protect Network Traffic from Sniffer is to use encryption such as **Secure Sockets Layer** (SSL) or **Transport Layer Security** (TLS). Encryption does not prevent Packet Sniffer from source information and destination information, but encryption blocks the payload's data packet to see all of the sniffers are coded incorrectly.

Whether you try to manipulate or inject data into data packets is likely to fail because messing up the encrypted data will cause an error to be evident when the information is encrypted. decoded at the other end.

Sniffer are great tools to diagnose network system problems. However, sniffer is also a useful tool for hackers.

The important thing for security professionals is to get used to this tool is to see how a hacker uses this tool to fight their network.

You can refer to more:

1. Technical Network Address Translation (NAT)
2. Learn about the mechanism of NAT (Network Address Translation) (Part 1)
3. Learn about NAT configuration (part 2)

Good luck!