IP分片包处理

时间：2015/12/2

背景：在开发ipdecap\_extend解析GRE数据包程序\_IP分片包时发现出现两片数据包关联不上；

数据包格式如图1：



图 1 IP分片包数据包格式

描述：当将第一片包中payload中PPP\_data部分进行去头，去尾，反转义7d；一系列操作之后，payload部分数据字长将会改变成任意合法字长（非8Byte倍数）；但是在IP协议规范中提到分片包中ip.ip\_off字长必须是8的倍数，所以这里就出现了下一片分片包的offset该怎么去设置；东哥之前提议说设置ip里面的opt字长匹配data为8的整数倍时，但是这个shiite不可能的，其一:ip.opt必须是4的倍数，不是一个任意可以设置的值； 其二：不管opt的字长是多少，其都是ip字段字长，并不算到data字段中来；所以设置ip.opt是不可用的；这个问题还不知道怎么解决；

之后尝试将第一片数据包中进行填充0字节，使其data为8的倍数，如图2；同时设置下一片数据包的offset为1480，如图3；

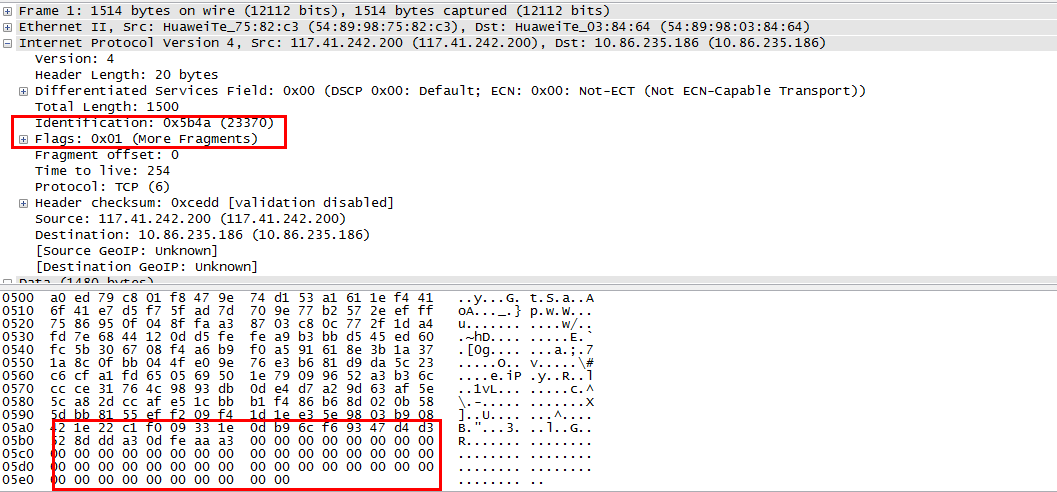


图 2 IP分片包\_第一片data8字节对齐

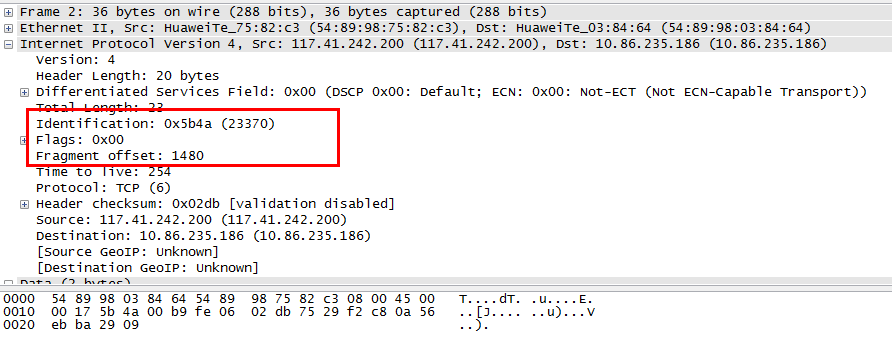


图 3 IP分片包\_第二片\_设置offset

显示：但是使用wireshark打开第二片数据包时，并没有显示关联；估计是data被填充0，没有办法被IP上层协议tcp所解析；

结果：需要进一步讨论解决；