> 学习pcap文件格式

简介

pcap是一种常用的数据包储存格式，里面的数据按照特定的格式储存和解析

文件格式

pcap文件格式由 **文件头--数据包头--数据包--数据包头2--数据包2** 这类格式组成，其中头文件只有一个，数据包头和数据包可以有很多个

Pcap header

文件头格式如下:

```
  typedef struct pcap_hdr_s {
          guint32 magic_number;   /* magic number */
          guint16 version_major;  /* major version number */
          guint16 version_minor;  /* minor version number */
          gint32  thiszone;       /* GMT to local correction */
          guint32 sigfigs;        /* accuracy of timestamps */
          guint32 snaplen;        /* max length of captured packets, in octets
*/
          guint32 network;        /* data link type */
  } pcap_hdr_t;
```

header field	size	explain
Magic	4B	用来识别文件和字节顺序,大端或小端
Major	2B	当前Pcap文件的主要版本号，一般为0x0200
Minor	2B	当前Pcap文件的次要版本号，一般为0x0400
ThisZone	4B	当地的标准事件，如果用的是GMT则全零，一般全零
SigFlags	4B	时间戳的精度，一般为全零
SnapLen	4B	所抓获的数据包的最大长度
LinkType	4B	数据链路类型

Packet header

数据包头格式如下:

```
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;
```

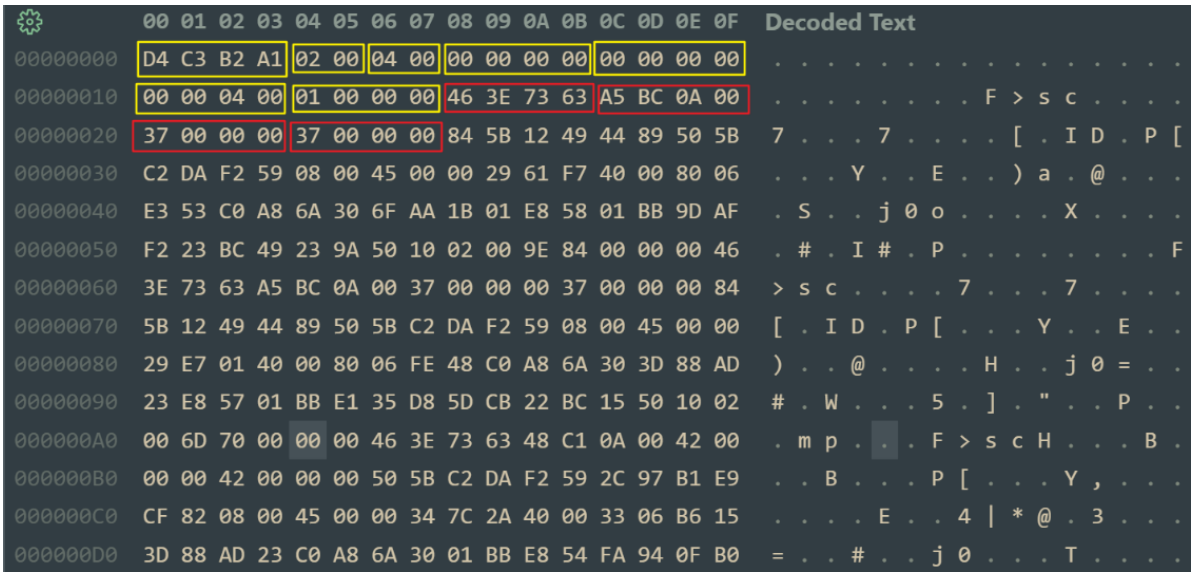
header field	size	explain
Timestamp	4B	时间戳高位，精确到seconds
Timestamp	4B	时间戳低位，能够精确到microseconds
Caplen	4B	即抓取到的数据帧长度，由此可以得到下一个数据帧的位置。
Len	4B	实际的数据帧长度,一般不大于Caplen,多数情况一样

Packet data

数据包数据，其长度为上面的Caplen

实例

如图：



黄色框框是文件头，红色框框是数据包头,具体值如下：

文件头：

header field	value
Magic	0xD4C3B2A1 表示小端，后面的数据要反过来读。0xA1B2C3D4为大端模式
Major	0x0002
Minor	0x0004
ThisZone	0x0000
SigFlags	0x0000
SnapLen	0x00040000
LinkType	0x00000001

数据包头：

header field	value
Timestamp	0x63733E46
Timestamp	0x000ABCA5
Caplen	0x00000037
Len	0x00000037

数据包大小则为0x00000037 = 55Bytes