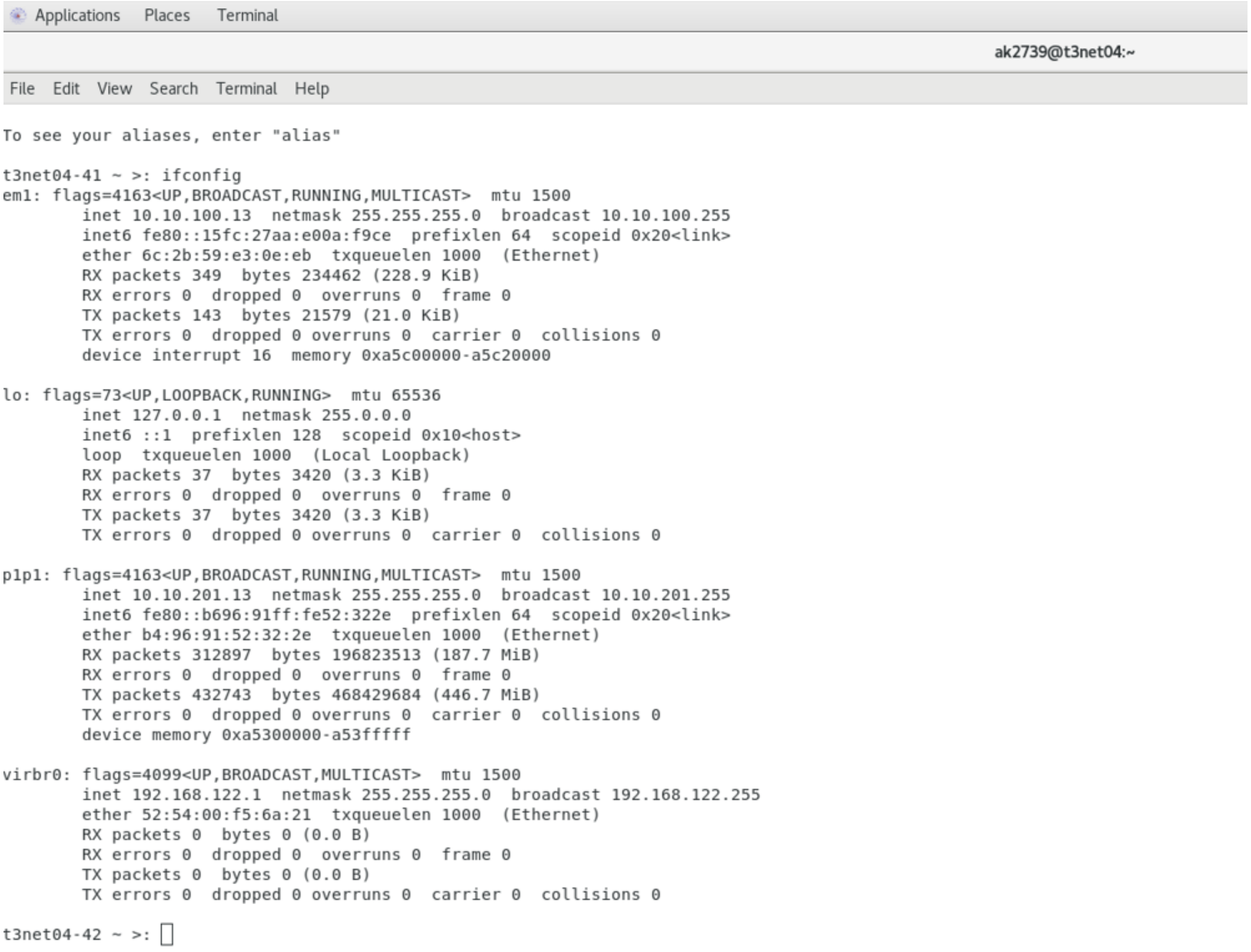
ECE 636
COMPUTER NETWORKING LABORATORY

Ayush Kale
31573799
ak2739@njit.edu

IP Routing (Lab 4)

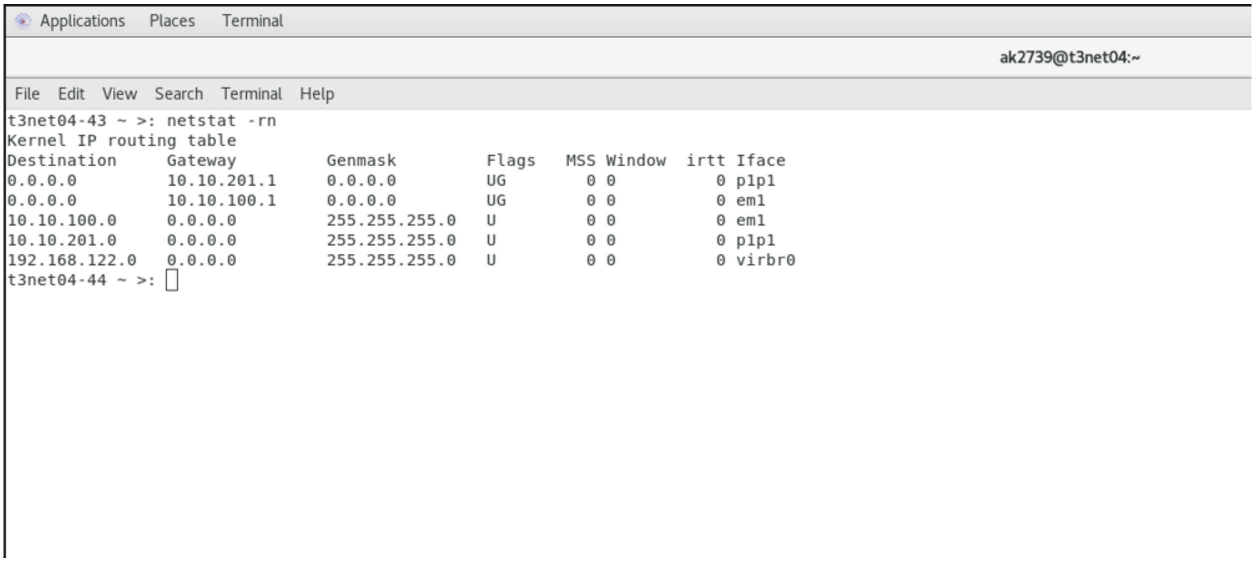
Lab Descriptions

4.2.1 Observe your workstation's routing table


Applications Places Terminal
ak2739@t3net04:~
File Edit View Search Terminal Help

```
To see your aliases, enter "alias"

t3net04-41 ~ >: ifconfig
em1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.100.13  netmask 255.255.255.0  broadcast 10.10.100.255
        inet6 fe80::15fc:27aa:e00a:f9ce  prefixlen 64  scopeid 0x20<link>
        ether 6c:2b:59:e3:0e:eb  txqueuelen 1000  (Ethernet)
        RX packets 349  bytes 234462 (228.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 143  bytes 21579 (21.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16  memory 0xa5c00000-a5c20000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 37  bytes 3420 (3.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 37  bytes 3420 (3.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

p1p1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.201.13  netmask 255.255.255.0  broadcast 10.10.201.255
        inet6 fe80::b696:91ff:fe52:322e  prefixlen 64  scopeid 0x20<link>
        ether b4:96:91:52:32:2e  txqueuelen 1000  (Ethernet)
        RX packets 312897  bytes 196823513 (187.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 432743  bytes 468429684 (446.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0xa5300000-a53fffff

virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
        ether 52:54:00:f5:6a:21  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

t3net04-42 ~ >: 
```

Workstation is t3net04
Description of the workstation: There are 2 interfaces em1 and p1p1. em1 has an ip address of 10.10.100.13 and p1p1 has an ip address of 10.10.201.13.



```
t3net04-43 ~ >: netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         10.10.201.1     0.0.0.0         UG        0 0          0 p1p1
0.0.0.0         10.10.100.1     0.0.0.0         UG        0 0          0 em1
10.10.100.0     0.0.0.0         255.255.255.0   U         0 0          0 em1
10.10.201.0     0.0.0.0         255.255.255.0   U         0 0          0 p1p1
192.168.122.0   0.0.0.0         255.255.255.0   U         0 0          0 virbr0
t3net04-44 ~ >: 
```

Workstation's routing table using the command netstat -rn
The routing table has 5 entries. 2 entries are for 0.0.0.0 destination with gateways 10.10.100.1(ip address from the subnet of em1 interface) and 10.10.201.1 (ip address from the subnet of p1p1 interface).

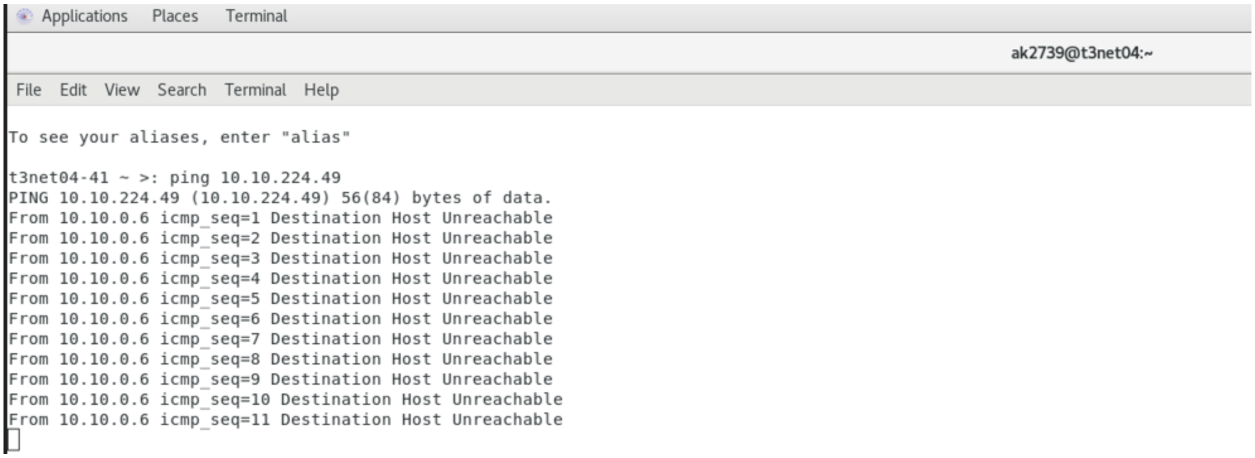
There are 3 entries in the routing table cache.

1. Destination of 10.10.100.0 with subnet mask of 255.255.255.0
2. Destination of 10.10.201.0 with subnet mask of 255.255.255.0
3. Destination of 192.168.122.0 with subnet mask of 255.255.255.0

Each of the entries have a U flag and different interfaces, em1, p1p1 and virbr0 respectively.

4.2.2 Ping a host in the Internet which is unreachable

For the unreachable host in the internet , used an ip address in the lab which is in a different subnet than the workstation (t3net04)
IP address used for ping command: 10.10.224.49

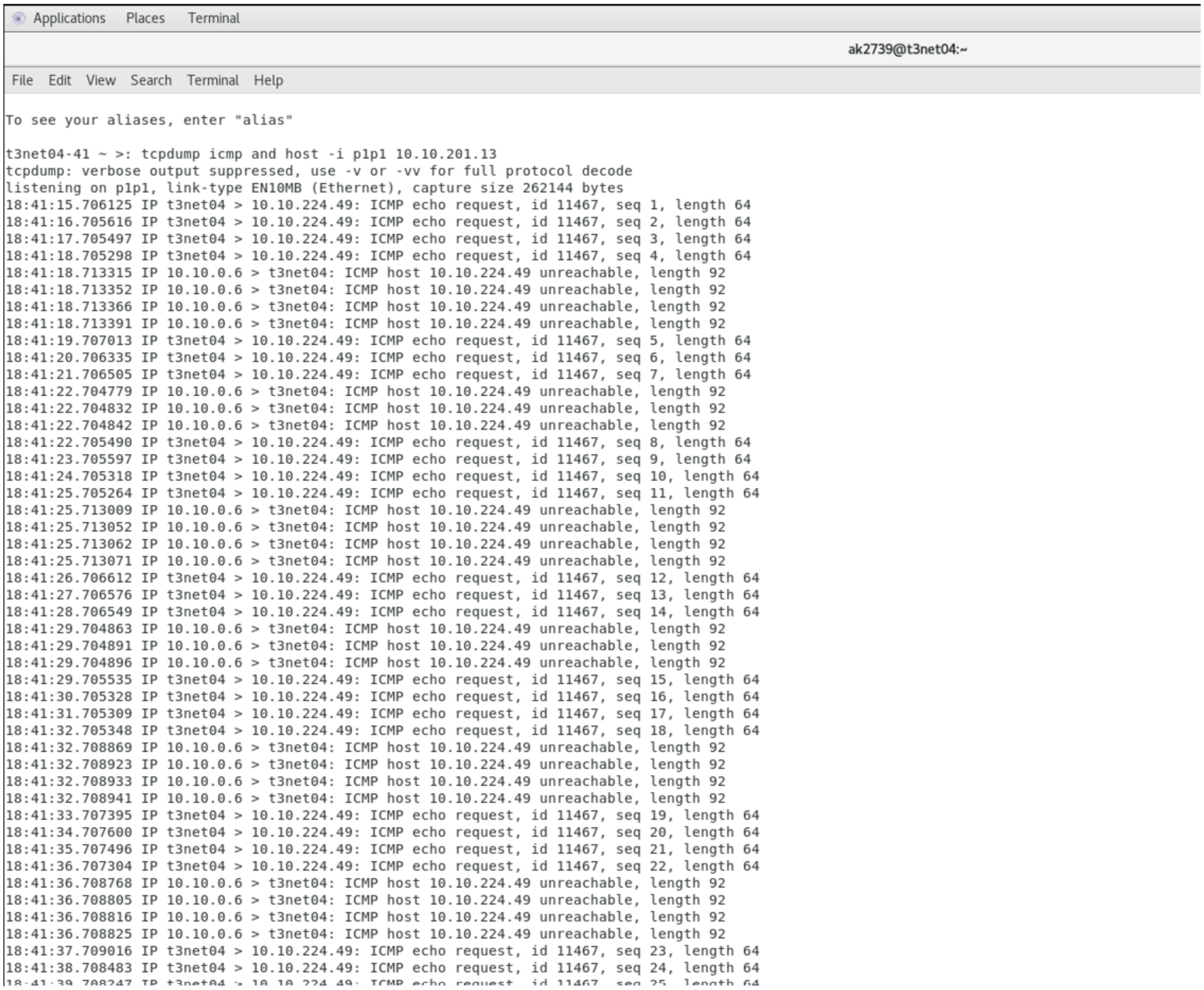


```
To see your aliases, enter "alias"

t3net04-41 ~ >: ping 10.10.224.49
PING 10.10.224.49 (10.10.224.49) 56(84) bytes of data.
From 10.10.0.6 icmp_seq=1 Destination Host Unreachable
From 10.10.0.6 icmp_seq=2 Destination Host Unreachable
From 10.10.0.6 icmp_seq=3 Destination Host Unreachable
From 10.10.0.6 icmp_seq=4 Destination Host Unreachable
From 10.10.0.6 icmp_seq=5 Destination Host Unreachable
From 10.10.0.6 icmp_seq=6 Destination Host Unreachable
From 10.10.0.6 icmp_seq=7 Destination Host Unreachable
From 10.10.0.6 icmp_seq=8 Destination Host Unreachable
From 10.10.0.6 icmp_seq=9 Destination Host Unreachable
From 10.10.0.6 icmp_seq=10 Destination Host Unreachable
From 10.10.0.6 icmp_seq=11 Destination Host Unreachable
```

Result of the ping command
Icmp packets starting from sequence number equal to 1 with the message, “Destination host unreachable”

To observe the icmp messages tcpdump command was used at the same time in another terminal.

The tcp dump output consists of echo request with id 11467 and sequence number starting with 1 for the ip address of the destination 10.10.224.49.
Each message is 64 bytes.
The result for 3 echo request messages is 3 icmp packets with length of 92 bytes with ICMP host 10.10.224.49 unreachable messages.

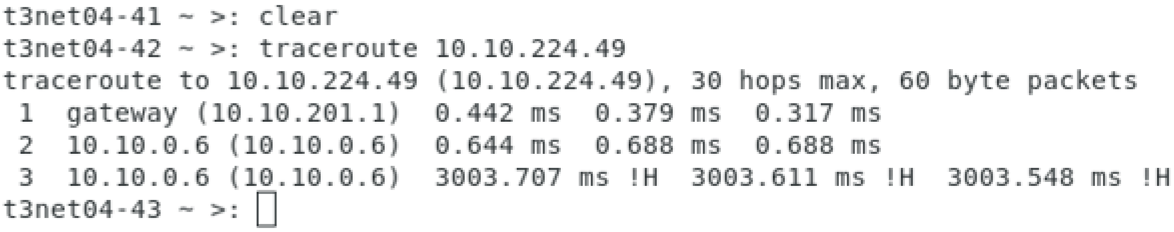

Applications Places Terminal
ak2739@t3net04:~
File Edit View Search Terminal Help

```
To see your aliases, enter "alias"

t3net04-41 ~ >: tcpdump icmp and host -i p1p1 10.10.201.13
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on p1p1, link-type EN10MB (Ethernet), capture size 262144 bytes
18:41:15.706125 IP t3net04 > 10.10.224.49: ICMP echo request, id 11467, seq 1, length 64
18:41:16.705616 IP t3net04 > 10.10.224.49: ICMP echo request, id 11467, seq 2, length 64
18:41:17.705497 IP t3net04 > 10.10.224.49: ICMP echo request, id 11467, seq 3, length 64
18:41:18.705298 IP t3net04 > 10.10.224.49: ICMP echo request, id 11467, seq 4, length 64
18:41:18.713315 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 92
18:41:18.713352 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 92
18:41:18.713366 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 92
18:41:18.713391 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 92
18:41:19.707013 IP t3net04 > 10.10.224.49: ICMP echo request, id 11467, seq 5, length 64
18:41:20.706335 IP t3net04 > 10.10.224.49: ICMP echo request, id 11467, seq 6, length 64
18:41:21.706505 IP t3net04 > 10.10.224.49: ICMP echo request, id 11467, seq 7, length 64
18:41:22.704779 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 92
18:41:22.704832 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 92
18:41:22.704842 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 92
18:41:22.705490 IP t3net04 > 10.10.224.49: ICMP echo request, id 11467, seq 8, length 64
18:41:23.705597 IP t3net04 > 10.10.224.49: ICMP echo request, id 11467, seq 9, length 64
18:41:24.705318 IP t3net04 > 10.10.224.49: ICMP echo request, id 11467, seq 10, length 64
18:41:25.705264 IP t3net04 > 10.10.224.49: ICMP echo request, id 11467, seq 11, length 64
18:41:25.713009 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 92
18:41:25.713052 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 92
18:41:25.713062 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 92
18:41:25.713071 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 92
18:41:26.706612 IP t3net04 > 10.10.224.49: ICMP echo request, id 11467, seq 12, length 64
18:41:27.706576 IP t3net04 > 10.10.224.49: ICMP echo request, id 11467, seq 13, length 64
18:41:28.706549 IP t3net04 > 10.10.224.49: ICMP echo request, id 11467, seq 14, length 64
18:41:29.704863 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 92
18:41:29.704891 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 92
18:41:29.704896 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 92
18:41:29.705535 IP t3net04 > 10.10.224.49: ICMP echo request, id 11467, seq 15, length 64
18:41:30.705328 IP t3net04 > 10.10.224.49: ICMP echo request, id 11467, seq 16, length 64
18:41:31.705309 IP t3net04 > 10.10.224.49: ICMP echo request, id 11467, seq 17, length 64
18:41:32.705348 IP t3net04 > 10.10.224.49: ICMP echo request, id 11467, seq 18, length 64
18:41:32.708869 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 92
18:41:32.708923 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 92
18:41:32.708933 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 92
18:41:32.708941 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 92
18:41:33.707395 IP t3net04 > 10.10.224.49: ICMP echo request, id 11467, seq 19, length 64
18:41:34.707600 IP t3net04 > 10.10.224.49: ICMP echo request, id 11467, seq 20, length 64
18:41:35.707496 IP t3net04 > 10.10.224.49: ICMP echo request, id 11467, seq 21, length 64
18:41:36.707304 IP t3net04 > 10.10.224.49: ICMP echo request, id 11467, seq 22, length 64
18:41:36.708768 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 92
18:41:36.708805 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 92
18:41:36.708816 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 92
18:41:36.708825 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 92
18:41:37.709016 IP t3net04 > 10.10.224.49: ICMP echo request, id 11467, seq 23, length 64
18:41:38.708483 IP t3net04 > 10.10.224.49: ICMP echo request, id 11467, seq 24, length 64
18:41:39.708247 IP t3net04 > 10.10.224.49: ICMP echo request, id 11467, seq 25, length 64
```

Tcp dump output for ICMP packets

4.2.3 Use “traceroute <unreachable host>”

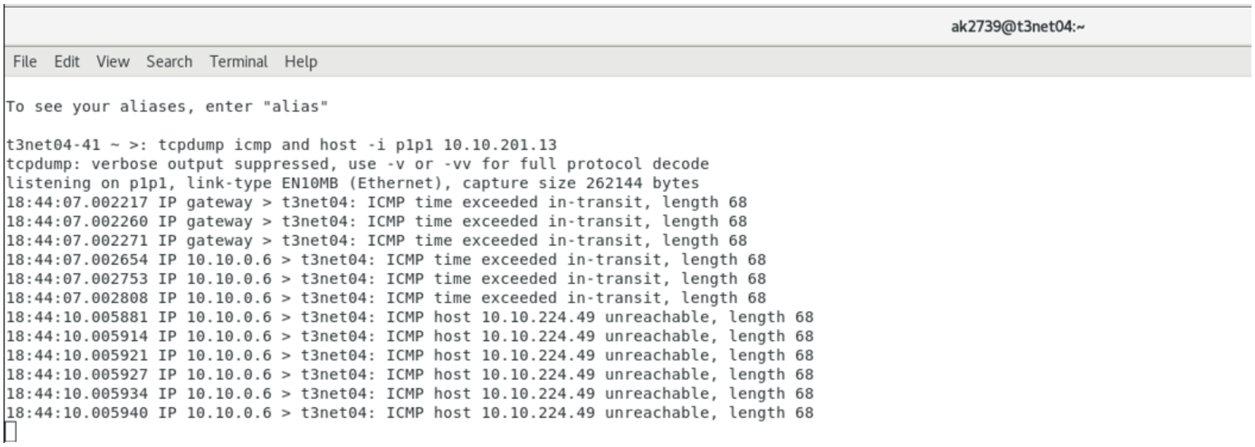
Used traceroute command to get the route towards the gateway which issued ICMP messages.



```
t3net04-41 ~ >: clear
t3net04-42 ~ >: traceroute 10.10.224.49
traceroute to 10.10.224.49 (10.10.224.49), 30 hops max, 60 byte packets
 1  gateway (10.10.201.1)  0.442 ms  0.379 ms  0.317 ms
 2  10.10.0.6 (10.10.0.6)  0.644 ms  0.688 ms  0.688 ms
 3  10.10.0.6 (10.10.0.6)  3003.707 ms !H  3003.611 ms !H  3003.548 ms !H
t3net04-43 ~ >: 
```

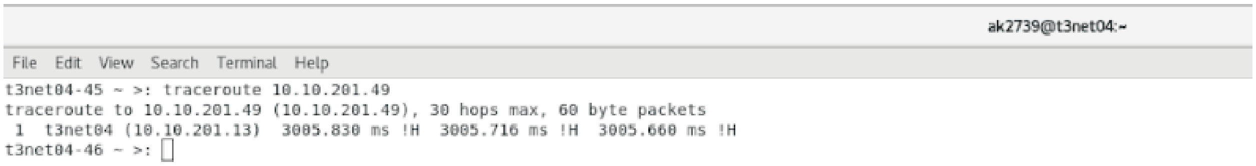
Used the command traceroute 10.10.224.49

Tcp dump output when the traceroute command is running on another terminal



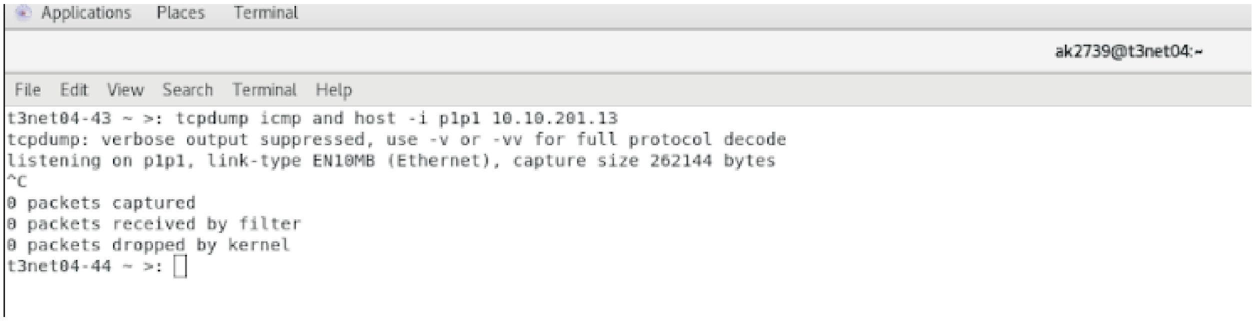
```
To see your aliases, enter "alias"

t3net04-41 ~ >: tcpdump icmp and host -i p1p1 10.10.201.13
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on p1p1, link-type EN10MB (Ethernet), capture size 262144 bytes
18:44:07.002217 IP gateway > t3net04: ICMP time exceeded in-transit, length 68
18:44:07.002260 IP gateway > t3net04: ICMP time exceeded in-transit, length 68
18:44:07.002271 IP gateway > t3net04: ICMP time exceeded in-transit, length 68
18:44:07.002654 IP 10.10.0.6 > t3net04: ICMP time exceeded in-transit, length 68
18:44:07.002753 IP 10.10.0.6 > t3net04: ICMP time exceeded in-transit, length 68
18:44:07.002808 IP 10.10.0.6 > t3net04: ICMP time exceeded in-transit, length 68
18:44:10.005881 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 68
18:44:10.005914 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 68
18:44:10.005921 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 68
18:44:10.005927 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 68
18:44:10.005934 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 68
18:44:10.005940 IP 10.10.0.6 > t3net04: ICMP host 10.10.224.49 unreachable, length 68
```

Used traceroute command to get the route towards the gateway which issued ICMP messages. The ip address for the unreachable host is in the same subnet as t3net04.



```
t3net04-45 ~ >: traceroute 10.10.201.49
traceroute to 10.10.201.49 (10.10.201.49), 30 hops max, 60 byte packets
 1  t3net04 (10.10.201.13)  3005.830 ms !H  3005.716 ms !H  3005.660 ms !H
t3net04-46 ~ >:
```

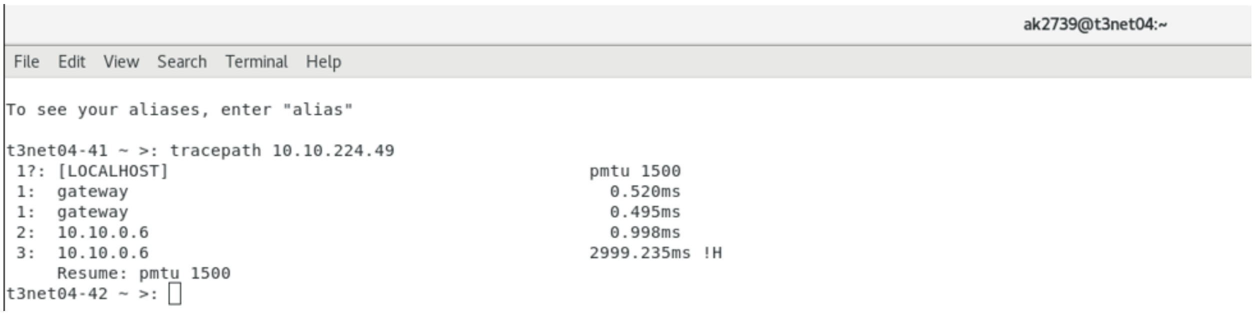
Tcp dump output when the traceroute command is running on another terminal


Applications Places Terminal
ak2739@t3net04:~
File Edit View Search Terminal Help

```
t3net04-43 ~ >: tcpdump icmp and host -i p1p1 10.10.201.13
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on p1p1, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
t3net04-44 ~ >:
```

!H in the traceroute command explains that the ip network is available however the destination host is unreachable. Which clearly explains the traceroute 10.10.201.49 command because the ip address 10.10.201.49 is not a workstation and non-existing host.

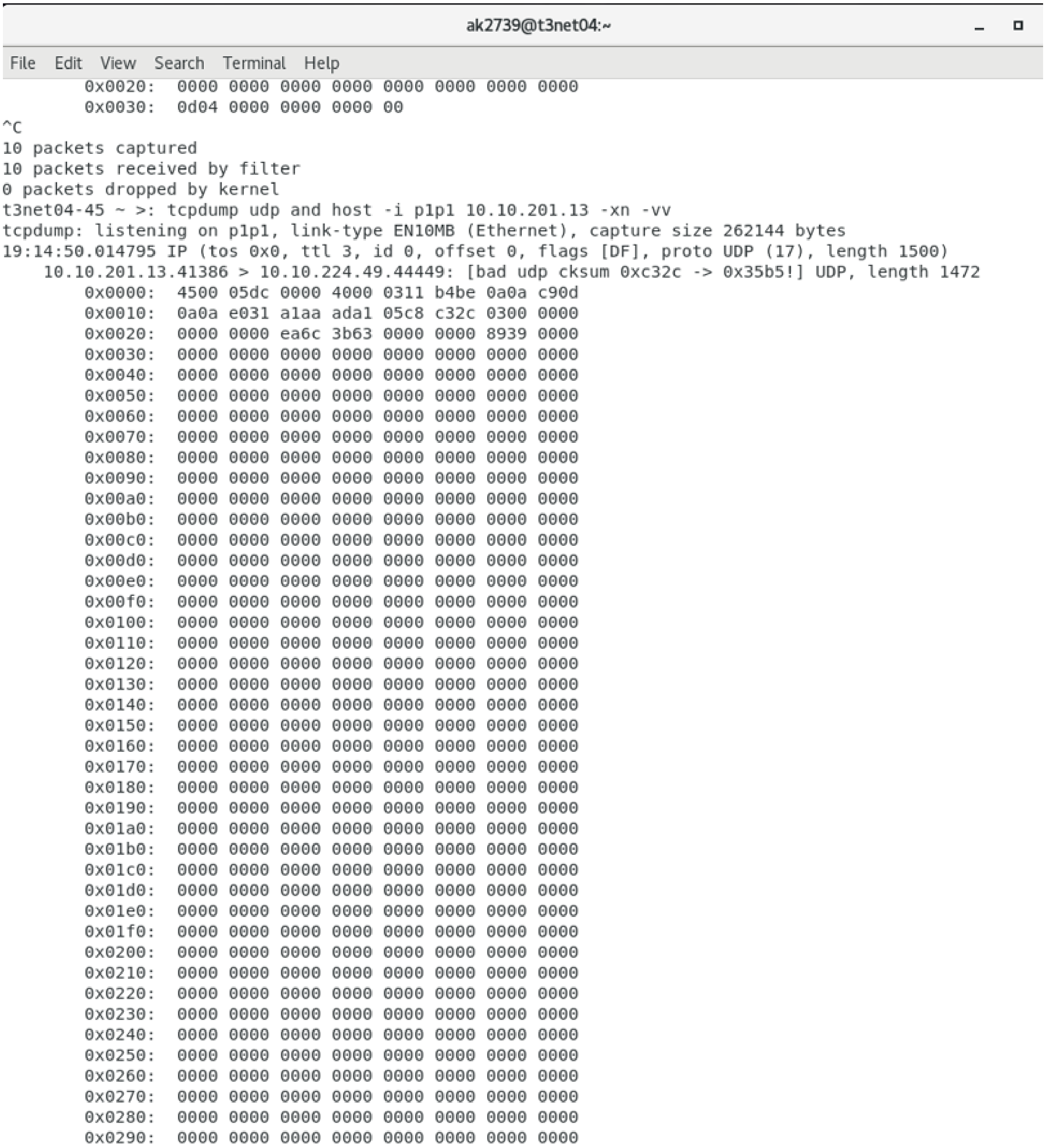
4.2.4 Use “tracepath <unreachable host>”



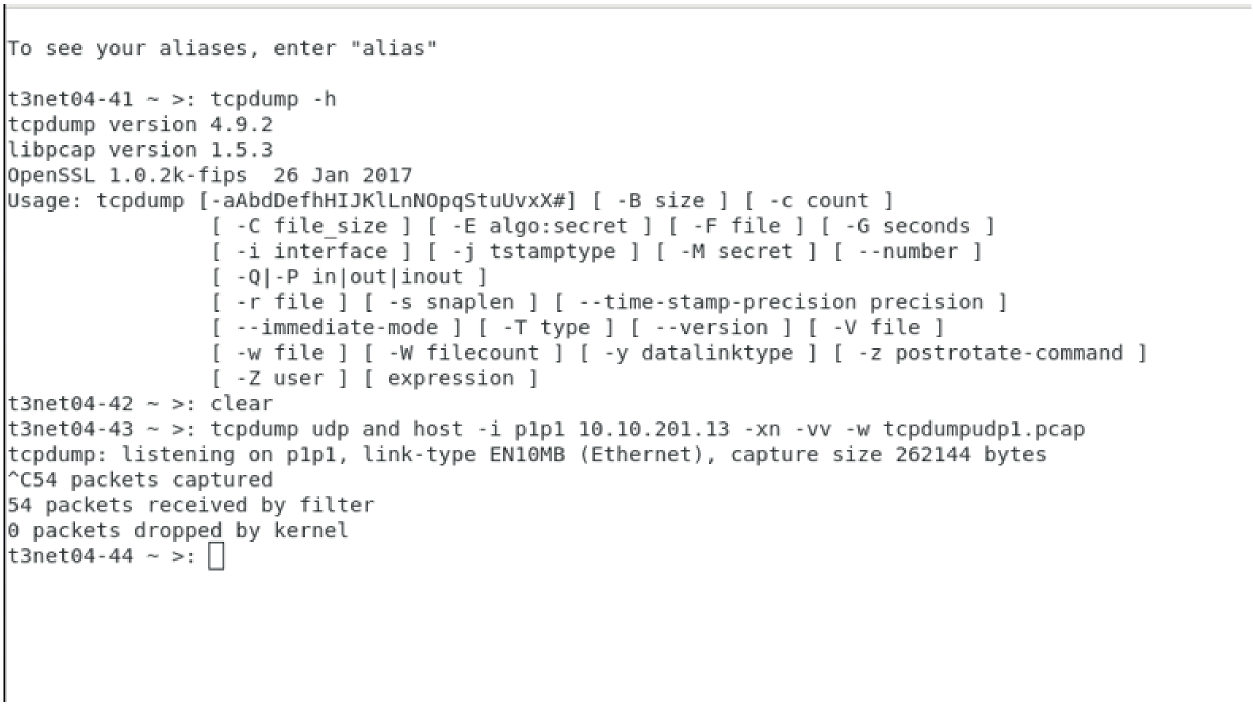
```
To see your aliases, enter "alias"

t3net04-41 ~ >: tracepath 10.10.224.49
 1?: [LOCALHOST]                                         pmtu 1500
 1:  gateway                                               0.520ms
 1:  gateway                                               0.495ms
 2:  10.10.0.6                                             0.998ms
 3:  10.10.0.6                                           2999.235ms !H
     Resume: pmtu 1500
t3net04-42 ~ >: 
```

Traceroute and tracepath are very similar and they map the route data takes from one point in a network to a specific IP server.

Tracepath traces a path to a specific destination using UDP packets.

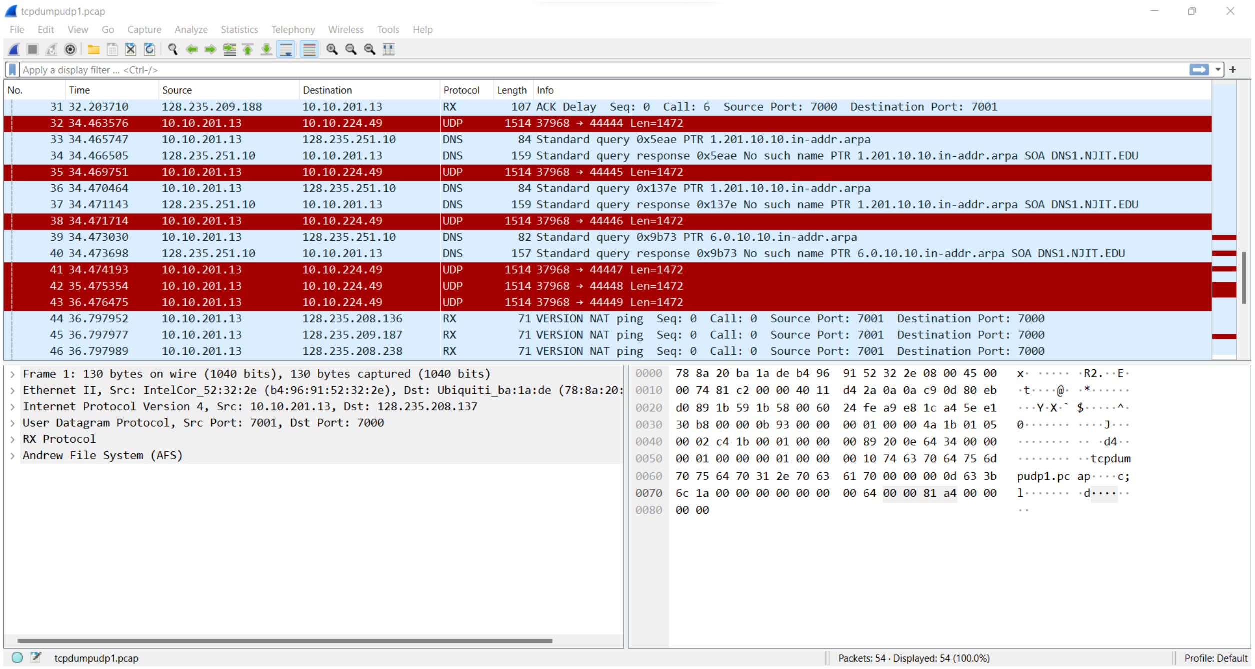


```
        0x0020:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0030:  0d04 0000 0000 0000 00
^C
10 packets captured
10 packets received by filter
0 packets dropped by kernel
t3net04-45 ~ >: tcpdump udp and host -i p1p1 10.10.201.13 -xn -vv
tcpdump: listening on p1p1, link-type EN10MB (Ethernet), capture size 262144 bytes
19:14:50.014795 IP (tos 0x0, ttl 3, id 0, offset 0, flags [DF], proto UDP (17), length 1500)
    10.10.201.13.41386 > 10.10.224.49.44449: [bad udp cksum 0xc32c -> 0x35b5!] UDP, length 1472
        0x0000:  4500 05dc 0000 4000 0311 b4be 0a0a c90d
        0x0010:  0a0a e031 a1aa ada1 05c8 c32c 0300 0000
        0x0020:  0000 0000 ea6c 3b63 0000 0000 8939 0000
        0x0030:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0040:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0050:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0060:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0070:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0080:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0090:  0000 0000 0000 0000 0000 0000 0000 0000
        0x00a0:  0000 0000 0000 0000 0000 0000 0000 0000
        0x00b0:  0000 0000 0000 0000 0000 0000 0000 0000
        0x00c0:  0000 0000 0000 0000 0000 0000 0000 0000
        0x00d0:  0000 0000 0000 0000 0000 0000 0000 0000
        0x00e0:  0000 0000 0000 0000 0000 0000 0000 0000
        0x00f0:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0100:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0110:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0120:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0130:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0140:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0150:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0160:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0170:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0180:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0190:  0000 0000 0000 0000 0000 0000 0000 0000
        0x01a0:  0000 0000 0000 0000 0000 0000 0000 0000
        0x01b0:  0000 0000 0000 0000 0000 0000 0000 0000
        0x01c0:  0000 0000 0000 0000 0000 0000 0000 0000
        0x01d0:  0000 0000 0000 0000 0000 0000 0000 0000
        0x01e0:  0000 0000 0000 0000 0000 0000 0000 0000
        0x01f0:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0200:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0210:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0220:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0230:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0240:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0250:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0260:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0270:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0280:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0290:  0000 0000 0000 0000 0000 0000 0000 0000
```



```
To see your aliases, enter "alias"

t3net04-41 ~ >: tcpdump -h
tcpdump version 4.9.2
libpcap version 1.5.3
OpenSSL 1.0.2k-fips  26 Jan 2017
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqStuUvxX#] [ -B size ] [ -c count ]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ -j tstamptype ] [ -M secret ] [ --number ]
                [ -Q|-P in|out|inout ]
                [ -r file ] [ -s snaplen ] [ --time-stamp-precision precision ]
                [ --immediate-mode ] [ -T type ] [ --version ] [ -V file ]
                [ -w file ] [ -W filecount ] [ -y datalinktype ] [ -z postrotate-command ]
                [ -Z user ] [ expression ]
t3net04-42 ~ >: clear
t3net04-43 ~ >: tcpdump udp and host -i p1p1 10.10.201.13 -xn -vv -w tcpdumpudp1.pcap
tcpdump: listening on p1p1, link-type EN10MB (Ethernet), capture size 262144 bytes
^C54 packets captured
54 packets received by filter
0 packets dropped by kernel
t3net04-44 ~ >: 
```

The command used to save the output of the tcp dump and save it as a .pcap file

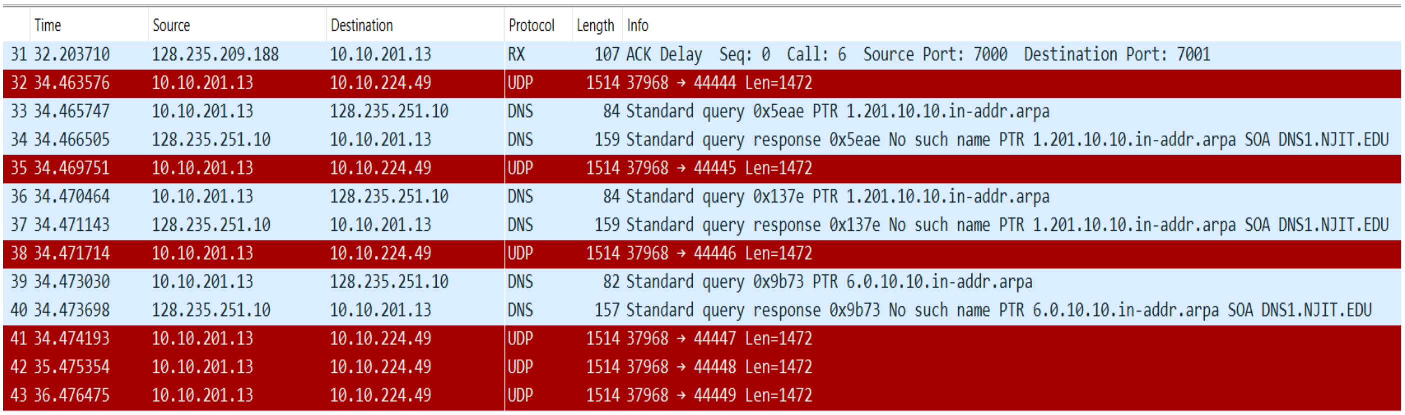

tcpdumpudp1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
tcpdumpudp1.pcap
Packets: 54 · Displayed: 54 (100.0%)
Profile: Default

```
No.   Time       Source            Destination      Protocol Length Info
   31 32.203710  128.235.209.188   10.10.201.13     RX        107 ACK Delay  Seq: 0  Call: 6  Source Port: 7000  Destination Port: 7001
   32 34.463576  10.10.201.13      10.10.224.49     UDP      1514 37968 → 44444 Len=1472
   33 34.465747  10.10.201.13      128.235.251.10   DNS        84 Standard query 0x5eae PTR 1.201.10.10.in-addr.arpa
   34 34.466505  128.235.251.10    10.10.201.13     DNS       159 Standard query response 0x5eae No such name PTR 1.201.10.10.in-addr.arpa SOA DNS1.NJIT.EDU
   35 34.469751  10.10.201.13      10.10.224.49     UDP      1514 37968 → 44445 Len=1472
   36 34.470464  10.10.201.13      128.235.251.10   DNS        84 Standard query 0x137e PTR 1.201.10.10.in-addr.arpa
   37 34.471143  128.235.251.10    10.10.201.13     DNS       159 Standard query response 0x137e No such name PTR 1.201.10.10.in-addr.arpa SOA DNS1.NJIT.EDU
   38 34.471714  10.10.201.13      10.10.224.49     UDP      1514 37968 → 44446 Len=1472
   39 34.473030  10.10.201.13      128.235.251.10   DNS        82 Standard query 0x9b73 PTR 6.0.10.10.in-addr.arpa
   40 34.473698  128.235.251.10    10.10.201.13     DNS       157 Standard query response 0x9b73 No such name PTR 6.0.10.10.in-addr.arpa SOA DNS1.NJIT.EDU
   41 34.474193  10.10.201.13      10.10.224.49     UDP      1514 37968 → 44447 Len=1472
   42 35.475354  10.10.201.13      10.10.224.49     UDP      1514 37968 → 44448 Len=1472
   43 36.476475  10.10.201.13      10.10.224.49     UDP      1514 37968 → 44449 Len=1472
   44 36.797952  10.10.201.13      128.235.208.136  RX         71 VERSION NAT ping  Seq: 0  Call: 0  Source Port: 7001  Destination Port: 7000
   45 36.797977  10.10.201.13      128.235.209.187  RX         71 VERSION NAT ping  Seq: 0  Call: 0  Source Port: 7001  Destination Port: 7000
   46 36.797989  10.10.201.13      128.235.208.238  RX         71 VERSION NAT ping  Seq: 0  Call: 0  Source Port: 7001  Destination Port: 7000
```

```
> Frame 1: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits)
> Ethernet II, Src: IntelCor_52:32:2e (b4:96:91:52:32:2e), Dst: Ubiquiti_ba:1a:de (78:8a:20:
> Internet Protocol Version 4, Src: 10.10.201.13, Dst: 128.235.208.137
> User Datagram Protocol, Src Port: 7001, Dst Port: 7000
> RX Protocol
> Andrew File System (AFS)
```

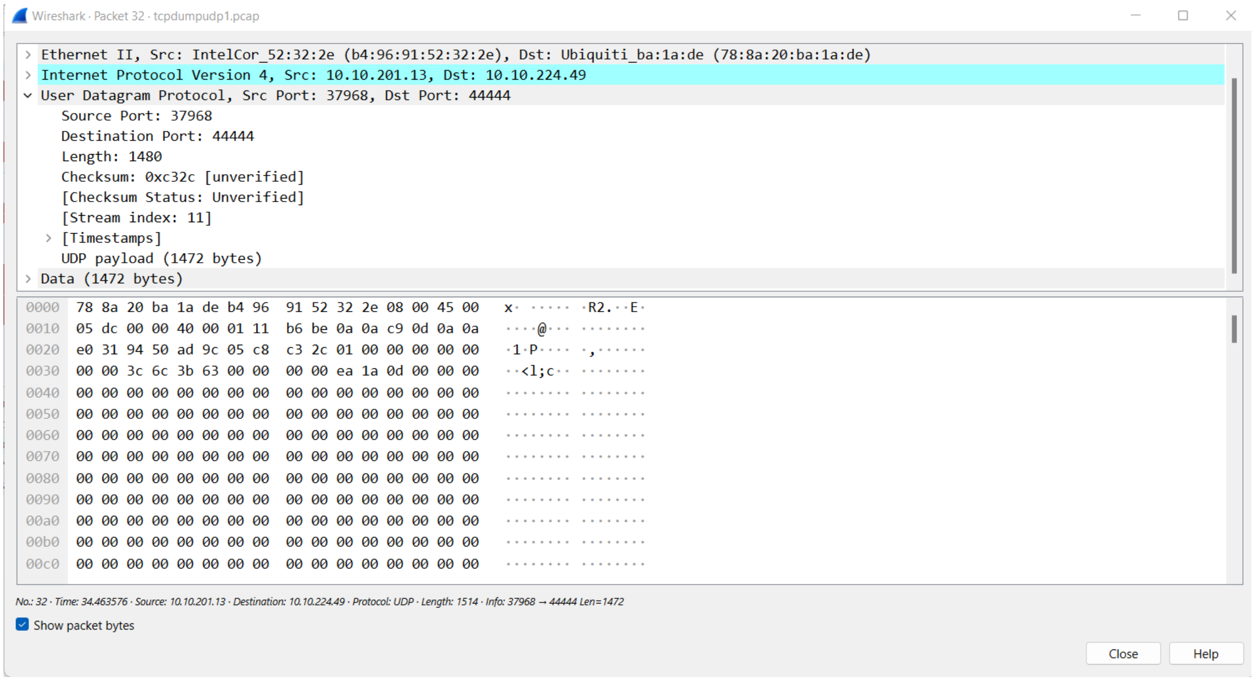
```
0000  78 8a 20 ba 1a de b4 96  91 52 32 2e 08 00 45 00   x· ····· ·R2.··E·
0010  00 74 81 c2 00 00 40 11  d4 2a 0a 0a c9 0d 80 eb   ·t····@· ·*······
0020  d0 89 1b 59 1b 58 00 60  24 fe a9 e8 1c a4 5e e1   ···Y·X·` $·····^·
0030  30 b8 00 00 0b 93 00 00  00 01 00 00 4a 1b 01 05   0······· ····J···
0040  00 02 c4 1b 00 01 00 00  00 89 20 0e 64 34 00 00   ········ ·· ·d4··
0050  00 01 00 00 00 01 00 00  00 10 74 63 70 64 75 6d   ········ ··tcpdum
0060  70 75 64 70 31 2e 70 63  61 70 00 00 00 0d 63 3b   pudp1.pc ap····c;
0070  6c 1a 00 00 00 00 00 00  00 64 00 00 81 a4 00 00   l······· ·d······
0080  00 00                                              ··
```

Using wireshark to decode the .pcap files. The red highlighted packets are of the udp.



```
   Time          Source            Destination     Protocol  Length  Info
31 32.203710     128.235.209.188   10.10.201.13    RX          107 ACK Delay  Seq: 0  Call: 6  Source Port: 7000  Destination Port: 7001
32 34.463576     10.10.201.13      10.10.224.49    UDP        1514 37968 → 44444 Len=1472
33 34.465747     10.10.201.13      128.235.251.10  DNS          84 Standard query 0x5eae PTR 1.201.10.10.in-addr.arpa
34 34.466505     128.235.251.10    10.10.201.13    DNS         159 Standard query response 0x5eae No such name PTR 1.201.10.10.in-addr.arpa SOA DNS1.NJIT.EDU
35 34.469751     10.10.201.13      10.10.224.49    UDP        1514 37968 → 44445 Len=1472
36 34.470464     10.10.201.13      128.235.251.10  DNS          84 Standard query 0x137e PTR 1.201.10.10.in-addr.arpa
37 34.471143     128.235.251.10    10.10.201.13    DNS         159 Standard query response 0x137e No such name PTR 1.201.10.10.in-addr.arpa SOA DNS1.NJIT.EDU
38 34.471714     10.10.201.13      10.10.224.49    UDP        1514 37968 → 44446 Len=1472
39 34.473030     10.10.201.13      128.235.251.10  DNS          82 Standard query 0x9b73 PTR 6.0.10.10.in-addr.arpa
40 34.473698     128.235.251.10    10.10.201.13    DNS         157 Standard query response 0x9b73 No such name PTR 6.0.10.10.in-addr.arpa SOA DNS1.NJIT.EDU
41 34.474193     10.10.201.13      10.10.224.49    UDP        1514 37968 → 44447 Len=1472
42 35.475354     10.10.201.13      10.10.224.49    UDP        1514 37968 → 44448 Len=1472
43 36.476475     10.10.201.13      10.10.224.49    UDP        1514 37968 → 44449 Len=1472
```

The udp packets are highlighted in red.



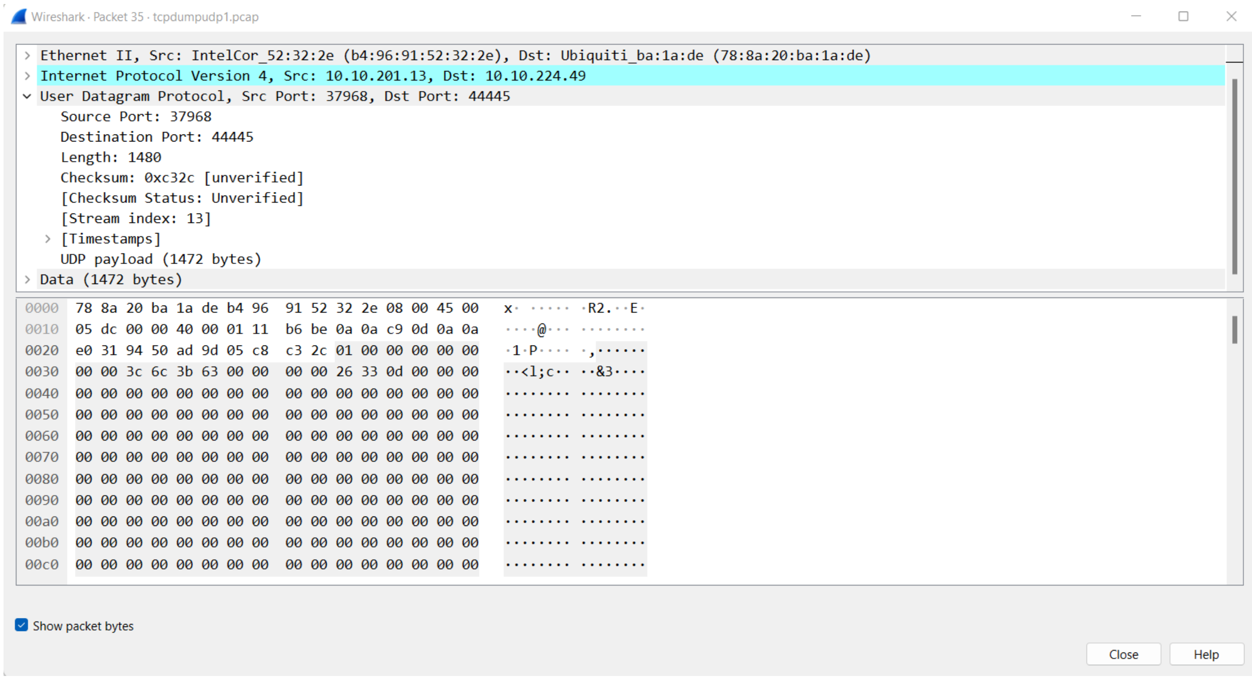
```
> Ethernet II, Src: IntelCor_52:32:2e (b4:96:91:52:32:2e), Dst: Ubiquiti_ba:1a:de (78:8a:20:ba:1a:de)
> Internet Protocol Version 4, Src: 10.10.201.13, Dst: 10.10.224.49
v User Datagram Protocol, Src Port: 37968, Dst Port: 44444
    Source Port: 37968
    Destination Port: 44444
    Length: 1480
    Checksum: 0xc32c [unverified]
    [Checksum Status: Unverified]
    [Stream index: 11]
  > [Timestamps]
    UDP payload (1472 bytes)
> Data (1472 bytes)
```

```
0000  78 8a 20 ba 1a de b4 96  91 52 32 2e 08 00 45 00   x·······R2.··E·
0010  05 dc 00 00 40 00 01 11  b6 be 0a 0a c9 0d 0a 0a   ····@···········
0020  e0 31 94 50 ad 9c 05 c8  c3 2c 01 00 00 00 00 00   ·1·P·····,······
0030  00 00 3c 6c 3b 63 00 00  00 00 ea 1a 0d 00 00 00   ··<l;c··········
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
```

No.: 32 · Time: 34.463576 · Source: 10.10.201.13 · Destination: 10.10.224.49 · Protocol: UDP · Length: 1514 · Info: 37968 → 44444 Len=1472

☑ Show packet bytes

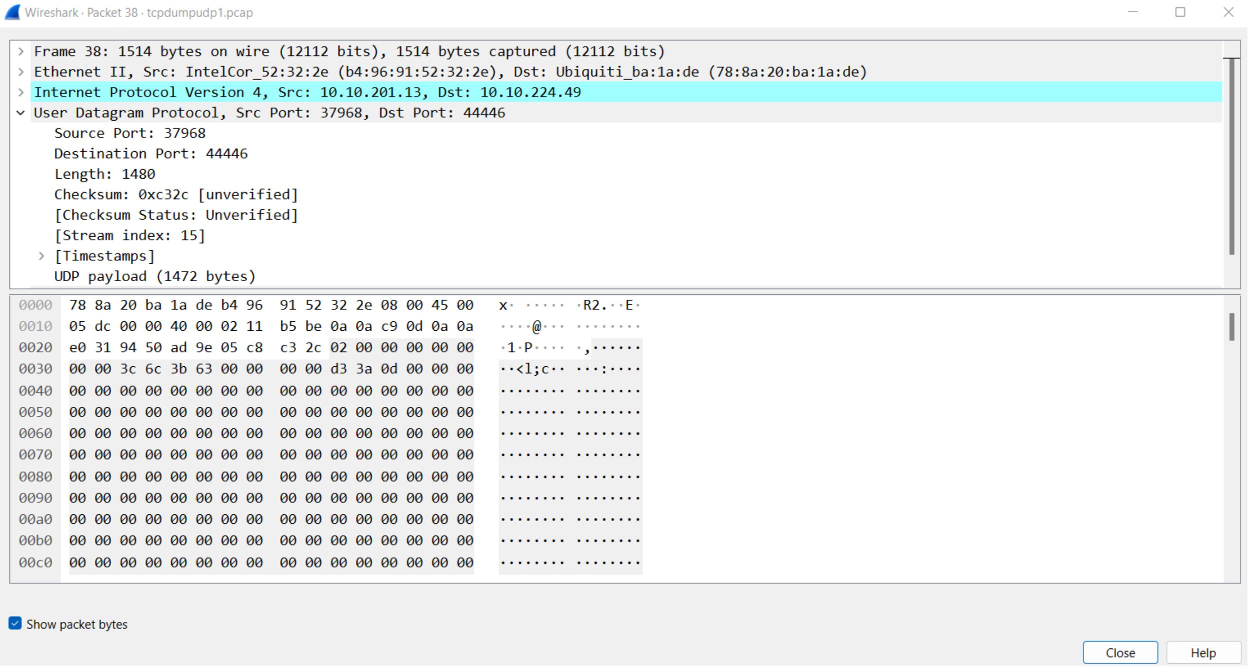
Information about the udp packet. Source port = 37968 and Destination port = 44444. The length of the packet is 1480 bytes and UDP payload = 1472 bytes which means that the data in the UDP packet is 1472 bytes. The message in the figure above shows the actual message that UDP is sending.



```
> Ethernet II, Src: IntelCor_52:32:2e (b4:96:91:52:32:2e), Dst: Ubiquiti_ba:1a:de (78:8a:20:ba:1a:de)
> Internet Protocol Version 4, Src: 10.10.201.13, Dst: 10.10.224.49
v User Datagram Protocol, Src Port: 37968, Dst Port: 44445
    Source Port: 37968
    Destination Port: 44445
    Length: 1480
    Checksum: 0xc32c [unverified]
    [Checksum Status: Unverified]
    [Stream index: 13]
  > [Timestamps]
    UDP payload (1472 bytes)
> Data (1472 bytes)

0000  78 8a 20 ba 1a de b4 96  91 52 32 2e 08 00 45 00   x·······R2.··E·
0010  05 dc 00 00 40 00 01 11  b6 be 0a 0a c9 0d 0a 0a   ····@··· ········
0020  e0 31 94 50 ad 9d 05 c8  c3 2c 01 00 00 00 00 00   ·1·P···· ·,······
0030  00 00 3c 6c 3b 63 00 00  00 00 26 33 0d 00 00 00   ··<l;c·· ··&3····
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

☑ Show packet bytes

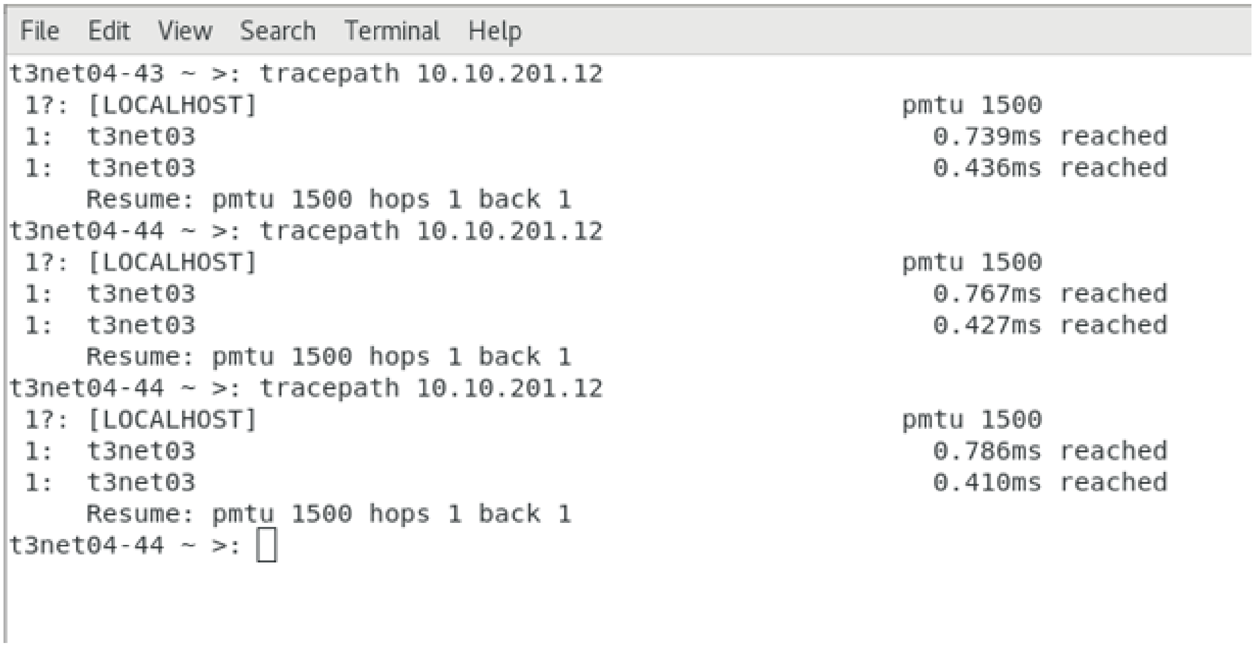
Information about the udp packet. Source port = 37968 and Destination port = 44445. The length of the packet is 1480 bytes and UDP payload = 1472 bytes which means that the data in the UDP packet is 1472 bytes. The message in the figure above shows the actual message that UDP is sending.



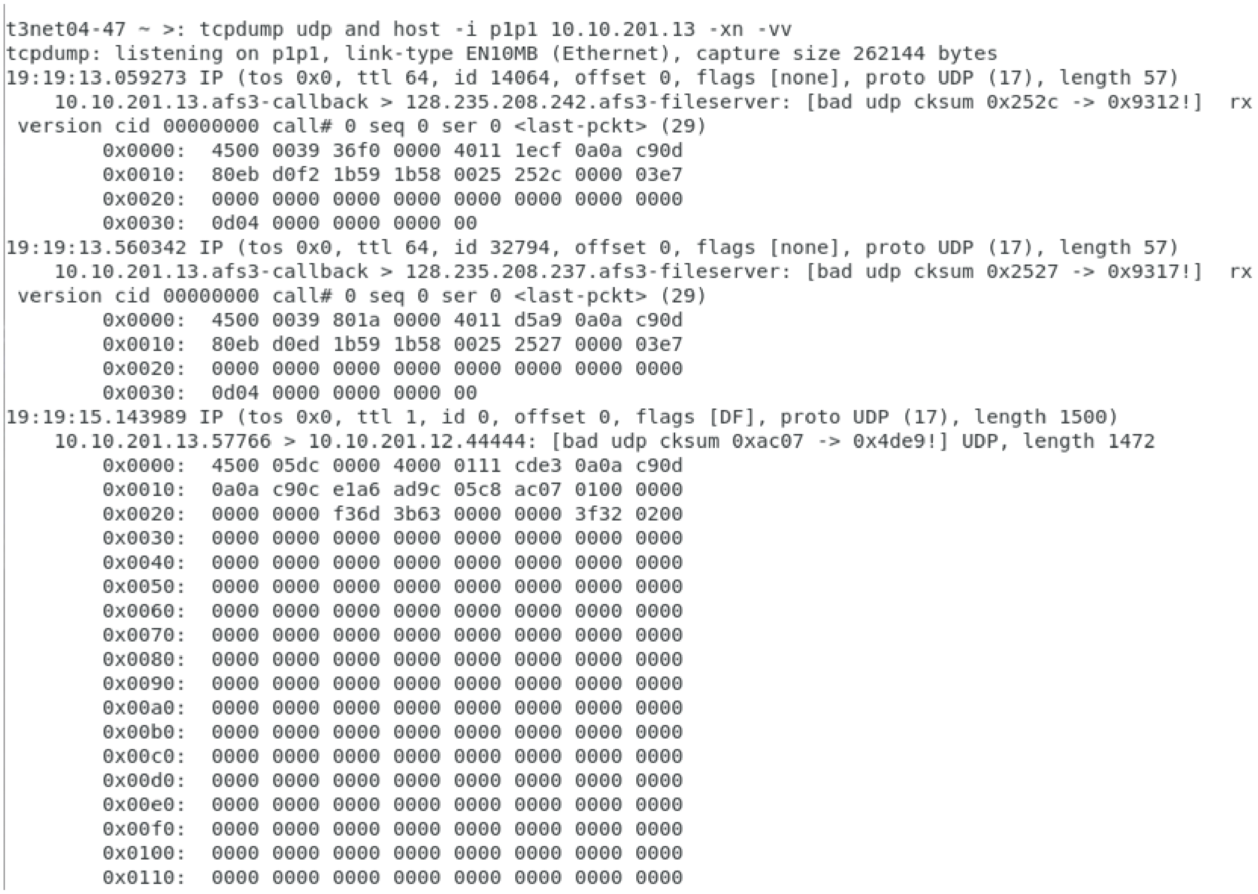
```
> Frame 38: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
> Ethernet II, Src: IntelCor_52:32:2e (b4:96:91:52:32:2e), Dst: Ubiquiti_ba:1a:de (78:8a:20:ba:1a:de)
> Internet Protocol Version 4, Src: 10.10.201.13, Dst: 10.10.224.49
v User Datagram Protocol, Src Port: 37968, Dst Port: 44446
    Source Port: 37968
    Destination Port: 44446
    Length: 1480
    Checksum: 0xc32c [unverified]
    [Checksum Status: Unverified]
    [Stream index: 15]
  > [Timestamps]
    UDP payload (1472 bytes)

0000  78 8a 20 ba 1a de b4 96  91 52 32 2e 08 00 45 00   x·······R2.··E·
0010  05 dc 00 00 40 00 02 11  b5 be 0a 0a c9 0d 0a 0a   ····@··· ········
0020  e0 31 94 50 ad 9e 05 c8  c3 2c 02 00 00 00 00 00   ·1·P···· ·,······
0030  00 00 3c 6c 3b 63 00 00  00 00 d3 3a 0d 00 00 00   ··<l;c·· ···:····
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

☑ Show packet bytes

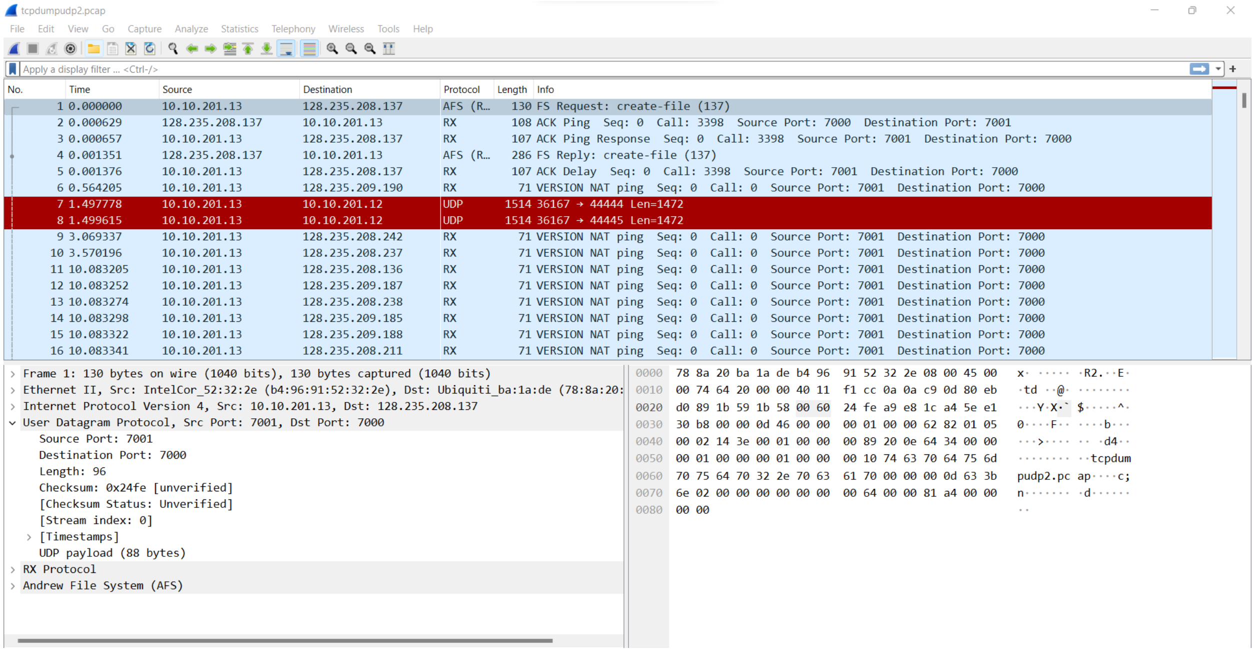
Information about the udp packet. Source port = 37968 and Destination port = 44446. The length of the packet is 1480 bytes and UDP payload = 1472 bytes which means that the data in the UDP packet is 1472 bytes. The message in the figure above shows the actual message that UDP is sending.



```
t3net04-43 ~ >: tracepath 10.10.201.12
 1?: [LOCALHOST]                                         pmtu 1500
 1:  t3net03                                               0.739ms reached
 1:  t3net03                                               0.436ms reached
     Resume: pmtu 1500 hops 1 back 1
t3net04-44 ~ >: tracepath 10.10.201.12
 1?: [LOCALHOST]                                         pmtu 1500
 1:  t3net03                                               0.767ms reached
 1:  t3net03                                               0.427ms reached
     Resume: pmtu 1500 hops 1 back 1
t3net04-44 ~ >: tracepath 10.10.201.12
 1?: [LOCALHOST]                                         pmtu 1500
 1:  t3net03                                               0.786ms reached
 1:  t3net03                                               0.410ms reached
     Resume: pmtu 1500 hops 1 back 1
t3net04-44 ~ >: 
```



```
t3net04-47 ~ >: tcpdump udp and host -i p1p1 10.10.201.13 -xn -vv
tcpdump: listening on p1p1, link-type EN10MB (Ethernet), capture size 262144 bytes
19:19:13.059273 IP (tos 0x0, ttl 64, id 14064, offset 0, flags [none], proto UDP (17), length 57)
    10.10.201.13.afs3-callback > 128.235.208.242.afs3-fileserver: [bad udp cksum 0x252c -> 0x9312!]  rx
 version cid 00000000 call# 0 seq 0 ser 0 <last-pckt> (29)
        0x0000:  4500 0039 36f0 0000 4011 1ecf 0a0a c90d
        0x0010:  80eb d0f2 1b59 1b58 0025 252c 0000 03e7
        0x0020:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0030:  0d04 0000 0000 0000 00
19:19:13.560342 IP (tos 0x0, ttl 64, id 32794, offset 0, flags [none], proto UDP (17), length 57)
    10.10.201.13.afs3-callback > 128.235.208.237.afs3-fileserver: [bad udp cksum 0x2527 -> 0x9317!]  rx
 version cid 00000000 call# 0 seq 0 ser 0 <last-pckt> (29)
        0x0000:  4500 0039 801a 0000 4011 d5a9 0a0a c90d
        0x0010:  80eb d0ed 1b59 1b58 0025 2527 0000 03e7
        0x0020:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0030:  0d04 0000 0000 0000 00
19:19:15.143989 IP (tos 0x0, ttl 1, id 0, offset 0, flags [DF], proto UDP (17), length 1500)
    10.10.201.13.57766 > 10.10.201.12.44444: [bad udp cksum 0xac07 -> 0x4de9!] UDP, length 1472
        0x0000:  4500 05dc 0000 4000 0111 cde3 0a0a c90d
        0x0010:  0a0a c90c e1a6 ad9c 05c8 ac07 0100 0000
        0x0020:  0000 0000 f36d 3b63 0000 0000 3f32 0200
        0x0030:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0040:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0050:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0060:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0070:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0080:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0090:  0000 0000 0000 0000 0000 0000 0000 0000
        0x00a0:  0000 0000 0000 0000 0000 0000 0000 0000
        0x00b0:  0000 0000 0000 0000 0000 0000 0000 0000
        0x00c0:  0000 0000 0000 0000 0000 0000 0000 0000
        0x00d0:  0000 0000 0000 0000 0000 0000 0000 0000
        0x00e0:  0000 0000 0000 0000 0000 0000 0000 0000
        0x00f0:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0100:  0000 0000 0000 0000 0000 0000 0000 0000
        0x0110:  0000 0000 0000 0000 0000 0000 0000 0000
```

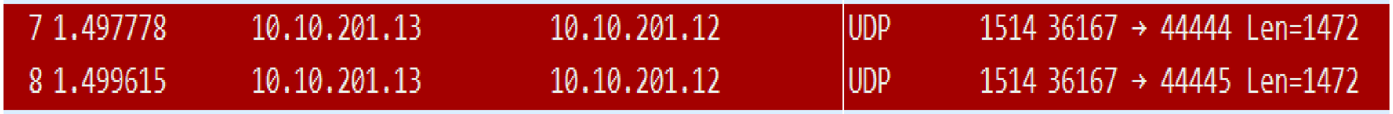


```
No.  Time       Source          Destination     Protocol Length Info
   1 0.000000   10.10.201.13    128.235.208.137 AFS (R…   130 FS Request: create-file (137)
   2 0.000629   128.235.208.137 10.10.201.13    RX        108 ACK Ping  Seq: 0  Call: 3398  Source Port: 7000  Destination Port: 7001
   3 0.000657   10.10.201.13    128.235.208.137 RX        107 ACK Ping Response  Seq: 0  Call: 3398  Source Port: 7001  Destination Port: 7000
   4 0.001351   128.235.208.137 10.10.201.13    AFS (R…   286 FS Reply: create-file (137)
   5 0.001376   10.10.201.13    128.235.208.137 RX        107 ACK Delay  Seq: 0  Call: 3398  Source Port: 7001  Destination Port: 7000
   6 0.564205   10.10.201.13    128.235.209.190 RX         71 VERSION NAT ping  Seq: 0  Call: 0  Source Port: 7001  Destination Port: 7000
   7 1.497778   10.10.201.13    10.10.201.12    UDP      1514 36167 → 44444 Len=1472
   8 1.499615   10.10.201.13    10.10.201.12    UDP      1514 36167 → 44445 Len=1472
   9 3.069337   10.10.201.13    128.235.208.242 RX         71 VERSION NAT ping  Seq: 0  Call: 0  Source Port: 7001  Destination Port: 7000
  10 3.570196   10.10.201.13    128.235.208.237 RX         71 VERSION NAT ping  Seq: 0  Call: 0  Source Port: 7001  Destination Port: 7000
  11 10.083205  10.10.201.13    128.235.208.136 RX         71 VERSION NAT ping  Seq: 0  Call: 0  Source Port: 7001  Destination Port: 7000
  12 10.083252  10.10.201.13    128.235.209.187 RX         71 VERSION NAT ping  Seq: 0  Call: 0  Source Port: 7001  Destination Port: 7000
  13 10.083274  10.10.201.13    128.235.208.238 RX         71 VERSION NAT ping  Seq: 0  Call: 0  Source Port: 7001  Destination Port: 7000
  14 10.083298  10.10.201.13    128.235.209.185 RX         71 VERSION NAT ping  Seq: 0  Call: 0  Source Port: 7001  Destination Port: 7000
  15 10.083322  10.10.201.13    128.235.209.188 RX         71 VERSION NAT ping  Seq: 0  Call: 0  Source Port: 7001  Destination Port: 7000
  16 10.083341  10.10.201.13    128.235.208.211 RX         71 VERSION NAT ping  Seq: 0  Call: 0  Source Port: 7001  Destination Port: 7000
```

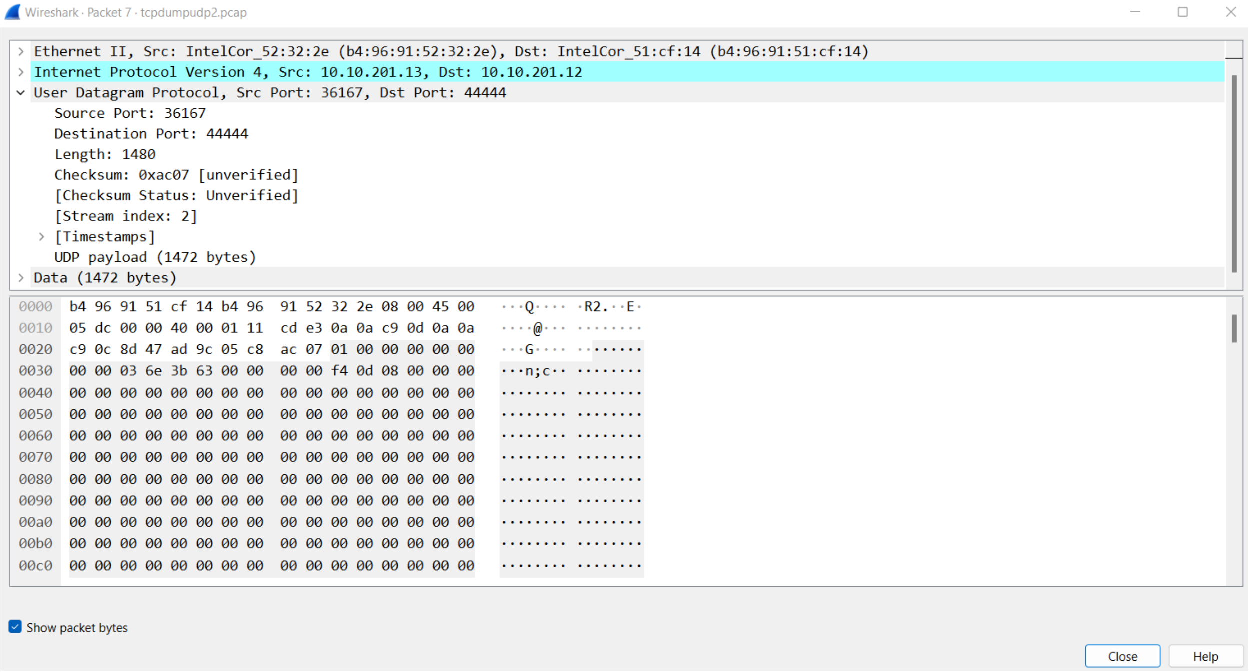
```
> Frame 1: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits)
> Ethernet II, Src: IntelCor_52:32:2e (b4:96:91:52:32:2e), Dst: Ubiquiti_ba:1a:de (78:8a:20:
> Internet Protocol Version 4, Src: 10.10.201.13, Dst: 128.235.208.137
v User Datagram Protocol, Src Port: 7001, Dst Port: 7000
    Source Port: 7001
    Destination Port: 7000
    Length: 96
    Checksum: 0x24fe [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (88 bytes)
> RX Protocol
> Andrew File System (AFS)
```

```
0000  78 8a 20 ba 1a de b4 96  91 52 32 2e 08 00 45 00   x· ····· ·R2.··E·
0010  00 74 64 20 00 00 40 11  f1 cc 0a 0a c9 0d 80 eb   ·td ··@· ········
0020  d0 89 1b 59 1b 58 00 60  24 fe a9 e8 1c a4 5e e1   ···Y·X·` $·····^·
0030  30 b8 00 00 0d 46 00 00  00 01 00 00 62 82 01 05   0····F·· ····b···
0040  00 02 14 3e 00 01 00 00  00 89 20 0e 64 34 00 00   ···>···· ·· ·d4··
0050  00 01 00 00 00 01 00 00  00 10 74 63 70 64 75 6d   ········ ··tcpdum
0060  70 75 64 70 32 2e 70 63  61 70 00 00 00 0d 63 3b   pudp2.pc ap····c;
0070  6e 02 00 00 00 00 00 00  00 64 00 00 81 a4 00 00   n······· ·d······
0080  00 00                                              ··
```

Using wireshark to decode the UDP packets saved i the .pcap file



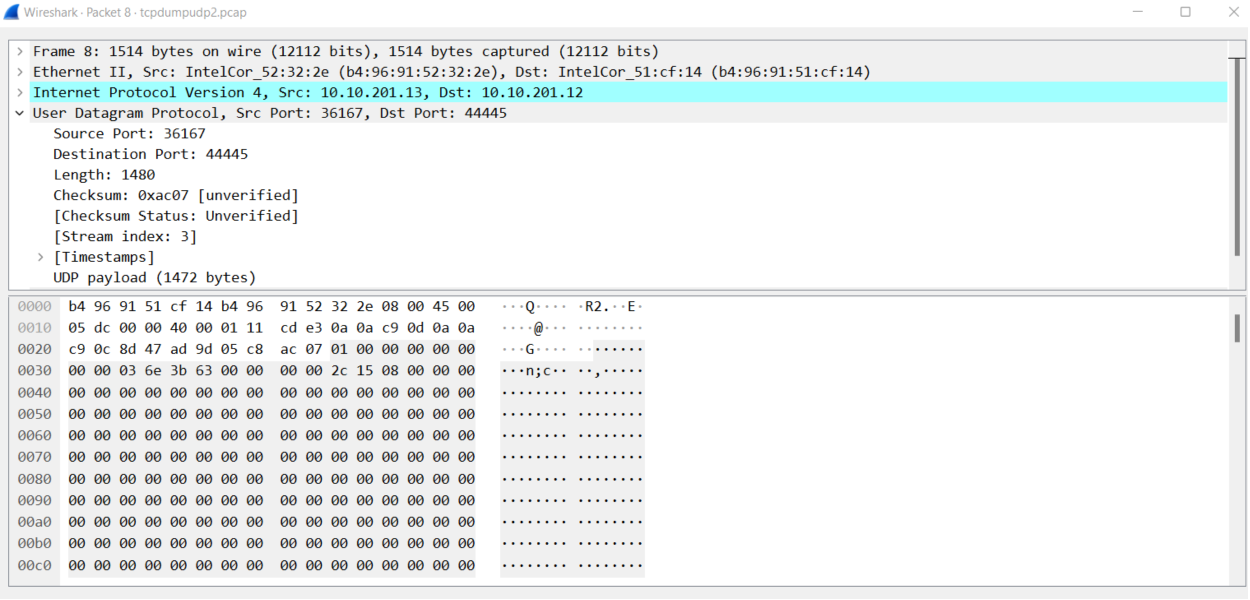
```
7 1.497778    10.10.201.13    10.10.201.12    UDP    1514 36167 → 44444 Len=1472
8 1.499615    10.10.201.13    10.10.201.12    UDP    1514 36167 → 44445 Len=1472
```



```
> Ethernet II, Src: IntelCor_52:32:2e (b4:96:91:52:32:2e), Dst: IntelCor_51:cf:14 (b4:96:91:51:cf:14)
> Internet Protocol Version 4, Src: 10.10.201.13, Dst: 10.10.201.12
v User Datagram Protocol, Src Port: 36167, Dst Port: 44444
    Source Port: 36167
    Destination Port: 44444
    Length: 1480
    Checksum: 0xac07 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
  > [Timestamps]
    UDP payload (1472 bytes)
> Data (1472 bytes)

0000  b4 96 91 51 cf 14 b4 96  91 52 32 2e 08 00 45 00   ···Q···· ·R2.··E·
0010  05 dc 00 00 40 00 01 11  cd e3 0a 0a c9 0d 0a 0a   ····@··· ········
0020  c9 0c 8d 47 ad 9c 05 c8  ac 07 01 00 00 00 00 00   ···G···· ········
0030  00 00 03 6e 3b 63 00 00  00 00 f4 0d 08 00 00 00   ···n;c·· ········
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

☑ Show packet bytes

Information about the udp packet. Source port = 36167 and Destination port = 44444. The length of the packet is 1480 bytes and UDP payload = 1472 bytes which means that the data in the UDP packet is 1472 bytes. The message in the figure above shows the actual message that UDP is sending.

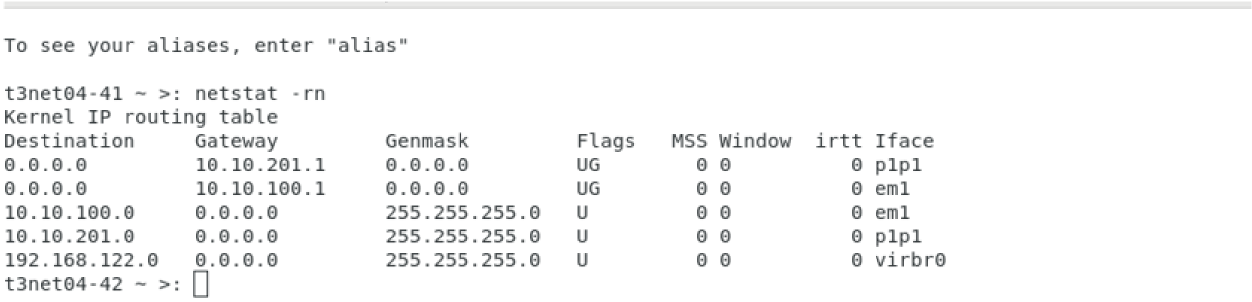


```
> Frame 8: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
> Ethernet II, Src: IntelCor_52:32:2e (b4:96:91:52:32:2e), Dst: IntelCor_51:cf:14 (b4:96:91:51:cf:14)
> Internet Protocol Version 4, Src: 10.10.201.13, Dst: 10.10.201.12
v User Datagram Protocol, Src Port: 36167, Dst Port: 44445
    Source Port: 36167
    Destination Port: 44445
    Length: 1480
    Checksum: 0xac07 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
  > [Timestamps]
    UDP payload (1472 bytes)
```

```
0000  b4 96 91 51 cf 14 b4 96  91 52 32 2e 08 00 45 00   ···Q···· ·R2.··E·
0010  05 dc 00 00 40 00 01 11  cd e3 0a 0a c9 0d 0a 0a   ····@··· ········
0020  c9 0c 8d 47 ad 9d 05 c8  ac 07 01 00 00 00 00 00   ···G···· ········
0030  00 00 03 6e 3b 63 00 00  00 00 2c 15 08 00 00 00   ···n;c·· ··,·····
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

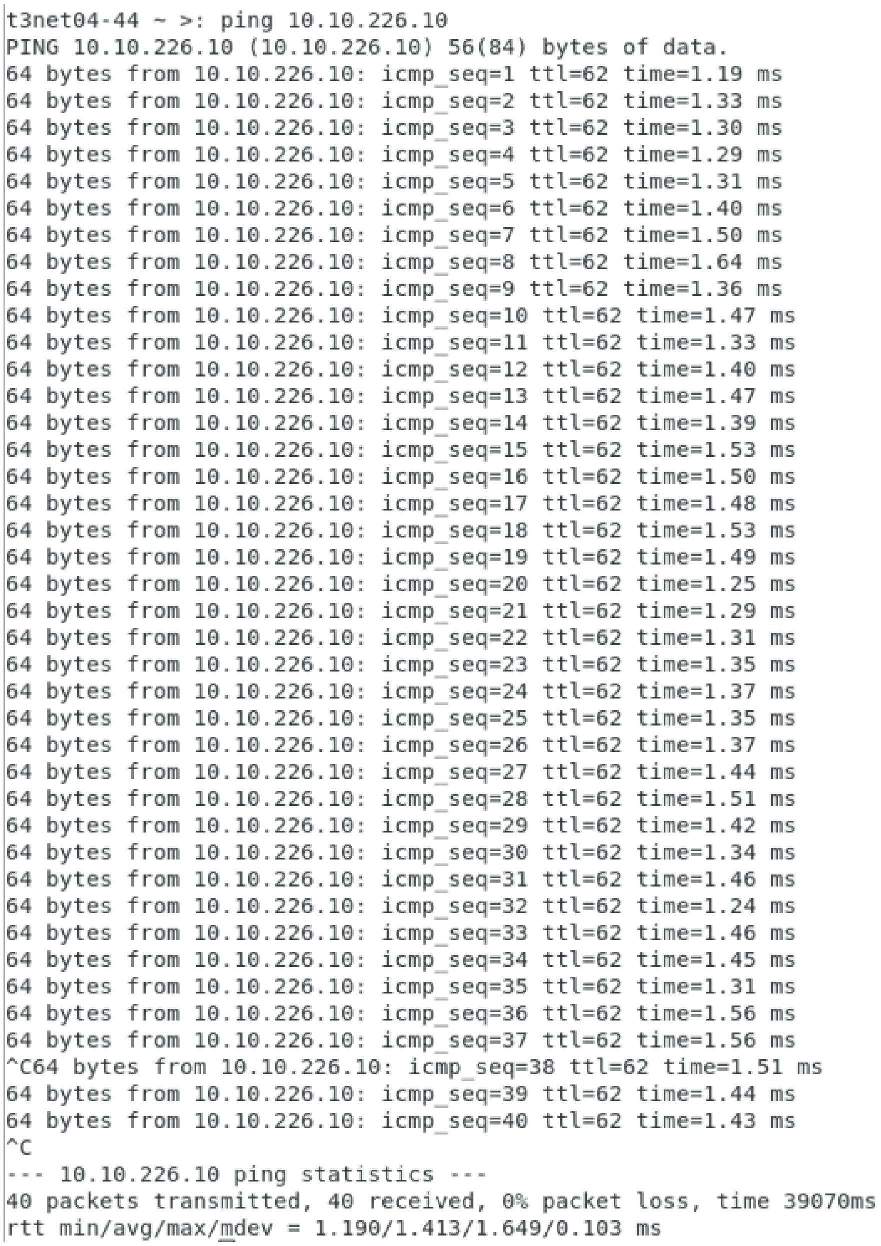
Information about the udp packet. Source port = 37968 and Destination port = 44445. The length of the packet is 1480 bytes and UDP payload = 1472 bytes which means that the data in the UDP packet is 1472 bytes. The message in the figure above shows the actual message that UDP is sending.

4.2.5 ICMP redirect message



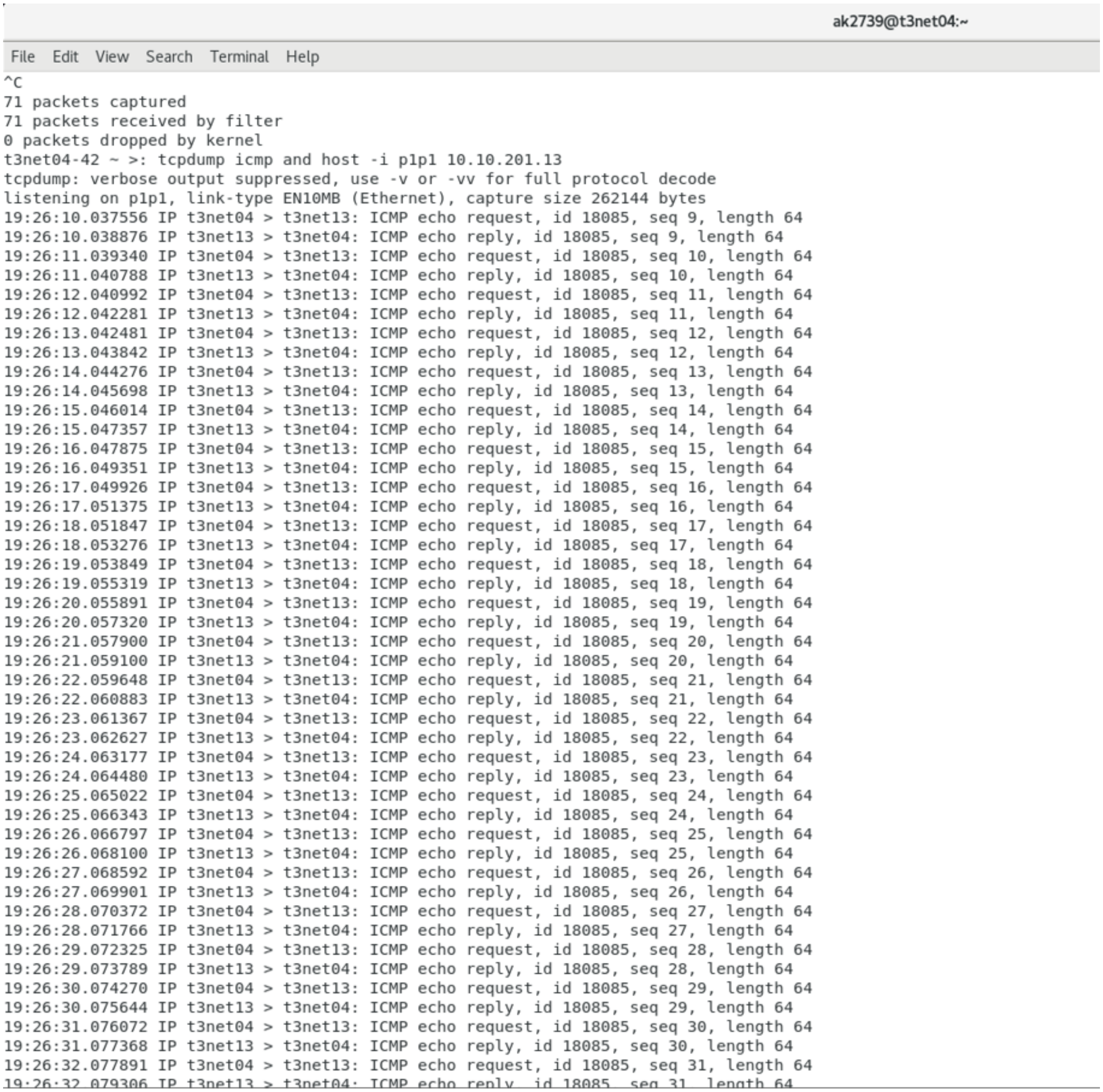
```
To see your aliases, enter "alias"

t3net04-41 ~ >: netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         10.10.201.1     0.0.0.0         UG        0 0          0 p1p1
0.0.0.0         10.10.100.1     0.0.0.0         UG        0 0          0 em1
10.10.100.0     0.0.0.0         255.255.255.0   U         0 0          0 em1
10.10.201.0     0.0.0.0         255.255.255.0   U         0 0          0 p1p1
192.168.122.0   0.0.0.0         255.255.255.0   U         0 0          0 virbr0
t3net04-42 ~ >: 
```

Netstat -rn command was used to find the routing table



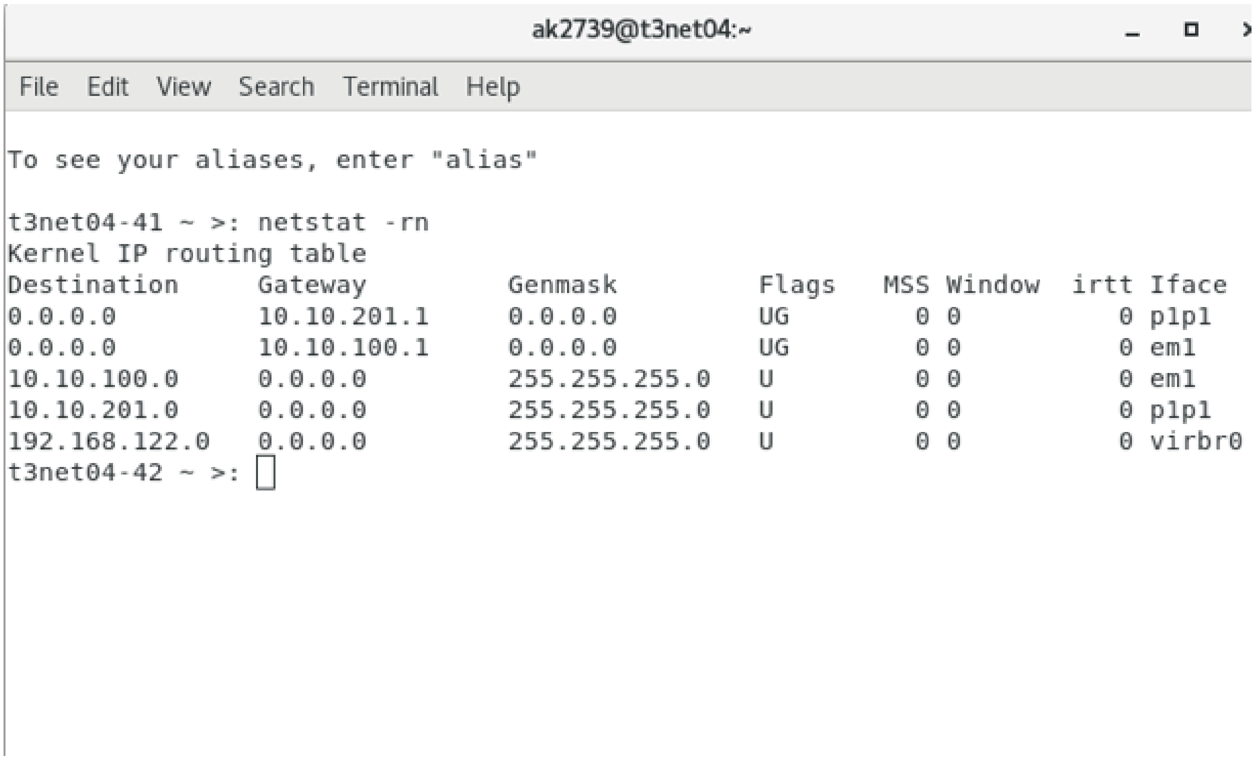
```
t3net04-44 ~ >: ping 10.10.226.10
PING 10.10.226.10 (10.10.226.10) 56(84) bytes of data.
64 bytes from 10.10.226.10: icmp_seq=1 ttl=62 time=1.19 ms
64 bytes from 10.10.226.10: icmp_seq=2 ttl=62 time=1.33 ms
64 bytes from 10.10.226.10: icmp_seq=3 ttl=62 time=1.30 ms
64 bytes from 10.10.226.10: icmp_seq=4 ttl=62 time=1.29 ms
64 bytes from 10.10.226.10: icmp_seq=5 ttl=62 time=1.31 ms
64 bytes from 10.10.226.10: icmp_seq=6 ttl=62 time=1.40 ms
64 bytes from 10.10.226.10: icmp_seq=7 ttl=62 time=1.50 ms
64 bytes from 10.10.226.10: icmp_seq=8 ttl=62 time=1.64 ms
64 bytes from 10.10.226.10: icmp_seq=9 ttl=62 time=1.36 ms
64 bytes from 10.10.226.10: icmp_seq=10 ttl=62 time=1.47 ms
64 bytes from 10.10.226.10: icmp_seq=11 ttl=62 time=1.33 ms
64 bytes from 10.10.226.10: icmp_seq=12 ttl=62 time=1.40 ms
64 bytes from 10.10.226.10: icmp_seq=13 ttl=62 time=1.47 ms
64 bytes from 10.10.226.10: icmp_seq=14 ttl=62 time=1.39 ms
64 bytes from 10.10.226.10: icmp_seq=15 ttl=62 time=1.53 ms
64 bytes from 10.10.226.10: icmp_seq=16 ttl=62 time=1.50 ms
64 bytes from 10.10.226.10: icmp_seq=17 ttl=62 time=1.48 ms
64 bytes from 10.10.226.10: icmp_seq=18 ttl=62 time=1.53 ms
64 bytes from 10.10.226.10: icmp_seq=19 ttl=62 time=1.49 ms
64 bytes from 10.10.226.10: icmp_seq=20 ttl=62 time=1.25 ms
64 bytes from 10.10.226.10: icmp_seq=21 ttl=62 time=1.29 ms
64 bytes from 10.10.226.10: icmp_seq=22 ttl=62 time=1.31 ms
64 bytes from 10.10.226.10: icmp_seq=23 ttl=62 time=1.35 ms
64 bytes from 10.10.226.10: icmp_seq=24 ttl=62 time=1.37 ms
64 bytes from 10.10.226.10: icmp_seq=25 ttl=62 time=1.35 ms
64 bytes from 10.10.226.10: icmp_seq=26 ttl=62 time=1.37 ms
64 bytes from 10.10.226.10: icmp_seq=27 ttl=62 time=1.44 ms
64 bytes from 10.10.226.10: icmp_seq=28 ttl=62 time=1.51 ms
64 bytes from 10.10.226.10: icmp_seq=29 ttl=62 time=1.42 ms
64 bytes from 10.10.226.10: icmp_seq=30 ttl=62 time=1.34 ms
64 bytes from 10.10.226.10: icmp_seq=31 ttl=62 time=1.46 ms
64 bytes from 10.10.226.10: icmp_seq=32 ttl=62 time=1.24 ms
64 bytes from 10.10.226.10: icmp_seq=33 ttl=62 time=1.46 ms
64 bytes from 10.10.226.10: icmp_seq=34 ttl=62 time=1.45 ms
64 bytes from 10.10.226.10: icmp_seq=35 ttl=62 time=1.31 ms
64 bytes from 10.10.226.10: icmp_seq=36 ttl=62 time=1.56 ms
64 bytes from 10.10.226.10: icmp_seq=37 ttl=62 time=1.56 ms
^C64 bytes from 10.10.226.10: icmp_seq=38 ttl=62 time=1.51 ms
64 bytes from 10.10.226.10: icmp_seq=39 ttl=62 time=1.44 ms
64 bytes from 10.10.226.10: icmp_seq=40 ttl=62 time=1.43 ms
^C
--- 10.10.226.10 ping statistics ---
40 packets transmitted, 40 received, 0% packet loss, time 39070ms
rtt min/avg/max/mdev = 1.190/1.413/1.649/0.103 ms
```

Ping command for the host with p1p1 interface address.



```
^C
71 packets captured
71 packets received by filter
0 packets dropped by kernel
t3net04-42 ~ >: tcpdump icmp and host -i p1p1 10.10.201.13
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on p1p1, link-type EN10MB (Ethernet), capture size 262144 bytes
19:26:10.037556 IP t3net04 > t3net13: ICMP echo request, id 18085, seq 9, length 64
19:26:10.038876 IP t3net13 > t3net04: ICMP echo reply, id 18085, seq 9, length 64
19:26:11.039340 IP t3net04 > t3net13: ICMP echo request, id 18085, seq 10, length 64
19:26:11.040788 IP t3net13 > t3net04: ICMP echo reply, id 18085, seq 10, length 64
19:26:12.040992 IP t3net04 > t3net13: ICMP echo request, id 18085, seq 11, length 64
19:26:12.042281 IP t3net13 > t3net04: ICMP echo reply, id 18085, seq 11, length 64
19:26:13.042481 IP t3net04 > t3net13: ICMP echo request, id 18085, seq 12, length 64
19:26:13.043842 IP t3net13 > t3net04: ICMP echo reply, id 18085, seq 12, length 64
19:26:14.044276 IP t3net04 > t3net13: ICMP echo request, id 18085, seq 13, length 64
19:26:14.045698 IP t3net13 > t3net04: ICMP echo reply, id 18085, seq 13, length 64
19:26:15.046014 IP t3net04 > t3net13: ICMP echo request, id 18085, seq 14, length 64
19:26:15.047357 IP t3net13 > t3net04: ICMP echo reply, id 18085, seq 14, length 64
19:26:16.047875 IP t3net04 > t3net13: ICMP echo request, id 18085, seq 15, length 64
19:26:16.049351 IP t3net13 > t3net04: ICMP echo reply, id 18085, seq 15, length 64
19:26:17.049926 IP t3net04 > t3net13: ICMP echo request, id 18085, seq 16, length 64
19:26:17.051375 IP t3net13 > t3net04: ICMP echo reply, id 18085, seq 16, length 64
19:26:18.051847 IP t3net04 > t3net13: ICMP echo request, id 18085, seq 17, length 64
19:26:18.053276 IP t3net13 > t3net04: ICMP echo reply, id 18085, seq 17, length 64
19:26:19.053849 IP t3net04 > t3net13: ICMP echo request, id 18085, seq 18, length 64
19:26:19.055319 IP t3net13 > t3net04: ICMP echo reply, id 18085, seq 18, length 64
19:26:20.055891 IP t3net04 > t3net13: ICMP echo request, id 18085, seq 19, length 64
19:26:20.057320 IP t3net13 > t3net04: ICMP echo reply, id 18085, seq 19, length 64
19:26:21.057900 IP t3net04 > t3net13: ICMP echo request, id 18085, seq 20, length 64
19:26:21.059100 IP t3net13 > t3net04: ICMP echo reply, id 18085, seq 20, length 64
19:26:22.059648 IP t3net04 > t3net13: ICMP echo request, id 18085, seq 21, length 64
19:26:22.060883 IP t3net13 > t3net04: ICMP echo reply, id 18085, seq 21, length 64
19:26:23.061367 IP t3net04 > t3net13: ICMP echo request, id 18085, seq 22, length 64
19:26:23.062627 IP t3net13 > t3net04: ICMP echo reply, id 18085, seq 22, length 64
19:26:24.063177 IP t3net04 > t3net13: ICMP echo request, id 18085, seq 23, length 64
19:26:24.064480 IP t3net13 > t3net04: ICMP echo reply, id 18085, seq 23, length 64
19:26:25.065022 IP t3net04 > t3net13: ICMP echo request, id 18085, seq 24, length 64
19:26:25.066343 IP t3net13 > t3net04: ICMP echo reply, id 18085, seq 24, length 64
19:26:26.066797 IP t3net04 > t3net13: ICMP echo request, id 18085, seq 25, length 64
19:26:26.068100 IP t3net13 > t3net04: ICMP echo reply, id 18085, seq 25, length 64
19:26:27.068592 IP t3net04 > t3net13: ICMP echo request, id 18085, seq 26, length 64
19:26:27.069901 IP t3net13 > t3net04: ICMP echo reply, id 18085, seq 26, length 64
19:26:28.070372 IP t3net04 > t3net13: ICMP echo request, id 18085, seq 27, length 64
19:26:28.071766 IP t3net13 > t3net04: ICMP echo reply, id 18085, seq 27, length 64
19:26:29.072325 IP t3net04 > t3net13: ICMP echo request, id 18085, seq 28, length 64
19:26:29.073789 IP t3net13 > t3net04: ICMP echo reply, id 18085, seq 28, length 64
19:26:30.074270 IP t3net04 > t3net13: ICMP echo request, id 18085, seq 29, length 64
19:26:30.075644 IP t3net13 > t3net04: ICMP echo reply, id 18085, seq 29, length 64
19:26:31.076072 IP t3net04 > t3net13: ICMP echo request, id 18085, seq 30, length 64
19:26:31.077368 IP t3net13 > t3net04: ICMP echo reply, id 18085, seq 30, length 64
19:26:32.077891 IP t3net04 > t3net13: ICMP echo request, id 18085, seq 31, length 64
19:26:32.079306 IP t3net13 > t3net04: ICMP echo reply, id 18085, seq 31, length 64
```

Tcp dump icmp packets results while the ping command was running in another terminal. It consists of icmp packets with echo request and echo reply. The id for each message is 18085 and the length for each packet is 64. The echo requests are issued from t3net04(current workstation) to t3net13(the plp1 interface where the ping command is running). And echo reply messages are from t3net14 to t3net04.



```
To see your aliases, enter "alias"

t3net04-41 ~ >: netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         10.10.201.1     0.0.0.0         UG        0 0          0 p1p1
0.0.0.0         10.10.100.1     0.0.0.0         UG        0 0          0 em1
10.10.100.0     0.0.0.0         255.255.255.0   U         0 0          0 em1
10.10.201.0     0.0.0.0         255.255.255.0   U         0 0          0 p1p1
192.168.122.0   0.0.0.0         255.255.255.0   U         0 0          0 virbr0
t3net04-42 ~ >: 
```

The current routing table observed using the netstat -rn command. There are no new entries and the values of the flags for each entry in the routing table is the same.

The ICMP - Redirect message is sent when a host sends a datagram (or packet) to its gateway (the destination of which is on a different network), and the gateway in turn forwards the same datagram to the next gateway (the next hop), which is on the same network as the host. This ICMP message will be created by the second gateway and sent to the host where the datagram originated.

Since, there are no second gateway added to the routing table after the icmp packets were generated, that result is different from the theoretical explanation of icmp redirect messages.