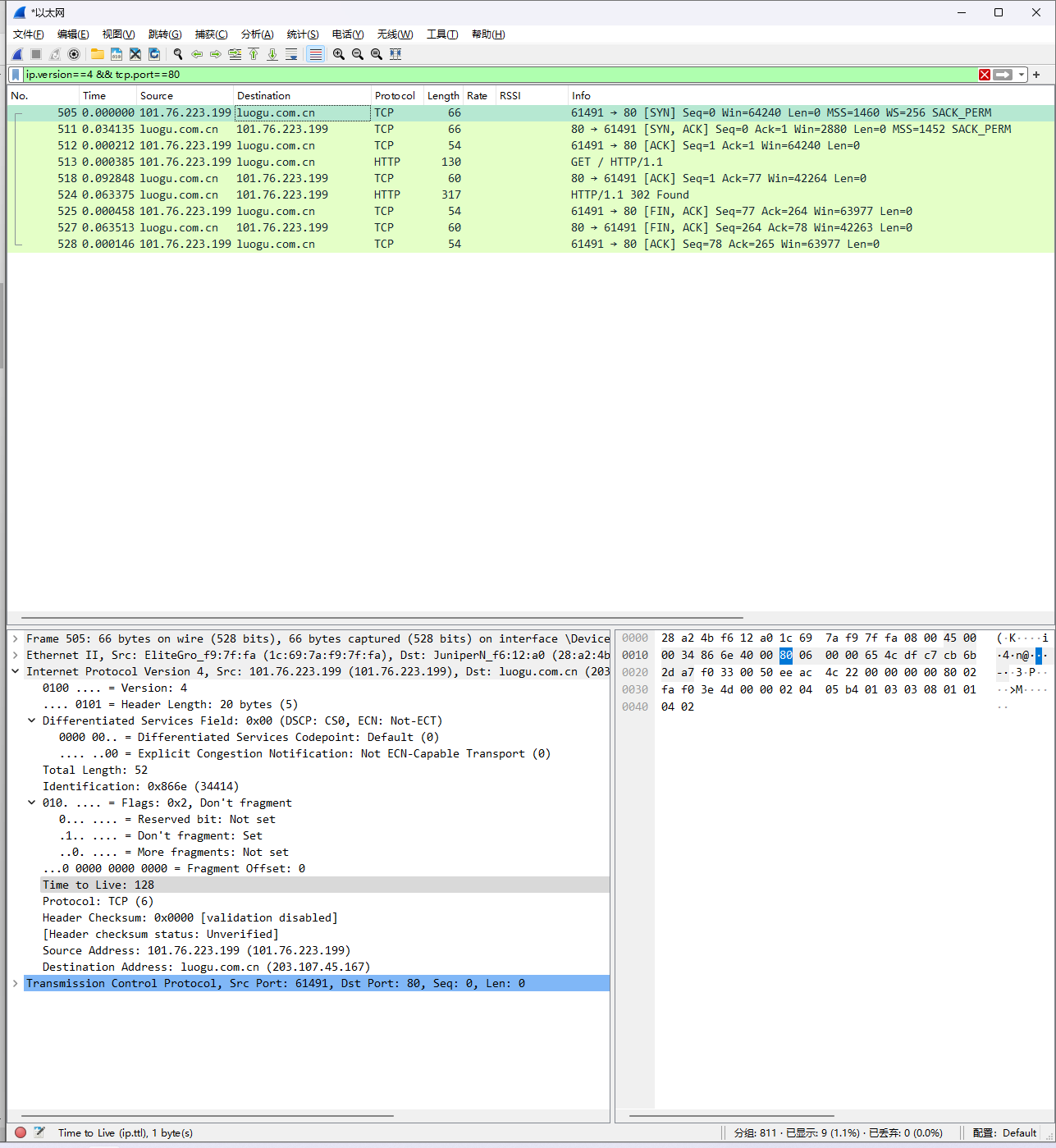
Wireshark Lab 5-1

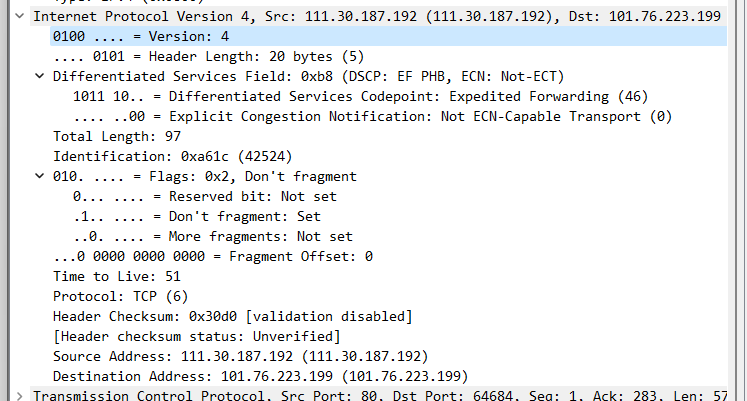
202022300317 杨业昶

## Step 1: Fetch a Trace





## Step 2: Inspect the Trace



## Step 3: IP Packet Structure

What are the IP addresses of your computer and the remote server?

>>> 192.168.250.250; 203.107.45.167

Does the Total Length field include the IP header plus IP payload, or just the IP payload?

>>> IP header plus IP payload

How does the value of the Identification field change or stay the same for different packets? For instance, does it hold the same value for all packets in a TCP connection or does it differ for each packet? Is it the same in both directions? Can you see any pattern if the value does change?

>>> In the same group of fragments are the same; No; both directions increasing.

What is the initial value of the TTL field for packets sent from your computer? Is it the maximum possible value, or some lower value?

>>> Time to Live: 128; some lower value

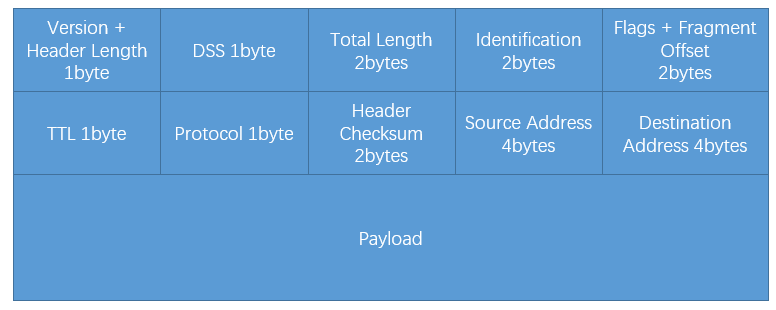
How can you tell from looking at a packet that it has not been fragmented?

>>> .1.. .... = Don't fragment: Set

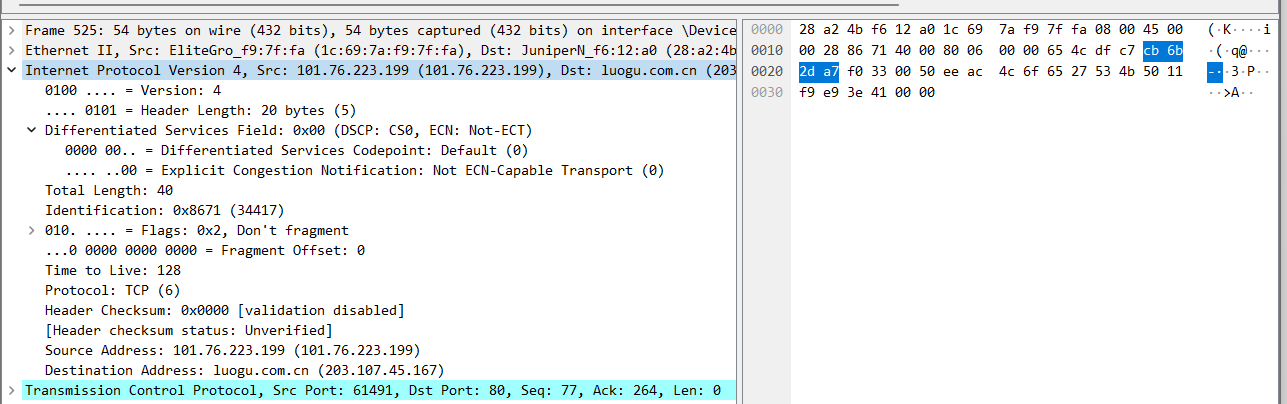
What is the length of the IP Header and how is this encoded in the header length field?

>>>.... 0101 = Header Length: 20 bytes (5); 20/4 = 5

## Step 4: Internet Paths



## Step 5: IP Header Checksum



Checksum = 0x751a; Corresponds with packet