利用Wireshark进行抓包

1.实验所需软件

Wireshark

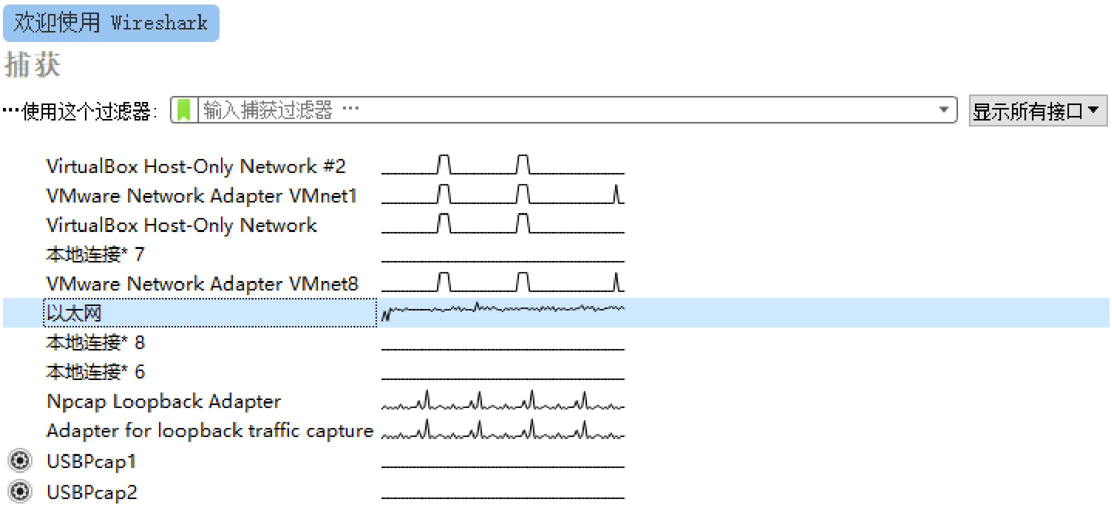
2.实验目的

使用工具Wireshark进行抓包

3.实验步骤

1.筛选出ip地址为172.18.139.91的数据包

(1)打开Wireshark选择以太网



欢迎使用 Wireshark

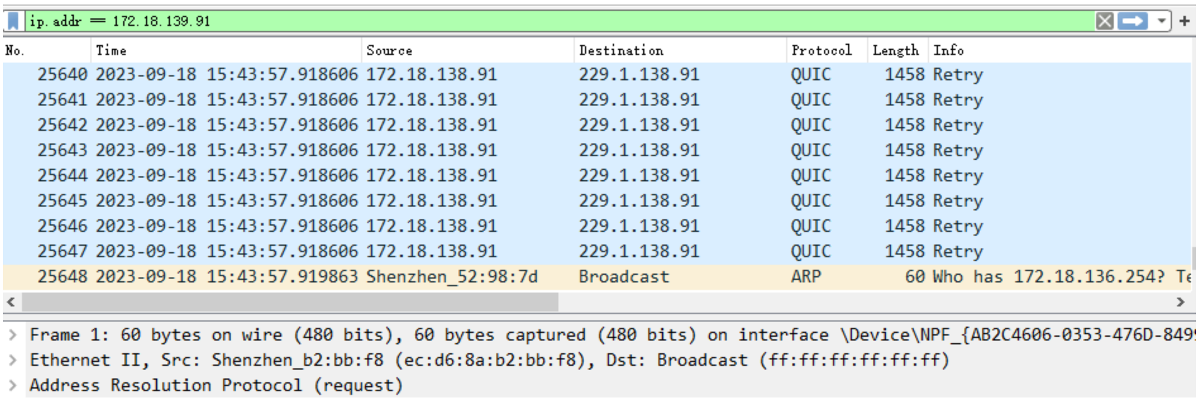
捕获

…使用这个过滤器: 输入捕获过滤器 …

显示所有接口▾

```
VirtualBox Host-Only Network #2
VMware Network Adapter VMnet1
VirtualBox Host-Only Network
本地连接* 7
VMware Network Adapter VMnet8
以太网
本地连接* 8
本地连接* 6
Npcap Loopback Adapter
Adapter for loopback traffic capture
USBPcap1
USBPcap2
```

(2)搜索栏输入ip.addr == 172.18.139.91(背景为淡绿色是语法正确 否则就是语法有问题)

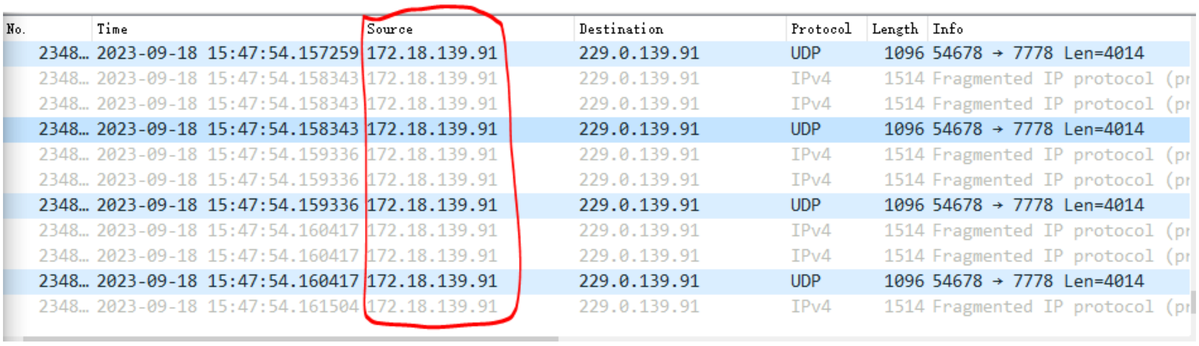


```
ip.addr == 172.18.139.91

No.   Time                       Source              Destination     Protocol  Length Info
25640 2023-09-18 15:43:57.918606 172.18.138.91       229.1.138.91    QUIC        1458 Retry
25641 2023-09-18 15:43:57.918606 172.18.138.91       229.1.138.91    QUIC        1458 Retry
25642 2023-09-18 15:43:57.918606 172.18.138.91       229.1.138.91    QUIC        1458 Retry
25643 2023-09-18 15:43:57.918606 172.18.138.91       229.1.138.91    QUIC        1458 Retry
25644 2023-09-18 15:43:57.918606 172.18.138.91       229.1.138.91    QUIC        1458 Retry
25645 2023-09-18 15:43:57.918606 172.18.138.91       229.1.138.91    QUIC        1458 Retry
25646 2023-09-18 15:43:57.918606 172.18.138.91       229.1.138.91    QUIC        1458 Retry
25647 2023-09-18 15:43:57.918606 172.18.138.91       229.1.138.91    QUIC        1458 Retry
25648 2023-09-18 15:43:57.919863 Shenzhen_52:98:7d   Broadcast       ARP           60 Who has 172.18.136.254? Te

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{AB2C4606-0353-476D-849
> Ethernet II, Src: Shenzhen_b2:bb:f8 (ec:d6:8a:b2:bb:f8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

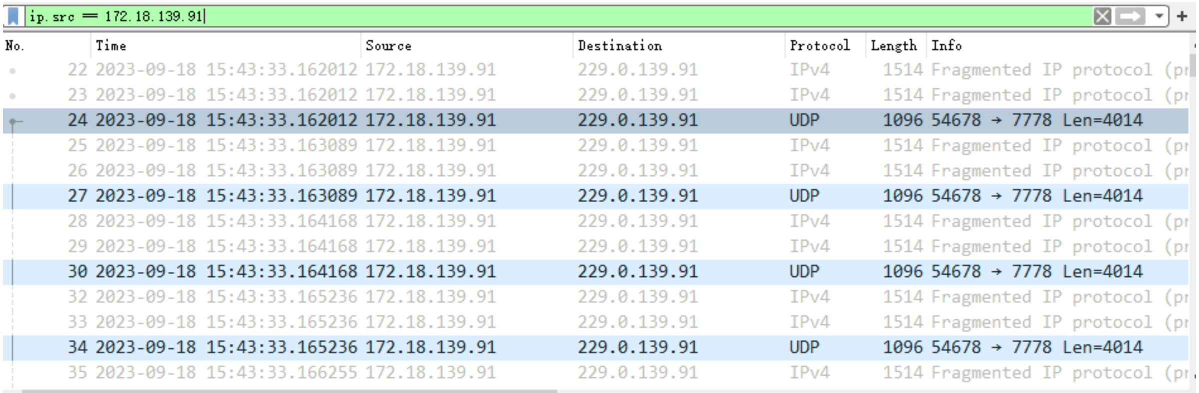
(3)输入完毕后回车查看 此时可以看见ip地址都是172.18.139.91



No.	Time	Source	Destination	Protocol	Length	Info
2348…	2023-09-18 15:47:54.157259	172.18.139.91	229.0.139.91	UDP	1096	54678 → 7778 Len=4014
2348…	2023-09-18 15:47:54.158343	172.18.139.91	229.0.139.91	IPv4	1514	Fragmented IP protocol (pr
2348…	2023-09-18 15:47:54.158343	172.18.139.91	229.0.139.91	IPv4	1514	Fragmented IP protocol (pr
2348…	2023-09-18 15:47:54.158343	172.18.139.91	229.0.139.91	UDP	1096	54678 → 7778 Len=4014
2348…	2023-09-18 15:47:54.159336	172.18.139.91	229.0.139.91	IPv4	1514	Fragmented IP protocol (pr
2348…	2023-09-18 15:47:54.159336	172.18.139.91	229.0.139.91	IPv4	1514	Fragmented IP protocol (pr
2348…	2023-09-18 15:47:54.159336	172.18.139.91	229.0.139.91	UDP	1096	54678 → 7778 Len=4014
2348…	2023-09-18 15:47:54.160417	172.18.139.91	229.0.139.91	IPv4	1514	Fragmented IP protocol (pr
2348…	2023-09-18 15:47:54.160417	172.18.139.91	229.0.139.91	IPv4	1514	Fragmented IP protocol (pr
2348…	2023-09-18 15:47:54.160417	172.18.139.91	229.0.139.91	UDP	1096	54678 → 7778 Len=4014
2348…	2023-09-18 15:47:54.161504	172.18.139.91	229.0.139.91	IPv4	1514	Fragmented IP protocol (pr

2.筛选出源ip地址为172.18.139.91 的数据包

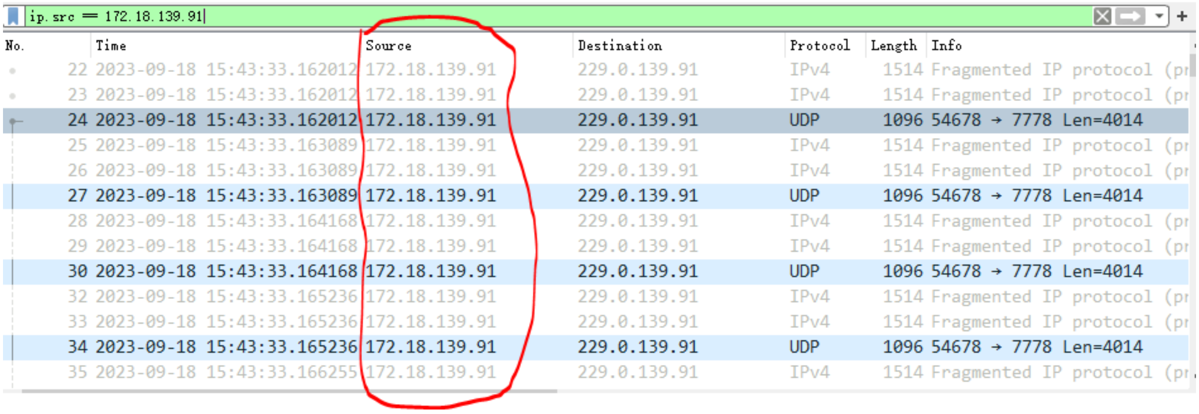
(1)搜索栏输入ip.src == 172.18.139.91 (背景为淡绿色是语法正确 否则就是语法有问题)



ip.src == 172.18.139.91

No.	Time	Source	Destination	Protocol	Length	Info
22	2023-09-18 15:43:33.162012	172.18.139.91	229.0.139.91	IPv4	1514	Fragmented IP protocol (pr
23	2023-09-18 15:43:33.162012	172.18.139.91	229.0.139.91	IPv4	1514	Fragmented IP protocol (pr
24	2023-09-18 15:43:33.162012	172.18.139.91	229.0.139.91	UDP	1096	54678 → 7778 Len=4014
25	2023-09-18 15:43:33.163089	172.18.139.91	229.0.139.91	IPv4	1514	Fragmented IP protocol (pr
26	2023-09-18 15:43:33.163089	172.18.139.91	229.0.139.91	IPv4	1514	Fragmented IP protocol (pr
27	2023-09-18 15:43:33.163089	172.18.139.91	229.0.139.91	UDP	1096	54678 → 7778 Len=4014
28	2023-09-18 15:43:33.164168	172.18.139.91	229.0.139.91	IPv4	1514	Fragmented IP protocol (pr
29	2023-09-18 15:43:33.164168	172.18.139.91	229.0.139.91	IPv4	1514	Fragmented IP protocol (pr
30	2023-09-18 15:43:33.164168	172.18.139.91	229.0.139.91	UDP	1096	54678 → 7778 Len=4014
32	2023-09-18 15:43:33.165236	172.18.139.91	229.0.139.91	IPv4	1514	Fragmented IP protocol (pr
33	2023-09-18 15:43:33.165236	172.18.139.91	229.0.139.91	IPv4	1514	Fragmented IP protocol (pr
34	2023-09-18 15:43:33.165236	172.18.139.91	229.0.139.91	UDP	1096	54678 → 7778 Len=4014
35	2023-09-18 15:43:33.166255	172.18.139.91	229.0.139.91	IPv4	1514	Fragmented IP protocol (pr

(2)输入完毕后回车查看 此时可以看见源ip地址为172.18.139.91

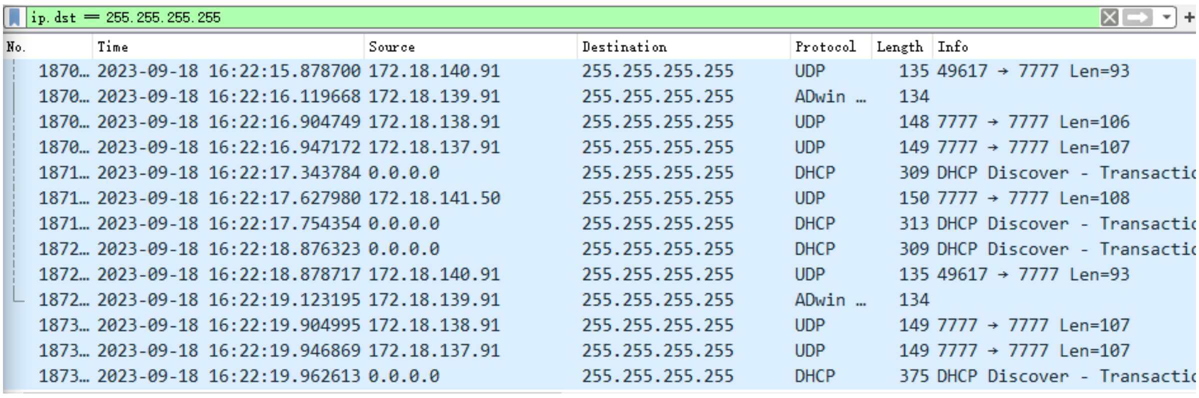


ip.src == 172.18.139.91

No.	Time	Source	Destination	Protocol	Length	Info
22	2023-09-18 15:43:33.162012	172.18.139.91	229.0.139.91	IPv4	1514	Fragmented IP protocol (pr
23	2023-09-18 15:43:33.162012	172.18.139.91	229.0.139.91	IPv4	1514	Fragmented IP protocol (pr
24	2023-09-18 15:43:33.162012	172.18.139.91	229.0.139.91	UDP	1096	54678 → 7778 Len=4014
25	2023-09-18 15:43:33.163089	172.18.139.91	229.0.139.91	IPv4	1514	Fragmented IP protocol (pr
26	2023-09-18 15:43:33.163089	172.18.139.91	229.0.139.91	IPv4	1514	Fragmented IP protocol (pr
27	2023-09-18 15:43:33.163089	172.18.139.91	229.0.139.91	UDP	1096	54678 → 7778 Len=4014
28	2023-09-18 15:43:33.164168	172.18.139.91	229.0.139.91	IPv4	1514	Fragmented IP protocol (pr
29	2023-09-18 15:43:33.164168	172.18.139.91	229.0.139.91	IPv4	1514	Fragmented IP protocol (pr
30	2023-09-18 15:43:33.164168	172.18.139.91	229.0.139.91	UDP	1096	54678 → 7778 Len=4014
32	2023-09-18 15:43:33.165236	172.18.139.91	229.0.139.91	IPv4	1514	Fragmented IP protocol (pr
33	2023-09-18 15:43:33.165236	172.18.139.91	229.0.139.91	IPv4	1514	Fragmented IP protocol (pr
34	2023-09-18 15:43:33.165236	172.18.139.91	229.0.139.91	UDP	1096	54678 → 7778 Len=4014
35	2023-09-18 15:43:33.166255	172.18.139.91	229.0.139.91	IPv4	1514	Fragmented IP protocol (pr

3.筛选出目标ip地址为255.255.255.255的数据包

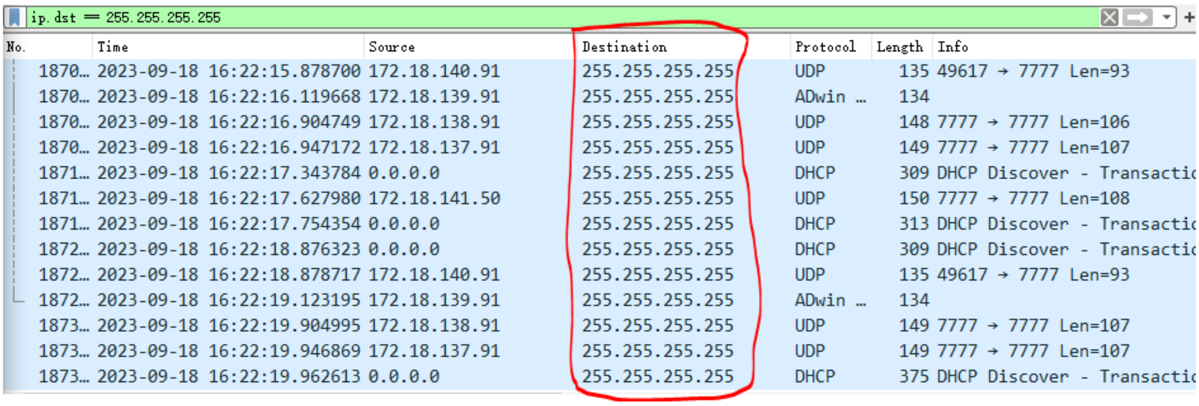
(1)搜索栏输入ip.dst == 255.255.255.255 (背景为淡绿色是语法正确 否则就是语法有问题)



ip.dst == 255.255.255.255

No.	Time	Source	Destination	Protocol	Length	Info
1870…	2023-09-18 16:22:15.878700	172.18.140.91	255.255.255.255	UDP	135	49617 → 7777 Len=93
1870…	2023-09-18 16:22:16.119668	172.18.139.91	255.255.255.255	ADwin …	134	
1870…	2023-09-18 16:22:16.904749	172.18.138.91	255.255.255.255	UDP	148	7777 → 7777 Len=106
1870…	2023-09-18 16:22:16.947172	172.18.137.91	255.255.255.255	UDP	149	7777 → 7777 Len=107
1871…	2023-09-18 16:22:17.343784	0.0.0.0	255.255.255.255	DHCP	309	DHCP Discover - Transactic
1871…	2023-09-18 16:22:17.627980	172.18.141.50	255.255.255.255	UDP	150	7777 → 7777 Len=108
1871…	2023-09-18 16:22:17.754354	0.0.0.0	255.255.255.255	DHCP	313	DHCP Discover - Transactic
1872…	2023-09-18 16:22:18.876323	0.0.0.0	255.255.255.255	DHCP	309	DHCP Discover - Transactic
1872…	2023-09-18 16:22:18.878717	172.18.140.91	255.255.255.255	UDP	135	49617 → 7777 Len=93
1872…	2023-09-18 16:22:19.123195	172.18.139.91	255.255.255.255	ADwin …	134	
1873…	2023-09-18 16:22:19.904995	172.18.138.91	255.255.255.255	UDP	149	7777 → 7777 Len=107
1873…	2023-09-18 16:22:19.946869	172.18.137.91	255.255.255.255	UDP	149	7777 → 7777 Len=107
1873…	2023-09-18 16:22:19.962613	0.0.0.0	255.255.255.255	DHCP	375	DHCP Discover - Transactic

(2)输入完毕后回车查看 此时可以看见目标ip地址为255.255.255.255的数据包

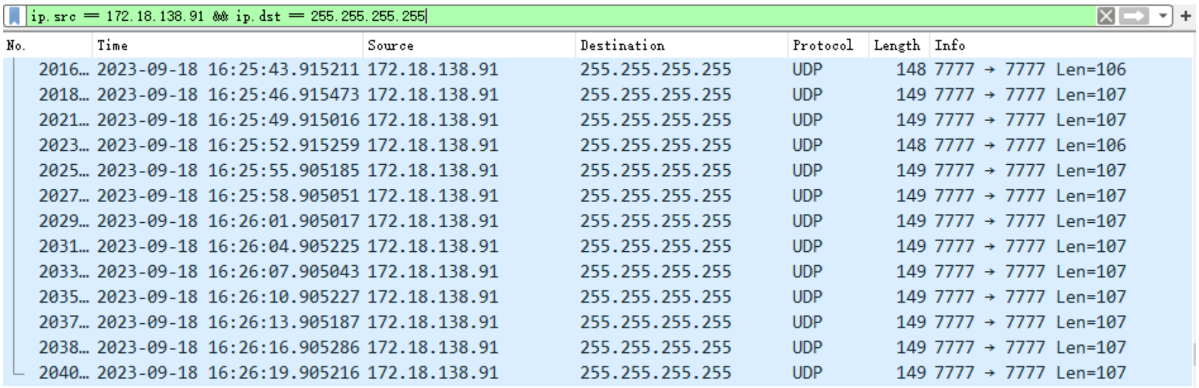


```
ip.dst == 255.255.255.255

No.     Time                       Source          Destination      Protocol  Length  Info
1870… 2023-09-18 16:22:15.878700 172.18.140.91   255.255.255.255  UDP        135 49617 → 7777 Len=93
1870… 2023-09-18 16:22:16.119668 172.18.139.91   255.255.255.255  ADwin …    134
1870… 2023-09-18 16:22:16.904749 172.18.138.91   255.255.255.255  UDP        148 7777 → 7777 Len=106
1870… 2023-09-18 16:22:16.947172 172.18.137.91   255.255.255.255  UDP        149 7777 → 7777 Len=107
1871… 2023-09-18 16:22:17.343784 0.0.0.0         255.255.255.255  DHCP       309 DHCP Discover - Transactio
1871… 2023-09-18 16:22:17.627980 172.18.141.50   255.255.255.255  UDP        150 7777 → 7777 Len=108
1871… 2023-09-18 16:22:17.754354 0.0.0.0         255.255.255.255  DHCP       313 DHCP Discover - Transactio
1872… 2023-09-18 16:22:18.876323 0.0.0.0         255.255.255.255  DHCP       309 DHCP Discover - Transactio
1872… 2023-09-18 16:22:18.878717 172.18.140.91   255.255.255.255  UDP        135 49617 → 7777 Len=93
1872… 2023-09-18 16:22:19.123195 172.18.139.91   255.255.255.255  ADwin …    134
1873… 2023-09-18 16:22:19.904995 172.18.138.91   255.255.255.255  UDP        149 7777 → 7777 Len=107
1873… 2023-09-18 16:22:19.946869 172.18.137.91   255.255.255.255  UDP        149 7777 → 7777 Len=107
1873… 2023-09-18 16:22:19.962613 0.0.0.0         255.255.255.255  DHCP       375 DHCP Discover - Transactio
```

4.筛选出源ip地址为172.18.138.91 目标ip地址为255.255.255.255的数据包

(1)搜索栏输入ip.src == 172.18.138.91 && ip.dst == 255.255.255.255 (背景为淡绿色是语法正确 否则就是语法有问题)

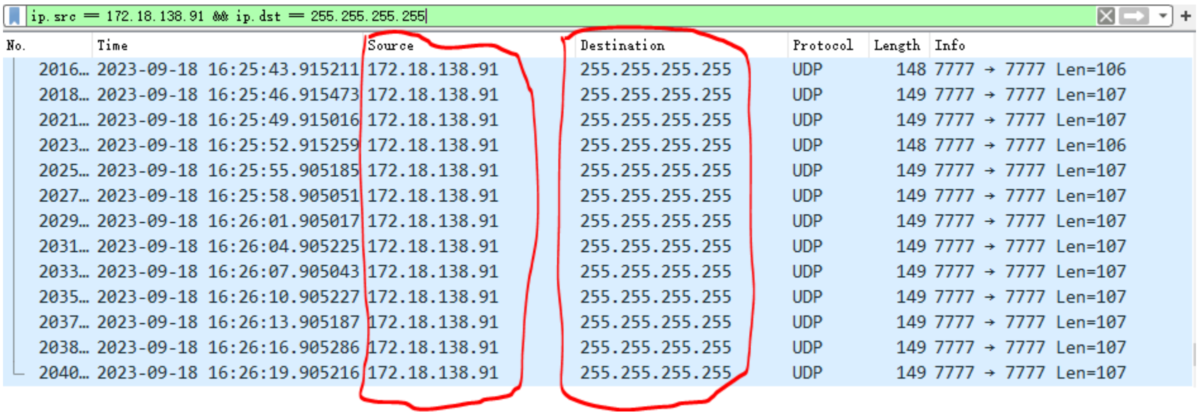


```
ip.src == 172.18.138.91 && ip.dst == 255.255.255.255

No.     Time                       Source          Destination      Protocol  Length  Info
2016… 2023-09-18 16:25:43.915211 172.18.138.91   255.255.255.255  UDP        148 7777 → 7777 Len=106
2018… 2023-09-18 16:25:46.915473 172.18.138.91   255.255.255.255  UDP        149 7777 → 7777 Len=107
2021… 2023-09-18 16:25:49.915016 172.18.138.91   255.255.255.255  UDP        149 7777 → 7777 Len=107
2023… 2023-09-18 16:25:52.915259 172.18.138.91   255.255.255.255  UDP        148 7777 → 7777 Len=106
2025… 2023-09-18 16:25:55.905185 172.18.138.91   255.255.255.255  UDP        149 7777 → 7777 Len=107
2027… 2023-09-18 16:25:58.905051 172.18.138.91   255.255.255.255  UDP        149 7777 → 7777 Len=107
2029… 2023-09-18 16:26:01.905017 172.18.138.91   255.255.255.255  UDP        149 7777 → 7777 Len=107
2031… 2023-09-18 16:26:04.905225 172.18.138.91   255.255.255.255  UDP        149 7777 → 7777 Len=107
2033… 2023-09-18 16:26:07.905043 172.18.138.91   255.255.255.255  UDP        149 7777 → 7777 Len=107
2035… 2023-09-18 16:26:10.905227 172.18.138.91   255.255.255.255  UDP        149 7777 → 7777 Len=107
2037… 2023-09-18 16:26:13.905187 172.18.138.91   255.255.255.255  UDP        149 7777 → 7777 Len=107
2038… 2023-09-18 16:26:16.905286 172.18.138.91   255.255.255.255  UDP        149 7777 → 7777 Len=107
2040… 2023-09-18 16:26:19.905216 172.18.138.91   255.255.255.255  UDP        149 7777 → 7777 Len=107
```

(2)输入完毕后回车查看 此时可以看见源ip地址为172.18.138.91 目标地址为255.255.255.255的数据包

![

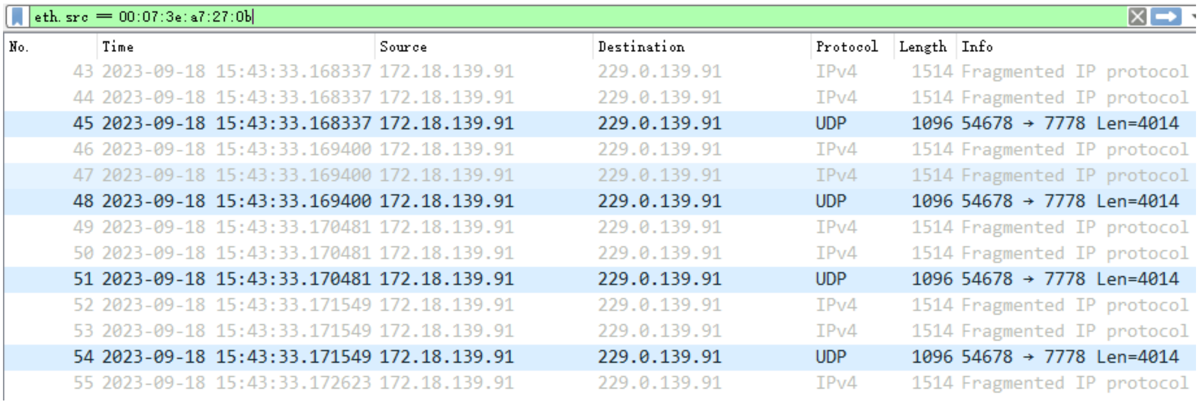


```
ip.src == 172.18.138.91 && ip.dst == 255.255.255.255

No.     Time                       Source          Destination      Protocol  Length  Info
2016… 2023-09-18 16:25:43.915211 172.18.138.91   255.255.255.255  UDP        148 7777 → 7777 Len=106
2018… 2023-09-18 16:25:46.915473 172.18.138.91   255.255.255.255  UDP        149 7777 → 7777 Len=107
2021… 2023-09-18 16:25:49.915016 172.18.138.91   255.255.255.255  UDP        149 7777 → 7777 Len=107
2023… 2023-09-18 16:25:52.915259 172.18.138.91   255.255.255.255  UDP        148 7777 → 7777 Len=106
2025… 2023-09-18 16:25:55.905185 172.18.138.91   255.255.255.255  UDP        149 7777 → 7777 Len=107
2027… 2023-09-18 16:25:58.905051 172.18.138.91   255.255.255.255  UDP        149 7777 → 7777 Len=107
2029… 2023-09-18 16:26:01.905017 172.18.138.91   255.255.255.255  UDP        149 7777 → 7777 Len=107
2031… 2023-09-18 16:26:04.905225 172.18.138.91   255.255.255.255  UDP        149 7777 → 7777 Len=107
2033… 2023-09-18 16:26:07.905043 172.18.138.91   255.255.255.255  UDP        149 7777 → 7777 Len=107
2035… 2023-09-18 16:26:10.905227 172.18.138.91   255.255.255.255  UDP        149 7777 → 7777 Len=107
2037… 2023-09-18 16:26:13.905187 172.18.138.91   255.255.255.255  UDP        149 7777 → 7777 Len=107
2038… 2023-09-18 16:26:16.905286 172.18.138.91   255.255.255.255  UDP        149 7777 → 7777 Len=107
2040… 2023-09-18 16:26:19.905216 172.18.138.91   255.255.255.255  UDP        149 7777 → 7777 Len=107
```

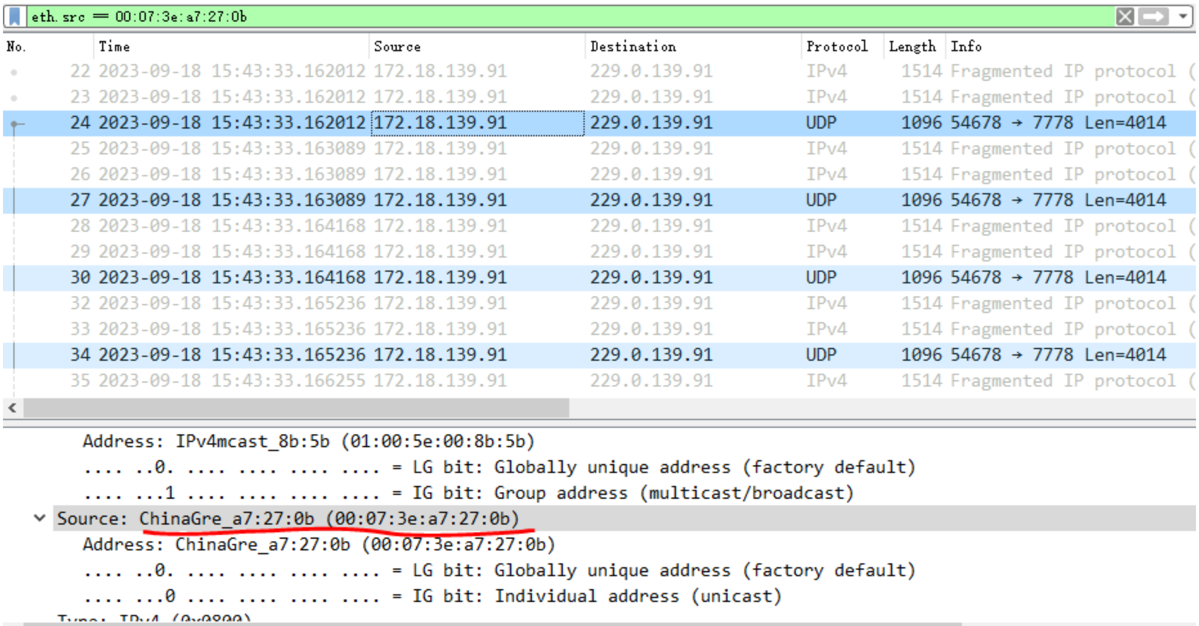
5.筛选出mac地址为eth.src == 00:07:3e:a7:27:0b的数据包

(1)搜索栏输入eth.src == 00:07:3e:a7:27:0b (背景为淡绿色是语法正确 否则就是语法有问题)



```
eth.src == 00:07:3e:a7:27:0b
No.   Time                       Source         Destination    Protocol Length Info
   43 2023-09-18 15:43:33.168337 172.18.139.91  229.0.139.91   IPv4     1514 Fragmented IP protocol
   44 2023-09-18 15:43:33.168337 172.18.139.91  229.0.139.91   IPv4     1514 Fragmented IP protocol
   45 2023-09-18 15:43:33.168337 172.18.139.91  229.0.139.91   UDP      1096 54678 → 7778 Len=4014
   46 2023-09-18 15:43:33.169400 172.18.139.91  229.0.139.91   IPv4     1514 Fragmented IP protocol
   47 2023-09-18 15:43:33.169400 172.18.139.91  229.0.139.91   IPv4     1514 Fragmented IP protocol
   48 2023-09-18 15:43:33.169400 172.18.139.91  229.0.139.91   UDP      1096 54678 → 7778 Len=4014
   49 2023-09-18 15:43:33.170481 172.18.139.91  229.0.139.91   IPv4     1514 Fragmented IP protocol
   50 2023-09-18 15:43:33.170481 172.18.139.91  229.0.139.91   IPv4     1514 Fragmented IP protocol
   51 2023-09-18 15:43:33.170481 172.18.139.91  229.0.139.91   UDP      1096 54678 → 7778 Len=4014
   52 2023-09-18 15:43:33.171549 172.18.139.91  229.0.139.91   IPv4     1514 Fragmented IP protocol
   53 2023-09-18 15:43:33.171549 172.18.139.91  229.0.139.91   IPv4     1514 Fragmented IP protocol
   54 2023-09-18 15:43:33.171549 172.18.139.91  229.0.139.91   UDP      1096 54678 → 7778 Len=4014
   55 2023-09-18 15:43:33.172623 172.18.139.91  229.0.139.91   IPv4     1514 Fragmented IP protocol
```

(2)输入完毕后回车查看 此时可以看见MAC地址为 00:07:3e:a7:27:0b的数据包

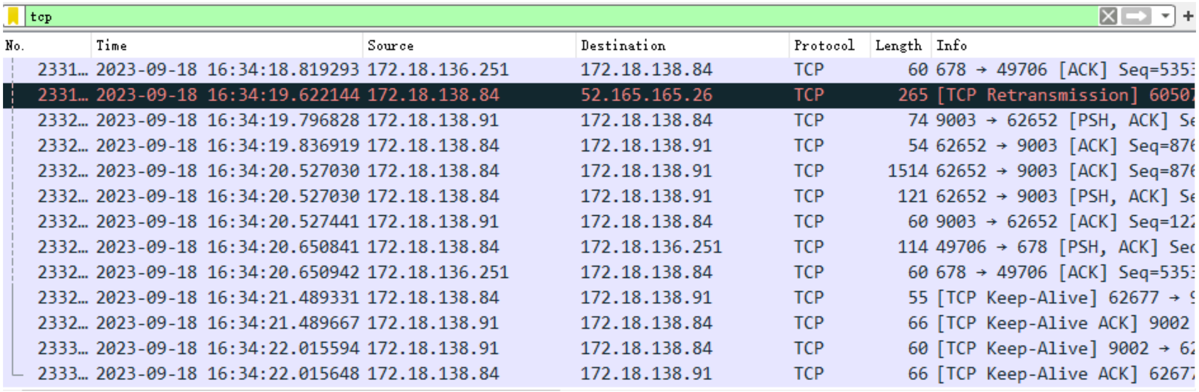


```
eth.src == 00:07:3e:a7:27:0b
No.   Time                       Source         Destination    Protocol Length Info
   22 2023-09-18 15:43:33.162012 172.18.139.91  229.0.139.91   IPv4     1514 Fragmented IP protocol (
   23 2023-09-18 15:43:33.162012 172.18.139.91  229.0.139.91   IPv4     1514 Fragmented IP protocol (
   24 2023-09-18 15:43:33.162012 172.18.139.91  229.0.139.91   UDP      1096 54678 → 7778 Len=4014
   25 2023-09-18 15:43:33.163089 172.18.139.91  229.0.139.91   IPv4     1514 Fragmented IP protocol (
   26 2023-09-18 15:43:33.163089 172.18.139.91  229.0.139.91   IPv4     1514 Fragmented IP protocol (
   27 2023-09-18 15:43:33.163089 172.18.139.91  229.0.139.91   UDP      1096 54678 → 7778 Len=4014
   28 2023-09-18 15:43:33.164168 172.18.139.91  229.0.139.91   IPv4     1514 Fragmented IP protocol (
   29 2023-09-18 15:43:33.164168 172.18.139.91  229.0.139.91   IPv4     1514 Fragmented IP protocol (
   30 2023-09-18 15:43:33.164168 172.18.139.91  229.0.139.91   UDP      1096 54678 → 7778 Len=4014
   32 2023-09-18 15:43:33.165236 172.18.139.91  229.0.139.91   IPv4     1514 Fragmented IP protocol (
   33 2023-09-18 15:43:33.165236 172.18.139.91  229.0.139.91   IPv4     1514 Fragmented IP protocol (
   34 2023-09-18 15:43:33.165236 172.18.139.91  229.0.139.91   UDP      1096 54678 → 7778 Len=4014
   35 2023-09-18 15:43:33.166255 172.18.139.91  229.0.139.91   IPv4     1514 Fragmented IP protocol (

        Address: IPv4mcast_8b:5b (01:00:5e:00:8b:5b)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
    Source: ChinaGre_a7:27:0b (00:07:3e:a7:27:0b)
        Address: ChinaGre_a7:27:0b (00:07:3e:a7:27:0b)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
```

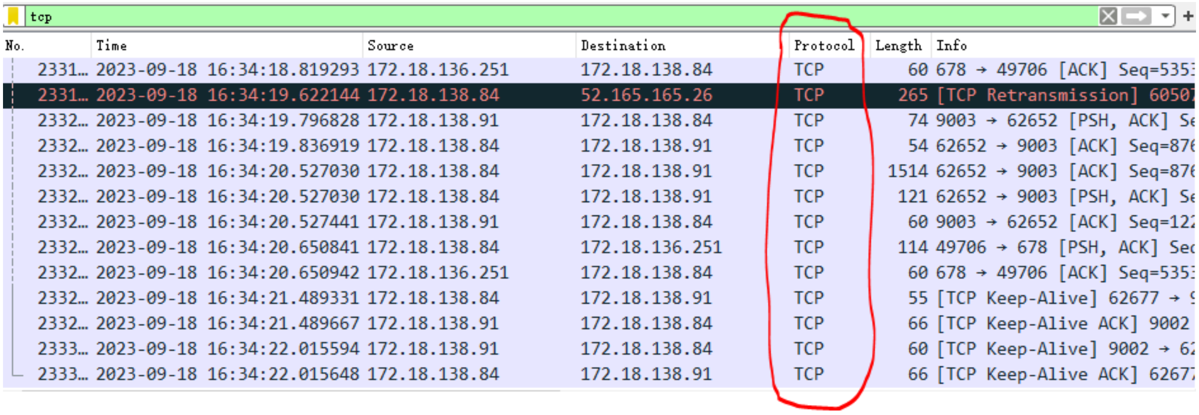
6.筛选出TCP的数据包

(1)搜索栏输入tcp (背景为淡绿色是语法正确 否则就是语法有问题)



```
tcp
No.   Time                       Source          Destination     Protocol Length Info
2331… 2023-09-18 16:34:18.819293 172.18.136.251  172.18.138.84   TCP        60 678 → 49706 [ACK] Seq=535
2331… 2023-09-18 16:34:19.622144 172.18.138.84   52.165.165.26   TCP       265 [TCP Retransmission] 6050
2332… 2023-09-18 16:34:19.796828 172.18.138.91   172.18.138.84   TCP        74 9003 → 62652 [PSH, ACK] Se
2332… 2023-09-18 16:34:19.836919 172.18.138.84   172.18.138.91   TCP        54 62652 → 9003 [ACK] Seq=87
2332… 2023-09-18 16:34:20.527030 172.18.138.84   172.18.138.91   TCP      1514 62652 → 9003 [ACK] Seq=87
2332… 2023-09-18 16:34:20.527030 172.18.138.84   172.18.138.91   TCP       121 62652 → 9003 [PSH, ACK] Se
2332… 2023-09-18 16:34:20.527441 172.18.138.91   172.18.138.84   TCP        60 9003 → 62652 [ACK] Seq=12
2332… 2023-09-18 16:34:20.650841 172.18.138.84   172.18.136.251  TCP       114 49706 → 678 [PSH, ACK] Se
2332… 2023-09-18 16:34:20.650942 172.18.136.251  172.18.138.84   TCP        60 678 → 49706 [ACK] Seq=535
2332… 2023-09-18 16:34:21.489331 172.18.138.84   172.18.138.91   TCP        55 [TCP Keep-Alive] 62677 →
2332… 2023-09-18 16:34:21.489667 172.18.138.91   172.18.138.84   TCP        66 [TCP Keep-Alive ACK] 9002
2333… 2023-09-18 16:34:22.015594 172.18.138.91   172.18.138.84   TCP        60 [TCP Keep-Alive] 9002 → 6
2333… 2023-09-18 16:34:22.015648 172.18.138.84   172.18.138.91   TCP        66 [TCP Keep-Alive ACK] 6267
```

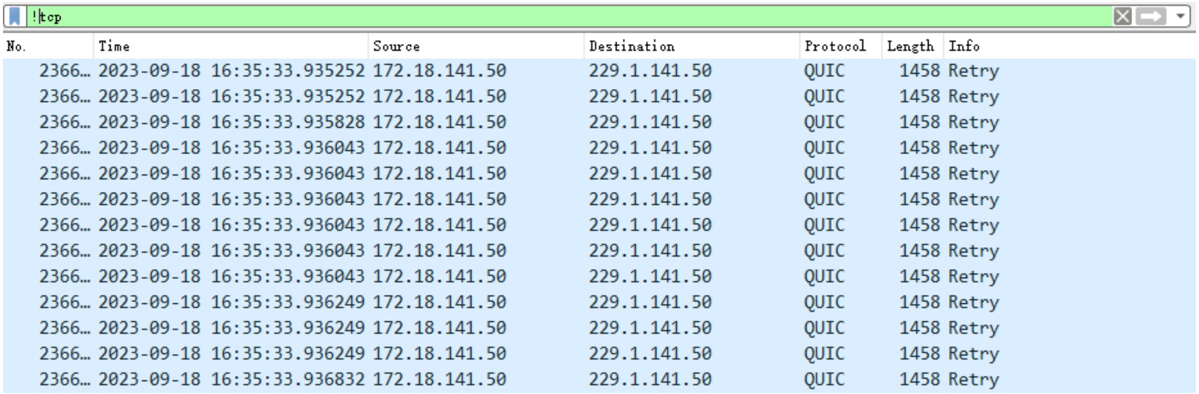
(2)输入完毕后回车查看 此时可以看见所有协议为TCP的数据包



```
tcp
No.    Time                       Source          Destination      Protocol  Length  Info
 2331… 2023-09-18 16:34:18.819293 172.18.136.251 172.18.138.84    TCP         60 678 → 49706 [ACK] Seq=535
 2331… 2023-09-18 16:34:19.622144 172.18.138.84  52.165.165.26    TCP        265 [TCP Retransmission] 6050
 2332… 2023-09-18 16:34:19.796828 172.18.138.91  172.18.138.84    TCP         74 9003 → 62652 [PSH, ACK] Se
 2332… 2023-09-18 16:34:19.836919 172.18.138.84  172.18.138.91    TCP         54 62652 → 9003 [ACK] Seq=87
 2332… 2023-09-18 16:34:20.527030 172.18.138.84  172.18.138.91    TCP       1514 62652 → 9003 [ACK] Seq=87
 2332… 2023-09-18 16:34:20.527030 172.18.138.84  172.18.138.91    TCP        121 62652 → 9003 [PSH, ACK] Se
 2332… 2023-09-18 16:34:20.527441 172.18.138.91  172.18.138.84    TCP         60 9003 → 62652 [ACK] Seq=12
 2332… 2023-09-18 16:34:20.650841 172.18.138.84  172.18.136.251   TCP        114 49706 → 678 [PSH, ACK] Sec
 2332… 2023-09-18 16:34:20.650942 172.18.136.251 172.18.138.84    TCP         60 678 → 49706 [ACK] Seq=535
 2332… 2023-09-18 16:34:21.489331 172.18.138.84  172.18.138.91    TCP         55 [TCP Keep-Alive] 62677 →
 2332… 2023-09-18 16:34:21.489667 172.18.138.91  172.18.138.84    TCP         66 [TCP Keep-Alive ACK] 9002
 2333… 2023-09-18 16:34:22.015594 172.18.138.91  172.18.138.84    TCP         60 [TCP Keep-Alive] 9002 → 6
 2333… 2023-09-18 16:34:22.015648 172.18.138.84  172.18.138.91    TCP         66 [TCP Keep-Alive ACK] 6267
```

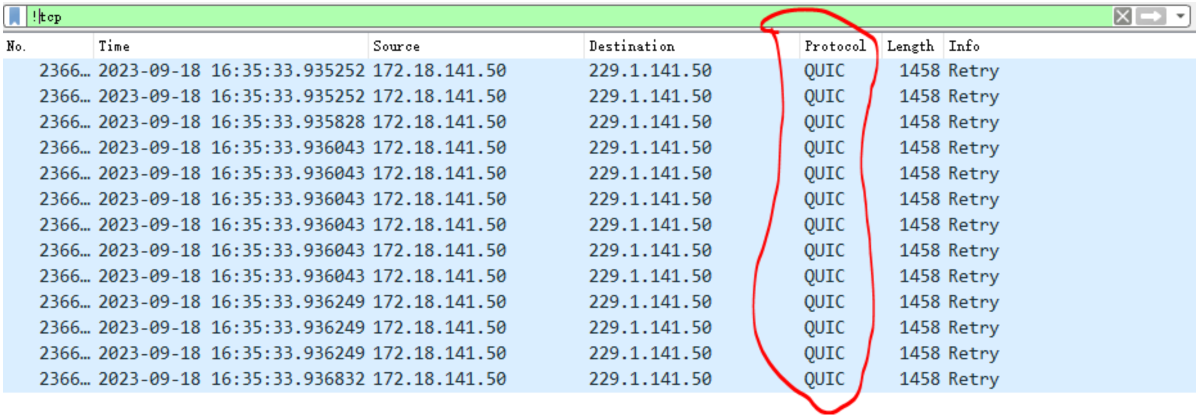
7.筛选出不是TCP的数据包

(1)搜索栏输入!tcp (背景为淡绿色是语法正确 否则就是语法有问题)



```
!tcp
No.    Time                       Source          Destination      Protocol  Length  Info
 2366… 2023-09-18 16:35:33.935252 172.18.141.50  229.1.141.50     QUIC      1458 Retry
 2366… 2023-09-18 16:35:33.935252 172.18.141.50  229.1.141.50     QUIC      1458 Retry
 2366… 2023-09-18 16:35:33.935828 172.18.141.50  229.1.141.50     QUIC      1458 Retry
 2366… 2023-09-18 16:35:33.936043 172.18.141.50  229.1.141.50     QUIC      1458 Retry
 2366… 2023-09-18 16:35:33.936043 172.18.141.50  229.1.141.50     QUIC      1458 Retry
 2366… 2023-09-18 16:35:33.936043 172.18.141.50  229.1.141.50     QUIC      1458 Retry
 2366… 2023-09-18 16:35:33.936043 172.18.141.50  229.1.141.50     QUIC      1458 Retry
 2366… 2023-09-18 16:35:33.936043 172.18.141.50  229.1.141.50     QUIC      1458 Retry
 2366… 2023-09-18 16:35:33.936043 172.18.141.50  229.1.141.50     QUIC      1458 Retry
 2366… 2023-09-18 16:35:33.936249 172.18.141.50  229.1.141.50     QUIC      1458 Retry
 2366… 2023-09-18 16:35:33.936249 172.18.141.50  229.1.141.50     QUIC      1458 Retry
 2366… 2023-09-18 16:35:33.936249 172.18.141.50  229.1.141.50     QUIC      1458 Retry
 2366… 2023-09-18 16:35:33.936832 172.18.141.50  229.1.141.50     QUIC      1458 Retry
```

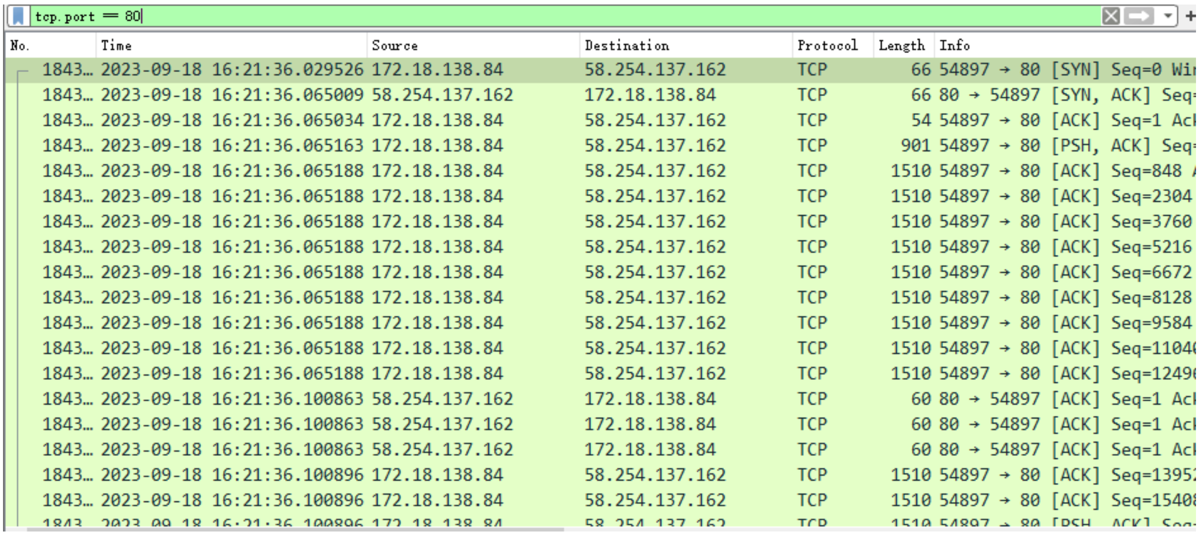
(2)输入完毕后回车查看 此时可以看见所有协议不为TCP的数据包



```
!tcp
No.    Time                       Source          Destination      Protocol  Length  Info
 2366… 2023-09-18 16:35:33.935252 172.18.141.50  229.1.141.50     QUIC      1458 Retry
 2366… 2023-09-18 16:35:33.935252 172.18.141.50  229.1.141.50     QUIC      1458 Retry
 2366… 2023-09-18 16:35:33.935828 172.18.141.50  229.1.141.50     QUIC      1458 Retry
 2366… 2023-09-18 16:35:33.936043 172.18.141.50  229.1.141.50     QUIC      1458 Retry
 2366… 2023-09-18 16:35:33.936043 172.18.141.50  229.1.141.50     QUIC      1458 Retry
 2366… 2023-09-18 16:35:33.936043 172.18.141.50  229.1.141.50     QUIC      1458 Retry
 2366… 2023-09-18 16:35:33.936043 172.18.141.50  229.1.141.50     QUIC      1458 Retry
 2366… 2023-09-18 16:35:33.936043 172.18.141.50  229.1.141.50     QUIC      1458 Retry
 2366… 2023-09-18 16:35:33.936043 172.18.141.50  229.1.141.50     QUIC      1458 Retry
 2366… 2023-09-18 16:35:33.936249 172.18.141.50  229.1.141.50     QUIC      1458 Retry
 2366… 2023-09-18 16:35:33.936249 172.18.141.50  229.1.141.50     QUIC      1458 Retry
 2366… 2023-09-18 16:35:33.936249 172.18.141.50  229.1.141.50     QUIC      1458 Retry
 2366… 2023-09-18 16:35:33.936832 172.18.141.50  229.1.141.50     QUIC      1458 Retry
```

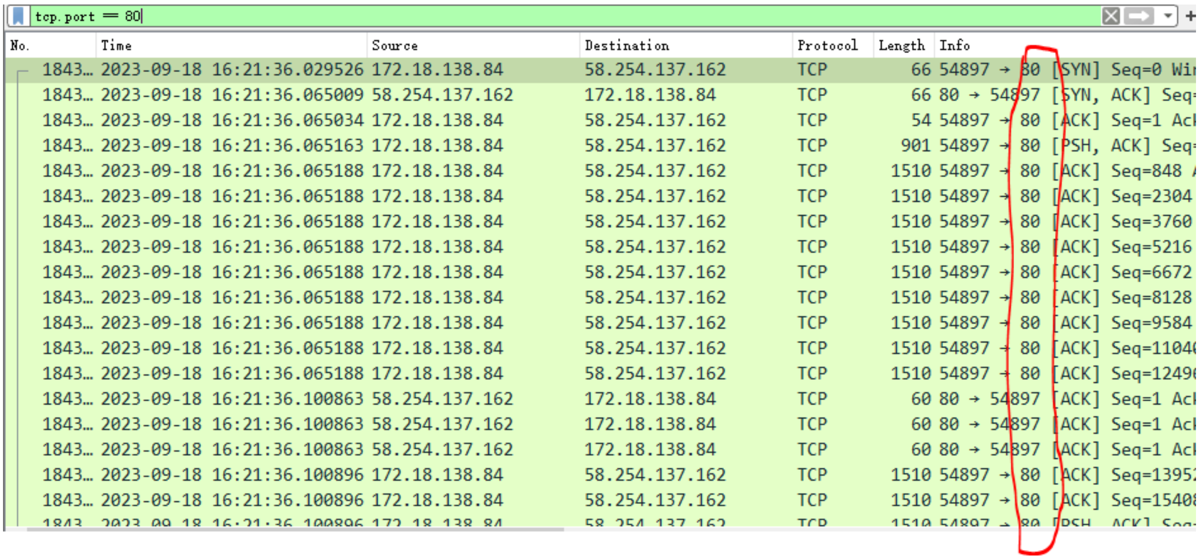
8.筛选出端口是80的数据包

(1)搜索栏输入tcp.port == 80 (背景为淡绿色是语法正确 否则就是语法有问题)



```
tcp.port == 80
No.     Time                        Source          Destination     Protocol Length Info
1843… 2023-09-18 16:21:36.029526 172.18.138.84   58.254.137.162  TCP        66 54897 → 80 [SYN] Seq=0 Wi
1843… 2023-09-18 16:21:36.065009 58.254.137.162  172.18.138.84   TCP        66 80 → 54897 [SYN, ACK] Seq=
1843… 2023-09-18 16:21:36.065034 172.18.138.84   58.254.137.162  TCP        54 54897 → 80 [ACK] Seq=1 Ac
1843… 2023-09-18 16:21:36.065163 172.18.138.84   58.254.137.162  TCP       901 54897 → 80 [PSH, ACK] Seq=
1843… 2023-09-18 16:21:36.065188 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=848 A
1843… 2023-09-18 16:21:36.065188 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=2304
1843… 2023-09-18 16:21:36.065188 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=3760
1843… 2023-09-18 16:21:36.065188 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=5216
1843… 2023-09-18 16:21:36.065188 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=6672
1843… 2023-09-18 16:21:36.065188 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=8128
1843… 2023-09-18 16:21:36.065188 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=9584
1843… 2023-09-18 16:21:36.065188 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=1104
1843… 2023-09-18 16:21:36.065188 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=1249
1843… 2023-09-18 16:21:36.100863 58.254.137.162  172.18.138.84   TCP        60 80 → 54897 [ACK] Seq=1 Ac
1843… 2023-09-18 16:21:36.100863 58.254.137.162  172.18.138.84   TCP        60 80 → 54897 [ACK] Seq=1 Ac
1843… 2023-09-18 16:21:36.100863 58.254.137.162  172.18.138.84   TCP        60 80 → 54897 [ACK] Seq=1 Ac
1843… 2023-09-18 16:21:36.100896 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=1395
1843… 2023-09-18 16:21:36.100896 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=1540
1843… 2023-09-18 16:21:36.100896 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [PSH, ACK] Seq=
```

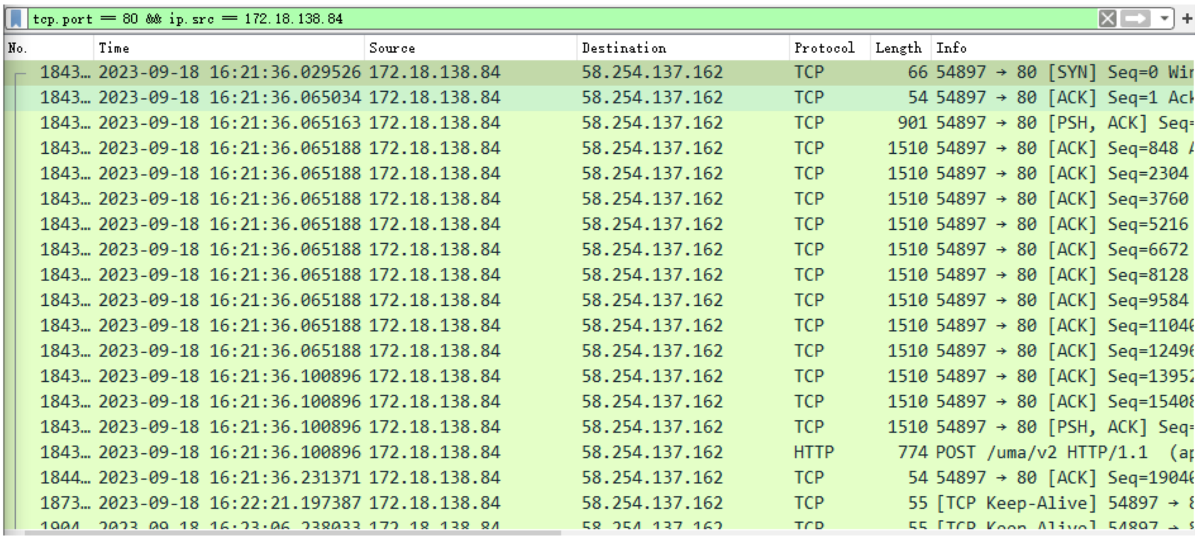
(2)输入完毕后回车查看 此时可以看见所有经过80的数据包



```
tcp.port == 80
No.     Time                        Source          Destination     Protocol Length Info
1843… 2023-09-18 16:21:36.029526 172.18.138.84   58.254.137.162  TCP        66 54897 → 80 [SYN] Seq=0 Wi
1843… 2023-09-18 16:21:36.065009 58.254.137.162  172.18.138.84   TCP        66 80 → 54897 [SYN, ACK] Seq=
1843… 2023-09-18 16:21:36.065034 172.18.138.84   58.254.137.162  TCP        54 54897 → 80 [ACK] Seq=1 Ac
1843… 2023-09-18 16:21:36.065163 172.18.138.84   58.254.137.162  TCP       901 54897 → 80 [PSH, ACK] Seq=
1843… 2023-09-18 16:21:36.065188 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=848 A
1843… 2023-09-18 16:21:36.065188 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=2304
1843… 2023-09-18 16:21:36.065188 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=3760
1843… 2023-09-18 16:21:36.065188 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=5216
1843… 2023-09-18 16:21:36.065188 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=6672
1843… 2023-09-18 16:21:36.065188 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=8128
1843… 2023-09-18 16:21:36.065188 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=9584
1843… 2023-09-18 16:21:36.065188 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=1104
1843… 2023-09-18 16:21:36.065188 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=1249
1843… 2023-09-18 16:21:36.100863 58.254.137.162  172.18.138.84   TCP        60 80 → 54897 [ACK] Seq=1 Ac
1843… 2023-09-18 16:21:36.100863 58.254.137.162  172.18.138.84   TCP        60 80 → 54897 [ACK] Seq=1 Ac
1843… 2023-09-18 16:21:36.100863 58.254.137.162  172.18.138.84   TCP        60 80 → 54897 [ACK] Seq=1 Ac
1843… 2023-09-18 16:21:36.100896 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=1395
1843… 2023-09-18 16:21:36.100896 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=1540
1843… 2023-09-18 16:21:36.100896 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [PSH, ACK] Seq=
```

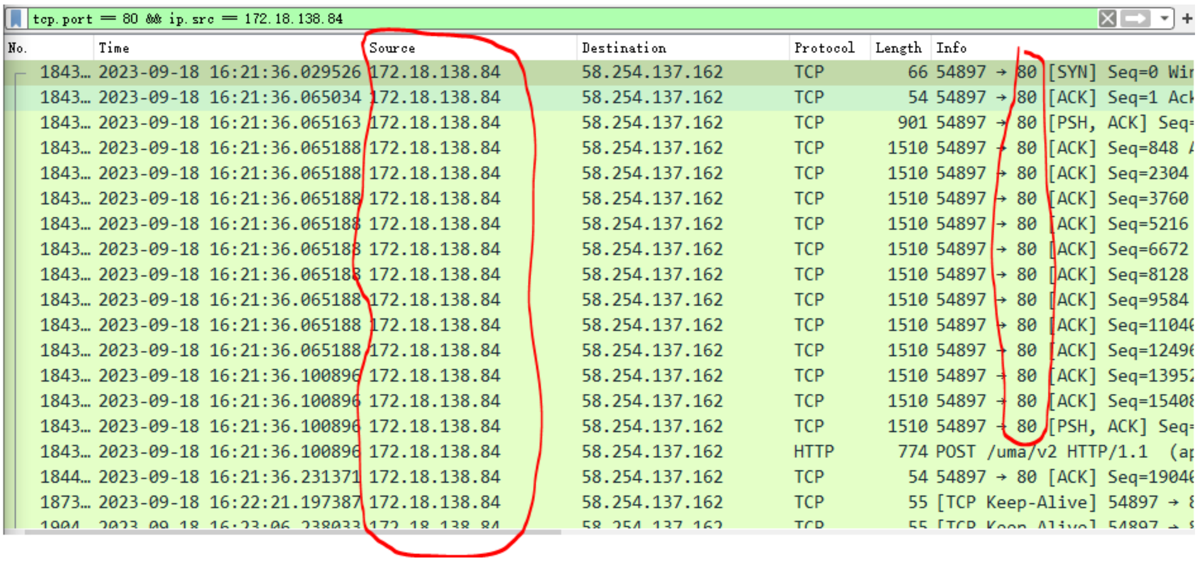
9.筛选出指定的源IP地址为172.18.138.84并且端口是80的数据包

(1)搜索栏输入tcp.port == 80 && ip.src == 172.18.138.84 (背景为淡绿色是语法正确 否则就是语法有问题)



```
tcp.port == 80 && ip.src == 172.18.138.84
No.     Time                        Source          Destination     Protocol Length Info
1843… 2023-09-18 16:21:36.029526 172.18.138.84   58.254.137.162  TCP        66 54897 → 80 [SYN] Seq=0 Wi
1843… 2023-09-18 16:21:36.065034 172.18.138.84   58.254.137.162  TCP        54 54897 → 80 [ACK] Seq=1 Ack
1843… 2023-09-18 16:21:36.065163 172.18.138.84   58.254.137.162  TCP       901 54897 → 80 [PSH, ACK] Seq=
1843… 2023-09-18 16:21:36.065188 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=848 A
1843… 2023-09-18 16:21:36.065188 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=2304
1843… 2023-09-18 16:21:36.065188 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=3760
1843… 2023-09-18 16:21:36.065188 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=5216
1843… 2023-09-18 16:21:36.065188 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=6672
1843… 2023-09-18 16:21:36.065188 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=8128
1843… 2023-09-18 16:21:36.065188 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=9584
1843… 2023-09-18 16:21:36.065188 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=1104
1843… 2023-09-18 16:21:36.065188 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=1249
1843… 2023-09-18 16:21:36.100896 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=1395
1843… 2023-09-18 16:21:36.100896 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [ACK] Seq=1540
1843… 2023-09-18 16:21:36.100896 172.18.138.84   58.254.137.162  TCP      1510 54897 → 80 [PSH, ACK] Seq=
1843… 2023-09-18 16:21:36.100896 172.18.138.84   58.254.137.162  HTTP      774 POST /uma/v2 HTTP/1.1  (ap
1844… 2023-09-18 16:21:36.231371 172.18.138.84   58.254.137.162  TCP        54 54897 → 80 [ACK] Seq=1904
1873… 2023-09-18 16:22:21.197387 172.18.138.84   58.254.137.162  TCP        55 [TCP Keep-Alive] 54897 → 8
1904… 2023-09-18 16:23:06.238033 172.18.138.84   58.254.137.162  TCP        55 [TCP Keep-Alive] 54897 → 8
```

(2)输入完毕后回车查看 此时可以看见端口是80并且源ip是172.18.138.84的数据包

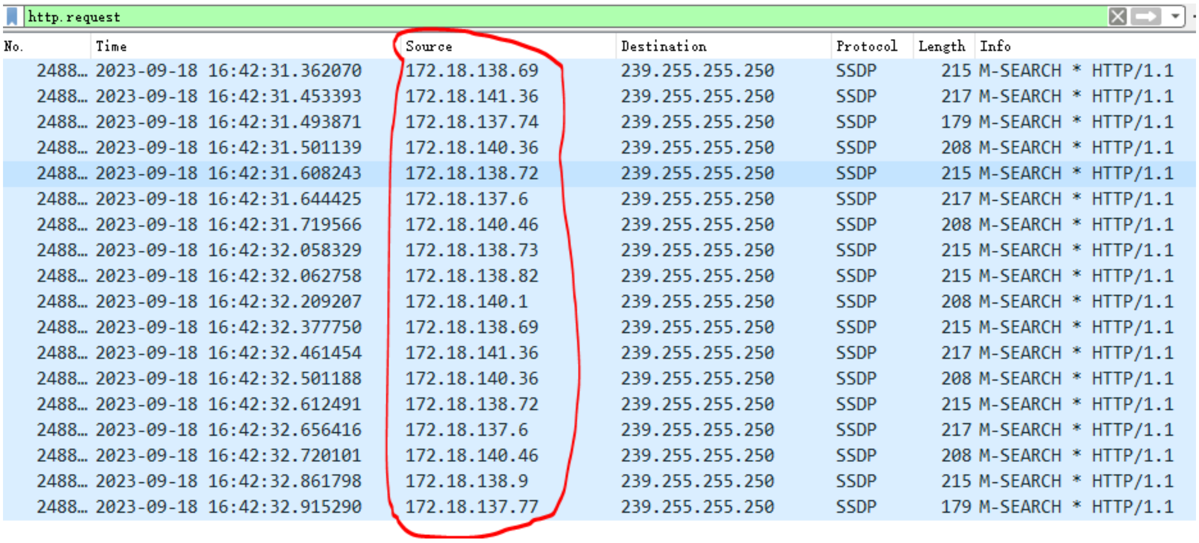


tcp.port == 80 && ip.src == 172.18.138.84

No.	Time	Source	Destination	Protocol	Length	Info
1843…	2023-09-18 16:21:36.029526	172.18.138.84	58.254.137.162	TCP	66	54897 → 80 [SYN] Seq=0 Wir
1843…	2023-09-18 16:21:36.065034	172.18.138.84	58.254.137.162	TCP	54	54897 → 80 [ACK] Seq=1 Ack
1843…	2023-09-18 16:21:36.065163	172.18.138.84	58.254.137.162	TCP	901	54897 → 80 [PSH, ACK] Seq=
1843…	2023-09-18 16:21:36.065188	172.18.138.84	58.254.137.162	TCP	1510	54897 → 80 [ACK] Seq=848 A
1843…	2023-09-18 16:21:36.065188	172.18.138.84	58.254.137.162	TCP	1510	54897 → 80 [ACK] Seq=2304
1843…	2023-09-18 16:21:36.065188	172.18.138.84	58.254.137.162	TCP	1510	54897 → 80 [ACK] Seq=3760
1843…	2023-09-18 16:21:36.065188	172.18.138.84	58.254.137.162	TCP	1510	54897 → 80 [ACK] Seq=5216
1843…	2023-09-18 16:21:36.065188	172.18.138.84	58.254.137.162	TCP	1510	54897 → 80 [ACK] Seq=6672
1843…	2023-09-18 16:21:36.065188	172.18.138.84	58.254.137.162	TCP	1510	54897 → 80 [ACK] Seq=8128
1843…	2023-09-18 16:21:36.065188	172.18.138.84	58.254.137.162	TCP	1510	54897 → 80 [ACK] Seq=9584
1843…	2023-09-18 16:21:36.065188	172.18.138.84	58.254.137.162	TCP	1510	54897 → 80 [ACK] Seq=1104
1843…	2023-09-18 16:21:36.065188	172.18.138.84	58.254.137.162	TCP	1510	54897 → 80 [ACK] Seq=1249
1843…	2023-09-18 16:21:36.100896	172.18.138.84	58.254.137.162	TCP	1510	54897 → 80 [ACK] Seq=1395
1843…	2023-09-18 16:21:36.100896	172.18.138.84	58.254.137.162	TCP	1510	54897 → 80 [ACK] Seq=1540
1843…	2023-09-18 16:21:36.100896	172.18.138.84	58.254.137.162	TCP	1510	54897 → 80 [PSH, ACK] Seq=
1843…	2023-09-18 16:21:36.100896	172.18.138.84	58.254.137.162	HTTP	774	POST /uma/v2 HTTP/1.1 (ap
1844…	2023-09-18 16:21:36.231371	172.18.138.84	58.254.137.162	TCP	54	54897 → 80 [ACK] Seq=1904
1873…	2023-09-18 16:22:21.197387	172.18.138.84	58.254.137.162	TCP	55	[TCP Keep-Alive] 54897 → 8
1904…	2023-09-18 16:23:06.238033	172.18.138.84	58.254.137.162	TCP	55	[TCP Keep-Alive] 54897 → 8

10.应用层过滤

(1)搜索栏输入http.request (背景为淡绿色是语法正确 否则就是语法有问题)

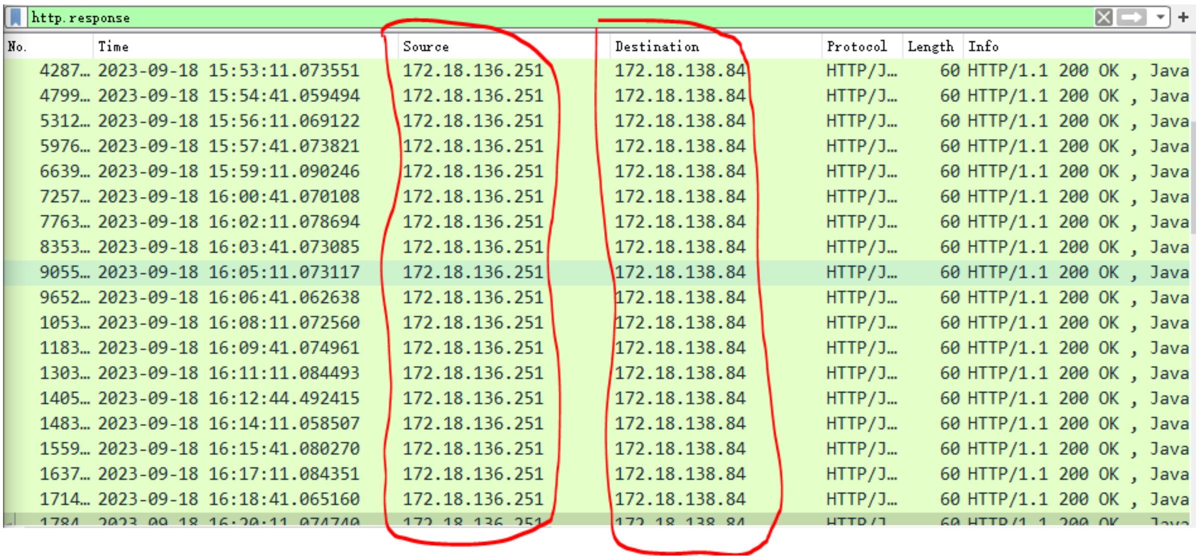


http.request

No.	Time	Source	Destination	Protocol	Length	Info
2488…	2023-09-18 16:42:31.362070	172.18.138.69	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
2488…	2023-09-18 16:42:31.453393	172.18.141.36	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
2488…	2023-09-18 16:42:31.493871	172.18.137.74	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
2488…	2023-09-18 16:42:31.501139	172.18.140.36	239.255.255.250	SSDP	208	M-SEARCH * HTTP/1.1
2488…	2023-09-18 16:42:31.608243	172.18.138.72	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
2488…	2023-09-18 16:42:31.644425	172.18.137.6	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
2488…	2023-09-18 16:42:31.719566	172.18.140.46	239.255.255.250	SSDP	208	M-SEARCH * HTTP/1.1
2488…	2023-09-18 16:42:32.058329	172.18.138.73	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
2488…	2023-09-18 16:42:32.062758	172.18.138.82	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
2488…	2023-09-18 16:42:32.209207	172.18.140.1	239.255.255.250	SSDP	208	M-SEARCH * HTTP/1.1
2488…	2023-09-18 16:42:32.377750	172.18.138.69	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
2488…	2023-09-18 16:42:32.461454	172.18.141.36	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
2488…	2023-09-18 16:42:32.501188	172.18.140.36	239.255.255.250	SSDP	208	M-SEARCH * HTTP/1.1
2488…	2023-09-18 16:42:32.612491	172.18.138.72	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
2488…	2023-09-18 16:42:32.656416	172.18.137.6	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
2488…	2023-09-18 16:42:32.720101	172.18.140.46	239.255.255.250	SSDP	208	M-SEARCH * HTTP/1.1
2488…	2023-09-18 16:42:32.861798	172.18.138.9	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
2488…	2023-09-18 16:42:32.915290	172.18.137.77	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1

源IP地址在变化 目标ip地址都是239.255.255.250

(2)搜索栏输入http.response (背景为淡绿色是语法正确 否则就是语法有问题)

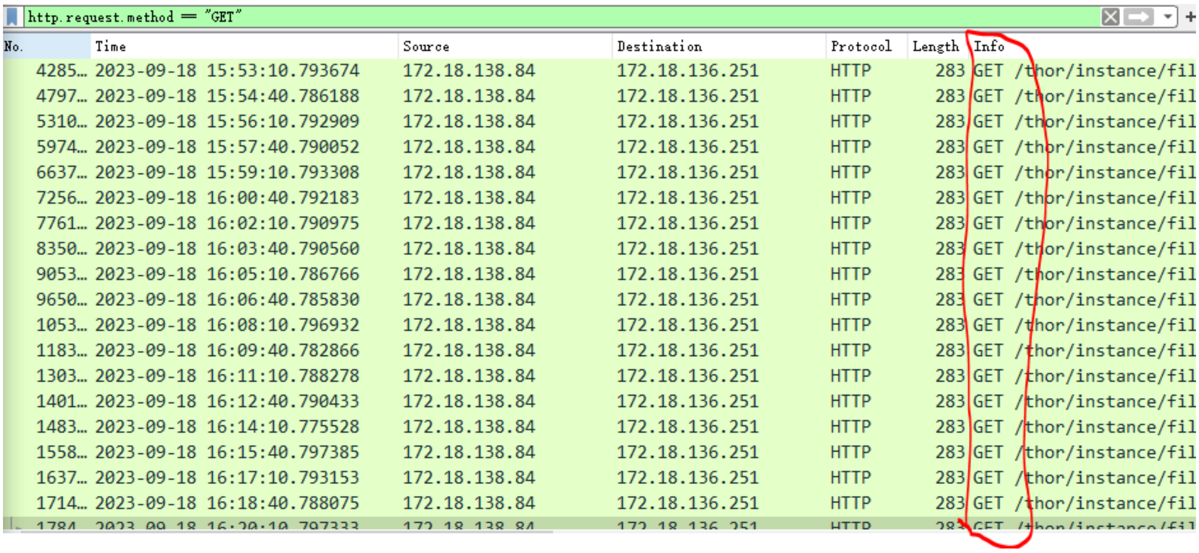


http.response

No.	Time	Source	Destination	Protocol	Length	Info
4287…	2023-09-18 15:53:11.073551	172.18.136.251	172.18.138.84	HTTP/J…	60	HTTP/1.1 200 OK , Java
4799…	2023-09-18 15:54:41.059494	172.18.136.251	172.18.138.84	HTTP/J…	60	HTTP/1.1 200 OK , Java
5312…	2023-09-18 15:56:11.069122	172.18.136.251	172.18.138.84	HTTP/J…	60	HTTP/1.1 200 OK , Java
5976…	2023-09-18 15:57:41.073821	172.18.136.251	172.18.138.84	HTTP/J…	60	HTTP/1.1 200 OK , Java
6639…	2023-09-18 15:59:11.090246	172.18.136.251	172.18.138.84	HTTP/J…	60	HTTP/1.1 200 OK , Java
7257…	2023-09-18 16:00:41.070108	172.18.136.251	172.18.138.84	HTTP/J…	60	HTTP/1.1 200 OK , Java
7763…	2023-09-18 16:02:11.078694	172.18.136.251	172.18.138.84	HTTP/J…	60	HTTP/1.1 200 OK , Java
8353…	2023-09-18 16:03:41.073085	172.18.136.251	172.18.138.84	HTTP/J…	60	HTTP/1.1 200 OK , Java
9055…	2023-09-18 16:05:11.073117	172.18.136.251	172.18.138.84	HTTP/J…	60	HTTP/1.1 200 OK , Java
9652…	2023-09-18 16:06:41.062638	172.18.136.251	172.18.138.84	HTTP/J…	60	HTTP/1.1 200 OK , Java
1053…	2023-09-18 16:08:11.072560	172.18.136.251	172.18.138.84	HTTP/J…	60	HTTP/1.1 200 OK , Java
1183…	2023-09-18 16:09:41.074961	172.18.136.251	172.18.138.84	HTTP/J…	60	HTTP/1.1 200 OK , Java
1303…	2023-09-18 16:11:11.084493	172.18.136.251	172.18.138.84	HTTP/J…	60	HTTP/1.1 200 OK , Java
1405…	2023-09-18 16:12:44.492415	172.18.136.251	172.18.138.84	HTTP/J…	60	HTTP/1.1 200 OK , Java
1483…	2023-09-18 16:14:11.058507	172.18.136.251	172.18.138.84	HTTP/J…	60	HTTP/1.1 200 OK , Java
1559…	2023-09-18 16:15:41.080270	172.18.136.251	172.18.138.84	HTTP/J…	60	HTTP/1.1 200 OK , Java
1637…	2023-09-18 16:17:11.084351	172.18.136.251	172.18.138.84	HTTP/J…	60	HTTP/1.1 200 OK , Java
1714…	2023-09-18 16:18:41.065160	172.18.136.251	172.18.138.84	HTTP/J…	60	HTTP/1.1 200 OK , Java
1784…	2023-09-18 16:20:11.074740	172.18.136.251	172.18.138.84	HTTP/J…	60	HTTP/1.1 200 OK , Java

部分的源IP和目标IP相同

(2)搜索栏输入http.request.method == "GET" (背景为淡绿色是语法正确 否则就是语法有问题)

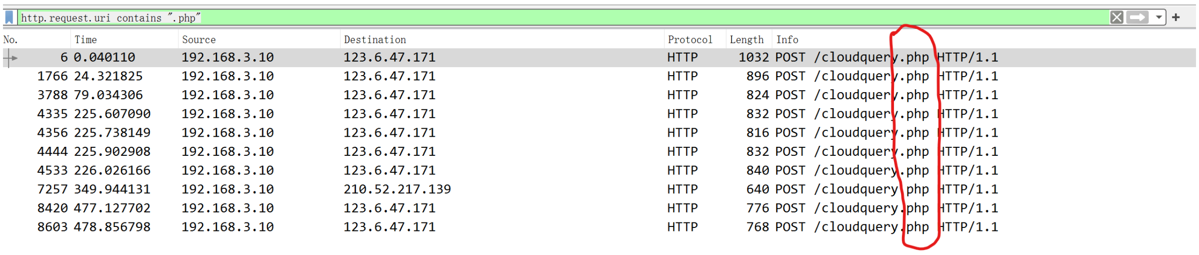


http.request.method == "GET"

No.	Time	Source	Destination	Protocol	Length	Info
4285…	2023-09-18 15:53:10.793674	172.18.138.84	172.18.136.251	HTTP	283	GET /thor/instance/fil
4797…	2023-09-18 15:54:40.786188	172.18.138.84	172.18.136.251	HTTP	283	GET /thor/instance/fil
5310…	2023-09-18 15:56:10.792909	172.18.138.84	172.18.136.251	HTTP	283	GET /thor/instance/fil
5974…	2023-09-18 15:57:40.790052	172.18.138.84	172.18.136.251	HTTP	283	GET /thor/instance/fil
6637…	2023-09-18 15:59:10.793308	172.18.138.84	172.18.136.251	HTTP	283	GET /thor/instance/fil
7256…	2023-09-18 16:00:40.792183	172.18.138.84	172.18.136.251	HTTP	283	GET /thor/instance/fil
7761…	2023-09-18 16:02:10.790975	172.18.138.84	172.18.136.251	HTTP	283	GET /thor/instance/fil
8350…	2023-09-18 16:03:40.790560	172.18.138.84	172.18.136.251	HTTP	283	GET /thor/instance/fil
9053…	2023-09-18 16:05:10.786766	172.18.138.84	172.18.136.251	HTTP	283	GET /thor/instance/fil
9650…	2023-09-18 16:06:40.785830	172.18.138.84	172.18.136.251	HTTP	283	GET /thor/instance/fil
1053…	2023-09-18 16:08:10.796932	172.18.138.84	172.18.136.251	HTTP	283	GET /thor/instance/fil
1183…	2023-09-18 16:09:40.782866	172.18.138.84	172.18.136.251	HTTP	283	GET /thor/instance/fil
1303…	2023-09-18 16:11:10.788278	172.18.138.84	172.18.136.251	HTTP	283	GET /thor/instance/fil
1401…	2023-09-18 16:12:40.790433	172.18.138.84	172.18.136.251	HTTP	283	GET /thor/instance/fil
1483…	2023-09-18 16:14:10.775528	172.18.138.84	172.18.136.251	HTTP	283	GET /thor/instance/fil
1558…	2023-09-18 16:15:40.797385	172.18.138.84	172.18.136.251	HTTP	283	GET /thor/instance/fil
1637…	2023-09-18 16:17:10.793153	172.18.138.84	172.18.136.251	HTTP	283	GET /thor/instance/fil
1714…	2023-09-18 16:18:40.788075	172.18.138.84	172.18.136.251	HTTP	283	GET /thor/instance/fil
1784…	2023-09-18 16:20:10.797333	172.18.138.84	172.18.136.251	HTTP	283	GET /thor/instance/fil

页面信息都显示HTTP GET方法的请求

(3)搜索栏输入http.request.uri contains ".php"(背景为淡绿色是语法正确 否则就是语法有问题)

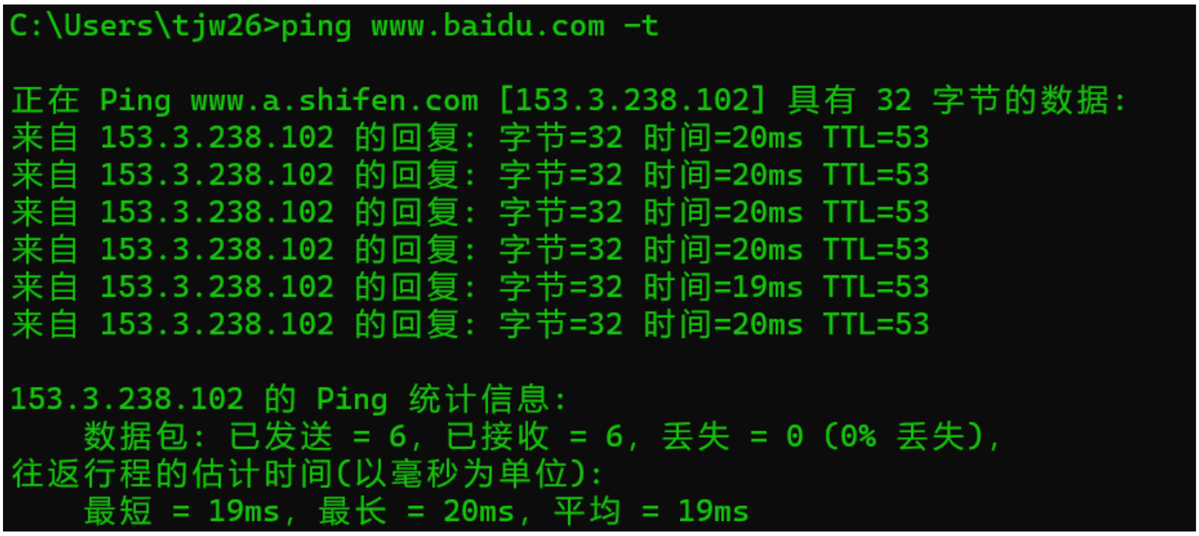


http.request.uri contains ".php"

No.	Time	Source	Destination	Protocol	Length	Info
6	0.040110	192.168.3.10	123.6.47.171	HTTP	1032	POST /cloudquery.php HTTP/1.1
1766	24.321825	192.168.3.10	123.6.47.171	HTTP	896	POST /cloudquery.php HTTP/1.1
3788	79.034306	192.168.3.10	123.6.47.171	HTTP	824	POST /cloudquery.php HTTP/1.1
4335	225.607090	192.168.3.10	123.6.47.171	HTTP	832	POST /cloudquery.php HTTP/1.1
4356	225.738149	192.168.3.10	123.6.47.171	HTTP	816	POST /cloudquery.php HTTP/1.1
4444	225.902908	192.168.3.10	123.6.47.171	HTTP	832	POST /cloudquery.php HTTP/1.1
4533	226.026166	192.168.3.10	123.6.47.171	HTTP	840	POST /cloudquery.php HTTP/1.1
7257	349.944131	192.168.3.10	210.52.217.139	HTTP	640	POST /cloudquery.php HTTP/1.1
8420	477.127702	192.168.3.10	123.6.47.171	HTTP	776	POST /cloudquery.php HTTP/1.1
8603	478.856798	192.168.3.10	123.6.47.171	HTTP	768	POST /cloudquery.php HTTP/1.1

11.使用ICMP协议抓取百度的数据包

(1)在cmd下执行ping www.baidu.com -t 命令 显示百度的IP地址为153.3.238.102

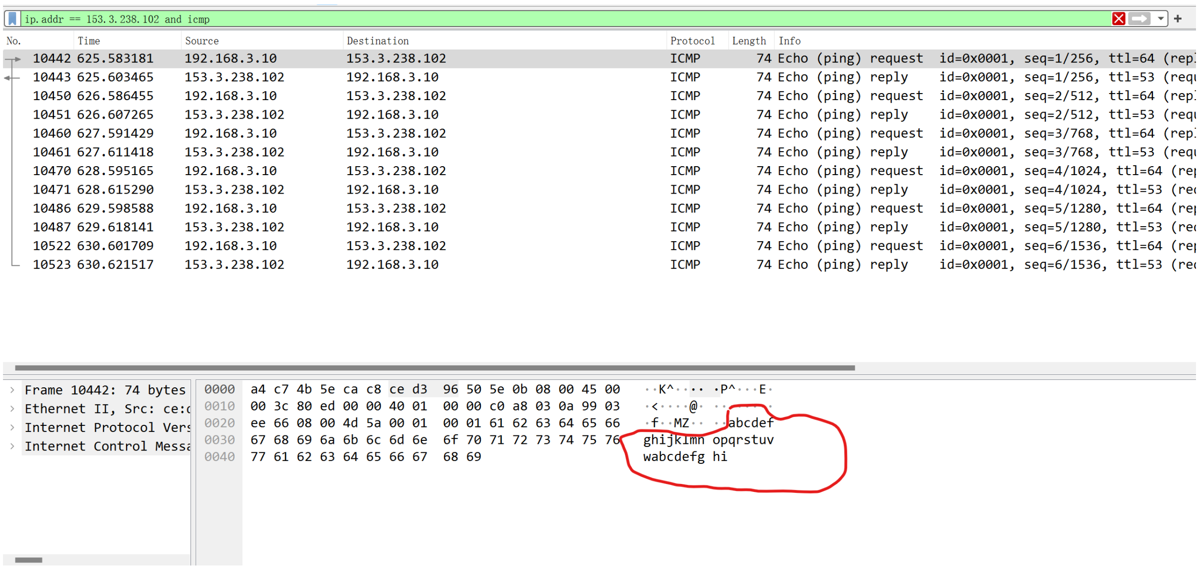


```
C:\Users\tjw26>ping www.baidu.com -t

正在 Ping www.a.shifen.com [153.3.238.102] 具有 32 字节的数据:
来自 153.3.238.102 的回复: 字节=32 时间=20ms TTL=53
来自 153.3.238.102 的回复: 字节=32 时间=20ms TTL=53
来自 153.3.238.102 的回复: 字节=32 时间=20ms TTL=53
来自 153.3.238.102 的回复: 字节=32 时间=20ms TTL=53
来自 153.3.238.102 的回复: 字节=32 时间=19ms TTL=53
来自 153.3.238.102 的回复: 字节=32 时间=20ms TTL=53

153.3.238.102 的 Ping 统计信息:
    数据包: 已发送 = 6，已接收 = 6，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 19ms，最长 = 20ms，平均 = 19ms
```

(2)在Wireshark中输入 ip.addr == 153.3.238.102 and icmp

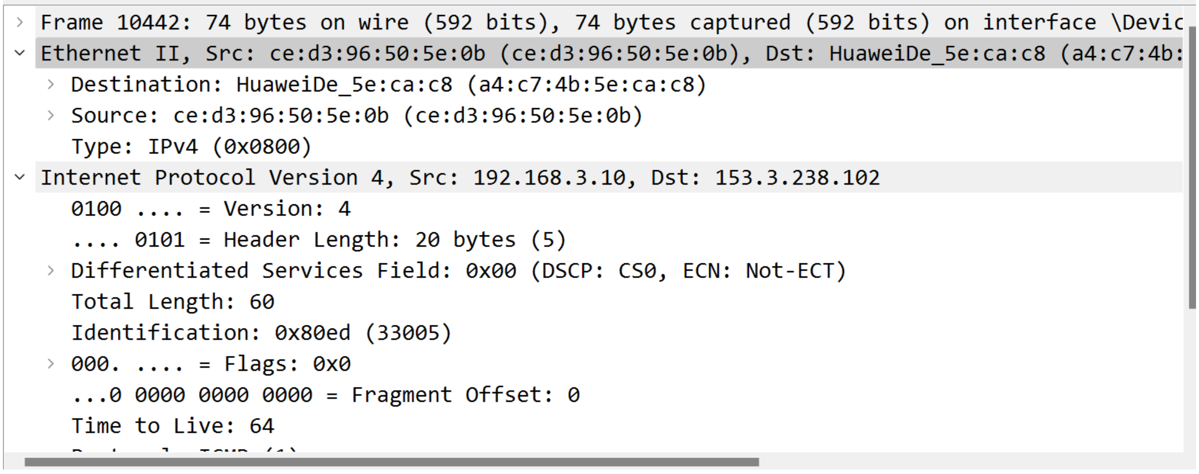


ip.addr == 153.3.238.102 and icmp

```
No.   Time       Source          Destination     Protocol Length Info
10442 625.583181 192.168.3.10    153.3.238.102   ICMP     74 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (repl
10443 625.603465 153.3.238.102   192.168.3.10    ICMP     74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=53 (requ
10450 626.586455 192.168.3.10    153.3.238.102   ICMP     74 Echo (ping) request  id=0x0001, seq=2/512, ttl=64 (repl
10451 626.607265 153.3.238.102   192.168.3.10    ICMP     74 Echo (ping) reply    id=0x0001, seq=2/512, ttl=53 (requ
10460 627.591429 192.168.3.10    153.3.238.102   ICMP     74 Echo (ping) request  id=0x0001, seq=3/768, ttl=64 (repl
10461 627.611418 153.3.238.102   192.168.3.10    ICMP     74 Echo (ping) reply    id=0x0001, seq=3/768, ttl=53 (requ
10470 628.595165 192.168.3.10    153.3.238.102   ICMP     74 Echo (ping) request  id=0x0001, seq=4/1024, ttl=64 (rep
10471 628.615290 153.3.238.102   192.168.3.10    ICMP     74 Echo (ping) reply    id=0x0001, seq=4/1024, ttl=53 (req
10486 629.598588 192.168.3.10    153.3.238.102   ICMP     74 Echo (ping) request  id=0x0001, seq=5/1280, ttl=64 (rep
10487 629.618141 153.3.238.102   192.168.3.10    ICMP     74 Echo (ping) reply    id=0x0001, seq=5/1280, ttl=53 (req
10522 630.601709 192.168.3.10    153.3.238.102   ICMP     74 Echo (ping) request  id=0x0001, seq=6/1536, ttl=64 (rep
10523 630.621517 153.3.238.102   192.168.3.10    ICMP     74 Echo (ping) reply    id=0x0001, seq=6/1536, ttl=53 (req
```

```
> Frame 10442: 74 bytes      0000  a4 c7 4b 5e ca c8 ce d3  96 50 5e 0b 08 00 45 00   ··K^···· ·P^···E·
> Ethernet II, Src: ce:c     0010  00 3c 80 ed 00 00 40 01  00 00 c0 a8 03 0a 99 03   ·<····@· ········
> Internet Protocol Vers     0020  ee 66 08 00 4d 5a 00 01  00 01 61 62 63 64 65 66   ·f··MZ·· ··abcdef
> Internet Control Messa     0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
                             0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

(3)单击串口左侧三角，可显示抓到的数据包的详细信息



```
> Frame 10442: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Devic
v Ethernet II, Src: ce:d3:96:50:5e:0b (ce:d3:96:50:5e:0b), Dst: HuaweiDe_5e:ca:c8 (a4:c7:4b:
  > Destination: HuaweiDe_5e:ca:c8 (a4:c7:4b:5e:ca:c8)
  > Source: ce:d3:96:50:5e:0b (ce:d3:96:50:5e:0b)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 192.168.3.10, Dst: 153.3.238.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x80ed (33005)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
```