例题

**6. Protocol analysis （10 points）**

The data flow was captured (捕获) and listed blow in hexadecimal（十六进制）, context of the data includes Ethernet frame header, IP header and transport layer segment, according to the information answer the following questions.

0x0000 00 04 61 8f b1 f8 00 1a a9 7d e4 1e 08 00 45 00

0x0010 02 31 63 23 40 00 35 06 a4 25 da 12 67 26 ca c1

0x0020 30 84 1e 1d 04 23 c7 6d dd e6 94 c8 fb 83 50 18

0x0030 06 c0 17 a9 00 00 ……

1. What is the source MAC address ? 00 04 61 8f b1 f8 00 1a a9 7d e4 1e 08 00 45 00

答：00 1a a9 7d e4 1e

2. What is the length of IP packet?

45 00

0x0010 02 31 63 23 40 00 35 06 a4 25 da 12 67 26 ca c1

0x0020 30 84 1e 1d 04 23 c7 6d dd e6 94 c8 fb 83 50 18

0x0030 06 c0 17 a9 00 00 ……

答：0x0231=561

1. What is the source address and destination address in the network layer?

A: Source address: 0xda 12 67 26 = 218.18.103.38

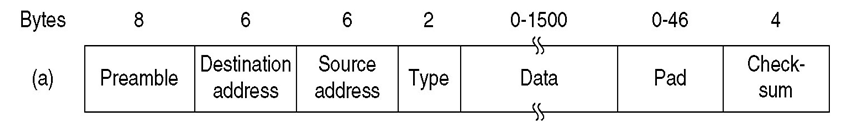
Destination address: 0xca c1 30 84 = 202.193.48.132

1. Is this a TCP or UDP protocol in the transport layer?

A: IP包中Protocol字段的值为：06 ，所以为TCP

1. What is the source port?

A: Source port: 0x1e 1d= 7709



（注：以上捕获的数据中无preamble）

