pcap

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 libpcap known as **WinPcap**.

Monitoring software may use libpcap and/or WinPcap to capture packets travelling over a network and, in newer versions, to transmit packets on a network at the link layer, as well as to get a list of network interfaces for possible use with libpcap 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 libpcap or WinPcap itself. C++ programs may link directly to the C API or use an object-oriented wrapper

libpcap

Developer(s)	The Tcpdump team
Stable release	1.8.1 / October 25, 2016[1]
Repository	libpcap on GitHub
Written in	C (programming language)
Operating system	Linux, Solaris, FreeBSD, NetBSD, OpenBSD, macOS, additional *NIX systems
Type	Library for packet capture
License	BSD license[2]
Website	www.tcpdump.org

WinPcap

Developer(s)	Riverbed Technology
Last release	4.1.3 / March 8, 2013[3]
Operating system	Microsoft Windows
Type	Library for packet capture
License	Freeware
Website	www.winpcap.org

Contents

Features

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

libpcap and WinPcap also support saving captured packets to a file, and reading files containing saved packets; applications can be written, using libpcap 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 libpcap 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 libpcap and WinPcap is application/vnd.tcpdump.pcap The typical file extension is .pcap, although .cap and .dmp are also in common use.[4]

History

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

pcap libraries for Windows

While libpcap was originally developed for Unix-like operating systems, a successful port for Windows was made, called WinPcap. WinPcap has been unmaintained since 2013,[7] and several competing forks have been released with new features and support for newer versions of Windows.

WinPcap

WinPcap consists of:[8]

- x86 and x86-64 drivers for the Windows NT family (Windows NT 4.0, 2000, XP, Server 2003, Vista, 7, 8, and 10), which use NDIS 5.x to read packets directly from a network adapter;
- implementations of a lower-level library for the listed operating systems, to communicate with those drivers;
- a port of libpcap that uses the API offered by the low-level library implementations.

Programmers at the Politecnico di 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.[9]

Because WinPcap uses the older NDIS 5.x APIs, it does not work on some builds of Windows 10, which have deprecated or removed those APIs in favor of the newer NDIS 6.x APIs. It also forces some limitations such as being unable to capture 802.1Q VLAN tags in Ethernet headers.

Npcap

Npcap is the Nmap Project's packet sniffing library for Windows.[10] It is based on the Winpcap / Libpcap libraries, but with improved speed, portability, security, and efficiency. Npcap offers:

- **NDIS 6 Support**: Npcap makes use of new NDIS 6 Light-Weight Filter (LWF) API in Windows Vista and later (the legacy driver is used on XP). It's faster than the deprecated NDIS 5 API.
- **Latest libpcap API Support**: Npcap provides support for the latest libpcap API by accepting libpcap as a Git submodule. The latest libpcap 1.8.0 has integrated more fascinating features and functions than the deprecated libpcap 1.0.0 shipped by WinPcap. Moreover, since Linux already has a good support for latest libpcap API, using Npcap on Windows facilitates software to base on the same API on both Windows and Linux.
- **Extra Security**: Npcap can be restricted so that only Administrators can sniff packets. Non-Admin user will have to pass a User Account Control (UAC) dialog to utilize the driver. This is conceptually similar to UNIX, where root access is generally required to capture packets. The driver also has Windows ASLR and DEP security features enabled.
- **WinPcap compatibility**: If selected, Npcap will use the WinPcap-style DLL directories ("c:\Windows\System32") and service name ("npf"), allowing software built with WinPcap in mind to transparently use Npcap instead. If compatibility mode is not selected, Npcap is installed in a different location with a different service name so that both drivers can coexist on the same system.
- **Loopback Packet Capture**: Npcap is able to sniff loopback packets (transmissions between services on the same machine) by using the Windows Filtering Platform (WFP). After installation, Npcap will create an adapter named Npcap Loopback Adapter
- **Loopback Packet Injection**: Npcap is also able to send loopback packets using the Winsock Kernel (WSK) technique.

- **Raw 802.11 Packet Capture** Npcap is able to see 802.11 packets instead of fake Ethernet packets on ordinary wireless adapters.

Win10Pcap

Win10Pcap implementation is also based on the NDIS 6 driver model and works stably with Windows 10.[11]

Programs that use libpcap

- Apache Drill, an open source SQL engine for interactive analysis of large scale datasets.
- Bit-Twist, a libpcap-based Ethernet packet generator and editor for BSD, Linux, and Windows.
- Cain and Abel, a password recovery tool for Microsoft Windows
- EtherApe, a graphical tool for monitoring network traffic and bandwidth usage in real time.
- Firesheep, an extension for the Firefox web browser that captures packets and performs session hijacking
- iftop, a tool for displaying bandwidth usage (like top for network traffic)
- Kismet, for 802.11 wireless LANs
- L0phtCrack, a password auditing and recovery application.
- McAfee ePolicy Orchestrator, Rogue System Detection feature
- NetSim a network simulation software for network R & D
- ngrep, aka "network grep", isolate strings in packets, show packet data in human-friendly output.
- Nmap, a port-scanning and fingerprinting network utility
- Pirni, a network security tool for jailbroken iOS devices.
- Scapy, a packet manipulation tool for computer networks, written in Python by Philippe Biondi.
- Snort, a network-intrusion-detection system.
- Suricata, a network intrusion prevention and analysis platform.
- Symantec Data Loss Prevention, Used to monitor and identify sensitive data, track its use, and location. Data loss policies allow sensitive data to be blocked from leaving the network or copied to another device.
- tcpdump, a tool for capturing and dumping packets for further analysis, and WinDump, the Windows port of tcpdump
- the Bro IDS and network monitoring platform.
- URL Snooper, locate the URLs of audio and video files in order to allow recording them.
- WhatPulse, a statistical (input, network, uptime) measuring application.
- Wireshark (formerly Ethereal), a graphical packet-capture and protocol-analysis tool.
- Tranalyzer, a free software for flow and packet based traffic analysis and network troubleshooting
- XLink Kai Software that allows various LAN console games to be played online
- Xplico, a network forensics analysis tool (NFAT).

Wrapper libraries for libpcap

- C++: Libtins, Libcrafter, PcapPlusPlus
- Perl: Net::Pcap
- Python: python-libpcap, Pcapy, WinPcapy
- Ruby: PacketFu
- Rust: pcap
- Tcl: tclpcap, tcap, pktsrc
- Java: jpcap, jNetPcap, Jpcap, Pcap4j, Jxnet
- .NET: WinPcapNET, SharpPcap, Pcap.Net
- Haskell: pcap
- OCaml: mlpcap
- Chicken Scheme: pcap
- Common Lisp: PLOKAMI
- Racket: SPeaCAP
- Go: pcap by Andreas Krennmair, pcap fork of the previous by Miek Gieben, pcap developed as part of the gopacket package
- Erlang: epcap

- Node.js: node_pcap

Non-pcap code that reads pcap files

- Python: pycapfile
- Python: PyPCAPKit

References

1. "tcpdump and libpcap latest release" (https://www.tcpdump.org/#latest-release) tcpdump.org. Retrieved 2015-05-31.
2. "tcpdump and libpcap license" (https://www.tcpdump.org/license.html) tcpdump.org. Retrieved 2012-04-13.
3. "WinPcap Changelog" (http://www.winpcap.org/misc/changelog.htm).
4. "IANA record of application for MIME type application/vnd.tcpdump.pcap" (http://www.iana.org/assignments/media-types/application/vnd.tcpdump.pcap)
5. McCanne, Steve. "libpcap: An Architecture and Optimization Methodology for Packet Capture" (http://sharkfest.wireshark.org/sharkfest.11/presentations/McCanne-Sharkfest'11_Keynote_Address.pdf) (PDF). Retrieved December 27, 2013.
6. "TCPDUMP/LIBPCAP public repository" (https://www.tcpdump.org/). Retrieved December 27, 2013.
7. "WinPcap News" (https://www.winpcap.org/news.htm) Retrieved November 6, 2017.
8. "WinPcap internals" (http://www.winpcap.org/docs/docs_412/html/group__internals.html) Retrieved December 27, 2013.
9. "Riverbed Expands Further Into The Application-Aware Network Performance Management Market with the Acquisition of CACE Technologies" (http://www.riverbed.com/us/company/news/press_releases/2010/press_102110.php). Riverbed Technology. 2010-10-21. Retrieved 2010-10-21.
10. "Npcap" (https://nmap.org/npcap/)
11. "Win10Pcap: WinPcap for Windows 10" (http://www.win10pcap.org).

External links

- Official site for libpcap (and tcpdump)
- Official site for WinPcap (and WinDump)
- List of publicly available PCAP files