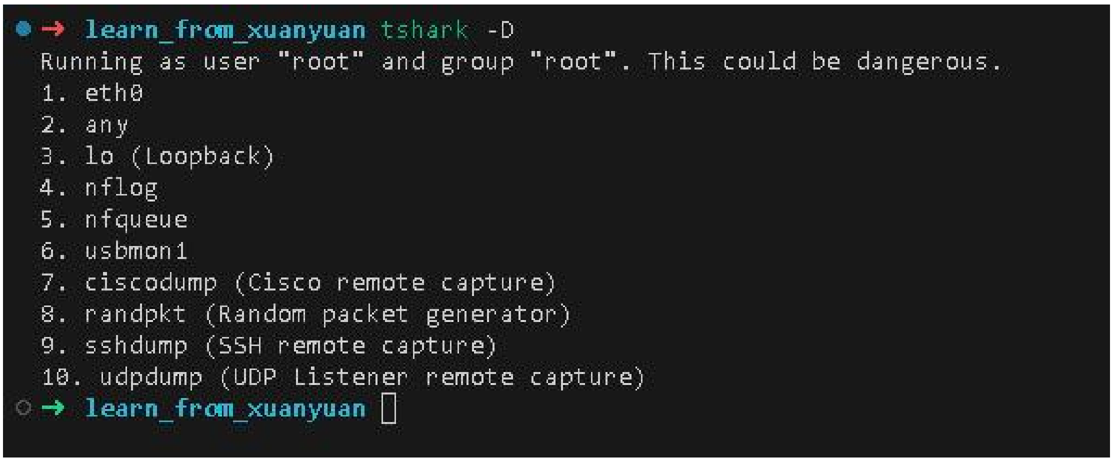
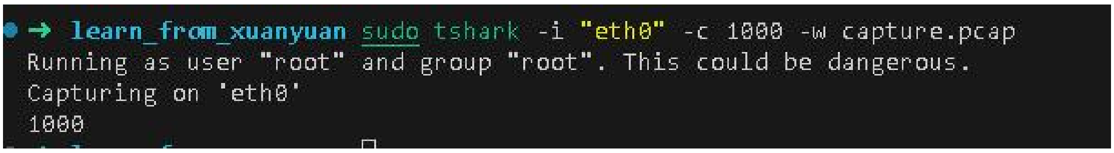
## tshark 命令练习

tshark -D 查看网卡



```
● → learn_from_xuanyuan tshark -D
  Running as user "root" and group "root". This could be dangerous.
  1. eth0
  2. any
  3. lo (Loopback)
  4. nflog
  5. nfqueue
  6. usbmon1
  7. ciscodump (Cisco remote capture)
  8. randpkt (Random packet generator)
  9. sshdump (SSH remote capture)
  10. udpdump (UDP Listener remote capture)
○ → learn_from_xuanyuan
```

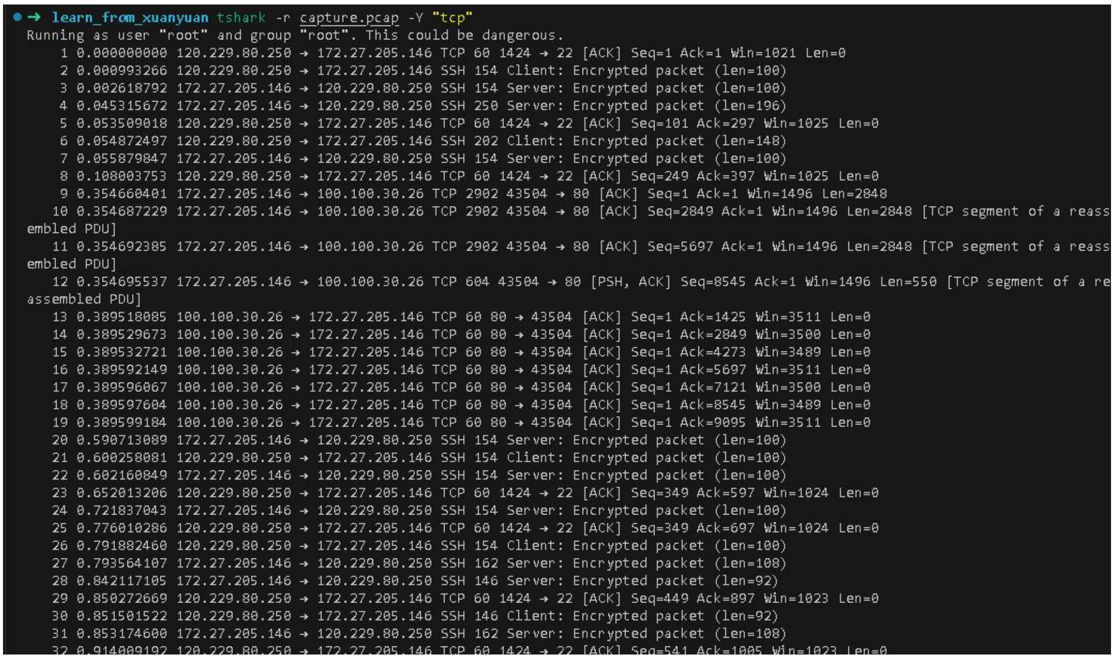
tshark -i “eth0” -c 1000 -w capture.pcap



```
● → learn_from_xuanyuan sudo tshark -i "eth0" -c 1000 -w capture.pcap
  Running as user "root" and group "root". This could be dangerous.
  Capturing on 'eth0'
  1000
```

抓取一千个数据包保存为 capture.pcap

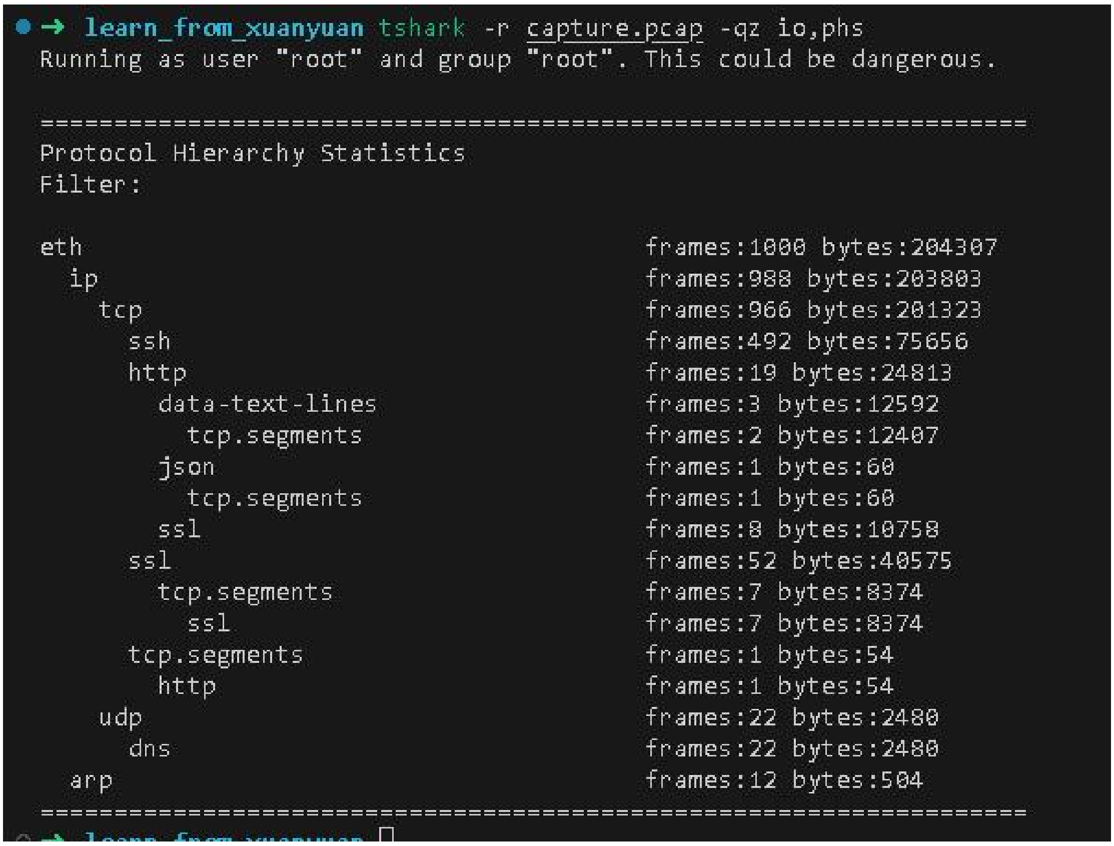
查看 capture.pcap 里面的 tcp 数据



```
● → learn_from_xuanyuan tshark -r capture.pcap -Y "tcp"
  Running as user "root" and group "root". This could be dangerous.
      1 0.000000000 120.229.80.250 → 172.27.205.146 TCP 60 1424 → 22 [ACK] Seq=1 Ack=1 Win=1021 Len=0
      2 0.000993266 120.229.80.250 → 172.27.205.146 SSH 154 Client: Encrypted packet (len=100)
      3 0.002618792 172.27.205.146 → 120.229.80.250 SSH 154 Server: Encrypted packet (len=100)
      4 0.045315672 172.27.205.146 → 120.229.80.250 SSH 250 Server: Encrypted packet (len=196)
      5 0.053509018 120.229.80.250 → 172.27.205.146 TCP 60 1424 → 22 [ACK] Seq=101 Ack=297 Win=1025 Len=0
      6 0.054872497 120.229.80.250 → 172.27.205.146 SSH 202 Client: Encrypted packet (len=148)
      7 0.055879847 172.27.205.146 → 120.229.80.250 SSH 154 Server: Encrypted packet (len=100)
      8 0.108003753 120.229.80.250 → 172.27.205.146 TCP 60 1424 → 22 [ACK] Seq=249 Ack=397 Win=1025 Len=0
      9 0.354660401 172.27.205.146 → 100.100.30.26 TCP 2902 43504 → 80 [ACK] Seq=1 Ack=1 Win=1496 Len=2848
     10 0.354687229 172.27.205.146 → 100.100.30.26 TCP 2902 43504 → 80 [ACK] Seq=2849 Ack=1 Win=1496 Len=2848 [TCP segment of a reass
  embled PDU]
     11 0.354692385 172.27.205.146 → 100.100.30.26 TCP 2902 43504 → 80 [ACK] Seq=5697 Ack=1 Win=1496 Len=2848 [TCP segment of a reass
  embled PDU]
     12 0.354695537 172.27.205.146 → 100.100.30.26 TCP 604 43504 → 80 [PSH, ACK] Seq=8545 Ack=1 Win=1496 Len=550 [TCP segment of a re
  assembled PDU]
     13 0.389518085 100.100.30.26 → 172.27.205.146 TCP 60 80 → 43504 [ACK] Seq=1 Ack=1425 Win=3511 Len=0
     14 0.389529673 100.100.30.26 → 172.27.205.146 TCP 60 80 → 43504 [ACK] Seq=1 Ack=2849 Win=3500 Len=0
     15 0.389532721 100.100.30.26 → 172.27.205.146 TCP 60 80 → 43504 [ACK] Seq=1 Ack=4273 Win=3489 Len=0
     16 0.389592149 100.100.30.26 → 172.27.205.146 TCP 60 80 → 43504 [ACK] Seq=1 Ack=5697 Win=3511 Len=0
     17 0.389596067 100.100.30.26 → 172.27.205.146 TCP 60 80 → 43504 [ACK] Seq=1 Ack=7121 Win=3500 Len=0
     18 0.389597604 100.100.30.26 → 172.27.205.146 TCP 60 80 → 43504 [ACK] Seq=1 Ack=8545 Win=3489 Len=0
     19 0.389599184 100.100.30.26 → 172.27.205.146 TCP 60 80 → 43504 [ACK] Seq=1 Ack=9095 Win=3511 Len=0
     20 0.590713089 172.27.205.146 → 120.229.80.250 SSH 154 Server: Encrypted packet (len=100)
     21 0.600258081 120.229.80.250 → 172.27.205.146 SSH 154 Client: Encrypted packet (len=100)
     22 0.602160849 172.27.205.146 → 120.229.80.250 SSH 154 Server: Encrypted packet (len=100)
     23 0.652013206 120.229.80.250 → 172.27.205.146 TCP 60 1424 → 22 [ACK] Seq=349 Ack=597 Win=1024 Len=0
     24 0.721837043 172.27.205.146 → 120.229.80.250 SSH 154 Server: Encrypted packet (len=100)
     25 0.776010286 120.229.80.250 → 172.27.205.146 TCP 60 1424 → 22 [ACK] Seq=349 Ack=697 Win=1024 Len=0
     26 0.791882460 120.229.80.250 → 172.27.205.146 SSH 154 Client: Encrypted packet (len=100)
     27 0.793564107 172.27.205.146 → 120.229.80.250 SSH 162 Server: Encrypted packet (len=108)
     28 0.842117105 172.27.205.146 → 120.229.80.250 SSH 146 Server: Encrypted packet (len=92)
     29 0.850272669 120.229.80.250 → 172.27.205.146 TCP 60 1424 → 22 [ACK] Seq=449 Ack=897 Win=1023 Len=0
     30 0.851501522 120.229.80.250 → 172.27.205.146 SSH 146 Client: Encrypted packet (len=92)
     31 0.853174600 172.27.205.146 → 120.229.80.250 SSH 162 Server: Encrypted packet (len=108)
     32 0.914009192 120.229.80.250 → 172.27.205.146 TCP 60 1424 → 22 [ACK] Seq=541 Ack=1005 Win=1023 Len=0
```

统计数据包里面协议层次统计信息

tshark -r capture.pcap -qz io,phs



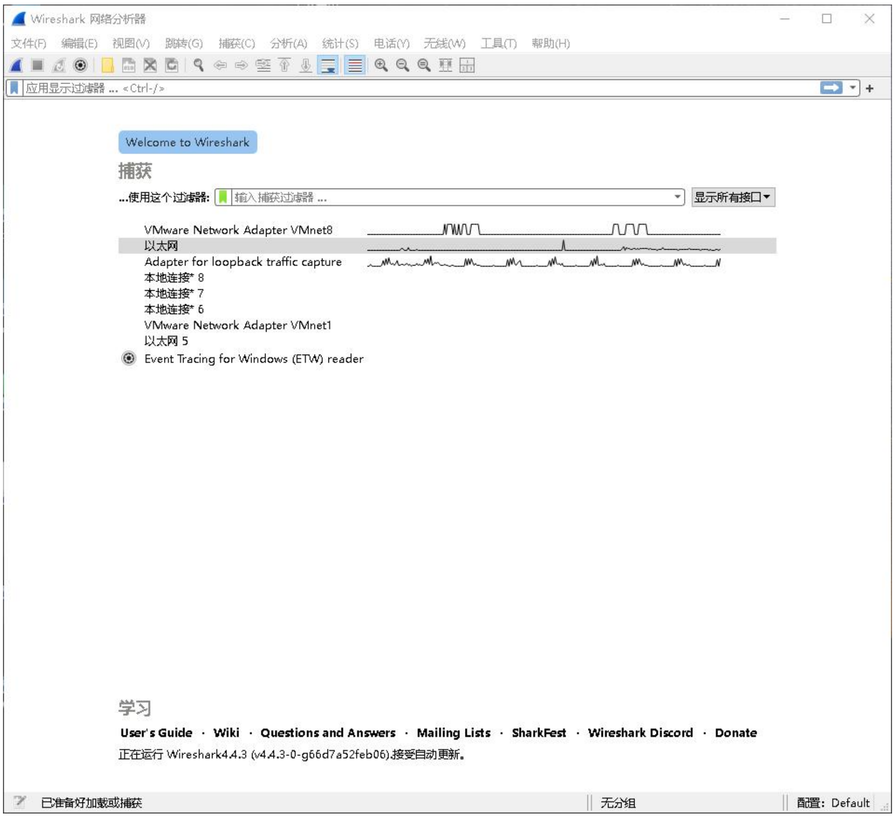
```
● → learn_from_xuanyuan tshark -r capture.pcap -qz io,phs
  Running as user "root" and group "root". This could be dangerous.

  ===================================================================
  Protocol Hierarchy Statistics
  Filter:

  eth                                      frames:1000 bytes:204307
    ip                                     frames:988 bytes:203803
      tcp                                  frames:966 bytes:201323
        ssh                                frames:492 bytes:75656
        http                               frames:19 bytes:24813
          data-text-lines                  frames:3 bytes:12592
            tcp.segments                   frames:2 bytes:12407
          json                             frames:1 bytes:60
            tcp.segments                   frames:1 bytes:60
          ssl                              frames:8 bytes:10758
        ssl                                frames:52 bytes:40575
          tcp.segments                     frames:7 bytes:8374
            ssl                            frames:7 bytes:8374
        tcp.segments                       frames:1 bytes:54
          http                             frames:1 bytes:54
      udp                                  frames:22 bytes:2480
        dns                                frames:22 bytes:2480
    arp                                    frames:12 bytes:504
  ===================================================================
○ → learn_from_xuanyuan 
```

## wireshark 使用

进入界面


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)
应用显示过滤器 ... <Ctrl-/>
Welcome to Wireshark
显示所有接口▾

捕获

...使用这个过滤器: 输入捕获过滤器 ...

VMware Network Adapter VMnet8
以太网
Adapter for loopback traffic capture
本地连接* 8
本地连接* 7
本地连接* 6
VMware Network Adapter VMnet1
以太网 5
Event Tracing for Windows (ETW) reader

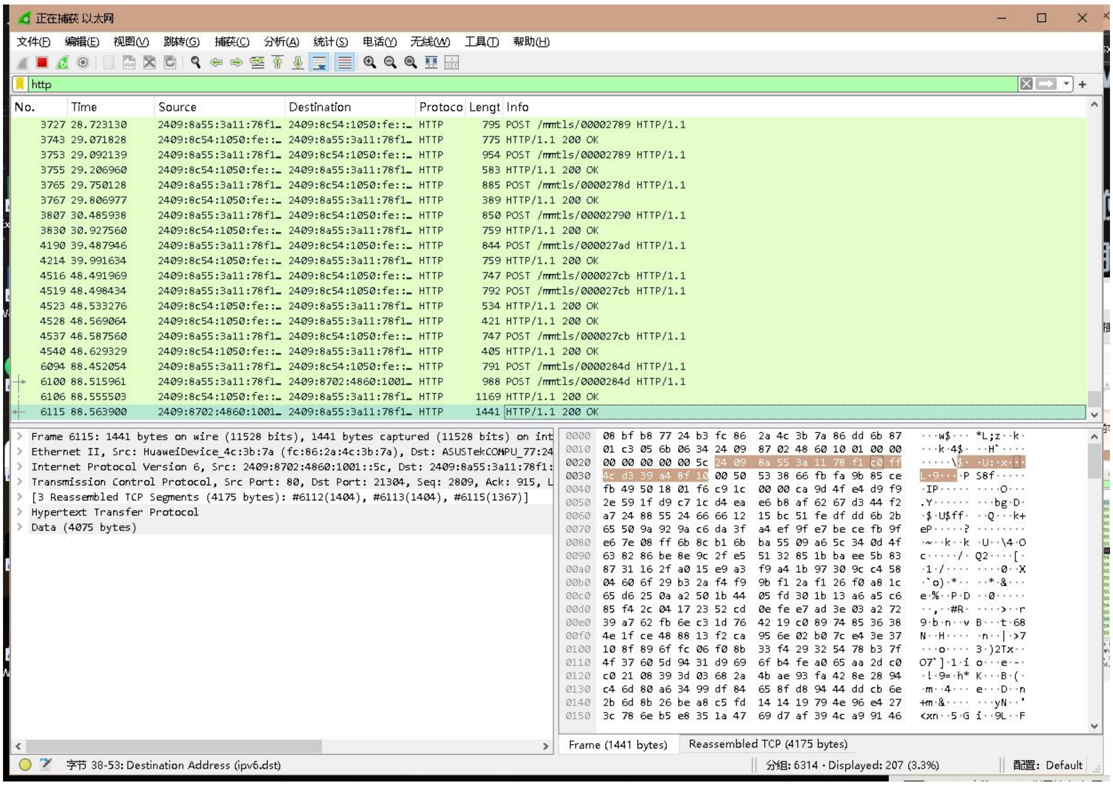
学习

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

正在运行 Wireshark4.4.3 (v4.4.3-0-g66d7a52feb06).接受自动更新。

已准备好加载或捕获 | 无分组 | 配置: Default

进入”以太网”网卡进行捕获登录微信期间产生的 HTTP 数据包



http

```
No.   Time      Source                Destination           Protoco Lengt Info
 3727 28.723130 2409:8a55:3a11:78f1…  2409:8c54:1050:fe::…  HTTP     795 POST /mmtls/00002789 HTTP/1.1
 3743 29.071828 2409:8c54:1050:fe::…  2409:8a55:3a11:78f1…  HTTP     775 HTTP/1.1 200 OK
 3753 29.092139 2409:8a55:3a11:78f1…  2409:8c54:1050:fe::…  HTTP     954 POST /mmtls/00002789 HTTP/1.1
 3755 29.206960 2409:8c54:1050:fe::…  2409:8a55:3a11:78f1…  HTTP     583 HTTP/1.1 200 OK
 3765 29.750128 2409:8a55:3a11:78f1…  2409:8c54:1050:fe::…  HTTP     885 POST /mmtls/0000278d HTTP/1.1
 3767 29.806977 2409:8c54:1050:fe::…  2409:8a55:3a11:78f1…  HTTP     389 HTTP/1.1 200 OK
 3807 30.485938 2409:8a55:3a11:78f1…  2409:8c54:1050:fe::…  HTTP     850 POST /mmtls/00002790 HTTP/1.1
 3830 30.927560 2409:8c54:1050:fe::…  2409:8a55:3a11:78f1…  HTTP     759 HTTP/1.1 200 OK
 4190 39.487946 2409:8a55:3a11:78f1…  2409:8c54:1050:fe::…  HTTP     844 POST /mmtls/000027ad HTTP/1.1
 4214 39.991634 2409:8c54:1050:fe::…  2409:8a55:3a11:78f1…  HTTP     759 HTTP/1.1 200 OK
 4516 48.491969 2409:8a55:3a11:78f1…  2409:8c54:1050:fe::…  HTTP     747 POST /mmtls/000027cb HTTP/1.1
 4519 48.498434 2409:8a55:3a11:78f1…  2409:8c54:1050:fe::…  HTTP     792 POST /mmtls/000027cb HTTP/1.1
 4523 48.533276 2409:8c54:1050:fe::…  2409:8a55:3a11:78f1…  HTTP     534 HTTP/1.1 200 OK
 4528 48.569064 2409:8c54:1050:fe::…  2409:8a55:3a11:78f1…  HTTP     421 HTTP/1.1 200 OK
 4537 48.587560 2409:8a55:3a11:78f1…  2409:8c54:1050:fe::…  HTTP     747 POST /mmtls/000027cb HTTP/1.1
 4540 48.629329 2409:8c54:1050:fe::…  2409:8a55:3a11:78f1…  HTTP     405 HTTP/1.1 200 OK
 6094 88.452054 2409:8a55:3a11:78f1…  2409:8c54:1050:fe::…  HTTP     791 POST /mmtls/0000284d HTTP/1.1
 6100 88.515961 2409:8a55:3a11:78f1…  2409:8702:4860:1001…  HTTP     988 POST /mmtls/0000284d HTTP/1.1
 6106 88.555503 2409:8c54:1050:fe::…  2409:8a55:3a11:78f1…  HTTP    1169 HTTP/1.1 200 OK
 6115 88.563900 2409:8702:4860:1001…  2409:8a55:3a11:78f1…  HTTP    1441 HTTP/1.1 200 OK
```

```
> Frame 6115: 1441 bytes on wire (11528 bits), 1441 bytes captured (11528 bits) on int
> Ethernet II, Src: HuaweiDevice_4c:3b:7a (fc:86:2a:4c:3b:7a), Dst: ASUSTekCOMPU_77:24
> Internet Protocol Version 6, Src: 2409:8702:4860:1001::5c, Dst: 2409:8a55:3a11:78f1:
> Transmission Control Protocol, Src Port: 80, Dst Port: 21304, Seq: 2809, Ack: 915, L
> [3 Reassembled TCP Segments (4175 bytes): #6112(1404), #6113(1404), #6115(1367)]
> Hypertext Transfer Protocol
> Data (4075 bytes)
```

```
0000  08 bf b8 77 24 b3 fc 86  2a 4c 3b 7a 86 dd 6b 87   ···w$··· *L;z··k·
0010  01 c3 05 6b 06 34 24 09  87 02 48 60 10 01 00 00   ···k·4$· ··H`····
0020  00 00 00 00 00 5c 24 09  8a 55 3a 11 78 f1 c0 ff   ·····\$· ·U:·x···
0030  4c d3 39 a4 8f 10 00 50  53 38 66 fb fa 9b 85 ce   L·9····P S8f·····
0040  fb 49 50 18 01 f6 c9 1c  00 00 ca 9d 4f e4 d9 f9   ·IP····· ····O···
0050  2e 59 1f d9 c7 1c d4 ea  e6 b8 af 62 67 d3 44 f2   .Y······ ···bg·D·
0060  a7 24 88 55 24 66 66 12  15 bc 51 fe df dd 6b 2b   ·$·U$ff· ·Q···k+
0070  65 50 9a 92 9a c6 da 3f  a4 ef 9f e7 be ce fb 9f   eP·····? ········
0080  e6 7e 08 ff 6b 8c b1 6b  ba 55 09 a6 5c 34 0d 4f   ·~··k··k ·U··\4·O
0090  63 82 86 be 8e 9c 2f e5  51 32 85 1b ba ee 5b 83   c·····/· Q2····[·
00a0  87 31 16 2f a0 15 e9 a3  f9 a4 1b 97 30 9c c4 58   ·1·/···· ····0··X
00b0  04 60 6f 29 b3 2a f4 f9  9b f1 2a f1 26 f0 a8 1c   ·`o)·*·· ··*·&···
00c0  65 d6 25 0a a2 50 1b 44  05 fd 30 1b 13 a6 a5 c6   e·%··P·D ··0·····
00d0  85 f4 2c 04 17 23 52 cd  0e fe e7 ad 3e 03 a2 72   ··,··#R· ····>··r
00e0  39 a7 62 fb 6e c3 1d 76  42 19 c0 89 74 85 36 38   9·b·n··v B···t·68
00f0  4e 1f ce 48 88 13 f2 ca  95 6e 02 b0 7c e4 3e 37   N··H···· ·n··|·>7
0100  10 8f 89 6f fc 06 f0 8b  33 f4 29 32 54 78 b3 7f   ···o···· 3·)2Tx··
0110  4f 37 60 5d 94 31 d9 69  6f b4 fe a0 65 aa 2d c0   O7`]·1·i o···e·-·
0120  c0 21 08 39 3d 03 68 2a  4b ae 93 fa 42 8e 28 94   ·!·9=·h* K···B·(·
0130  c4 6d 80 a6 34 99 df 84  65 8f d8 94 44 dd cb 6e   ·m··4··· e···D··n
0140  2b 6d 8b 26 be a8 c5 fd  14 14 19 79 4e 96 e4 27   +m·&···· ···yN··'
0150  3c 78 6e b5 e8 35 1a 47  69 d7 af 39 4c a9 91 46   <xn··5·G i··9L··F
```

字节 38-53: Destination Address (ipv6.dst)

分组: 6314 · Displayed: 207 (3.3%)

配置: Default