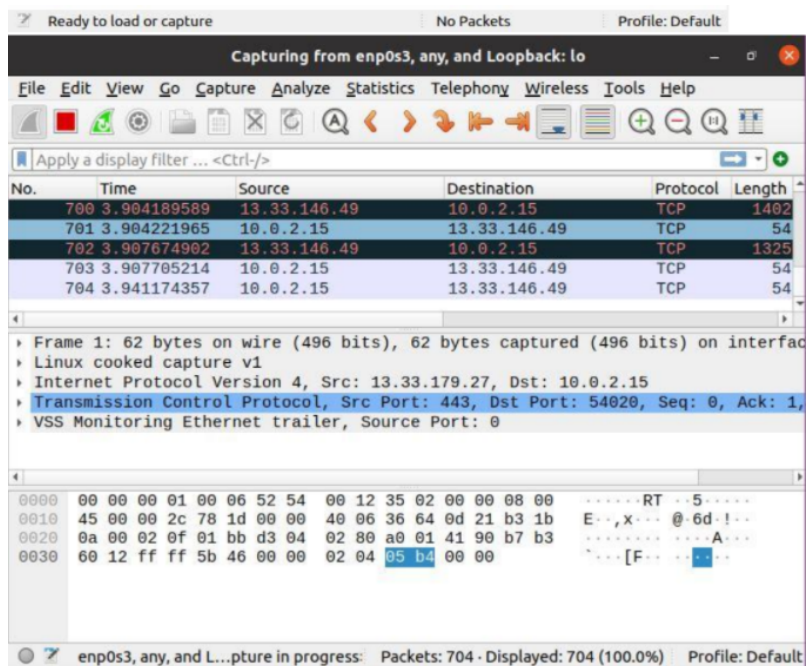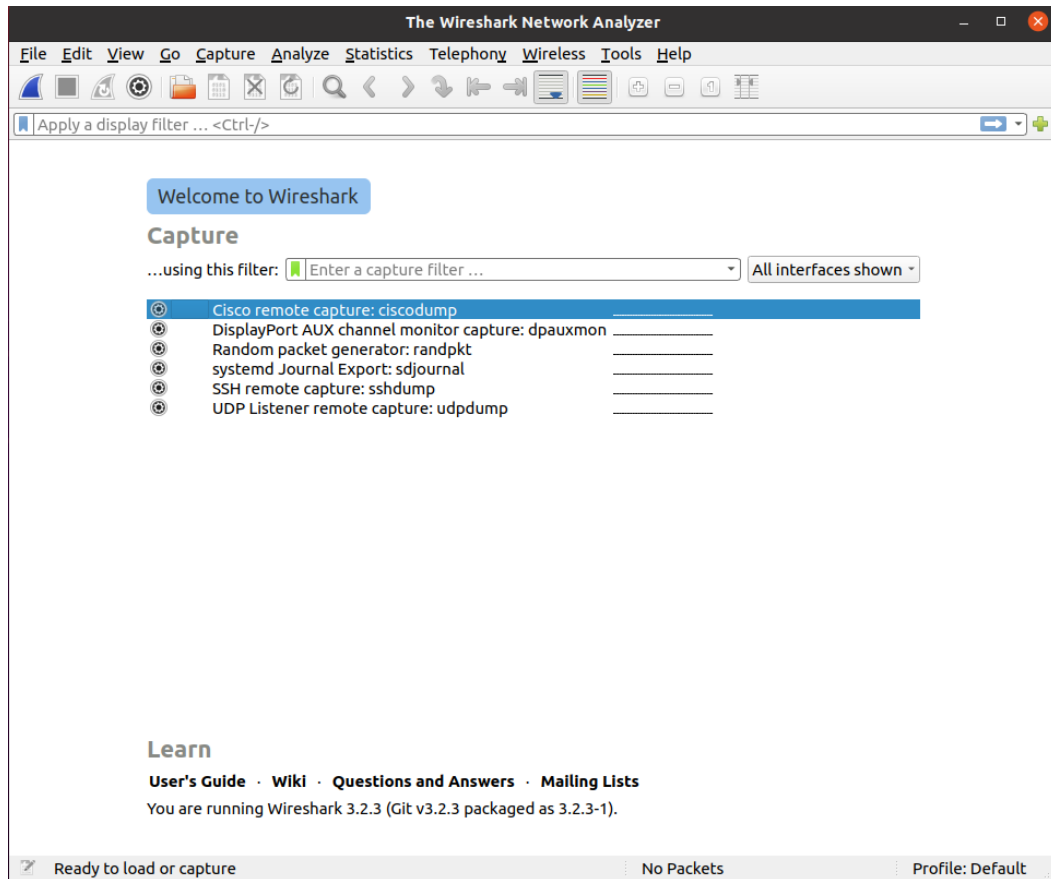Ashish Wilson
S2MCA_A
Roll no:28

Analyzing network packet stream using wireshark. Perform basic network service tests using nc.

sudo apt-get install wireshark

```
ashish@ubuntu:~$ sudo apt-get install wireshark
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libzip5
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  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:
  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 wireshark-common wireshark-qt
0 upgraded, 28 newly installed, 0 to remove and 25 not upgraded.
Need to get 2,190 kB/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 libqt5core5a amd64 5.12.8+dfsg-0ubuntu1 [2,005 kB]
Get:2 http://ppa.launchpad.net/ondrej/php/ubuntu focal/main amd64 libpcre2-16-0 amd64 10.36-2+ubuntu20.04.1+deb.sury.org+2 [184 kB]
Fetched 2,092 kB in 11s (198 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libdouble-conversion3:amd64.
(Reading database ... 215187 files and directories currently installed.)
Preparing to unpack .../00-libdouble-conversion3_3.1.5-4ubuntu1_amd64.deb ...
Unpacking libdouble-conversion3:amd64 (3.1.5-4ubuntu1) ...
Selecting previously unselected package libpcre2-16-0:amd64.
Preparing to unpack .../01-libpcre2-16-0_10.36-2+ubuntu20.04.1+deb.sury.org+2_amd64.deb ...
Unpacking libpcre2-16-0:amd64 (10.36-2+ubuntu20.04.1+deb.sury.org+2) ...
Selecting previously unselected package libqt5core5a:amd64.
Preparing to unpack .../02-libqt5core5a_5.12.8+dfsg-0ubuntu1_amd64.deb ...
Unpacking libqt5core5a:amd64 (5.12.8+dfsg-0ubuntu1) ...
Selecting previously unselected package libqt5dbus5:amd64.
Preparing to unpack .../03-libqt5dbus5_5.12.8+dfsg-0ubuntu1_amd64.deb ...
Unpacking libqt5dbus5:amd64 (5.12.8+dfsg-0ubuntu1) ...
Selecting previously unselected package libqt5network5:amd64.
Preparing to unpack .../04-libqt5network5_5.12.8+dfsg-0ubuntu1_amd64.deb ...
Unpacking libqt5network5:amd64 (5.12.8+dfsg-0ubuntu1) ...
Selecting previously unselected package libxcb-xinerama0:amd64.
Preparing to unpack .../05-libxcb-xinerama0_1.14-2_amd64.deb ...
Unpacking libxcb-xinerama0:amd64 (1.14-2) ...
```

sudo dpkg-reconfigure wireshark-common

```
ashish@ubuntu:~$ sudo dpkg-reconfigure wireshark-common
ashish@ubuntu:~$
```

The Wireshark Network Analyzer

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Welcome to Wireshark

Capture

...using this filter: Enter a capture filter ...   All interfaces shown

⊙	Cisco remote capture: ciscodump
⊙	DisplayPort AUX channel monitor capture: dpauxmon
⊙	Random packet generator: randpkt
⊙	systemd Journal Export: sdjournal
⊙	SSH remote capture: sshdump
⊙	UDP Listener remote capture: udpdump

Learn

User's Guide · **Wiki** · **Questions and Answers** · **Mailing Lists**
You are running Wireshark 3.2.3 (Git v3.2.3 packaged as 3.2.3-1).

Ready to load or capture   No Packets   Profile: Default

Ready to load or capture   No Packets   Profile: Default

Capturing from enp0s3, any, and Loopback: lo

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length
700	3.904189589	13.33.146.49	10.0.2.15	TCP	1402
701	3.904221965	10.0.2.15	13.33.146.49	TCP	54
702	3.907674902	13.33.146.49	10.0.2.15	TCP	1325
703	3.907705214	10.0.2.15	13.33.146.49	TCP	54
704	3.941174357	10.0.2.15	13.33.146.49	TCP	54

> Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interfac
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 13.33.179.27, Dst: 10.0.2.15
> Transmission Control Protocol, Src Port: 443, Dst Port: 54020, Seq: 0, Ack: 1,
> VSS Monitoring Ethernet trailer, Source Port: 0

```
0000  00 00 00 01 00 06 52 54  00 12 35 02 00 00 08 00   ······RT ··5·····
0010  45 00 00 2c 78 1d 00 00  40 06 36 64 0d 21 b3 1b   E··,x··· @·6d·!··
0020  0a 00 02 0f 01 bb d3 04  02 80 a0 01 41 90 b7 b3   ········ ····A···
0030  60 12 ff ff 5b 46 00 00  02 04 05 b4 00 00         `···[F·· ······
```

enp0s3, any, and L...pture in progress: Packets: 704 · Displayed: 704 (100.0%) Profile: Default

nc -z -v 10.0.2.15 20-80

```
ashish@ubuntu:~$ nc -z -v 10.0.2.15 20-80
nc: connect to 10.0.2.15 port 20 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 21 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 22 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 23 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 24 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 25 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 26 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 27 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 28 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 29 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 30 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 31 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 32 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 33 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 34 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 35 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 36 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 37 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 38 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 39 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 40 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 41 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 42 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 43 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 44 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 45 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 46 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 47 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 48 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 49 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 50 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 51 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 52 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 53 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 54 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 55 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 56 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 57 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 58 (tcp) failed: Connection refused
nc: connect to 10.0.2.15 port 59 (tcp) failed: Connection refused
```