Computer Networks Lab(EEP 703)

Assignment 10: Generating and analyzing network traffic

Name : Harshit Kumar Gupta
Entry Number : 2013EET2369

Computer Technology
Department of Electrical Engineering

Indian Institute of Technology Delhi

February 5, 2014

Contents

1 Problem Statement:

In this assignment, we will learn to capture traffic on our system and analyze it using Wireshark tool.

1. Accomplish the following tasks:
2. Using wireshark, observe normal network traffic. Can you separately see TCP/IP traffic, IPX traffic and NETBEUI traffic? What is the meaning of these different types of traffic?
3. Using wireshark, observe normal network traffic. Can you separately see TCP/IP traffic, IPX traffic and NETBEUI traffic? What is the meaning of these different types of traffic?
4. Using Ostinato, configure and generate connectionless and connectionoriented packet services in your system. Generate such traffic for following two cases:
5. CASE 1: Low transmission rate with small packet length
6. CASE 2: High transmission rate with large packet length.
7. Find throughput for both the cases for each packet service (connectionless and connectionoriented) and comment on what you observe.

Perform following and comment on the response you get:

1. Increase the rate at which ostinato is sending data. As you do so, observe that you seem to be able to send at whatever data rate you want. This is obviously wrong what could be happening ?
2. If you were given the task of developing a ostinato like generator , how would you start and go about it ? How would you test your generator ?

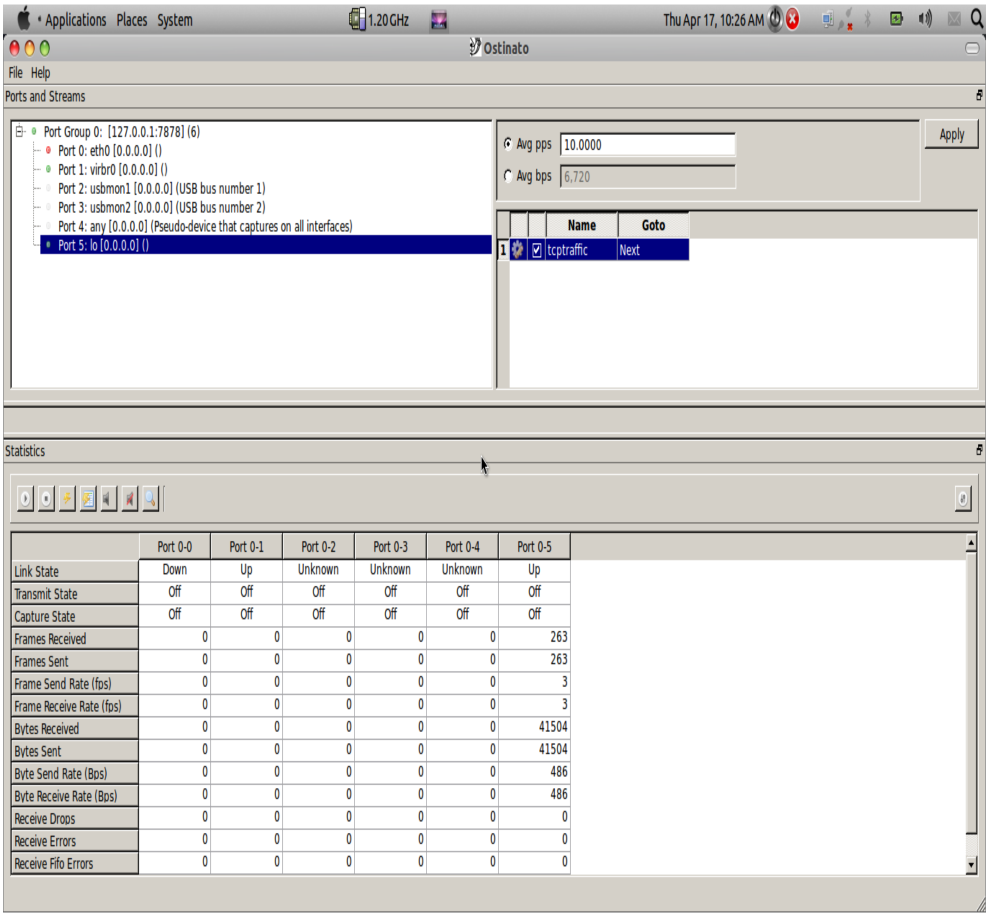
2 Abstract

In this experiment we will create analyze our present network using a network tool called WIRESHARK. We would learn how to recognise the network internet protocol addresses (IP) of various websites and to analye the network and various packets sent to/from the website using wireshark software.We also analyse the packets sent by the website and learn about various terminologies assocaited with it like various headers ,IP versions etc.

3 Execution Directive

Type the following commands on the terminal window in order to perform the given task.

1. Open wireshark as root user.
2. Open interface ethernet to capture the network
3. Start the interface and open the website whose analysis is to be seen.
4. Open Ostinato and the select a port for transmission.
5. Modify the properties of the transmission and start the transmission
6. Start capture.
7. View the capture ion wireshark.



Port Group 0: [127.0.0.1:7878] (6)
- Port 0: eth0 [0.0.0.0] ()
- Port 1: virbr0 [0.0.0.0] ()
- Port 2: usbmon1 [0.0.0.0] (USB bus number 1)
- Port 3: usbmon2 [0.0.0.0] (USB bus number 2)
- Port 4: any [0.0.0.0] (Pseudo-device that captures on all interfaces)
- Port 5: lo [0.0.0.0] ()

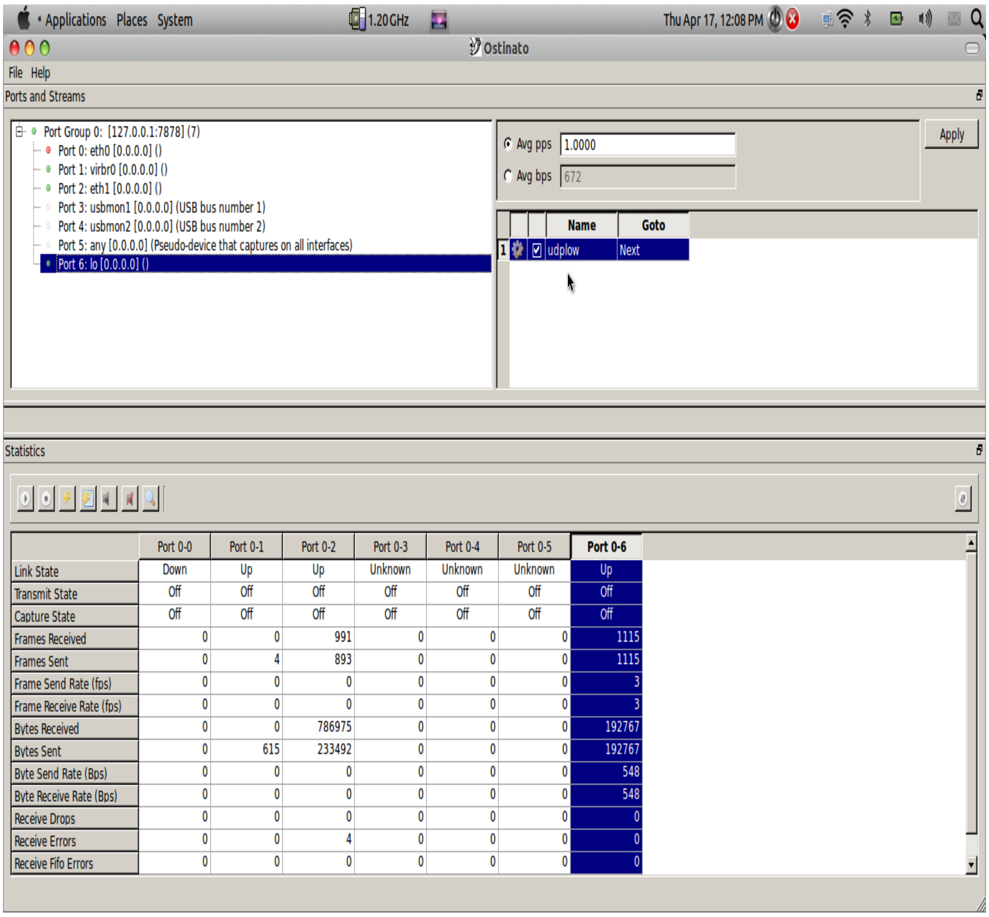
● Avg pps 10.0000

○ Avg bps 6,720

			Name	Goto
1		☑	tcptraffic	Next

	Port 0-0	Port 0-1	Port 0-2	Port 0-3	Port 0-4	Port 0-5
Link State	Down	Up	Unknown	Unknown	Unknown	Up
Transmit State	Off	Off	Off	Off	Off	Off
Capture State	Off	Off	Off	Off	Off	Off
Frames Received	0	0	0	0	0	263
Frames Sent	0	0	0	0	0	263
Frame Send Rate (fps)	0	0	0	0	0	3
Frame Receive Rate (fps)	0	0	0	0	0	3
Bytes Received	0	0	0	0	0	41504
Bytes Sent	0	0	0	0	0	41504
Byte Send Rate (Bps)	0	0	0	0	0	486
Byte Receive Rate (Bps)	0	0	0	0	0	486
Receive Drops	0	0	0	0	0	0
Receive Errors	0	0	0	0	0	0
Receive Fifo Errors	0	0	0	0	0	0

Generation of TCP traffic



- Port Group 0: [127.0.0.1:7878] (7)
  - Port 0: eth0 [0.0.0.0] ()
  - Port 1: virbr0 [0.0.0.0] ()
  - Port 2: eth1 [0.0.0.0] ()
  - Port 3: usbmon1 [0.0.0.0] (USB bus number 1)
  - Port 4: usbmon2 [0.0.0.0] (USB bus number 2)
  - Port 5: any [0.0.0.0] (Pseudo-device that captures on all interfaces)
  - Port 6: lo [0.0.0.0] ()

● Avg pps 1.0000

○ Avg bps 672

			Name	Goto
1		☑	udplow	Next

	Port 0-0	Port 0-1	Port 0-2	Port 0-3	Port 0-4	Port 0-5	Port 0-6
Link State	Down	Up	Up	Unknown	Unknown	Unknown	Up
Transmit State	Off	Off	Off	Off	Off	Off	Off
Capture State	Off	Off	Off	Off	Off	Off	Off
Frames Received	0	0	991	0	0	0	1115
Frames Sent	0	4	893	0	0	0	1115
Frame Send Rate (fps)	0	0	0	0	0	0	3
Frame Receive Rate (fps)	0	0	0	0	0	0	3
Bytes Received	0	0	786975	0	0	0	192767
Bytes Sent	0	615	233492	0	0	0	192767
Byte Send Rate (Bps)	0	0	0	0	0	0	548
Byte Receive Rate (Bps)	0	0	0	0	0	0	548
Receive Drops	0	0	0	0	0	0	0
Receive Errors	0	0	4	0	0	0	0
Receive Fifo Errors	0	0	0	0	0	0	0

Generation of UDP traffic

4 Result And Discussions

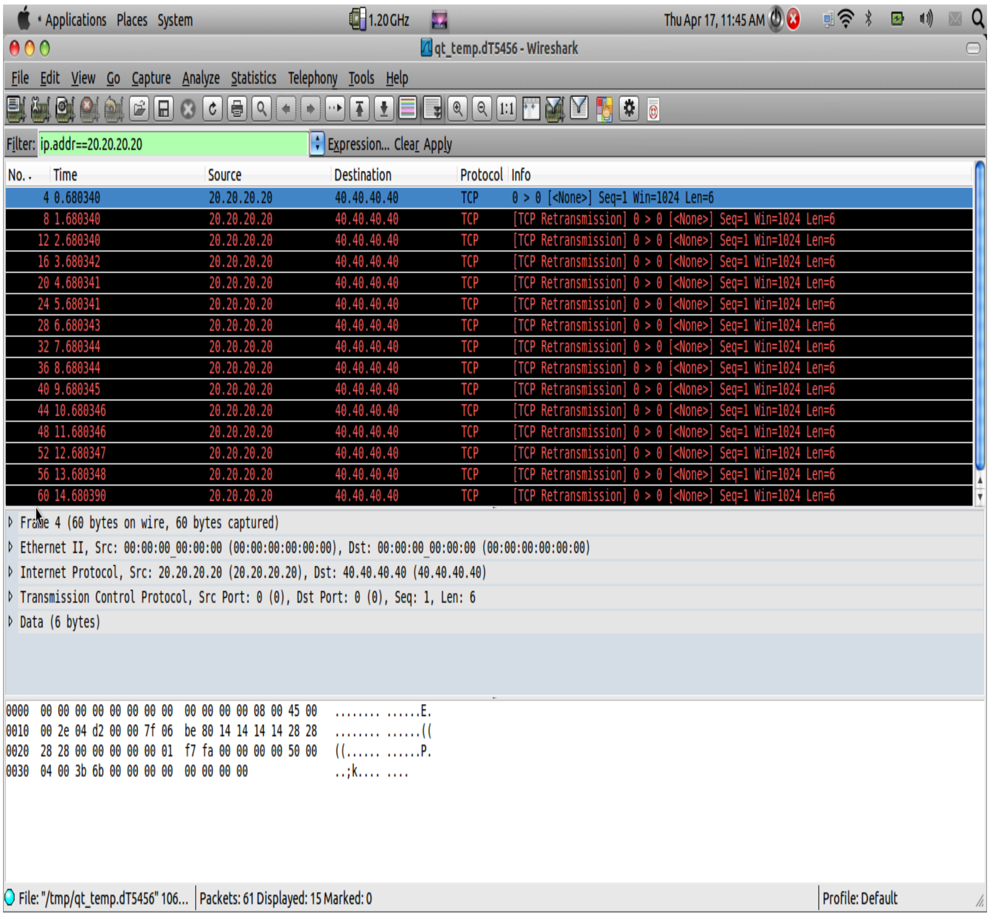
1. Problem Statement 1

   (a) Yes we can see the the TCP/IP,IPX and NETBEUI traffic in the wireshark network capture.IPX/SPX and TCP/IP are both operational on OSI model as layer 3 and layer 4 network protocols.IPX is basically well suited for local networks whereas TCP/IP is mainly used for interenet and WLANs. Their comparison along with a brief description of the NETBIOS protocol is given below-

   (b) Transmission Control Protocol / Internet Protocol (TCP/IP) :: TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

   (c) TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message.

   (d) The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination. Each gateway computer on the network checks this address to see where to forward the message. Even though some packets from the same message are routed differently than others, they'll be reassembled at the destination.


Applications Places System
1.20GHz
Thu Apr 17, 11:45 AM
qt_temp.dT5456 - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression... Clear Apply

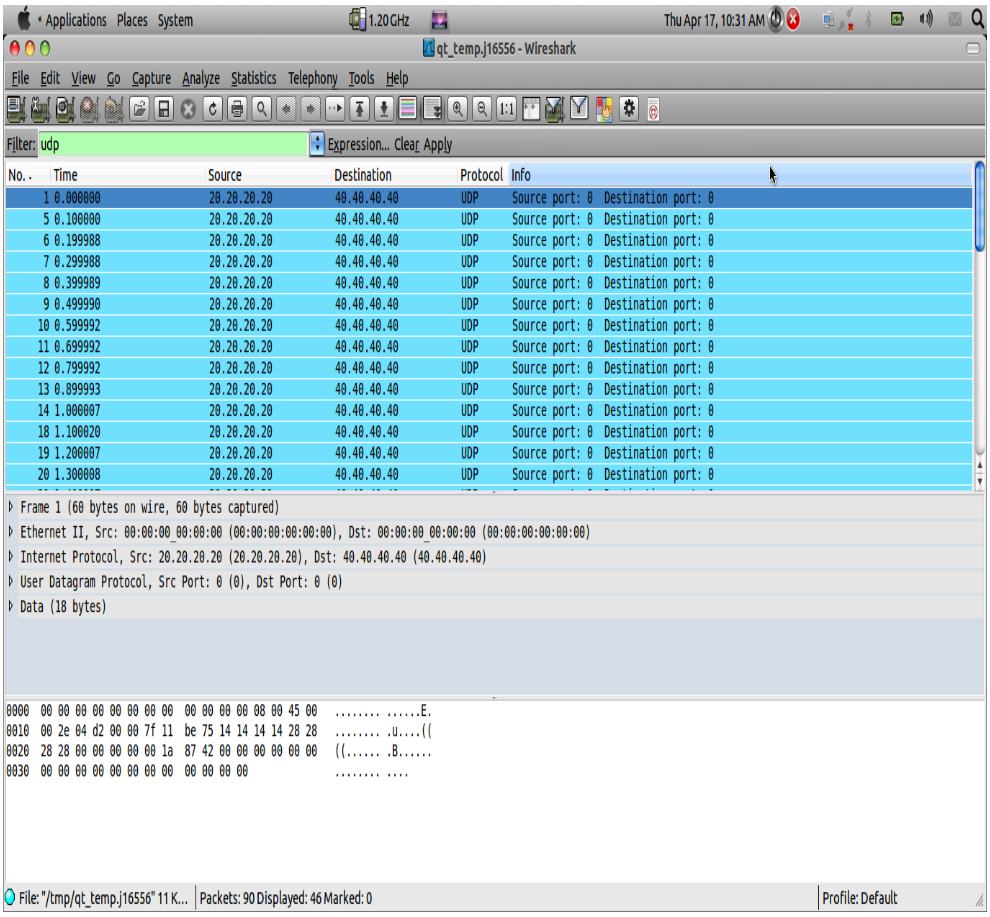
Filter: ip.addr==20.20.20.20

No.	Time	Source	Destination	Protocol	Info
4	0.680340	20.20.20.20	40.40.40.40	TCP	0 > 0 [<None>] Seq=1 Win=1024 Len=6
8	1.680340	20.20.20.20	40.40.40.40	TCP	[TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6
12	2.680340	20.20.20.20	40.40.40.40	TCP	[TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6
16	3.680342	20.20.20.20	40.40.40.40	TCP	[TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6
20	4.680341	20.20.20.20	40.40.40.40	TCP	[TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6
24	5.680341	20.20.20.20	40.40.40.40	TCP	[TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6
28	6.680343	20.20.20.20	40.40.40.40	TCP	[TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6
32	7.680344	20.20.20.20	40.40.40.40	TCP	[TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6
36	8.680344	20.20.20.20	40.40.40.40	TCP	[TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6
40	9.680345	20.20.20.20	40.40.40.40	TCP	[TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6
44	10.680346	20.20.20.20	40.40.40.40	TCP	[TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6
48	11.680346	20.20.20.20	40.40.40.40	TCP	[TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6
52	12.680347	20.20.20.20	40.40.40.40	TCP	[TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6
56	13.680348	20.20.20.20	40.40.40.40	TCP	[TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6
60	14.680390	20.20.20.20	40.40.40.40	TCP	[TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6

```
▷ Frame 4 (60 bytes on wire, 60 bytes captured)
▷ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▷ Internet Protocol, Src: 20.20.20.20 (20.20.20.20), Dst: 40.40.40.40 (40.40.40.40)
▷ Transmission Control Protocol, Src Port: 0 (0), Dst Port: 0 (0), Seq: 1, Len: 6
▷ Data (6 bytes)
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ........ ......E.
0010  00 2e 04 d2 00 00 7f 06  be 80 14 14 14 14 28 28   ........ ......((
0020  28 28 00 00 00 00 00 01  f7 fa 00 00 00 00 50 00   ((...... ......P.
0030  04 00 3b 6b 00 00 00 00  00 00 00 00               ..;k.... ....
```

File: "/tmp/qt_temp.dT5456" 106... | Packets: 61 Displayed: 15 Marked: 0 | Profile: Default



Applications Places System
1.20GHz
Thu Apr 17, 10:31 AM
qt_temp.j16556 - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: udp
Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	20.20.20.20	40.40.40.40	UDP	Source port: 0 Destination port: 0
5	0.100000	20.20.20.20	40.40.40.40	UDP	Source port: 0 Destination port: 0
6	0.199988	20.20.20.20	40.40.40.40	UDP	Source port: 0 Destination port: 0
7	0.299988	20.20.20.20	40.40.40.40	UDP	Source port: 0 Destination port: 0
8	0.399989	20.20.20.20	40.40.40.40	UDP	Source port: 0 Destination port: 0
9	0.499990	20.20.20.20	40.40.40.40	UDP	Source port: 0 Destination port: 0
10	0.599992	20.20.20.20	40.40.40.40	UDP	Source port: 0 Destination port: 0
11	0.699992	20.20.20.20	40.40.40.40	UDP	Source port: 0 Destination port: 0
12	0.799992	20.20.20.20	40.40.40.40	UDP	Source port: 0 Destination port: 0
13	0.899993	20.20.20.20	40.40.40.40	UDP	Source port: 0 Destination port: 0
14	1.000007	20.20.20.20	40.40.40.40	UDP	Source port: 0 Destination port: 0
18	1.100020	20.20.20.20	40.40.40.40	UDP	Source port: 0 Destination port: 0
19	1.200007	20.20.20.20	40.40.40.40	UDP	Source port: 0 Destination port: 0
20	1.300008	20.20.20.20	40.40.40.40	UDP	Source port: 0 Destination port: 0

```
▷ Frame 1 (60 bytes on wire, 60 bytes captured)
▷ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▷ Internet Protocol, Src: 20.20.20.20 (20.20.20.20), Dst: 40.40.40.40 (40.40.40.40)
▷ User Datagram Protocol, Src Port: 0 (0), Dst Port: 0 (0)
▷ Data (18 bytes)
```

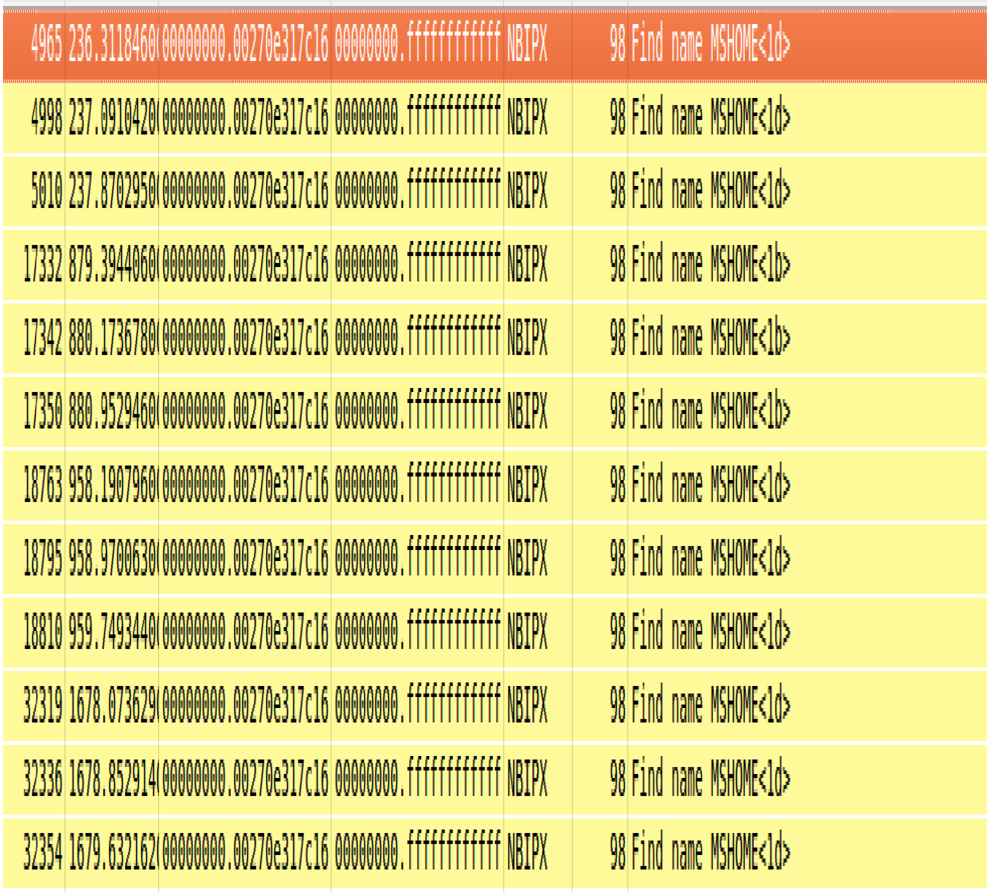
```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ........ ......E.
0010  00 2e 04 d2 00 00 7f 11  be 75 14 14 14 14 28 28   ........ .u....((
0020  28 28 00 00 00 00 00 1a  87 42 00 00 00 00 00 00   ((...... .B......
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

File: "/tmp/qt_temp.j16556" 11 K... | Packets: 90 Displayed: 46 Marked: 0 | Profile: Default

(a) Internetwork Packet eXchange (IPX) :: Internetwork Packet Exchange (IPX) is the OSI-model Network layer protocol in the IPX/SPX protocol stack.

(b) A big advantage of IPX is an easy configuration of the client computers.

(c) However, IPX did not scale enough for large networks such as the internet[1] and as such, IPX usage decreased as the boom of the Internet made TCP/IP nearly universal. Computers and networks can run multiple network protocols, so almost all IPX sites will be running TCP/IP as well to allow for Internet connectivity.[

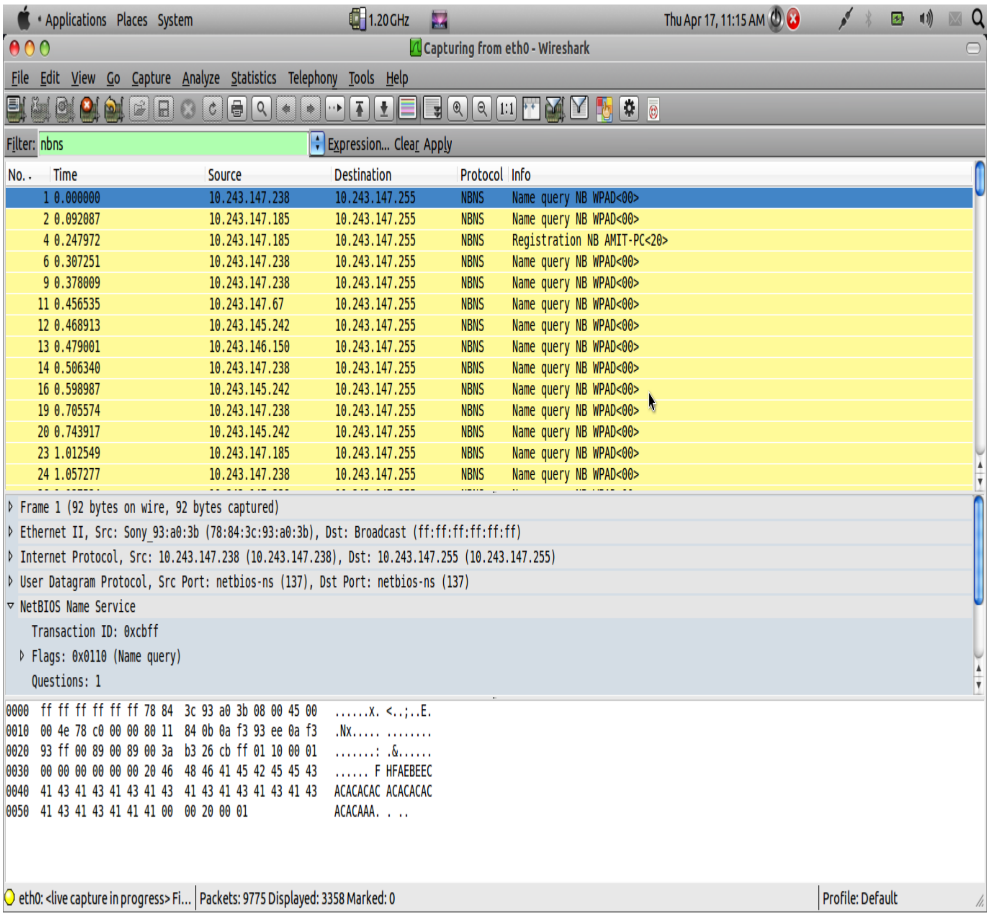


```
 4965 236.3118460 00000000.00270e317c16 00000000.ffffffffffff NBIPX     98 Find name MSHOME<1d>
 4998 237.0910420 00000000.00270e317c16 00000000.ffffffffffff NBIPX     98 Find name MSHOME<1d>
 5010 237.8702950 00000000.00270e317c16 00000000.ffffffffffff NBIPX     98 Find name MSHOME<1d>
17332 879.3944060 00000000.00270e317c16 00000000.ffffffffffff NBIPX     98 Find name MSHOME<1b>
17342 880.1736780 00000000.00270e317c16 00000000.ffffffffffff NBIPX     98 Find name MSHOME<1b>
17350 880.9529460 00000000.00270e317c16 00000000.ffffffffffff NBIPX     98 Find name MSHOME<1b>
18763 958.1907960 00000000.00270e317c16 00000000.ffffffffffff NBIPX     98 Find name MSHOME<1d>
18795 958.9700630 00000000.00270e317c16 00000000.ffffffffffff NBIPX     98 Find name MSHOME<1d>
18810 959.7493440 00000000.00270e317c16 00000000.ffffffffffff NBIPX     98 Find name MSHOME<1d>
32319 1678.073629 00000000.00270e317c16 00000000.ffffffffffff NBIPX     98 Find name MSHOME<1d>
32336 1678.852914 00000000.00270e317c16 00000000.ffffffffffff NBIPX     98 Find name MSHOME<1d>
32354 1679.632162 00000000.00270e317c16 00000000.ffffffffffff NBIPX     98 Find name MSHOME<1d>
```

(a) Network Basic Input/Output System (NETBEUI/NETBIOS : t provides services related to the session layer of the OSI model allowing applications on separate computers to communicate over a local area network.

(b) As strictly an API, NetBIOS is not a networking protocol.

(c) NetBios can work over IPX/SPX using the NetBIOS Frames (NBF) and IPX/SPX (NBX) protocols. In modern networks, NetBIOS normally runs over TCP/IP via the NetBIOS over TCP/IP (NBT) protocol.


Applications Places System
1.20GHz
Thu Apr 17, 11:15 AM
Capturing from eth0 - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression... Clear Apply
Profile: Default

Filter: nbns

```
No. . Time        Source          Destination     Protocol Info
    1 0.000000    10.243.147.238  10.243.147.255  NBNS     Name query NB WPAD<00>
    2 0.092087    10.243.147.185  10.243.147.255  NBNS     Name query NB WPAD<00>
    4 0.247972    10.243.147.185  10.243.147.255  NBNS     Registration NB AMIT-PC<20>
    6 0.307251    10.243.147.238  10.243.147.255  NBNS     Name query NB WPAD<00>
    9 0.378009    10.243.147.238  10.243.147.255  NBNS     Name query NB WPAD<00>
   11 0.456535    10.243.147.67   10.243.147.255  NBNS     Name query NB WPAD<00>
   12 0.468913    10.243.145.242  10.243.147.255  NBNS     Name query NB WPAD<00>
   13 0.479001    10.243.146.150  10.243.147.255  NBNS     Name query NB WPAD<00>
   14 0.506340    10.243.147.238  10.243.147.255  NBNS     Name query NB WPAD<00>
   16 0.598987    10.243.145.242  10.243.147.255  NBNS     Name query NB WPAD<00>
   19 0.705574    10.243.147.238  10.243.147.255  NBNS     Name query NB WPAD<00>
   20 0.743917    10.243.145.242  10.243.147.255  NBNS     Name query NB WPAD<00>
   23 1.012549    10.243.147.185  10.243.147.255  NBNS     Name query NB WPAD<00>
   24 1.057277    10.243.147.238  10.243.147.255  NBNS     Name query NB WPAD<00>
```

```
▷ Frame 1 (92 bytes on wire, 92 bytes captured)
▷ Ethernet II, Src: Sony_93:a0:3b (78:84:3c:93:a0:3b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Internet Protocol, Src: 10.243.147.238 (10.243.147.238), Dst: 10.243.147.255 (10.243.147.255)
▷ User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
▽ NetBIOS Name Service
    Transaction ID: 0xcbff
  ▷ Flags: 0x0110 (Name query)
    Questions: 1
```

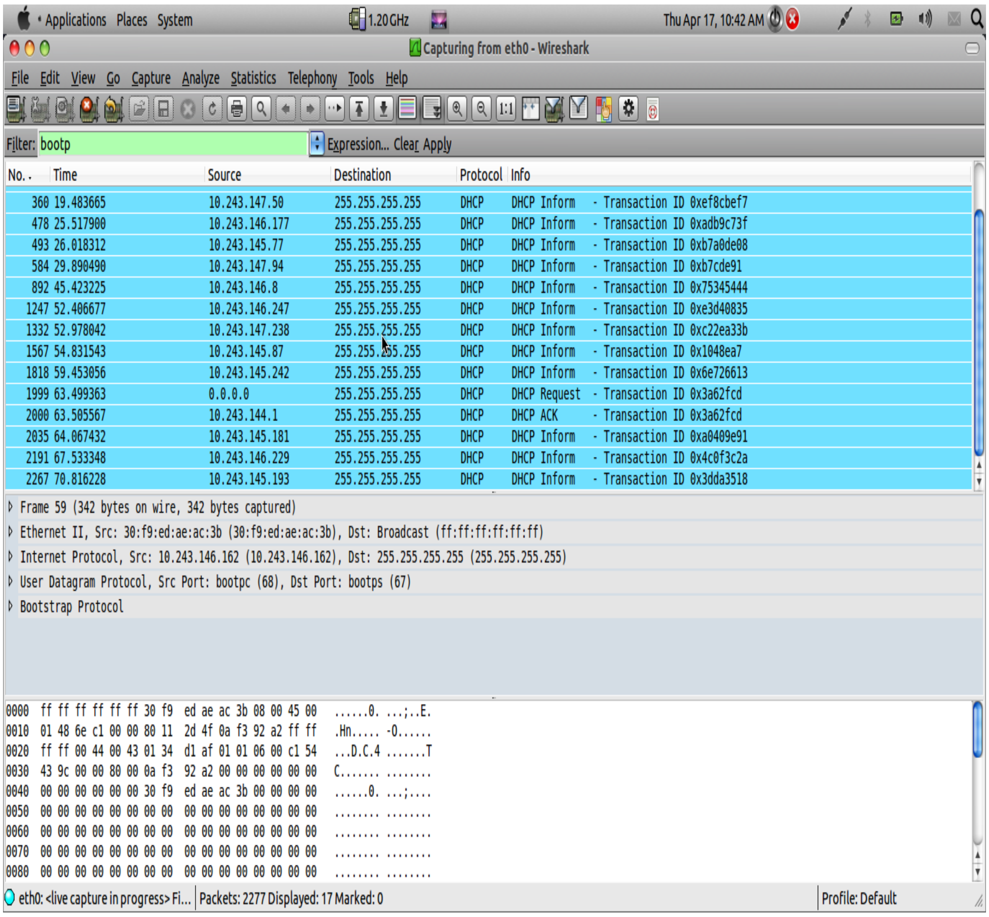
```
0000  ff ff ff ff ff ff 78 84  3c 93 a0 3b 08 00 45 00   ......x. <..;..E.
0010  00 4e 78 c0 00 00 80 11  84 0b 0a f3 93 ee 0a f3   .Nx..... ........
0020  93 ff 00 89 00 89 00 3a  b3 26 cb ff 01 10 00 01   .......: .&......
0030  00 00 00 00 00 00 20 46  48 46 41 45 42 45 45 43   ...... F HFAEBEEC
0040  41 43 41 43 41 43 41 43  41 43 41 43 41 43 41 43   ACACACAC ACACACAC
0050  41 43 41 43 41 41 41 00  00 20 00 01               ACACAAA. . ..
```

eth0: <live capture in progress> Fi... Packets: 9775 Displayed: 3358 Marked: 0

1. The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.

2. With DHCP computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user from having to configure these settings manually.

3. Yes we can see DHCP packets in the Wireshark capture.


Applications Places System
1.20GHz
Thu Apr 17, 10:42 AM
Capturing from eth0 - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression... Clear Apply
Profile: Default

Filter: bootp

```
No. .  Time               Source            Destination       Protocol  Info
   360 19.483665          10.243.147.50     255.255.255.255   DHCP      DHCP Inform   - Transaction ID 0xef8cbef7
   478 25.517900          10.243.146.177    255.255.255.255   DHCP      DHCP Inform   - Transaction ID 0xadb9c73f
   493 26.018312          10.243.145.77     255.255.255.255   DHCP      DHCP Inform   - Transaction ID 0xb7a0de08
   584 29.890490          10.243.147.94     255.255.255.255   DHCP      DHCP Inform   - Transaction ID 0xb7cde91
   892 45.423225          10.243.146.8      255.255.255.255   DHCP      DHCP Inform   - Transaction ID 0x75345444
  1247 52.406677          10.243.146.247    255.255.255.255   DHCP      DHCP Inform   - Transaction ID 0xe3d40835
  1332 52.978042          10.243.147.238    255.255.255.255   DHCP      DHCP Inform   - Transaction ID 0xc22ea33b
  1567 54.831543          10.243.145.87     255.255.255.255   DHCP      DHCP Inform   - Transaction ID 0x1048ea7
  1818 59.453056          10.243.145.242    255.255.255.255   DHCP      DHCP Inform   - Transaction ID 0x6e726613
  1999 63.499363          0.0.0.0           255.255.255.255   DHCP      DHCP Request  - Transaction ID 0x3a62fcd
  2000 63.505567          10.243.144.1      255.255.255.255   DHCP      DHCP ACK      - Transaction ID 0x3a62fcd
  2035 64.067432          10.243.145.181    255.255.255.255   DHCP      DHCP Inform   - Transaction ID 0xa0409e91
  2191 67.533348          10.243.146.229    255.255.255.255   DHCP      DHCP Inform   - Transaction ID 0x4c0f3c2a
  2267 70.816228          10.243.145.193    255.255.255.255   DHCP      DHCP Inform   - Transaction ID 0x3dda3518
```

```
▷ Frame 59 (342 bytes on wire, 342 bytes captured)
▷ Ethernet II, Src: 30:f9:ed:ae:ac:3b (30:f9:ed:ae:ac:3b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Internet Protocol, Src: 10.243.146.162 (10.243.146.162), Dst: 255.255.255.255 (255.255.255.255)
▷ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
▷ Bootstrap Protocol
```

```
0000  ff ff ff ff ff ff 30 f9  ed ae ac 3b 08 00 45 00   ......0. ...;..E.
0010  01 48 6e c1 00 00 80 11  2d 4f 0a f3 92 a2 ff ff   .Hn..... -O......
0020  ff ff 00 44 00 43 01 34  d1 af 01 01 06 00 c1 54   ...D.C.4 .......T
0030  43 9c 00 00 80 00 0a f3  92 a2 00 00 00 00 00 00   C....... ........
0040  00 00 00 00 00 00 30 f9  ed ae ac 3b 00 00 00 00   ......0. ...;....
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   ........ ........
```

eth0: <live capture in progress> Fi... | Packets: 2277 Displayed: 17 Marked: 0

1. MECHANISM ::

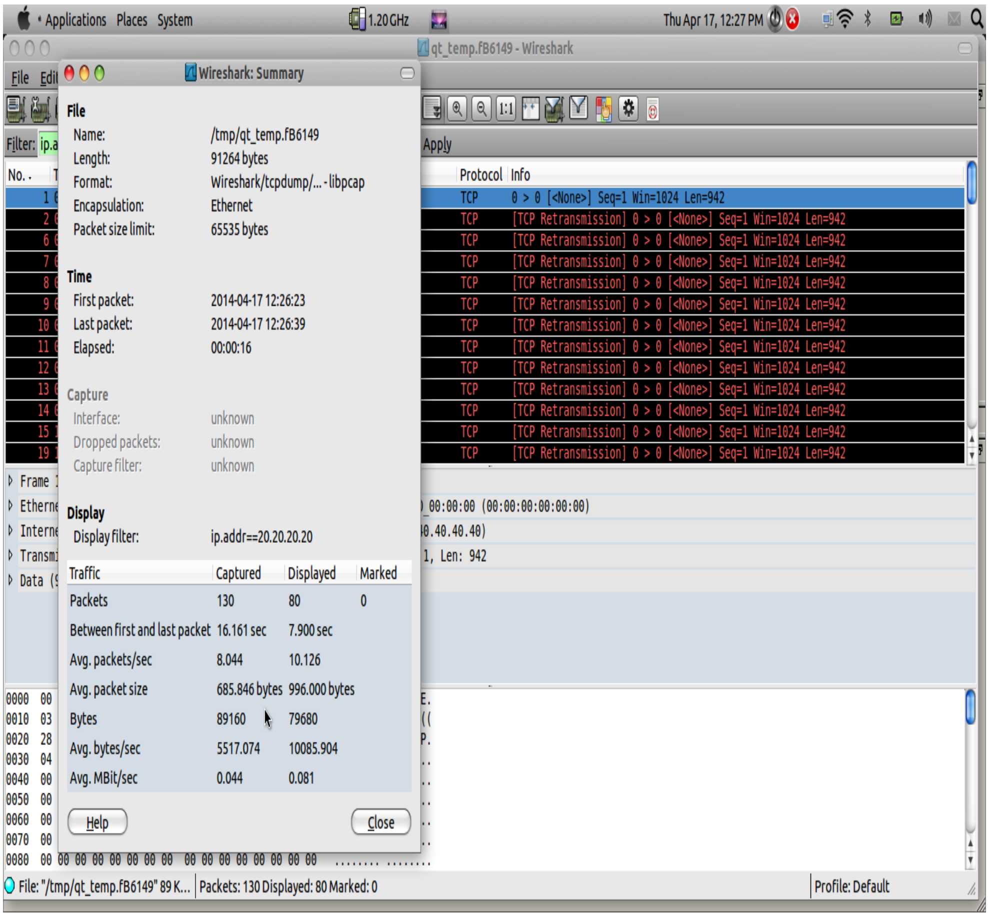
2. The client broadcasts messages on the network subnet using the destination address 255.255.255.255 or the specific subnet broadcast address.

3. A DHCP client may also request its last-known IP address.

4. If the client remains connected to the same network, the server may grant the request.

5. Otherwise, it depends whether the server is set up as authoritative or not.

6. An authoritative server denies the request, causing the client issue a new request.



File

Name:	/tmp/qt_temp.fB6149
Length:	91264 bytes
Format:	Wireshark/tcpdump/... - libpcap
Encapsulation:	Ethernet
Packet size limit:	65535 bytes

Time

First packet:	2014-04-17 12:26:23
Last packet:	2014-04-17 12:26:39
Elapsed:	00:00:16

Capture

Interface:	unknown
Dropped packets:	unknown
Capture filter:	unknown

Display

Display filter:	ip.addr==20.20.20.20

Traffic	Captured	Displayed	Marked
Packets	130	80	0
Between first and last packet	16.161 sec	7.900 sec	
Avg. packets/sec	8.044	10.126	
Avg. packet size	685.846 bytes	996.000 bytes	
Bytes	89160	79680	
Avg. bytes/sec	5517.074	10085.904	
Avg. MBit/sec	0.044	0.081	

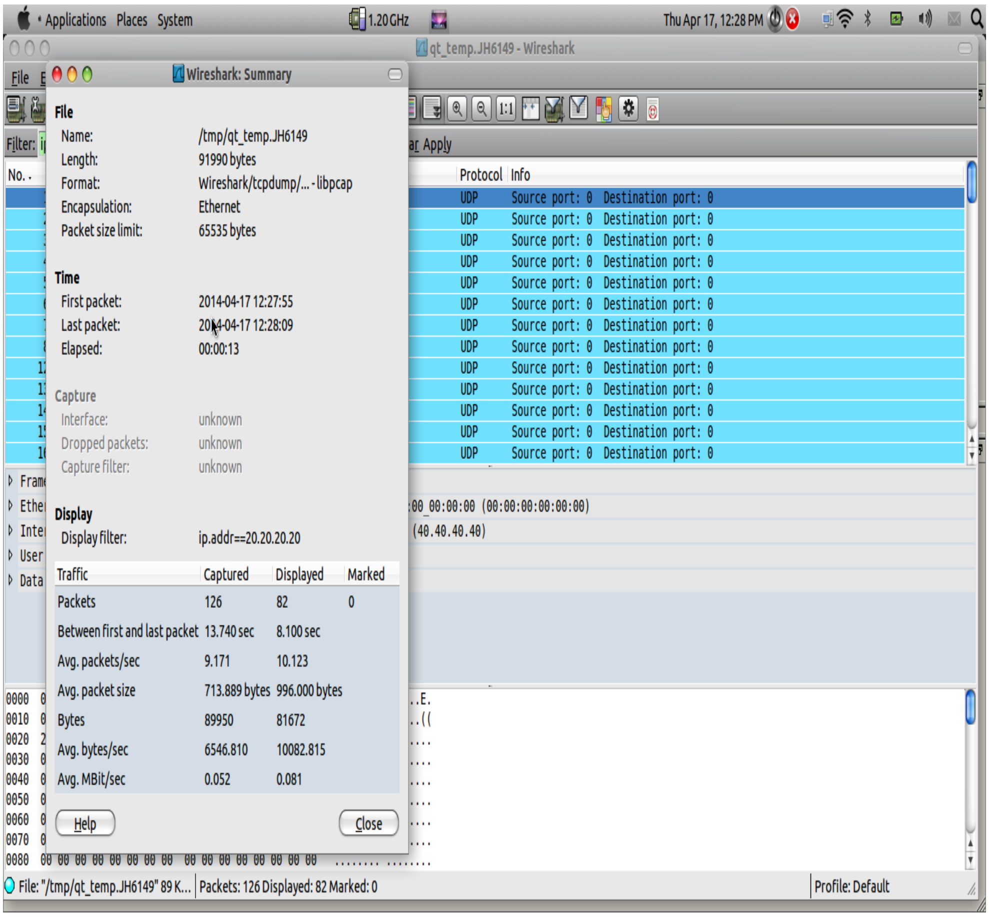
```
No. .  T                                  Protocol Info
 1 (                                      TCP      0 > 0 [<None>] Seq=1 Win=1024 Len=942
 2 (                                      TCP      [TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=942
 6 (                                      TCP      [TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=942
 7 (                                      TCP      [TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=942
 8 (                                      TCP      [TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=942
 9 (                                      TCP      [TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=942
10 (                                      TCP      [TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=942
11 (                                      TCP      [TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=942
12 (                                      TCP      [TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=942
13 (                                      TCP      [TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=942
14 (                                      TCP      [TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=942
15 1                                      TCP      [TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=942
19 1                                      TCP      [TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=942
```

```
▷ Frame 1                                 
▷ Etherne                                 ) 00:00:00 (00:00:00:00:00:00)
▷ Interne                                 0.40.40.40)
▷ Transmi                                 1, Len: 942
▷ Data (9
```

```
0000  00                                          E.
0010  03                                          ((
0020  28                                          P.
0030  04                                          ..
0040  00                                          ..
0050  00                                          ..
0060  00                                          ..
0070  00                                          ..
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

File: "/tmp/qt_temp.fB6149" 89 K... | Packets: 130 Displayed: 80 Marked: 0

High Transmission rate High packet size :: TCP



```
UDP   Source port: 0  Destination port: 0
UDP   Source port: 0  Destination port: 0
UDP   Source port: 0  Destination port: 0
UDP   Source port: 0  Destination port: 0
UDP   Source port: 0  Destination port: 0
UDP   Source port: 0  Destination port: 0
UDP   Source port: 0  Destination port: 0
UDP   Source port: 0  Destination port: 0
UDP   Source port: 0  Destination port: 0
UDP   Source port: 0  Destination port: 0
UDP   Source port: 0  Destination port: 0
UDP   Source port: 0  Destination port: 0
UDP   Source port: 0  Destination port: 0
```

File

Name: /tmp/qt_temp.JH6149

Length: 91990 bytes

Format: Wireshark/tcpdump/... - libpcap

Encapsulation: Ethernet

Packet size limit: 65535 bytes

Time

First packet: 2014-04-17 12:27:55

Last packet: 2014-04-17 12:28:09

Elapsed: 00:00:13

Capture

Interface: unknown

Dropped packets: unknown

Capture filter: unknown

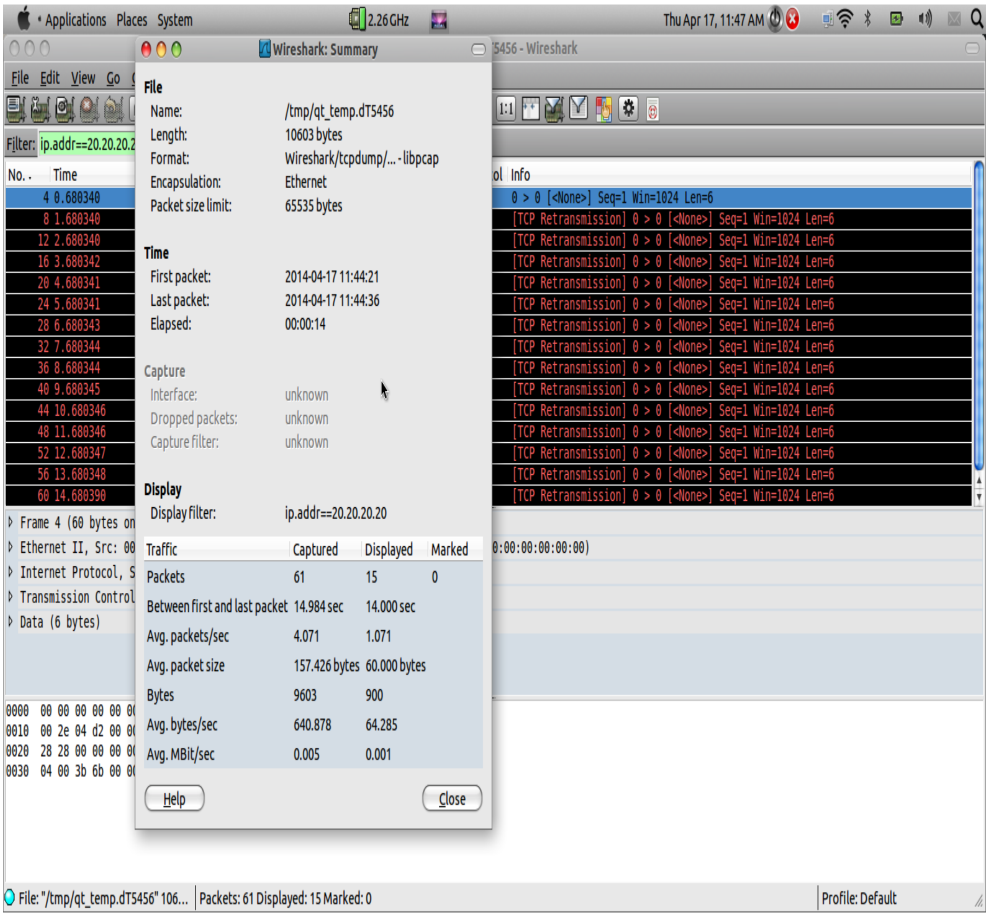
Display

Display filter: ip.addr==20.20.20.20

Traffic	Captured	Displayed	Marked
Packets	126	82	0
Between first and last packet	13.740 sec	8.100 sec	
Avg. packets/sec	9.171	10.123	
Avg. packet size	713.889 bytes	996.000 bytes	
Bytes	89950	81672	
Avg. bytes/sec	6546.810	10082.815	
Avg. MBit/sec	0.052	0.081	

File: "/tmp/qt_temp.JH6149" 89 K... | Packets: 126 Displayed: 82 Marked: 0 | Profile: Default

High Transmission rate High packet size :: UDP



Filter: ip.addr==20.20.20.2

```
No. .  Time         ol  Info
    4 0.680340          0 > 0 [<None>] Seq=1 Win=1024 Len=6
    8 1.680340          [TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6
   12 2.680340          [TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6
   16 3.680342          [TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6
   20 4.680341          [TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6
   24 5.680341          [TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6
   28 6.680343          [TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6
   32 7.680344          [TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6
   36 8.680344          [TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6
   40 9.680345          [TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6
   44 10.680346         [TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6
   48 11.680346         [TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6
   52 12.680347         [TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6
   56 13.680348         [TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6
   60 14.680390         [TCP Retransmission] 0 > 0 [<None>] Seq=1 Win=1024 Len=6

▷ Frame 4 (60 bytes on
▷ Ethernet II, Src: 00                  0:00:00:00:00:00)
▷ Internet Protocol, S
▷ Transmission Control
▷ Data (6 bytes)

0000  00 00 00 00 00 00
0010  00 2e 04 d2 00 00
0020  28 28 00 00 00 00
0030  04 00 3b 6b 00 00
```

File

Name: /tmp/qt_temp.dT5456

Length: 10603 bytes

Format: Wireshark/tcpdump/... - libpcap

Encapsulation: Ethernet

Packet size limit: 65535 bytes

Time

First packet: 2014-04-17 11:44:21

Last packet: 2014-04-17 11:44:36

Elapsed: 00:00:14

Capture

Interface: unknown

Dropped packets: unknown

Capture filter: unknown

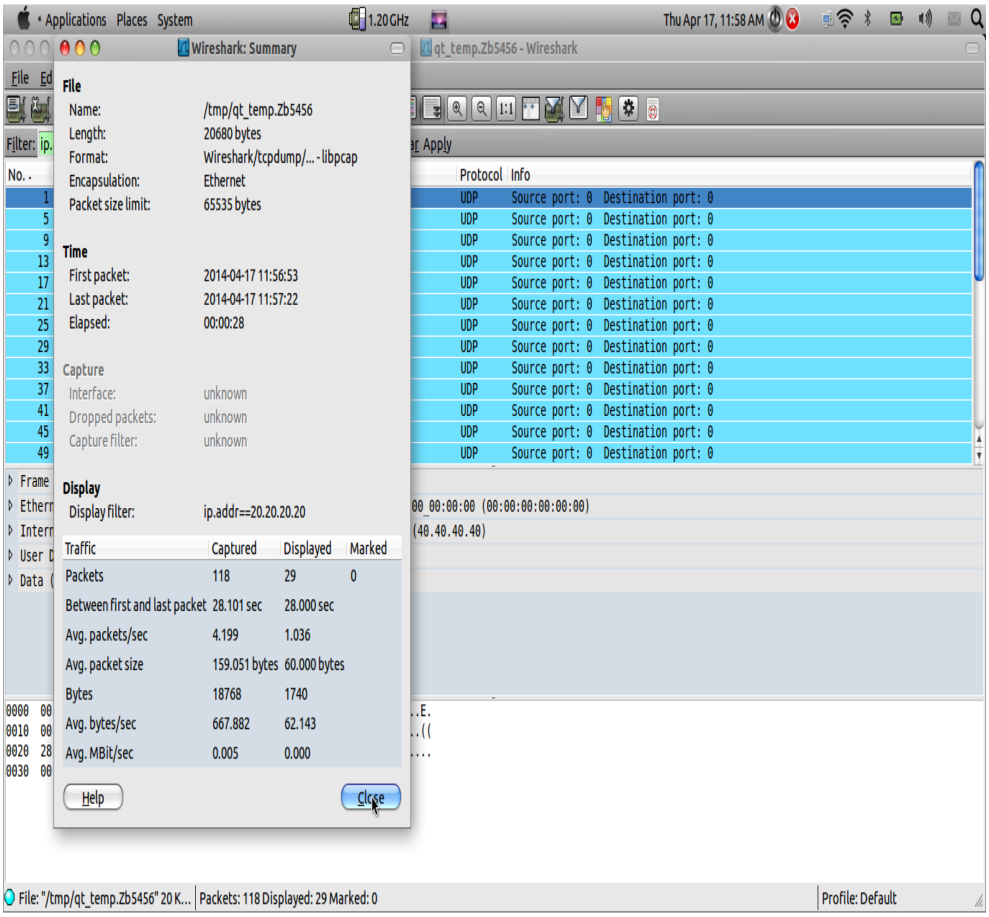
Display

Display filter: ip.addr==20.20.20.20

Traffic	Captured	Displayed	Marked
Packets	61	15	0
Between first and last packet	14.984 sec	14.000 sec	
Avg. packets/sec	4.071	1.071	
Avg. packet size	157.426 bytes	60.000 bytes	
Bytes	9603	900	
Avg. bytes/sec	640.878	64.285	
Avg. MBit/sec	0.005	0.001	

File: "/tmp/qt_temp.dT5456" 106... | Packets: 61 Displayed: 15 Marked: 0

Low Transmission rate Low packet size :: TCP



File

Name:	/tmp/qt_temp.Zb5456
Length:	20680 bytes
Format:	Wireshark/tcpdump/... - libpcap
Encapsulation:	Ethernet
Packet size limit:	65535 bytes

Time

First packet:	2014-04-17 11:56:53
Last packet:	2014-04-17 11:57:22
Elapsed:	00:00:28

Capture

Interface:	unknown
Dropped packets:	unknown
Capture filter:	unknown

Display

Display filter:	ip.addr==20.20.20.20

Traffic	Captured	Displayed	Marked
Packets	118	29	0
Between first and last packet	28.101 sec	28.000 sec	
Avg. packets/sec	4.199	1.036	
Avg. packet size	159.051 bytes	60.000 bytes	
Bytes	18768	1740	
Avg. bytes/sec	667.882	62.143	
Avg. MBit/sec	0.005	0.000	

```
No. .   Protocol Info
    1   UDP      Source port: 0  Destination port: 0
    5   UDP      Source port: 0  Destination port: 0
    9   UDP      Source port: 0  Destination port: 0
   13   UDP      Source port: 0  Destination port: 0
   17   UDP      Source port: 0  Destination port: 0
   21   UDP      Source port: 0  Destination port: 0
   25   UDP      Source port: 0  Destination port: 0
   29   UDP      Source port: 0  Destination port: 0
   33   UDP      Source port: 0  Destination port: 0
   37   UDP      Source port: 0  Destination port: 0
   41   UDP      Source port: 0  Destination port: 0
   45   UDP      Source port: 0  Destination port: 0
   49   UDP      Source port: 0  Destination port: 0

▷ Frame
▷ Ethern   00 00:00:00 (00:00:00:00:00:00)
▷ Intern   (40.40.40.40)
▷ User D
▷ Data (

0000  00   ..E.
0010  00   ..((
0020  28   ....
0030  00
```

File: "/tmp/qt_temp.Zb5456" 20 K... | Packets: 118 Displayed: 29 Marked: 0

Low Transmission rate Low packet size :: UDP