# CS305 Lab2

**Name: 胡玉斌**
**Student Id: 11712121**

1. **Introduction**
    - Introduction to **Python**, learn how to use this interpreted high-level object-oriented programming language.
    - Introduction to **Wireshark**, it is a free and open-source packet analyzer. It is used for network trouble shooting, nalysis, software and communications protocol development, and education.
2. **Procedure**

    **Python**

    - Install python
    - Read-Eval-Print Loop
    - Basic Types and Operations
    - Sequence Types
    - Unpacking from Sequence Types
    - Set & Dict
    - Immutable & Mutable
    - Boolean Values
    - Flow Contril -- if
    - Flow Contril -- for
    - Flow Contril -- while
    - Defining Functions
    - Closure
    - Defining Classes
    - Duck Type
    - Module

    **Wireshark**

    - Capture Filter
        - Capture filter allows you to select the packets you want all the packets captured by Wireshark.
        - A proper capture filter can reduce the workload of Wireshark and the size of raw packets.
    - Display Filter

- After the capture starts, the display filter can be set to accurately hide the packet you don't care
- Display filter can be change at anytime on teh fly

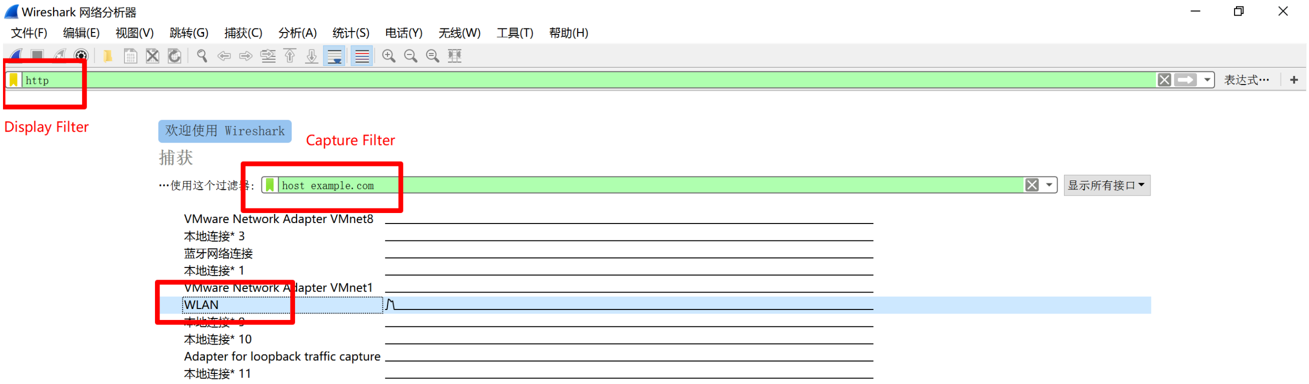
3. **Result** & **Analysis** (including answer of question)

**Assignment2.2**

Use Wiresharktocapturepackets and answer the questions with your screenshots:

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

> We need `http` display filter to filter out HTTP packets.


Wireshark 网络分析器
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
表达式…
+
欢迎使用 Wireshark
捕获
…使用这个过滤器:
显示所有接口
VMware Network Adapter VMnet8
本地连接* 3
蓝牙网络连接
本地连接* 1
VMware Network Adapter VMnet1
WLAN
本地连接* 9
本地连接* 10
Adapter for loopback traffic capture
本地连接* 11

http

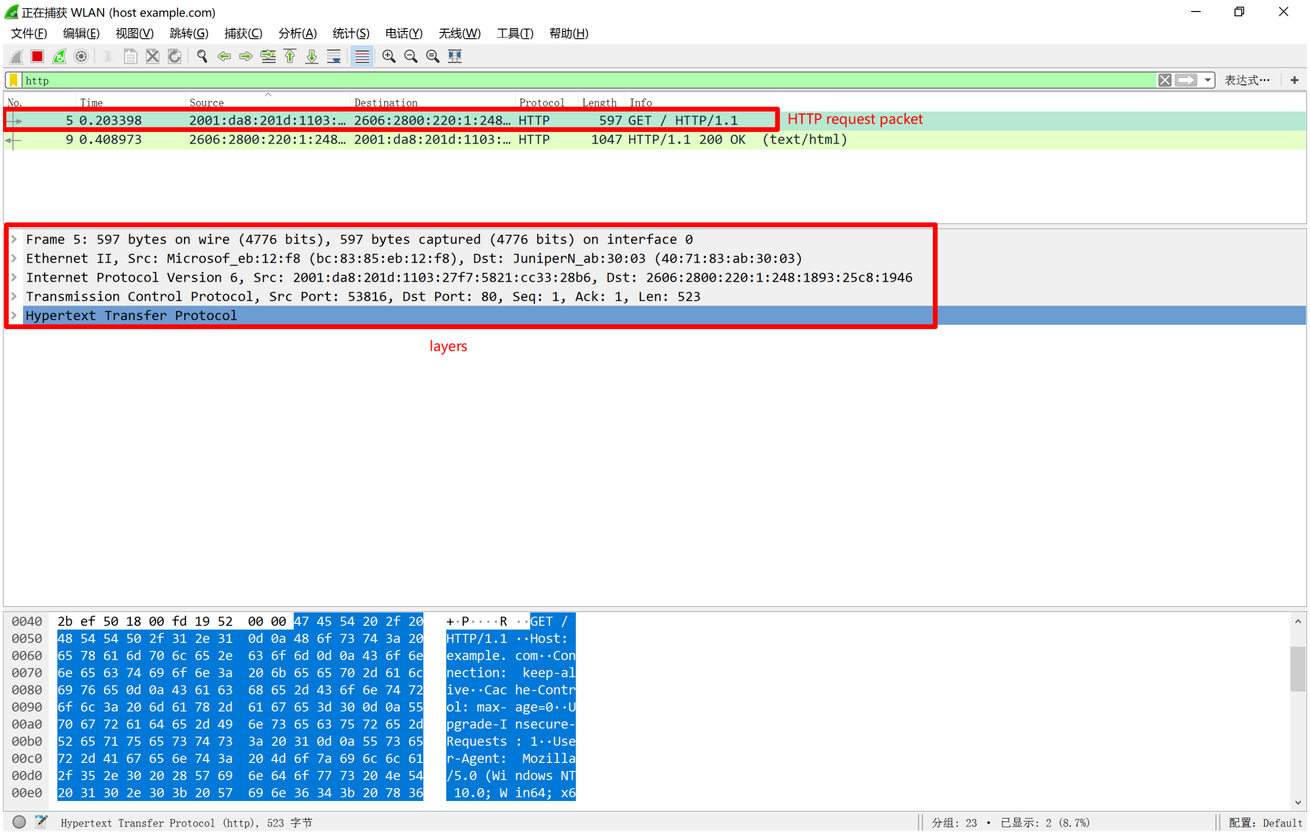
Display Filter

host example.com

Capture Filter

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

> There are `4` layers in the HTTP request packet.
>
> Line 2: Ethernet II, Src: link layer
>
> Line 3: ipv6: network layer
>
> Line 4: tcp: transport layer ``
>
> Line 5: http: application layer
>
> Line 1 is the packet imformation


正在捕获 WLAN (host example.com)
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
http
表达式…
+

```
No.   Time        Source                Destination           Protocol  Length  Info
    5 0.203398    2001:da8:201d:1103:…  2606:2800:220:1:248…  HTTP         597  GET / HTTP/1.1
    9 0.408973    2606:2800:220:1:248…  2001:da8:201d:1103:…  HTTP        1047  HTTP/1.1 200 OK  (text/html)
```

HTTP request packet

```
> Frame 5: 597 bytes on wire (4776 bits), 597 bytes captured (4776 bits) on interface 0
> Ethernet II, Src: Microsof_eb:12:f8 (bc:83:85:eb:12:f8), Dst: JuniperN_ab:30:03 (40:71:83:ab:30:03)
> Internet Protocol Version 6, Src: 2001:da8:201d:1103:27f7:5821:cc33:28b6, Dst: 2606:2800:220:1:248:1893:25c8:1946
> Transmission Control Protocol, Src Port: 53816, Dst Port: 80, Seq: 1, Ack: 1, Len: 523
> Hypertext Transfer Protocol
```

layers

```
0040  2b ef 50 18 00 fd 19 52  00 00 47 45 54 20 2f 20   +·P····R ··GET / 
0050  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1 ··Host: 
0060  65 78 61 6d 70 6c 65 2e  63 6f 6d 0d 0a 43 6f 6e   example. com··Con
0070  6e 65 63 74 69 6f 6e 3a  20 6b 65 65 70 2d 61 6c   nection:  keep-al
0080  69 76 65 0d 0a 43 61 63  68 65 2d 43 6f 6e 74 72   ive··Cac he-Contr
0090  6f 6c 3a 20 6d 61 78 2d  61 67 65 3d 30 0d 0a 55   ol: max- age=0··U
00a0  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d   pgrade-I nsecure-
00b0  52 65 71 75 65 73 74 73  3a 20 31 0d 0a 55 73 65   Requests : 1··Use
00c0  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:  Mozilla
00d0  2f 35 2e 30 20 28 57 69  6e 64 6f 77 73 20 4e 54   /5.0 (Wi ndows NT
00e0  20 31 30 2e 30 3b 20 57  69 6e 36 34 3b 20 78 36    10.0; W in64; x6
```

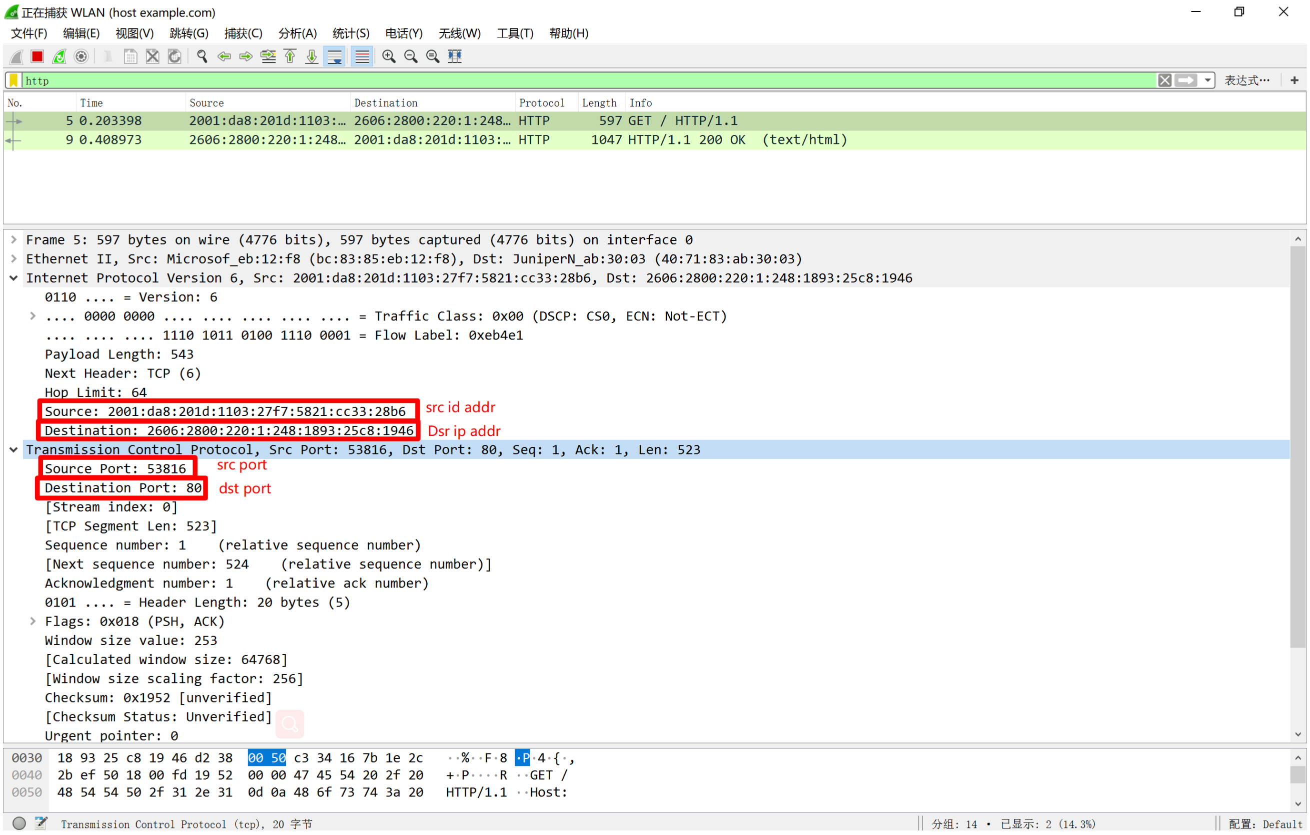
Hypertext Transfer Protocol (http), 523 字节 | 分组: 23 · 已显示: 2 (8.7%) | 配置: Default

src ip addr: 2001:da8:201d:1103:27f7:5821:cc33:28b6

src port: 53816

detip addr: 2606:2800:220:1:248:1893:25c8:1946

detip port: 80


正在捕获 WLAN (host example.com)
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
http
表达式…
+

```
No.   Time        Source                Destination           Protocol  Length  Info
    5 0.203398    2001:da8:201d:1103:…  2606:2800:220:1:248…  HTTP         597  GET / HTTP/1.1
    9 0.408973    2606:2800:220:1:248…  2001:da8:201d:1103:…  HTTP        1047  HTTP/1.1 200 OK  (text/html)
```

```
> Frame 5: 597 bytes on wire (4776 bits), 597 bytes captured (4776 bits) on interface 0
> Ethernet II, Src: Microsof_eb:12:f8 (bc:83:85:eb:12:f8), Dst: JuniperN_ab:30:03 (40:71:83:ab:30:03)
v Internet Protocol Version 6, Src: 2001:da8:201d:1103:27f7:5821:cc33:28b6, Dst: 2606:2800:220:1:248:1893:25c8:1946
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 1110 1011 0100 1110 0001 = Flow Label: 0xeb4e1
    Payload Length: 543
    Next Header: TCP (6)
    Hop Limit: 64
    Source: 2001:da8:201d:1103:27f7:5821:cc33:28b6
    Destination: 2606:2800:220:1:248:1893:25c8:1946
v Transmission Control Protocol, Src Port: 53816, Dst Port: 80, Seq: 1, Ack: 1, Len: 523
    Source Port: 53816
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 523]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 524    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window size value: 253
    [Calculated window size: 64768]
    [Window size scaling factor: 256]
    Checksum: 0x1952 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
```

src id addr

Dsr ip addr

src port

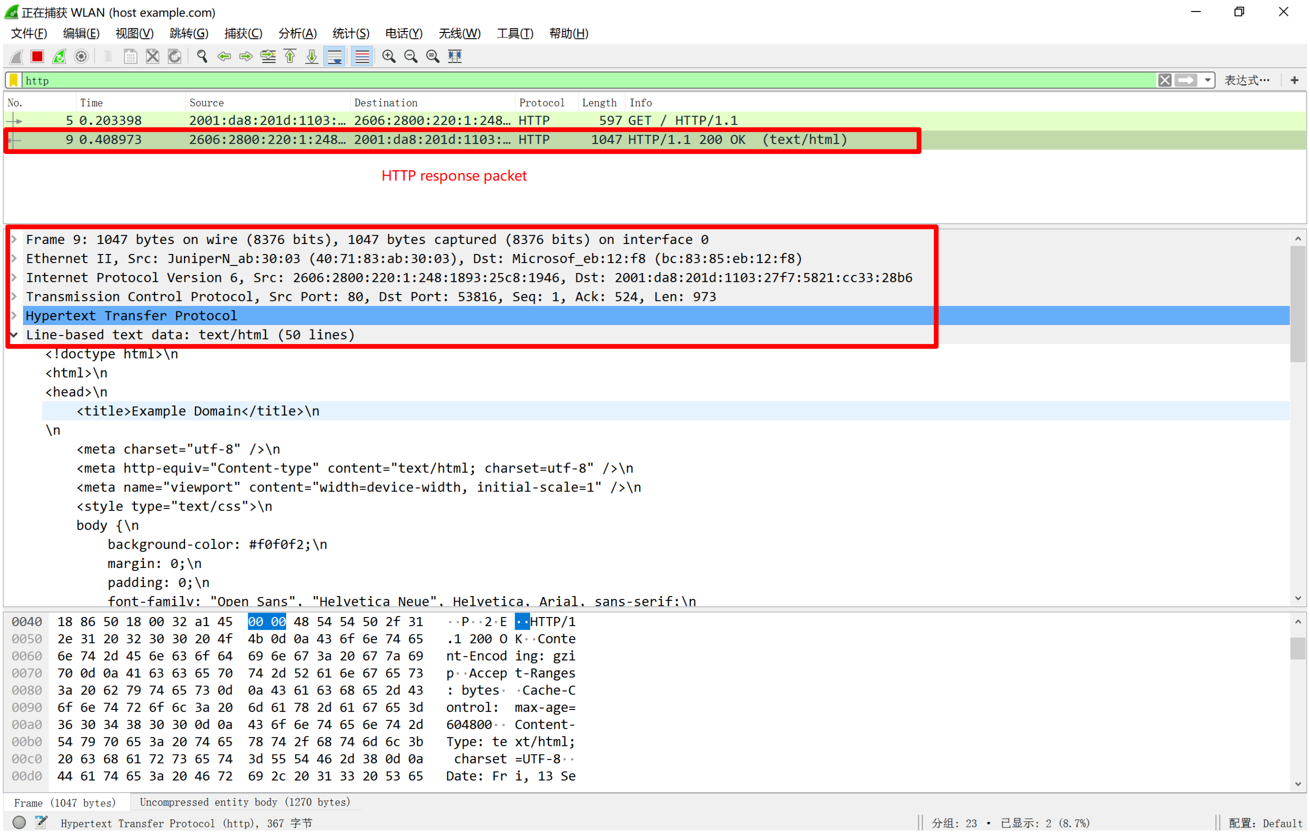
dst port

```
0030  18 93 25 c8 19 46 d2 38  00 50 c3 34 16 7b 1e 2c   ··%··F·8 ·P·4·{·,
0040  2b ef 50 18 00 fd 19 52  00 00 47 45 54 20 2f 20   +·P····R ··GET / 
0050  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1 ··Host: 
```

Transmission Control Protocol (tcp), 20 字节 | 分组: 14 · 已显示: 2 (14.3%) | 配置: Default

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?

There 6 kinds of information can be found in the HTTP response packet.


正在捕获 WLAN (host example.com)
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
表达式…
+

```
http
```

```
No.   Time       Source                Destination           Protocol  Length  Info
    5 0.203398   2001:da8:201d:1103:…  2606:2800:220:1:248…  HTTP         597  GET / HTTP/1.1
    9 0.408973   2606:2800:220:1:248…  2001:da8:201d:1103:…  HTTP        1047  HTTP/1.1 200 OK  (text/html)
```

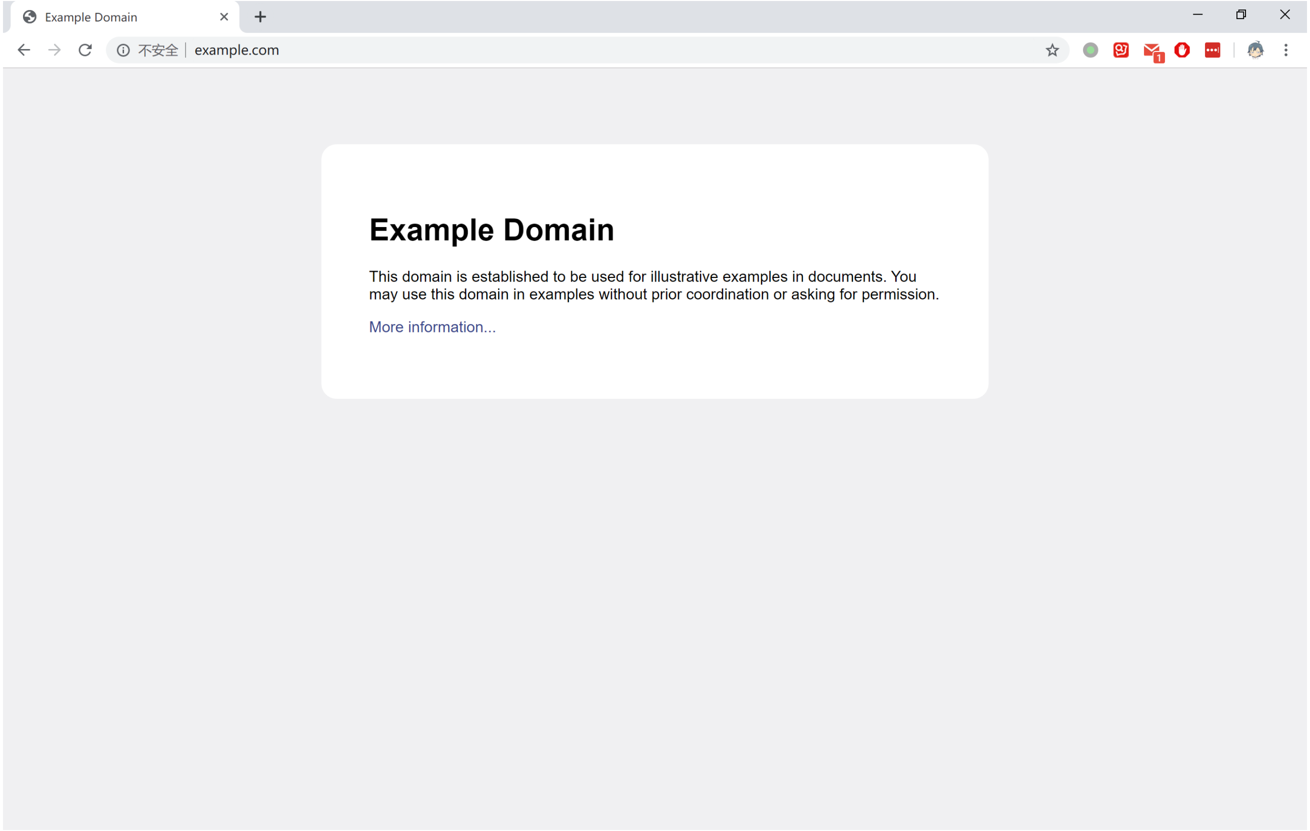
HTTP response packet

```
> Frame 9: 1047 bytes on wire (8376 bits), 1047 bytes captured (8376 bits) on interface 0
> Ethernet II, Src: JuniperN_ab:30:03 (40:71:83:ab:30:03), Dst: Microsof_eb:12:f8 (bc:83:85:eb:12:f8)
> Internet Protocol Version 6, Src: 2606:2800:220:1:248:1893:25c8:1946, Dst: 2001:da8:201d:1103:27f7:5821:cc33:28b6
> Transmission Control Protocol, Src Port: 80, Dst Port: 53816, Seq: 1, Ack: 524, Len: 973
> Hypertext Transfer Protocol
v Line-based text data: text/html (50 lines)
    <!doctype html>\n
    <html>\n
    <head>\n
        <title>Example Domain</title>\n
    \n
        <meta charset="utf-8" />\n
        <meta http-equiv="Content-type" content="text/html; charset=utf-8" />\n
        <meta name="viewport" content="width=device-width, initial-scale=1" />\n
        <style type="text/css">\n
        body {\n
            background-color: #f0f0f2;\n
            margin: 0;\n
            padding: 0;\n
            font-family: "Open Sans", "Helvetica Neue", Helvetica, Arial, sans-serif;\n
```

```
0040  18 86 50 18 00 32 a1 45  00 00 48 54 54 50 2f 31   ··P··2·E ··HTTP/1
0050  2e 31 20 32 30 30 20 4f  4b 0d 0a 43 6f 6e 74 65   .1 200 O K··Conte
0060  6e 74 2d 45 6e 63 6f 64  69 6e 67 3a 20 67 7a 69   nt-Encod ing: gzi
0070  70 0d 0a 41 63 63 65 70  74 2d 52 61 6e 67 65 73   p··Accep t-Ranges
0080  3a 20 62 79 74 65 73 0d  0a 43 61 63 68 65 2d 43   : bytes· ·Cache-C
0090  6f 6e 74 72 6f 6c 3a 20  6d 61 78 2d 61 67 65 3d   ontrol:  max-age=
00a0  36 30 34 38 30 30 0d 0a  43 6f 6e 74 65 6e 74 2d   604800·· Content-
00b0  54 79 70 65 3a 20 74 65  78 74 2f 68 74 6d 6c 3b   Type: te xt/html;
00c0  20 63 68 61 72 73 65 74  3d 55 54 46 2d 38 0d 0a    charset =UTF-8··
00d0  44 61 74 65 3a 20 46 72  69 2c 20 31 33 20 53 65   Date: Fr i, 13 Se
```

Frame (1047 bytes)
Uncompressed entity body (1270 bytes)
Hypertext Transfer Protocol (http), 367 字节
分组: 23 · 已显示: 2 (8.7%)
配置: Default

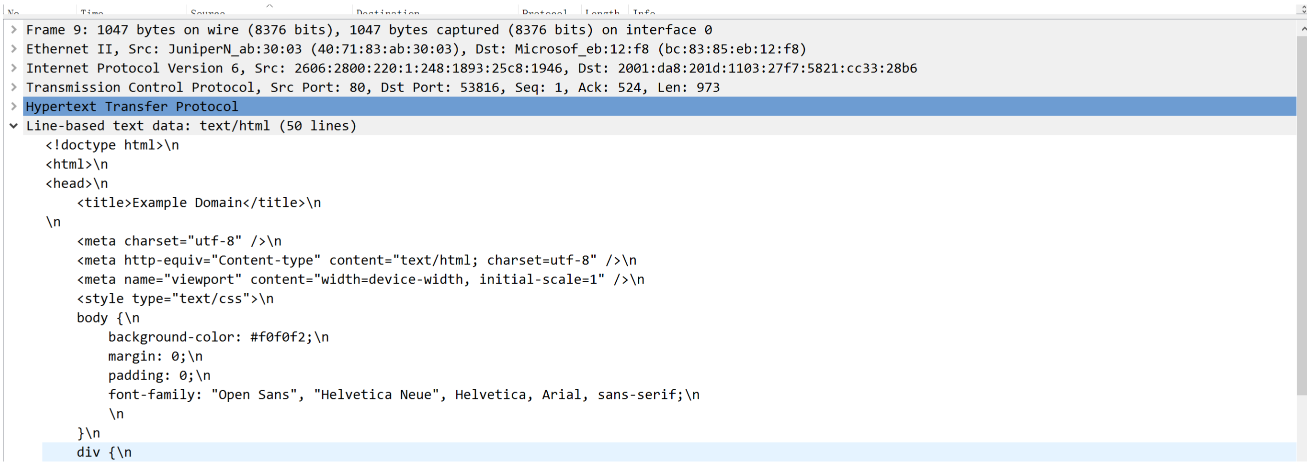
The HTTP response packet has Line-based test data: text/html, it is the same as the website source code displayed on the browser



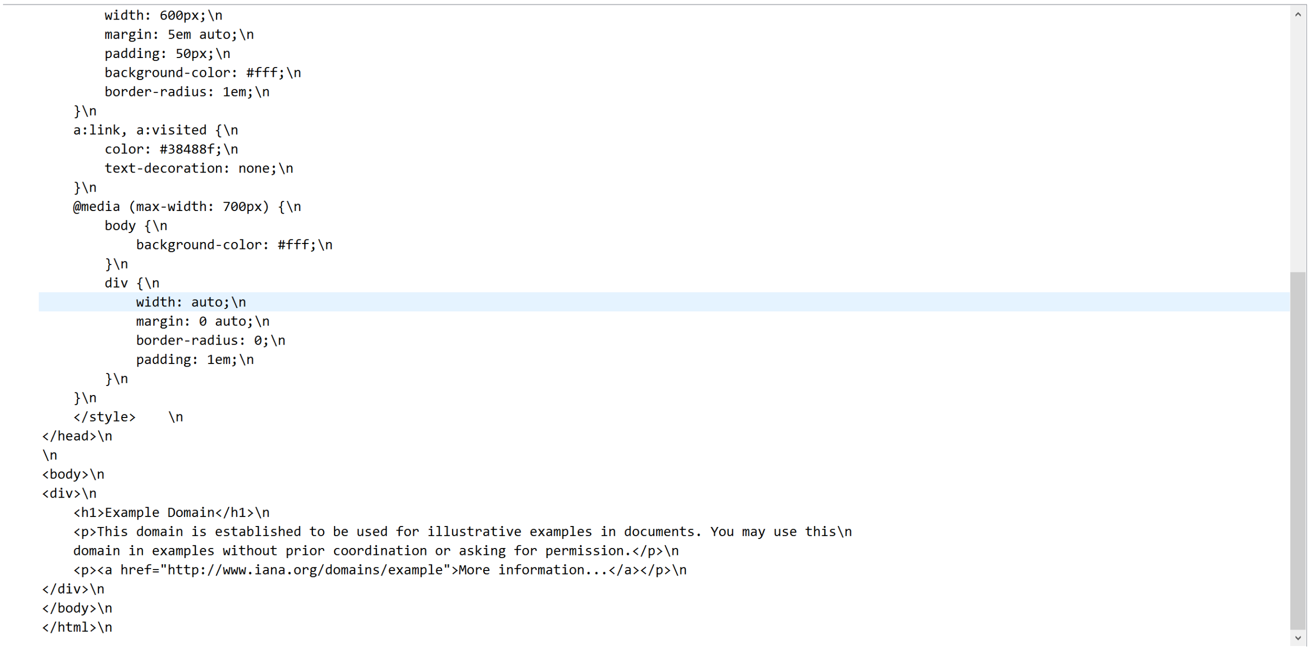
## Example Domain

This domain is established to be used for illustrative examples in documents. You may use this domain in examples without prior coordination or asking for permission.

More information...



```
> Frame 9: 1047 bytes on wire (8376 bits), 1047 bytes captured (8376 bits) on interface 0
> Ethernet II, Src: JuniperN_ab:30:03 (40:71:83:ab:30:03), Dst: Microsof_eb:12:f8 (bc:83:85:eb:12:f8)
> Internet Protocol Version 6, Src: 2606:2800:220:1:248:1893:25c8:1946, Dst: 2001:da8:201d:1103:27f7:5821:cc33:28b6
> Transmission Control Protocol, Src Port: 80, Dst Port: 53816, Seq: 1, Ack: 524, Len: 973
> Hypertext Transfer Protocol
v Line-based text data: text/html (50 lines)
    <!doctype html>\n
    <html>\n
    <head>\n
        <title>Example Domain</title>\n
    \n
        <meta charset="utf-8" />\n
        <meta http-equiv="Content-type" content="text/html; charset=utf-8" />\n
        <meta name="viewport" content="width=device-width, initial-scale=1" />\n
        <style type="text/css">\n
        body {\n
            background-color: #f0f0f2;\n
            margin: 0;\n
            padding: 0;\n
            font-family: "Open Sans", "Helvetica Neue", Helvetica, Arial, sans-serif;\n
            \n
        }\n
        div {\n
```



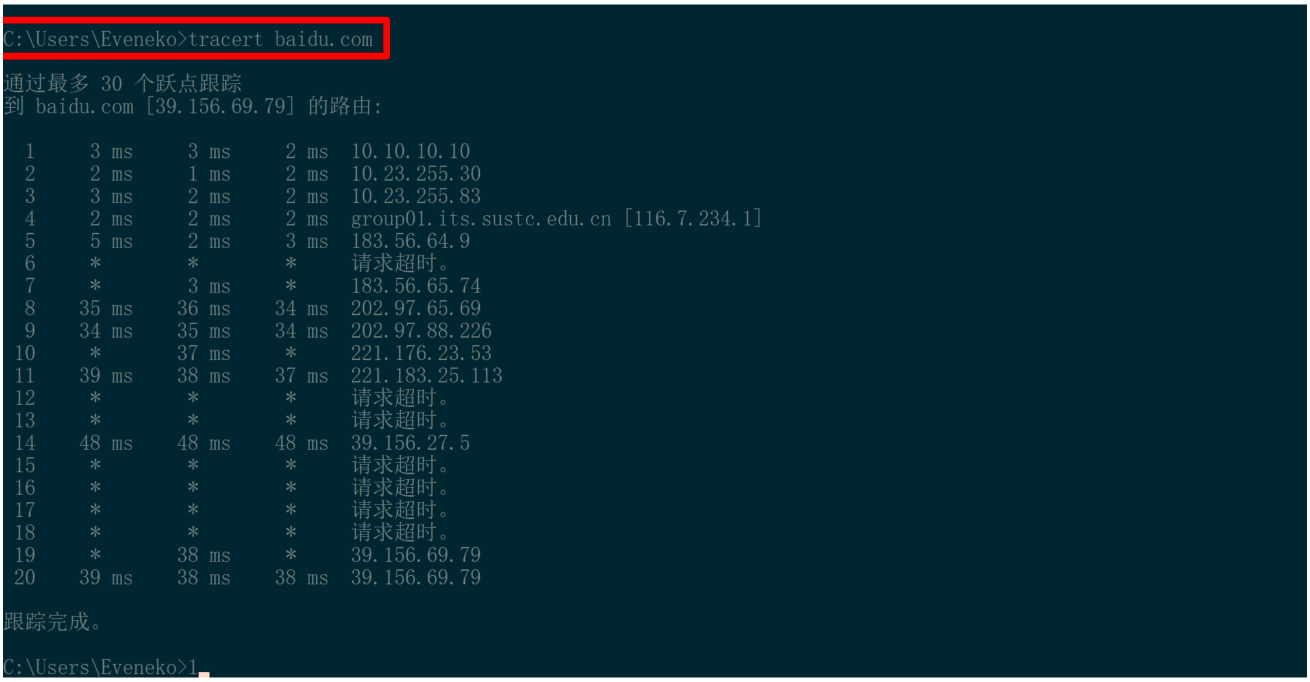
```
        width: 600px;\n
        margin: 5em auto;\n
        padding: 50px;\n
        background-color: #fff;\n
        border-radius: 1em;\n
    }\n
    a:link, a:visited {\n
        color: #38488f;\n
        text-decoration: none;\n
    }\n
    @media (max-width: 700px) {\n
        body {\n
            background-color: #fff;\n
        }\n
        div {\n
            width: auto;\n
            margin: 0 auto;\n
            border-radius: 0;\n
            padding: 1em;\n
        }\n
    }\n
    </style>    \n
</head>\n
\n
<body>\n
<div>\n
    <h1>Example Domain</h1>\n
    <p>This domain is established to be used for illustrative examples in documents. You may use this\n
    domain in examples without prior coordination or asking for permission.</p>\n
    <p><a href="http://www.iana.org/domains/example">More information...</a></p>\n
</div>\n
</body>\n
</html>\n
```

## Assignment2.3

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

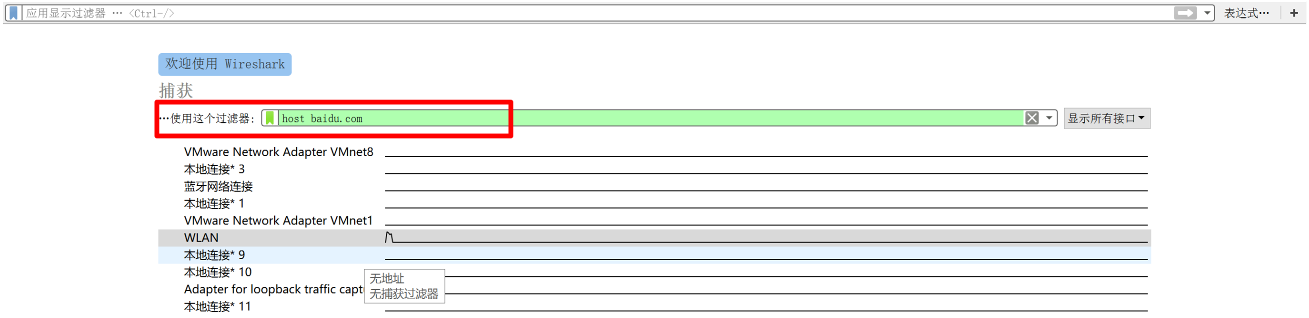
1. Using a proper capture filter/display filter to capture/display a tracert traffic. And start tracert baidu.com

> tracert baidu.com

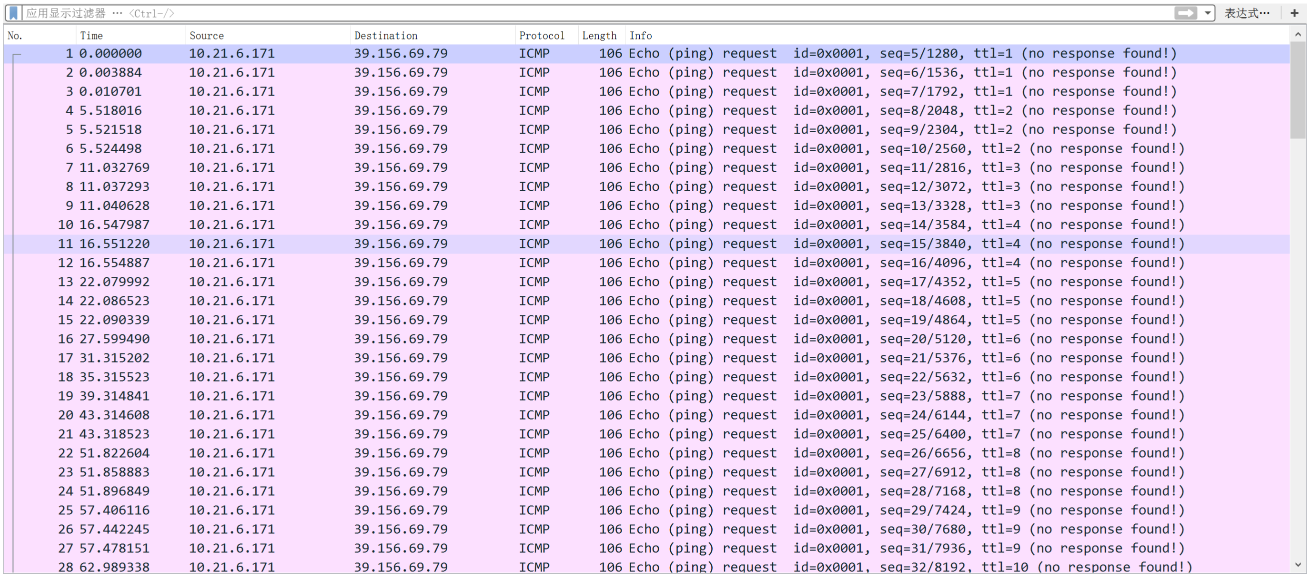


```
C:\Users\Eveneko>tracert baidu.com

通过最多 30 个跃点跟踪
到 baidu.com [39.156.69.79] 的路由:

  1     3 ms     3 ms     2 ms  10.10.10.10
  2     2 ms     1 ms     2 ms  10.23.255.30
  3     3 ms     2 ms     2 ms  10.23.255.83
  4     2 ms     2 ms     2 ms  group01.its.sustc.edu.cn [116.7.234.1]
  5     5 ms     2 ms     3 ms  183.56.64.9
  6     *        *        *     请求超时。
  7     *        3 ms     *     183.56.65.74
  8    35 ms    36 ms    34 ms  202.97.65.69
  9    34 ms    35 ms    34 ms  202.97.88.226
 10     *       37 ms     *     221.176.23.53
 11    39 ms    38 ms    37 ms  221.183.25.113
 12     *        *        *     请求超时。
 13     *        *        *     请求超时。
 14    48 ms    48 ms    48 ms  39.156.27.5
 15     *        *        *     请求超时。
 16     *        *        *     请求超时。
 17     *        *        *     请求超时。
 18     *        *        *     请求超时。
 19     *       38 ms     *     39.156.69.79
 20    39 ms    38 ms    38 ms  39.156.69.79

跟踪完成。

C:\Users\Eveneko>1
```

capture filter: host baidu.com

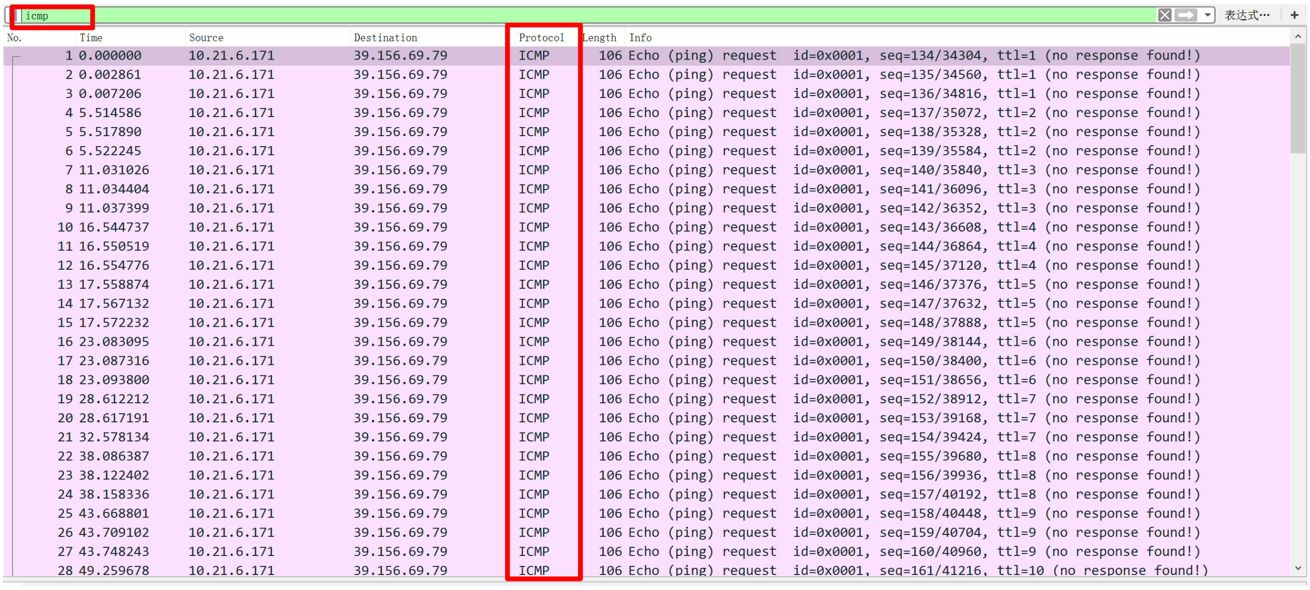


…使用这个过滤器: host baidu.com



```
No.  Time        Source       Destination   Protocol Length Info
   1 0.000000    10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=5/1280, ttl=1 (no response found!)
   2 0.003884    10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=6/1536, ttl=1 (no response found!)
   3 0.010701    10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=7/1792, ttl=1 (no response found!)
   4 5.518016    10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=8/2048, ttl=2 (no response found!)
   5 5.521518    10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=9/2304, ttl=2 (no response found!)
   6 5.524498    10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=10/2560, ttl=2 (no response found!)
   7 11.032769   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=11/2816, ttl=3 (no response found!)
   8 11.037293   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=12/3072, ttl=3 (no response found!)
   9 11.040628   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=13/3328, ttl=3 (no response found!)
  10 16.547987   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=14/3584, ttl=4 (no response found!)
  11 16.551220   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=15/3840, ttl=4 (no response found!)
  12 16.554887   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=16/4096, ttl=4 (no response found!)
  13 22.079992   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=17/4352, ttl=5 (no response found!)
  14 22.086523   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=18/4608, ttl=5 (no response found!)
  15 22.090339   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=19/4864, ttl=5 (no response found!)
  16 27.599490   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=20/5120, ttl=6 (no response found!)
  17 31.315202   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=21/5376, ttl=6 (no response found!)
  18 35.315523   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=22/5632, ttl=6 (no response found!)
  19 39.314841   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=23/5888, ttl=7 (no response found!)
  20 43.314608   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=24/6144, ttl=7 (no response found!)
  21 43.318523   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=25/6400, ttl=7 (no response found!)
  22 51.822604   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=26/6656, ttl=8 (no response found!)
  23 51.858883   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=27/6912, ttl=8 (no response found!)
  24 51.896849   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=28/7168, ttl=8 (no response found!)
  25 57.406116   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=29/7424, ttl=9 (no response found!)
  26 57.442245   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=30/7680, ttl=9 (no response found!)
  27 57.478151   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=31/7936, ttl=9 (no response found!)
  28 62.989338   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=32/8192, ttl=10 (no response found!)
```

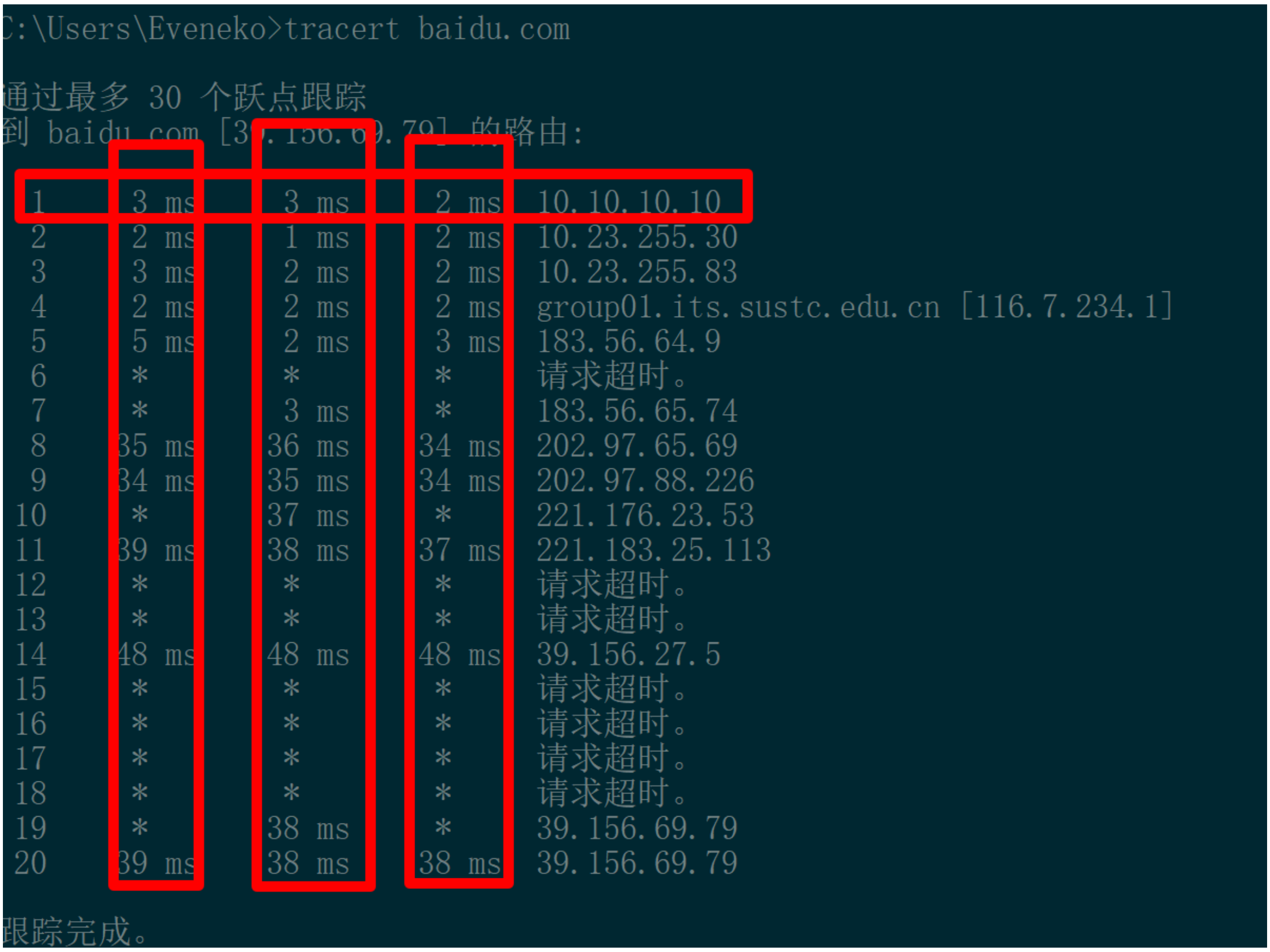
display filter: icmp



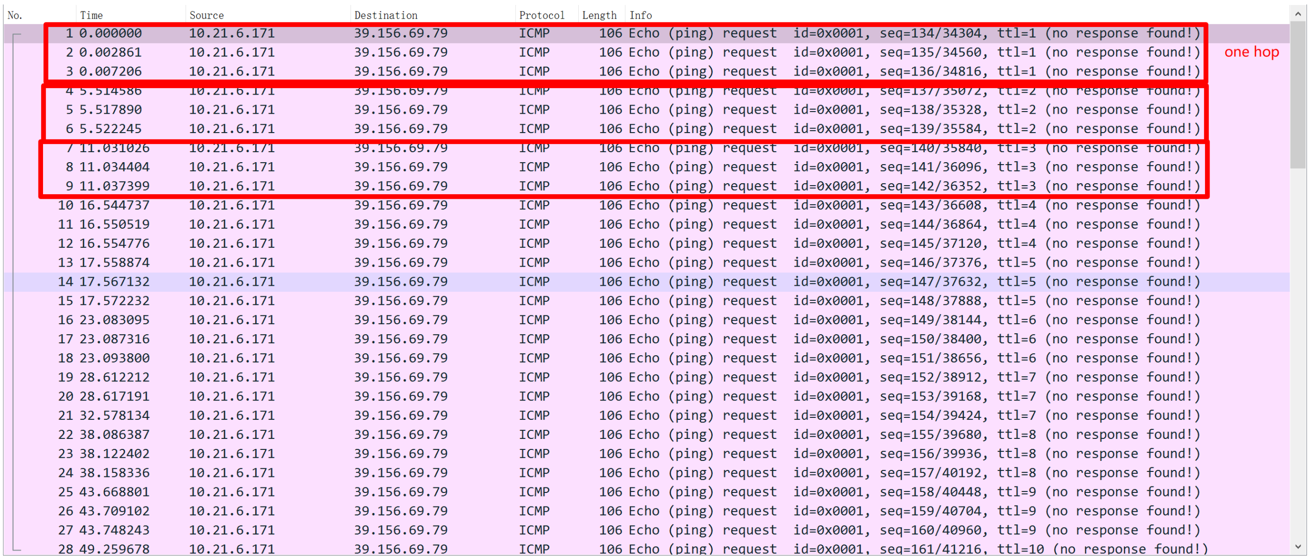
```
No.  Time       Source       Destination   Protocol Length Info
   1 0.000000   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=134/34304, ttl=1 (no response found!)
   2 0.002861   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=135/34560, ttl=1 (no response found!)
   3 0.007206   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=136/34816, ttl=1 (no response found!)
   4 5.514586   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=137/35072, ttl=2 (no response found!)
   5 5.517890   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=138/35328, ttl=2 (no response found!)
   6 5.522245   10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=139/35584, ttl=2 (no response found!)
   7 11.031026  10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=140/35840, ttl=3 (no response found!)
   8 11.034404  10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=141/36096, ttl=3 (no response found!)
   9 11.037399  10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=142/36352, ttl=3 (no response found!)
  10 16.544737  10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=143/36608, ttl=4 (no response found!)
  11 16.550519  10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=144/36864, ttl=4 (no response found!)
  12 16.554776  10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=145/37120, ttl=4 (no response found!)
  13 17.558874  10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=146/37376, ttl=5 (no response found!)
  14 17.567132  10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=147/37632, ttl=5 (no response found!)
  15 17.572232  10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=148/37888, ttl=5 (no response found!)
  16 23.083095  10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=149/38144, ttl=6 (no response found!)
  17 23.087316  10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=150/38400, ttl=6 (no response found!)
  18 23.093800  10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=151/38656, ttl=6 (no response found!)
  19 28.612212  10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=152/38912, ttl=7 (no response found!)
  20 28.617191  10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=153/39168, ttl=7 (no response found!)
  21 32.578134  10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=154/39424, ttl=7 (no response found!)
  22 38.086387  10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=155/39680, ttl=8 (no response found!)
  23 38.122402  10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=156/39936, ttl=8 (no response found!)
  24 38.158336  10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=157/40192, ttl=8 (no response found!)
  25 43.668801  10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=158/40448, ttl=9 (no response found!)
  26 43.709102  10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=159/40704, ttl=9 (no response found!)
  27 43.748243  10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=160/40960, ttl=9 (no response found!)
  28 49.259678  10.21.6.171  39.156.69.79  ICMP     106 Echo (ping) request  id=0x0001, seq=161/41216, ttl=10 (no response found!)
```

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

There 3 packets did tracert send for each hop.



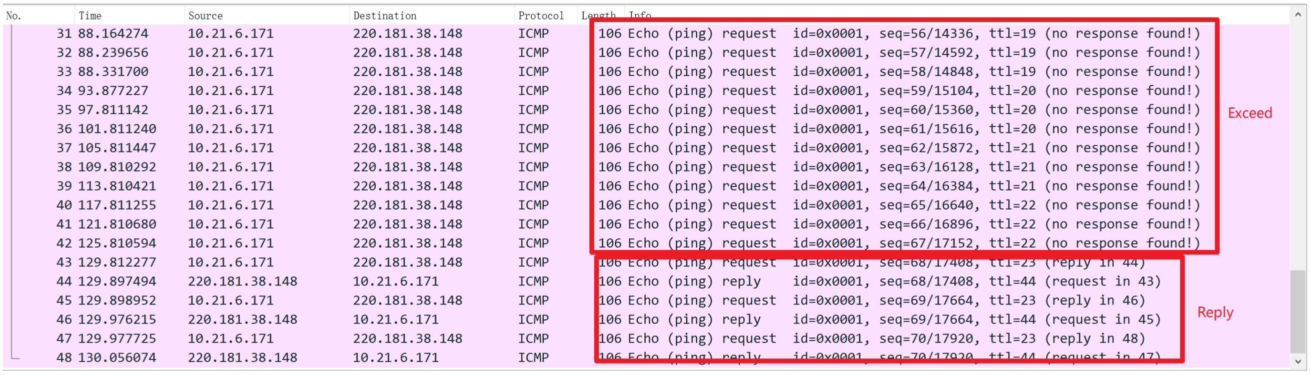
```
C:\Users\Eveneko>tracert baidu.com

通过最多 30 个跃点跟踪
到 baidu.com [39.156.69.79] 的路由:

  1     3 ms     3 ms     2 ms  10.10.10.10
  2     2 ms     1 ms     2 ms  10.23.255.30
  3     3 ms     2 ms     2 ms  10.23.255.83
  4     2 ms     2 ms     2 ms  group01.its.sustc.edu.cn [116.7.234.1]
  5     5 ms     2 ms     3 ms  183.56.64.9
  6     *        *        *     请求超时。
  7     *        3 ms     *     183.56.65.74
  8    35 ms    36 ms    34 ms  202.97.65.69
  9    34 ms    35 ms    34 ms  202.97.88.226
 10     *       37 ms     *     221.176.23.53
 11    39 ms    38 ms    37 ms  221.183.25.113
 12     *        *        *     请求超时。
 13     *        *        *     请求超时。
 14    48 ms    48 ms    48 ms  39.156.27.5
 15     *        *        *     请求超时。
 16     *        *        *     请求超时。
 17     *        *        *     请求超时。
 18     *        *        *     请求超时。
 19     *       38 ms     *     39.156.69.79
 20    39 ms    38 ms    38 ms  39.156.69.79

跟踪完成。
```



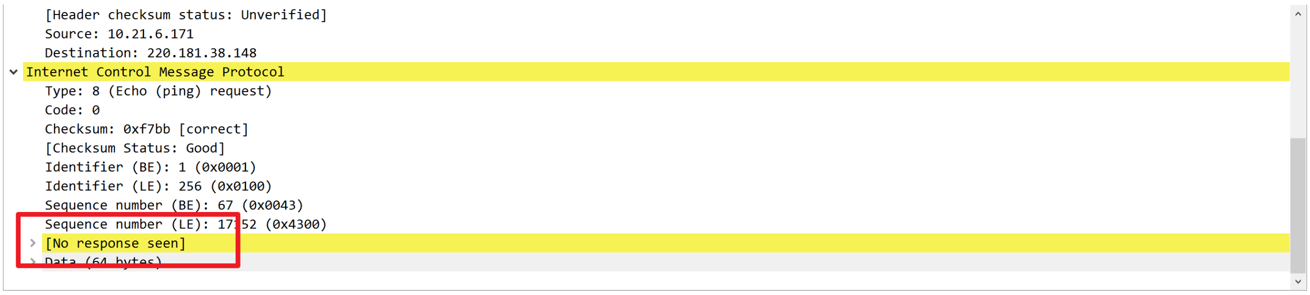
```
No.     Time        Source          Destination     Protocol  Length  Info
  1 0.000000    10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=134/34304, ttl=1 (no response found!)
  2 0.002861    10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=135/34560, ttl=1 (no response found!)
  3 0.007206    10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=136/34816, ttl=1 (no response found!)
  4 5.514586    10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=137/35072, ttl=2 (no response found!)
  5 5.517890    10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=138/35328, ttl=2 (no response found!)
  6 5.522245    10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=139/35584, ttl=2 (no response found!)
  7 11.031026   10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=140/35840, ttl=3 (no response found!)
  8 11.034404   10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=141/36096, ttl=3 (no response found!)
  9 11.037399   10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=142/36352, ttl=3 (no response found!)
 10 16.544737   10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=143/36608, ttl=4 (no response found!)
 11 16.550519   10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=144/36864, ttl=4 (no response found!)
 12 16.554776   10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=145/37120, ttl=4 (no response found!)
 13 17.558874   10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=146/37376, ttl=5 (no response found!)
 14 17.567132   10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=147/37632, ttl=5 (no response found!)
 15 17.572232   10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=148/37888, ttl=5 (no response found!)
 16 23.083095   10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=149/38144, ttl=6 (no response found!)
 17 23.087316   10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=150/38400, ttl=6 (no response found!)
 18 23.093800   10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=151/38656, ttl=6 (no response found!)
 19 28.612212   10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=152/38912, ttl=7 (no response found!)
 20 28.617191   10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=153/39168, ttl=7 (no response found!)
 21 32.578134   10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=154/39424, ttl=7 (no response found!)
 22 38.086387   10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=155/39680, ttl=8 (no response found!)
 23 38.122402   10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=156/39936, ttl=8 (no response found!)
 24 38.158336   10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=157/40192, ttl=8 (no response found!)
 25 43.668801   10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=158/40448, ttl=9 (no response found!)
 26 43.709102   10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=159/40704, ttl=9 (no response found!)
 27 43.748243   10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=160/40960, ttl=9 (no response found!)
 28 49.259678   10.21.6.171     39.156.69.79    ICMP      106 Echo (ping) request  id=0x0001, seq=161/41216, ttl=10 (no response found!)
```

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

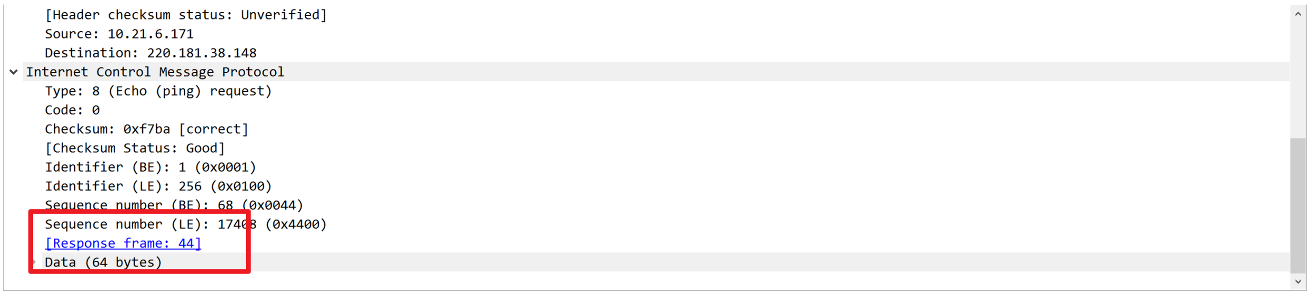
There are 2 kinds of response. They are **exceed** and **reply**.



```
No.     Time         Source          Destination      Protocol  Length  Info
 31 88.164274    10.21.6.171     220.181.38.148   ICMP      106 Echo (ping) request  id=0x0001, seq=56/14336, ttl=19 (no response found!)
 32 88.239656    10.21.6.171     220.181.38.148   ICMP      106 Echo (ping) request  id=0x0001, seq=57/14592, ttl=19 (no response found!)
 33 88.331700    10.21.6.171     220.181.38.148   ICMP      106 Echo (ping) request  id=0x0001, seq=58/14848, ttl=19 (no response found!)
 34 93.877227    10.21.6.171     220.181.38.148   ICMP      106 Echo (ping) request  id=0x0001, seq=59/15104, ttl=20 (no response found!)
 35 97.811142    10.21.6.171     220.181.38.148   ICMP      106 Echo (ping) request  id=0x0001, seq=60/15360, ttl=20 (no response found!)
 36 101.811240   10.21.6.171     220.181.38.148   ICMP      106 Echo (ping) request  id=0x0001, seq=61/15616, ttl=20 (no response found!)
 37 105.811447   10.21.6.171     220.181.38.148   ICMP      106 Echo (ping) request  id=0x0001, seq=62/15872, ttl=21 (no response found!)
 38 109.810292   10.21.6.171     220.181.38.148   ICMP      106 Echo (ping) request  id=0x0001, seq=63/16128, ttl=21 (no response found!)
 39 113.810421   10.21.6.171     220.181.38.148   ICMP      106 Echo (ping) request  id=0x0001, seq=64/16384, ttl=21 (no response found!)
 40 117.811255   10.21.6.171     220.181.38.148   ICMP      106 Echo (ping) request  id=0x0001, seq=65/16640, ttl=22 (no response found!)
 41 121.810680   10.21.6.171     220.181.38.148   ICMP      106 Echo (ping) request  id=0x0001, seq=66/16896, ttl=22 (no response found!)
 42 125.810594   10.21.6.171     220.181.38.148   ICMP      106 Echo (ping) request  id=0x0001, seq=67/17152, ttl=22 (no response found!)
 43 129.812277   10.21.6.171     220.181.38.148   ICMP      106 Echo (ping) request  id=0x0001, seq=68/17408, ttl=23 (reply in 44)
 44 129.897494   220.181.38.148  10.21.6.171      ICMP      106 Echo (ping) reply    id=0x0001, seq=68/17408, ttl=44 (request in 43)
 45 129.898952   10.21.6.171     220.181.38.148   ICMP      106 Echo (ping) request  id=0x0001, seq=69/17664, ttl=23 (reply in 46)
 46 129.976215   220.181.38.148  10.21.6.171      ICMP      106 Echo (ping) reply    id=0x0001, seq=69/17664, ttl=44 (request in 45)
 47 129.977725   10.21.6.171     220.181.38.148   ICMP      106 Echo (ping) request  id=0x0001, seq=70/17920, ttl=23 (reply in 48)
 48 130.056074   220.181.38.148  10.21.6.171      ICMP      106 Echo (ping) reply    id=0x0001, seq=70/17920, ttl=44 (request in 47)
```



```
    [Header checksum status: Unverified]
    Source: 10.21.6.171
    Destination: 220.181.38.148
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7bb [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 67 (0x0043)
    Sequence number (LE): 17152 (0x4300)
  > [No response seen]
  > Data (64 bytes)
```



```
    [Header checksum status: Unverified]
    Source: 10.21.6.171
    Destination: 220.181.38.148
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7ba [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 68 (0x0044)
    Sequence number (LE): 17408 (0x4400)
    [Response frame: 44]
  > Data (64 bytes)
```

The source IP address:

10.10.10.10

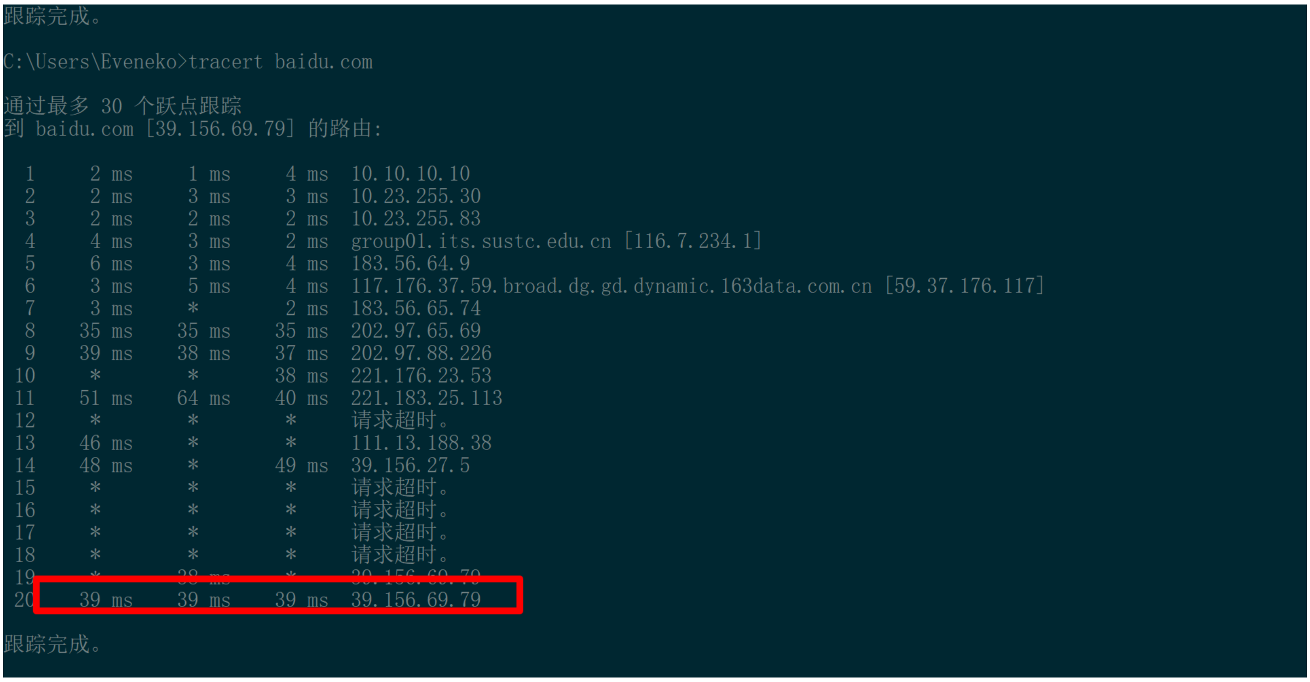
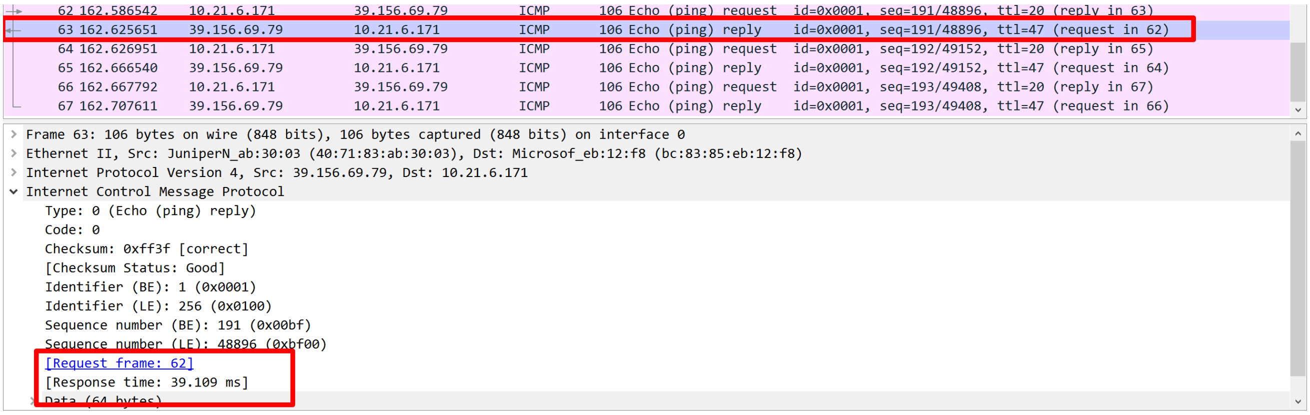
10.23.255.30

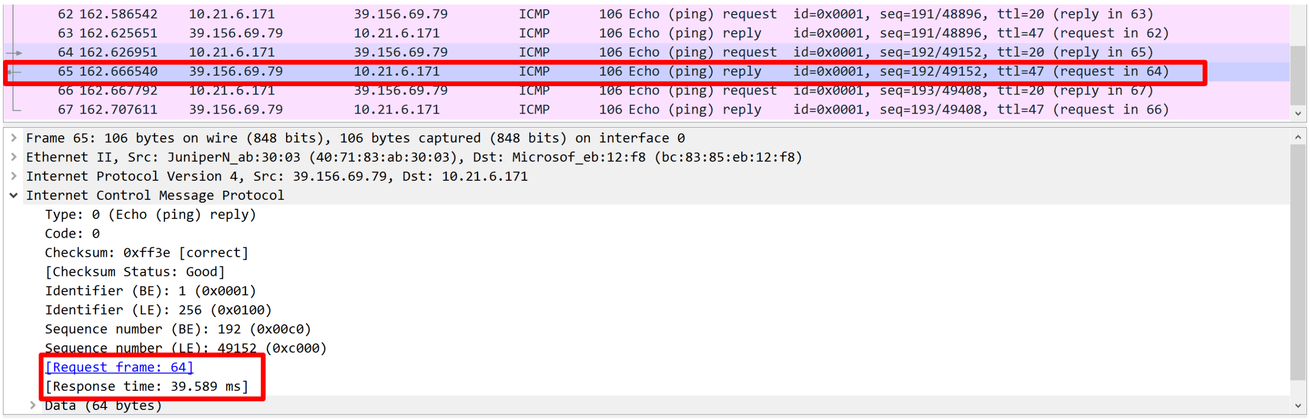
10.23.255.83

183.56.64.9

> 183.56.65.74
>
> 202.97.65.69
>
> 202.97.88.226
>
> 221.176.23.53
>
> 221.183.25.113
>
> 39.156.27.5
>
> 39.156.69.79

1. 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?

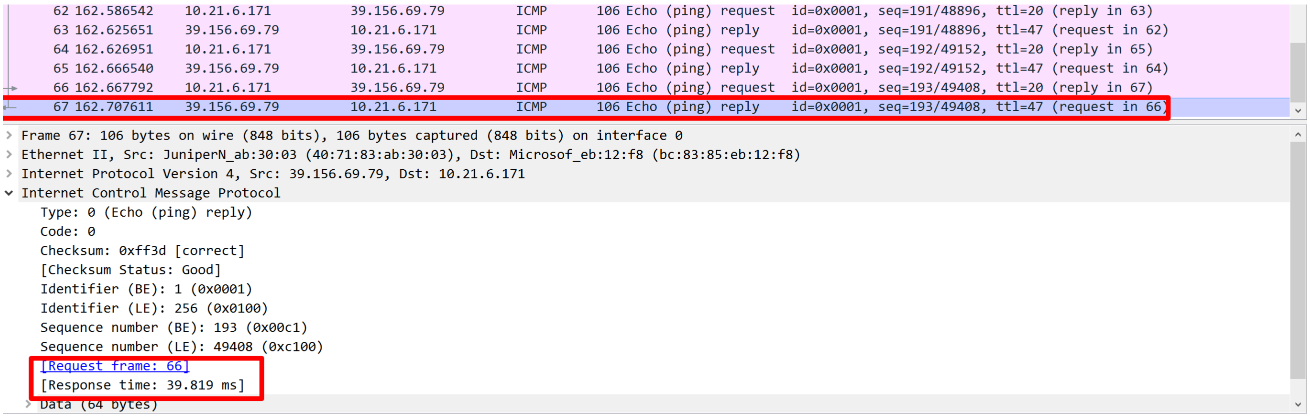
> ICMP sent from baidu.com[39.156.69.79]
>
> Tracert display: 39ms 39ms 39ms
>
> 
>
> ```
> 跟踪完成。
>
> C:\Users\Eveneko>tracert baidu.com
>
> 通过最多 30 个跃点跟踪
> 到 baidu.com [39.156.69.79] 的路由:
>
>   1     2 ms     1 ms     4 ms  10.10.10.10
>   2     2 ms     3 ms     3 ms  10.23.255.30
>   3     2 ms     2 ms     2 ms  10.23.255.83
>   4     4 ms     3 ms     2 ms  group01.its.sustc.edu.cn [116.7.234.1]
>   5     6 ms     3 ms     4 ms  183.56.64.9
>   6     3 ms     5 ms     4 ms  117.176.37.59.broad.dg.gd.dynamic.163data.com.cn [59.37.176.117]
>   7     3 ms     *        2 ms  183.56.65.74
>   8    35 ms    35 ms    35 ms  202.97.65.69
>   9    39 ms    38 ms    37 ms  202.97.88.226
>  10     *        *       38 ms  221.176.23.53
>  11    51 ms    64 ms    40 ms  221.183.25.113
>  12     *        *        *     请求超时。
>  13    46 ms     *        *     111.13.188.38
>  14    48 ms     *       49 ms  39.156.27.5
>  15     *        *        *     请求超时。
>  16     *        *        *     请求超时。
>  17     *        *        *     请求超时。
>  18     *        *        *     请求超时。
>  19     *       38 ms     *     39.156.69.79
>  20    39 ms    39 ms    39 ms  39.156.69.79
>
> 跟踪完成。
> ```
>
> Capture filter: 39.109ms
>
> 
>
> ```
> 62 162.586542   10.21.6.171     39.156.69.79    ICMP    106 Echo (ping) request  id=0x0001, seq=191/48896, ttl=20 (reply in 63)
> 63 162.625651   39.156.69.79    10.21.6.171     ICMP    106 Echo (ping) reply    id=0x0001, seq=191/48896, ttl=47 (request in 62)
> 64 162.626951   10.21.6.171     39.156.69.79    ICMP    106 Echo (ping) request  id=0x0001, seq=192/49152, ttl=20 (reply in 65)
> 65 162.666540   39.156.69.79    10.21.6.171     ICMP    106 Echo (ping) reply    id=0x0001, seq=192/49152, ttl=47 (request in 64)
> 66 162.667792   10.21.6.171     39.156.69.79    ICMP    106 Echo (ping) request  id=0x0001, seq=193/49408, ttl=20 (reply in 67)
> 67 162.707611   39.156.69.79    10.21.6.171     ICMP    106 Echo (ping) reply    id=0x0001, seq=193/49408, ttl=47 (request in 66)
>
> > Frame 63: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
> > Ethernet II, Src: JuniperN_ab:30:03 (40:71:83:ab:30:03), Dst: Microsof_eb:12:f8 (bc:83:85:eb:12:f8)
> > Internet Protocol Version 4, Src: 39.156.69.79, Dst: 10.21.6.171
> v Internet Control Message Protocol
>     Type: 0 (Echo (ping) reply)
>     Code: 0
>     Checksum: 0xff3f [correct]
>     [Checksum Status: Good]
>     Identifier (BE): 1 (0x0001)
>     Identifier (LE): 256 (0x0100)
>     Sequence number (BE): 191 (0x00bf)
>     Sequence number (LE): 48896 (0xbf00)
>     [Request frame: 62]
>     [Response time: 39.109 ms]
>   > Data (64 bytes)
> ```
>
> Capture filter: 39.589ms



```
62 162.586542   10.21.6.171      39.156.69.79     ICMP    106 Echo (ping) request  id=0x0001, seq=191/48896, ttl=20 (reply in 63)
63 162.625651   39.156.69.79     10.21.6.171      ICMP    106 Echo (ping) reply    id=0x0001, seq=191/48896, ttl=47 (request in 62)
64 162.626951   10.21.6.171      39.156.69.79     ICMP    106 Echo (ping) request  id=0x0001, seq=192/49152, ttl=20 (reply in 65)
65 162.666540   39.156.69.79     10.21.6.171      ICMP    106 Echo (ping) reply    id=0x0001, seq=192/49152, ttl=47 (request in 64)
66 162.667792   10.21.6.171      39.156.69.79     ICMP    106 Echo (ping) request  id=0x0001, seq=193/49408, ttl=20 (reply in 67)
67 162.707611   39.156.69.79     10.21.6.171      ICMP    106 Echo (ping) reply    id=0x0001, seq=193/49408, ttl=47 (request in 66)
```

```
> Frame 65: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
> Ethernet II, Src: JuniperN_ab:30:03 (40:71:83:ab:30:03), Dst: Microsof_eb:12:f8 (bc:83:85:eb:12:f8)
> Internet Protocol Version 4, Src: 39.156.69.79, Dst: 10.21.6.171
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xff3e [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 192 (0x00c0)
    Sequence number (LE): 49152 (0xc000)
    [Request frame: 64]
    [Response time: 39.589 ms]
  > Data (64 bytes)
```

Capture filter: 39.819ms



```
62 162.586542   10.21.6.171      39.156.69.79     ICMP    106 Echo (ping) request  id=0x0001, seq=191/48896, ttl=20 (reply in 63)
63 162.625651   39.156.69.79     10.21.6.171      ICMP    106 Echo (ping) reply    id=0x0001, seq=191/48896, ttl=47 (request in 62)
64 162.626951   10.21.6.171      39.156.69.79     ICMP    106 Echo (ping) request  id=0x0001, seq=192/49152, ttl=20 (reply in 65)
65 162.666540   39.156.69.79     10.21.6.171      ICMP    106 Echo (ping) reply    id=0x0001, seq=192/49152, ttl=47 (request in 64)
66 162.667792   10.21.6.171      39.156.69.79     ICMP    106 Echo (ping) request  id=0x0001, seq=193/49408, ttl=20 (reply in 67)
67 162.707611   39.156.69.79     10.21.6.171      ICMP    106 Echo (ping) reply    id=0x0001, seq=193/49408, ttl=47 (request in 66)
```

```
> Frame 67: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
> Ethernet II, Src: JuniperN_ab:30:03 (40:71:83:ab:30:03), Dst: Microsof_eb:12:f8 (bc:83:85:eb:12:f8)
> Internet Protocol Version 4, Src: 39.156.69.79, Dst: 10.21.6.171
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xff3d [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 193 (0x00c1)
    Sequence number (LE): 49408 (0xc100)
    [Request frame: 66]
    [Response time: 39.819 ms]
  > Data (64 bytes)
```

They are the same with tracert display.

4. **Conclusion and Experience：**

   1. For layers, we have:

   - application layer: supporting network applications
     - FTP, SMTP, HTTP
   - presentation layer: allow applications to interpret meaning of data, e.g., encryption, compression, machine-specific conventions
   - session layer: synchronization, checkpointing, recovery of data exchange
   - transport layer: process-process data transfer
     - TCP, UDP
   - network layer: routing of datagrams from source to destination
     - IP, routing protocols
   - link layer: data transfer between neighboring network elements
     - Ethernet, 802.111 (WiFi), PPP
   - physical layer: bits “on the wire”

   1. When we tracert baidu.com in different place and time, the result maybe different. Even the ip address, 220.181.38.148 and 39.156.69.79 are both baidu.com ip address.
   2. When we visit a website, we will request some information and get some response by packets, so that we can use wireshark to catch them.
   3. HTTP means HyperText Transfer Protocol. HTTP is the underlying protocol used by the World Wide Web and this protocol defines how messages are formatted and transmitted,

and what actions Web servers and browsers should take in response to various commands.

4. The Internet Control Message Protocol (ICMP) is a supporting protocol in the Internet protocol suite. It is used by network devices, including routers, to send error messages and operational information indicating success or failure when communicating with another IP address.