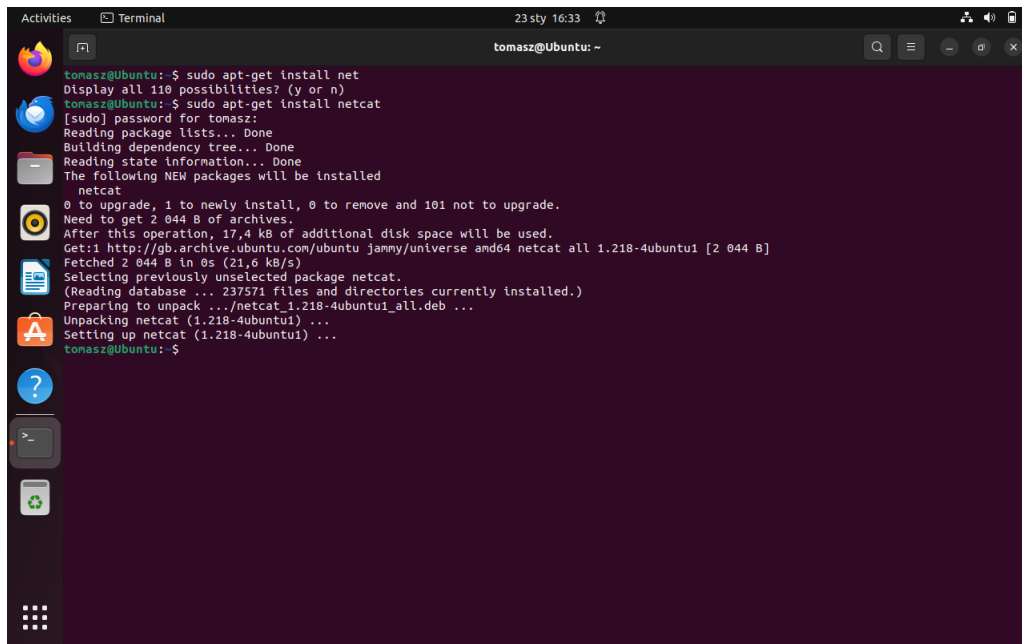


1 Tools

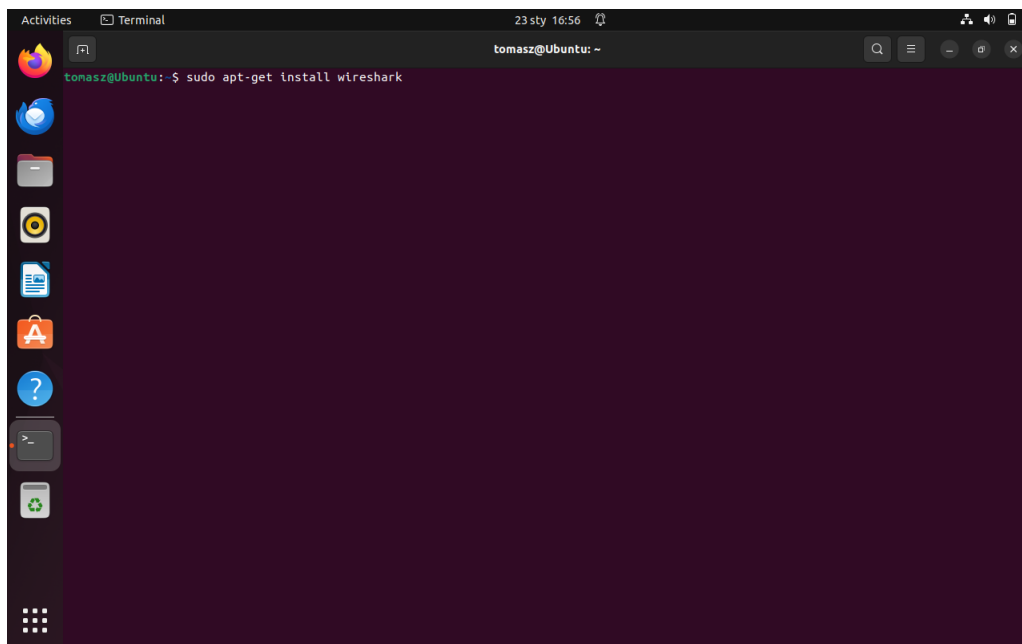
1.1 Install netcat



```
Activities Terminal 23 sty 16:33 tomasz@Ubuntu: ~
tomasz@Ubuntu:~$ sudo apt-get install net
Display all 110 possibilities? (y or n)
tomasz@Ubuntu:~$ sudo apt-get install netcat
[sudo] password for tomasz:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed
  netcat
0 to upgrade, 1 to newly install, 0 to remove and 101 not to upgrade.
Need to get 2 044 B of archives.
After this operation, 17,4 kB of additional disk space will be used.
Get:1 http://gb.archive.ubuntu.com/ubuntu jammy/universe amd64 netcat all 1.218-4ubuntu1 [2 044 B]
Fetched 2 044 B in 0s (21,6 kB/s)
Selecting previously unselected package netcat.
(Reading database ... 237571 files and directories currently installed.)
Preparing to unpack .../netcat_1.218-4ubuntu1_all.deb ...
Unpacking netcat (1.218-4ubuntu1) ...
Setting up netcat (1.218-4ubuntu1) ...
tomasz@Ubuntu:~$
```

Figure 1: Install netcat

1.2 Install Wireshark



```
Activities Terminal 23 sty 16:56 tomasz@Ubuntu: ~
tomasz@Ubuntu:~$ sudo apt-get install wireshark
```

Figure 2: Install Wireshark

2 Traffic investigation

2.1 Wireshark

According to task, all the traffic should be captured with use of Wireshark.

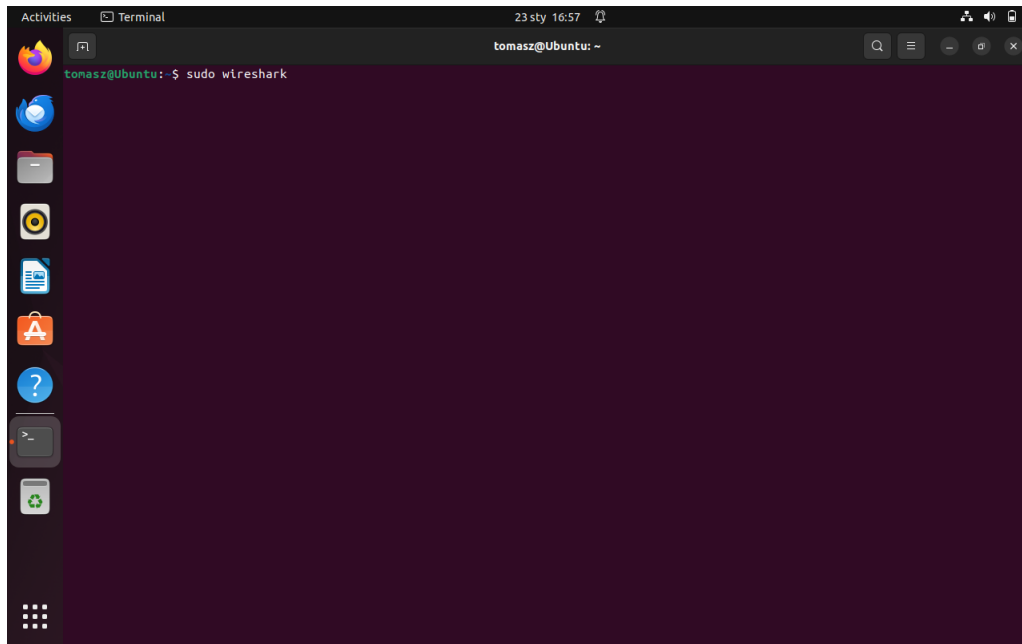


Figure 3: Starting Wireshark

2.2 TCP Server

With netcat, a new tcp server listening on port 27664 has been started.

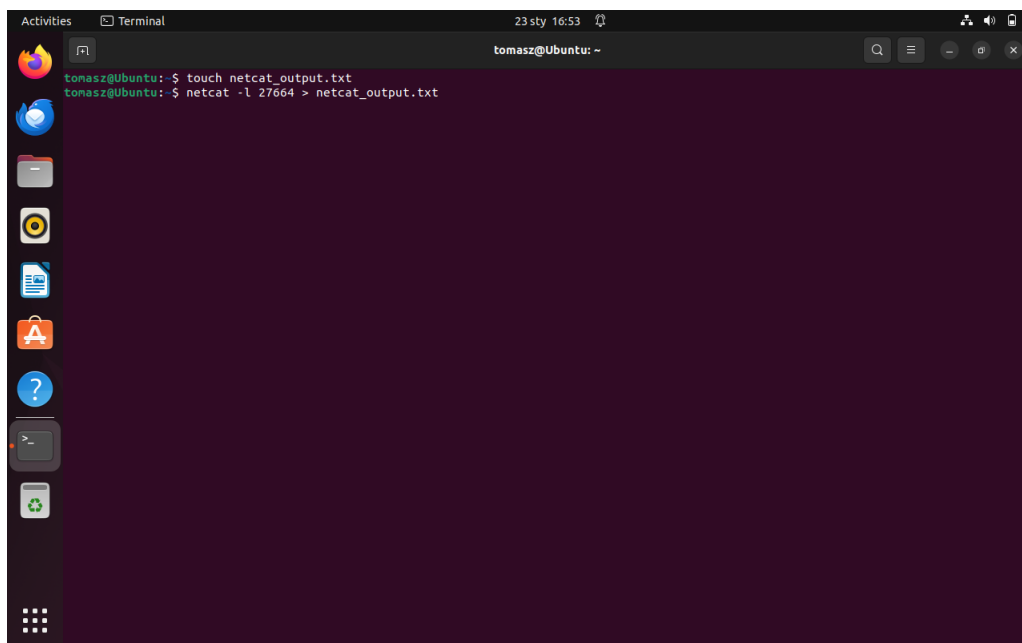


Figure 4: Starting TCP server on port 27664. All incoming messages are piped to file netcat_output.txt

2.3 Connecting to port 27664 via telnet

On separate command terminal, a connection to port 27664 has been established.

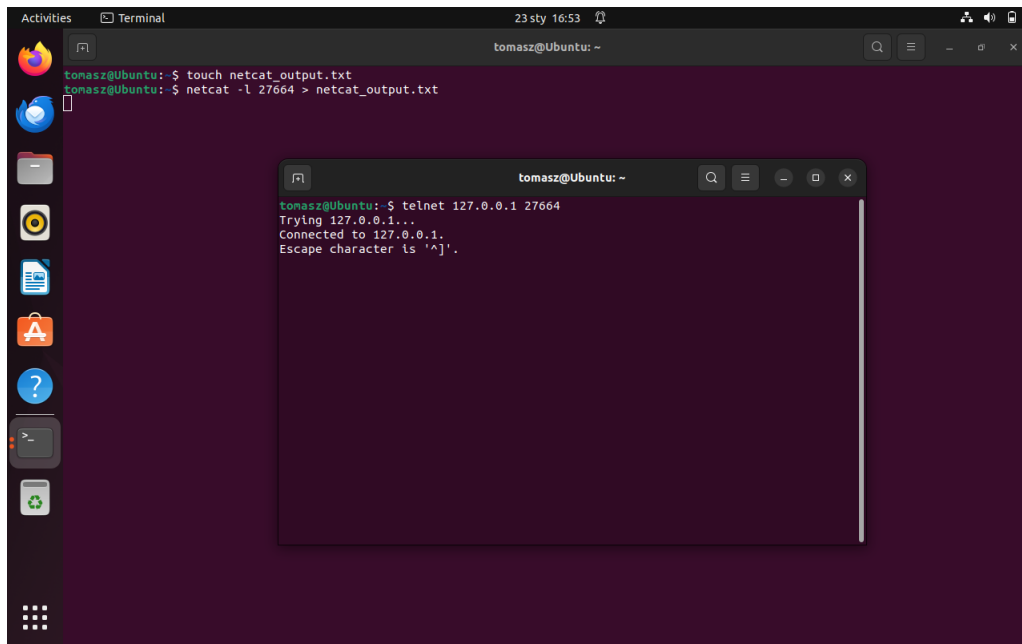


Figure 5: Starting telnet connection

2.4 Redirecting output

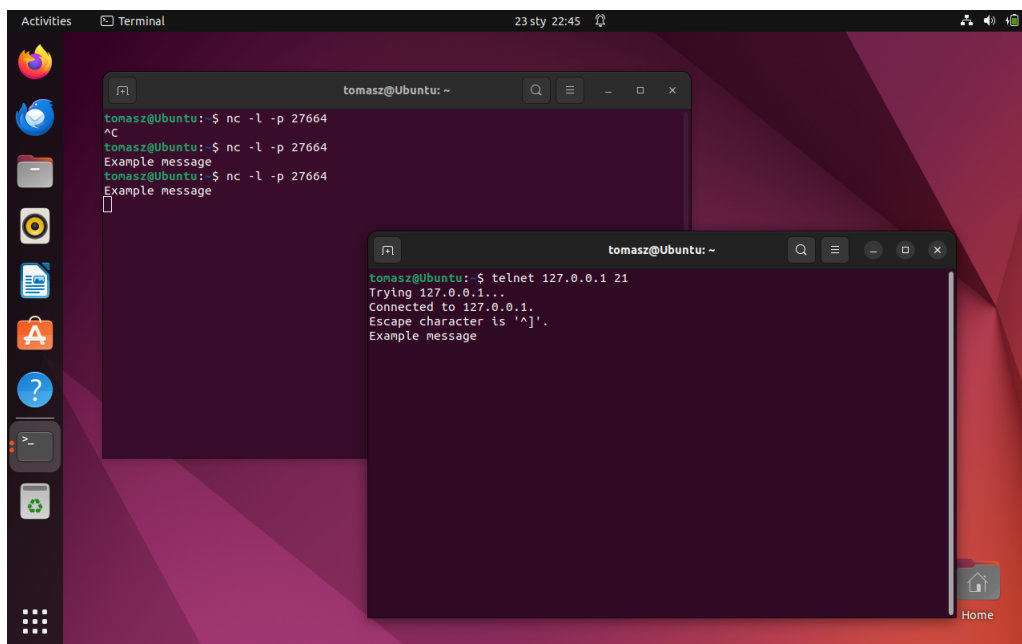


Figure 6: Redirecting output from 21th port to port 27644

3 Output

After connection close, a traffic capture on Wireshark has been stopped. (All traffic has been captured)

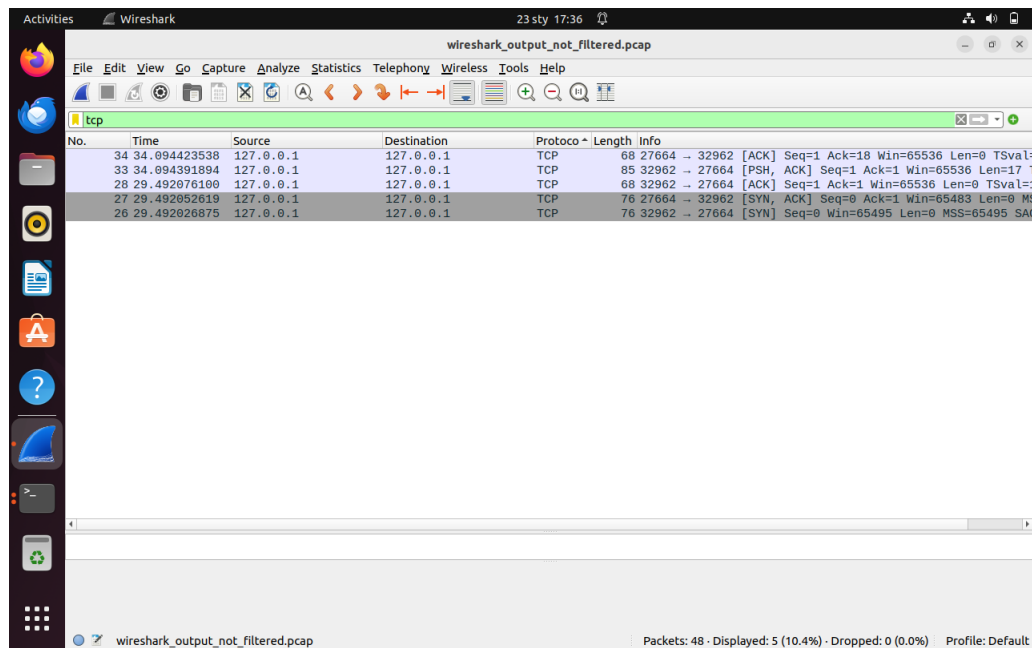


Figure 7: Filtered Wireshark output

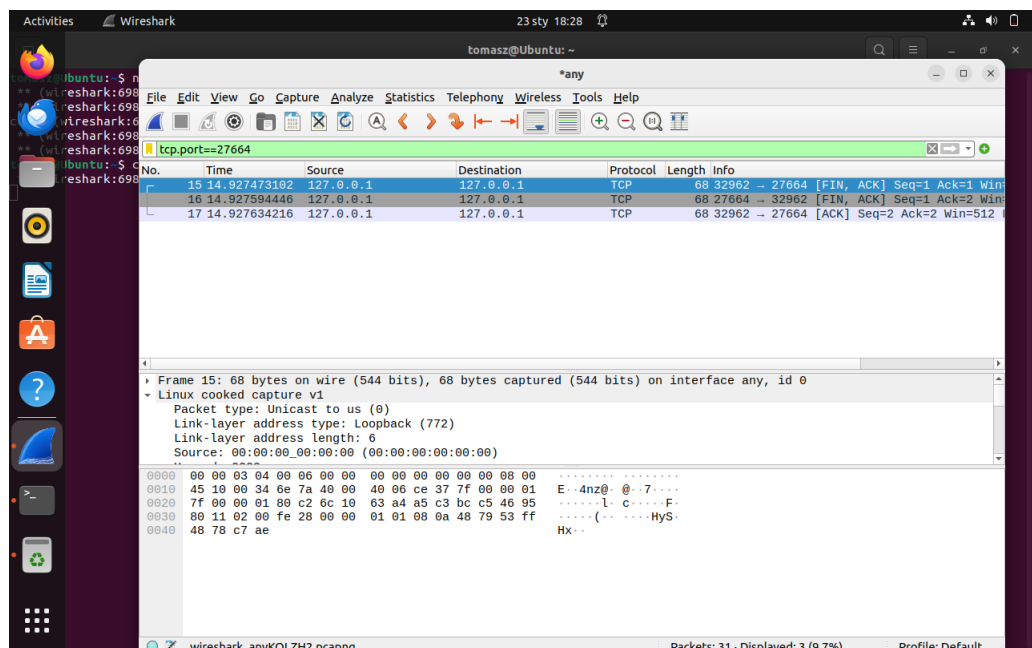


Figure 8: Filtered Wireshark output, end

3.1 Output analysis

- From telnet port (32962) a packet with SYN flag is sent to destination port (27664)
- Server on port 27664 answers with packet with flags SYN and ACK (confirmng reception of initial packet)
- From telnet port a acknowledgment of received packet has been send.
- Sender (telnet port) sends a packet with PSH requesting immediate data delivery to host. Inside the packet is message "Example message"

- Server sends acknowledgment of receiving packet with data
- At the end message with FIN and ACK flags are send

3.2 Output with redirecting

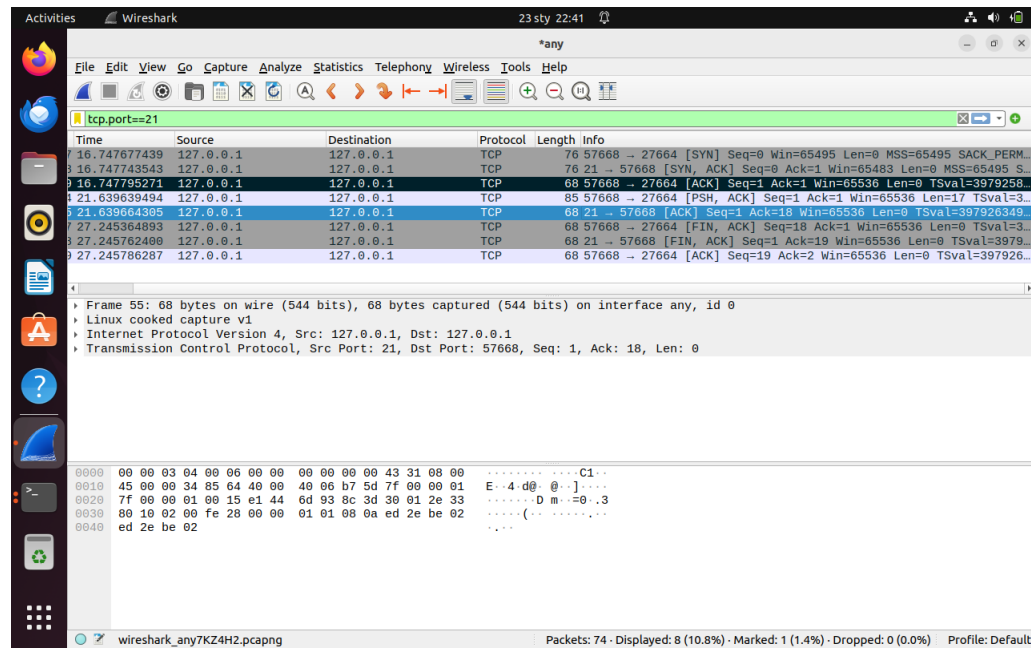


Figure 9: Filtered output of wireshark with port redirection