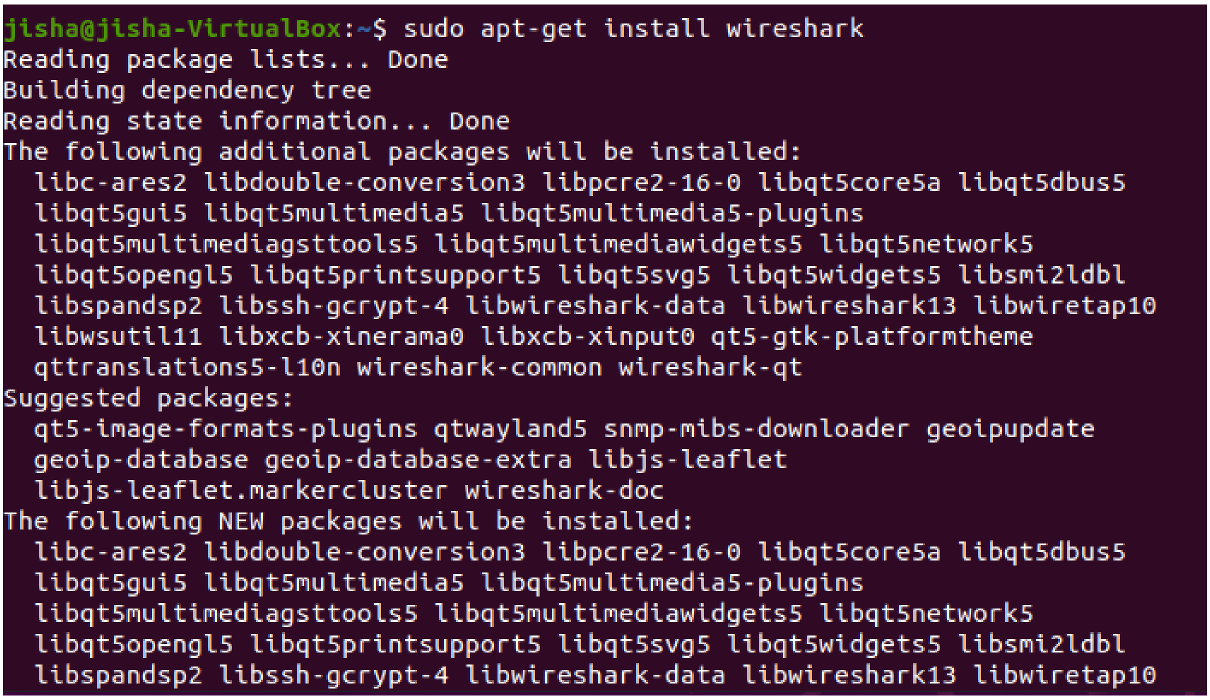
ASSIGNMENT

Submitted by:Jisha Chacko

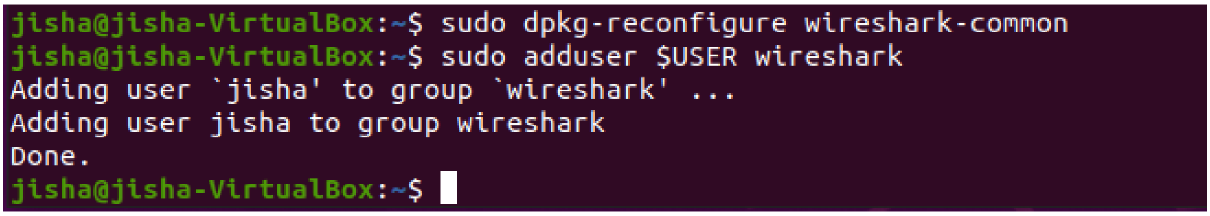
S2RMCA:A

RollNo:44

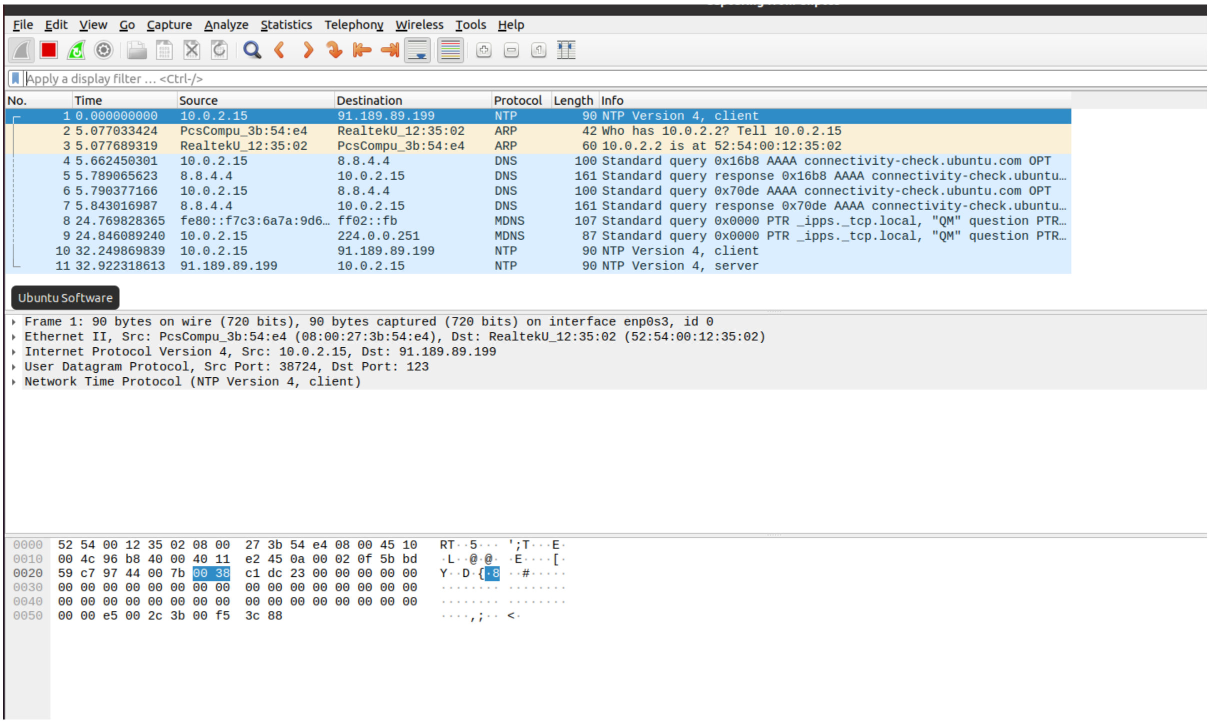
Wireshark installation



```
jisha@jisha-VirtualBox:~$ sudo apt-get install wireshark
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libc-ares2 libdouble-conversion3 libpcre2-16-0 libqt5core5a libqt5dbus5
  libqt5gui5 libqt5multimedia5 libqt5multimedia5-plugins
  libqt5multimediagsttools5 libqt5multimediawidgets5 libqt5network5
  libqt5opengl5 libqt5printsupport5 libqt5svg5 libqt5widgets5 libsmi2ldbl
  libspandsp2 libssh-gcrypt-4 libwireshark-data libwireshark13 libwiretap10
  libwsutil11 libxcb-xinerama0 libxcb-xinput0 qt5-gtk-platformtheme
  qttranslations5-l10n wireshark-common wireshark-qt
Suggested packages:
  qt5-image-formats-plugins qtwayland5 snmp-mibs-downloader geoipupdate
  geoip-database geoip-database-extra libjs-leaflet
  libjs-leaflet.markercluster wireshark-doc
The following NEW packages will be installed:
  libc-ares2 libdouble-conversion3 libpcre2-16-0 libqt5core5a libqt5dbus5
  libqt5gui5 libqt5multimedia5 libqt5multimedia5-plugins
  libqt5multimediagsttools5 libqt5multimediawidgets5 libqt5network5
  libqt5opengl5 libqt5printsupport5 libqt5svg5 libqt5widgets5 libsmi2ldbl
  libspandsp2 libssh-gcrypt-4 libwireshark-data libwireshark13 libwiretap10
```



```
jisha@jisha-VirtualBox:~$ sudo dpkg-reconfigure wireshark-common
jisha@jisha-VirtualBox:~$ sudo adduser $USER wireshark
Adding user `jisha' to group `wireshark' ...
Adding user jisha to group wireshark
Done.
jisha@jisha-VirtualBox:~$ 
```

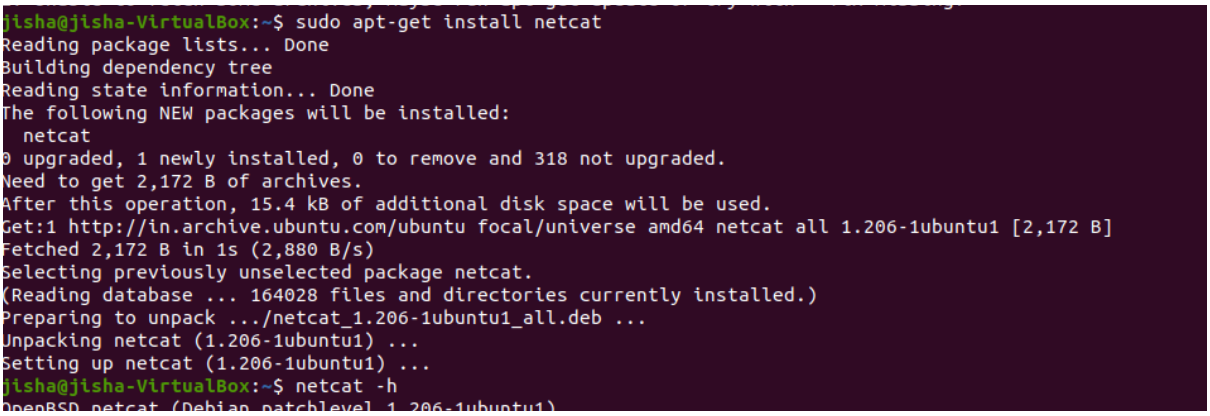


```
No.     Time           Source                 Destination       Protocol  Length Info
      1 0.000000000    10.0.2.15              91.189.89.199     NTP         90 NTP Version 4, client
      2 5.077033424    PcsCompu_3b:54:e4      RealtekU_12:35:02 ARP         42 Who has 10.0.2.2? Tell 10.0.2.15
      3 5.077689319    RealtekU_12:35:02      PcsCompu_3b:54:e4 ARP         60 10.0.2.2 is at 52:54:00:12:35:02
      4 5.662450301    10.0.2.15              8.8.4.4           DNS        100 Standard query 0x16b8 AAAA connectivity-check.ubuntu.com OPT
      5 5.789065623    8.8.4.4                10.0.2.15         DNS        161 Standard query response 0x16b8 AAAA connectivity-check.ubuntu…
      6 5.790377166    10.0.2.15              8.8.4.4           DNS        100 Standard query 0x70de AAAA connectivity-check.ubuntu.com OPT
      7 5.843016987    8.8.4.4                10.0.2.15         DNS        161 Standard query response 0x70de AAAA connectivity-check.ubuntu…
      8 24.769828365   fe80::f7c3:6a7a:9d6…   ff02::fb          MDNS       107 Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR…
      9 24.846089240   10.0.2.15              224.0.0.251       MDNS        87 Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR…
     10 32.249869839   10.0.2.15              91.189.89.199     NTP         90 NTP Version 4, client
     11 32.922318613   91.189.89.199          10.0.2.15         NTP         90 NTP Version 4, server
```

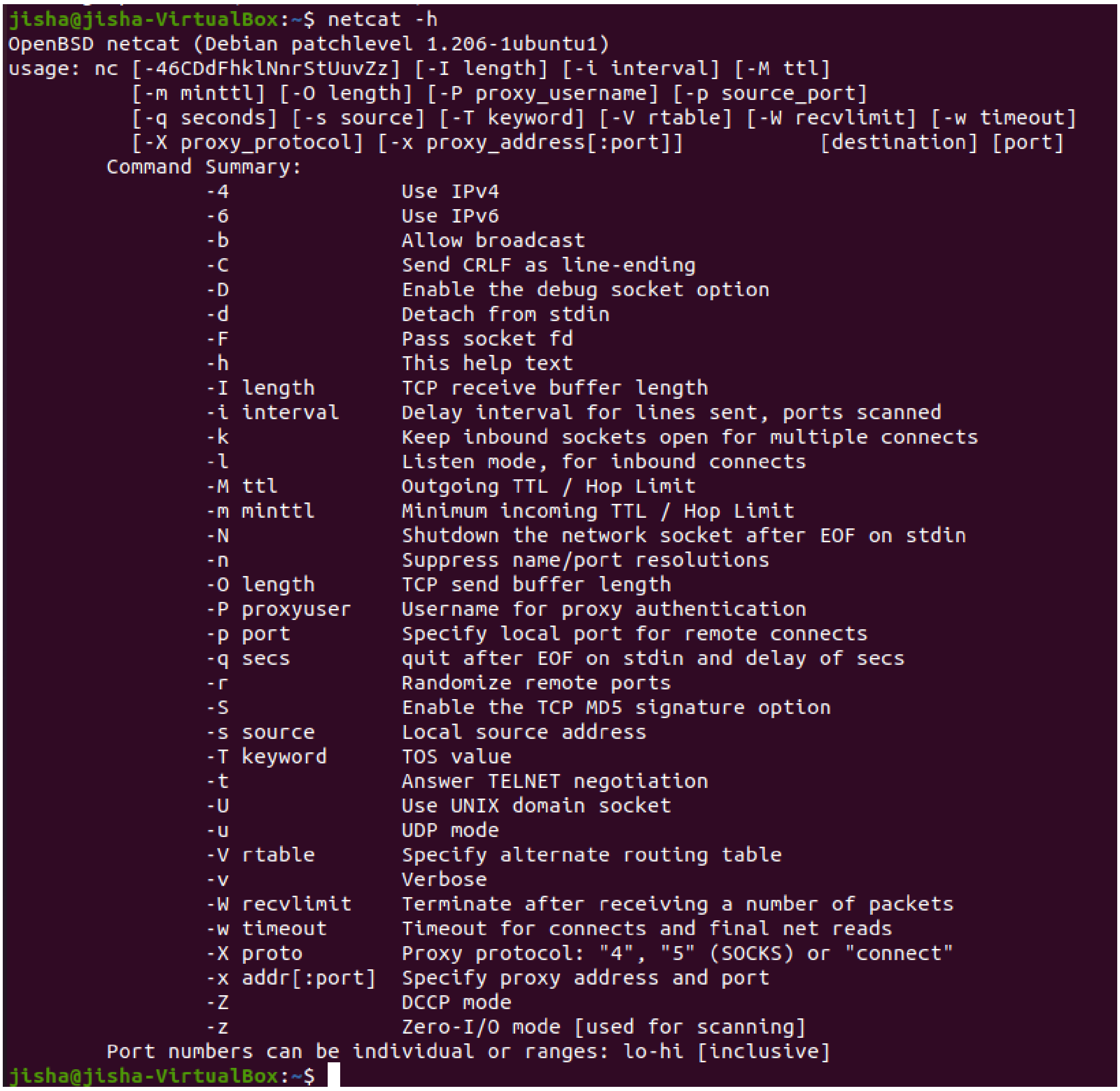
```
▸ Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: PcsCompu_3b:54:e4 (08:00:27:3b:54:e4), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 91.189.89.199
▸ User Datagram Protocol, Src Port: 38724, Dst Port: 123
▸ Network Time Protocol (NTP Version 4, client)
```

```
0000  52 54 00 12 35 02 08 00  27 3b 54 e4 08 00 45 10   RT··5···  ';T···E·
0010  00 4c 96 b8 40 00 40 11  e2 45 0a 00 02 0f 5b bd   ·L··@·@·  ·E····[·
0020  59 c7 97 44 00 7b 00 38  c1 dc 23 00 00 00 00 00   Y··D·{·8  ··#·····
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ········
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ········
0050  00 00 e5 00 2c 3b 00 f5  3c 88                     ····,;··  <·
```

NETCAT



```
jisha@jisha-VirtualBox:~$ sudo apt-get install netcat
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  netcat
0 upgraded, 1 newly installed, 0 to remove and 318 not upgraded.
Need to get 2,172 B of archives.
After this operation, 15.4 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 netcat all 1.206-1ubuntu1 [2,172 B]
Fetched 2,172 B in 1s (2,880 B/s)
Selecting previously unselected package netcat.
(Reading database ... 164028 files and directories currently installed.)
Preparing to unpack .../netcat_1.206-1ubuntu1_all.deb ...
Unpacking netcat (1.206-1ubuntu1) ...
Setting up netcat (1.206-1ubuntu1) ...
jisha@jisha-VirtualBox:~$ netcat -h
OpenBSD netcat (Debian patchlevel 1.206-1ubuntu1)
```



```
jisha@jisha-VirtualBox:~$ netcat -h
OpenBSD netcat (Debian patchlevel 1.206-1ubuntu1)
usage: nc [-46CDdFhklNnrStUuvZz] [-I length] [-i interval] [-M ttl]
          [-m minttl] [-O length] [-P proxy_username] [-p source_port]
          [-q seconds] [-s source] [-T keyword] [-V rtable] [-W recvlimit] [-w timeout]
          [-X proxy_protocol] [-x proxy_address[:port]]           [destination] [port]
        Command Summary:
                -4              Use IPv4
                -6              Use IPv6
                -b              Allow broadcast
                -C              Send CRLF as line-ending
                -D              Enable the debug socket option
                -d              Detach from stdin
                -F              Pass socket fd
                -h              This help text
                -I length       TCP receive buffer length
                -i interval     Delay interval for lines sent, ports scanned
                -k              Keep inbound sockets open for multiple connects
                -l              Listen mode, for inbound connects
                -M ttl          Outgoing TTL / Hop Limit
                -m minttl       Minimum incoming TTL / Hop Limit
                -N              Shutdown the network socket after EOF on stdin
                -n              Suppress name/port resolutions
                -O length       TCP send buffer length
                -P proxyuser    Username for proxy authentication
                -p port         Specify local port for remote connects
                -q secs         quit after EOF on stdin and delay of secs
                -r              Randomize remote ports
                -S              Enable the TCP MD5 signature option
                -s source       Local source address
                -T keyword      TOS value
                -t              Answer TELNET negotiation
                -U              Use UNIX domain socket
                -u              UDP mode
                -V rtable       Specify alternate routing table
                -v              Verbose
                -W recvlimit    Terminate after receiving a number of packets
                -w timeout      Timeout for connects and final net reads
                -X proto        Proxy protocol: "4", "5" (SOCKS) or "connect"
                -x addr[:port]  Specify proxy address and port
                -Z              DCCP mode
                -z              Zero-I/O mode [used for scanning]
        Port numbers can be individual or ranges: lo-hi [inclusive]
jisha@jisha-VirtualBox:~$
```