ASSIGNMENT

ANALYZING NETWORK PACKET STREAM USING NC AND WIRESHARK

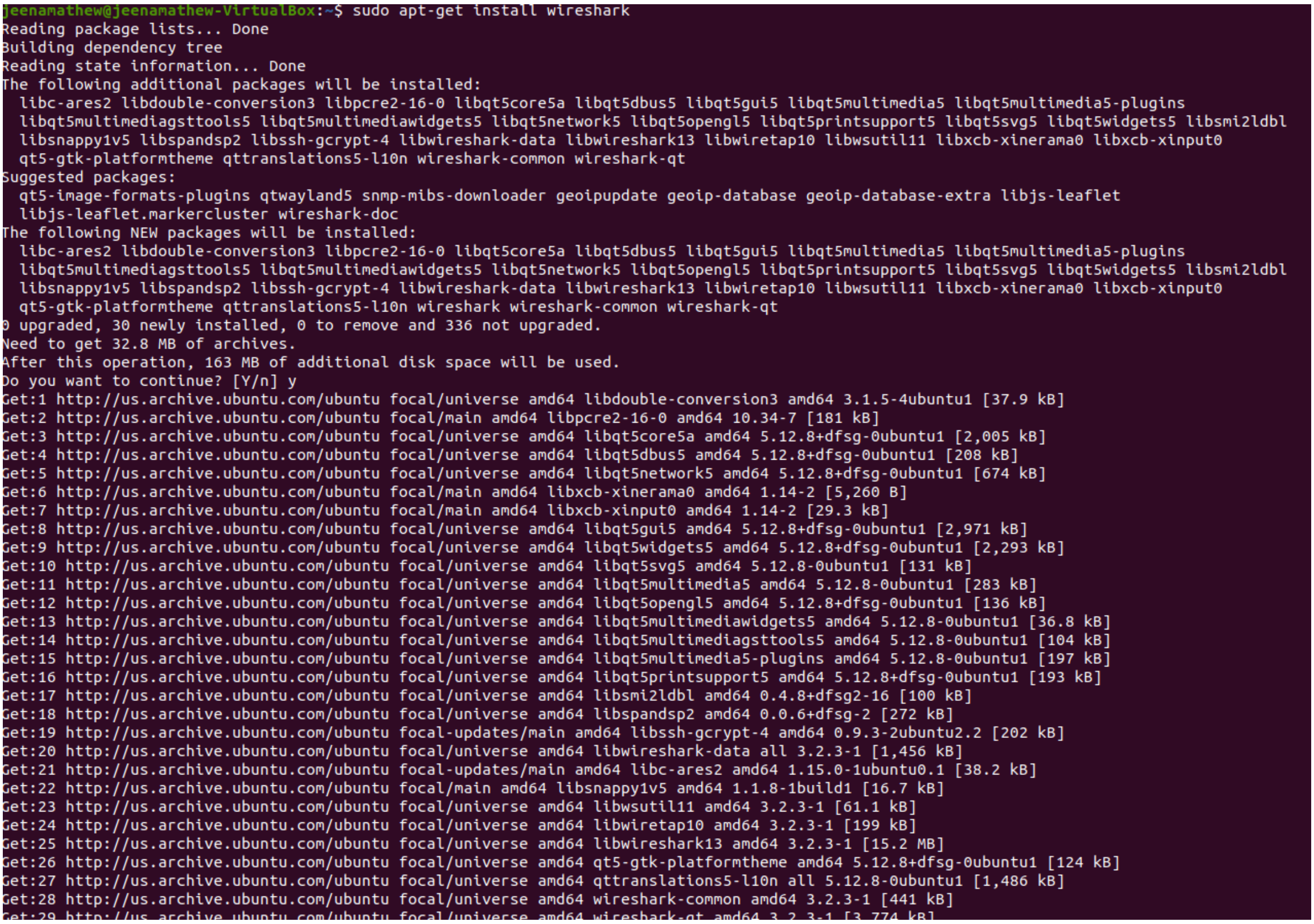
Submitted By:

Jeena Mathew

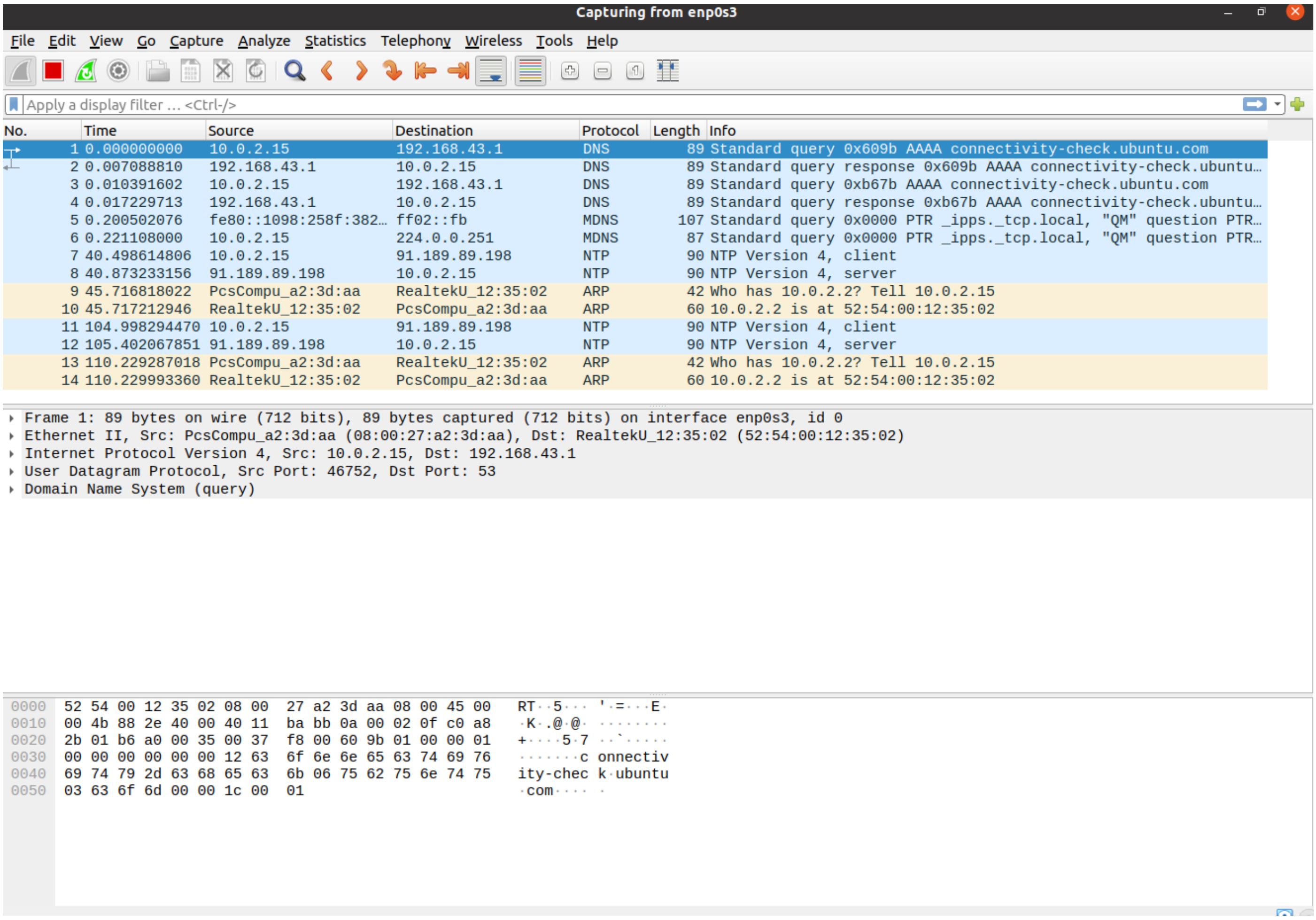
Rollno:42

S2RMCA_A

Installation of wireshark



```
jeenamathew@jeenamathew-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
  libsnappy1v5 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
  libsnappy1v5 libspandsp2 libssh-gcrypt-4 libwireshark-data libwireshark13 libwiretap10 libwsutil11 libxcb-xinerama0 libxcb-xinput0
  qt5-gtk-platformtheme qttranslations5-l10n wireshark wireshark-common wireshark-qt
0 upgraded, 30 newly installed, 0 to remove and 336 not upgraded.
Need to get 32.8 MB of archives.
After this operation, 163 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 libdouble-conversion3 amd64 3.1.5-4ubuntu1 [37.9 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu focal/main amd64 libpcre2-16-0 amd64 10.34-7 [181 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5core5a amd64 5.12.8+dfsg-0ubuntu1 [2,005 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5dbus5 amd64 5.12.8+dfsg-0ubuntu1 [208 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5network5 amd64 5.12.8+dfsg-0ubuntu1 [674 kB]
Get:6 http://us.archive.ubuntu.com/ubuntu focal/main amd64 libxcb-xinerama0 amd64 1.14-2 [5,260 B]
Get:7 http://us.archive.ubuntu.com/ubuntu focal/main amd64 libxcb-xinput0 amd64 1.14-2 [29.3 kB]
Get:8 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5gui5 amd64 5.12.8+dfsg-0ubuntu1 [2,971 kB]
Get:9 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5widgets5 amd64 5.12.8+dfsg-0ubuntu1 [2,293 kB]
Get:10 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5svg5 amd64 5.12.8-0ubuntu1 [131 kB]
Get:11 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5multimedia5 amd64 5.12.8-0ubuntu1 [283 kB]
Get:12 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5opengl5 amd64 5.12.8+dfsg-0ubuntu1 [136 kB]
Get:13 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5multimediawidgets5 amd64 5.12.8-0ubuntu1 [36.8 kB]
Get:14 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5multimediagsttools5 amd64 5.12.8-0ubuntu1 [104 kB]
Get:15 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5multimedia5-plugins amd64 5.12.8-0ubuntu1 [197 kB]
Get:16 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5printsupport5 amd64 5.12.8+dfsg-0ubuntu1 [193 kB]
Get:17 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 libsmi2ldbl amd64 0.4.8+dfsg2-16 [100 kB]
Get:18 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 libspandsp2 amd64 0.0.6+dfsg-2 [272 kB]
Get:19 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 libssh-gcrypt-4 amd64 0.9.3-2ubuntu2.2 [202 kB]
Get:20 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 libwireshark-data all 3.2.3-1 [1,456 kB]
Get:21 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 libc-ares2 amd64 1.15.0-1ubuntu0.1 [38.2 kB]
Get:22 http://us.archive.ubuntu.com/ubuntu focal/main amd64 libsnappy1v5 amd64 1.1.8-1build1 [16.7 kB]
Get:23 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 libwsutil11 amd64 3.2.3-1 [61.1 kB]
Get:24 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 libwiretap10 amd64 3.2.3-1 [199 kB]
Get:25 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 libwireshark13 amd64 3.2.3-1 [15.2 MB]
Get:26 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 qt5-gtk-platformtheme amd64 5.12.8+dfsg-0ubuntu1 [124 kB]
Get:27 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 qttranslations5-l10n all 5.12.8-0ubuntu1 [1,486 kB]
Get:28 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 wireshark-common amd64 3.2.3-1 [441 kB]
Get:29 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 wireshark-qt amd64 3.2.3-1 [3,774 kB]
```

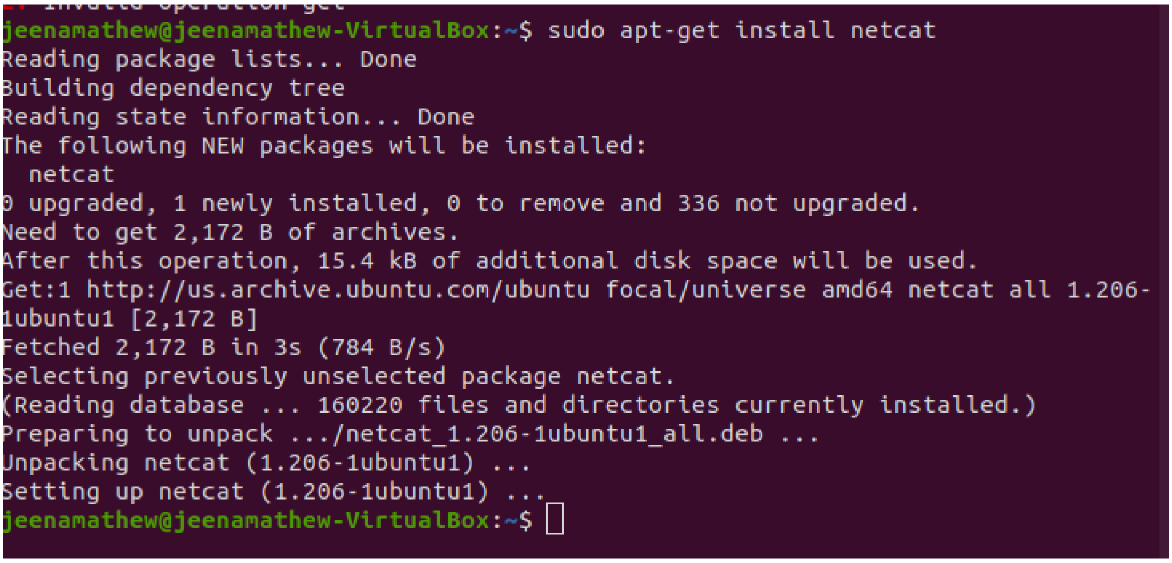


Capturing from enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

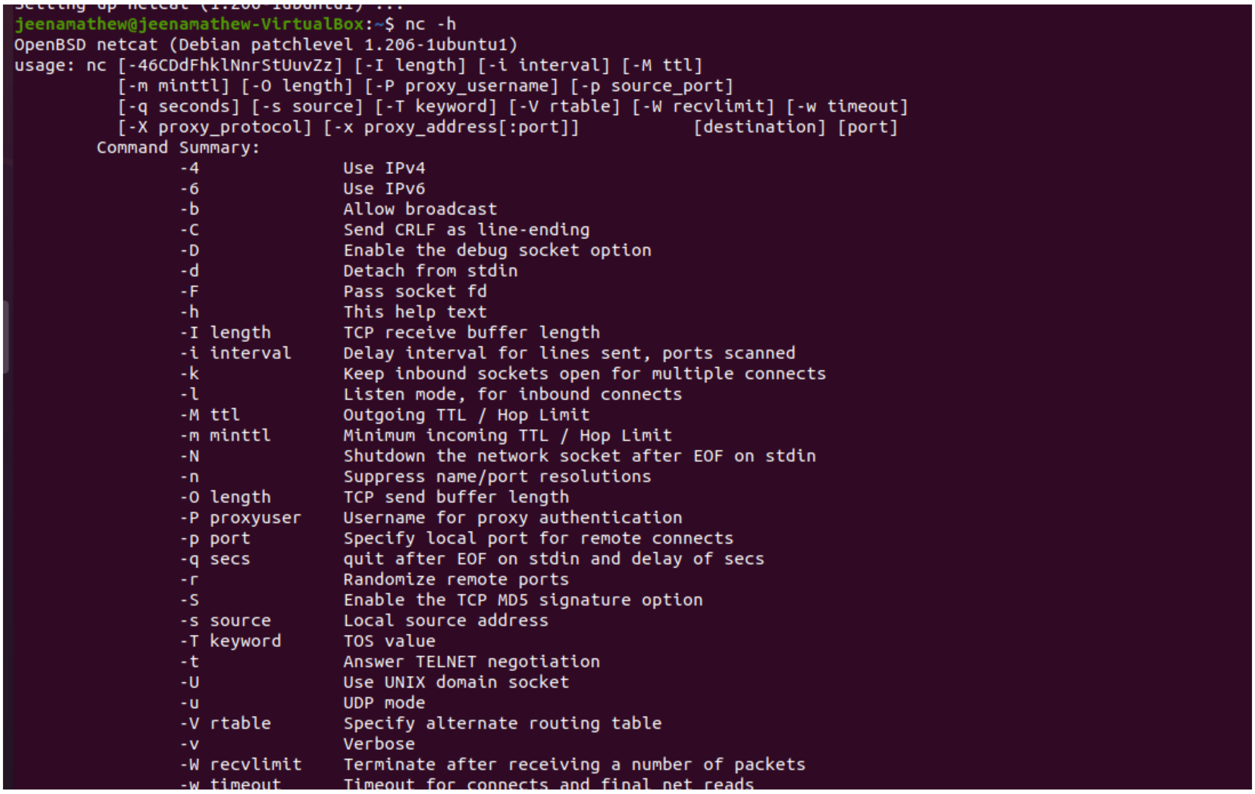
```
No.   Time            Source                  Destination       Protocol  Length Info
    1 0.000000000     10.0.2.15               192.168.43.1      DNS          89 Standard query 0x609b AAAA connectivity-check.ubuntu.com
    2 0.007088810     192.168.43.1            10.0.2.15         DNS          89 Standard query response 0x609b AAAA connectivity-check.ubuntu…
    3 0.010391602     10.0.2.15               192.168.43.1      DNS          89 Standard query 0xb67b AAAA connectivity-check.ubuntu.com
    4 0.017229713     192.168.43.1            10.0.2.15         DNS          89 Standard query response 0xb67b AAAA connectivity-check.ubuntu…
    5 0.200502076     fe80::1098:258f:382…    ff02::fb          MDNS        107 Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR…
    6 0.221108000     10.0.2.15               224.0.0.251       MDNS         87 Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR…
    7 40.498614806    10.0.2.15               91.189.89.198     NTP          90 NTP Version 4, client
    8 40.873233156    91.189.89.198           10.0.2.15         NTP          90 NTP Version 4, server
    9 45.716818022    PcsCompu_a2:3d:aa       RealtekU_12:35:02 ARP          42 Who has 10.0.2.2? Tell 10.0.2.15
   10 45.717212946    RealtekU_12:35:02       PcsCompu_a2:3d:aa ARP          60 10.0.2.2 is at 52:54:00:12:35:02
   11 104.998294470   10.0.2.15               91.189.89.198     NTP          90 NTP Version 4, client
   12 105.402067851   91.189.89.198           10.0.2.15         NTP          90 NTP Version 4, server
   13 110.229287018   PcsCompu_a2:3d:aa       RealtekU_12:35:02 ARP          42 Who has 10.0.2.2? Tell 10.0.2.15
   14 110.229993360   RealtekU_12:35:02       PcsCompu_a2:3d:aa ARP          60 10.0.2.2 is at 52:54:00:12:35:02
```

```
› Frame 1: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface enp0s3, id 0
› Ethernet II, Src: PcsCompu_a2:3d:aa (08:00:27:a2:3d:aa), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.43.1
› User Datagram Protocol, Src Port: 46752, Dst Port: 53
› Domain Name System (query)
```

```
0000  52 54 00 12 35 02 08 00  27 a2 3d aa 08 00 45 00   RT··5··· '·=···E·
0010  00 4b 88 2e 40 00 40 11  ba bb 0a 00 02 0f c0 a8   ·K·.@·@· ········
0020  2b 01 b6 a0 00 35 00 37  f8 00 60 9b 01 00 00 01   +····5·7 ··`·····
0030  00 00 00 00 00 00 12 63  6f 6e 6e 65 63 74 69 76   ·······c onnectiv
0040  69 74 79 2d 63 68 65 63  6b 06 75 62 75 6e 74 75   ity-chec k·ubuntu
0050  03 63 6f 6d 00 00 1c 00  01                        ·com···· ·
```



```
E: Invalid operation get
jeenamathew@jeenamathew-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 336 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://us.archive.ubuntu.com/ubuntu focal/universe amd64 netcat all 1.206-
1ubuntu1 [2,172 B]
Fetched 2,172 B in 3s (784 B/s)
Selecting previously unselected package netcat.
(Reading database ... 160220 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) ...
jeenamathew@jeenamathew-VirtualBox:~$ 
```



```
Setting up netcat (1.206-1ubuntu1) ...
jeenamathew@jeenamathew-VirtualBox:~$ nc -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
```