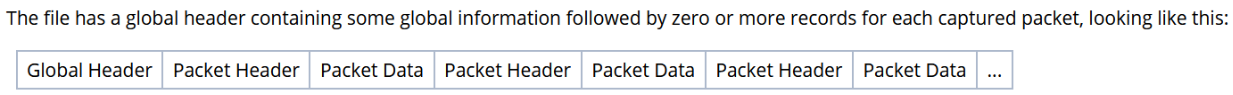
PCAP file explanation:

Filename – project1.pcap

For reference : https://wiki.wireshark.org/Development/LibpcapFileFormat



The file has a global header containing some global information followed by zero or more records for each captured packet, looking like this:

Global Header	Packet Header	Packet Data	Packet Header	Packet Data	Packet Header	Packet Data	...

Global header:

This header starts the libpcap file and is present at the beginning of the hexdata. The provided file we only have the below hexdata as Global header.

d4c3 b2a1 0200 0400 0000 0000 0000 0000

0000 0400 0100 0000

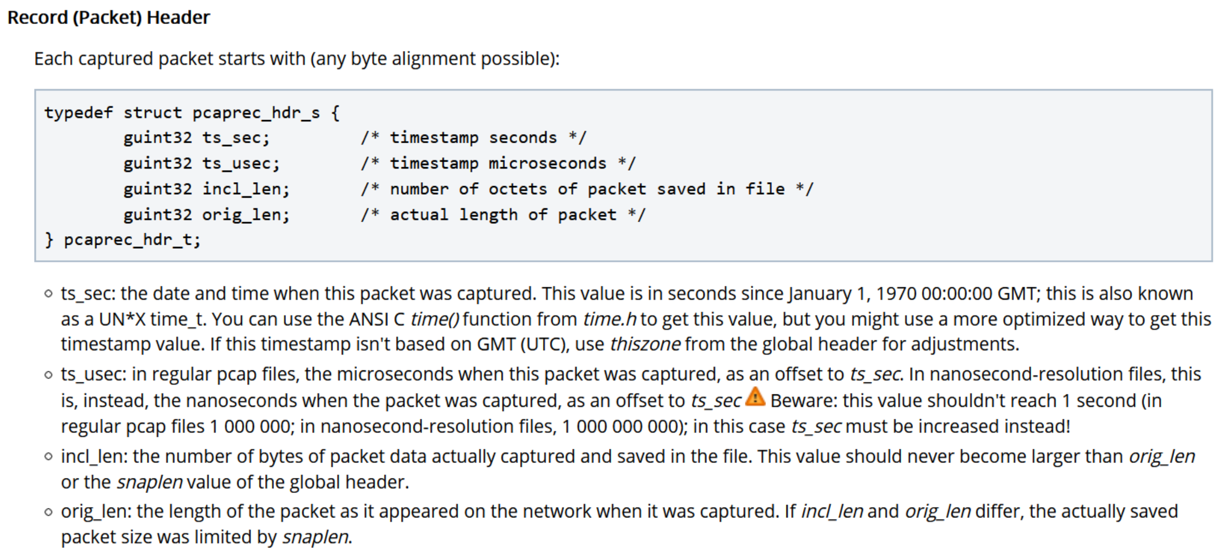
The Global header will not be seen in the wireshark hexdata. Open it in a text editor to look at these hexdata.

Packet Header:

This hexdata is present for all the packet and is usually 16 bytes long.

f907 3f5f cc75 0100 2e00 0000 2e00 0000.

The information will be present for all the packet.



Record (Packet) Header

Each captured packet starts with (any byte alignment possible):

```
typedef struct pcaprec_hdr_s {
        guint32 ts_sec;         /* timestamp seconds */
        guint32 ts_usec;        /* timestamp microseconds */
        guint32 incl_len;       /* number of octets of packet saved in file */
        guint32 orig_len;       /* actual length of packet */
} pcaprec_hdr_t;
```

- ts_sec: the date and time when this packet was captured. This value is in seconds since January 1, 1970 00:00:00 GMT; this is also known as a UN*X time_t. You can use the ANSI C *time()* function from *time.h* to get this value, but you might use a more optimized way to get this timestamp value. If this timestamp isn't based on GMT (UTC), use *thiszone* from the global header for adjustments.
- ts_usec: in regular pcap files, the microseconds when this packet was captured, as an offset to *ts_sec*. In nanosecond-resolution files, this is, instead, the nanoseconds when the packet was captured, as an offset to *ts_sec* ⚠ Beware: this value shouldn't reach 1 second (in regular pcap files 1 000 000; in nanosecond-resolution files, 1 000 000 000); in this case *ts_sec* must be increased instead!
- incl_len: the number of bytes of packet data actually captured and saved in the file. This value should never become larger than *orig_len* or the *snaplen* value of the global header.
- orig_len: the length of the packet as it appeared on the network when it was captured. If *incl_len* and *orig_len* differ, the actually saved packet size was limited by *snaplen*.

Packet data:

Any data following the Packet header is the contents of the packet.