1901

631907060603

wireshark

(　　)

2020　　10　　16

1.
本部分按照数据链路层、网络层、传输层以及应用层进行分类，共有 10 个实验。需要使用协议分析软件 Wireshark 进行，请根据简介部分自行下载安装。
2.
3.

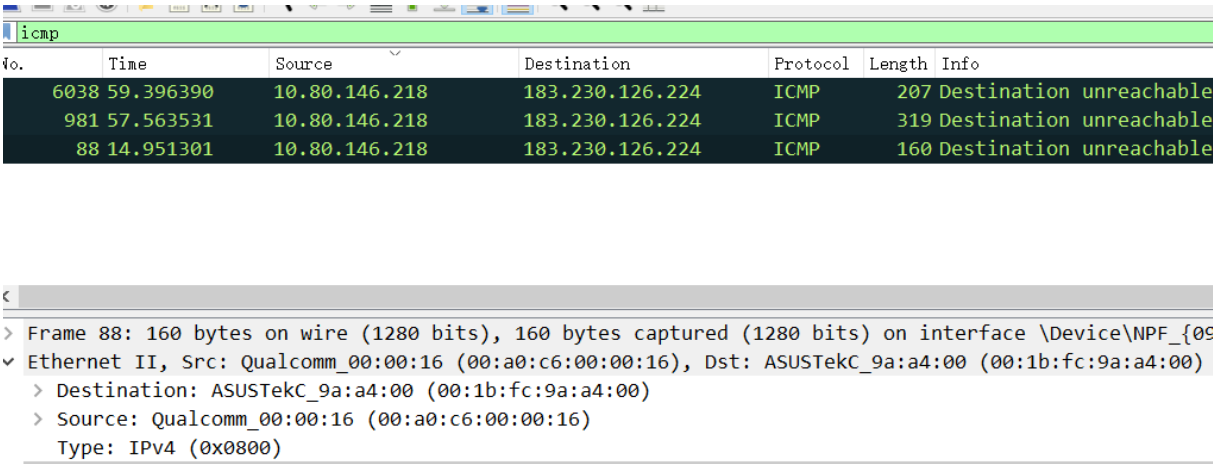
Wireshark

/
Wireshark

1 数据链路层

Ethernet

Wireshark Ethernet MAC MAC



```
icmp
No.   Time          Source          Destination      Protocol  Length Info
 6038 59.396390     10.80.146.218   183.230.126.224  ICMP      207 Destination unreachable
  981 57.563531     10.80.146.218   183.230.126.224  ICMP      319 Destination unreachable
   88 14.951301     10.80.146.218   183.230.126.224  ICMP      160 Destination unreachable

> Frame 88: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\NPF_{09
v Ethernet II, Src: Qualcomm_00:00:16 (00:a0:c6:00:00:16), Dst: ASUSTekC_9a:a4:00 (00:1b:fc:9a:a4:00)
  > Destination: ASUSTekC_9a:a4:00 (00:1b:fc:9a:a4:00)
  > Source: Qualcomm_00:00:16 (00:a0:c6:00:00:16)
    Type: IPv4 (0x0800)
```

减去前三个属性的字节剩下就是数据(字段)

Wireshark

/ **MAC**

ping Wireshark icmp
MAC MAC
MAC

mac

Ethernet II, Src: IntelCor_5e:40:89 (f4:d1:08:5e:40:89), Dst: IntelCor_77:72:d4 (38:00:25:77:72:d4)

Ethernet II, Src: IntelCor_77:72:d4 (**38:00:25:77:72:d4**), Dst: IntelCor_5e:40:89 (**f4:d1:08:5e:40:89**)

f4:d1:08:5e:40:89 wifi mac
38:00:25:77:72:d4 Wifi mac

ping qige.io Wireshark icmp
MAC MAC
MAC

Ethernet II, Src: Qualcomm_00:00:16 (00:a0:c6:00:00:16), Dst: ASUSTekC_9a:a4:00 (00:1b:fc:9a:a4:00)
Ethernet II, Src: ASUSTekC_9a:a4:00 (00:1b:fc:9a:a4:00), Dst: Qualcomm_00:00:16 (00:a0:c6:00:00:16)

(00:a0:c6:00:00:16)
(00:1b:fc:9a:a4:00) mac

ping www.cqjtu.edu.cn Wireshark
icmp MAC MAC
MAC

Ethernet II, Src: Qualcomm_00:00:16 (00:a0:c6:00:00:16), Dst: ASUSTekC_9a:a4:00 (00:1b:fc:9a:a4:00)
Ethernet II, Src: ASUSTekC_9a:a4:00 (00:1b:fc:9a:a4:00), Dst: Qualcomm_00:00:16 (00:a0:c6:00:00:16)
(00:a0:c6:00:00:16)
(00:1b:fc:9a:a4:00) mac

✎

MAC

MAC

( )

( )

,

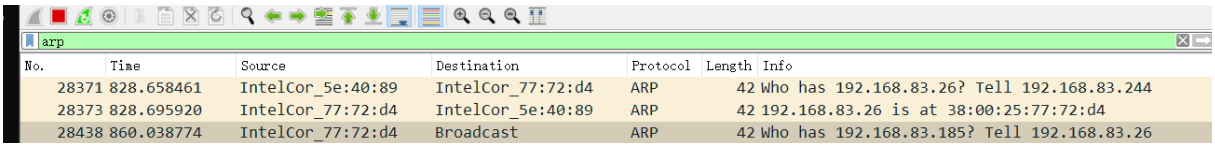
ARP

arp -d * arp

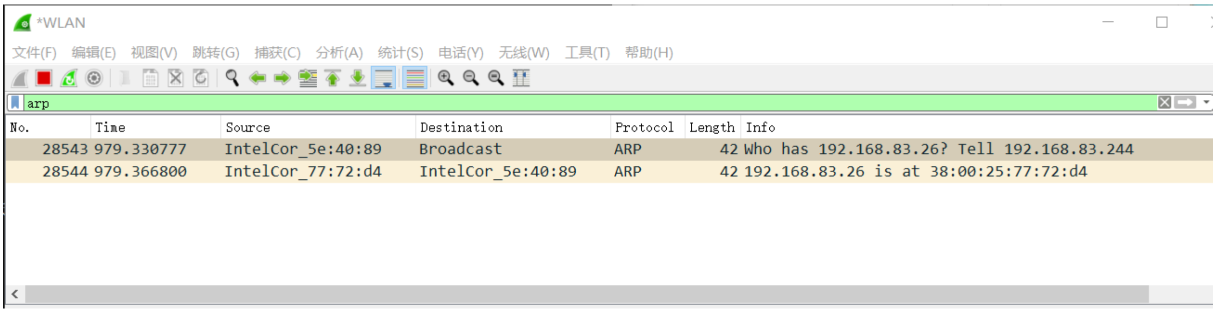
ping Wireshark arp

ARP MAC

MAC MAC



```
No.    Time        Source              Destination         Protocol Length Info
 28371 828.658461  IntelCor_5e:40:89   IntelCor_77:72:d4   ARP          42 Who has 192.168.83.26? Tell 192.168.83.244
 28373 828.695920  IntelCor_77:72:d4   IntelCor_5e:40:89   ARP          42 192.168.83.26 is at 38:00:25:77:72:d4
 28438 860.038774  IntelCor_77:72:d4   Broadcast           ARP          42 Who has 192.168.83.185? Tell 192.168.83.26
```



*WLAN
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)
arp

```
No.    Time        Source              Destination         Protocol Length Info
 28543 979.330777  IntelCor_5e:40:89   Broadcast           ARP          42 Who has 192.168.83.26? Tell 192.168.83.244
 28544 979.366800  IntelCor_77:72:d4   IntelCor_5e:40:89   ARP          42 192.168.83.26 is at 38:00:25:77:72:d4
```

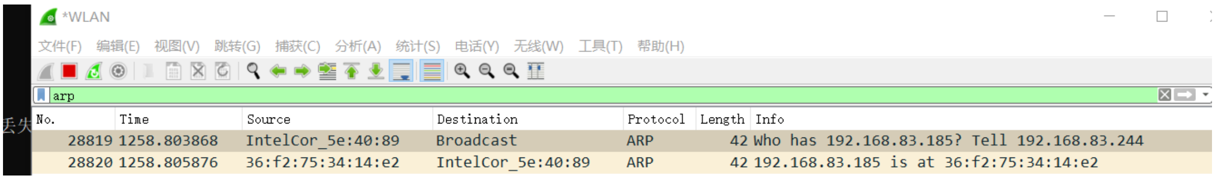
请求的目的地址为 Destination: Broadcast (ff:ff:ff:ff:ff:ff) 广播

回复的起始地址 Src: IntelCor_77:72:d4 (38:00:25:77:72:d4), 目的地址 Dst: IntelCor_5e:40:89 (f4:d1:08:5e:40:89)

arp -d * arp

ping qige.io Wireshark arp

ARP


*WLAN
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)
arp
丢失

```
No.    Time         Source              Destination         Protocol Length Info
 28819 1258.803868  IntelCor_5e:40:89   Broadcast           ARP         42 Who has 192.168.83.185? Tell 192.168.83.244
 28820 1258.805876  36:f2:75:34:14:e2   IntelCor_5e:40:89   ARP         42 192.168.83.185 is at 36:f2:75:34:14:e2
```

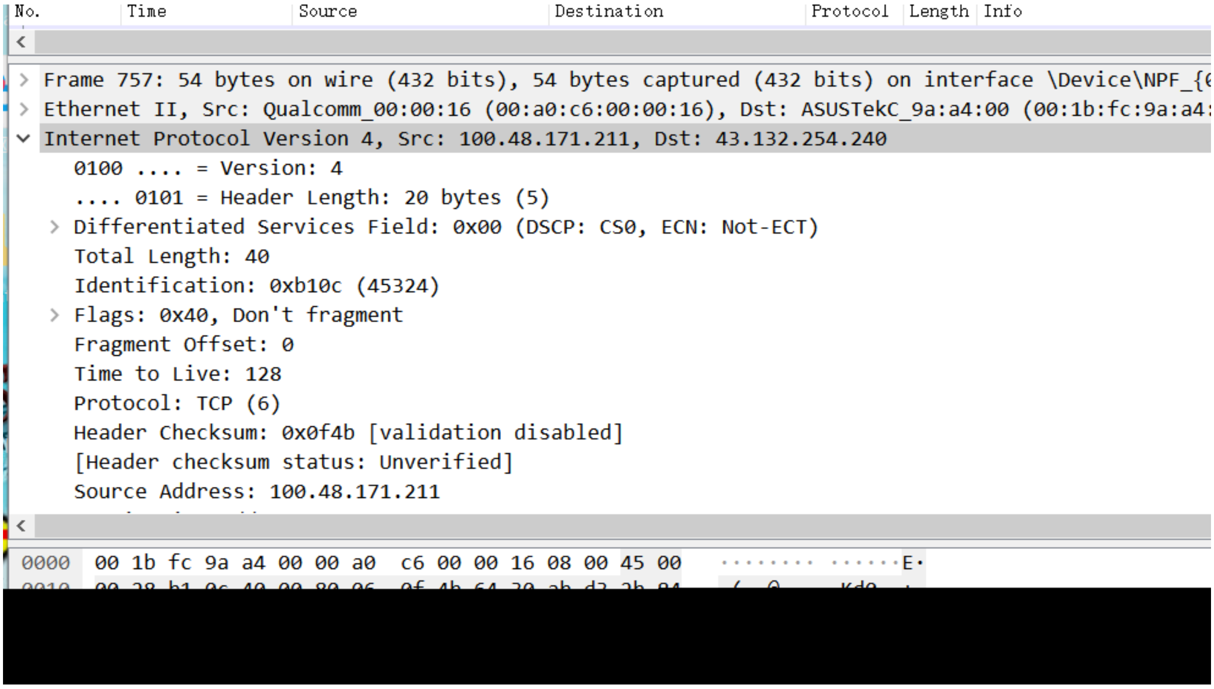
请求的目的地址为 Destination: Broadcast (ff:ff:ff:ff:ff:ff) 广播
回应的起始地址 Src: 36:f2:75:34:14:e2 (36:f2:75:34:14:e2),
目标地址:Dst: IntelCor_5e:40:89 (f4:d1:08:5e:40:89) (为网关 mac 地址)

ARP
IP ARP IP MAC
IP ARP MAC

IP ARP
IP
ARP ARP
Arp , ip ,
, ip ,

2

IP
Wireshark ip IP
TTL



```
> Frame 757: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{
> Ethernet II, Src: Qualcomm_00:00:16 (00:a0:c6:00:00:16), Dst: ASUSTekC_9a:a4:00 (00:1b:fc:9a:a4:
v Internet Protocol Version 4, Src: 100.48.171.211, Dst: 43.132.254.240
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0xb10c (45324)
  > Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0f4b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 100.48.171.211

0000  00 1b fc 9a a4 00 00 a0  c6 00 00 16 08 00 45 00   ········ ······E·
```

[redacted]

45(高 4 位为版本 低 4 位为头部长度)

00(差分服务字段)

00 28(总长度 这里为 40)

b1 0c(标识)

40(标志)

00(段落偏移)

80(ttl)

06(协议类型 tcp)

0f 4b (头校验和)

64 30 ab d3(目标地址)

2b 84 fe f0(源地址)

c7 d8 c9 3f d9 4d 92 f2 f0 c4 46 51 50 10 02 02 3e eb 00 00(内容)

+...

+...

IP IP

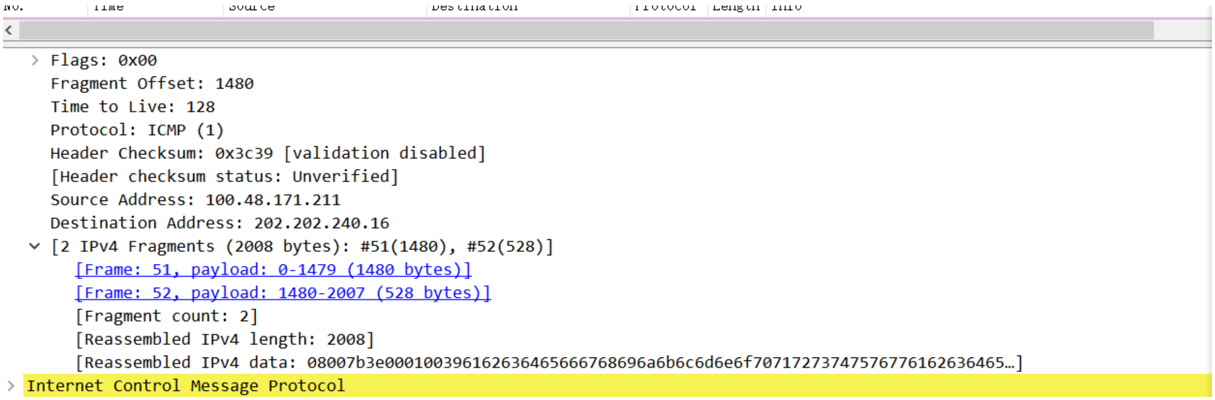
IP , ,

IP

IP 64K Ethernet IP

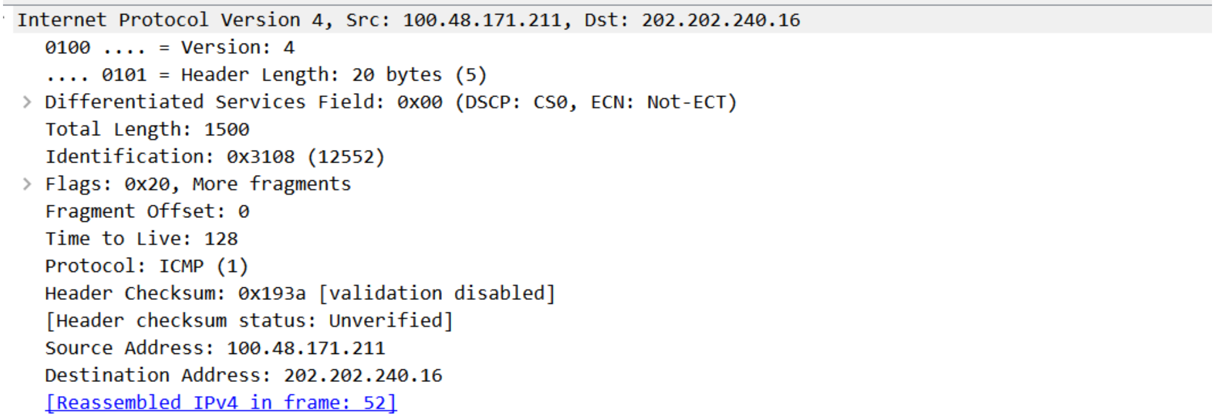
1500

ping 32 ping 202.202.240.16 -l 2000 Wireshark ip.addr == 202.202.240.16 IP



```
No.   Time   Source   Destination   Protocol  Length  Info
  > Flags: 0x00
    Fragment Offset: 1480
    Time to Live: 128
    Protocol: ICMP (1)
    Header Checksum: 0x3c39 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 100.48.171.211
    Destination Address: 202.202.240.16
  ∨ [2 IPv4 Fragments (2008 bytes): #51(1480), #52(528)]
      [Frame: 51, payload: 0-1479 (1480 bytes)]
      [Frame: 52, payload: 1480-2007 (528 bytes)]
      [Fragment count: 2]
      [Reassembled IPv4 length: 2008]
      [Reassembled IPv4 data: 08007b3e00010039616263646566676869 6a6b6c6d6e6f7071727374757677616263646 5…]
> Internet Control Message Protocol
```

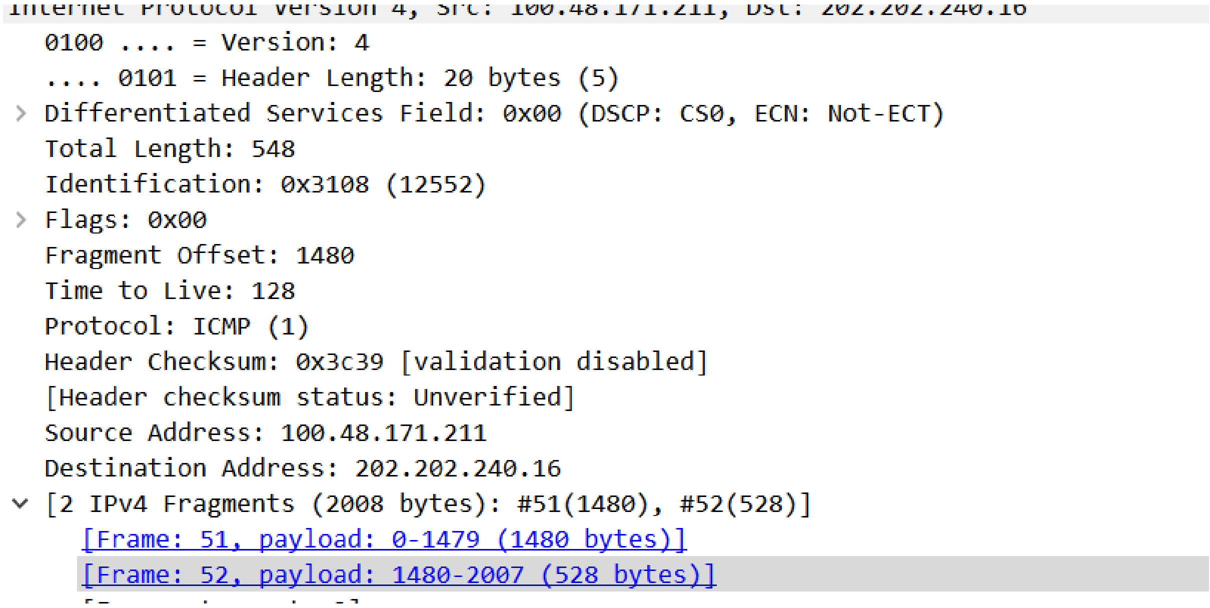
第一片 包大小为 1500



```
Internet Protocol Version 4, Src: 100.48.171.211, Dst: 202.202.240.16
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x3108 (12552)
  > Flags: 0x20, More fragments
    Fragment Offset: 0
    Time to Live: 128
    Protocol: ICMP (1)
    Header Checksum: 0x193a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 100.48.171.211
    Destination Address: 202.202.240.16
    [Reassembled IPv4 in frame: 52]
```

标识符为 0x3108 Total lenth 为 1500 fragment offset 为 0

第二片 包大小为 548



```
Internet Protocol Version 4, Src: 100.48.171.211, Dst: 202.202.240.16
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 548
    Identification: 0x3108 (12552)
  > Flags: 0x00
    Fragment Offset: 1480
    Time to Live: 128
    Protocol: ICMP (1)
    Header Checksum: 0x3c39 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 100.48.171.211
    Destination Address: 202.202.240.16
  ∨ [2 IPv4 Fragments (2008 bytes): #51(1480), #52(528)]
      [Frame: 51, payload: 0-1479 (1480 bytes)]
      [Frame: 52, payload: 1480-2007 (528 bytes)]
```

标识符为 0x3108　Total lenth 为 548　fragment offset 为 1480

IPv6 IPv6

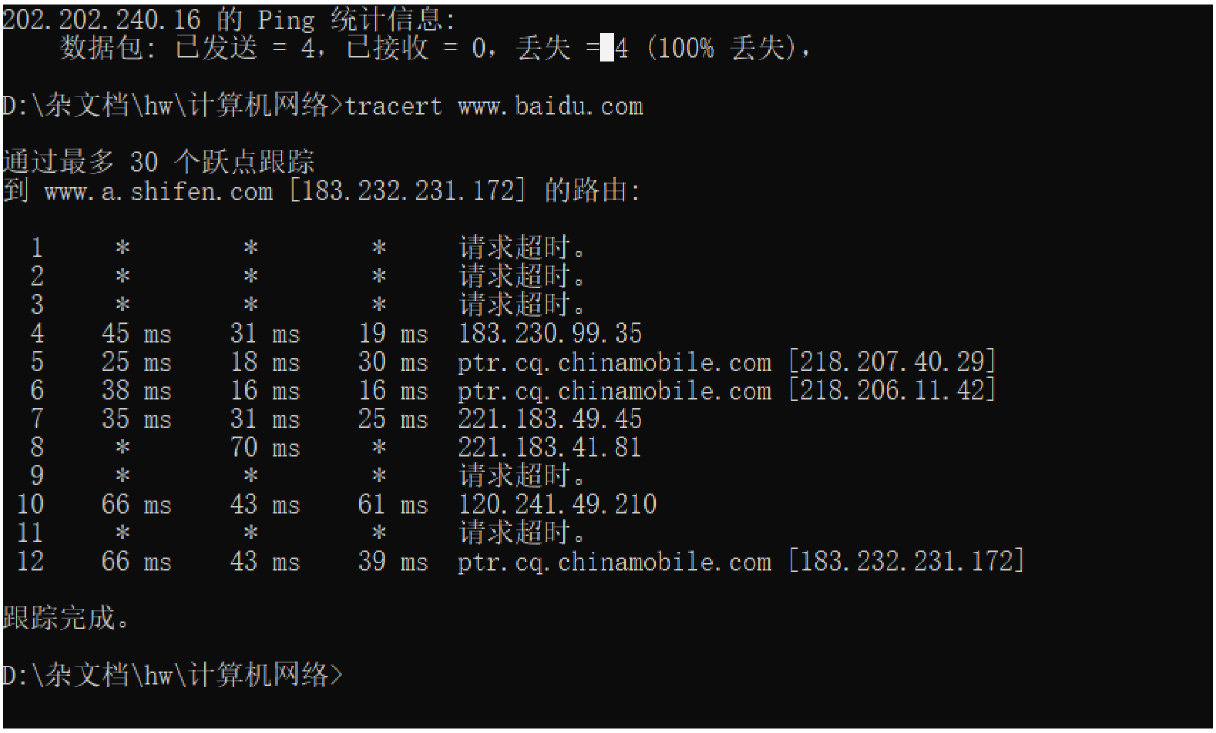
Ipv6

TTL

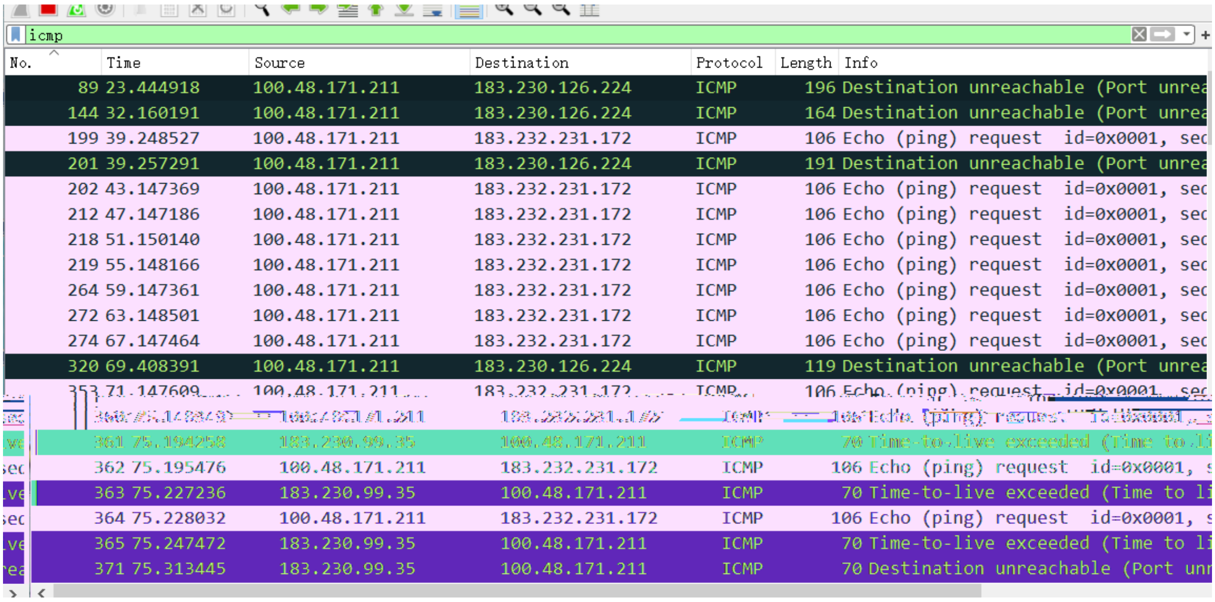
IP TTL Internet hops
64 128

tracert IP
TTL 1

tracert www.baidu.com Wireshark icmp
TTL



```
202.202.240.16 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 0，丢失 = 4 (100% 丢失)，

D:\杂文档\hw\计算机网络>tracert www.baidu.com

通过最多 30 个跃点跟踪
到 www.a.shifen.com [183.232.231.172] 的路由:

  1     *        *        *     请求超时。
  2     *        *        *     请求超时。
  3     *        *        *     请求超时。
  4    45 ms    31 ms    19 ms  183.230.99.35
  5    25 ms    18 ms    30 ms  ptr.cq.chinamobile.com [218.207.40.29]
  6    38 ms    16 ms    16 ms  ptr.cq.chinamobile.com [218.206.11.42]
  7    35 ms    31 ms    25 ms  221.183.49.45
  8     *       70 ms     *     221.183.41.81
  9     *        *        *     请求超时。
 10    66 ms    43 ms    61 ms  120.241.49.210
 11     *        *        *     请求超时。
 12    66 ms    43 ms    39 ms  ptr.cq.chinamobile.com [183.232.231.172]

跟踪完成。

D:\杂文档\hw\计算机网络>
```



```
icmp
No.  Time        Source           Destination       Protocol Length Info
  89 23.444918   100.48.171.211   183.230.126.224   ICMP     196 Destination unreachable (Port unrea
 144 32.160191   100.48.171.211   183.230.126.224   ICMP     164 Destination unreachable (Port unrea
 199 39.248527   100.48.171.211   183.232.231.172   ICMP     106 Echo (ping) request  id=0x0001, sec
 201 39.257291   100.48.171.211   183.230.126.224   ICMP     191 Destination unreachable (Port unrea
 202 43.147369   100.48.171.211   183.232.231.172   ICMP     106 Echo (ping) request  id=0x0001, sec
 212 47.147186   100.48.171.211   183.232.231.172   ICMP     106 Echo (ping) request  id=0x0001, sec
 218 51.150140   100.48.171.211   183.232.231.172   ICMP     106 Echo (ping) request  id=0x0001, sec
 219 55.148166   100.48.171.211   183.232.231.172   ICMP     106 Echo (ping) request  id=0x0001, sec
 264 59.147361   100.48.171.211   183.232.231.172   ICMP     106 Echo (ping) request  id=0x0001, sec
 272 63.148501   100.48.171.211   183.232.231.172   ICMP     106 Echo (ping) request  id=0x0001, sec
 274 67.147464   100.48.171.211   183.232.231.172   ICMP     106 Echo (ping) request  id=0x0001, sec
 320 69.408391   100.48.171.211   183.230.126.224   ICMP     119 Destination unreachable (Port unrea
 353 71.147609   100.48.171.211   183.232.231.172   ICMP     106 Echo (ping) request  id=0x0001, sec
 360 [illegible] 100.48.171.211   183.232.231.172   ICMP     106 Echo (ping) request  id=0x0001, s
 361 75.194258   183.230.99.35    100.48.171.211    ICMP      70 Time-to-live exceeded (Time to li
 362 75.195476   100.48.171.211   183.232.231.172   ICMP     106 Echo (ping) request  id=0x0001, s
 363 75.227236   183.230.99.35    100.48.171.211    ICMP      70 Time-to-live exceeded (Time to li
 364 75.228032   100.48.171.211   183.232.231.172   ICMP     106 Echo (ping) request  id=0x0001, s
 365 75.247472   183.230.99.35    100.48.171.211    ICMP      70 Time-to-live exceeded (Time to li
 371 75.313445   183.230.99.35    100.48.171.211    ICMP      70 Destination unreachable (Port unr
```

ttl

Tracet ttl n icmp (n)

RTB icmp IP IP

TTL 1 TTL 0 ICMP

Time Exceeded IP RTB

, ,

✎

IPv4 TTL Time To Live /

TTL 50

50

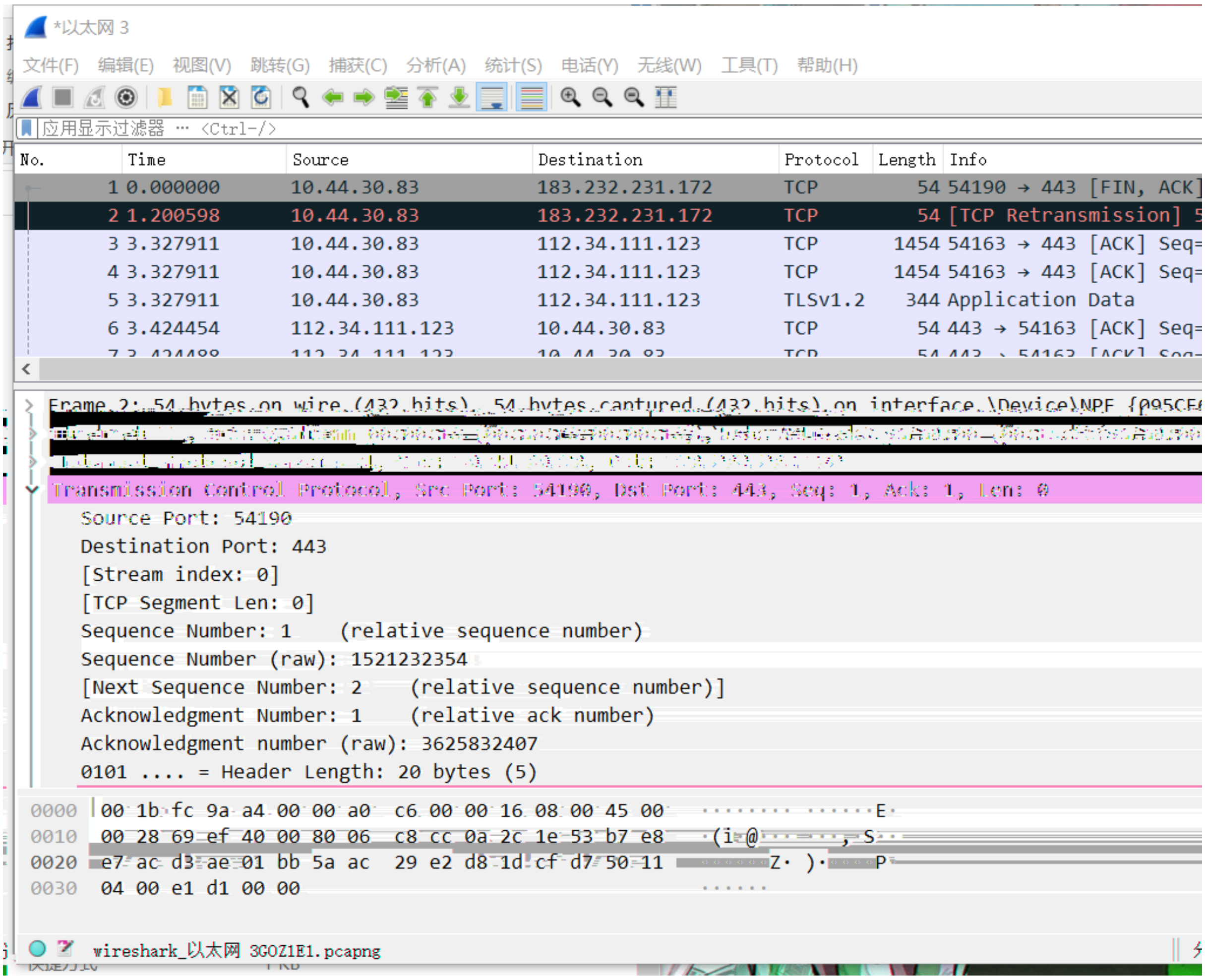
3

TCP UDP

Wireshark tcp TCP

Wireshark udp UDP

TCP:


*以太网 3
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)
应用显示过滤器 … <Ctrl-/>

```
No.   Time        Source           Destination      Protocol  Length Info
    1 0.000000    10.44.30.83      183.232.231.172  TCP           54 54190 → 443 [FIN, ACK]
    2 1.200598    10.44.30.83      183.232.231.172  TCP           54 [TCP Retransmission] 5
    3 3.327911    10.44.30.83      112.34.111.123   TCP         1454 54163 → 443 [ACK] Seq=
    4 3.327911    10.44.30.83      112.34.111.123   TCP         1454 54163 → 443 [ACK] Seq=
    5 3.327911    10.44.30.83      112.34.111.123   TLSv1.2      344 Application Data
    6 3.424454    112.34.111.123   10.44.30.83      TCP           54 443 → 54163 [ACK] Seq=
    7 3.424488    112.34.111.123   10.44.30.83      TCP           54 443 → 54163 [ACK] Seq=
```

```
> Frame 2: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{095CE
[redacted]
v Transmission Control Protocol, Src Port: 54190, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
    Source Port: 54190
    Destination Port: 443
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1521232354
    [Next Sequence Number: 2    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3625832407
    0101 .... = Header Length: 20 bytes (5)
```

```
0000  00 1b fc 9a a4 00 00 a0  c6 00 00 16 08 00 45 00   ········ ······E·
0010  00 28 69 ef 40 00 80 06  c8 cc 0a 2c 1e 53 b7 e8   ·(i·@··· ···,·S··
0020  e7 ac d3 ae 01 bb 5a ac  29 e2 d8 1d cf d7 50 11   ······Z· )·····P·
0030  04 00 e1 d1 00 00                                  ······
```

wireshark_以太网 3GOZ1E1.pcapng

Transmission Control Protocol, Src Port: 54190, Dst Port: 443, Seq: 1, Ack: 1, Len: 0

Source Port: 54190

Destination Port: 443

[Stream index: 0]

[TCP Segment Len: 0]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 1521232354

[Next Sequence Number: 2 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 3625832407

0101 .... = **Header Length:** 20 bytes (5)

Flags: 0x011 (FIN, ACK)

000. .... = Reserved: Not set

...0 .... = Nonce: Not set

.... 0... .... = Congestion Window Reduced (CWR): Not set

.... .0.. .... = ECN-Echo: Not set

.... ..0. .... = Urgent: Not set

....1 .... = Acknowledgment: Set

.... 0... = Push: Not set

.... .0.. = Reset: Not set

....0. = Syn: Not set

....1 = Fin: Set

[TCP Flags: · · · · · · · A · · · F]

Window: 1024

[Calculated window size: 1024]

[Window size scaling factor: -1 (unknown)]

Checksum: 0xe1d1 [unverified]

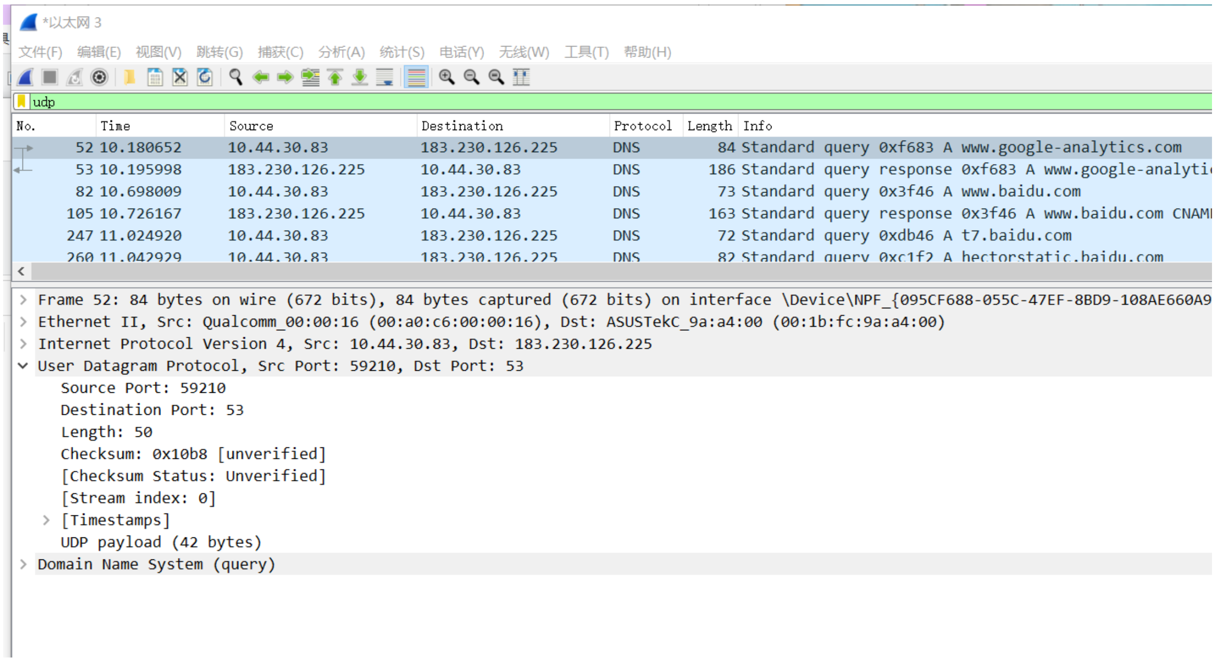
[Checksum Status: Unverified]

Urgent Pointer: 0

[SEQ/ACK analysis]

[Timestamps]

UDP:


*以太网 3
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)

```
udp
```

```
No.   Time       Source           Destination      Protocol Length Info
   52 10.180652  10.44.30.83      183.230.126.225  DNS          84 Standard query 0xf683 A www.google-analytics.com
   53 10.195998  183.230.126.225  10.44.30.83      DNS         186 Standard query response 0xf683 A www.google-analyti
   82 10.698009  10.44.30.83      183.230.126.225  DNS          73 Standard query 0x3f46 A www.baidu.com
  105 10.726167  183.230.126.225  10.44.30.83      DNS         163 Standard query response 0x3f46 A www.baidu.com CNAM
  247 11.024920  10.44.30.83      183.230.126.225  DNS          72 Standard query 0xdb46 A t7.baidu.com
  260 11.042929  10.44.30.83      183.230.126.225  DNS          82 Standard query 0xc1f2 A hectorstatic.baidu.com
```

```
> Frame 52: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{095CF688-055C-47EF-8BD9-108AE660A9
> Ethernet II, Src: Qualcomm_00:00:16 (00:a0:c6:00:00:16), Dst: ASUSTekC_9a:a4:00 (00:1b:fc:9a:a4:00)
> Internet Protocol Version 4, Src: 10.44.30.83, Dst: 183.230.126.225
v User Datagram Protocol, Src Port: 59210, Dst Port: 53
    Source Port: 59210
    Destination Port: 53
    Length: 50
    Checksum: 0x10b8 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (42 bytes)
> Domain Name System (query)
```

User Datagram Protocol, Src Port: 59210, Dst Port: 53

Source Port: 59210

Destination Port: 53

Length: 50

Checksum: 0x10b8 [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

[Timestamps]

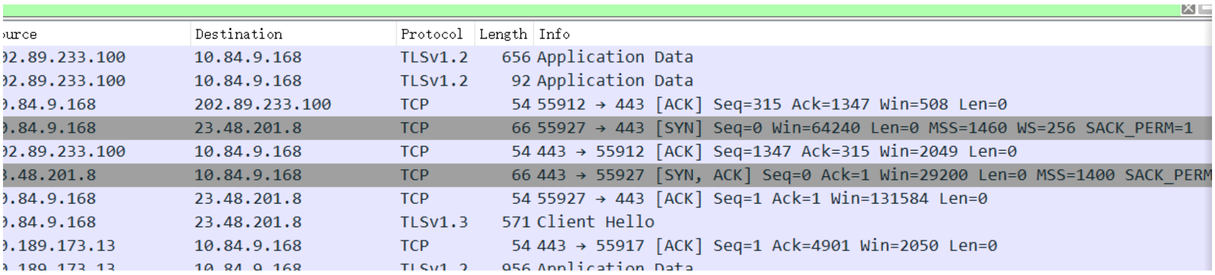
UDP payload (42 bytes)

Domain Name System (query)

UDP TCP

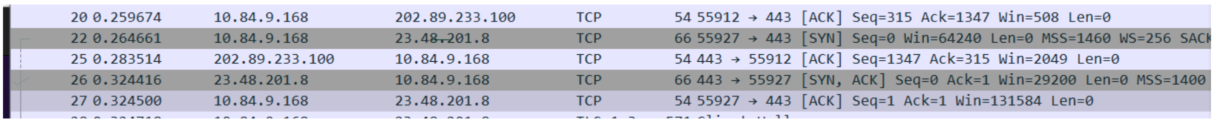
, ,
ip+

TCP
qige.io Wireshark tcp Follow
TCP Stream Wireshark



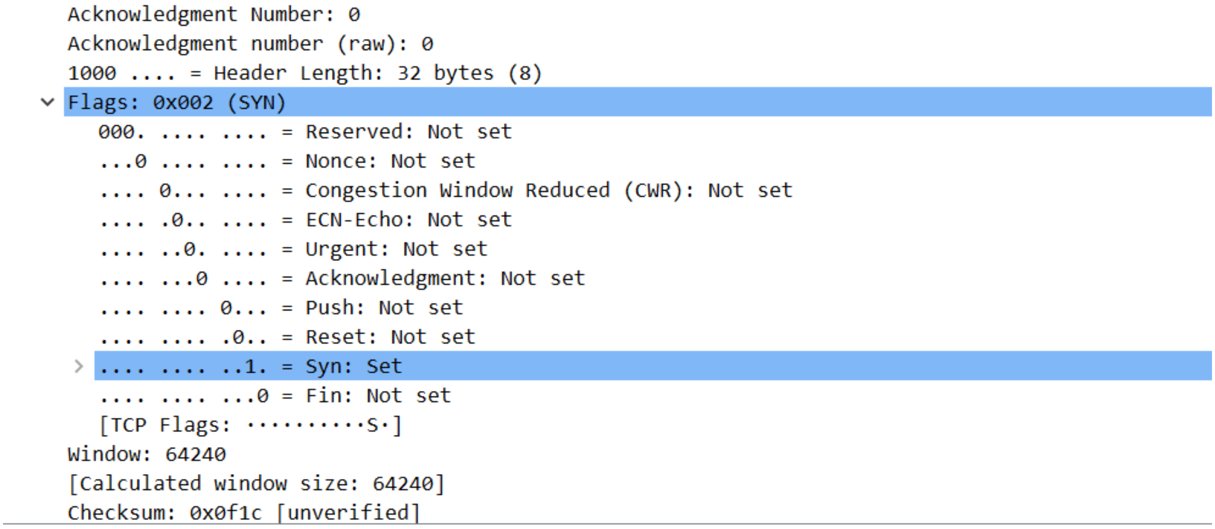
```
urce           Destination      Protocol Length Info
2.89.233.100   10.84.9.168      TLSv1.2    656 Application Data
2.89.233.100   10.84.9.168      TLSv1.2     92 Application Data
.84.9.168      202.89.233.100   TCP         54 55912 → 443 [ACK] Seq=315 Ack=1347 Win=508 Len=0
.84.9.168      23.48.201.8      TCP         66 55927 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2.89.233.100   10.84.9.168      TCP         54 443 → 55912 [ACK] Seq=1347 Ack=315 Win=2049 Len=0
.48.201.8      10.84.9.168      TCP         66 443 → 55927 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM
.84.9.168      23.48.201.8      TCP         54 55927 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
.84.9.168      23.48.201.8      TLSv1.3    571 Client Hello
.189.173.13    10.84.9.168      TCP         54 443 → 55917 [ACK] Seq=1 Ack=4901 Win=2050 Len=0
```

带阴影的三次 tcp 握手



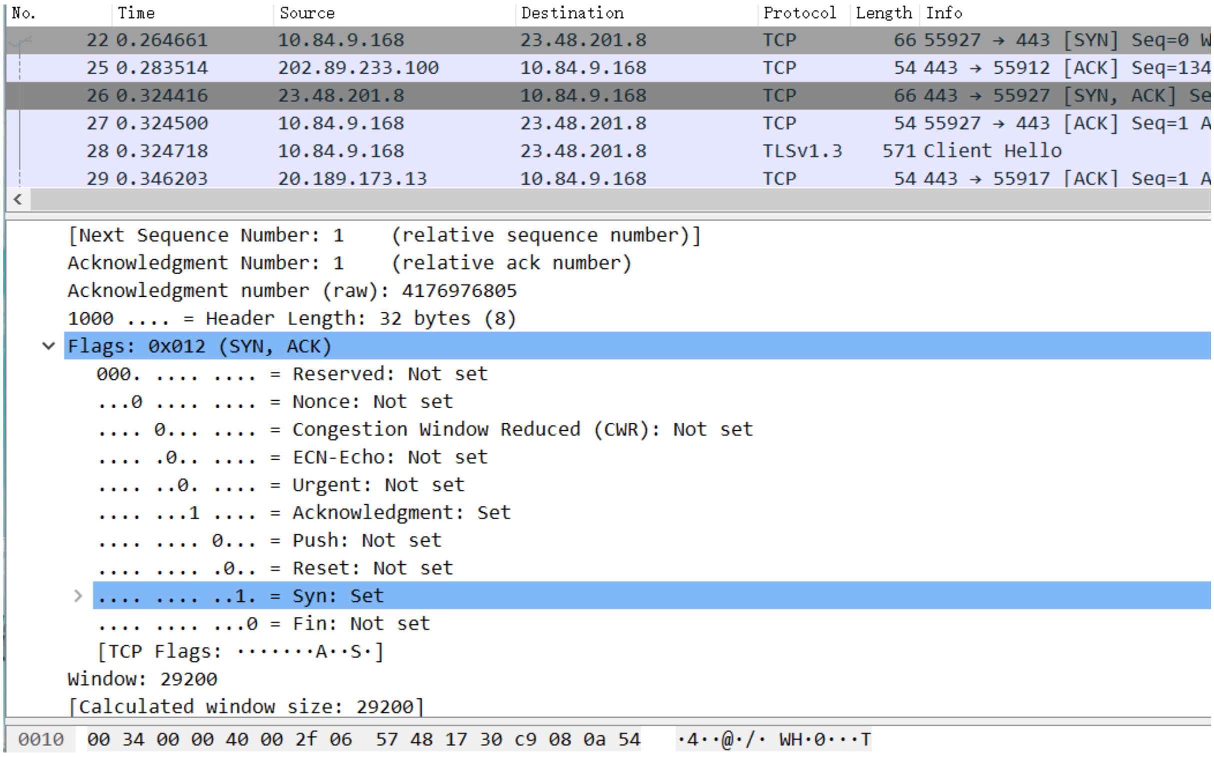
```
20 0.259674   10.84.9.168      202.89.233.100   TCP   54 55912 → 443 [ACK] Seq=315 Ack=1347 Win=508 Len=0
22 0.264661   10.84.9.168      23.48.201.8      TCP   66 55927 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK
25 0.283514   202.89.233.100   10.84.9.168      TCP   54 443 → 55912 [ACK] Seq=1347 Ack=315 Win=2049 Len=0
26 0.324416   23.48.201.8      10.84.9.168      TCP   66 443 → 55927 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
27 0.324500   10.84.9.168      23.48.201.8      TCP   54 55927 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
```

(SYN=1, seq=x)
TCP SYN 1
X, (Sequence Number)
SYN_SEND



```
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1000 .... = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...0 .... = Acknowledgment: Not set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..1. = Syn: Set
    .... .... ...0 = Fin: Not set
    [TCP Flags: ··········S·]
Window: 64240
[Calculated window size: 64240]
Checksum: 0x0f1c [unverified]
```

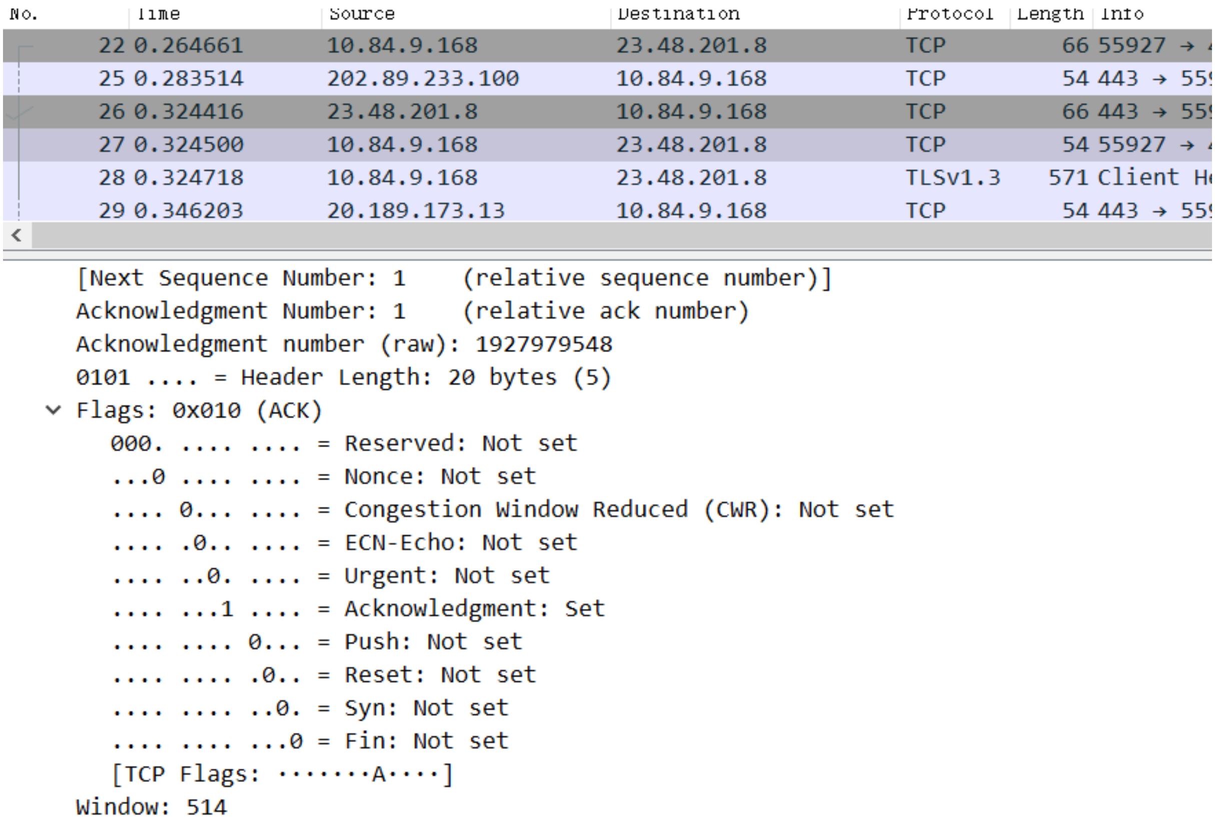
(SYN=1, ACK=1, seq=y, ACKnum=x+1)
(ACK) SYN ACK 1
ISN Seq (Acknowledgement Number)
ISN 1 X+1 SYN_RCVD



```
No.      Time       Source            Destination      Protocol  Length  Info
  22 0.264661   10.84.9.168       23.48.201.8      TCP          66 55927 → 443 [SYN] Seq=0 W
  25 0.283514   202.89.233.100    10.84.9.168      TCP          54 443 → 55912 [ACK] Seq=134
  26 0.324416   23.48.201.8       10.84.9.168      TCP          66 443 → 55927 [SYN, ACK] Se
  27 0.324500   10.84.9.168       23.48.201.8      TCP          54 55927 → 443 [ACK] Seq=1 A
  28 0.324718   10.84.9.168       23.48.201.8      TLSv1.3     571 Client Hello
  29 0.346203   20.189.173.13     10.84.9.168      TCP          54 443 → 55917 [ACK] Seq=1 A
```

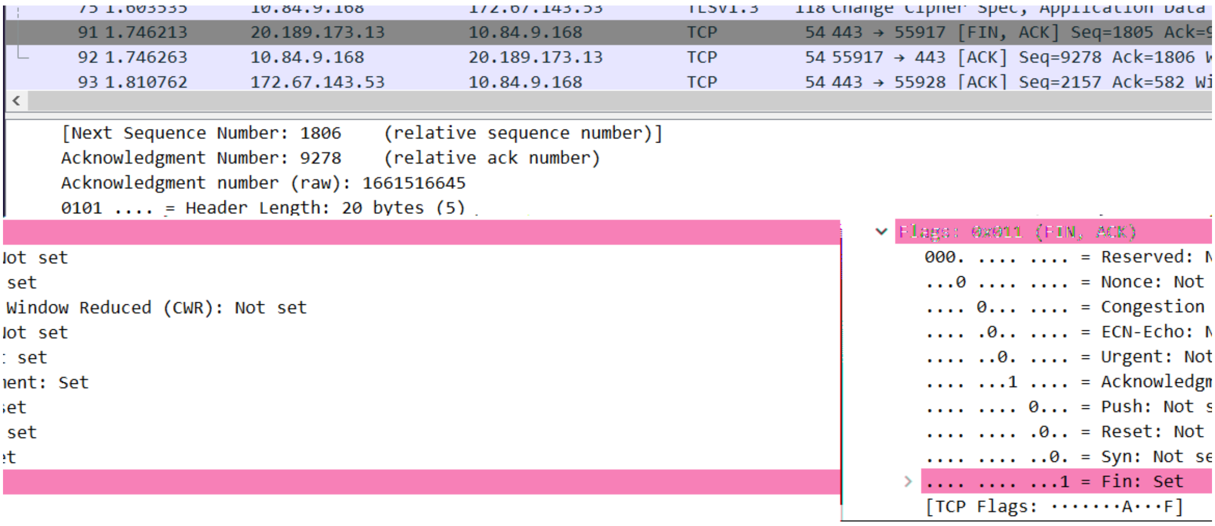
```
     [Next Sequence Number: 1    (relative sequence number)]
     Acknowledgment Number: 1    (relative ack number)
     Acknowledgment number (raw): 4176976805
     1000 .... = Header Length: 32 bytes (8)
   ⌄ Flags: 0x012 (SYN, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
      > .... .... ..1. = Syn: Set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·······A··S·]
     Window: 29200
     [Calculated window size: 29200]
0010   00 34 00 00 40 00 2f 06  57 48 17 30 c9 08 0a 54   ·4··@·/· WH·0···T
```

(ACK=1 ACKnum=y+1)
(ACK) SYN 0 ACK 1
ACK +1 ISN +1
ESTABLISHED
ESTABLISHED TCP



```
No.          Time            Source              Destination          Protocol  Length  Info
     22 0.264661     10.84.9.168          23.48.201.8          TCP          66 55927 → 4
     25 0.283514     202.89.233.100       10.84.9.168          TCP          54 443 → 559
     26 0.324416     23.48.201.8          10.84.9.168          TCP          66 443 → 559
     27 0.324500     10.84.9.168          23.48.201.8          TCP          54 55927 → 4
     28 0.324718     10.84.9.168          23.48.201.8          TLSv1.3     571 Client He
     29 0.346203     20.189.173.13        10.84.9.168          TCP          54 443 → 559
<
```

```
     [Next Sequence Number: 1    (relative sequence number)]
     Acknowledgment Number: 1    (relative ack number)
     Acknowledgment number (raw): 1927979548
     0101 .... = Header Length: 20 bytes (5)
   ⌄ Flags: 0x010 (ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·······A····]
     Window: 514
```



```
     75 1.603535     10.84.9.168          172.67.143.53        TLSv1.3     118 Change Cipher Spec, Application Data
     91 1.746213     20.189.173.13        10.84.9.168          TCP          54 443 → 55917 [FIN, ACK] Seq=1805 Ack=9
     92 1.746263     10.84.9.168          20.189.173.13        TCP          54 55917 → 443 [ACK] Seq=9278 Ack=1806 W
     93 1.810762     172.67.143.53        10.84.9.168          TCP          54 443 → 55928 [ACK] Seq=2157 Ack=582 Wi
<
```

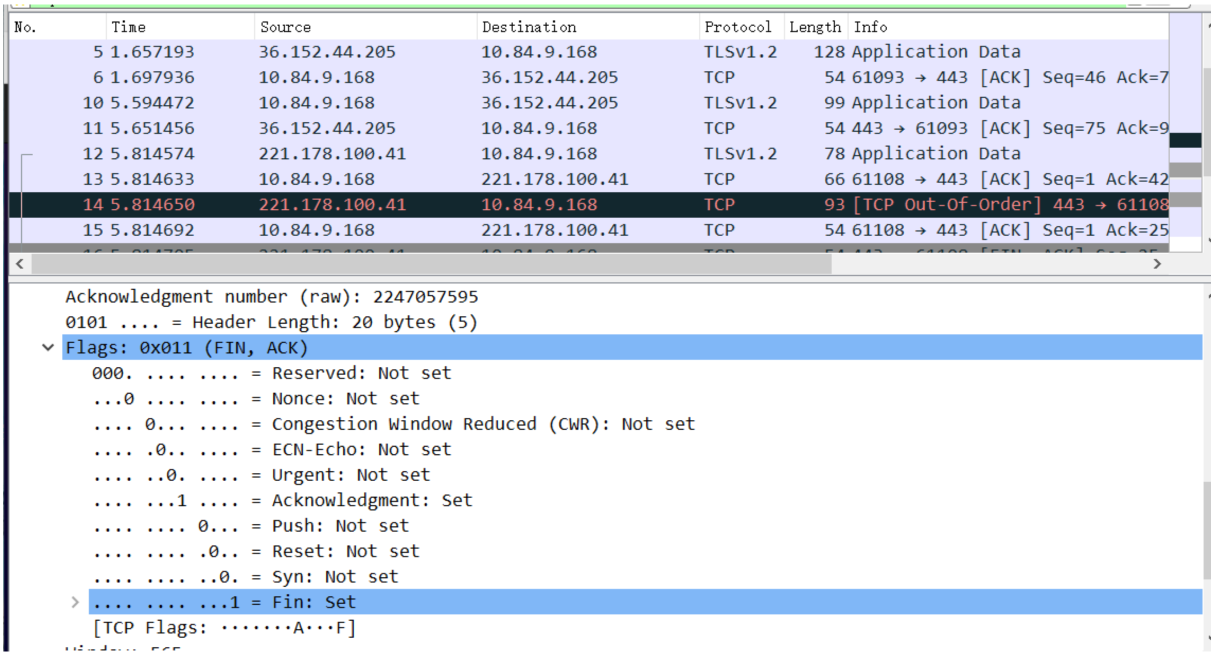
```
     [Next Sequence Number: 1806    (relative sequence number)]
     Acknowledgment Number: 9278    (relative ack number)
     Acknowledgment number (raw): 1661516645
     0101 .... = Header Length: 20 bytes (5)
```

```
Jot set
 set
 Window Reduced (CWR): Not set
Jot set
: set
ient: Set
;et
 set
:t
```

```
   ⌄ Flags: 0x011 (FIN, ACK)
        000. .... .... = Reserved: N
        ...0 .... .... = Nonce: Not
        .... 0... .... = Congestion
        .... .0.. .... = ECN-Echo: N
        .... ..0. .... = Urgent: Not
        .... ...1 .... = Acknowledgm
        .... .... 0... = Push: Not s
        .... .... .0.. = Reset: Not
        .... .... ..0. = Syn: Not se
      › .... .... ...1 = Fin: Set
        [TCP Flags: ·······A···F]
```

:客户端收到 FIN 之后，发送一个 ACK 报文作为应答

1 close FIN
FIN_WAIT_1

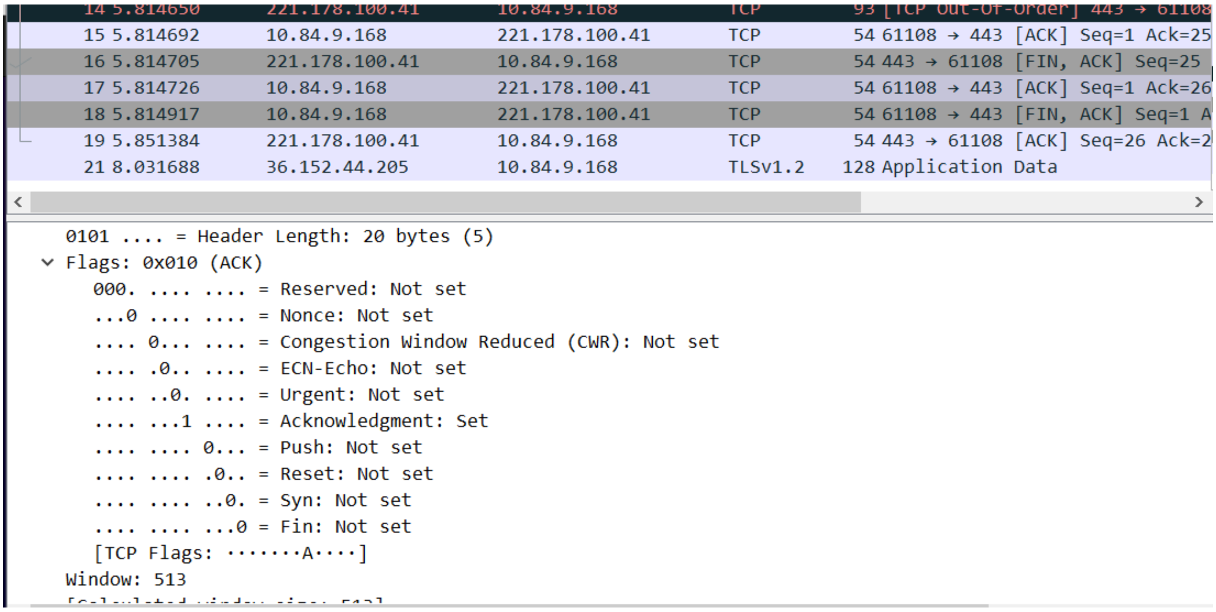


```
No.   Time        Source           Destination      Protocol  Length Info
    5 1.657193    36.152.44.205    10.84.9.168      TLSv1.2   128 Application Data
    6 1.697936    10.84.9.168      36.152.44.205    TCP        54 61093 → 443 [ACK] Seq=46 Ack=7
   10 5.594472    10.84.9.168      36.152.44.205    TLSv1.2    99 Application Data
   11 5.651456    36.152.44.205    10.84.9.168      TCP        54 443 → 61093 [ACK] Seq=75 Ack=9
   12 5.814574    221.178.100.41   10.84.9.168      TLSv1.2    78 Application Data
   13 5.814633    10.84.9.168      221.178.100.41   TCP        66 61108 → 443 [ACK] Seq=1 Ack=42
   14 5.814650    221.178.100.41   10.84.9.168      TCP        93 [TCP Out-Of-Order] 443 → 61108
   15 5.814692    10.84.9.168      221.178.100.41   TCP        54 61108 → 443 [ACK] Seq=1 Ack=25

    Acknowledgment number (raw): 2247057595
    0101 .... = Header Length: 20 bytes (5)
  ∨ Flags: 0x011 (FIN, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
    > .... .... ...1 = Fin: Set
      [TCP Flags: ·······A···F]
```

2 FIN FIN TCP ACK

FIN

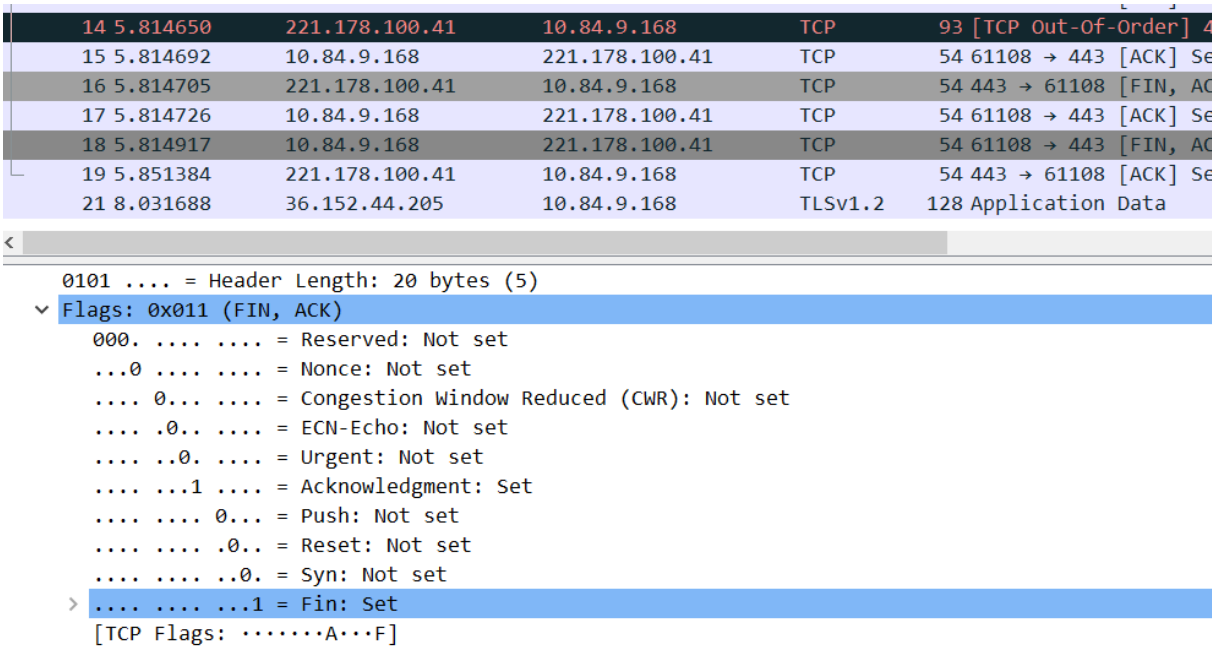
CLOSE_WAIT ACK FIN_WAIT_2



```
   15 5.814692    10.84.9.168      221.178.100.41   TCP        54 61108 → 443 [ACK] Seq=1 Ack=25
   16 5.814705    221.178.100.41   10.84.9.168      TCP        54 443 → 61108 [FIN, ACK] Seq=25
   17 5.814726    10.84.9.168      221.178.100.41   TCP        54 61108 → 443 [ACK] Seq=1 Ack=26
   18 5.814917    10.84.9.168      221.178.100.41   TCP        54 61108 → 443 [FIN, ACK] Seq=1 A
   19 5.851384    221.178.100.41   10.84.9.168      TCP        54 443 → 61108 [ACK] Seq=26 Ack=2
   21 8.031688    36.152.44.205    10.84.9.168      TLSv1.2   128 Application Data

    0101 .... = Header Length: 20 bytes (5)
  ∨ Flags: 0x010 (ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······A····]
    Window: 513
```

3 close

FIN LAST_ACK

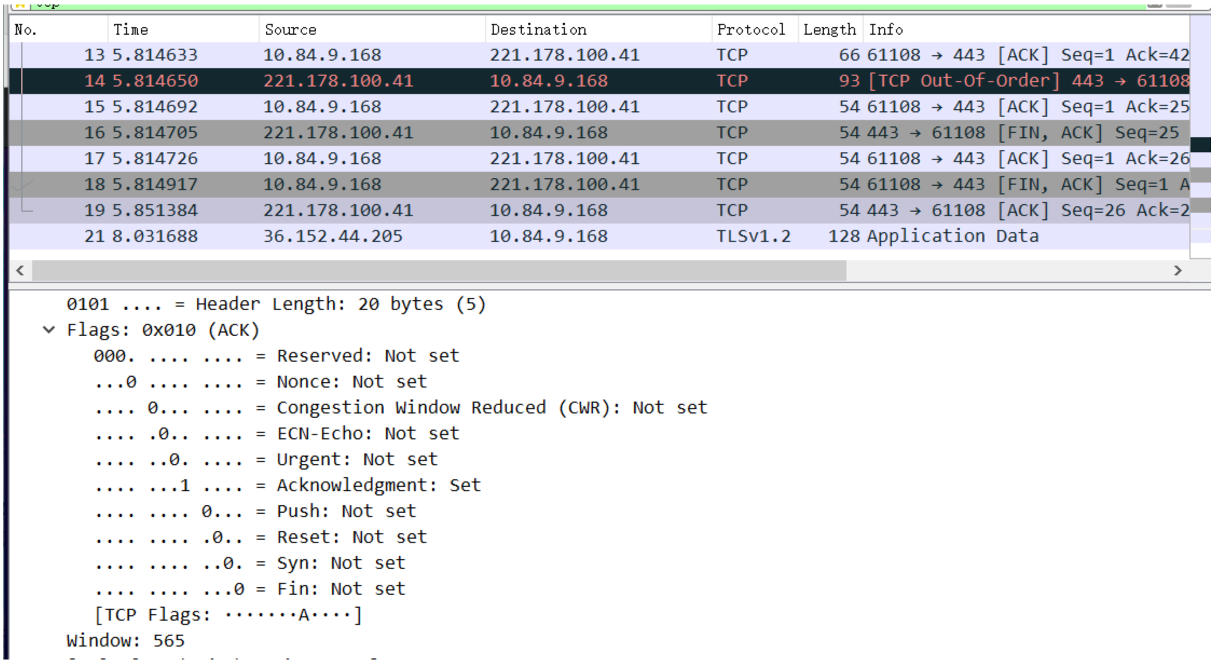


```
14 5.814650   221.178.100.41   10.84.9.168      TCP      93 [TCP Out-Of-Order] 4
15 5.814692   10.84.9.168      221.178.100.41   TCP      54 61108 → 443 [ACK] Se
16 5.814705   221.178.100.41   10.84.9.168      TCP      54 443 → 61108 [FIN, AC
17 5.814726   10.84.9.168      221.178.100.41   TCP      54 61108 → 443 [ACK] Se
18 5.814917   10.84.9.168      221.178.100.41   TCP      54 61108 → 443 [FIN, AC
19 5.851384   221.178.100.41   10.84.9.168      TCP      54 443 → 61108 [ACK] Se
21 8.031688   36.152.44.205    10.84.9.168      TLSv1.2 128 Application Data
```

```
    0101 .... = Header Length: 20 bytes (5)
  ⌄ Flags: 0x011 (FIN, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
    > .... .... ...1 = Fin: Set
      [TCP Flags: ·······A···F]
```

4 FIN TIME_WAIT ACK

ACK TCP TCP



```
No.  Time        Source           Destination      Protocol Length Info
13 5.814633   10.84.9.168      221.178.100.41   TCP      66 61108 → 443 [ACK] Seq=1 Ack=42
14 5.814650   221.178.100.41   10.84.9.168      TCP      93 [TCP Out-Of-Order] 443 → 61108
15 5.814692   10.84.9.168      221.178.100.41   TCP      54 61108 → 443 [ACK] Seq=1 Ack=25
16 5.814705   221.178.100.41   10.84.9.168      TCP      54 443 → 61108 [FIN, ACK] Seq=25
17 5.814726   10.84.9.168      221.178.100.41   TCP      54 61108 → 443 [ACK] Seq=1 Ack=26
18 5.814917   10.84.9.168      221.178.100.41   TCP      54 61108 → 443 [FIN, ACK] Seq=1 A
19 5.851384   221.178.100.41   10.84.9.168      TCP      54 443 → 61108 [ACK] Seq=26 Ack=2
21 8.031688   36.152.44.205    10.84.9.168      TLSv1.2 128 Application Data
```

```
    0101 .... = Header Length: 20 bytes (5)
  ⌄ Flags: 0x010 (ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······A····]
    Window: 565
```

✎

Follow TCP Stream TCP qige.io

, / ,

,

ACK=1

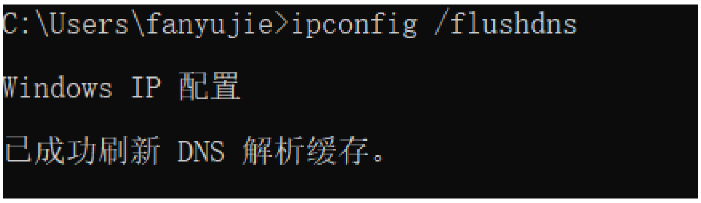
FIN=1

4

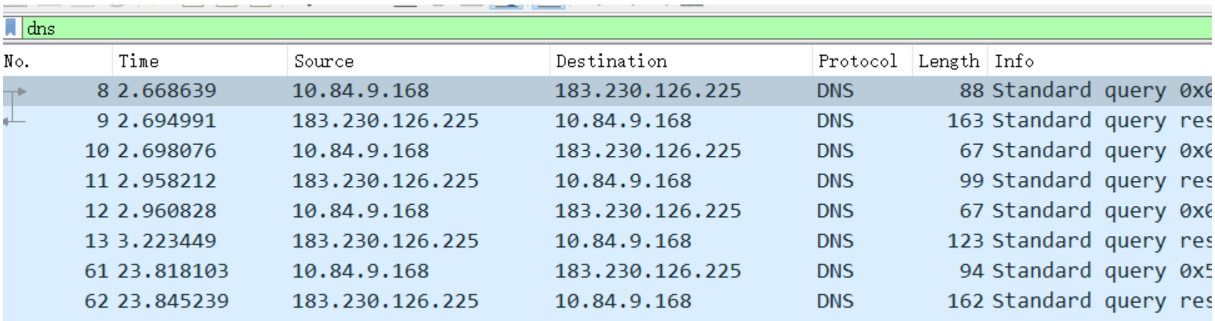
DNS

ipconfig /flushdns nslookup qige.io

Wireshark dns



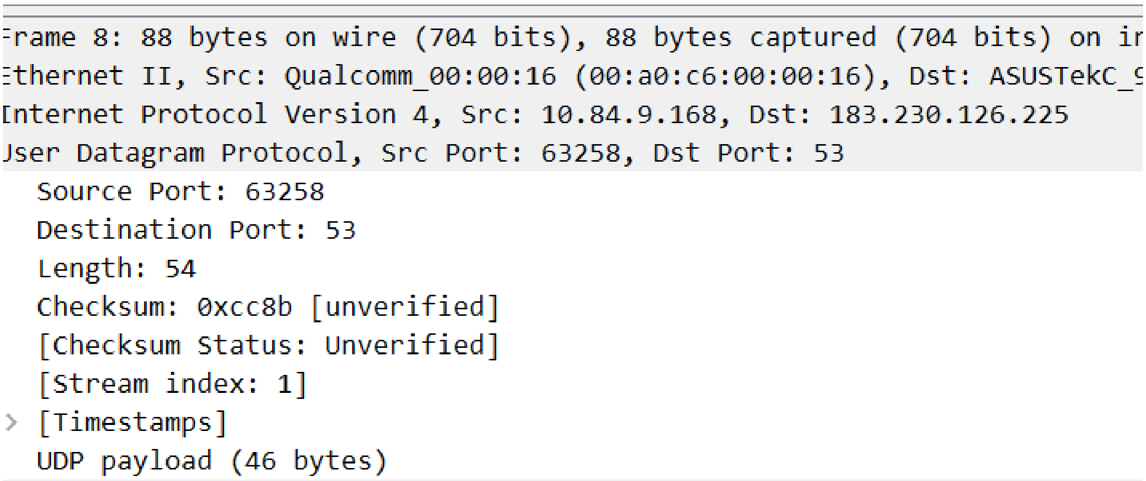
```
C:\Users\fanyujie>ipconfig /flushdns

Windows IP 配置

已成功刷新 DNS 解析缓存。
```



```
dns
No.   Time        Source            Destination       Protocol  Length  Info
    8 2.668639    10.84.9.168       183.230.126.225   DNS           88  Standard query 0x0
    9 2.694991    183.230.126.225   10.84.9.168       DNS          163  Standard query res
   10 2.698076    10.84.9.168       183.230.126.225   DNS           67  Standard query 0x0
   11 2.958212    183.230.126.225   10.84.9.168       DNS           99  Standard query res
   12 2.960828    10.84.9.168       183.230.126.225   DNS           67  Standard query 0x0
   13 3.223449    183.230.126.225   10.84.9.168       DNS          123  Standard query res
   61 23.818103   10.84.9.168       183.230.126.225   DNS           94  Standard query 0x5
   62 23.845239   183.230.126.225   10.84.9.168       DNS          162  Standard query res
```

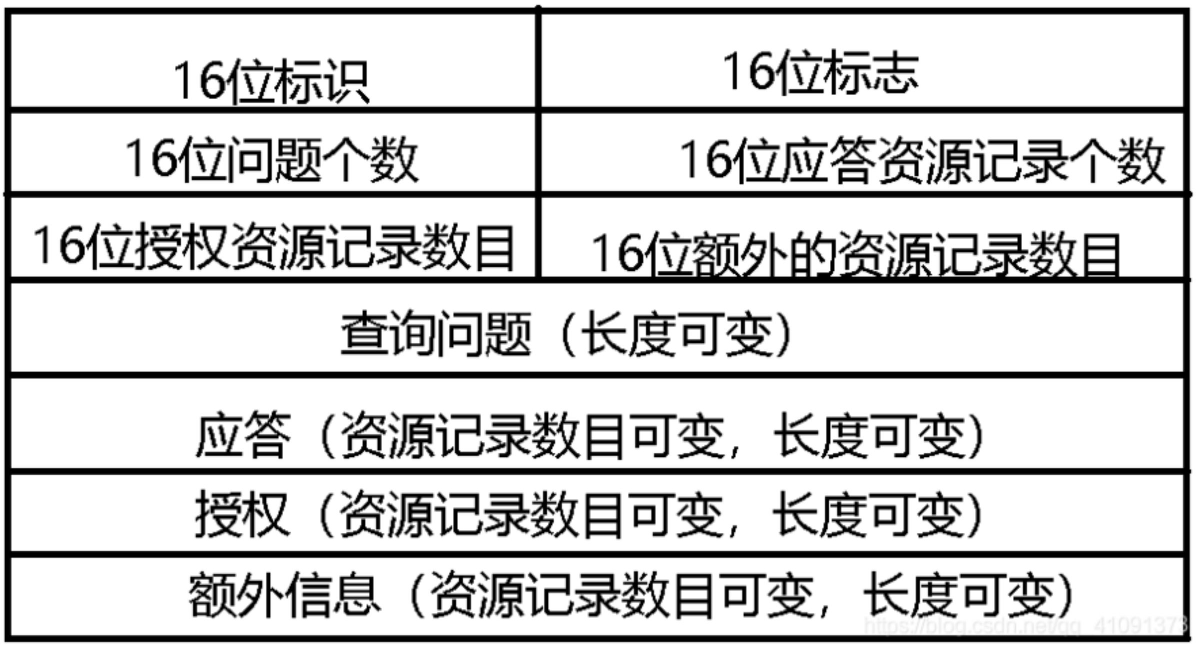
UDP DNS 53

DNS 53



```
Frame 8: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on ir
Ethernet II, Src: Qualcomm_00:00:16 (00:a0:c6:00:00:16), Dst: ASUSTekC_9
Internet Protocol Version 4, Src: 10.84.9.168, Dst: 183.230.126.225
User Datagram Protocol, Src Port: 63258, Dst Port: 53
  Source Port: 63258
  Destination Port: 53
  Length: 54
  Checksum: 0xcc8b [unverified]
  [Checksum Status: Unverified]
  [Stream index: 1]
> [Timestamps]
  UDP payload (46 bytes)
```

DNS



16位标识	16位标志
16位问题个数	16位应答资源记录个数
16位授权资源记录数目	16位额外的资源记录数目
查询问题（长度可变）	
应答（资源记录数目可变，长度可变）	
授权（资源记录数目可变，长度可变）	
额外信息（资源记录数目可变，长度可变）	

DNS

, ***dns***

IP ***“***
”

IP

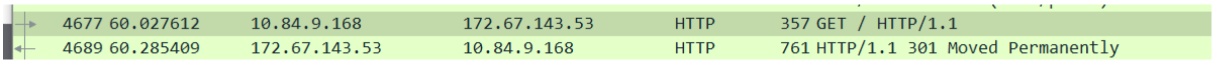
IP

IP

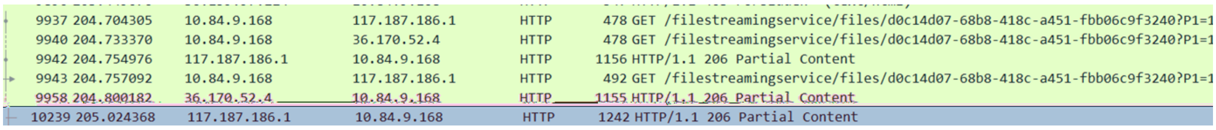
HTTP

qige.io Wireshark http Follow TCP Stream Wireshark

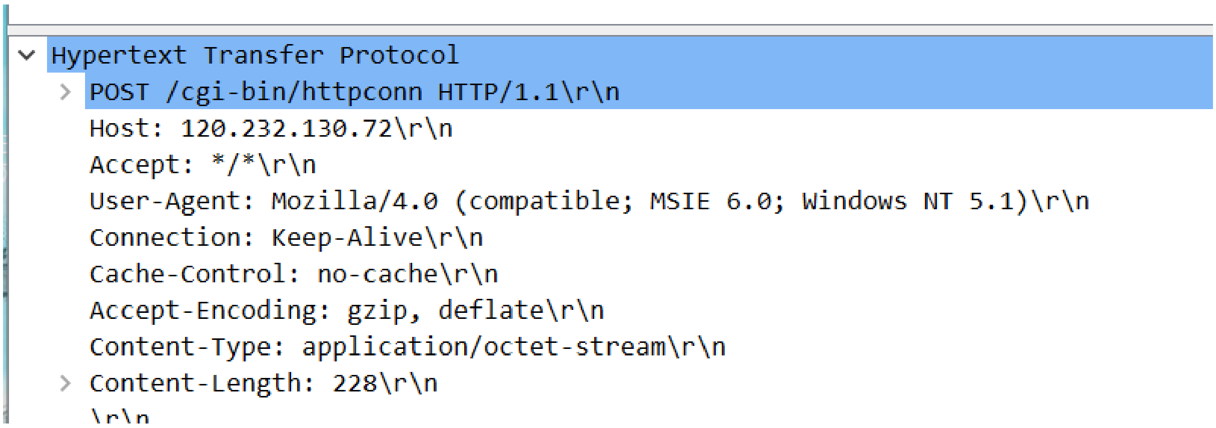
HTTP GET, POST



```
4677 60.027612   10.84.9.168     172.67.143.53   HTTP   357 GET / HTTP/1.1
4689 60.285409   172.67.143.53   10.84.9.168     HTTP   761 HTTP/1.1 301 Moved Permanently
```



```
9937 204.704305   10.84.9.168     117.187.186.1   HTTP   478 GET /filestreamingservice/files/d0c14d07-68b8-418c-a451-fbb06c9f3240?P1=1
9940 204.733370   10.84.9.168     36.170.52.4     HTTP   478 GET /filestreamingservice/files/d0c14d07-68b8-418c-a451-fbb06c9f3240?P1=1
9942 204.754976   117.187.186.1   10.84.9.168     HTTP   1156 HTTP/1.1 206 Partial Content
9943 204.757092   10.84.9.168     117.187.186.1   HTTP   492 GET /filestreamingservice/files/d0c14d07-68b8-418c-a451-fbb06c9f3240?P1=1
9958 204.800182   36.170.52.4     10.84.9.168     HTTP   1155 HTTP/1.1 206 Partial Content
10239 205.024368  117.187.186.1   10.84.9.168     HTTP   1242 HTTP/1.1 206 Partial Content
```



```
Hypertext Transfer Protocol
  > POST /cgi-bin/httpconn HTTP/1.1\r\n
    Host: 120.232.130.72\r\n
    Accept: */*\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)\r\n
    Connection: Keep-Alive\r\n
    Cache-Control: no-cache\r\n
    Accept-Encoding: gzip, deflate\r\n
    Content-Type: application/octet-stream\r\n
  > Content-Length: 228\r\n
    \r\n
```

HTTP 200, 304, 404

*Accept WEB / type/**
type/sub-type

Accept-Charset
Accept-Encoding
gzip deflate
Accept-Language
big5 gb2312 gbk

Accept-Ranges WEB
bytes none

Age

Authorization WEB WWW-Authenticate
WEB

Cache-Control no-cache WEB
max-age Age max-age
max-stale
max-stale
min-fresh Age min-fresh

public(Cached   )
private
no-cache   WEB
max-age
ALL: no-store

Connection   close   WEB

keepalive   WEB

close
keepalive
Keep-Alive   WEB

Keep-Alive   300

Content-Encoding   WEB   gzip   deflate

Content-Encoding   gzip
Content-Language   WEB
Content-Length   WEB
Content-Length: 26012
Content-Range   WEB
Content-Range: bytes 21010-47021/47022
Content-Type   WEB
Content-Type   application/xml

ETag   URL   html
Etag   ETag   Last-Modified
WEB
html   ETag
ETag   WEB   WEB
ETag   ETag

Expired   WEB
WEB
HTTP/1.0
Expires   Sat, 23 May 2009 10:02:12 GMT

Host   WEB   /IP
Host   rss.sina.com.cn

If-Match ETag

If-None-Match ETag

If-Modified-Since

304

If-Modified-Since Thu, 10 Apr 2008 09:14:42 GMT

If-Unmodified-Since

If-Range WEB

ETag WEB

Range

Last-Modified WEB

Last-Modified Tue, 06 May 2008 02:42:43 GMT

Location WEB

Location http://i0.sinaimg.cn/dy/deco/2008/0528/sinahome_0803_ws_005_text_0.gif

Pramga Pramga: no-cache Cache-Control no-cache Pragma no-cache

Proxy-Authenticate

Proxy-Authorization

Range Flashget WEB

Range: bytes=1173546-

Referer WEB /URL / /URL

Referer http://www.sina.com/

Server: WEB

Server Apache/2.0.61 (Unix)

User-Agent:

User-Agent Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN; rv:1.8.1.14) Gecko/20080404 Firefox/2.0.0.14

Transfer-Encoding: WEB

chunked

Transfer-Encoding: chunked

Vary: WEB Cache

WEB

Content-Encoding: gzip; Vary: Content-Encoding Cache

Accept-Encoding Vary

Cache

Cache

Vary Accept-Encoding

Via OCS

Via

Via

OCS

Via

Via 1.0 236-81.D07071953.sina.com.cn:80 (squid/2.6.STABLE13)

✍

HTTP Web

cookie

✎

qige.io 304

304 200

200

304

200

304 ***200***