计算机网络

实验报告

（2022学年秋季学期）

教学班级	**计科二班**	**专业（方向）**	**计算机科学与技术**
学号	**20337263**	**姓名**	**俞泽斌**

一、 实验题目

（1）要求掌握网络抓包软件wireshark的内容包括

1、捕获网络流量进行详细分析

2、利用专家分析系统诊断问题。

3、实时监控网络活动

4、收集网络利用率和错误等信息

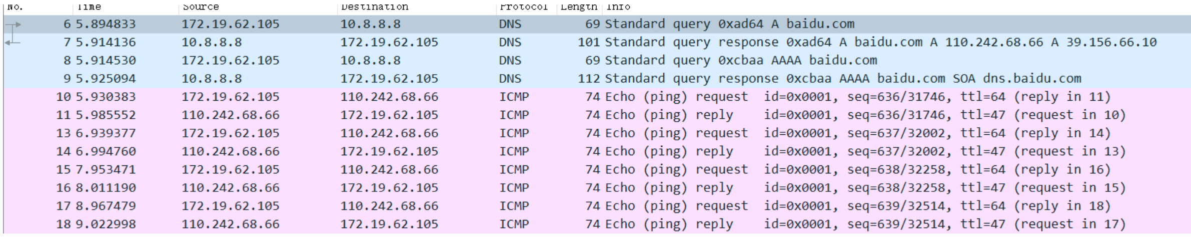
（2）协议分析1：IP协议，内容包括IP头的结构、IP数据包的数据结构分析

二、实验步骤

分析IP协议

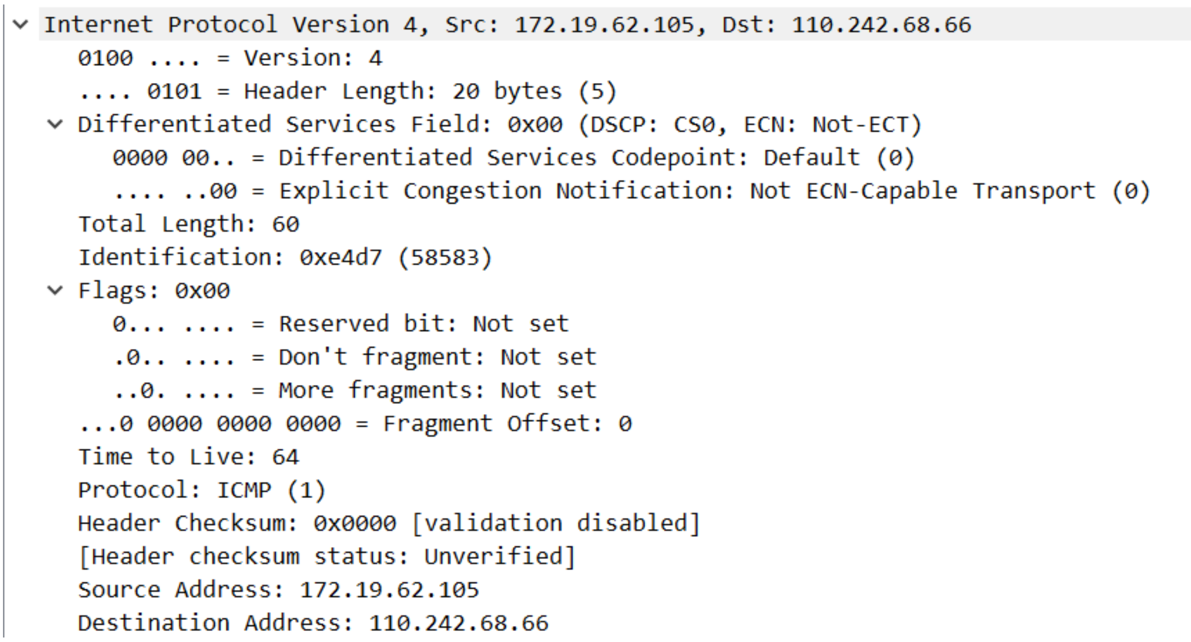
（1）打开wireshark并开始控制台内进入ping baidu.com

将过滤器设置为icmp||dns后得到结果如图



No.	Time	Source	Destination	Protocol	Length	Info
6	5.894833	172.19.62.105	10.8.8.8	DNS	69	Standard query 0xad64 A baidu.com
7	5.914136	10.8.8.8	172.19.62.105	DNS	101	Standard query response 0xad64 A baidu.com A 110.242.68.66 A 39.156.66.10
8	5.914530	172.19.62.105	10.8.8.8	DNS	69	Standard query 0xcbaa AAAA baidu.com
9	5.925094	10.8.8.8	172.19.62.105	DNS	112	Standard query response 0xcbaa AAAA baidu.com SOA dns.baidu.com
10	5.930383	172.19.62.105	110.242.68.66	ICMP	74	Echo (ping) request id=0x0001, seq=636/31746, ttl=64 (reply in 11)
11	5.985552	110.242.68.66	172.19.62.105	ICMP	74	Echo (ping) reply id=0x0001, seq=636/31746, ttl=47 (request in 10)
13	6.939377	172.19.62.105	110.242.68.66	ICMP	74	Echo (ping) request id=0x0001, seq=637/32002, ttl=64 (reply in 14)
14	6.994760	110.242.68.66	172.19.62.105	ICMP	74	Echo (ping) reply id=0x0001, seq=637/32002, ttl=47 (request in 13)
15	7.953471	172.19.62.105	110.242.68.66	ICMP	74	Echo (ping) request id=0x0001, seq=638/32258, ttl=64 (reply in 16)
16	8.011190	110.242.68.66	172.19.62.105	ICMP	74	Echo (ping) reply id=0x0001, seq=638/32258, ttl=47 (request in 15)
17	8.967479	172.19.62.105	110.242.68.66	ICMP	74	Echo (ping) request id=0x0001, seq=639/32514, ttl=64 (reply in 18)
18	9.022998	110.242.68.66	172.19.62.105	ICMP	74	Echo (ping) reply id=0x0001, seq=639/32514, ttl=47 (request in 17)

可以看到此时有四条DNS请求和回应，以及ICMP的request和reply操作，现在将ip协议展开，开始具体分析其中的字段



```
v Internet Protocol Version 4, Src: 172.19.62.105, Dst: 110.242.68.66
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 60
    Identification: 0xe4d7 (58583)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.19.62.105
    Destination Address: 110.242.68.66
```

具体建表如下

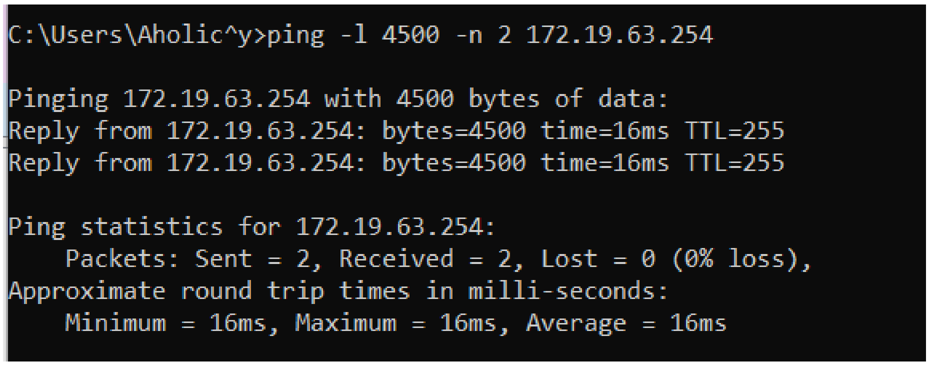
字段	值	具体字段值
版本	ipv4	Internet Protocol Version 4
首部长度	20 bytes	Header Length
区分服务	0x00	Differentiated Services Field
总长度	60	total length
标识	0xe4d7	Identification
标志	0x00	Flags
片偏移	0	Fragment offset
生存时间	64	Time to Live
协议	ICMP	Protocol
检验和	0x0000	Header Checksum
原IP地址	172.19.62.105	Src
目的IP地址	110.242.68.66	Destination

（2）当前网关为

```
Default Gateway . . . . . . . . . : fe80::a68:8dff:fea5:1e01%13
                                    172.19.63.254
```

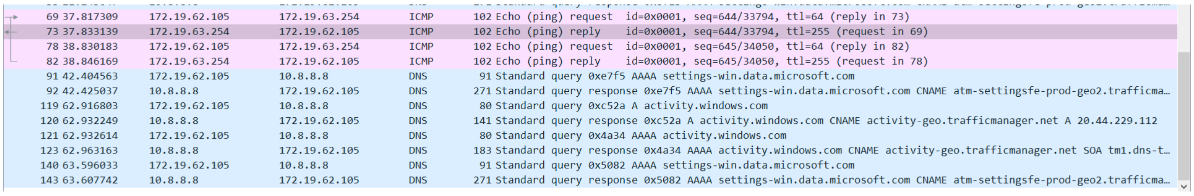
```
ping -l 4500 -n 2 172.19.63.254
```

输入上述命令后控制台结果

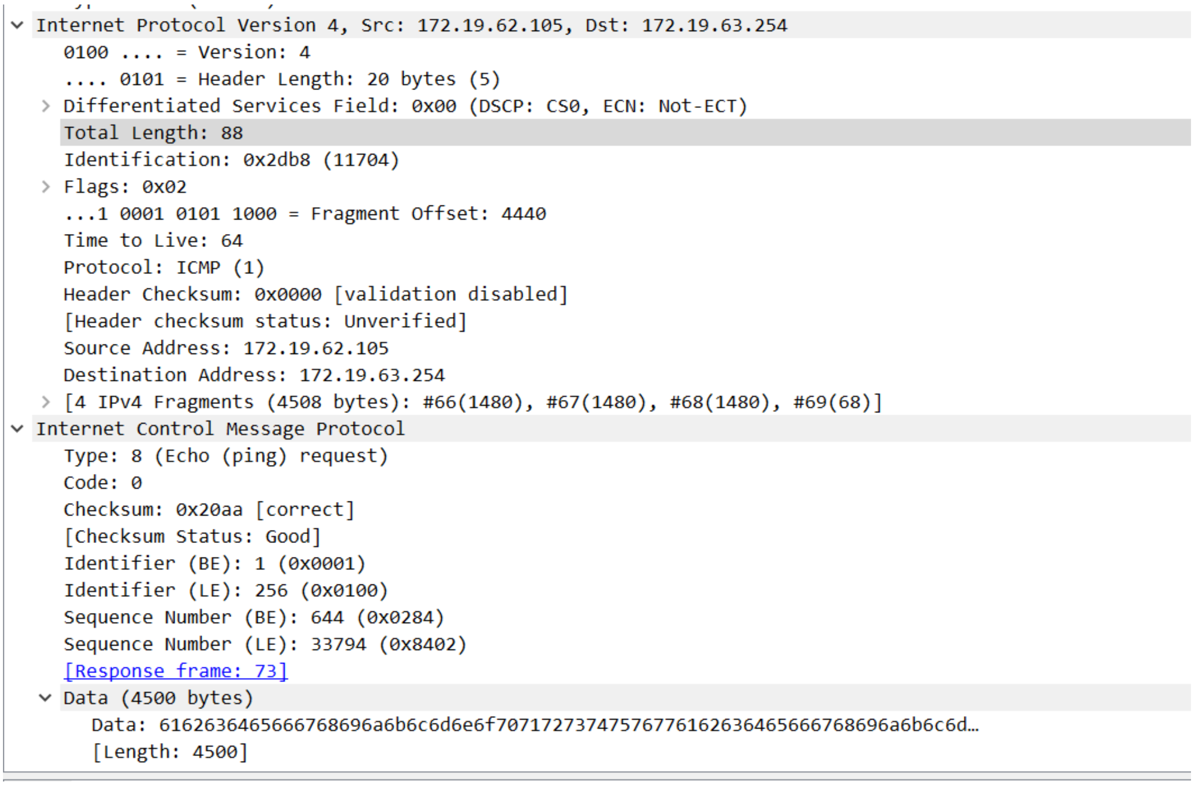


```
C:\Users\Aholic^y>ping -l 4500 -n 2 172.19.63.254

Pinging 172.19.63.254 with 4500 bytes of data:
Reply from 172.19.63.254: bytes=4500 time=16ms TTL=255
Reply from 172.19.63.254: bytes=4500 time=16ms TTL=255

Ping statistics for 172.19.63.254:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 16ms, Average = 16ms
```

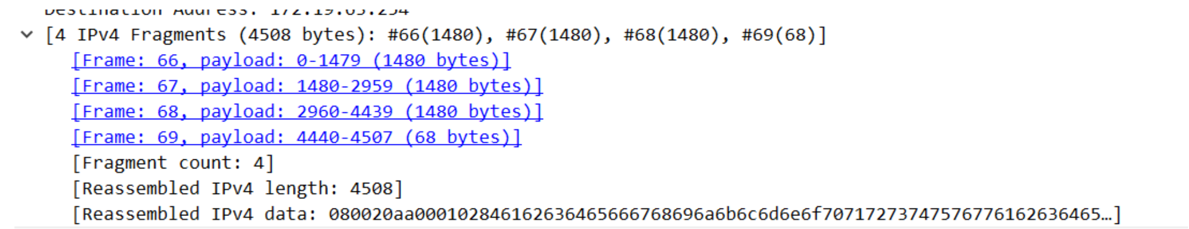
wireshark 捕获结果



```
 69 37.817309   172.19.62.105   172.19.63.254   ICMP   102 Echo (ping) request  id=0x0001, seq=644/33794, ttl=64 (reply in 73)
 73 37.833139   172.19.63.254   172.19.62.105   ICMP   102 Echo (ping) reply    id=0x0001, seq=644/33794, ttl=255 (request in 69)
 78 38.830183   172.19.62.105   172.19.63.254   ICMP   102 Echo (ping) request  id=0x0001, seq=645/34050, ttl=64 (reply in 82)
 82 38.846169   172.19.63.254   172.19.62.105   ICMP   102 Echo (ping) reply    id=0x0001, seq=645/34050, ttl=255 (request in 78)
 91 42.404563   172.19.62.105   10.8.8.8        DNS     91 Standard query 0xe7f5 AAAA settings-win.data.microsoft.com
 92 42.425037   10.8.8.8        172.19.62.105   DNS    271 Standard query response 0xe7f5 AAAA settings-win.data.microsoft.com CNAME atm-settingsfe-prod-geo2.trafficma…
119 62.916803   172.19.62.105   10.8.8.8        DNS     80 Standard query 0xc52a A activity.windows.com
120 62.932249   10.8.8.8        172.19.62.105   DNS    141 Standard query response 0xc52a A activity.windows.com CNAME activity-geo.trafficmanager.net A 20.44.229.112
121 62.932614   172.19.62.105   10.8.8.8        DNS     80 Standard query 0x4a34 AAAA activity.windows.com
123 62.963163   10.8.8.8        172.19.62.105   DNS    183 Standard query response 0x4a34 AAAA activity.windows.com CNAME activity-geo.trafficmanager.net SOA tm1.dns-t…
140 63.596033   172.19.62.105   10.8.8.8        DNS     91 Standard query 0x5082 AAAA settings-win.data.microsoft.com
143 63.607742   10.8.8.8        172.19.62.105   DNS    271 Standard query response 0x5082 AAAA settings-win.data.microsoft.com CNAME atm-settingsfe-prod-geo2.trafficma…
```



```
v Internet Protocol Version 4, Src: 172.19.62.105, Dst: 172.19.63.254
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 88
    Identification: 0x2db8 (11704)
  > Flags: 0x02
    ...1 0001 0101 1000 = Fragment Offset: 4440
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.19.62.105
    Destination Address: 172.19.63.254
  > [4 IPv4 Fragments (4508 bytes): #66(1480), #67(1480), #68(1480), #69(68)]
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x20aa [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 644 (0x0284)
    Sequence Number (LE): 33794 (0x8402)
    [Response frame: 73]
  v Data (4500 bytes)
      Data: 6162636465666768696a6b6c6d6e6f70717273747576776162636465666768696a6b6c6d…
      [Length: 4500]
```

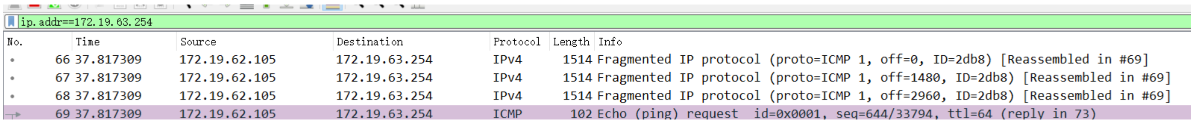


```
  Destination Address: 172.19.63.254
v [4 IPv4 Fragments (4508 bytes): #66(1480), #67(1480), #68(1480), #69(68)]
    [Frame: 66, payload: 0-1479 (1480 bytes)]
    [Frame: 67, payload: 1480-2959 (1480 bytes)]
    [Frame: 68, payload: 2960-4439 (1480 bytes)]
    [Frame: 69, payload: 4440-4507 (68 bytes)]
    [Fragment count: 4]
    [Reassembled IPv4 length: 4508]
    [Reassembled IPv4 data: 080020aa000102846162636465666768696a6b6c6d6e6f70717273747576776162636465…]
```

单独看上面的过滤器所产生的报文时发现，第一个报文内有4个分片

可以看到此时的data长度为1480bytes，头部的字段长度为20bytes，所以以太网的MTU为1500bytes。

上述发现一个报文内可能有多个分片，所以此时将过滤器改为ip.addr==172.19.63.254



```
ip.addr==172.19.63.254
No.   Time        Source          Destination     Protocol  Length Info
  66 37.817309   172.19.62.105   172.19.63.254   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=2db8) [Reassembled in #69]
  67 37.817309   172.19.62.105   172.19.63.254   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2db8) [Reassembled in #69]
  68 37.817309   172.19.62.105   172.19.63.254   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=2960, ID=2db8) [Reassembled in #69]
  69 37.817309   172.19.62.105   172.19.63.254   ICMP       102 Echo (ping) request  id=0x0001, seq=644/33794, ttl=64 (reply in 73)
```

属于同一个ICMP请求的分片有4个，分别为图中的No.66,67,68,69

每一个分片的满的有效长度为1480，若要将ping发起端发送的数据分为3个分片，ping命令中的报文长度应该设置为2961~4440之间

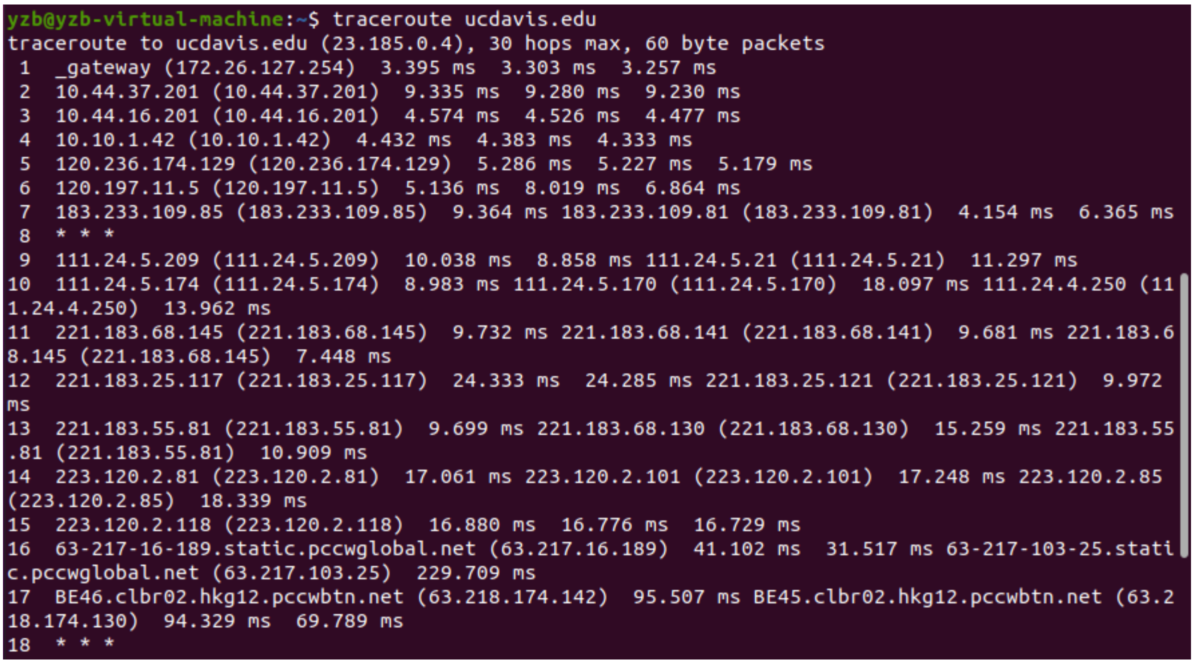
分析UDP协议

（1）因为windows下的tracert命令发送的是ICMP的包，所以这次实验采用在unbuntu虚拟机的环境下进行，

输入命令

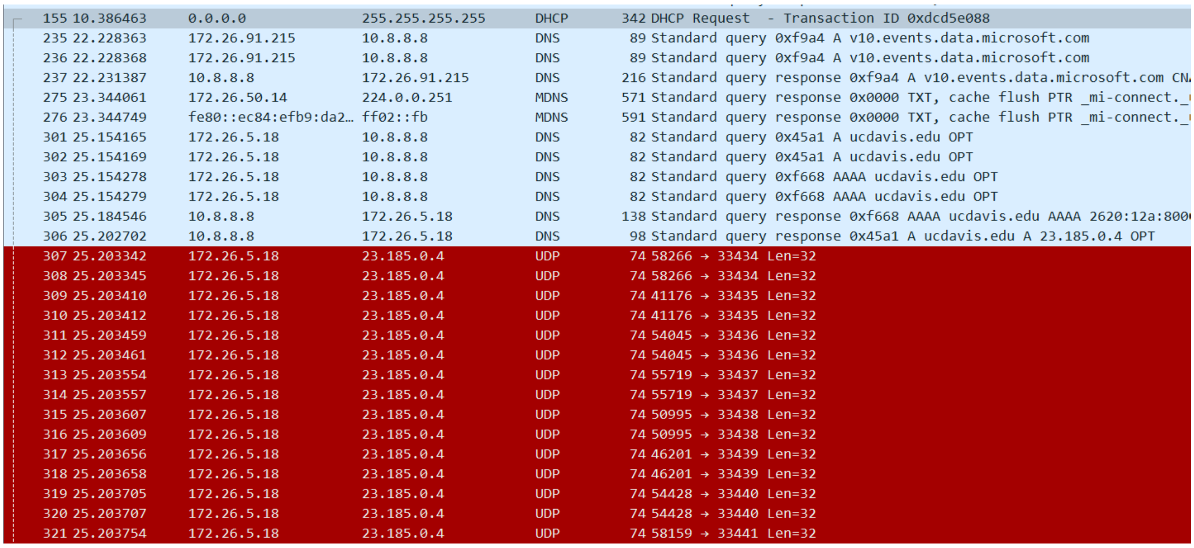
```
traceroute ucdavis.edu
```

控制台就结果如图



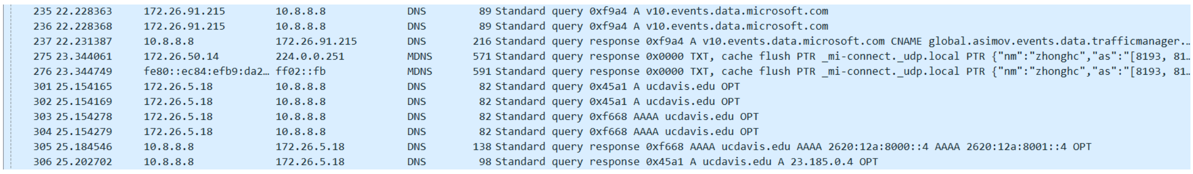
```
yzb@yzb-virtual-machine:~$ traceroute ucdavis.edu
traceroute to ucdavis.edu (23.185.0.4), 30 hops max, 60 byte packets
 1  _gateway (172.26.127.254)  3.395 ms  3.303 ms  3.257 ms
 2  10.44.37.201 (10.44.37.201)  9.335 ms  9.280 ms  9.230 ms
 3  10.44.16.201 (10.44.16.201)  4.574 ms  4.526 ms  4.477 ms
 4  10.10.1.42 (10.10.1.42)  4.432 ms  4.383 ms  4.333 ms
 5  120.236.174.129 (120.236.174.129)  5.286 ms  5.227 ms  5.179 ms
 6  120.197.11.5 (120.197.11.5)  5.136 ms  8.019 ms  6.864 ms
 7  183.233.109.85 (183.233.109.85)  9.364 ms 183.233.109.81 (183.233.109.81)  4.154 ms  6.365 ms
 8  * * *
 9  111.24.5.209 (111.24.5.209)  10.038 ms  8.858 ms 111.24.5.21 (111.24.5.21)  11.297 ms
10  111.24.5.174 (111.24.5.174)  8.983 ms 111.24.5.170 (111.24.5.170)  18.097 ms 111.24.4.250 (11
1.24.4.250)  13.962 ms
11  221.183.68.145 (221.183.68.145)  9.732 ms 221.183.68.141 (221.183.68.141)  9.681 ms 221.183.6
8.145 (221.183.68.145)  7.448 ms
12  221.183.25.117 (221.183.25.117)  24.333 ms  24.285 ms 221.183.25.121 (221.183.25.121)  9.972
ms
13  221.183.55.81 (221.183.55.81)  9.699 ms 221.183.68.130 (221.183.68.130)  15.259 ms 221.183.55
.81 (221.183.55.81)  10.909 ms
14  223.120.2.81 (223.120.2.81)  17.061 ms 223.120.2.101 (223.120.2.101)  17.248 ms 223.120.2.85
(223.120.2.85)  18.339 ms
15  223.120.2.118 (223.120.2.118)  16.880 ms  16.776 ms  16.729 ms
16  63-217-16-189.static.pccwglobal.net (63.217.16.189)  41.102 ms  31.517 ms 63-217-103-25.stati
c.pccwglobal.net (63.217.103.25)  229.709 ms
17  BE46.clbr02.hkg12.pccwbtn.net (63.218.174.142)  95.507 ms BE45.clbr02.hkg12.pccwbtn.net (63.2
18.174.130)  94.329 ms  69.789 ms
18  * * *
```

wireshark抓包得到结果如下



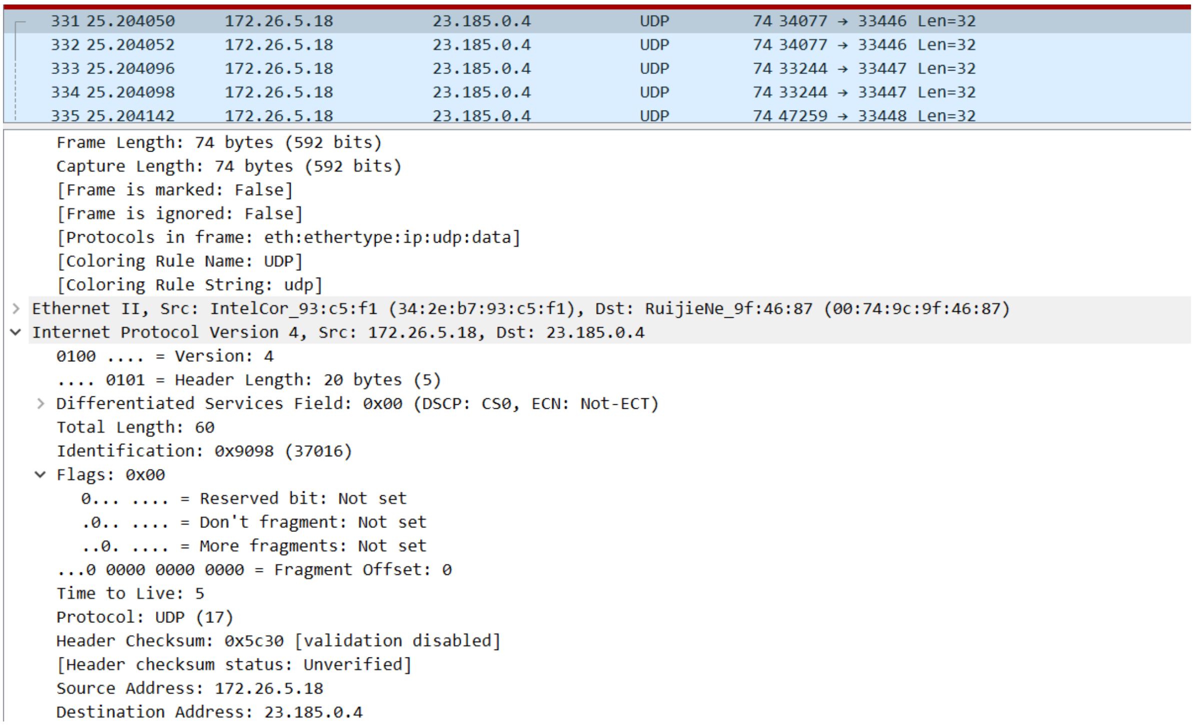
```
155 10.386463   0.0.0.0               255.255.255.255   DHCP    342 DHCP Request  - Transaction ID 0xdcd5e088
235 22.228363   172.26.91.215         10.8.8.8          DNS      89 Standard query 0xf9a4 A v10.events.data.microsoft.com
236 22.228368   172.26.91.215         10.8.8.8          DNS      89 Standard query 0xf9a4 A v10.events.data.microsoft.com
237 22.231387   10.8.8.8              172.26.91.215     DNS     216 Standard query response 0xf9a4 A v10.events.data.microsoft.com CN
275 23.344061   172.26.50.14          224.0.0.251       MDNS    571 Standard query response 0x0000 TXT, cache flush PTR _mi-connect._
276 23.344749   fe80::ec84:efb9:da2…  ff02::fb          MDNS    591 Standard query response 0x0000 TXT, cache flush PTR _mi-connect._
301 25.154165   172.26.5.18           10.8.8.8          DNS      82 Standard query 0x45a1 A ucdavis.edu OPT
302 25.154169   172.26.5.18           10.8.8.8          DNS      82 Standard query 0x45a1 A ucdavis.edu OPT
303 25.154278   172.26.5.18           10.8.8.8          DNS      82 Standard query 0xf668 AAAA ucdavis.edu OPT
304 25.154279   172.26.5.18           10.8.8.8          DNS      82 Standard query 0xf668 AAAA ucdavis.edu OPT
305 25.184546   10.8.8.8              172.26.5.18       DNS     138 Standard query response 0xf668 AAAA ucdavis.edu AAAA 2620:12a:800
306 25.202702   10.8.8.8              172.26.5.18       DNS      98 Standard query response 0x45a1 A ucdavis.edu A 23.185.0.4 OPT
307 25.203342   172.26.5.18           23.185.0.4        UDP      74 58266 → 33434 Len=32
308 25.203345   172.26.5.18           23.185.0.4        UDP      74 58266 → 33434 Len=32
309 25.203410   172.26.5.18           23.185.0.4        UDP      74 41176 → 33435 Len=32
310 25.203412   172.26.5.18           23.185.0.4        UDP      74 41176 → 33435 Len=32
311 25.203459   172.26.5.18           23.185.0.4        UDP      74 54045 → 33436 Len=32
312 25.203461   172.26.5.18           23.185.0.4        UDP      74 54045 → 33436 Len=32
313 25.203554   172.26.5.18           23.185.0.4        UDP      74 55719 → 33437 Len=32
314 25.203557   172.26.5.18           23.185.0.4        UDP      74 55719 → 33437 Len=32
315 25.203607   172.26.5.18           23.185.0.4        UDP      74 50995 → 33438 Len=32
316 25.203609   172.26.5.18           23.185.0.4        UDP      74 50995 → 33438 Len=32
317 25.203656   172.26.5.18           23.185.0.4        UDP      74 46201 → 33439 Len=32
318 25.203658   172.26.5.18           23.185.0.4        UDP      74 46201 → 33439 Len=32
319 25.203705   172.26.5.18           23.185.0.4        UDP      74 54428 → 33440 Len=32
320 25.203707   172.26.5.18           23.185.0.4        UDP      74 54428 → 33440 Len=32
321 25.203754   172.26.5.18           23.185.0.4        UDP      74 58159 → 33441 Len=32
```

下面来对信息具体分析



```
235 22.228363   172.26.91.215      10.8.8.8           DNS        89 Standard query 0xf9a4 A v10.events.data.microsoft.com
236 22.228368   172.26.91.215      10.8.8.8           DNS        89 Standard query 0xf9a4 A v10.events.data.microsoft.com
237 22.231387   10.8.8.8           172.26.91.215      DNS       216 Standard query response 0xf9a4 A v10.events.data.microsoft.com CNAME global.asimov.events.data.trafficmanager…
275 23.344061   172.26.50.14       224.0.0.251        MDNS      571 Standard query response 0x0000 TXT, cache flush PTR _mi-connect._udp.local PTR {"nm":"zhonghc","as":"[8193, 81…
276 23.344749   fe80::ec84:efb9:da2… ff02::fb         MDNS      591 Standard query response 0x0000 TXT, cache flush PTR _mi-connect._udp.local PTR {"nm":"zhonghc","as":"[8193, 81…
301 25.154165   172.26.5.18        10.8.8.8           DNS        82 Standard query 0x45a1 A ucdavis.edu OPT
302 25.154169   172.26.5.18        10.8.8.8           DNS        82 Standard query 0x45a1 A ucdavis.edu OPT
303 25.154278   172.26.5.18        10.8.8.8           DNS        82 Standard query 0xf668 AAAA ucdavis.edu OPT
304 25.154279   172.26.5.18        10.8.8.8           DNS        82 Standard query 0xf668 AAAA ucdavis.edu OPT
305 25.184546   10.8.8.8           172.26.5.18        DNS       138 Standard query response 0xf668 AAAA ucdavis.edu AAAA 2620:12a:8000::4 AAAA 2620:12a:8001::4 OPT
306 25.202702   10.8.8.8           172.26.5.18        DNS        98 Standard query response 0x45a1 A ucdavis.edu A 23.185.0.4 OPT
```

开始是对ucdavis.edu的域名解析，是用了DNS的协议来进行，具体的解析过程前面几个实验中也涉及到了，就是通过一层一层的DNS服务器来向本地返回所需要访问域名的ip地址



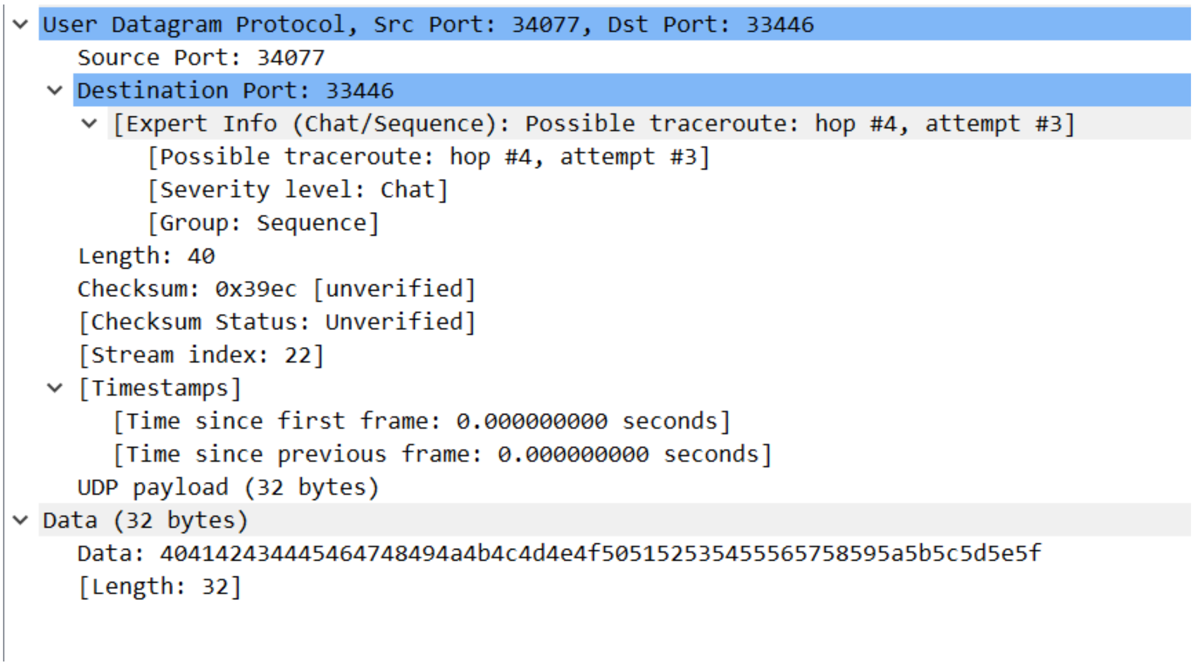
```
331 25.204050   172.26.5.18        23.185.0.4         UDP        74 34077 → 33446 Len=32
332 25.204052   172.26.5.18        23.185.0.4         UDP        74 34077 → 33446 Len=32
333 25.204096   172.26.5.18        23.185.0.4         UDP        74 33244 → 33447 Len=32
334 25.204098   172.26.5.18        23.185.0.4         UDP        74 33244 → 33447 Len=32
335 25.204142   172.26.5.18        23.185.0.4         UDP        74 47259 → 33448 Len=32
```

```
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:data]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
> Ethernet II, Src: IntelCor_93:c5:f1 (34:2e:b7:93:c5:f1), Dst: RuijieNe_9f:46:87 (00:74:9c:9f:46:87)
v Internet Protocol Version 4, Src: 172.26.5.18, Dst: 23.185.0.4
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x9098 (37016)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 5
    Protocol: UDP (17)
    Header Checksum: 0x5c30 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.26.5.18
    Destination Address: 23.185.0.4
```

具体分析其中一条udp协议请求，先截取了网络层的报文内容

字段	值	意义
Version	4	代码ipv4协议
Differentiated Services Field	0x00	区分服务
header length	20 bytes	头部字段长度
total length	60	总长度
Identification	0x9098	标识符
Time to live	5	生存时间
Protocol	UDP	UDP协议
Source Address	172.26.5.18	主机ip地址
Destination Address	23.185.0.4	目标ip地址

传输层/UDP层



```
User Datagram Protocol, Src Port: 34077, Dst Port: 33446
    Source Port: 34077
    Destination Port: 33446
        [Expert Info (Chat/Sequence): Possible traceroute: hop #4, attempt #3]
            [Possible traceroute: hop #4, attempt #3]
            [Severity level: Chat]
            [Group: Sequence]
    Length: 40
    Checksum: 0x39ec [unverified]
    [Checksum Status: Unverified]
    [Stream index: 22]
    [Timestamps]
        [Time since first frame: 0.000000000 seconds]
        [Time since previous frame: 0.000000000 seconds]
    UDP payload (32 bytes)
Data (32 bytes)
    Data: 404142434445464748494a4b4c4d4e4f505152535455565758595a5b5c5d5e5f
    [Length: 32]
```

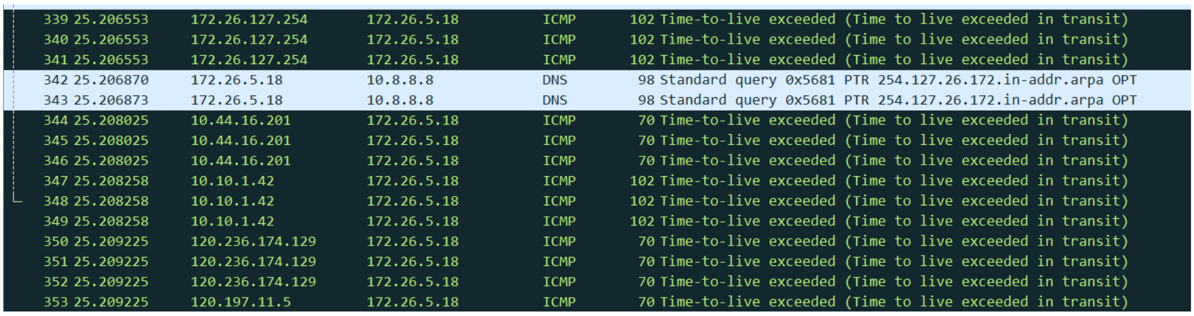
字段	值	意义
Src Port	34077	主机端口
Dst Port	33446	目标端口
checksum	0x39ec	数据校验和

所以traceroute ucdavis.edu的流程主要有以下几个方面

首先，本地开始解析ucdavis.edu这个域名的ip地址，向上一级DNS服务器进行请求，逐级请求下得到ucdavis.edu的ip地址为23.185.0.4

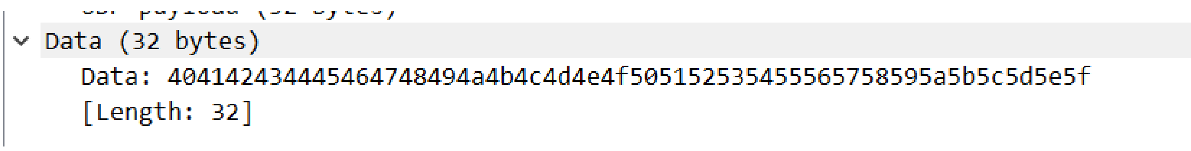
然后主机172.26.5.18开始想域名对应的ip地址发一个TTL=1的UDP数据包，而经过的第一个路由器收到这个数据包以后，就自动把TTL减1，而TTL变为0以后，路由器就把这个包给抛弃了，并同时产生 一个主机不可达的ICMP数据报给主机。

主机收到这个数据报以后再发一个TTL=2的UDP数据报给目的主机，然后刺激第二个路由器给主机发ICMP数据报。如此往复直到到达目的主机。



```
339 25.206553   172.26.127.254   172.26.5.18   ICMP   102 Time-to-live exceeded (Time to live exceeded in transit)
340 25.206553   172.26.127.254   172.26.5.18   ICMP   102 Time-to-live exceeded (Time to live exceeded in transit)
341 25.206553   172.26.127.254   172.26.5.18   ICMP   102 Time-to-live exceeded (Time to live exceeded in transit)
342 25.206870   172.26.5.18      10.8.8.8      DNS     98 Standard query 0x5681 PTR 254.127.26.172.in-addr.arpa OPT
343 25.206873   172.26.5.18      10.8.8.8      DNS     98 Standard query 0x5681 PTR 254.127.26.172.in-addr.arpa OPT
344 25.208025   10.44.16.201     172.26.5.18   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
345 25.208025   10.44.16.201     172.26.5.18   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
346 25.208025   10.44.16.201     172.26.5.18   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
347 25.208258   10.10.1.42       172.26.5.18   ICMP   102 Time-to-live exceeded (Time to live exceeded in transit)
348 25.208258   10.10.1.42       172.26.5.18   ICMP   102 Time-to-live exceeded (Time to live exceeded in transit)
349 25.208258   10.10.1.42       172.26.5.18   ICMP   102 Time-to-live exceeded (Time to live exceeded in transit)
350 25.209225   120.236.174.129  172.26.5.18   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
351 25.209225   120.236.174.129  172.26.5.18   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
352 25.209225   120.236.174.129  172.26.5.18   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
353 25.209225   120.197.11.5     172.26.5.18   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
```

ip数据包的内容为udp传输层下的data数据，如下图



```
    UDP payload (32 bytes)
Data (32 bytes)
    Data: 404142434445464748494a4b4c4d4e4f505152535455565758595a5b5c5d5e5f
    [Length: 32]
```