**Southern University of Science and Technology**

**Computer Networking Lab Report**

**唐润哲 11710418**

* ***Introduction：***

**2.2、Use Wireshark to capture packets and answer the questions with your screenshots:**

1. Open http://example.com in your browser, what kindof display filter do you need to filter out HTTP packets?

2. How many layers do you see in the HTTP requestpacket? What’s the src ip addr, src port, dst ip addr and dst port of the request packet?

3. What kind of information can be found in the HTTP response packet? Is there anything same with the information which is displayed on your browser?

**2.3、Use Wireshark to capture packets and answer those questions with your screenshots (both Wireshark and tracert display):**

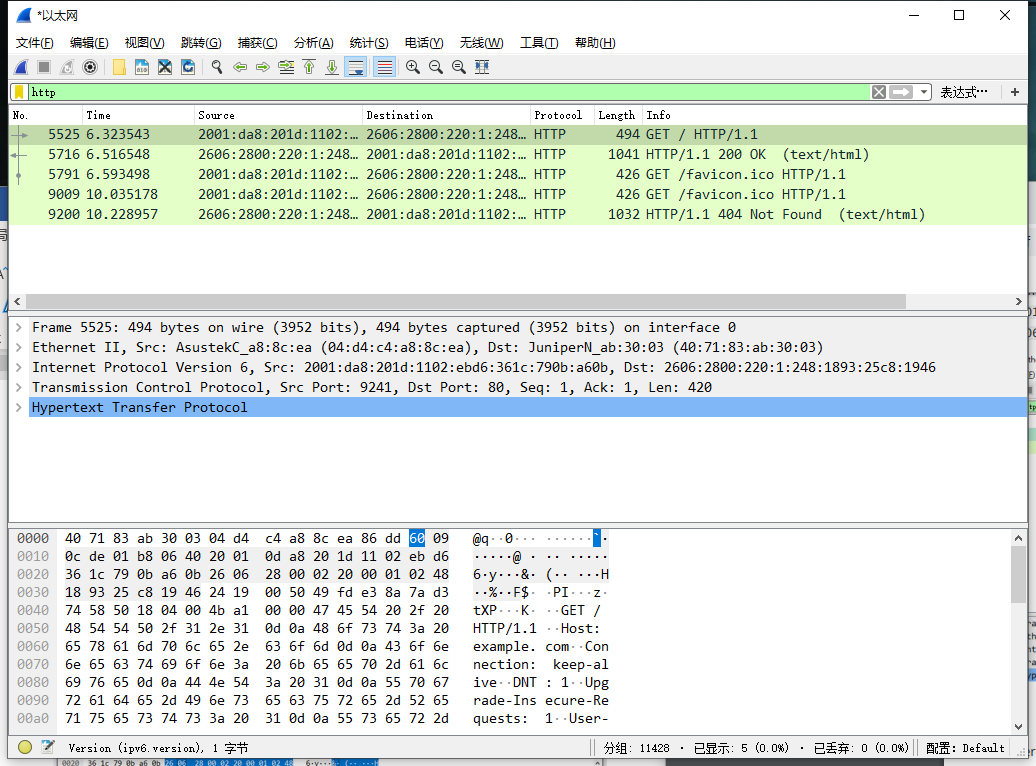
1. Using a proper capture filter/display filter to capture/display a tracert traffic. And start tracert baidu.com.

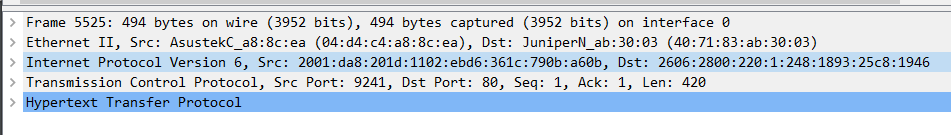
2. How many packets did tracert send for each hop?

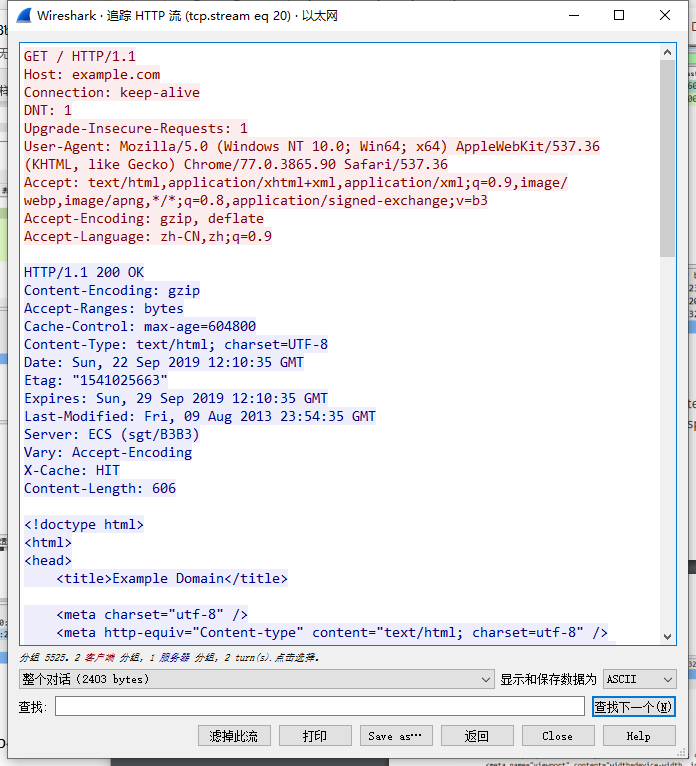
3. How many kinds of response did tracert receive from the remote? What’s the source IP address of these response message?

4. Try to calculate the RTT (round-trip time) between your host and baidu.com based on your capture instead of tracert display. Are they same with tracert display?

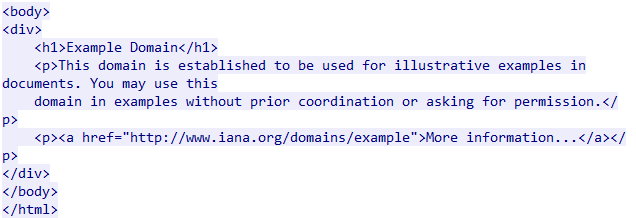
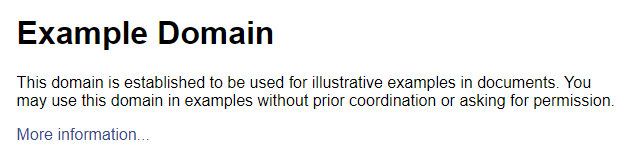
* ***Procedure and Result：***
* **Q2.2.1:**
  + Use “http” display filter to filter out all HTTP packets.

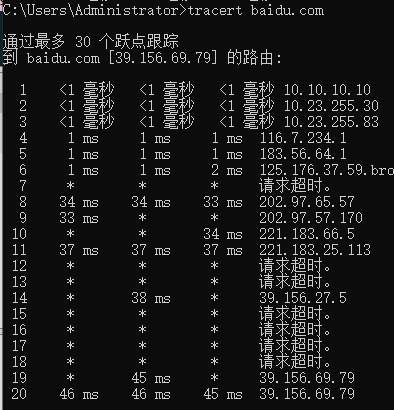


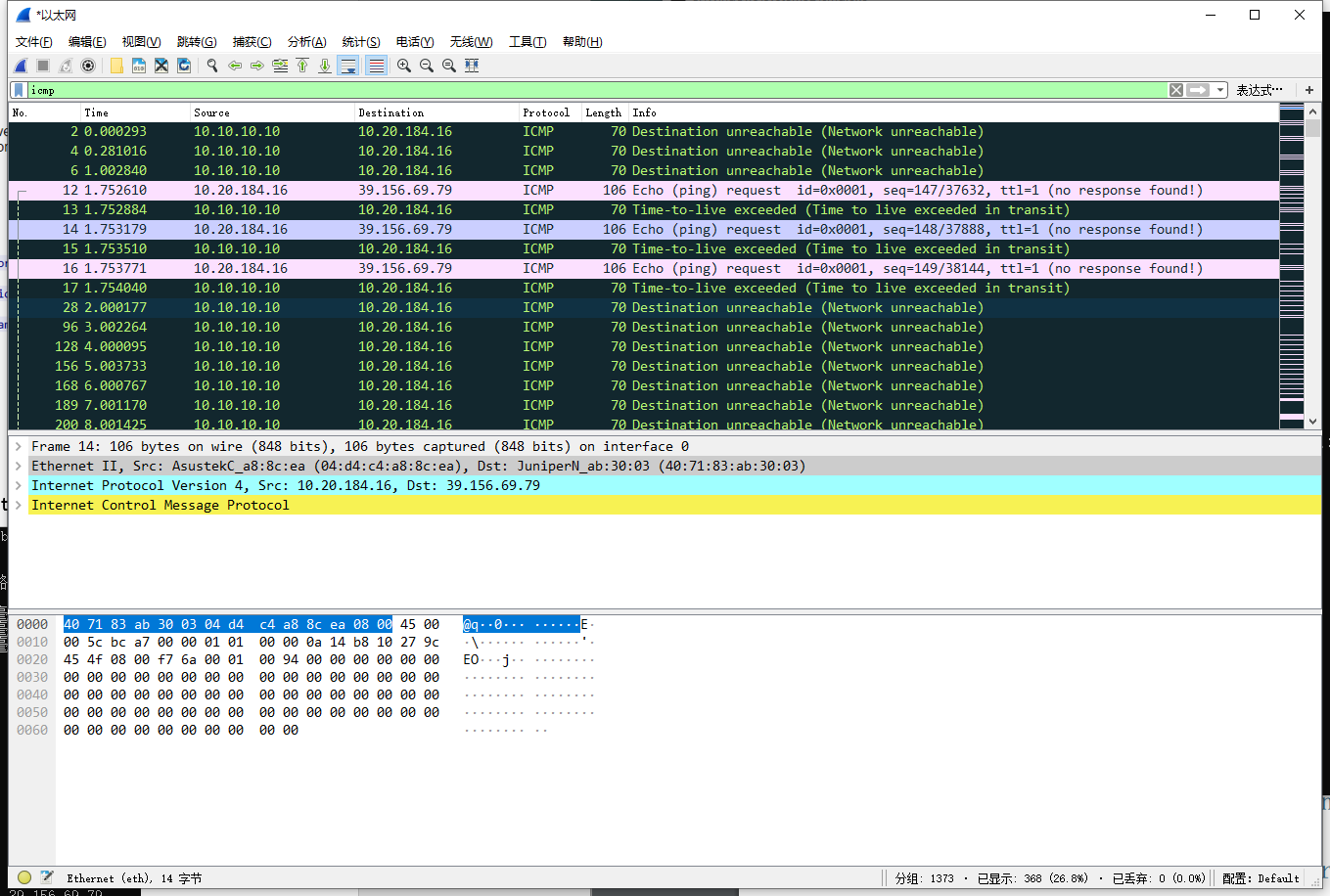
* **Q2.2.2:** 
  + There are Five layers in the request.
  + src ip addr: 2001:da8:201d:1102:ebd6:361c:790b:a60b
  + src port: 9241
  + dst ip addr: 2606:2800:220:1:248:1893:25c8:1946
  + dst port: 80
* **Q2.2.3:** As shown in the picture below,Content-Encoding、Cache-Control、Date、<html>、Content-Length and other information can be found in the http response packet.

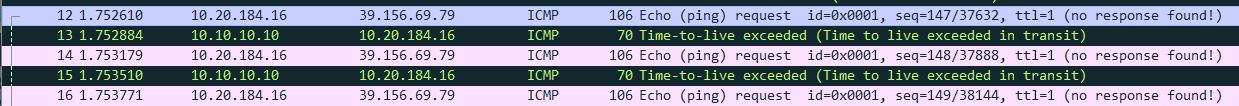


And a text included in the html file is the same with the information which is dispalyed on my borwser.



* **Q2.3.1:**
  + Using display filter “icmp”to display the tracert traffic.



* **Q2.3.2:**
  + There are three packets for each hop.
* **Q2.3.3:**
  + There are four kinds of response:

Time-to-live Exceeded(Time to live exceeded in transit)

Source IP:10.10.10.10,10.23.255.30,10.25.255.83,116.7.234.1,183.56.64.1,

59.37.176.125,202.97.65.57,202.97.57.170, 221.183.66.5, 221.183.25.113,

Echo(ping) request

Source IP:10.20.184.16,

Destination unreachable (Network unreachable)

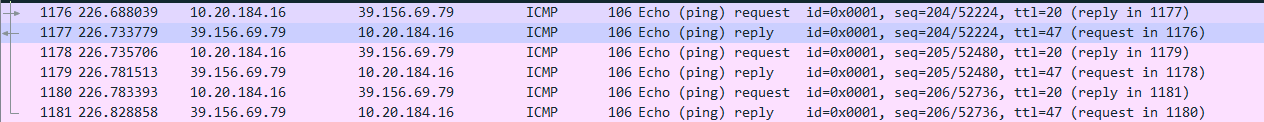
Source IP:10.10.10.10,

Destination unreachable (Port unreachable)

Source IP:10.23.255.83, 39.156.27.5,

* **Q2.3.4:**
  + The 20th hop response is long enough to calculate and easy enough to locate.

The RRT shown by the tracert display :46ms,46ms,45ms.

The RRT calculated based on wireshark:45.74ms,45.807ms,45,465ms

Obvously,they are the same.