

wireshark

Wireshark Cheatsheet

Wireshark is a free and open-source packet analyzer that allows you to see what's happening on your network at a microscopic level. Here are some of the key features and commands that you need to know when working with Wireshark.

Key Features

- ▶ **Capture and display packets:** Wireshark can capture and display packets from a wide range of network protocols, including Ethernet, Wi-Fi, Bluetooth, and many others.
- ▶ **Powerful filtering:** Wireshark provides a powerful filtering system that allows you to focus on the packets that matter most to you.
- ▶ **Live capture and offline analysis:** Wireshark can capture packets in real-time, as well as analyze packets that have been captured and saved to a file.
- ▶ **Customizable views:** Wireshark allows you to customize the way packets are displayed, including the color scheme, layout, and more.

Basic Commands

Here are some of the basic commands that you need to know when working with Wireshark:

Command	Description
<code>wireshark</code>	Start Wireshark
<code>wireshark -k</code>	Start Wireshark and immediately start capturing packets
<code>wireshark -r <file></code>	Open a capture file for analysis
<code>wireshark -f <filter></code>	Start Wireshark and immediately start capturing packets with the specified filter






Advanced Commands

Here are some of the advanced commands that you can use when working with Wireshark:

Command	Description
<code>tshark -i <interface></code>	Capture packets on the specified interface
<code>tshark -D</code>	List available capture interfaces
<code>tshark -r <file></code>	Analyze a capture file
<code>tshark -V</code>	Display packet details in verbose mode
<code>tshark -R <filter></code>	Apply a filter to the packets
<code>tshark -z <statistics></code>	Generate statistics on captured packets

Additional Resources

For more information on Wireshark and how to use it, check out the following resources:

- [Wireshark User Guide](#) 
- [Wireshark Tutorials](#) 
- [Wireshark Wiki](#) 
- [Wireshark Mailing Lists](#) 
- [Wireshark Bug Tracker](#) 

Content is available under the Public Domain, by lyuda.io. | Powered by [Wiki.js](#)