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

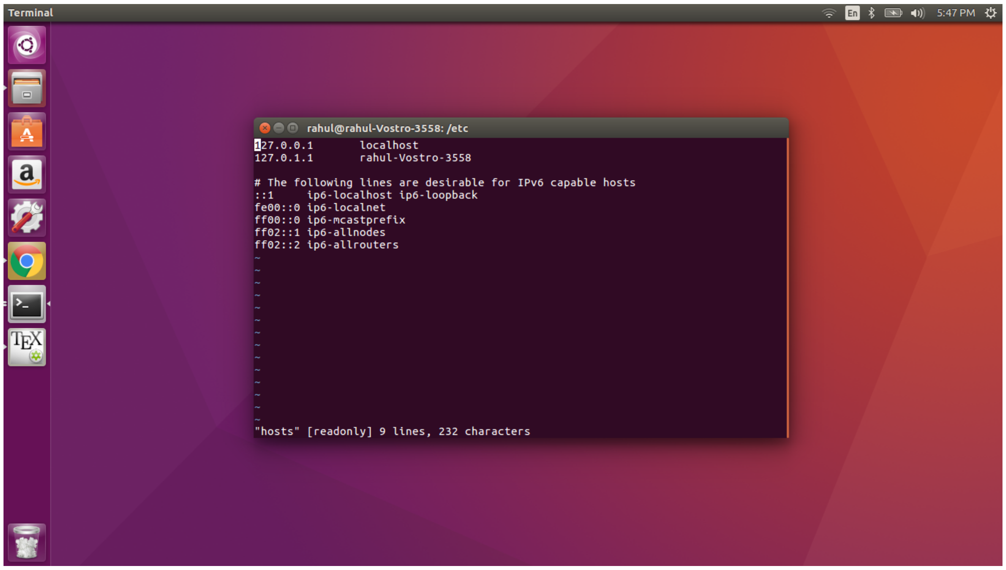
Rahul Byas Sherwan
Entry No. : 2016UCS0028

1: The First Problem

Note : If the screenshot is not available in the subparts below then it is because I am not able to find the file(iam using ubuntu 16.04 lts).So, in that case i have gathered information from internet and wrote that after understanding it.

(a) /etc/hosts:

/etc/hosts is an operating system file that translate hostsname or domain names to IP addresses.This is useful for testing websites changes or the SSL setup before taking a website publicly live.



```
127.0.0.1       localhost
127.0.1.1       rahul-Vostro-3558

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"hosts" [readonly] 9 lines, 232 characters
```

Figure 1: hosts file

As we can see a hosts file ,in the screenshot above,notice that 127.0.0.1 is written which is an IP address and many other addresses.So,the IP address 127.0.0.1 is a special-purpose IPv4 address called localhost or loopback address.

(b) /etc/sysconfig/network:

The /etc/sysconfig/network file is used to specify information about the desired network

configuration on our server. The following entries from /etc/sysconfig/network define that IPv4 networking is enabled, IPv6 networking is not enabled, the host name of the system, and the IP address of the default network gateway:
NETWORKING = yes
NETWORKING IPV6 = no
HOSTNAME = host20.rahul.com
GATEWAY = 192.168.1.1

(c) /etc/sysconfig/network-scripts/ifcfg-eth0:

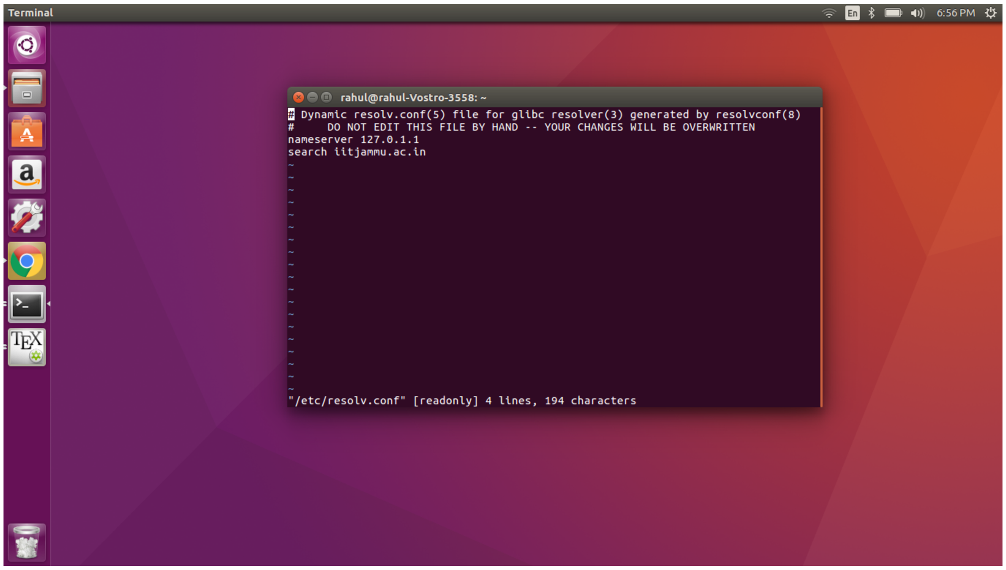
One of the most common interface files is /etc/sysconfig/network-scripts/ifcfg-eth0, which controls the first Ethernet network interface card or NIC in the system. In a system with multiple NICs, there are multiple ifcfg-ethX files (where X is a unique number corresponding to a specific interface). Because each device has its own configuration file, an administrator can control how each interface functions individually.

(d) /etc/default-route:

The default route is a setting on a computer that defines the packet forwarding rule to use when no specific route can be determined for a given Internet Protocol (IP) destination address. All packets for destinations not established in the routing table are sent via the default route.
The default route generally points to another router, which treats the packet the same way: if a route matches, the packet is forwarded accordingly, otherwise the packet is forwarded to the default route of that router.

(e) /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 (DNS) resolver.



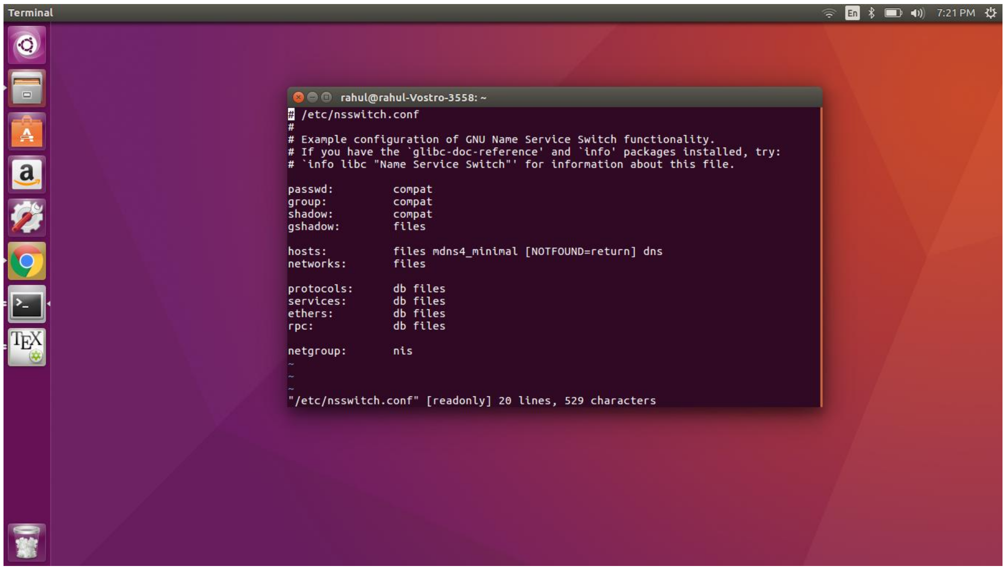
```
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 127.0.1.1
search iitjammu.ac.in
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/resolv.conf" [readonly] 4 lines, 194 characters
```

Figure 2: resolv.conf

As you can see in the above screenshot, the file resolv.conf typically contains directives that specify the default search domains , in my case it is iitjammu.ac.in.

(f) /etc/nsswitch.conf

The /etc/nsswitch.conf file defines the order in which to contact different name services.
For Internet use, it is important that dns shows up in the ”hosts” line.This instructs your computer to look up hostnames and IP addresses first in the /etc/hosts file, and to contact the DNS server if a given host does not occur in the local hosts file. Other possible name services to contact are LDAP, NIS and NIS+.



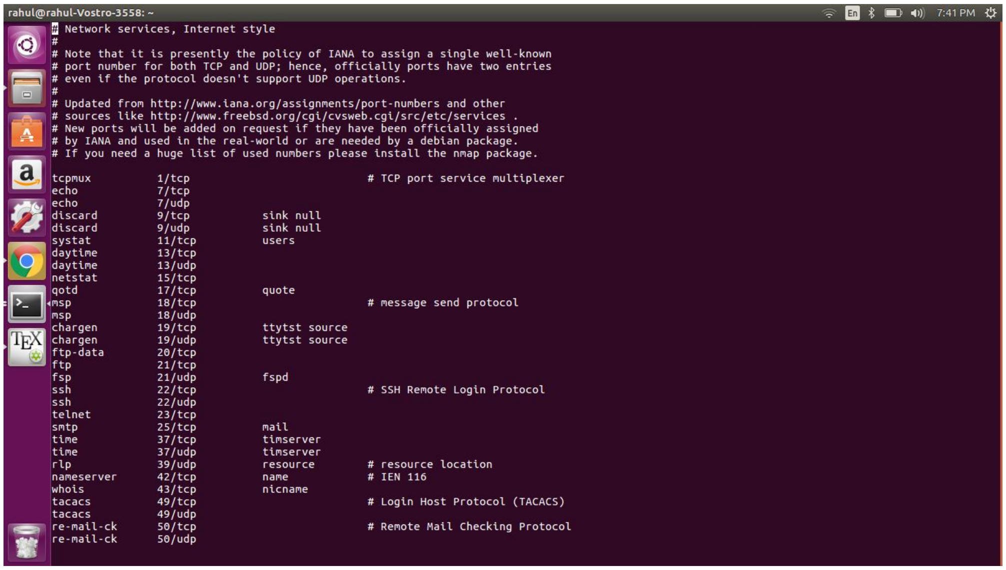
```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:         compat
group:          compat
shadow:         compat
gshadow:        files

hosts:          files mdns4_minimal [NOTFOUND=return] dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
~
~
~
"/etc/nsswitch.conf" [readonly] 20 lines, 529 characters
```

Figure 3: nsswitch.conf

2: The second problem

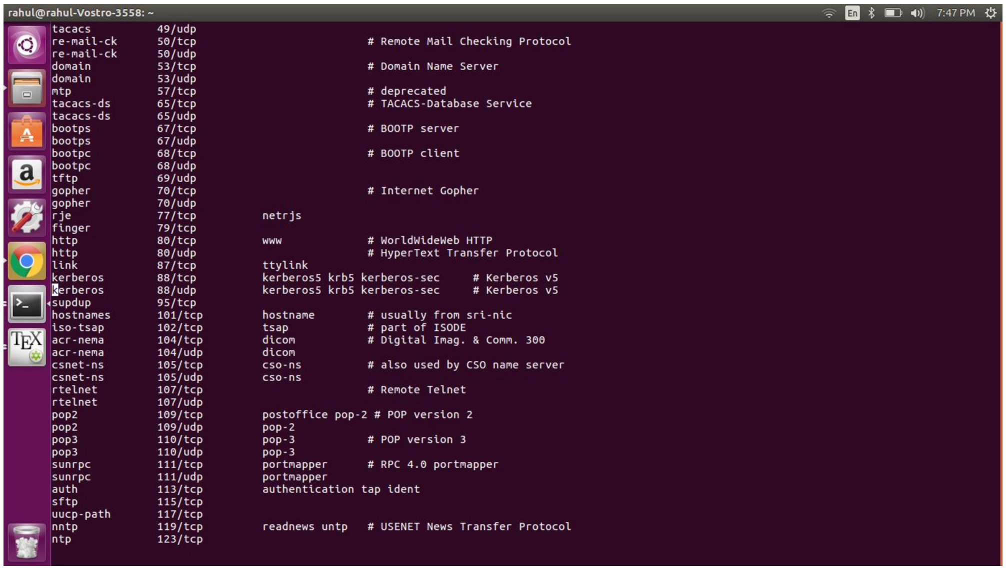
(a) Screenshots of services file:

Since the file content is quiet large . So, I have clicked 3 important parts of the file .In ”service file b.”(figure 5) you can notice the port no. of famous server (http) which is 80.



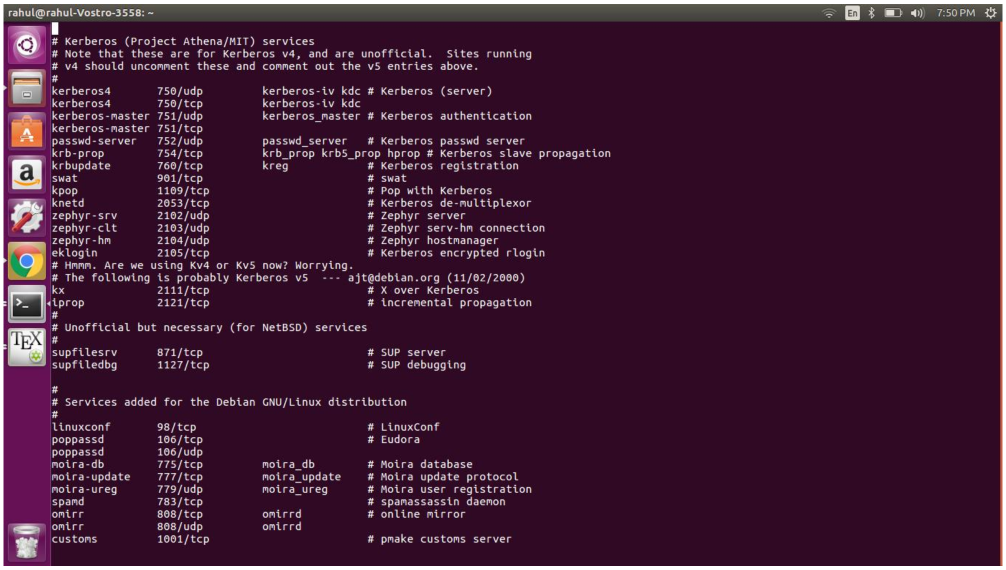
```
# Network services, Internet style
#
# Note that it is presently the policy of IANA to assign a single well-known
# port number for both TCP and UDP; hence, officially ports have two entries
# even if the protocol doesn't support UDP operations.
#
# Updated from http://www.iana.org/assignments/port-numbers and other
# sources like http://www.freebsd.org/cgi/cvsweb.cgi/src/etc/services .
# New ports will be added on request if they have been officially assigned
# by IANA and used in the real-world or are needed by a debian package.
# If you need a huge list of used numbers please install the nmap package.

tcpmux          1/tcp                           # TCP port service multiplexer
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
qotd            17/tcp          quote
msp             18/tcp                          # message send protocol
msp             18/udp
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
ftp-data        20/tcp
ftp             21/tcp
fsp             21/udp          fspd
ssh             22/tcp                          # SSH Remote Login Protocol
ssh             22/udp
telnet          23/tcp
smtp            25/tcp          mail
time            37/tcp          timserver
time            37/udp          timserver
rlp             39/udp          resource        # resource location
nameserver      42/tcp          name            # IEN 116
whois           43/tcp          nicname
tacacs          49/tcp                          # Login Host Protocol (TACACS)
tacacs          49/udp
re-mail-ck      50/tcp                          # Remote Mail Checking Protocol
re-mail-ck      50/udp
```

Figure 4: services file a.



```
tacacs          49/udp
re-mail-ck      50/tcp                          # Remote Mail Checking Protocol
re-mail-ck      50/udp
domain          53/tcp                          # Domain Name Server
domain          53/udp
mtp             57/tcp                          # deprecated
tacacs-ds       65/tcp                          # TACACS-Database Service
tacacs-ds       65/udp
bootps          67/tcp                          # BOOTP server
bootps          67/udp
bootpc          68/tcp                          # BOOTP client
bootpc          68/udp
tftp            69/udp
gopher          70/tcp                          # Internet Gopher
gopher          70/udp
rje             77/tcp          netrjs
finger          79/tcp
http            80/tcp          www             # WorldWideWeb HTTP
http            80/udp                          # HyperText Transfer Protocol
link            87/tcp          ttylink
kerberos        88/tcp          kerberos5 krb5 kerberos-sec     # Kerberos v5
kerberos        88/udp          kerberos5 krb5 kerberos-sec     # Kerberos v5
supdup          95/tcp
hostnames       101/tcp         hostname        # usually from sri-nic
iso-tsap        102/tcp         tsap            # part of ISODE
acr-nema        104/tcp         dicom           # Digital Imag. & Comm. 300
acr-nema        104/udp         dicom
csnet-ns        105/tcp         cso-ns          # also used by CSO name server
csnet-ns        105/udp         cso-ns
rtelnet         107/tcp                         # Remote Telnet
rtelnet         107/udp
pop2            109/tcp         postoffice pop-2 # POP version 2
pop2            109/udp         pop-2
pop3            110/tcp         pop-3           # POP version 3
pop3            110/udp         pop-3
sunrpc          111/tcp         portmapper      # RPC 4.0 portmapper
sunrpc          111/udp         portmapper
auth            113/tcp         authentication tap ident
sftp            115/tcp
uucp-path       117/tcp
nntp            119/tcp         readnews untp   # USENET News Transfer Protocol
ntp             123/tcp
```

Figure 5: services file b.



```
# Kerberos (Project Athena/MIT) services
# Note that these are for Kerberos v4, and are unofficial.  Sites running
# v4 should uncomment these and comment out the v5 entries above.
#
kerberos4       750/udp         kerberos-iv kdc # Kerberos (server)
kerberos4       750/tcp         kerberos-iv kdc
kerberos-master 751/udp         kerberos_master # Kerberos authentication
kerberos-master 751/tcp
passwd-server   752/udp         passwd_server   # Kerberos passwd server
krb-prop        754/tcp         krb_prop krb5_prop hprop # Kerberos slave propagation
krbupdate       760/tcp         kreg            # Kerberos registration
swat            901/tcp                         # swat
kpop            1109/tcp                        # Pop with Kerberos
knetd           2053/tcp                        # Kerberos de-multiplexor
zephyr-srv      2102/udp                        # Zephyr server
zephyr-clt      2103/udp                        # Zephyr serv-hm connection
zephyr-hm       2104/udp                        # Zephyr hostmanager
eklogin         2105/tcp                        # Kerberos encrypted rlogin
# Hmmm. Are we using Kv4 or Kv5 now? Worrying.
# The following is probably Kerberos v5  --- ajt@debian.org (11/02/2000)
kx              2111/tcp                        # X over Kerberos
iprop           2121/tcp                        # incremental propagation
#
# Unofficial but necessary (for NetBSD) services
#
supfilesrv      871/tcp                         # SUP server
supfiledbg      1127/tcp                        # SUP debugging

#
# Services added for the Debian GNU/Linux distribution
#
linuxconf       98/tcp                          # LinuxConf
poppassd        106/tcp                         # Eudora
poppassd        106/udp
moira-db        775/tcp         moira_db        # Moira database
moira-update    777/tcp         moira_update    # Moira update protocol
moira-ureg      779/udp         moira_ureg      # Moira user registration
spamd           783/tcp                         # spamassassin daemon
omirr           808/tcp         omirrd          # online mirror
omirr           808/udp         omirrd
customs         1001/tcp                        # pmake customs server
```

Figure 6: services file c.

(b) Use of services file:

It 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. The port numbers are mapped to specific services much like the hosts file on Windows computers map a hostname to an IP address. However, the UNIX operating system's services file does not include IP addresses but instead information like whether the service is TCP or UDP and what common names it might go by.

(c) Which layer in the TCP/IP protocol stack do you think would make use of this file ?:

Answer: Application layer.

(d) Are the port numbers shown in this file well-known port numbers or ephemeral port numbers ? Why are they so ?:

Answer: As we know that well known port numbers are upto 1023 and well registered port numbers are from 1024 - 49000(approx.) and finally comes the dhcp which is from 49000 to 65534 . So, as we can see in the screenshots above , we have both well-known port numbers and ephemeral port numbers.

3: The third problem

(a) arp:

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network.

(b) arping:

arping is a computer software tool for discovering and probing hosts on a computer network. Arping probes hosts on the attached network link by sending Link Layer frames using the Address Resolution Protocol (ARP) request method addressed to a host identified by its MAC address of the network interface.[1] The utility program may use ARP to resolve an IP address provided by the user.

(c) ifconfig:

ifconfig include setting the IP address and netmask of a network interface and disabling or enabling an interface.ifconfig is a system administration utility for network interface configuration.

(d) tcpdump:

tcpdump is a common packet analyzer that runs under the command line. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.

(e) ping:

PING (Packet INternet Groper) command is the best way to test connectivity between two nodes. Whether it is Local Area Network (LAN) or Wide Area Network (WAN). Ping use ICMP (Internet Control Message Protocol) to communicate to other devices. You can ping host name of ip address using below command.

(f) netstat:

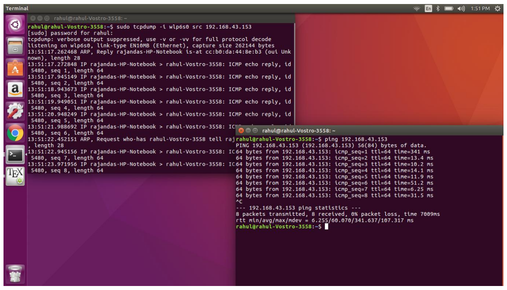
netstat (network statistics) is a command line tool for monitoring network connections both incoming and outgoing as well as viewing routing tables, interface statistics etc. netstat is one of the most basic network service debugging tools, telling you what ports are open and whether any programs are listening on ports.

(g) route:

In computer networking, a router is a device responsible for forwarding network traffic. When datagrams arrive at a router, the router must determine the best way to route them to their destination.

4: The fourth problem

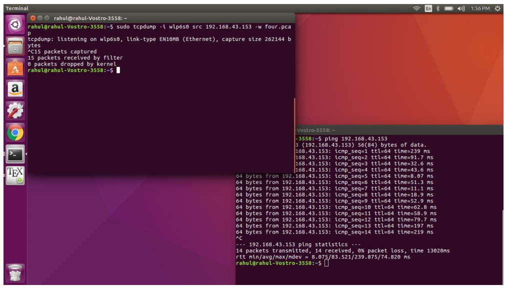
Given below are some screenshots of remote connections establishment check. In figure-7 as we can see that ping is working properly. In figure - 9 we can see the packages captured tcpdump packages (which is further written in a file named as ”four.pcap”) opened in wireshark.



```
rahul@rahul-Vostro-3558:~$ sudo tcpdump -i wlp6s0 src 192.168.43.153
[sudo] password for rahul:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlp6s0, link-type EN10MB (Ethernet), capture size 262144 bytes
13:51:17.262468 ARP, Reply rajandas-HP-Notebook is-at cc:b0:da:44:8e:b3 (oui Unk
nown), length 28
13:51:17.272848 IP rajandas-HP-Notebook > rahul-Vostro-3558: ICMP echo reply, id
 5480, seq 1, length 64
13:51:17.945149 IP rajandas-HP-Notebook > rahul-Vostro-3558: ICMP echo reply, id
 5480, seq 2, length 64
13:51:18.943673 IP rajandas-HP-Notebook > rahul-Vostro-3558: ICMP echo reply, id
 5480, seq 3, length 64
13:51:19.949051 IP rajandas-HP-Notebook > rahul-Vostro-3558: ICMP echo reply, id
 5480, seq 4, length 64
13:51:20.948249 IP rajandas-HP-Notebook > rahul-Vostro-3558: ICMP echo reply, id
 5480, seq 5, length 64
13:51:21.988692 IP rajandas-HP-Notebook > rahul-Vostro-3558: IC
 5480, seq 6, length 64
13:51:22.452151 ARP, Request who-has rahul-Vostro-3558 tell raj
, length 28
13:51:22.945156 IP rajandas-HP-Notebook > rahul-Vostro-3558: IC
 5480, seq 7, length 64
13:51:23.971956 IP rajandas-HP-Notebook > rahul-Vostro-3558: IC
 5480, seq 8, length 64
```

```
rahul@rahul-Vostro-3558:~$ ping 192.168.43.153
PING 192.168.43.153 (192.168.43.153) 56(84) bytes of data.
64 bytes from 192.168.43.153: icmp_seq=1 ttl=64 time=341 ms
64 bytes from 192.168.43.153: icmp_seq=2 ttl=64 time=13.4 ms
64 bytes from 192.168.43.153: icmp_seq=3 ttl=64 time=10.2 ms
64 bytes from 192.168.43.153: icmp_seq=4 ttl=64 time=14.1 ms
64 bytes from 192.168.43.153: icmp_seq=5 ttl=64 time=11.9 ms
64 bytes from 192.168.43.153: icmp_seq=6 ttl=64 time=51.2 ms
64 bytes from 192.168.43.153: icmp_seq=7 ttl=64 time=6.25 ms
64 bytes from 192.168.43.153: icmp_seq=8 ttl=64 time=31.5 ms
^C
--- 192.168.43.153 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7009ms
rtt min/avg/max/mdev = 6.255/60.070/341.637/107.317 ms
rahul@rahul-Vostro-3558:~$
```

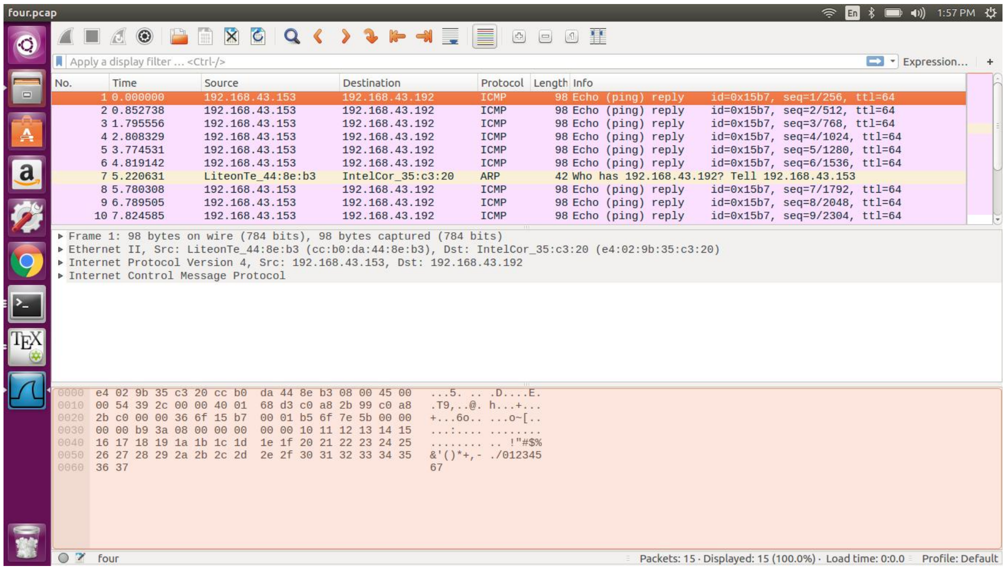
Figure 7: tcpdump and ping command



```
rahul@rahul-Vostro-3558:~$ sudo tcpdump -i wlp6s0 src 192.168.43.153 -w four.pca
p
tcpdump: listening on wlp6s0, link-type EN10MB (Ethernet), capture size 262144 b
ytes
^C15 packets captured
15 packets received by filter
0 packets dropped by kernel
rahul@rahul-Vostro-3558:~$ 
```

```
-3558:~$ ping 192.168.43.153
3 (192.168.43.153) 56(84) bytes of data.
168.43.153: icmp_seq=1 ttl=64 time=239 ms
168.43.153: icmp_seq=2 ttl=64 time=91.7 ms
168.43.153: icmp_seq=3 ttl=64 time=32.6 ms
168.43.153: icmp_seq=4 ttl=64 time=43.6 ms
64 bytes from 192.168.43.153: icmp_seq=5 ttl=64 time=8.07 ms
64 bytes from 192.168.43.153: icmp_seq=6 ttl=64 time=51.3 ms
64 bytes from 192.168.43.153: icmp_seq=7 ttl=64 time=11.1 ms
64 bytes from 192.168.43.153: icmp_seq=8 ttl=64 time=18.9 ms
64 bytes from 192.168.43.153: icmp_seq=9 ttl=64 time=52.9 ms
64 bytes from 192.168.43.153: icmp_seq=10 ttl=64 time=62.8 ms
64 bytes from 192.168.43.153: icmp_seq=11 ttl=64 time=58.9 ms
64 bytes from 192.168.43.153: icmp_seq=12 ttl=64 time=79.7 ms
64 bytes from 192.168.43.153: icmp_seq=13 ttl=64 time=197 ms
64 bytes from 192.168.43.153: icmp_seq=14 ttl=64 time=219 ms
^C
--- 192.168.43.153 ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 13020ms
rtt min/avg/max/mdev = 8.075/83.521/239.875/74.820 ms
rahul@rahul-Vostro-3558:~$ 
```

Figure 8: tcpdumb packets being saved in four.pcap file



```
No.  Time        Source             Destination        Protocol Length Info
   1 0.000000    192.168.43.153     192.168.43.192     ICMP       98 Echo (ping) reply    id=0x15b7, seq=1/256, ttl=64
   2 0.852738    192.168.43.153     192.168.43.192     ICMP       98 Echo (ping) reply    id=0x15b7, seq=2/512, ttl=64
   3 1.795556    192.168.43.153     192.168.43.192     ICMP       98 Echo (ping) reply    id=0x15b7, seq=3/768, ttl=64
   4 2.808329    192.168.43.153     192.168.43.192     ICMP       98 Echo (ping) reply    id=0x15b7, seq=4/1024, ttl=64
   5 3.774531    192.168.43.153     192.168.43.192     ICMP       98 Echo (ping) reply    id=0x15b7, seq=5/1280, ttl=64
   6 4.819142    192.168.43.153     192.168.43.192     ICMP       98 Echo (ping) reply    id=0x15b7, seq=6/1536, ttl=64
   7 5.220631    LiteonTe_44:8e:b3  IntelCor_35:c3:20  ARP        42 Who has 192.168.43.192? Tell 192.168.43.153
   8 5.780308    192.168.43.153     192.168.43.192     ICMP       98 Echo (ping) reply    id=0x15b7, seq=7/1792, ttl=64
   9 6.789505    192.168.43.153     192.168.43.192     ICMP       98 Echo (ping) reply    id=0x15b7, seq=8/2048, ttl=64
  10 7.824585    192.168.43.153     192.168.43.192     ICMP       98 Echo (ping) reply    id=0x15b7, seq=9/2304, ttl=64

▸ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▸ Ethernet II, Src: LiteonTe_44:8e:b3 (cc:b0:da:44:8e:b3), Dst: IntelCor_35:c3:20 (e4:02:9b:35:c3:20)
▸ Internet Protocol Version 4, Src: 192.168.43.153, Dst: 192.168.43.192
▸ Internet Control Message Protocol

0000  e4 02 9b 35 c3 20 cc b0  da 44 8e b3 08 00 45 00   ...5. .. .D....E.
0010  00 54 39 2c 00 00 40 01  68 d3 c0 a8 2b 99 c0 a8   .T9,..@. h...+...
0020  2b c0 00 00 36 6f 15 b7  00 01 b5 6f 7e 5b 00 00   +...6o.. ...o~[..
0030  00 00 b9 3a 08 00 00 00  00 00 10 11 12 13 14 15   ...:.... ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67

four        Packets: 15 · Displayed: 15 (100.0%) · Load time: 0:0.0        Profile: Default
```

Figure 9: captured pakages written in four.pcap file

5: The fifth problem

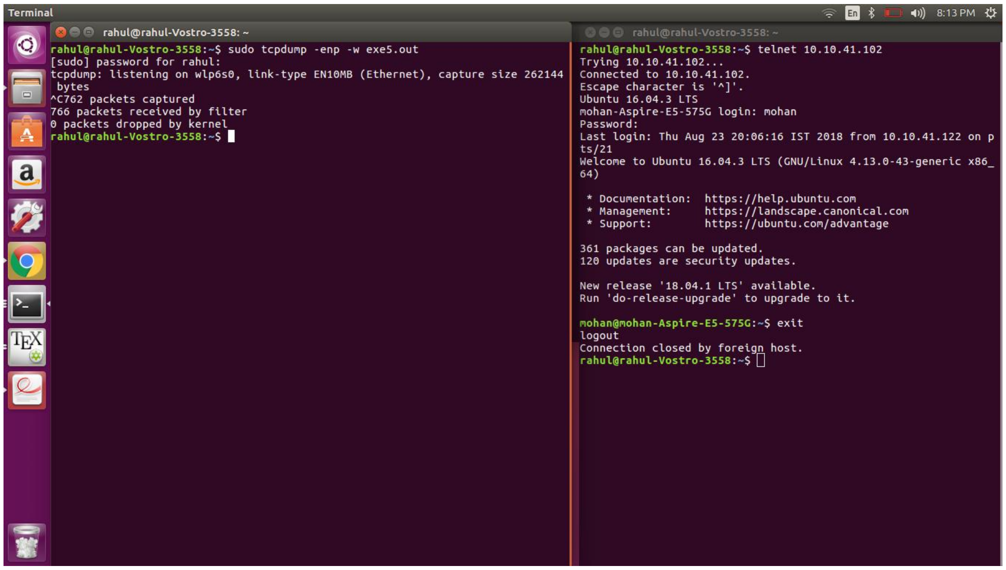
QUESTION: Run the command tcpdump enx w exe5.out. Do you see any output on the screen ? Why ?

ANSWER: After running the command , it says : "tcpdump: listening on wlp6s0, link-type EN10MB (Ethernet), capture size 262144 bytes" and writes the data into exe5.out. Here -enx is used for ethernet network.

Except these things ,we don't see any thing on the screen as the pakages captured are being written to exe5.out file.

Here wlp6s0 is the wireless network interface which enables wifi.

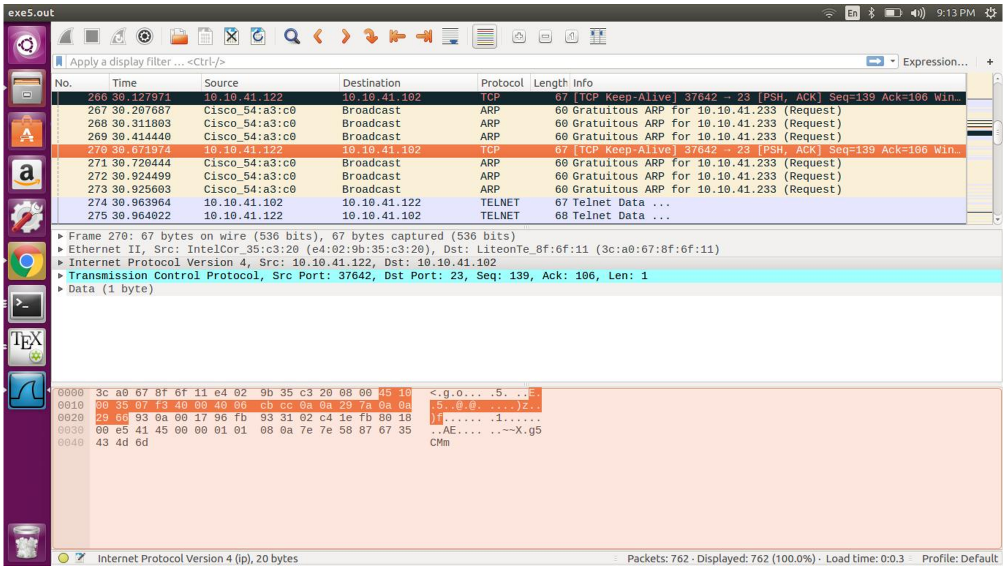
6: The sixth problem



```
rahul@rahul-Vostro-3558:~$ sudo tcpdump -enp -w exe5.out
[sudo] password for rahul:
tcpdump: listening on wlp6s0, link-type EN10MB (Ethernet), capture size 262144
 bytes
^C762 packets captured
766 packets received by filter
0 packets dropped by kernel
rahul@rahul-Vostro-3558:~$
```

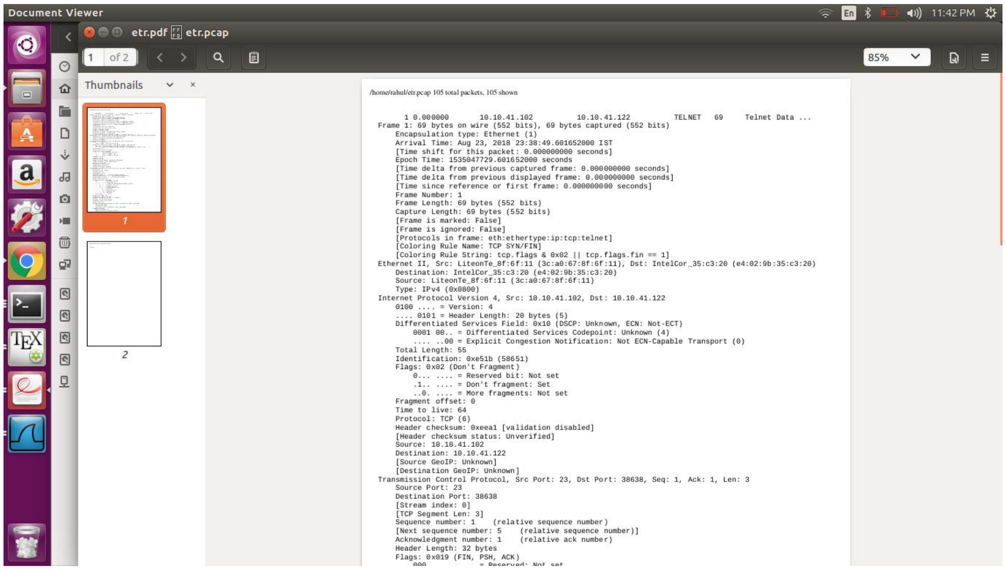
```
rahul@rahul-Vostro-3558:~$ telnet 10.10.41.102
Trying 10.10.41.102...
Connected to 10.10.41.102.
Escape character is '^]'.
Ubuntu 16.04.3 LTS
mohan-Aspire-E5-575G login: mohan
Password:
Last login: Thu Aug 23 20:06:16 IST 2018 from 10.10.41.122 on p
ts/21
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.13.0-43-generic x86_
64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

361 packages can be updated.
120 updates are security updates.

New release '18.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

mohan@mohan-Aspire-E5-575G:~$ exit
logout
Connection closed by foreign host.
rahul@rahul-Vostro-3558:~$
```

Figure 10: remote accessing



```
No.  Time       Source           Destination    Protocol  Length Info
 266 30.127971  10.10.41.122     10.10.41.102   TCP       67 [TCP Keep-Alive] 37642 → 23 [PSH, ACK] Seq=139 Ack=106 Win…
 267 30.207687  Cisco_54:a3:c0   Broadcast      ARP       60 Gratuitous ARP for 10.10.41.233 (Request)
 268 30.311803  Cisco_54:a3:c0   Broadcast      ARP       60 Gratuitous ARP for 10.10.41.233 (Request)
 269 30.414440  Cisco_54:a3:c0   Broadcast      ARP       60 Gratuitous ARP for 10.10.41.233 (Request)
 270 30.671974  10.10.41.122     10.10.41.102   TCP       67 [TCP Keep-Alive] 37642 → 23 [PSH, ACK] Seq=139 Ack=106 Win…
 271 30.720444  Cisco_54:a3:c0   Broadcast      ARP       60 Gratuitous ARP for 10.10.41.233 (Request)
 272 30.924499  Cisco_54:a3:c0   Broadcast      ARP       60 Gratuitous ARP for 10.10.41.233 (Request)
 273 30.925603  Cisco_54:a3:c0   Broadcast      ARP       60 Gratuitous ARP for 10.10.41.233 (Request)
 274 30.963964  10.10.41.102     10.10.41.122   TELNET    67 Telnet Data ...
 275 30.964022  10.10.41.122     10.10.41.102   TELNET    68 Telnet Data ...

▸ Frame 270: 67 bytes on wire (536 bits), 67 bytes captured (536 bits)
▸ Ethernet II, Src: IntelCor_35:c3:20 (e4:02:9b:35:c3:20), Dst: LiteonTe_8f:6f:11 (3c:a0:67:8f:6f:11)
▸ Internet Protocol Version 4, Src: 10.10.41.122, Dst: 10.10.41.102
▸ Transmission Control Protocol, Src Port: 37642, Dst Port: 23, Seq: 139, Ack: 106, Len: 1
▸ Data (1 byte)

0000  3c a0 67 8f 6f 11 e4 02  9b 35 c3 20 08 00 45 10   <.g.o... .5. ..E.
0010  00 35 07 f3 40 00 40 06  cb cc 0a 0a 29 7a 0a 0a   .5..@.@. ....)z..
0020  29 66 93 0a 00 17 96 fb  93 31 02 c4 1e fb 80 18   )f...... .1......
0030  00 e5 41 45 00 00 01 01  08 0a 7e 7e 58 87 67 35   ..AE.... ..~~X.g5
0040  43 4d 6d                                           CMm

Internet Protocol Version 4 (ip), 20 bytes     Packets: 762 · Displayed: 762 (100.0%) · Load time: 0:0.3     Profile: Default
```

Figure 11: captured packages



/home/rahul/etr.pcap 105 total packets, 105 shown

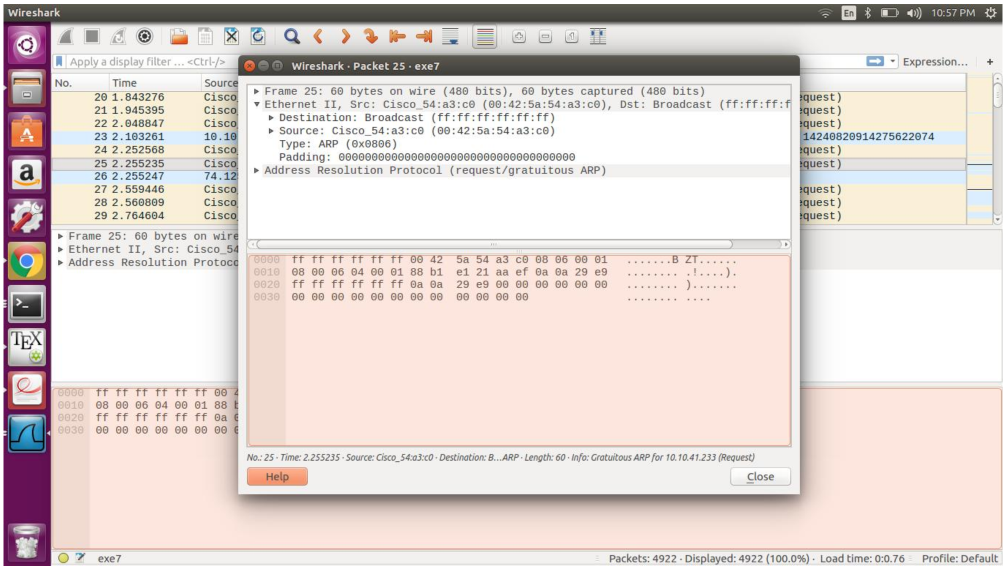
```
      1 0.000000       10.10.41.102          10.10.41.122          TELNET   69     Telnet Data ...
Frame 1: 69 bytes on wire (552 bits), 69 bytes captured (552 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 23, 2018 23:38:49.601652000 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1535047729.601652000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 69 bytes (552 bits)
    Capture Length: 69 bytes (552 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:telnet]
    [Coloring Rule Name: TCP SYN/FIN]
    [Coloring Rule String: tcp.flags & 0x02 || tcp.flags.fin == 1]
Ethernet II, Src: LiteonTe_8f:6f:11 (3c:a0:67:8f:6f:11), Dst: IntelCor_35:c3:20 (e4:02:9b:35:c3:20)
    Destination: IntelCor_35:c3:20 (e4:02:9b:35:c3:20)
    Source: LiteonTe_8f:6f:11 (3c:a0:67:8f:6f:11)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.10.41.102, Dst: 10.10.41.122
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
        0001 00.. = Differentiated Services Codepoint: Unknown (4)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 55
    Identification: 0xe51b (58651)
    Flags: 0x02 (Don't Fragment)
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0xeea1 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.10.41.102
    Destination: 10.10.41.122
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 23, Dst Port: 38638, Seq: 1, Ack: 1, Len: 3
    Source Port: 23
    Destination Port: 38638
    [Stream index: 0]
    [TCP Segment Len: 3]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 5    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Header Length: 32 bytes
    Flags: 0x019 (FIN, PSH, ACK)
```

Figure 12: headers

7: The seventh problem

(a) What is the value of the frame type field in an Ethernet frame carrying an ARP request and in an Ethernet frame carrying an ARP reply, respectively?

Answer: Type: ARP (0X0806)


Wireshark
10:57 PM
Apply a display filter ... <Ctrl-/>
Expression...
Wireshark · Packet 25 · exe7
Help
Close

```
No.  Time        Source
 20 1.843276     Cisco
 21 1.945395     Cisco
 22 2.048847     Cisco
 23 2.103261     10.10
 24 2.252568     Cisco
 25 2.255235     Cisco
 26 2.255247     74.12
 27 2.559446     Cisco
 28 2.560809     Cisco
 29 2.764604     Cisco
```

```
▸ Frame 25: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
▾ Ethernet II, Src: Cisco_54:a3:c0 (00:42:5a:54:a3:c0), Dst: Broadcast (ff:ff:ff:f
   ▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
   ▸ Source: Cisco_54:a3:c0 (00:42:5a:54:a3:c0)
     Type: ARP (0x0806)
     Padding: 000000000000000000000000000000000000
▸ Address Resolution Protocol (request/gratuitous ARP)
```

```
0000  ff ff ff ff ff ff 00 42  5a 54 a3 c0 08 06 00 01   .......B ZT......
0010  08 00 06 04 00 01 88 b1  e1 21 aa ef 0a 0a 29 e9   ........ .!....).
0020  ff ff ff ff ff ff 0a 0a  29 e9 00 00 00 00 00 00   ........ ).......
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

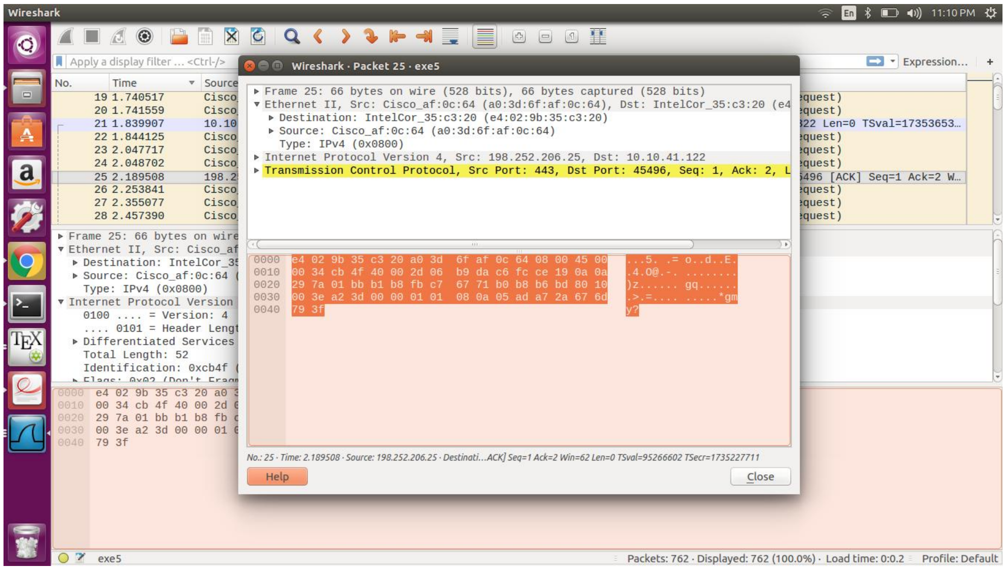
No.: 25 · Time: 2.255235 · Source: Cisco_54:a3:c0 · Destination: B...ARP · Length: 60 · Info: Gratuitous ARP for 10.10.41.233 (Request)

exe7 Packets: 4922 · Displayed: 4922 (100.0%) · Load time: 0:0.76 Profile: Default

Figure 13: ethernet frame type

(b) What is the value of the frame type field in an Ethernet frame carrying an IP datagram captured in the previous exercise?

Answer: Type: IPv4 (0X0800)



```
▸ Frame 25: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▾ Ethernet II, Src: Cisco_af:0c:64 (a0:3d:6f:af:0c:64), Dst: IntelCor_35:c3:20 (e4
  ▸ Destination: IntelCor_35:c3:20 (e4:02:9b:35:c3:20)
  ▸ Source: Cisco_af:0c:64 (a0:3d:6f:af:0c:64)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 198.252.206.25, Dst: 10.10.41.122
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 45496, Seq: 1, Ack: 2, L

0000  e4 02 9b 35 c3 20 a0 3d  6f af 0c 64 08 00 45 00   ...5. .= o..d..E.
0010  00 34 cb 4f 40 00 2d 06  b9 da c6 fc ce 19 0a 0a   .4.O@.-. ........
0020  29 7a 01 bb b1 b8 fb c7  67 71 b0 b8 b6 bd 80 10   )z...... gq......
0030  00 3e a2 3d 00 00 01 01  08 0a 05 ad a7 2a 67 6d   .>.=.... .....*gm
0040  79 3f                                              y?
```

No.: 25 · Time: 2.189508 · Source: 198.252.206.25 · Destinati...ACK] Seq=1 Ack=2 Win=62 Len=0 TSval=95266602 TSecr=1735227711

Wireshark
Wireshark · Packet 25 · exe5
Apply a display filter ... <Ctrl-/>
Expression...
Help
Close
exe5
Packets: 762 · Displayed: 762 (100.0%) · Load time: 0:0.2
Profile: Default
11:10 PM

Figure 14: ethernet frame type

(c) What is the use of the frame type field?

Answer:It carries small but useful information. It allows to recognize the many protocols that may go over Ethernet, be it IPv4, ARP, IPv6, IPX, AppleTalk, and so on.

9: The nineth problem

(a) What are the port numbers used by the remote and the local computer?:

Answer : Remote machine's port number : 23
Local machine's port number : 37838

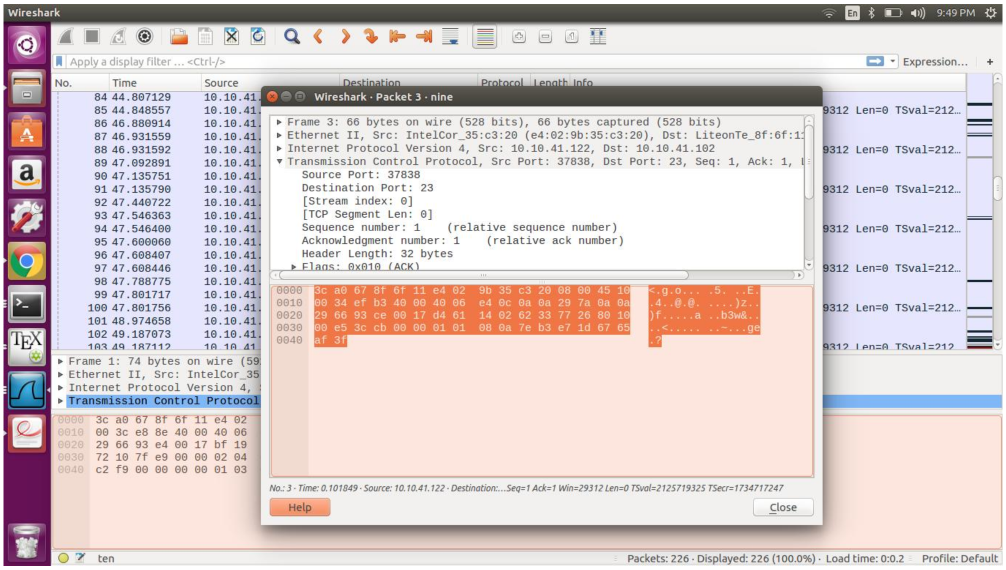
(b) Which machine's port number matches the port number listed for telnet in the /etc/services file?:

Answer : Remote machine's port number matches the port number listed for telnet. (as you can see in the screenshot below)

10: The tenth problem

(a) When you have two telnet sessions with your machine, what port number is used on the remote machine? Are both sessions connected to the same port number on the remote machine?:

Answer: Even in case of two telnet session , the remort machine has a single port number ,i.e. 23 (remote machine's port number).
Yes, both sessions connected to the same port number on the remote machine.(as one can notice



Wireshark
Apply a display filter … <Ctrl-/>
Expression…
Wireshark · Packet 3 · nine
Help
Close
9:49 PM

```
No.  Time       Source
 84 44.807129  10.10.41.
 85 44.848557  10.10.41.
 86 46.880914  10.10.41.
 87 46.931559  10.10.41.
 88 46.931592  10.10.41.
 89 47.092891  10.10.41.
 90 47.135751  10.10.41.
 91 47.135790  10.10.41.
 92 47.440722  10.10.41.
 93 47.546363  10.10.41.
 94 47.546400  10.10.41.
 95 47.600060  10.10.41.
 96 47.608407  10.10.41.
 97 47.608446  10.10.41.
 98 47.788775  10.10.41.
 99 47.801717  10.10.41.
100 47.801756  10.10.41.
101 48.974658  10.10.41.
102 49.187073  10.10.41.
103 49.187112  10.10.41.

9312 Len=0 TSval=212…
9312 Len=0 TSval=212…
9312 Len=0 TSval=212…
9312 Len=0 TSval=212…
9312 Len=0 TSval=212…
9312 Len=0 TSval=212…
9312 Len=0 TSval=212…

▸ Frame 1: 74 bytes on wire (59
▸ Ethernet II, Src: IntelCor_35
▸ Internet Protocol Version 4, S
▸ Transmission Control Protocol

0000  3c a0 67 8f 6f 11 e4 02
0010  00 3c e8 8e 40 00 40 06
0020  29 66 93 e4 00 17 bf 19
0030  72 10 7f e9 00 00 02 04
0040  c2 f9 00 00 00 00 01 03
```

```
▸ Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▸ Ethernet II, Src: IntelCor_35:c3:20 (e4:02:9b:35:c3:20), Dst: LiteonTe_8f:6f:1
▸ Internet Protocol Version 4, Src: 10.10.41.122, Dst: 10.10.41.102
▾ Transmission Control Protocol, Src Port: 37838, Dst Port: 23, Seq: 1, Ack: 1, L
    Source Port: 37838
    Destination Port: 23
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    Header Length: 32 bytes
  ▸ Flags: 0x010 (ACK)

0000  3c a0 67 8f 6f 11 e4 02  9b 35 c3 20 08 00 45 10   <.g.o... .5. ..E.
0010  00 34 ef b3 40 00 40 06  e4 0c 0a 0a 29 7a 0a 0a   .4..@.@. ....)z..
0020  29 66 93 ce 00 17 d4 61  14 02 62 33 77 26 80 10   )f.....a ..b3w&..
0030  00 e5 3c cb 00 00 01 01  08 0a 7e b3 e7 1d 67 65   ..<..... ..~...ge
0040  af 3f                                              .?

No.: 3 · Time: 0.101849 · Source: 10.10.41.122 · Destination:...Seq=1 Ack=1 Win=29312 Len=0 TSval=2125719325 TSecr=1734717247
```

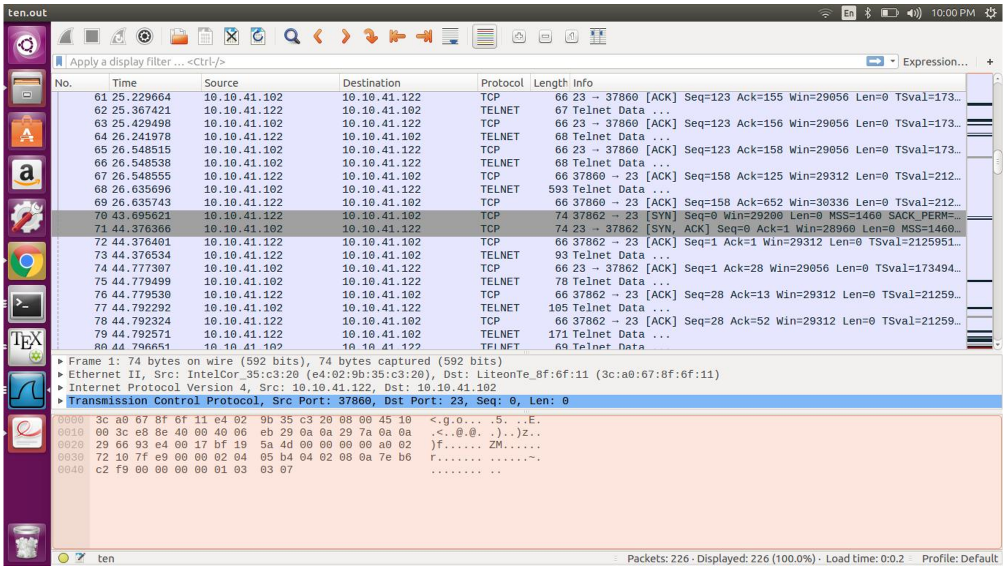
```
ten    Packets: 226 · Displayed: 226 (100.0%) · Load time: 0:0.2    Profile: Default
```

Figure 15: captured packages

in the screenshot given below).

(b) What port numbers are used in your machine for the first and second telnet, respectively?:

Answer: For our machine ,
the first session's port number is : 37860
the first session's port number is : 37862
(one can verify it by the image given below)



```
No.  Time       Source        Destination   Protocol Length Info
 61 25.229664  10.10.41.102  10.10.41.122  TCP        66 23 → 37860 [ACK] Seq=123 Ack=155 Win=29056 Len=0 TSval=173…
 62 25.367421  10.10.41.122  10.10.41.102  TELNET     67 Telnet Data ...
 63 25.429498  10.10.41.102  10.10.41.122  TCP        66 23 → 37860 [ACK] Seq=123 Ack=156 Win=29056 Len=0 TSval=173…
 64 26.241978  10.10.41.122  10.10.41.102  TELNET     68 Telnet Data ...
 65 26.548515  10.10.41.102  10.10.41.122  TCP        66 23 → 37860 [ACK] Seq=123 Ack=158 Win=29056 Len=0 TSval=173…
 66 26.548538  10.10.41.102  10.10.41.122  TELNET     68 Telnet Data ...
 67 26.548555  10.10.41.122  10.10.41.102  TCP        66 37860 → 23 [ACK] Seq=158 Ack=125 Win=29312 Len=0 TSval=212…
 68 26.635696  10.10.41.102  10.10.41.122  TELNET    593 Telnet Data ...
 69 26.635743  10.10.41.122  10.10.41.102  TCP        66 37860 → 23 [ACK] Seq=158 Ack=652 Win=30336 Len=0 TSval=212…
 70 43.695621  10.10.41.122  10.10.41.102  TCP        74 37862 → 23 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=…
 71 44.376366  10.10.41.102  10.10.41.122  TCP        74 23 → 37862 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460…
 72 44.376401  10.10.41.122  10.10.41.102  TCP        66 37862 → 23 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=2125951…
 73 44.376534  10.10.41.122  10.10.41.102  TELNET     93 Telnet Data ...
 74 44.777307  10.10.41.102  10.10.41.122  TCP        66 23 → 37862 [ACK] Seq=1 Ack=28 Win=29056 Len=0 TSval=173494…
 75 44.779499  10.10.41.102  10.10.41.122  TELNET     78 Telnet Data ...
 76 44.779530  10.10.41.122  10.10.41.102  TCP        66 37862 → 23 [ACK] Seq=28 Ack=13 Win=29312 Len=0 TSval=21259…
 77 44.792292  10.10.41.102  10.10.41.122  TELNET    105 Telnet Data ...
 78 44.792324  10.10.41.122  10.10.41.102  TCP        66 37862 → 23 [ACK] Seq=28 Ack=52 Win=29312 Len=0 TSval=21259…
 79 44.792571  10.10.41.122  10.10.41.102  TELNET    171 Telnet Data ...
 80 44.796651  10.10.41.102  10.10.41.122  TELNET     69 Telnet Data ...

▸ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
▸ Ethernet II, Src: IntelCor_35:c3:20 (e4:02:9b:35:c3:20), Dst: LiteonTe_8f:6f:11 (3c:a0:67:8f:6f:11)
▸ Internet Protocol Version 4, Src: 10.10.41.122, Dst: 10.10.41.102
▸ Transmission Control Protocol, Src Port: 37860, Dst Port: 23, Seq: 0, Len: 0

0000  3c a0 67 8f 6f 11 e4 02  9b 35 c3 20 08 00 45 10   <.g.o... .5. ..E.
0010  00 3c e8 8e 40 00 40 06  eb 29 0a 0a 29 7a 0a 0a   .<..@.@. .)..)z..
0020  29 66 93 e4 00 17 bf 19  5a 4d 00 00 00 00 a0 02   )f...... ZM......
0030  72 10 7f e9 00 00 02 04  05 b4 04 02 08 0a 7e b6   r....... ......~.
0040  c2 f9 00 00 00 00 01 03  03 07                     ........ ..

ten    Packets: 226 · Displayed: 226 (100.0%) · Load time: 0:0.2    Profile: Default
```

Figure 16: captured packages

(c) What is the range of Internet-wide well-known port numbers? What is the range

of well-known port numbers for Unix/Linux specific service? What is the range for a client port number? Compare your answer to the well-known port numbers defined in the /etc/services file. Are they consistent? In case they are not, try to discuss amongst peers and specify your view of the reason why they are not.:
Answer: The well-known ports cover the range of possible port numbers from 0 through 1023. The client ports cover the range of possible port numbers from 49152 to 65535.