



WIKIPEDIA  
The Free Encyclopedia

- Main page
- Contents
- Featured content
- Current events
- Random article
- Donate to Wikipedia
- Wikipedia Shop

- Interact on Wikipedia
- Help
- About Wikipedia
- Community portal
- Recent changes
- Contact page

- Tools
- Print/export

- Languages
- Deutsch
- Español
- فارسی
- Français
- 한국어
- Nederlands
- 日本語
- Русский
- Slovenčina

Edits

Article Talk


Read Edit

Search

## pcap

From Wikipedia, the free encyclopedia  
(Redirected from PCAP)

*This article is about the packet sniffing API. For the projected capacitance technology for touchscreens, see [projected capacitance](#).*

 This article **needs additional citations for verification**. Please help improve this article by adding citations to reliable sources. Unsourced material may be challenged and removed.  
(October 2010)

In the field of computer network administration, **pcap** (packet capture) consists of an application programming interface (API) for capturing network traffic. Unix-like systems implement pcap in the libpcap library; Windows uses a port of bpcap known as WinPcap.

Monitoring software may use bpcap and/or WinPcap to capture packets traveling over a network and, in newer versions, to transmit packets on a network at the network layer, as well as to get a list of network interfaces for possible use with bpcap or WinPcap.

The pcap API is written in C, so other languages such as Java, .NET languages, and scripting languages generally use a wrapper; no such wrappers are provided by bpcap or WinPcap itself. C++ programs may indirectly use the C API or use an object-oriented wrapper.

<b>Contents</b> [hide]
1 Features
2 libpcap
3 WinPcap
4 Programs that use libpcap/WinPcap
5 Wrapper libraries for libpcap/WinPcap
6 References
7 External links

### Features [edit]

bpcap and WinPcap provide the packet-capture and filtering engines of many open source and commercial network tools, including network protocol analyzers (packet sniffers), network monitors, network intrusion detection systems, traffic-generators and network-testers.

bpcap and WinPcap also support saving captured packets to a file, and reading files containing saved packets; applications can be written, using bpcap or WinPcap, to be able to capture network traffic and analyze it, or to read a saved capture and analyze it, using the same analysis code. A capture file saved in the format that bpcap and WinPcap use can be read by applications that understand that format, such as tcpdump, Wireshark, CA NetMaster, or Microsoft Network Monitor 3.x.

The MIME type for the file format created and read by bpcap and WinPcap is application/vnd.tcpdump.pcap. The typical file extensions .pcap, although .cap and .dmp are also in common use.<sup>[4]</sup>

### libpcap [edit]

bpcap was originally developed by the tcpdump developers in the Network Research Group at Lawrence Berkeley Laboratory. The open-source packet capture, capture file reading, and capture file writing code of tcpdump was extracted and made into a library, with which tcpdump was linked.<sup>[5]</sup> It is now developed by the same tcpdump.org group that develops tcpdump.<sup>[6]</sup>

### WinPcap [edit]

WinPcap consists of:<sup>[7]</sup>

- x86 and x86-64 drivers for the Windows NT family (Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7, etc.), which use NDIS to read packets directly from a network adapter;
- implementations of a low-level library for the standard operating systems, to communicate with those drivers;
- a port of bpcap that uses the API offered by the low-level library implementations.

Programmers at the Po Technico d Torino wrote the original code; as of 2008 CACE Technologies, a company set up by some of the WinPcap developers, develops and maintains the product. CACE Technologies was acquired by Riverbed Technology on October 21, 2010.<sup>[8]</sup>

### Programs that use libpcap/WinPcap [edit]

- tcpdump, a tool for capturing and dumping packets for further analysis, and WinDump, the Windows port of tcpdump.
- ngrep, aka "network grep", so it searches in packets, show packet data in human-friendly output.
- Wireshark (formerly Ethereal), a graphical packet-capture and protocol-analysis tool.
- Snort, a network-intrusion-detection system.

EXHIBIT E

Web2PDF

- **Nmap**, a port-scanning and fingerprinting network utility
- the **Bro IDS** and network-monitoring platform.
- **URL Snooper**, locate the URLs of audio and video files in order to allow recording them.
- **Kismet**, for 802.11 wireless LANs
- **L0phtCrack**, a password auditing and recovery application.
- **iftop**, a tool for displaying bandwidth usage (like **top** for network traffic)
- **EtherApe**, a graphical tool for monitoring network traffic and bandwidth usage in real time.
- **Bit-Twist**, a bpcap-based Ethernet packet generator and editor for BSD, Linux, and Windows.
- **Pm**, a network security tool for **ja broken OS** devices.
- **McAfee ePo**cy Orchestrator, Rogue System Detect on feature
- **XLink Ka** Software that allows various LAN console games to be played online
- **Freshfeed**, an extension for the Firefox web browser, that intercepts unencrypted cookies from certain websites (such as Facebook and Twitter) as the cookies are transmitted over networks, exploiting session hijacking vulnerabilities.
- **Suricata**, a network intrusion prevention and analysis platform.
- **WhatPu**se, a statistical (input, network, uptime) measuring application.
- **Xp**co, a network forensics analysis tool (NFAT).

## Wrapper libraries for libpcap/WinPcap [edit]

- **Perl**: **Net::Pcap**
- **Python**: **python-bpcap**, **Pcap**
- **Ruby**: **PacketFu**
- **Tcl**: **tcpcap**, **tcap**, **pktsrc**
- **Java**: **jpcap**, **jNetPcap**, **Jpcap**, **Pcap4j**
- **.NET**: **WinPcapNET**, **SharpPcap**, **Pcap.Net**
- **askes**: **pcap**
- **Objective Caml**: **mlpcap**
- **Chicken Scheme**: **pcap**
- **Common Lisp**: **PLOKAMI**
- **Go**: **pcap** by Andreas Krennmair, **pcap** fork of the previous by Mek Geben, **pcap** developed as part of the **gopacket** package

## References [edit]

- <sup>1</sup> ^ "tcpdump and libpcap latest release" tcpdump & libpcap 2013 05 20 Retrieved 2013 05 20
- <sup>2</sup> ^ "tcpdump and libpcap license" tcpdump & libpcap 2005 02 20 Retrieved 2012 04 13
- <sup>3</sup> ^ "WinPcap Changelog"
- <sup>4</sup> ^ "ANA record of application for MME type application/vnd.tcpdump.pcap"
- <sup>5</sup> ^ **Steve McCanne** "libpcap: An Architecture and Optimization Methodology for Packet Capture" Retrieved December 27 2013
- <sup>6</sup> ^ "TCPDUMP/LBPCAP public repository" Retrieved December 27 2013
- <sup>7</sup> ^ "WinPcap internals" Retrieved December 27 2013
- <sup>8</sup> ^ "Rverbid Expands Further into The Application Aware Network Performance Management Market with the Acquisition of CACE Technologies" Rverbid Technology 2010 10 21 Retrieved 2010 10 21

## External links [edit]

- **Official site** for bpcap (and tcpdump)
- **Official site** for WinPcap (and WinDump)
- **Great list** of publicly available PCAP files



[Categories: Network analyzers](#) | 
 [Unix network-related software](#) | 
 [Windows network-related software](#) | 
 [OS X network-related software](#) | 
 [Windows security software](#) | 
 [OS X security software](#) | 
 [Free software programmed in C](#) | 
 [Cross-platform free software](#) | 
 [Free network management software](#)

This page was last modified on 31 December 2013 at 11:38.

Text is available under the [Creative Commons Attribution-ShareAlike License](#); additional terms may apply. By using this site, you agree to the [Terms of Use](#) and [Privacy Policy](#).

Wikipedia® is a registered trademark of the [Wikimedia Foundation](#), a non-profit organization.

[Privacy policy](#) - [About Wikipedia](#) - [Disclaimers](#) - [Contact Wikipedia](#) - [Developers](#) - [Mobile view](#)

