

# Pcap Protocol Handler

## Prerequisites

The Pcap transport handler is located in the *Pcap Wrapper Feature*.

## The protocol itself

The source of this section is [Wikipedia](#).

In the field of computer network administration, **pcap** (**p**acket **c**apture) 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.

## Used library

This Odysseus feature uses [pcapng-decoder](#).

## Pcap protocol handler

In Odysseus, the output of the decoder is transformed into a KeyValueCollection that contains all available information. See the example below.

```
#PARSER PQL
#RUNQUERY
pcap_input := ACCESS({
    transport = 'file',
    protocol = 'pcap',
    wrapper = 'GenericPull',
    source = 'Pcap',
    datahandler = 'keyvalueobject',
    options = [
        ['filename', 'somepcapfile.pcap']
    ]
}
)
```