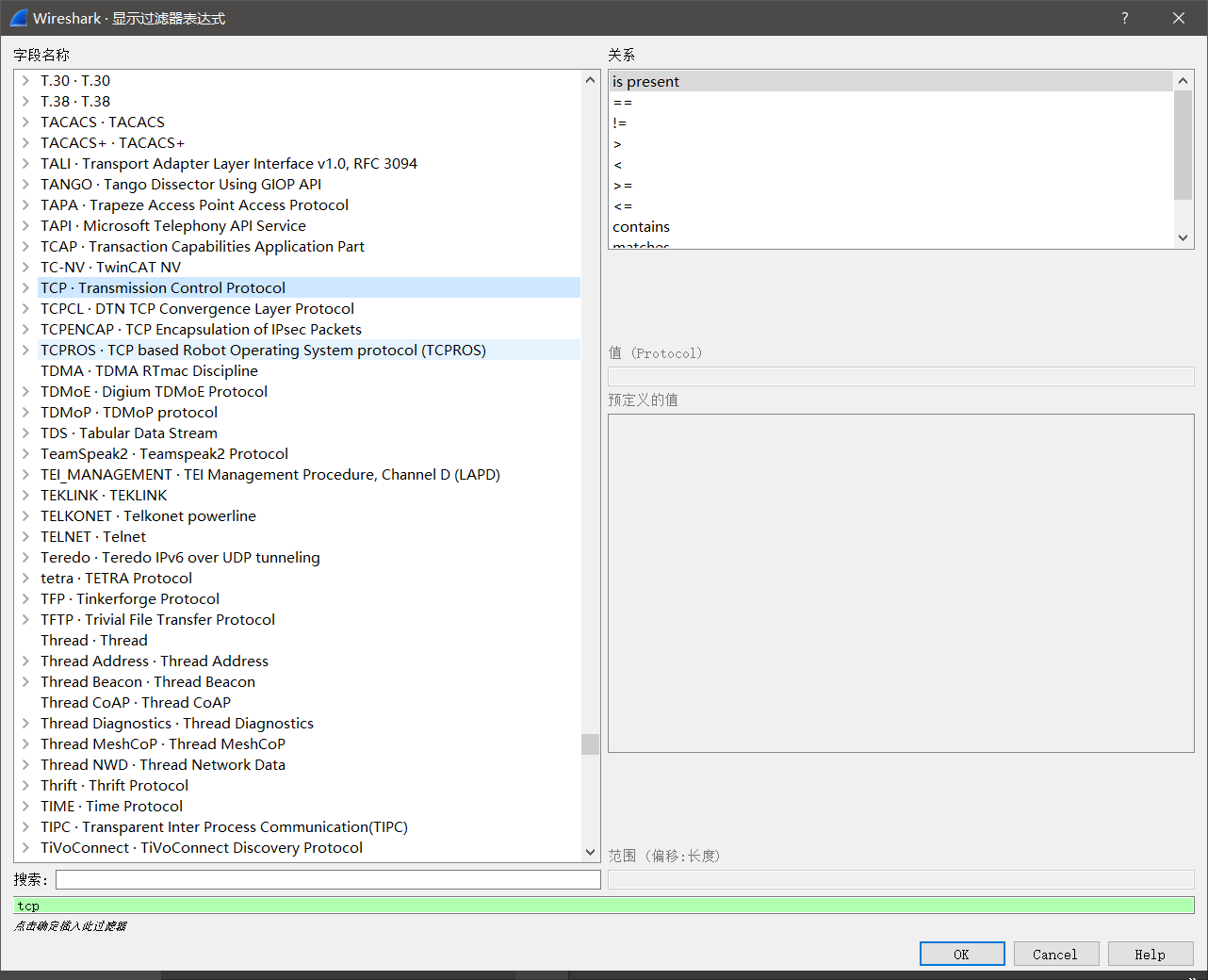
Lab02-Wireshark Filters

Yeah, now we have opened 3 tabs In NEU official website. Let’s go!

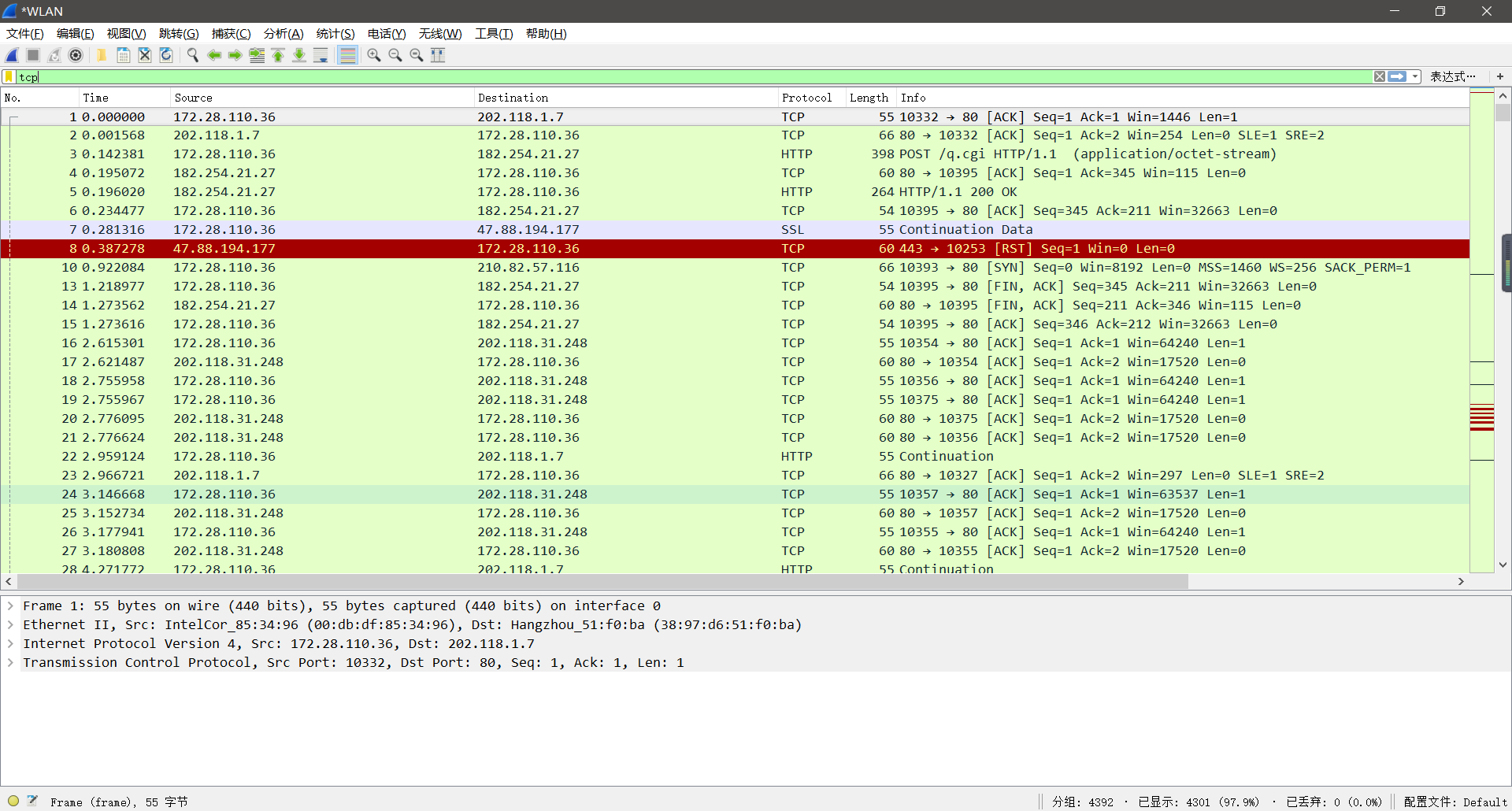
Part 1 *Create filters that display only those packets that:*

1. *use the TCP protocol*

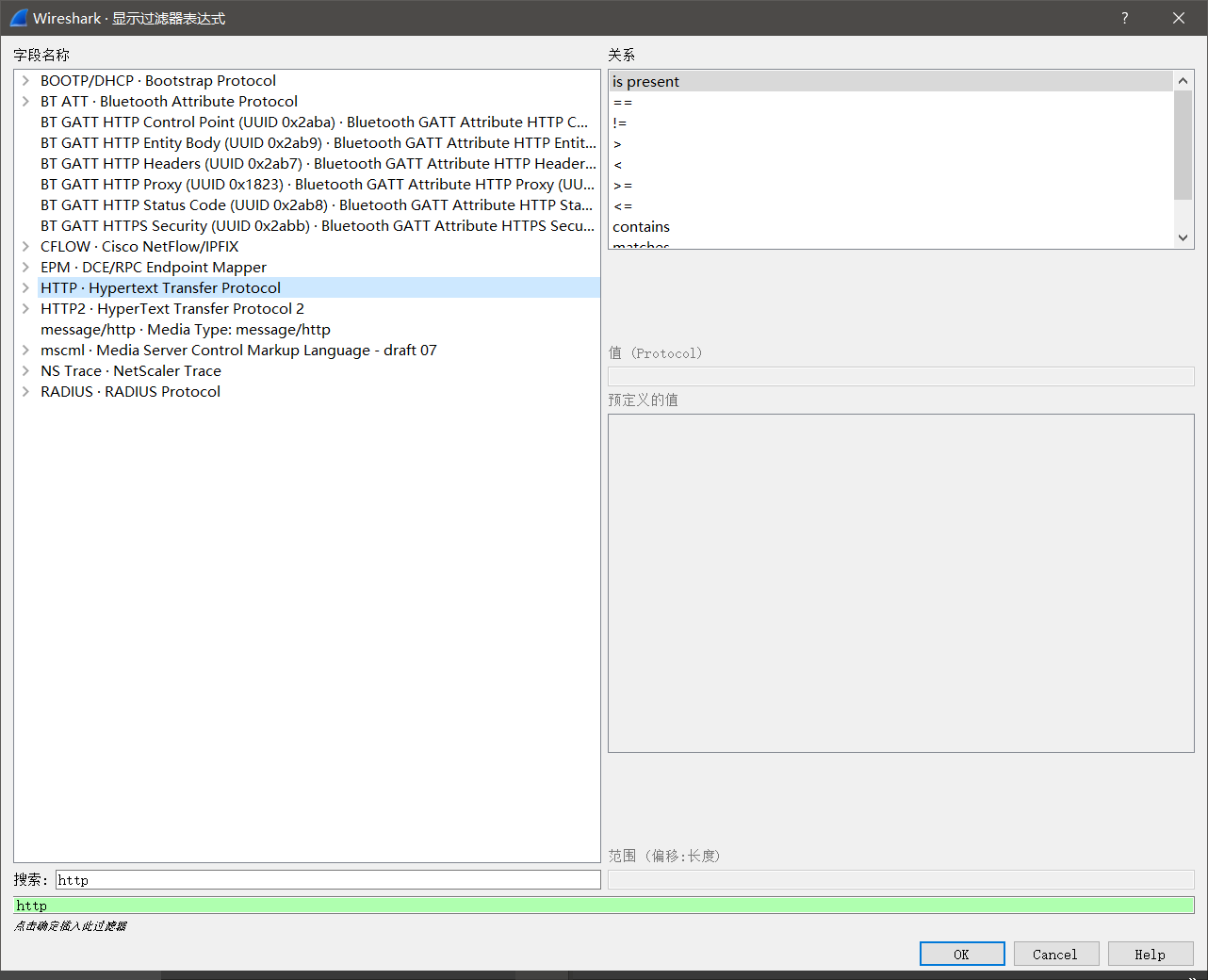
(1) select the filter



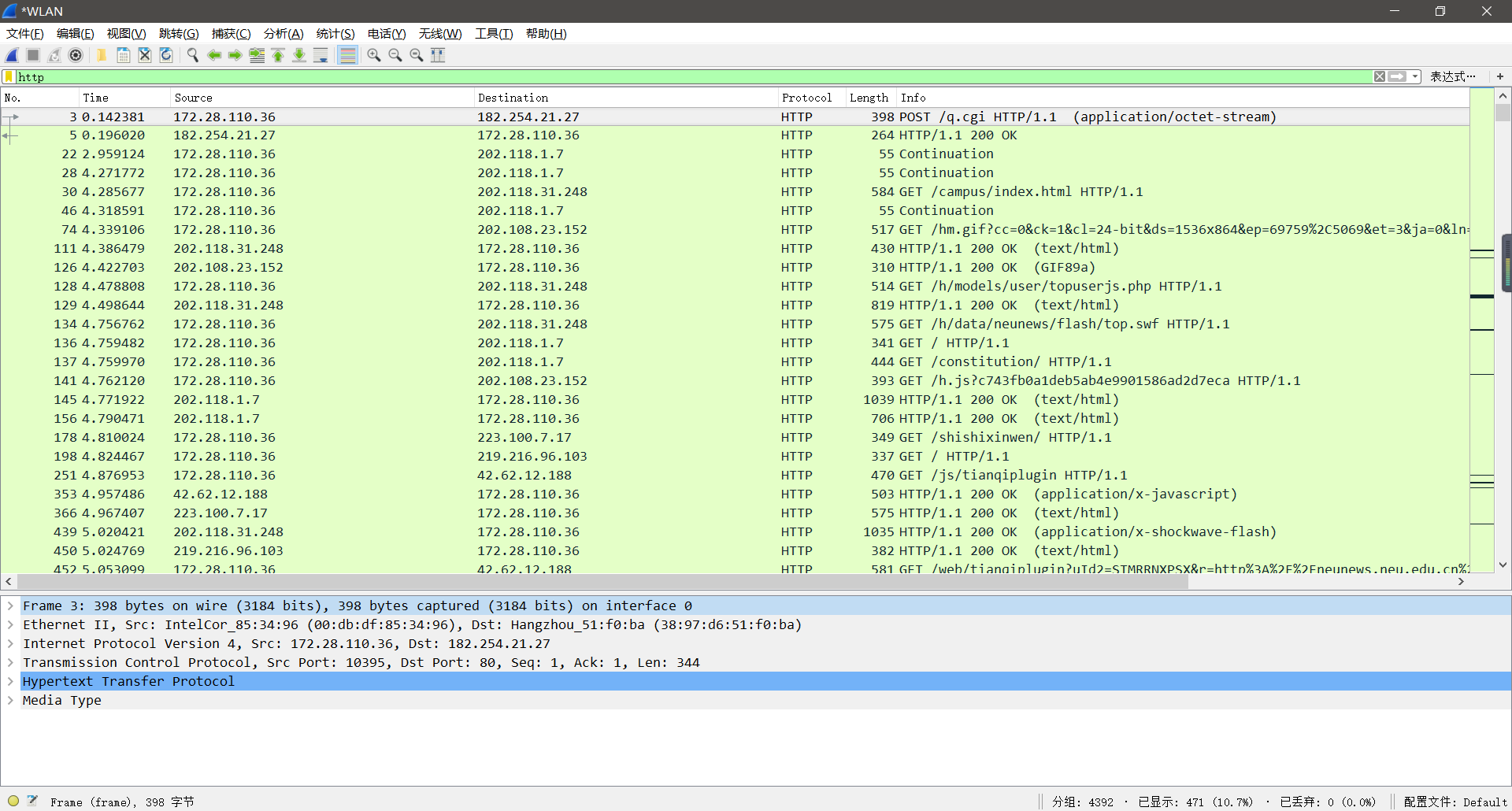
(2) display the filter



2. *use the HTTP protocol*

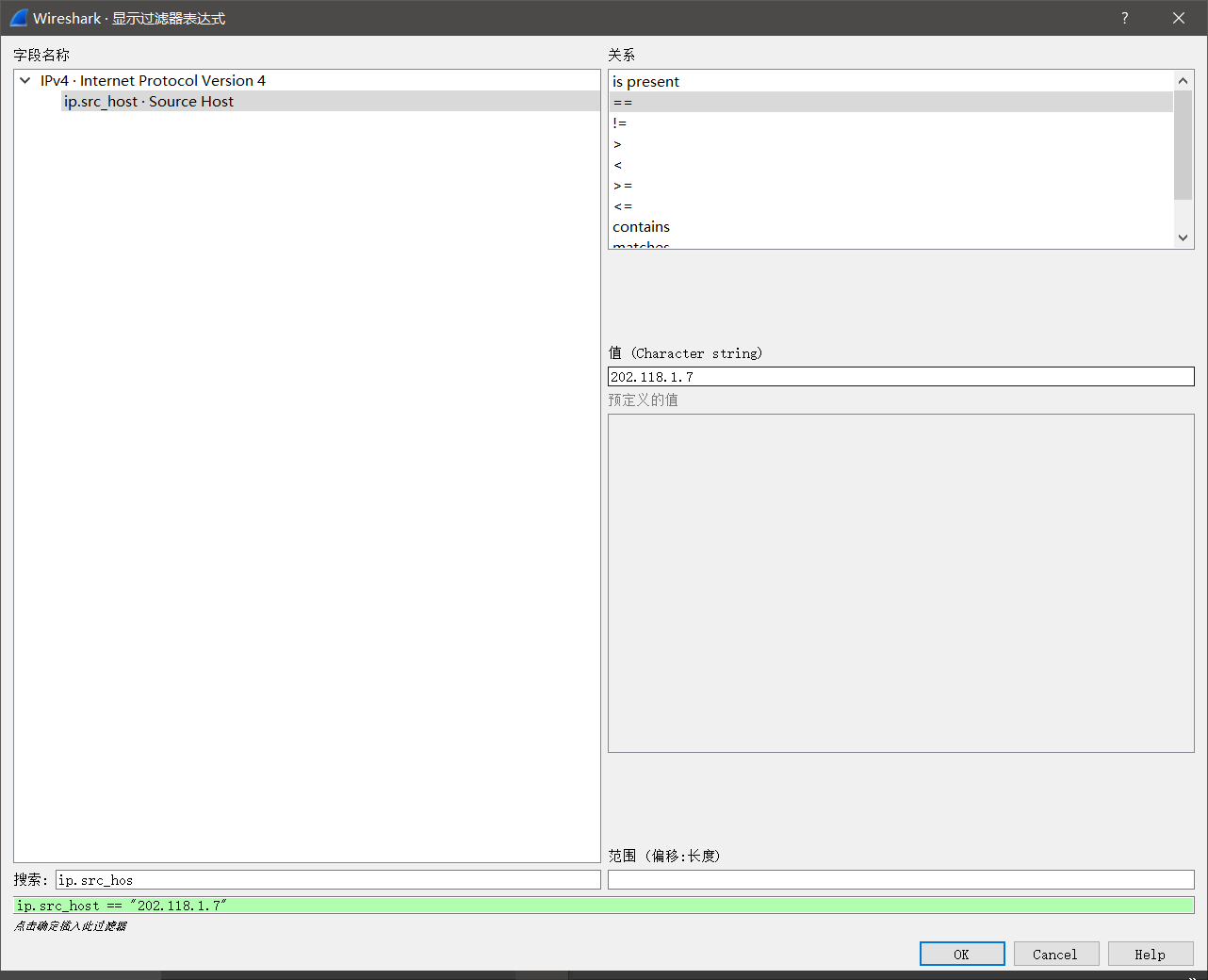
(1) select the filter 

(2) display the filter

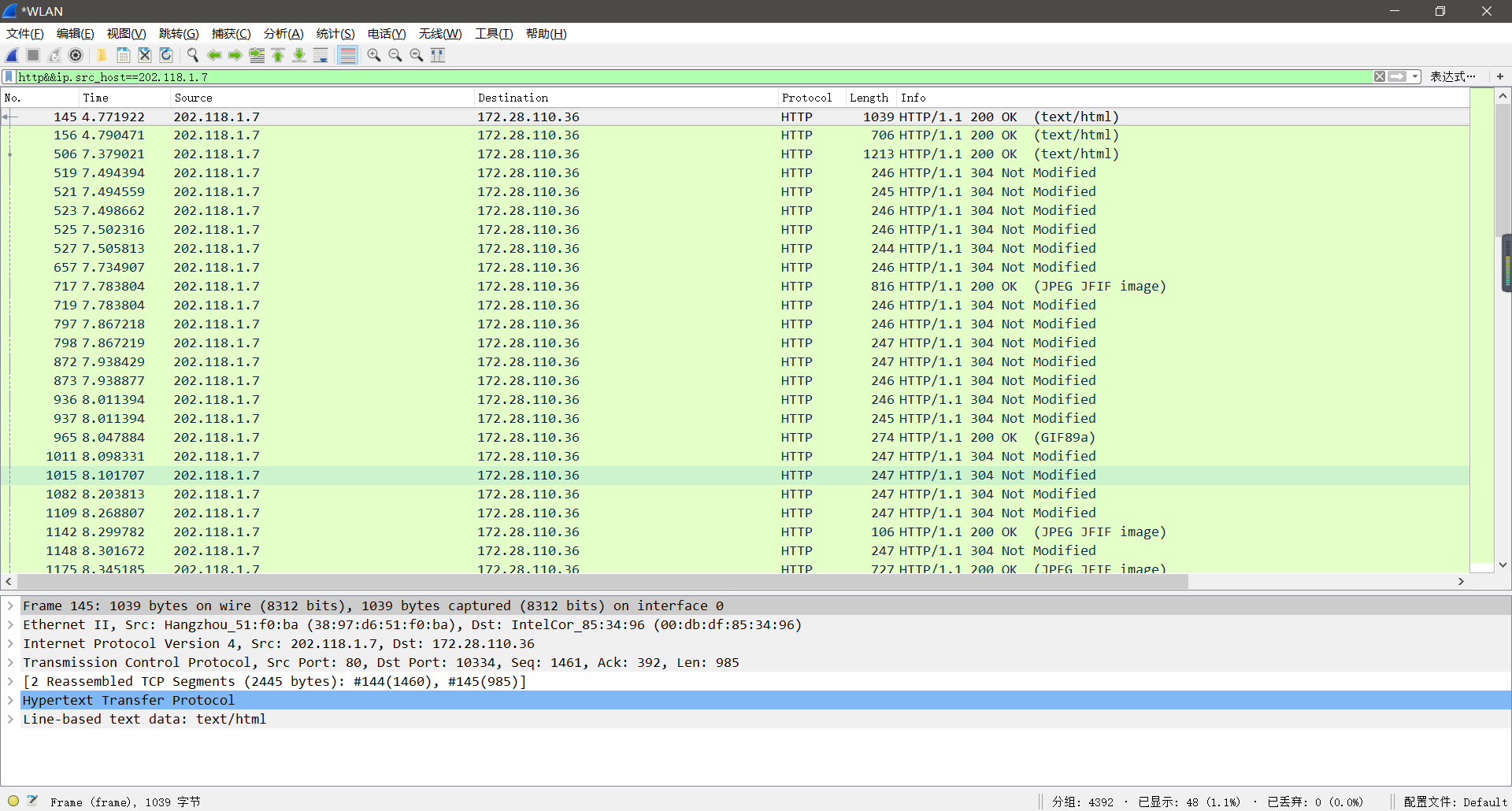


3 *request HTTP information from* [*http://www.neu.edu.cn*](http://www.neu.edu.cn)

(1) select the filter

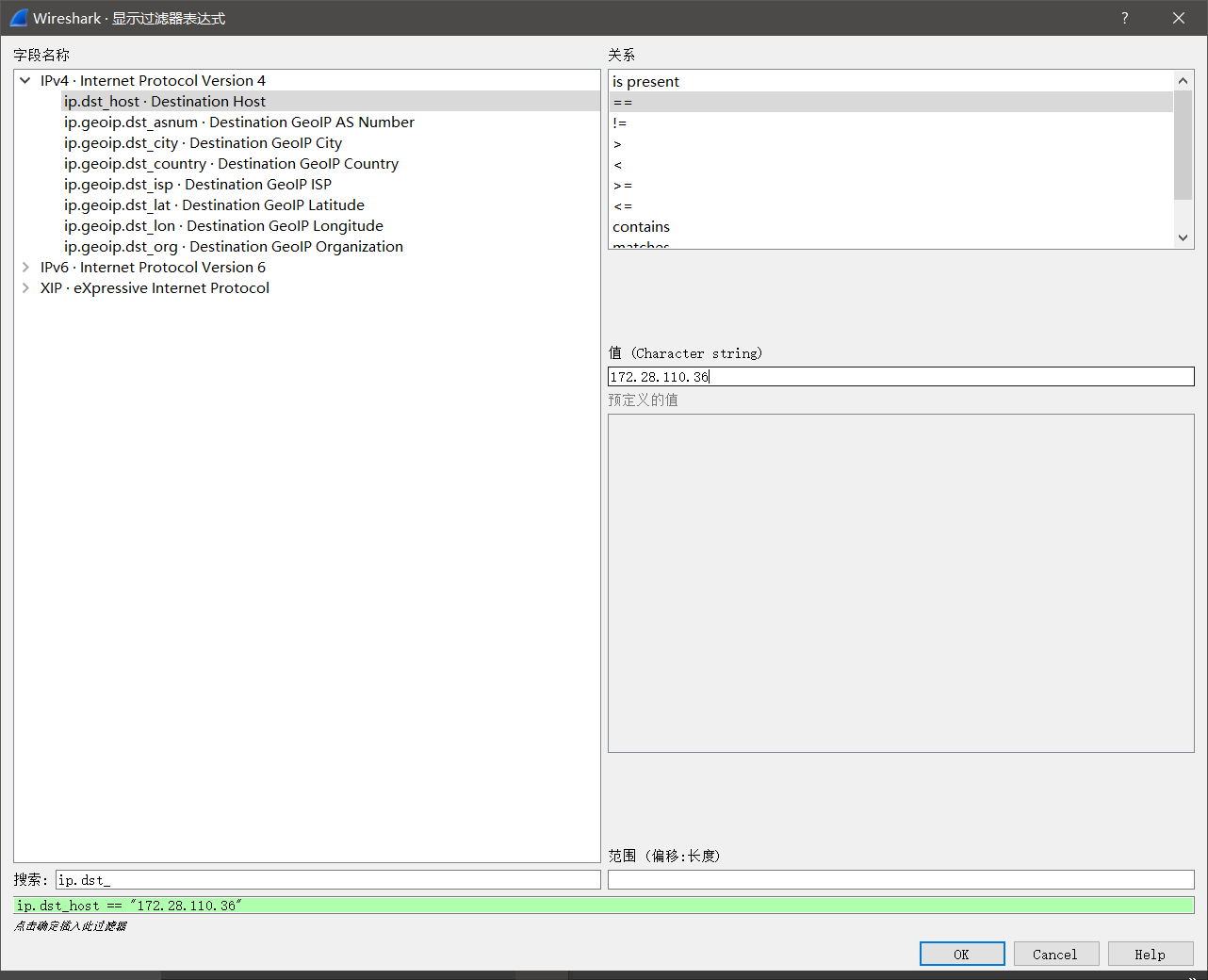


(2) display the filter

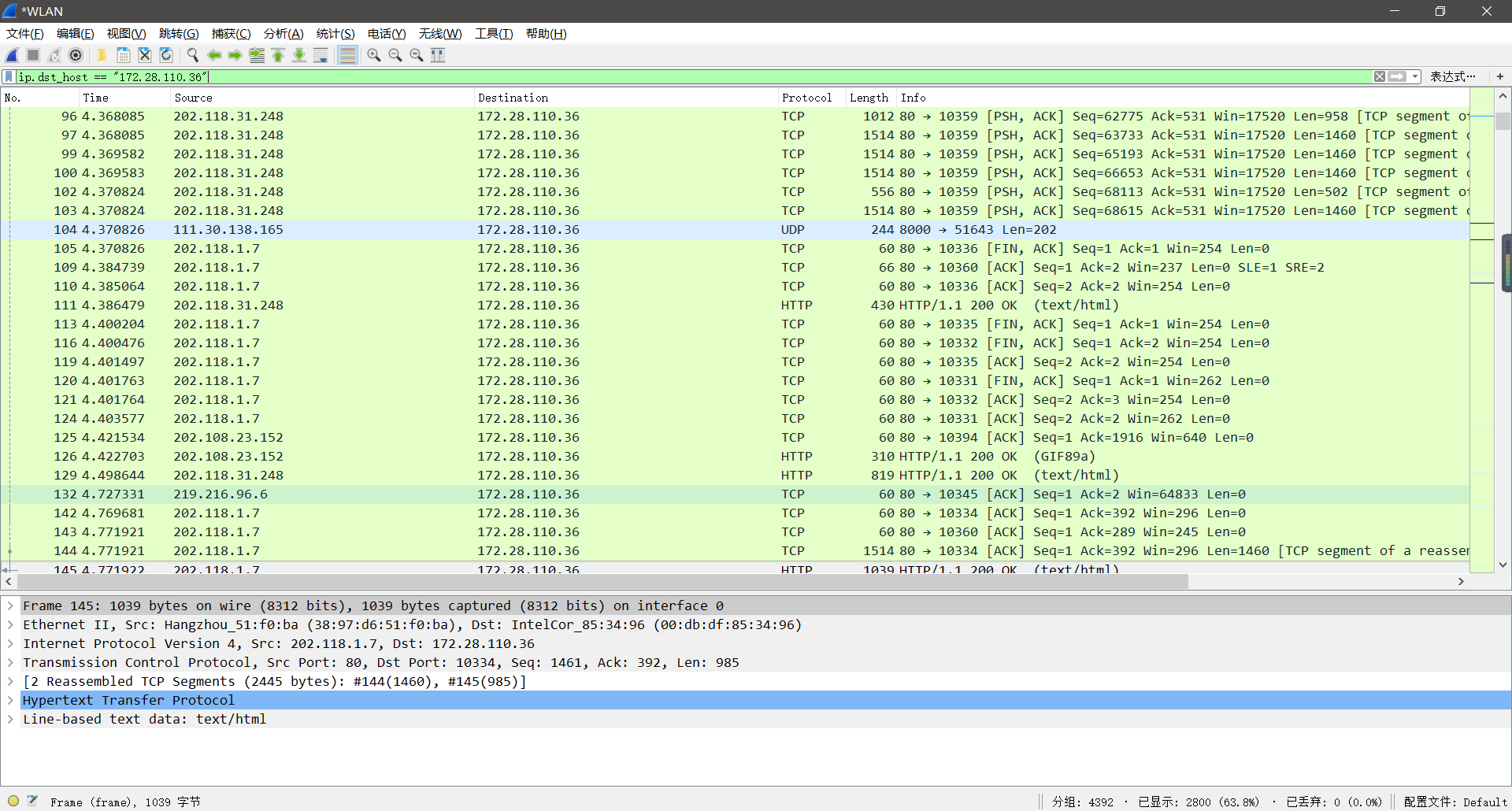


4. *are sent to your computer*

(1) select the filter

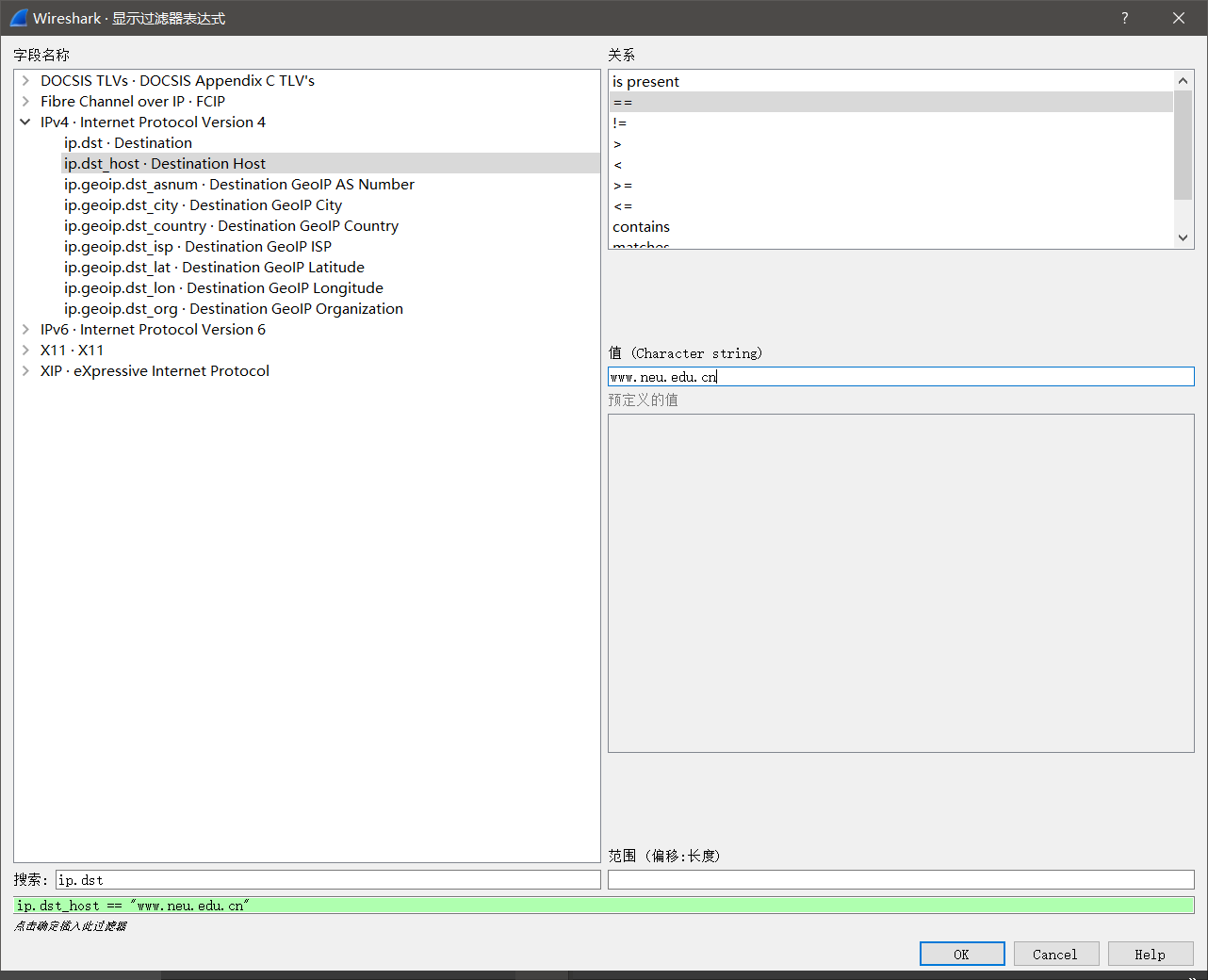


(2) display the filter

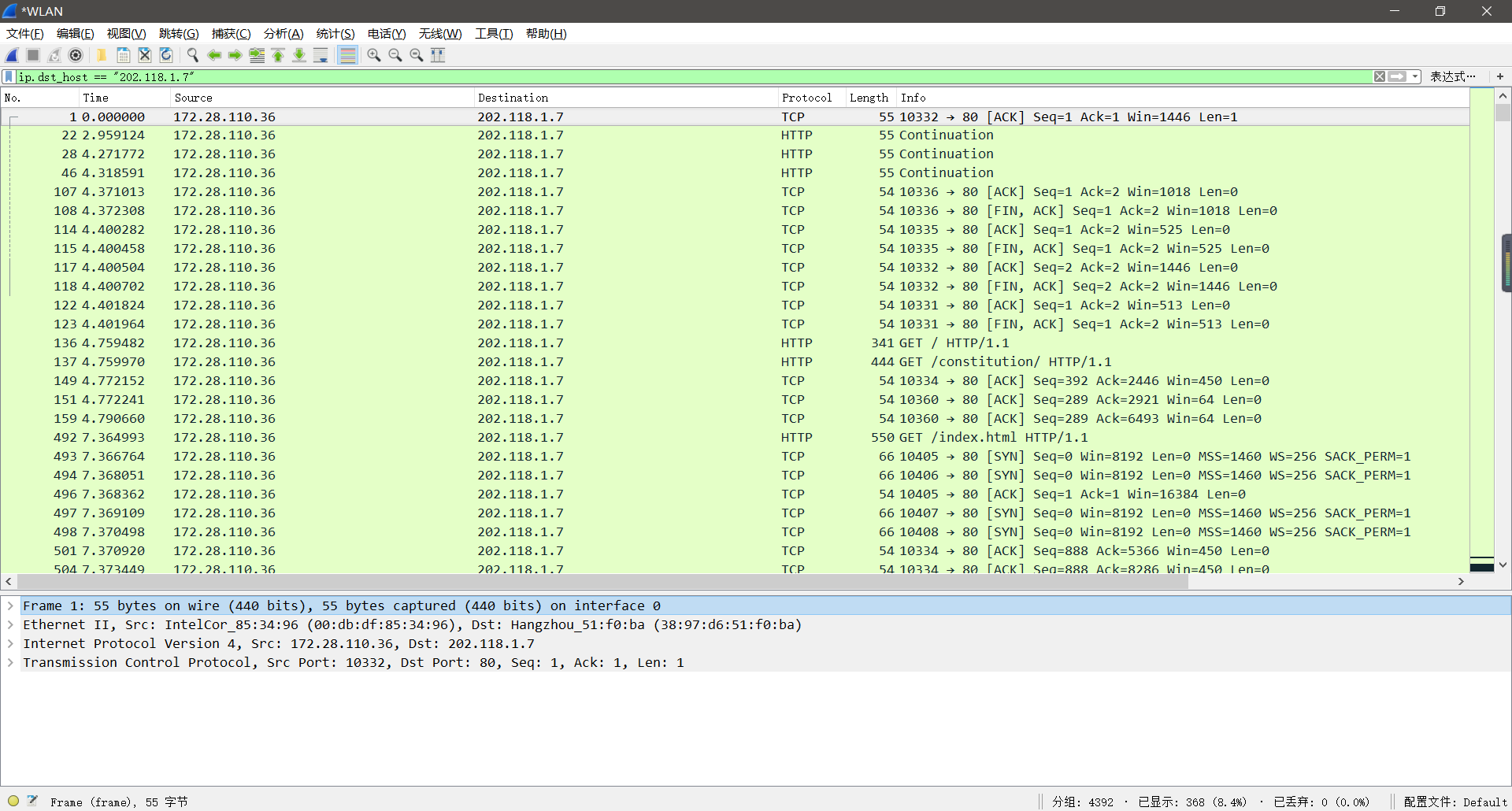


5. *are sent to the server at* [*http://www.neu.edu.cn*](http://www.neu.edu.cn)

(1) select the filter

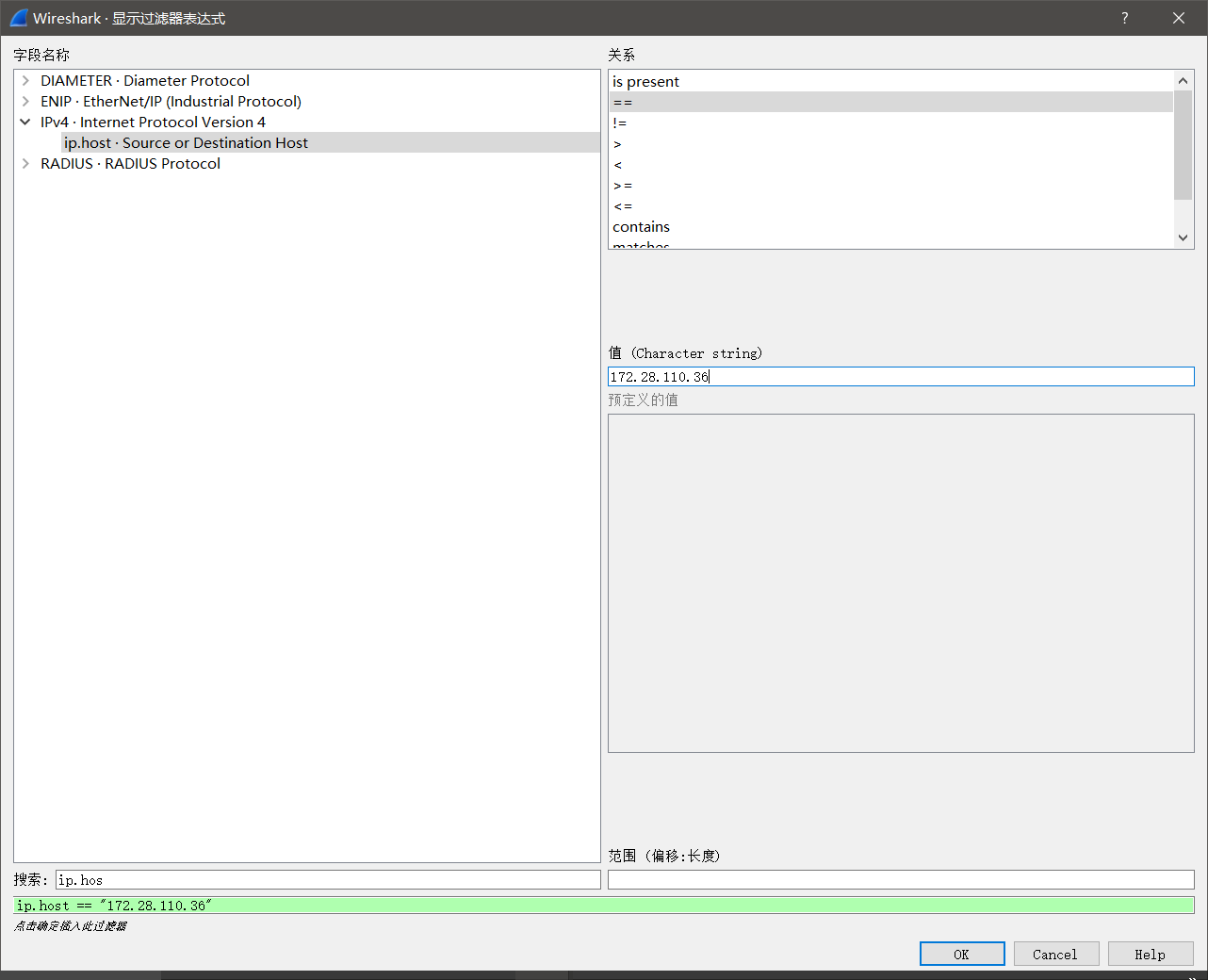


(2) display the filter

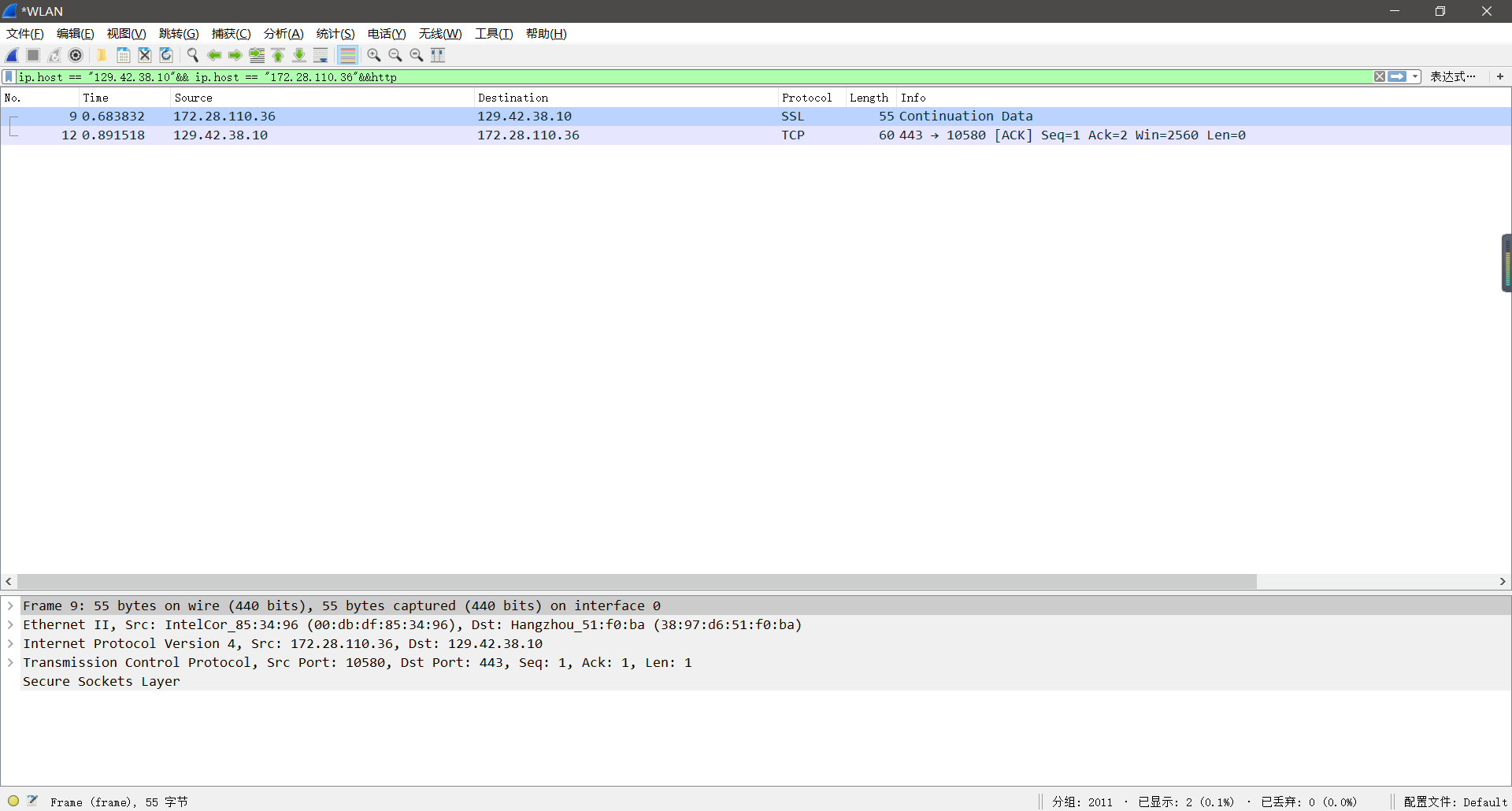


6. *are sent between your computer and to the server at* *[www.ibm.com](http://www.ibm.com) and use the HTTP protocol*

(1) select the filter

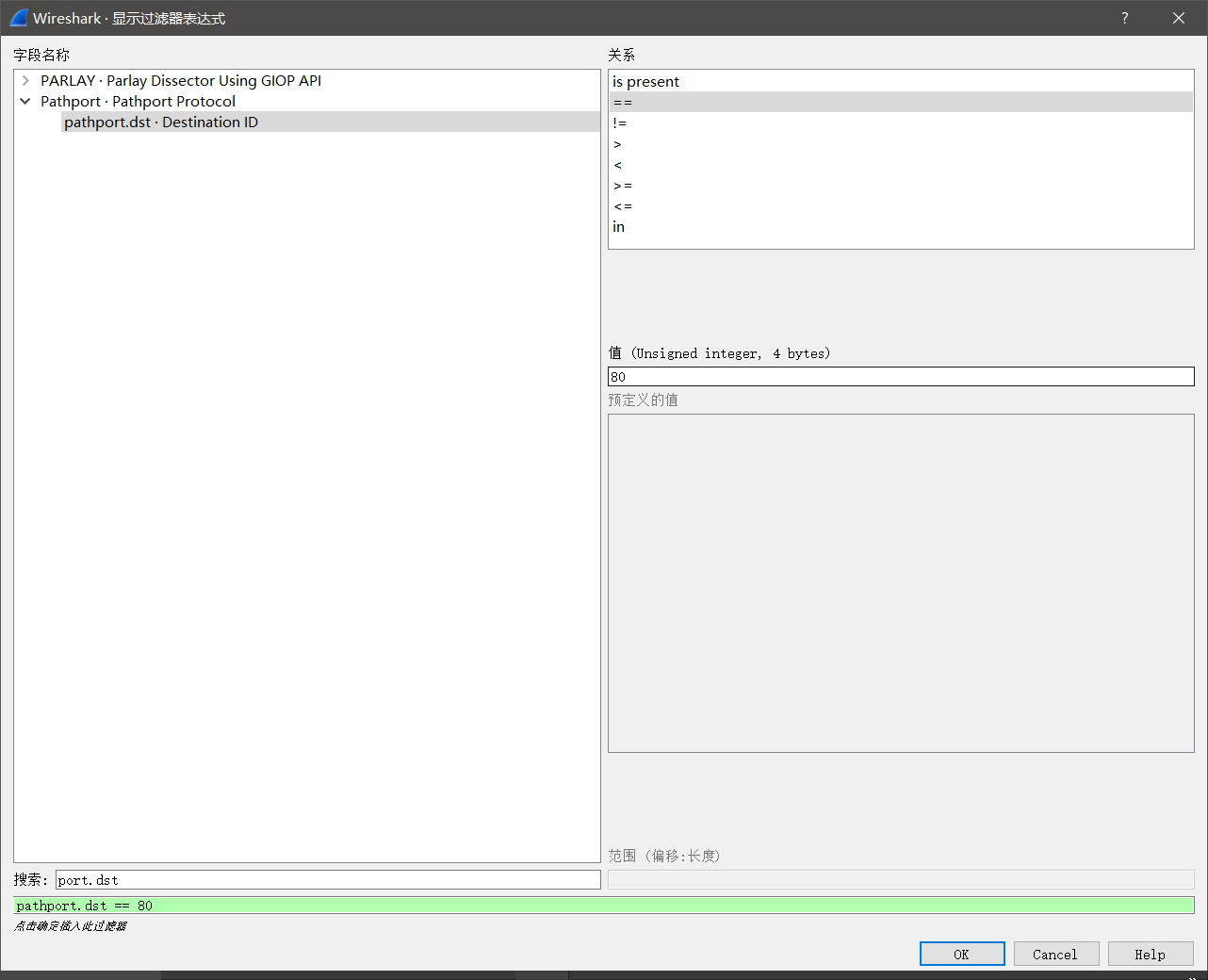


(2) display the filter

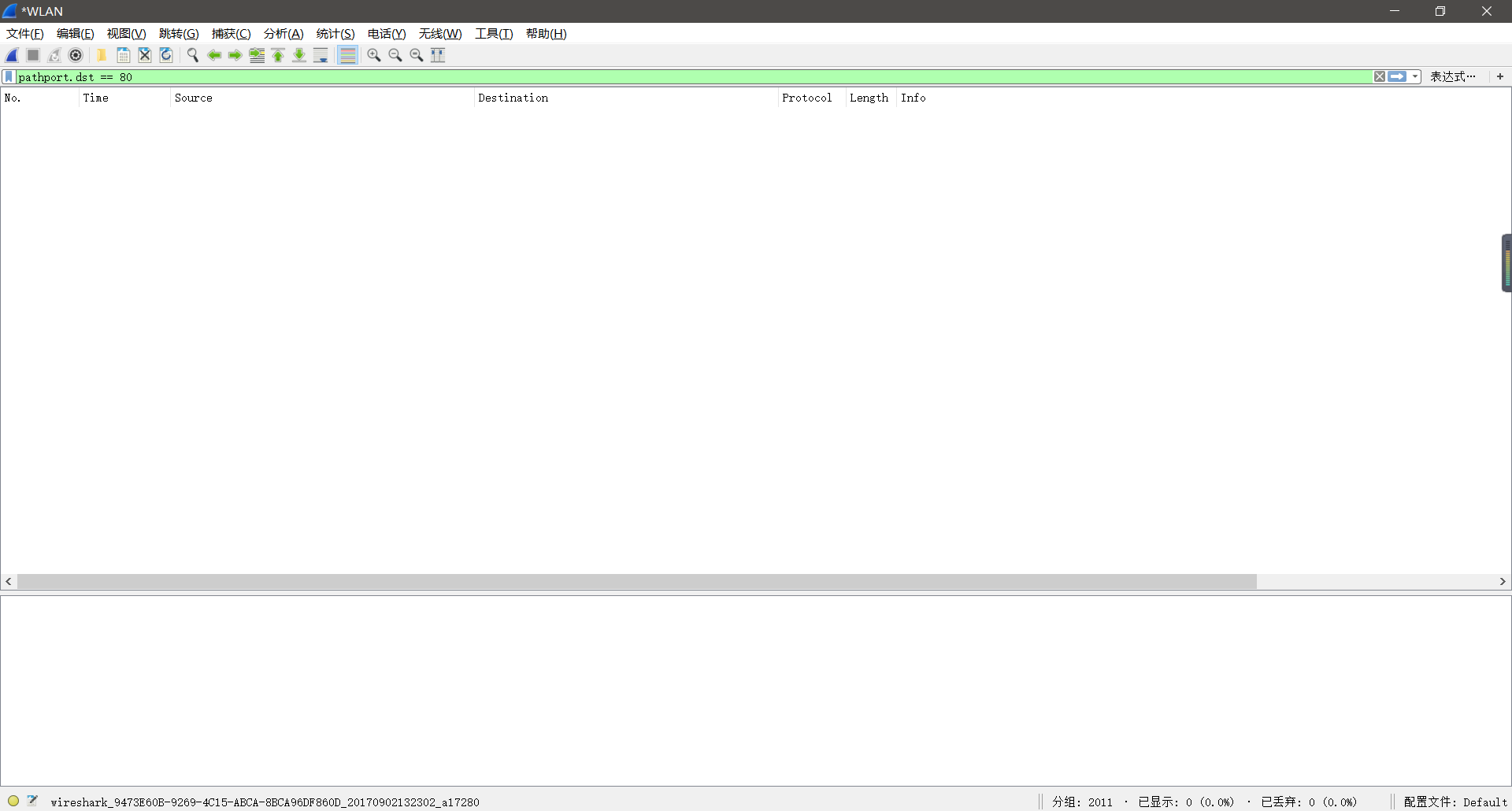


7. *are sent to port 80*

(1) select the filter

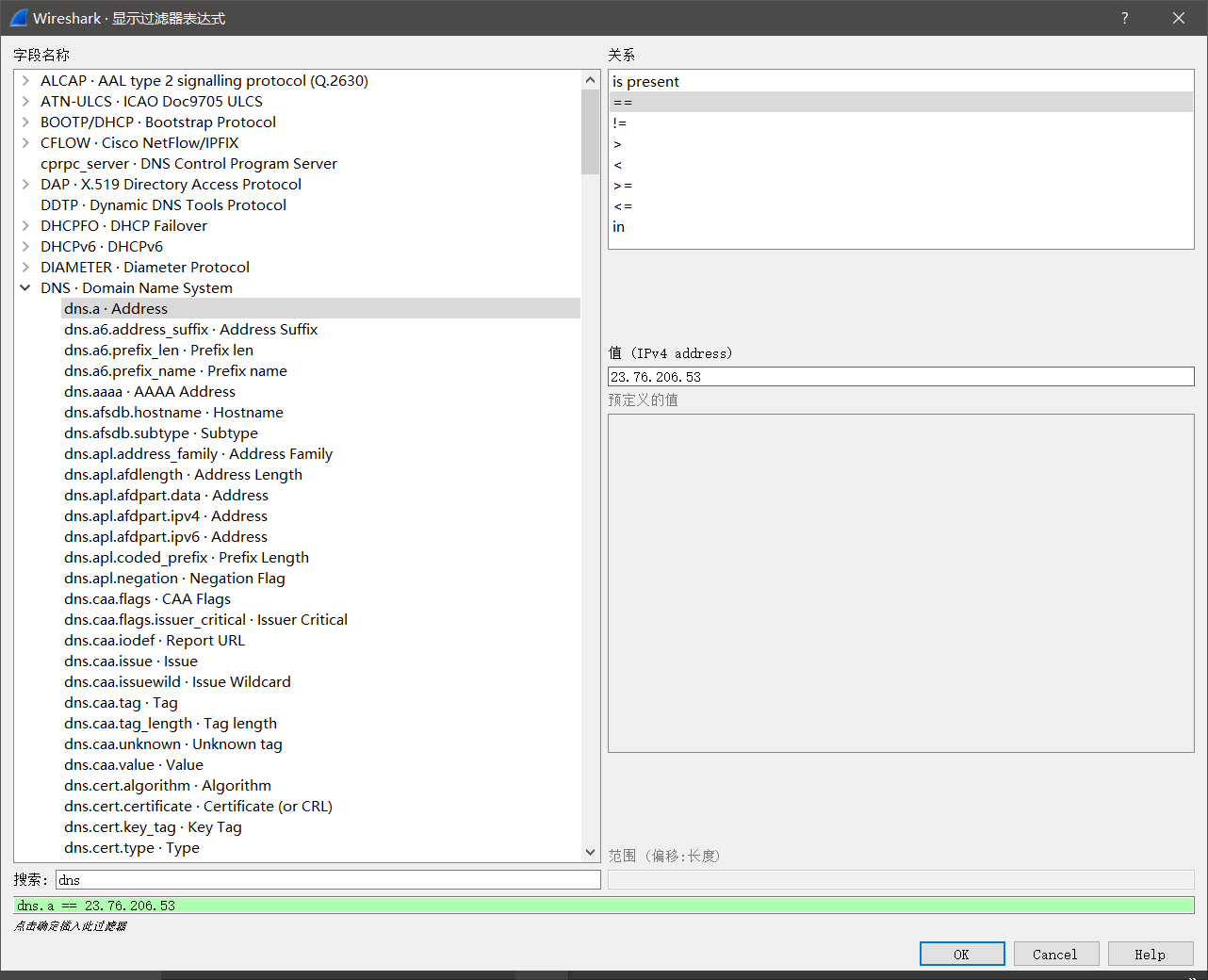


(2) display the filter

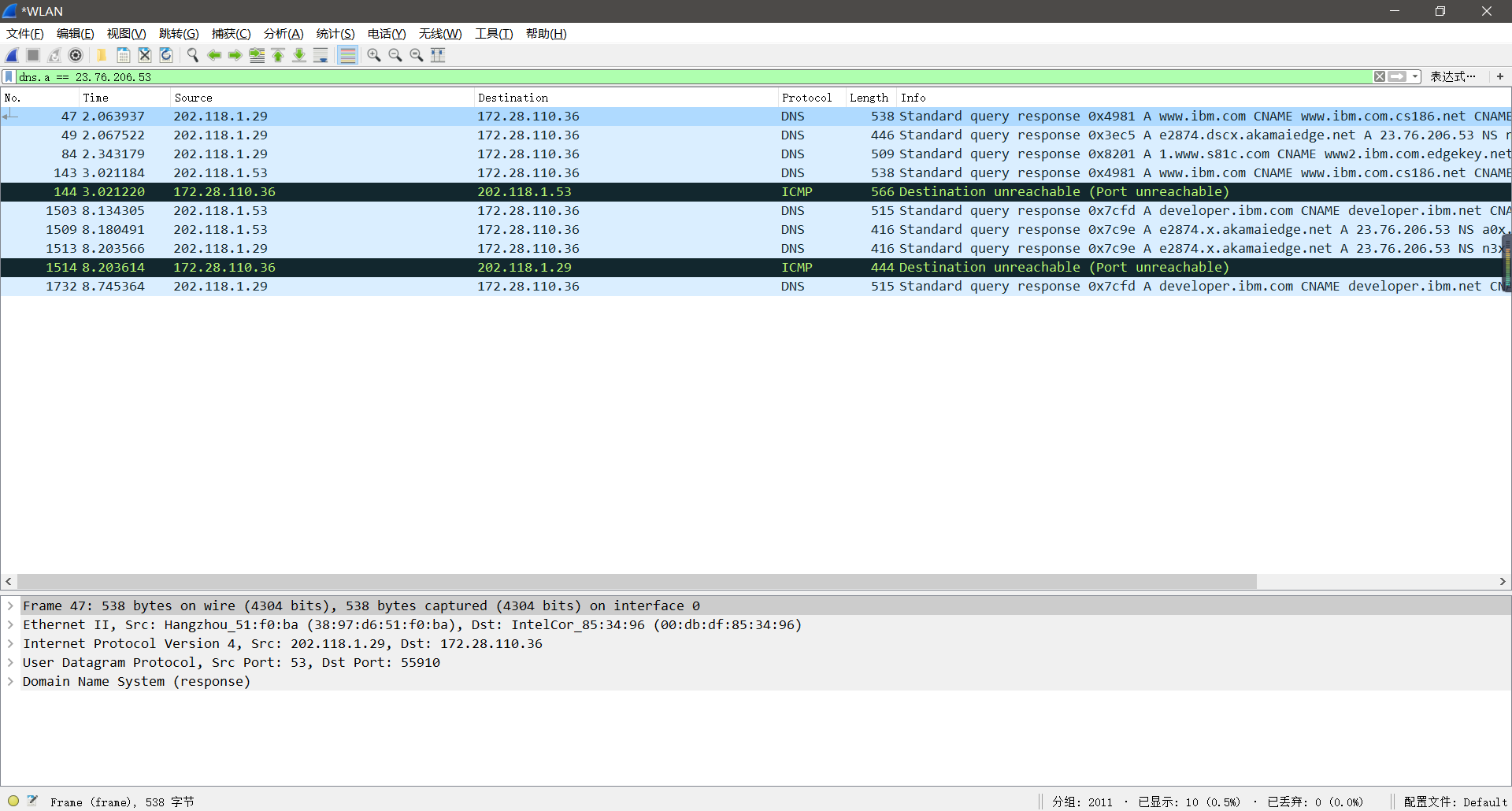


8. *transmit a standard DNS name query*

(1) select the filter



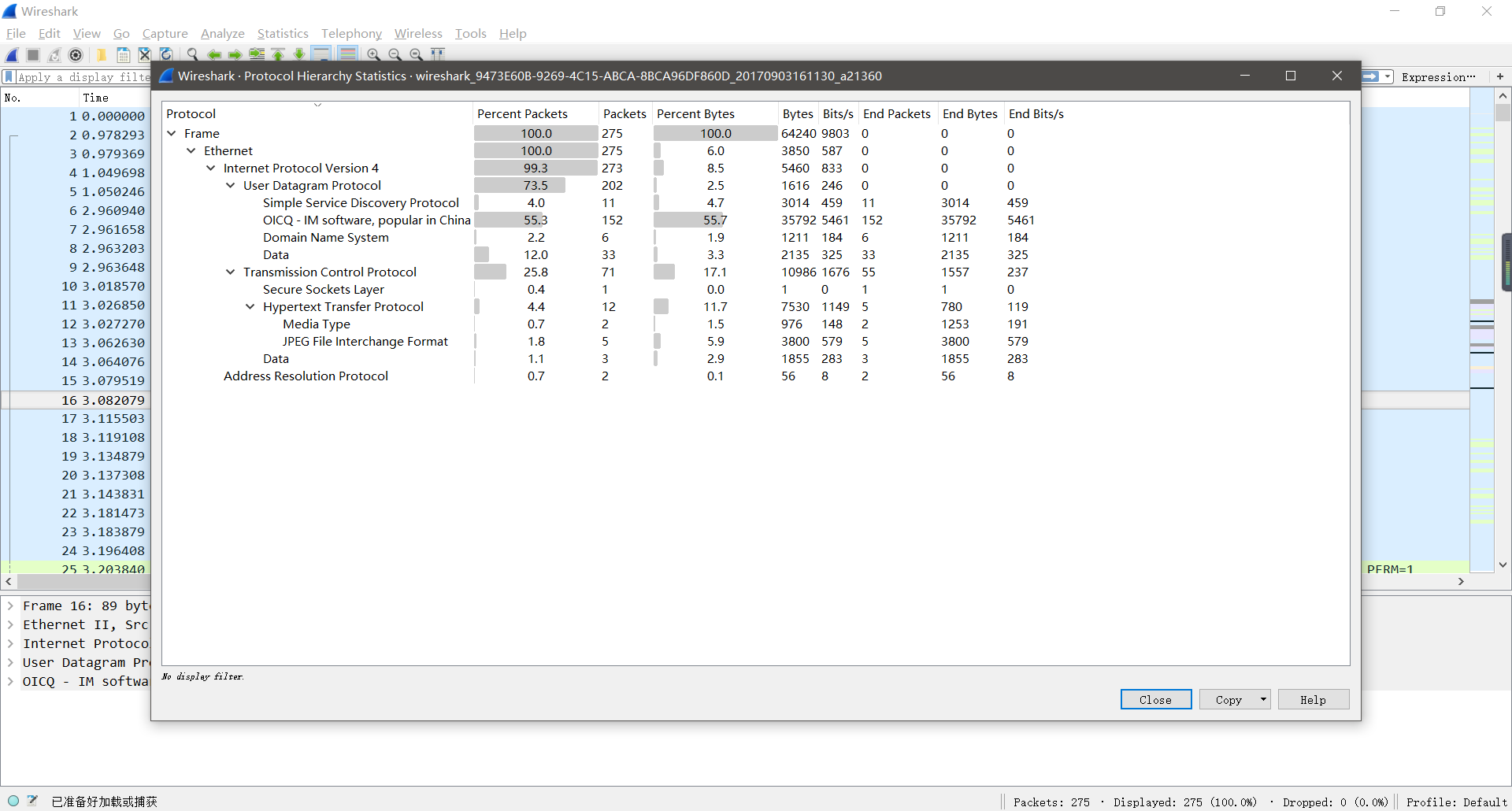
(2) display the filter



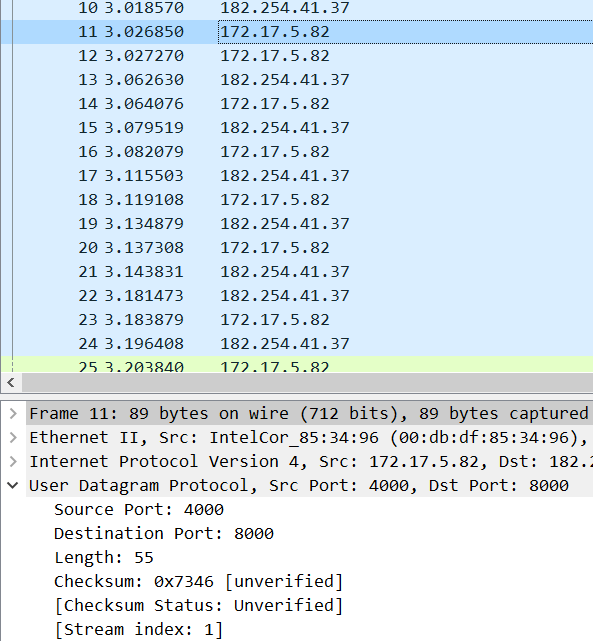
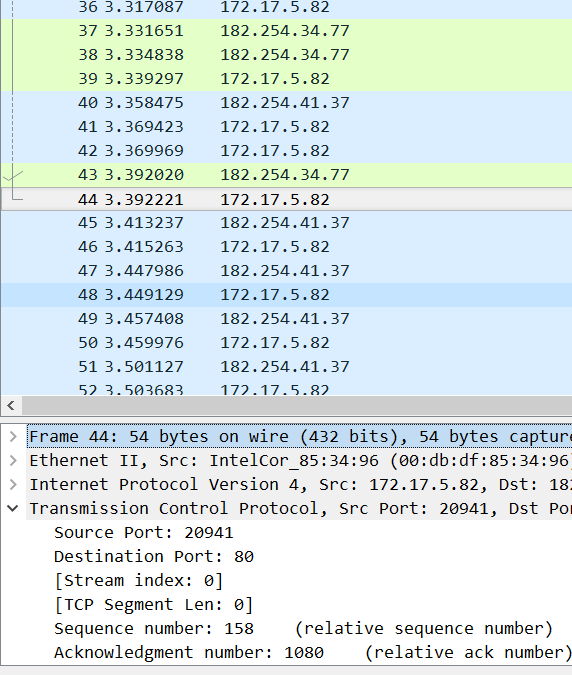
Part 2

*For the following exercises first apply the filter you created in the exercise above:*

1. *Q:Which protocol is used by all packets?*



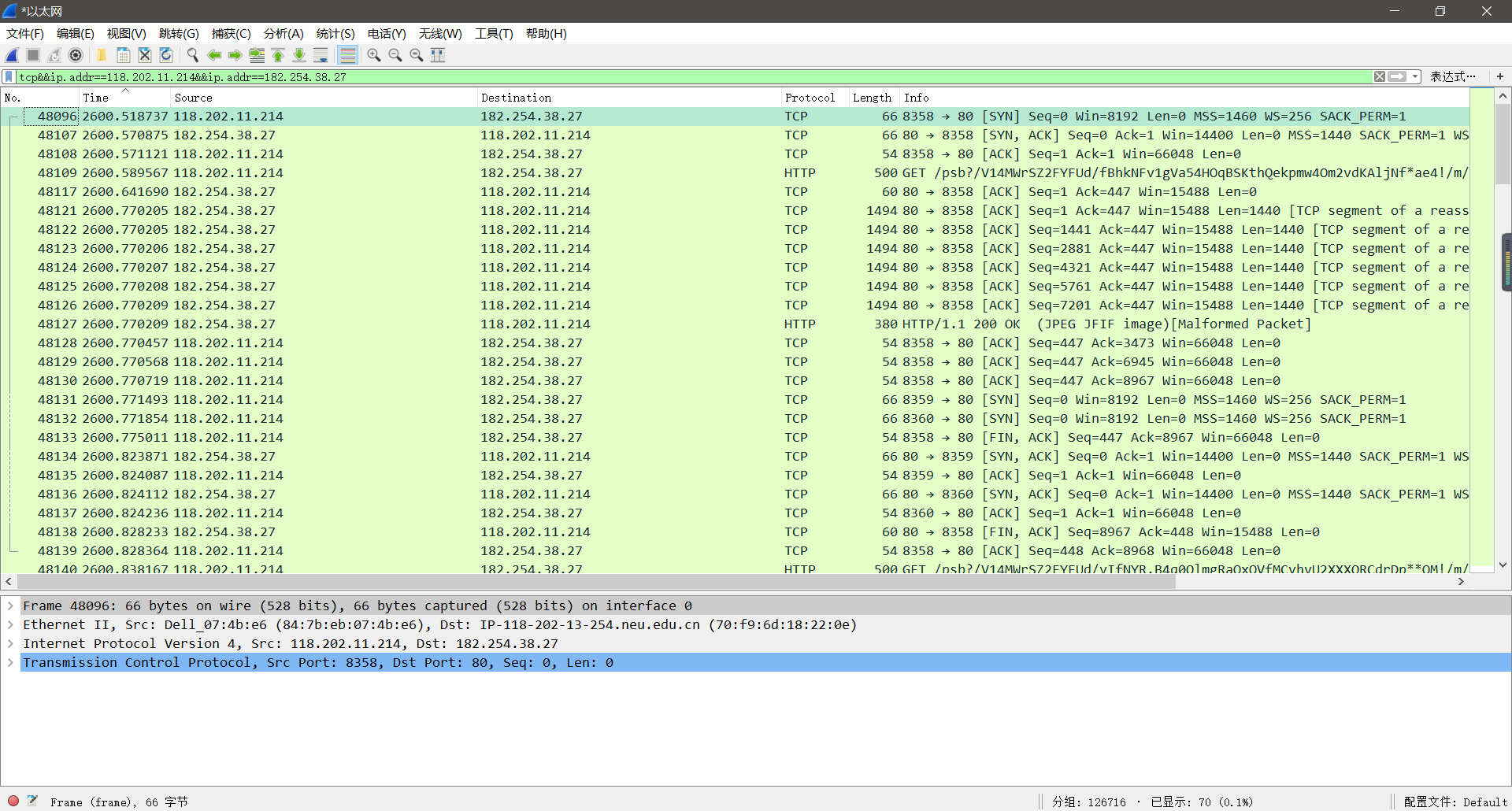
A:From the statistics picture, we can find that all packets used IP protocol. So, the answer should be **IP protocol**.

2. Q: *What are the source port values for these packets? (Select at least two different packets before answering this question)*

A: In the left picture, the source port is **20941**, and the other is **4000**.

3. *Q: Which Transport Control Protocol flags are set?*

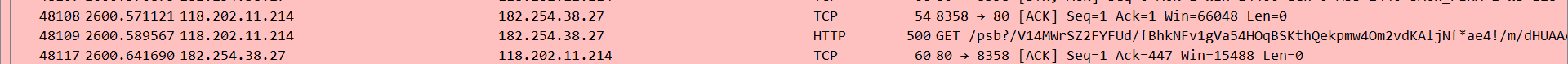
I select the filter that “tcp&&ip.addr==118.202.11.214&&ip.addr==182.254.38.27”

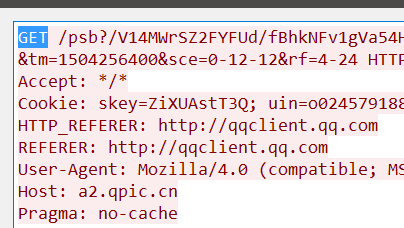


A: And from the picture, we can find SYN, ACK, FIN. these 3 kinds of flags.

4. *Q:* *Review an HTTP packet. Were you able to locate an HTTP request method? If so, which one is specified?*

Yes. For example, we can find that the HTTP is requesting **GET** method.





5. *Q: What is the HTTP request version?*

GET /psb?/V14MWrSZ2FYFUd/fBhkNFv1gVa54HOqBSKthQekpmw4Om2vdKAljNf\*ae4!/m/dHUAAAAAAAAA&ek=1&kp=1&pt=0&bo=vQG9AQAAAAARADc!&tm=1504256400&sce=0-12-12&rf=4-24 HTTP/1.1

Accept: \*/\*

Cookie: skey=ZiXUAstT3Q; uin=o0245791886; p\_skey=qppBBYcS3R3iCyEB0aCG401m1nvi87\*8oC5sGLV7-8o\_;

HTTP\_REFERER: http://qqclient.qq.com

REFERER: http://qqclient.qq.com

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

Host: a2.qpic.cn

Pragma: no-cache

A: The above text is the HTTP stream head part of mine. We can know that our HTTP request version is **1.1**.

6.Q: *What version of the Internet Protocol is being used?*

HTTP/1.1 200 OK

Server: httpserver

Last-Modified: Mon, 18 Dec 2006 07:25:14 GMT

Content-Length: 8674

Content-Type: image/jpeg

Size: 8674

Keep-Alive: timeout=57

Server-Time: 126

Timing-Allow-Origin: http://qqclient.qq.com

Cache-Control: max-age=31536000

Client-Ip: 118.202.11.214

A: The above text is the HTTP stream head part of theirs.

So, we can judge that the IP version is **IPv4** from the IP address “118.202.11.214”.

7. *Q: What is the IP header length in bytes?*

A: Also in the last text. We know that the IP header length is 8674.

8. *Q: Which IP flags are set?*

A: Also from the blue text, we know **MF** is set.

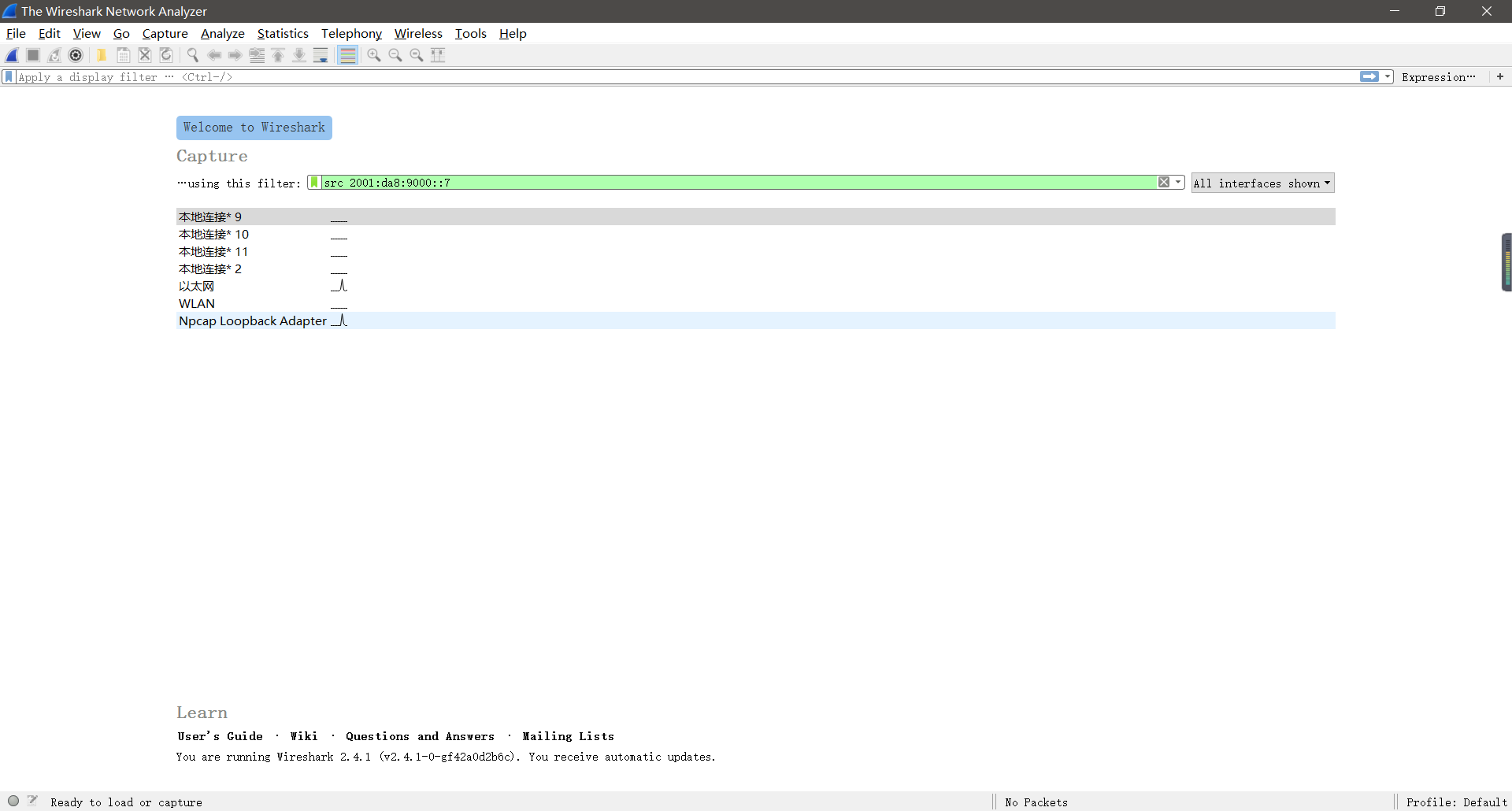
9. *Q: What is the IP Time-to-Live value in seconds?*

A: Also from the blue text, we know the Time-to-Live is **57**.

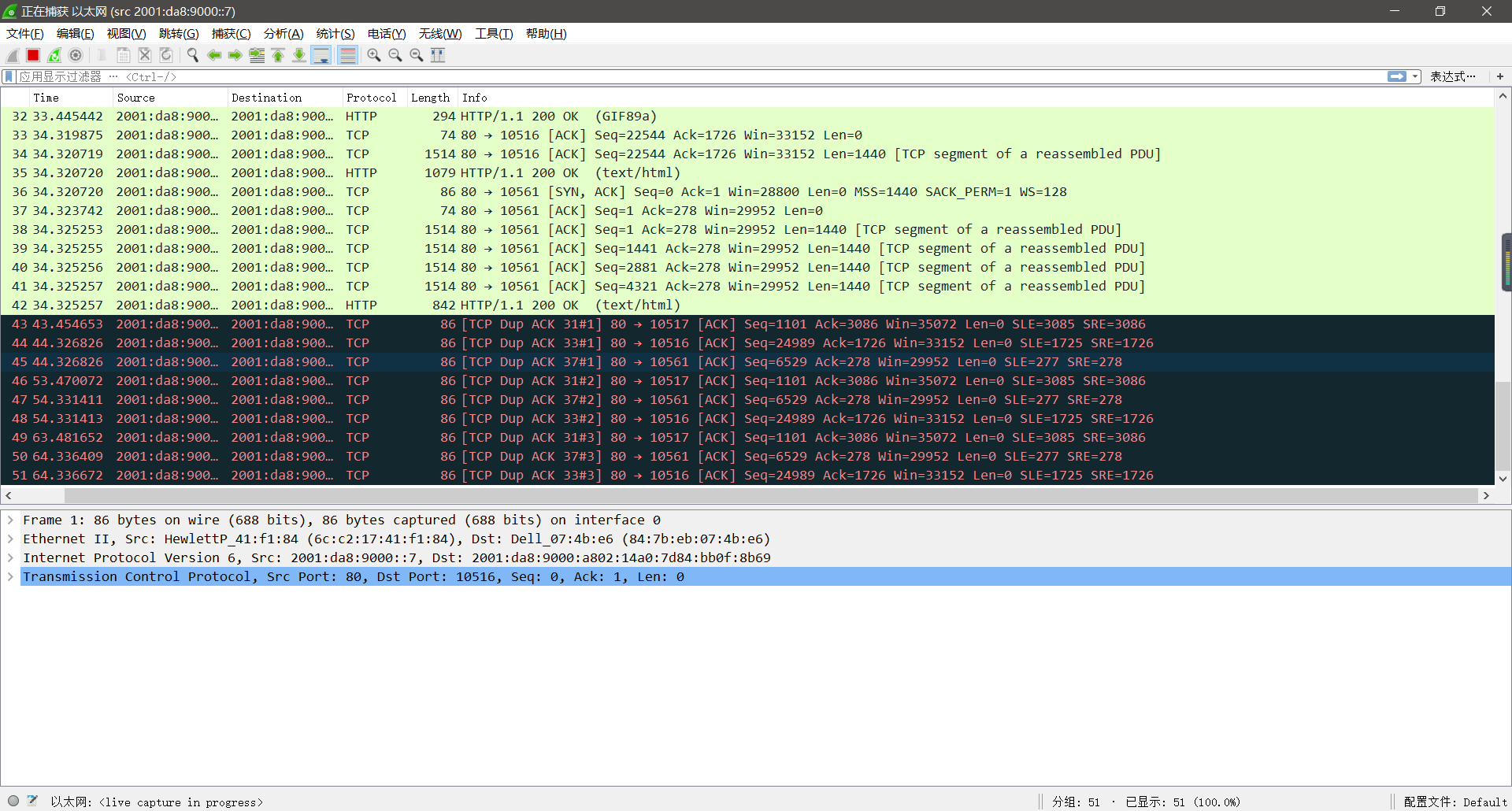
Part 3 *Browse to* [*http://www.neu.edu.cn*](http://www.neu.edu.cn) *from the Windows 7 machine and use Wireshark to capture the packets sent to your computer. Once you have opened at least 3 tabs on the* [*www.neu.edu.cn*](http://www.neu.edu.cn) *site end your browse session and stop the capture.*

1. *Sets web server as the source IP address*

(1) set the filter

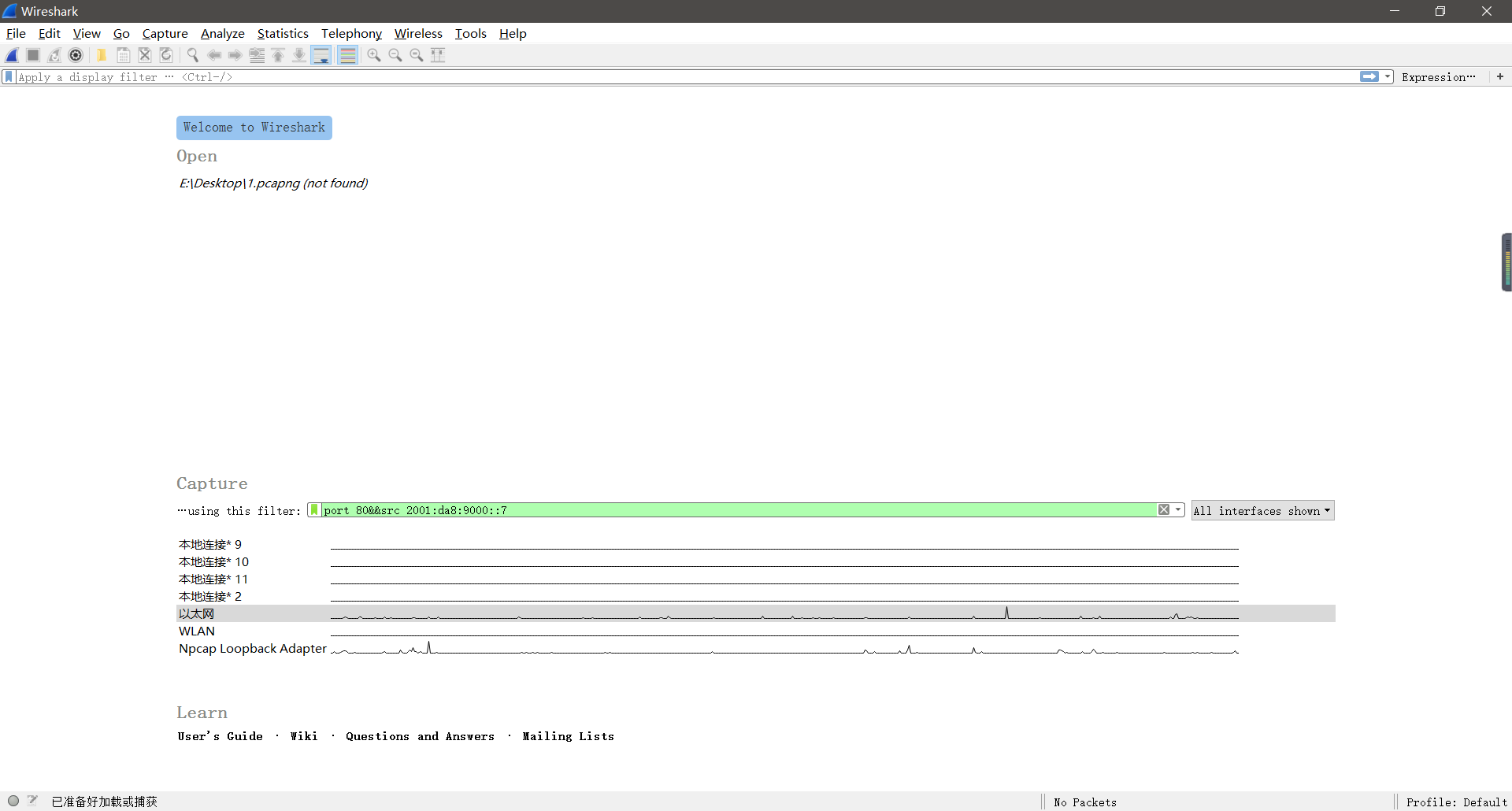


(2) start capturing

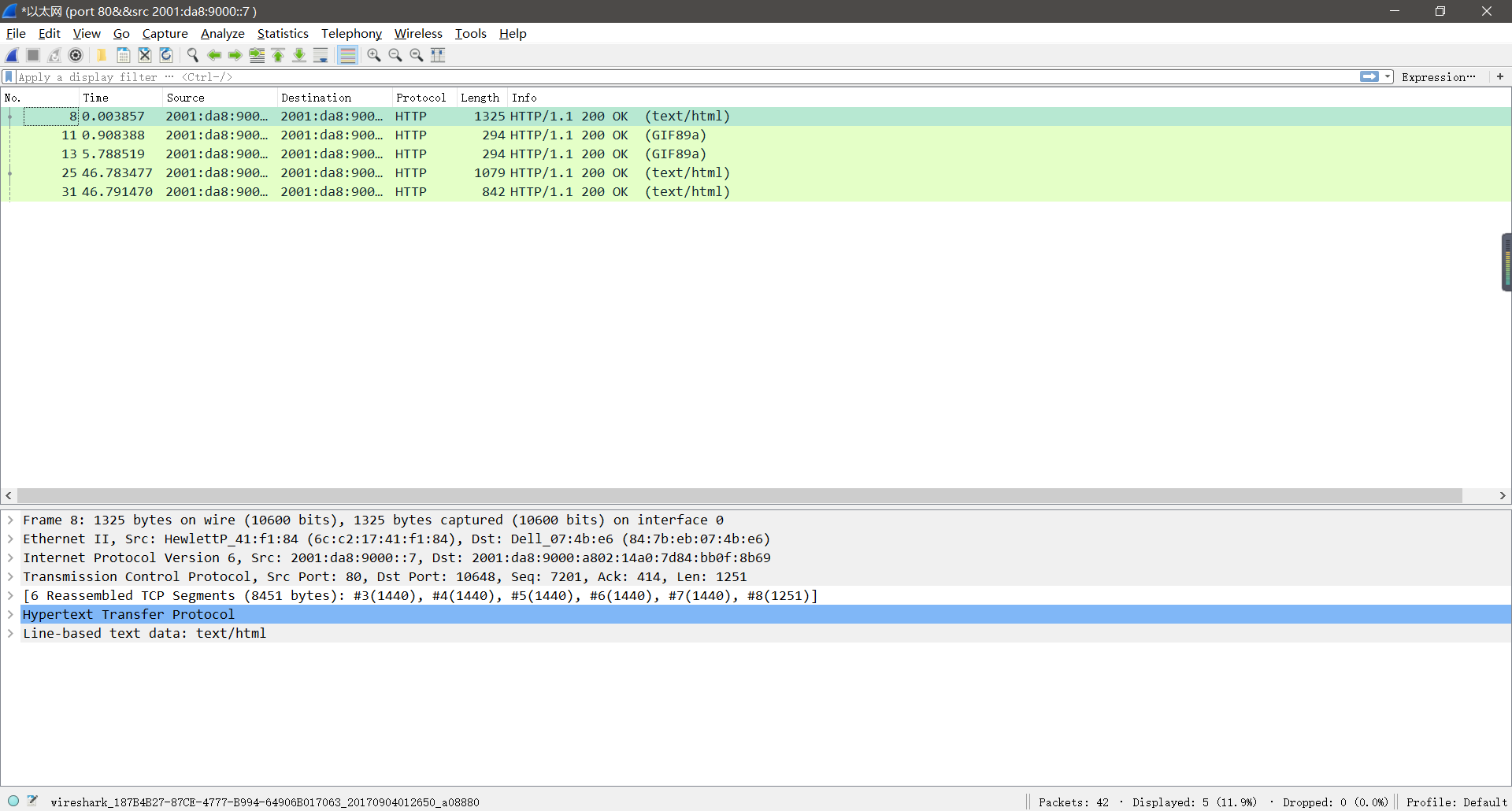


2. *Capture only HTTP traffic*

(1) set the filter

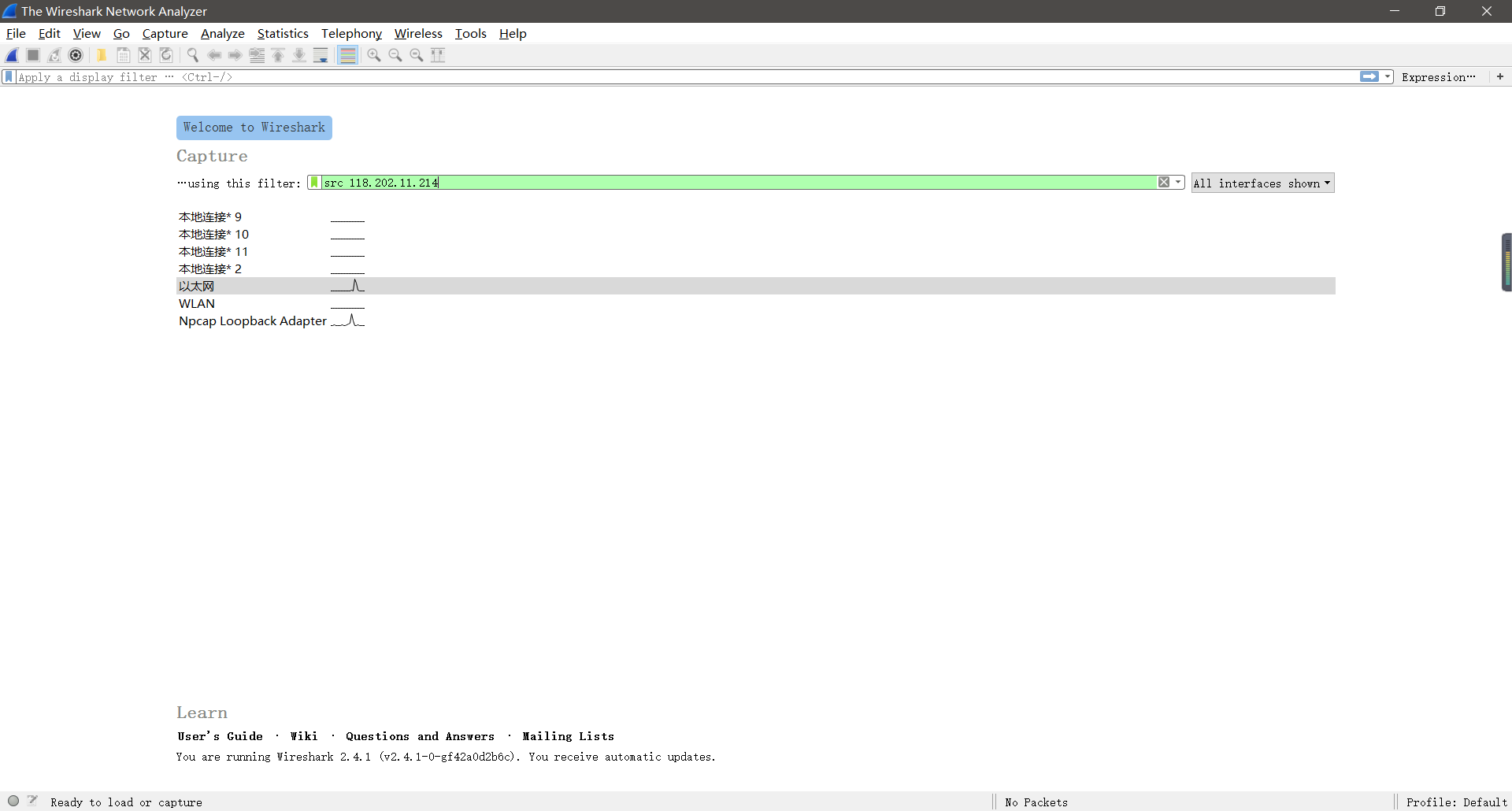


(2) start capturing

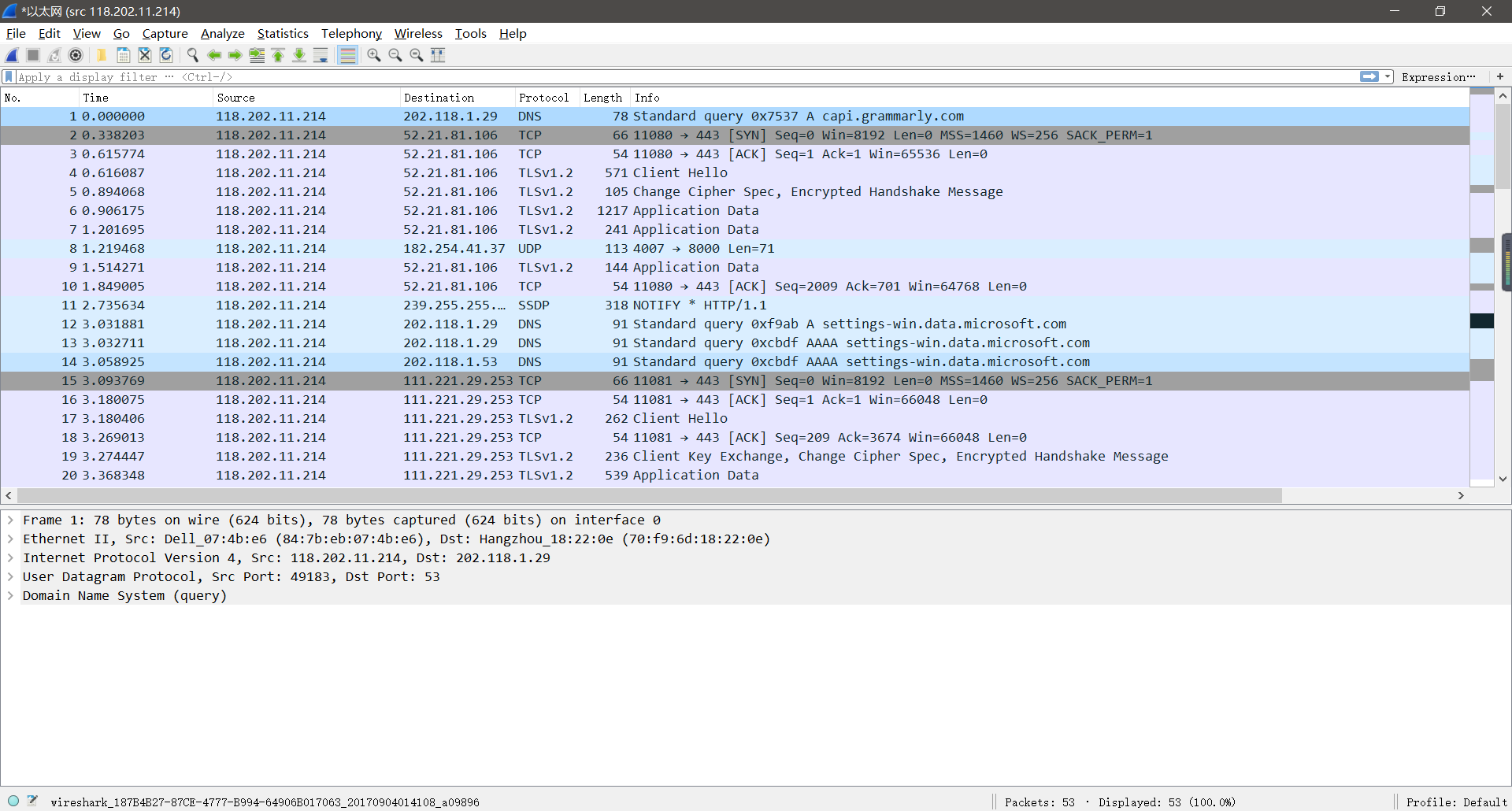


3. *Set Windows 7 machine as the source IP address*

(1) set the filter



(2) start capturing



4. *Q: How do the captures compare?*

A: There are two kinds of capture filters. First capture is set when we want to look through the result. And the other filter is set before we start our capturing. There are mainly 3 differences.

a. First method will capture more.

b. We just have one chance to set the filter if we use the second method.

c. The time to set them is different (before capturing or is capturing)

But what’s common is that we will see the same result if we set the same filter.