Working with raw format files

Victor Moreno

November 1, 2016

1 Objective

This document describes the structure of the "raw" format files generated by the usage of the HPCAP2 driver as explained in [**?**].

2 File data structures

A raw file is composed by a set of consecutive packets. Each packet is preceded by its corresponding header which contains information related to the packet just as shown in Fig.**??**:

Seconds 4 bytes containing the seconds field of the packet timestamp.

Nanoseconds 4 bytes containing the nanoseconds field of the packet timestamp.

Caplen 2 bytes containing the amount of bytes of the packet included in the file.

Len 2 bytes containing the real size of the packet.

The end of the file is denoted by the appearance of a pseudo packet showing the amount of padding bytes added at the end of the file (in order to generate files of the same size). The padding pseudo-packet has a similar header than any other packet in the file with the difference that both the "Seconds" and the "Nanoseconds" fields are set to zeros. Once the padding pseudo-packet has been located, the padding size can be read from any of the "Len" or "Caplen" fields. Note that the padding length could be zero.

3 Example code

The next pages show an example code for a programs that reads a raw file and generates a new pcap file with the contents of the first one.

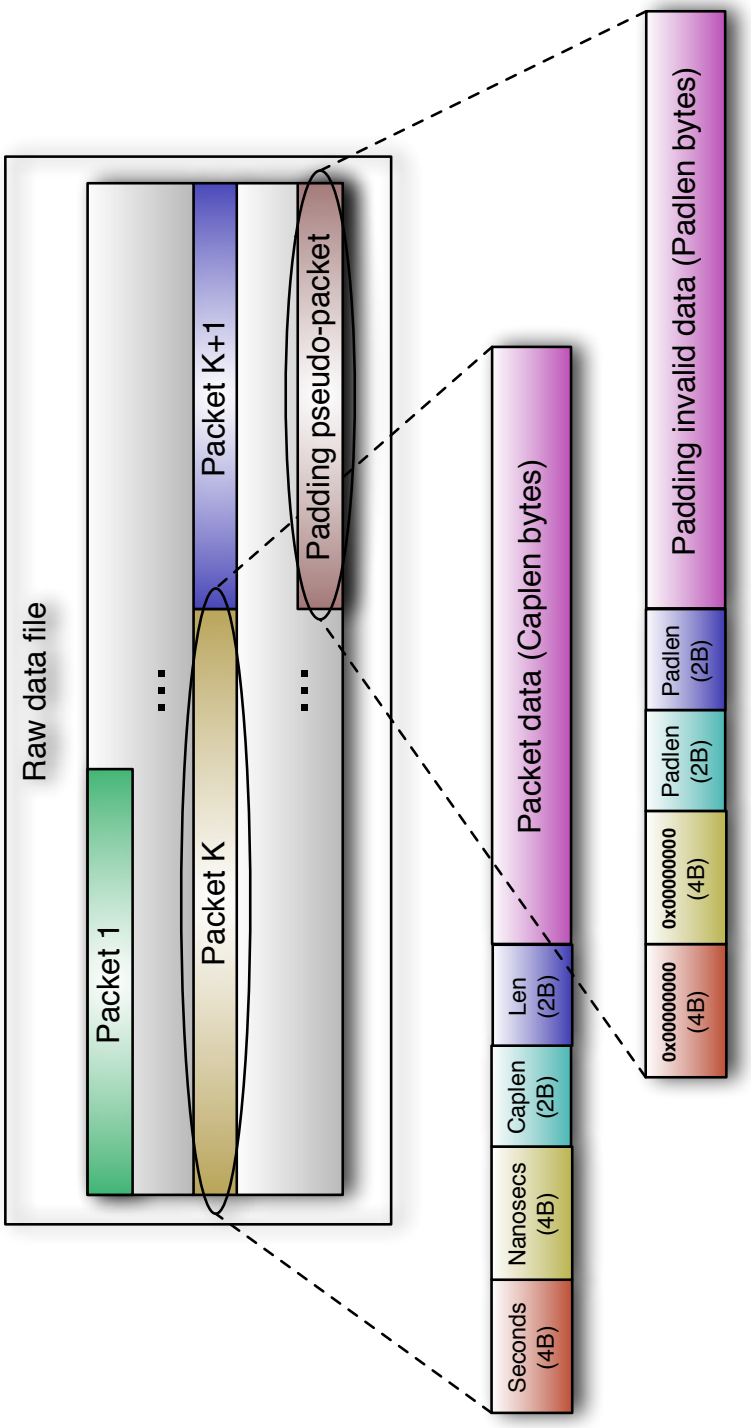

Figure 1: Raw file format