CSP334: Computer Networks
Lab Assignment No 2
Assignment on Linux Networking Commands

Abhishek Gupta 2016UCS0012

August 25, 2018

1 Q1: Examine the following files in Linux

1.1 /etc/hosts

As your machine gets started, it will need to know the mapping of some hostnames to IP addresses before DNS can be referenced. This mapping is kept in the /etc/hosts file. In the absence of a name server, any network program on your system consults this file to determine the IP address that corresponds to a host name.

1.2 /etc/sysconfig/network

The /etc/sysconfig/network file is used to specify information about the desired network configuration.It has the following values - Networking (yes or no), Hostname, Gateway (IP address of network's gateway) etc.

1.3 /etc/sysconfig/network-scripts/ifcfg-eth0

ifcfg-eth0 controls the first Ethernet network interface card or NIC in the system. In a system with multiple NICs, there are multiple ifcfg-eth<X> files (where <X> is a unique number corresponding to a specific interface).

1.4 /etc/default-route

This file contains the information about default-route. As we know when a packet comes to a router it find the best route to the destination (i.e. where the traffic is minimum) for that packet. When router was unable to find any specific route the packet go through this default route.

1.5 /etc/resolv.conf

resolv.conf is the name of a computer file used in various operating systems to configure the system's Domain Name System resolver.This resolver help in extractiong IP address from domain names which were sent from our system. This file contain the search domain and the IP address of the DNS server.

1.6 /etc/nsswitch.conf

/etc/nsswitch.conf, is used by the GNU C Library to determine the sources from which to obtain name-service information in a range of categories, and in what order. Each category of information is identified by a database name.

2 Q2: Info about /etc/services File

Services file at /etc/services stores information about numerous services that client applications might use on the computer. Within the file is the service name, port number and protocol it uses, and any applicable aliases.Transport Layer in the TCP/IP protocol stack make use of this file.The port numbers shown in this file are well-known port numbers. These are so becuase user can be sure not to use these port numbers while providing services to others.

3 Q3: MAN Pages

commandname	Purpose	Transportlayerprotocol	Networklayerprotocol
arp	It maps IP Address to Physical Address on local network	NA	ARP
arping	It is a tool for probing host on network,it may use utility arp to resole IP Adress	NA	ARP
ifconfig	It displays status of currently active network interfaces and used to set interfaces in kernel		
tcpdump	It provides description of the content of packets on a given network nterface		
ping	It Exchange packets between two host and measure strength of connection btw client and server		ICMP
netstat	It prints list of networking subsystems by default it displays list of all open sockets		
route	It controls Kernel IP routing tables and it route to specific network or host which has been configured with terminal		

4 Q4: TCPDUMP TRAFFIC

tcpdump hostname remotehostname and localhostname
tcpdump hostname remotehostIP and localhostIP

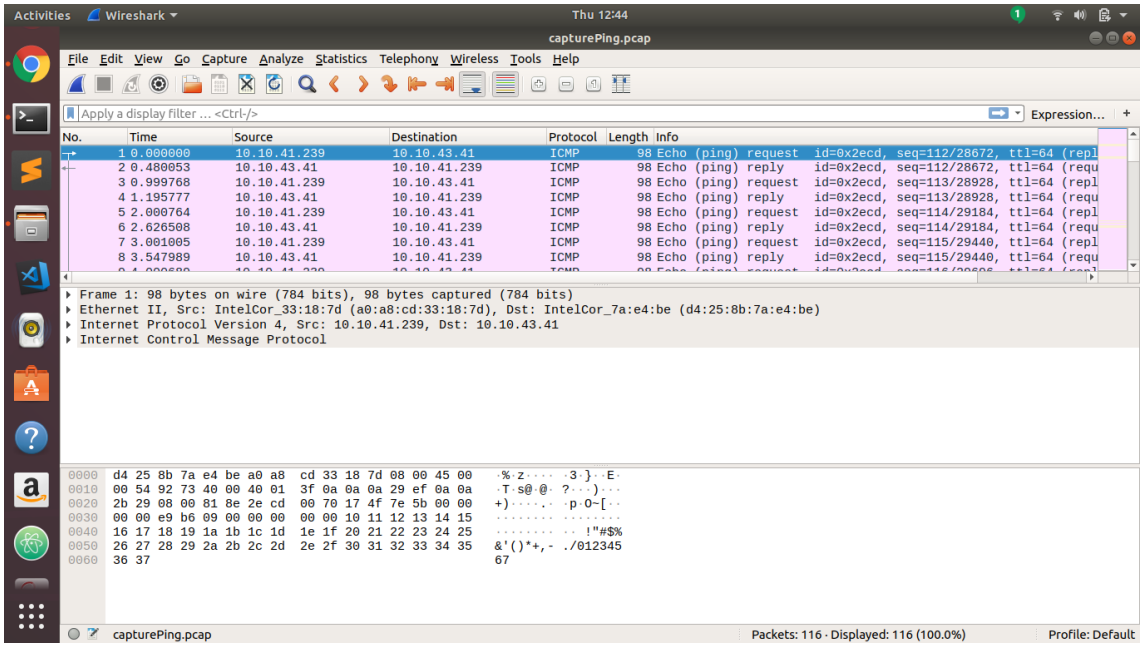

Figure 1: Screenshot of tcpdump file

4.1 Request

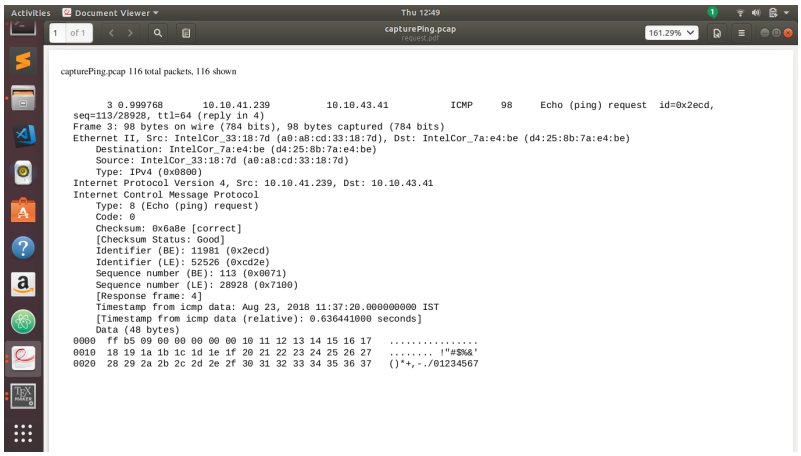

Figure 2: Ping Request.

4.2 Response

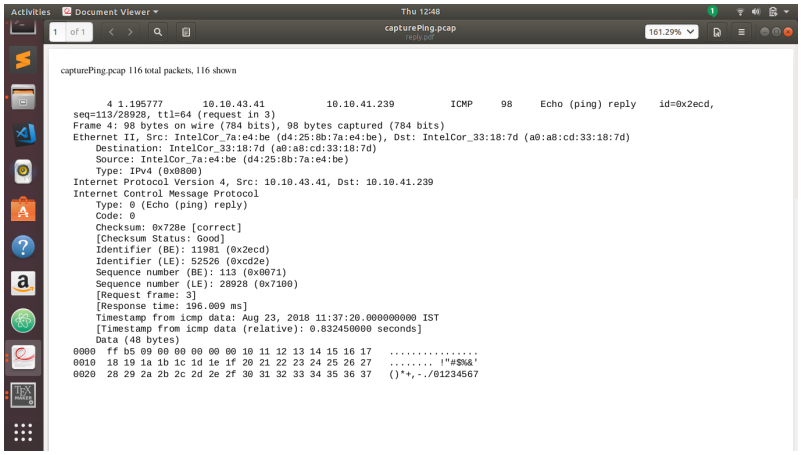

Figure 3: Ping reply

5 Q5: tcpdump −enx −w exe5.out

We will not be able to see anything on the terminal screen as all the output of tcpdump command is being written on exe5.out file

6 Q6: tcpdump −enx −w exe5.out

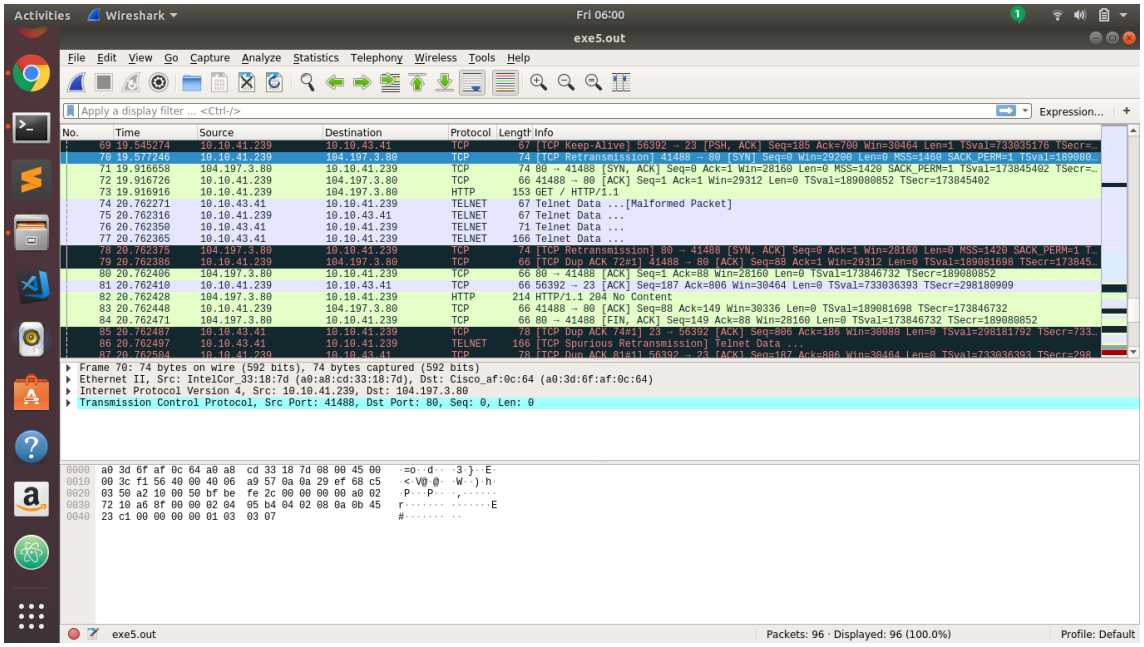

Figure 4: Screnshot of Tcpdump file.

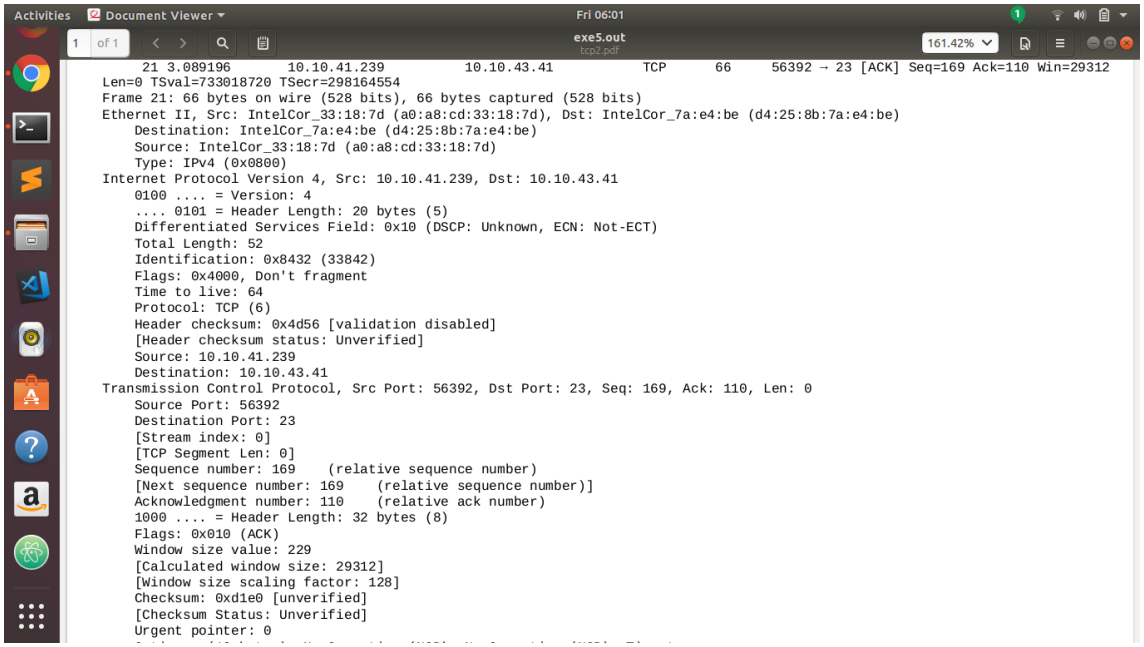

Figure 5: Screenshot of a tcp packet.

6.1 A

Table 1: IP header format

Version:0100....	Hdrlen 20bytes	DifrentiatedServices:0x10(16)	TotalLength:53
Identification:0x8432(33842)		Flag:0x4000(16384)	FragementOffset:0
TimeToLive:64	Protocols:TCP	HeaderCheckSum:0x3fed	
Source IP Address:10.10.41.239			
Destination IP Address:10.10.43.41			
Options:			
Data			

Table 2: TCP header format

Source Port Number:56392			Destination Port Number:23
Sequence Number:169			
Acknowledgement Number:110			
Hdr Len:32 bytes	Reserved:Not Set	Flags:0x010(16)(ACK)	Window Size:229
Tcp CheckSum:0xd1e0(53728)			Urgent Pointer:0
Options:			
Data:			

Table 3: Link header format

$IntelCor_3 3 : 18 : 7d$ (a0:a8:cd:33:18:7d)	$IntelCor_7 a : e4 : be$ (d4:25:8b:7a:e4:be)	FT:IPv4	Data	CRC

6.2 B

TCP 6 .The Protocol field in the IPv4 header contains a number indicating the type of data found in the payload portion of the datagram. The most common values are 17 (for UDP) and 6 (for

TCP). This field provides a demultiplexing feature so that the IP protocol can be used to carry payloads of more than one protocol type.

7 Q7: ARP

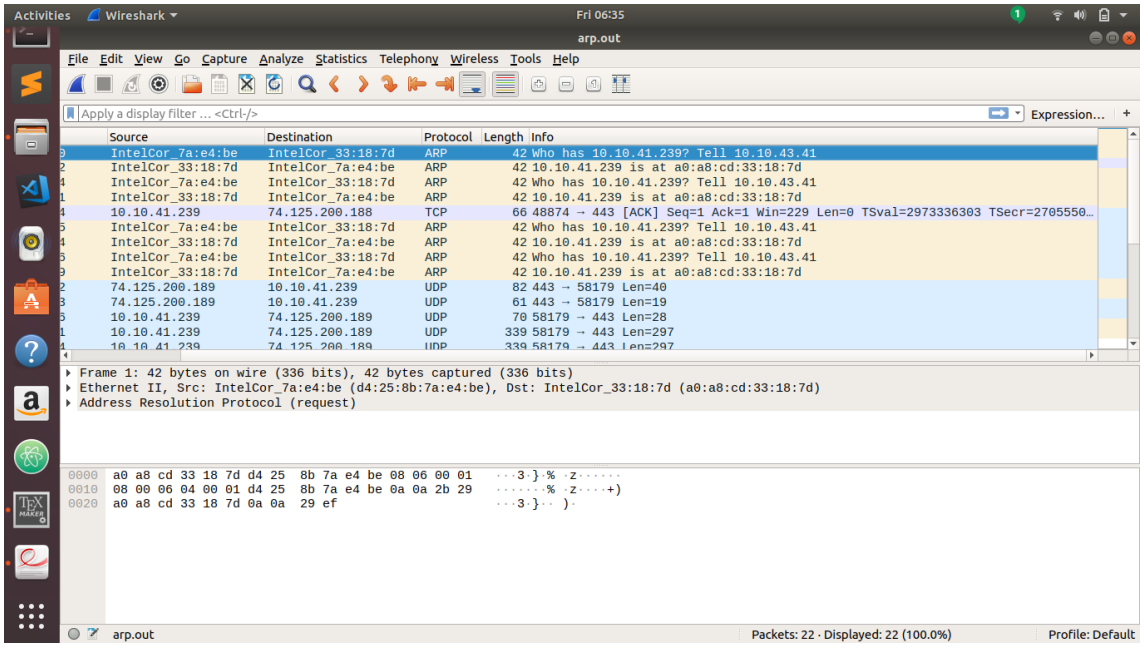

Figure 6: Screenshot of tcpdump file.

7.1 Request

Figure 7: Arping request

7.2 Reply

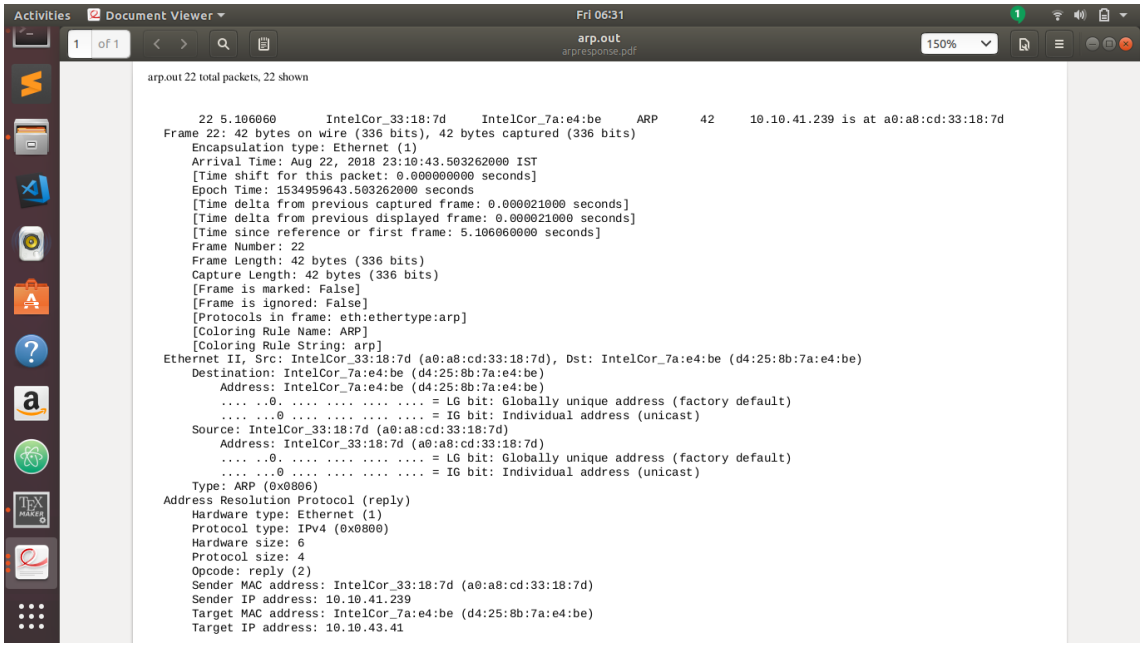

Figure 8: Arping reply.

7.3 A

REQUEST Type: ARP 0x0806(2054)
REPLY Type: ARP 0x0806(2054)

7.4 B

Type: IPv4 0x0800 (2048)

7.5 C

It is used to indicate which protocol is encapsulated in the payload of the frame. The same field is also used to indicate the size of some Ethernet frames

8 Q8: TCPDUMP Expressions

8.1 tcpdump udp port 520

UDP Port 520 may use a defined protocol to communicate depending on the application. UDP port 520 uses the Datagram Protocol, a communications protocol for the Internet network layer, transport layer, and session layer. This protocol when used over PORT 520 makes possible the transmission of a datagram message from one computer to an application running in another computer.

8.2 tcpdump -x -s 120 ip proto 89

To capture OCPF Packets with size 120 bits.Open Shortest Path First (OSPF) is a routing protocol for Internet Protocol networks. It uses a link state routing algorithm and falls into the group of interior gateway protocols, operating within a single autonomous system.

8.3 tcpdump -x -s 70 host ip addr1 and (ip addr2 or ip addr3)

To capture packets and trim down to size 70 bits either to and fro from IP1 or IP2.

8.4 tcpdump -x -s 70 host ip addr1 and not ip addr2

To capture packets where IP addr1 is either src or dst and IP addr2 is neither of src and dest . Also to trim packets to 70 bits.

9 Q9: tcpdump -n -nn host your host and remote host

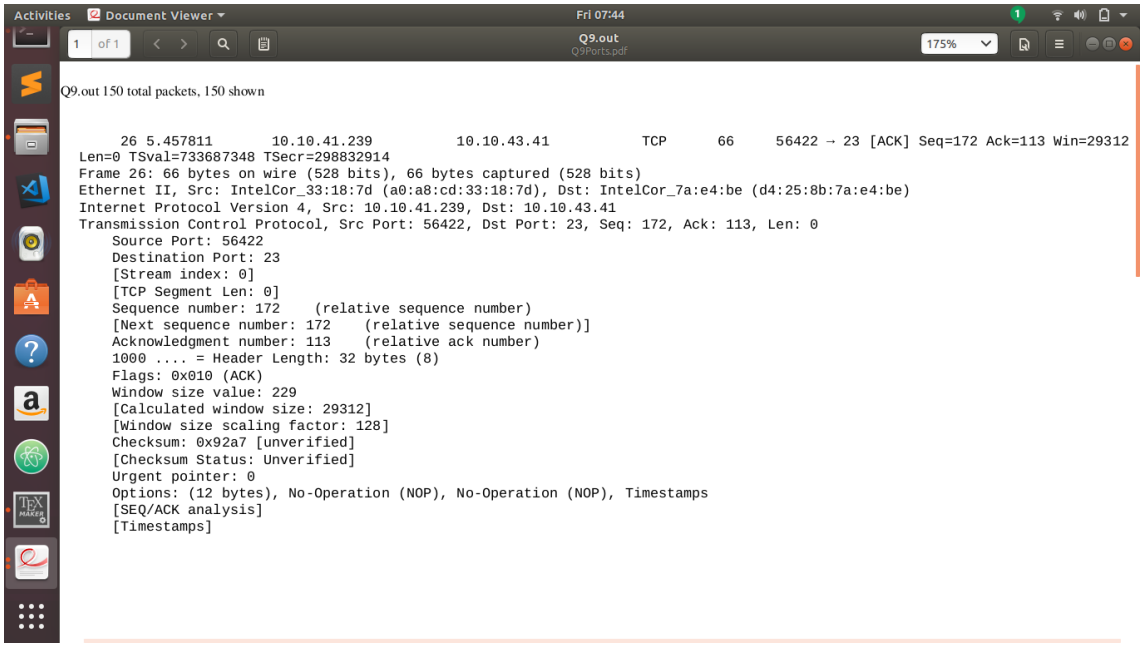

Figure 9: Screenshot of tcpdump packet

9.1 port numbers used by the remote and the local computer

Remote Port No : 23
Local Port No : 56422

9.2 Which machine port number matches the port number listed for telnet in the /etc/services file

Remote machine port no matches with the port number listed for telnet (23) in etc/services file

10 Q10: tcpdump -n -nn host your host and remote host

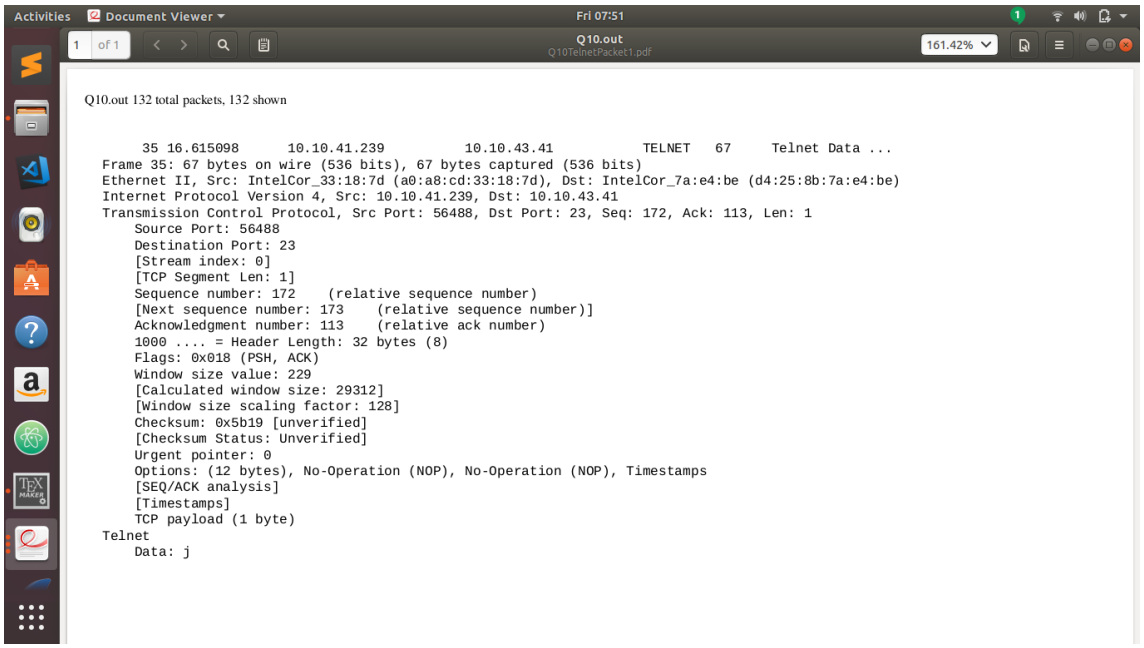

Figure 10: Screenshot of packet1.

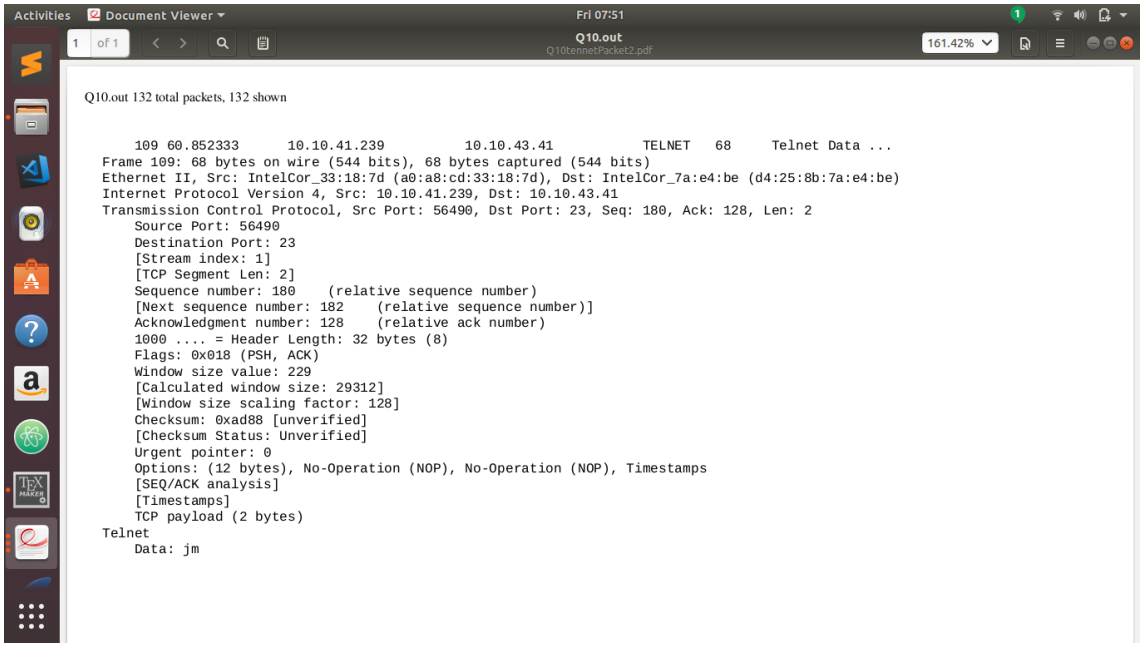

Figure 11: Screenshot of packet2.

10.1 A

Remote Machine Port No : 23
Yes both sessions are connected to the same port number on the remote machine.

10.2 B

1st Telnet session Local Machine Port No : 56488
2nd Telnet session Local Machine Port No : 56490

10.3 C

Internet-wide port number : 0 - 1023
For linux systems : 1 - 60179
client port numbers : 1024 - 65535
The ports in etc/services differ from 1 - 60000 range. Hence the client port number are not consistent.