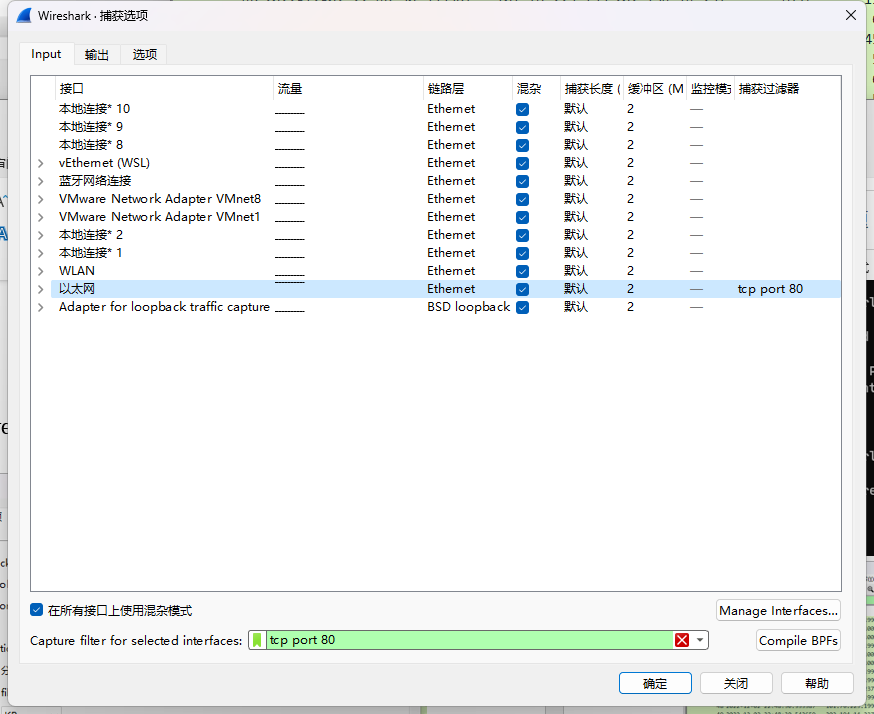
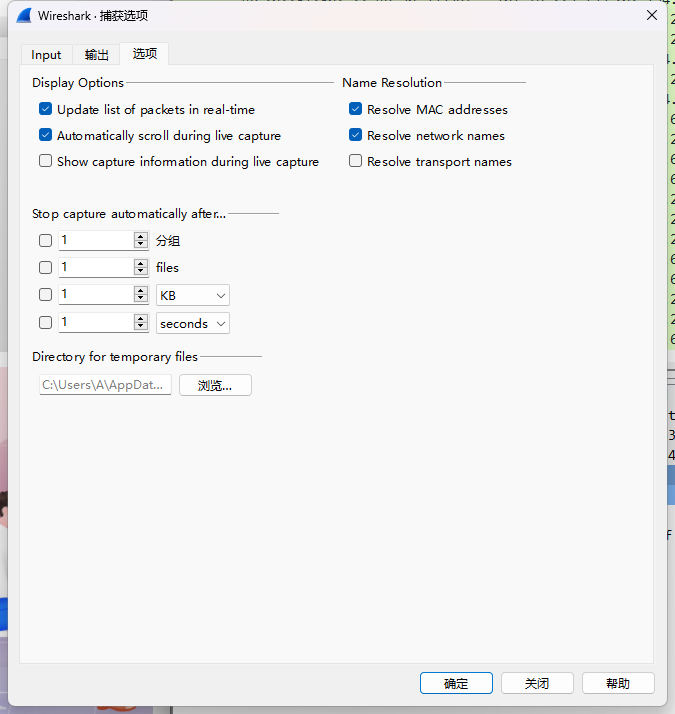
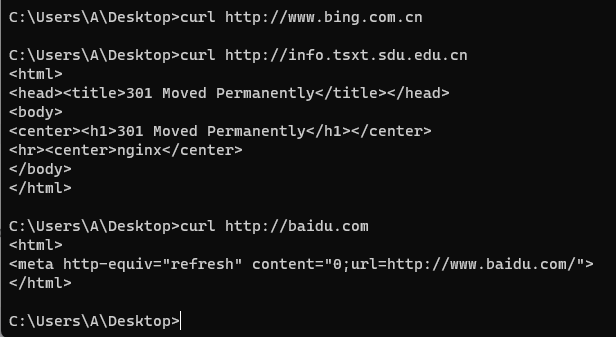
Wireshark Lab 1-2

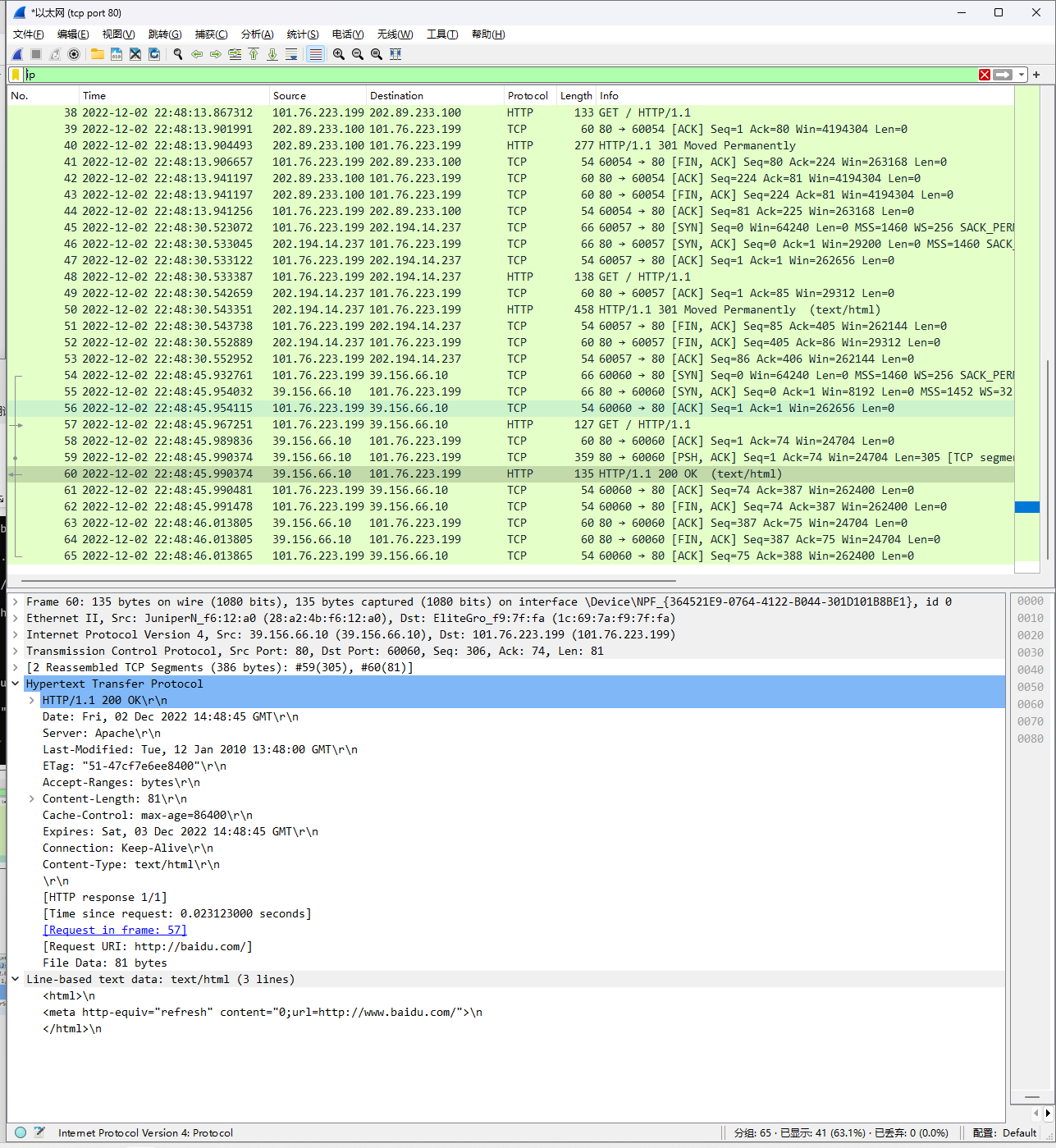
202022300317 杨业昶

## Step 1: Capture a Trace.

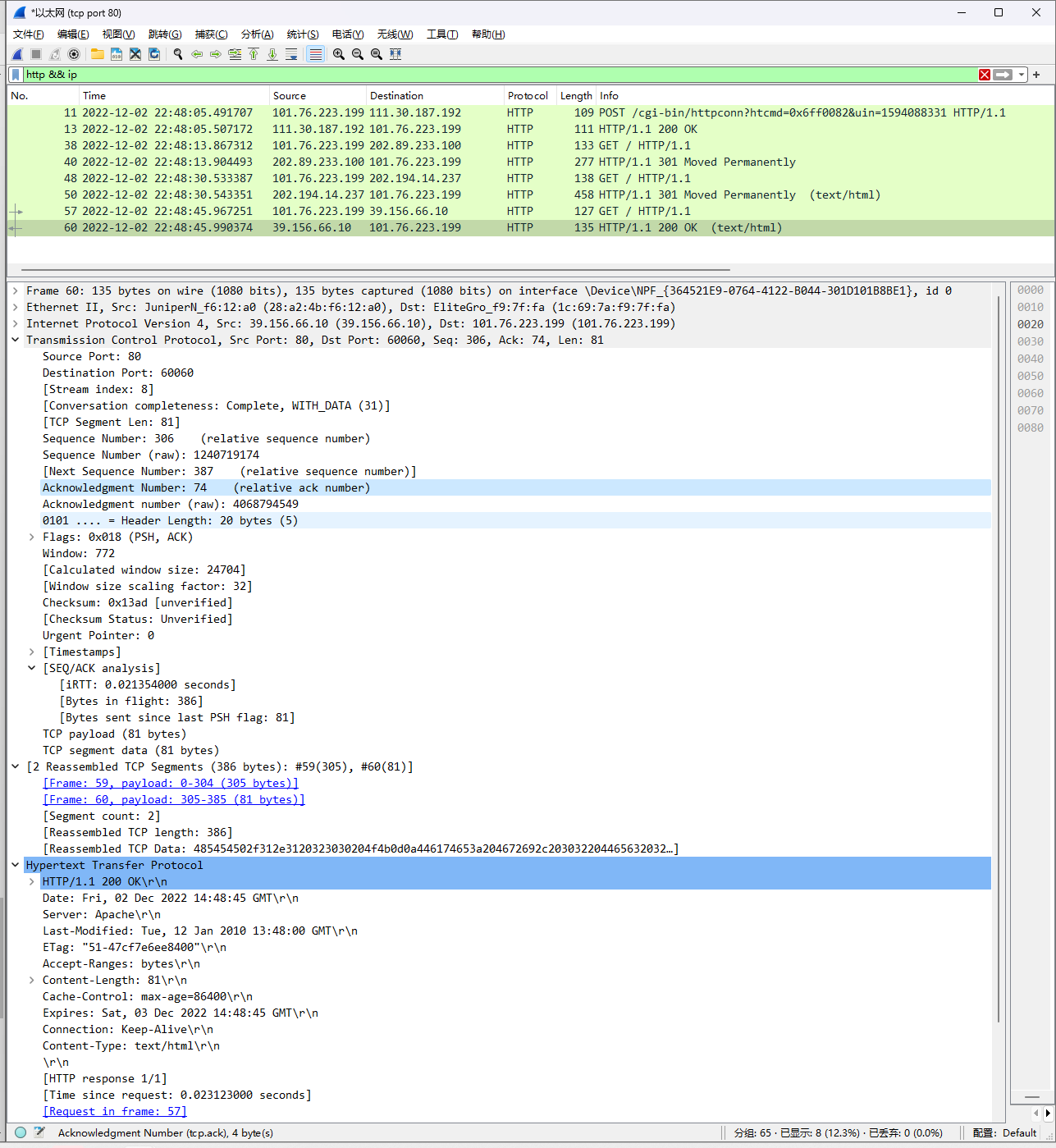






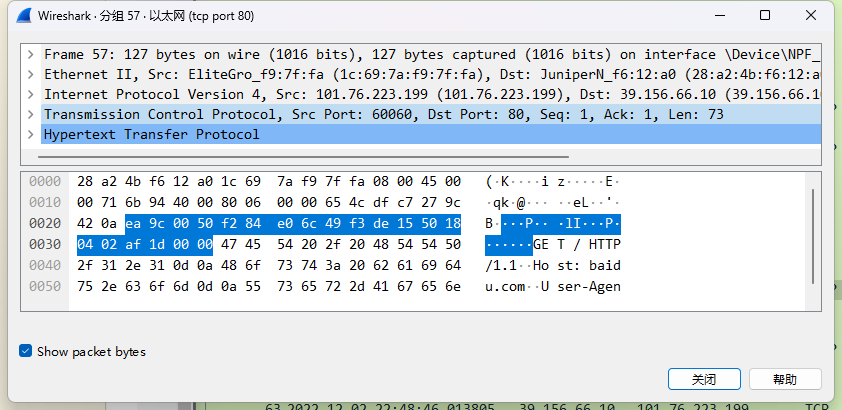


## Step 2: Inspect the Trace



## Step 3: Packet Structure

HTTP GET packet

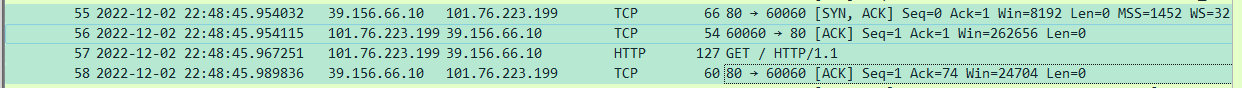




Structure as below:



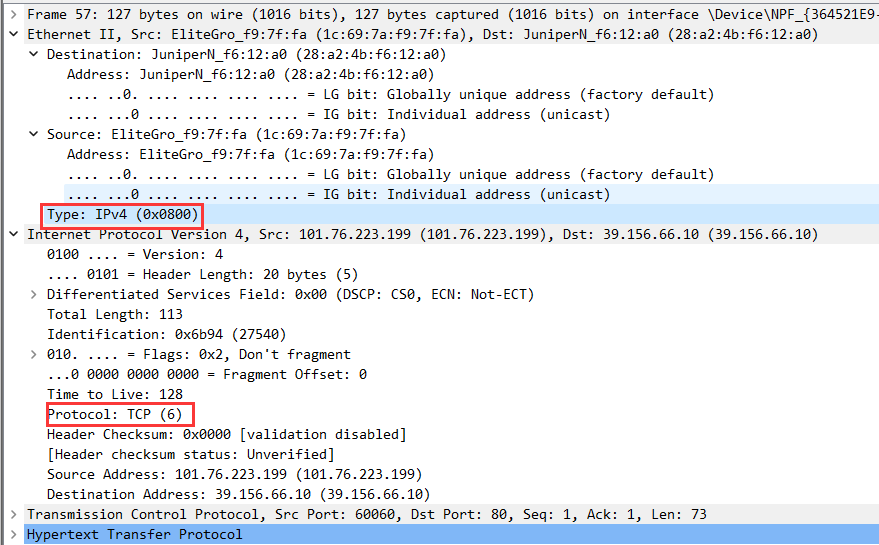
## Step 4: Protocol Overhead



Total length = 66+54+127+60 = 307bytes

http/total = 73/307 ~= 23.8%

## Step 5: Demultiplexing Keys



Which Ethernet header field is the demultiplexing key that tells it the next higher layer is IP?

>>> Ethernet type field

What value is used in this field to indicate “IP”?

>>> 0x80

Which IP header field is the demultiplexing key that tells it the next higher layer is TCP?

>>> IPv4 Protocol field

What value is used in this field to indicate “TCP”?

>>> 0x06