# 1 Tools

## 1.1 Install netcat

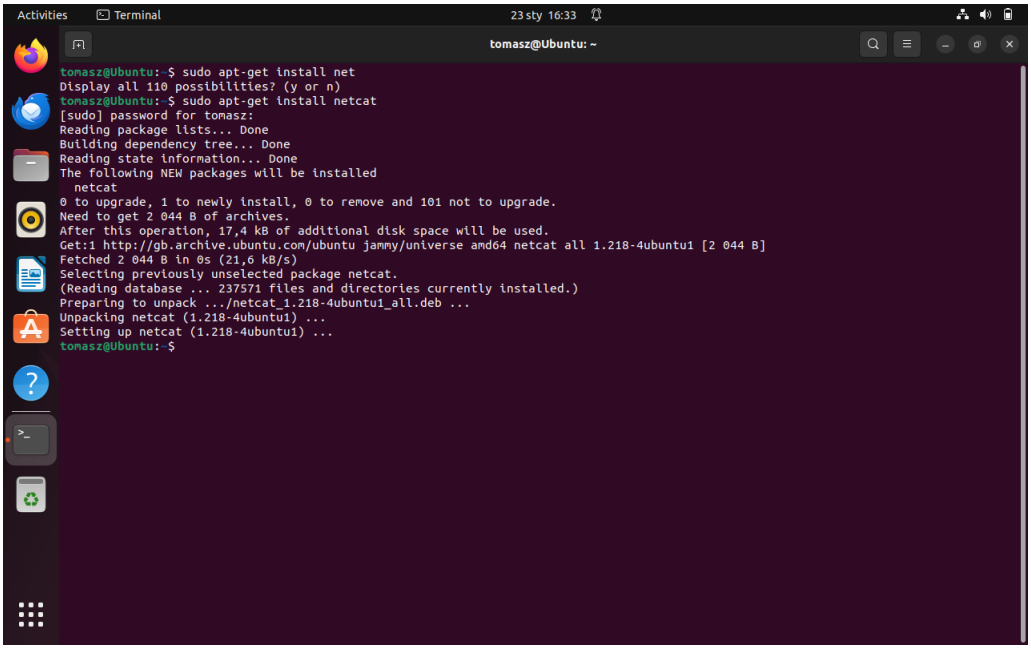


Figure 1: Install netcat

## 1.2 Install Wireshark

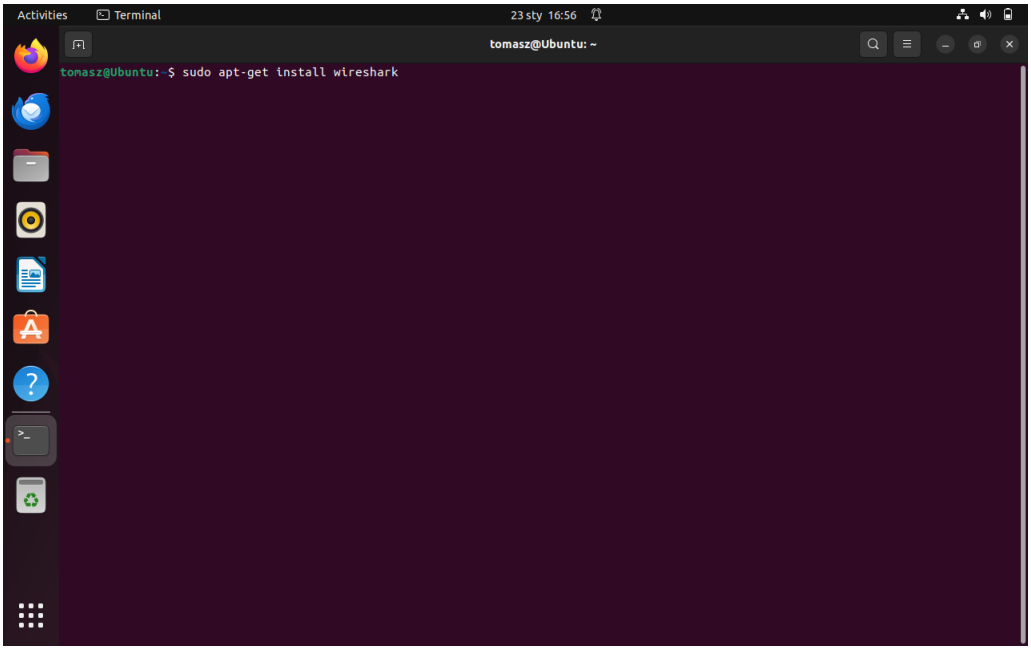


Figure 2: Install Wireshark

# 2 Traffic investigation

## 2.1 Wireshark

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

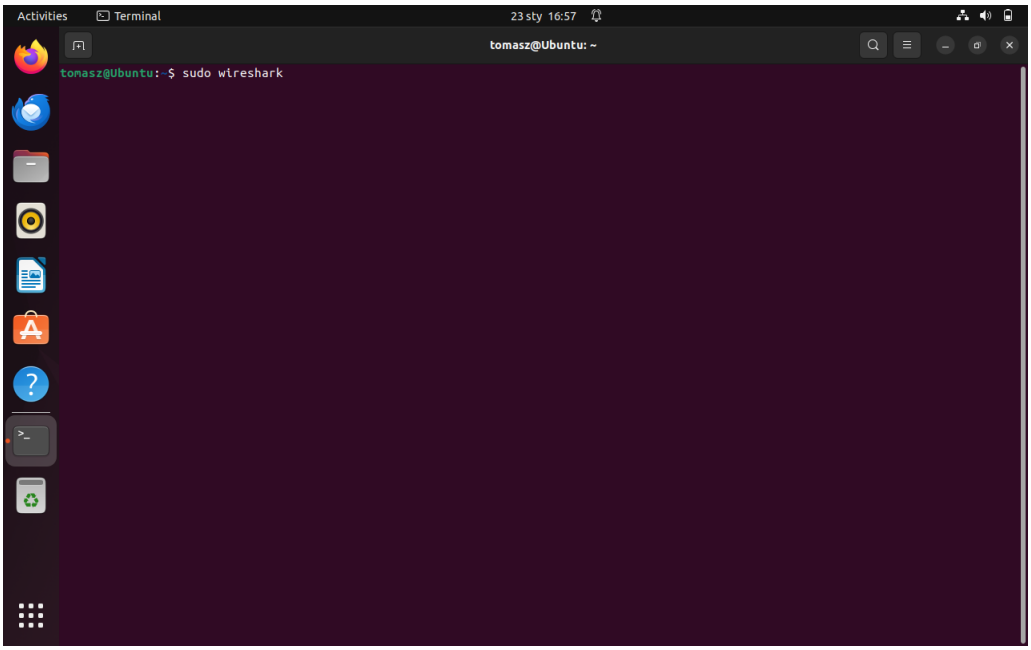


Figure 3: Starting Wireshark

## 2.2 TCP Server

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

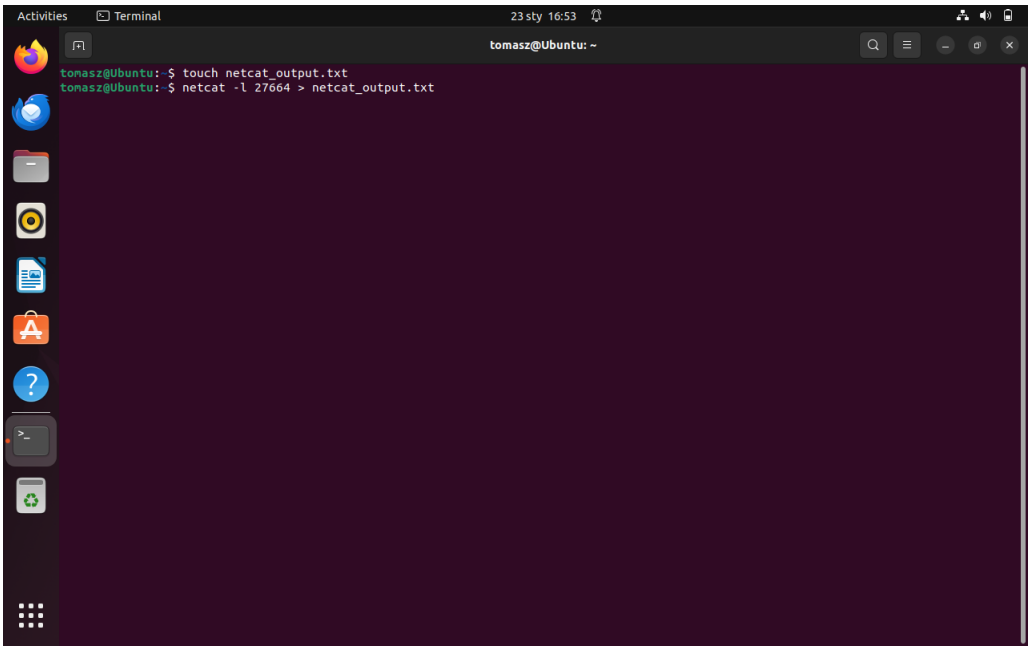


Figure 4: Starting TCP server on port 27664. All incoming messages are piped to file netcat_output.txt

## 2.3 Connecting to port 27664 via telnet

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

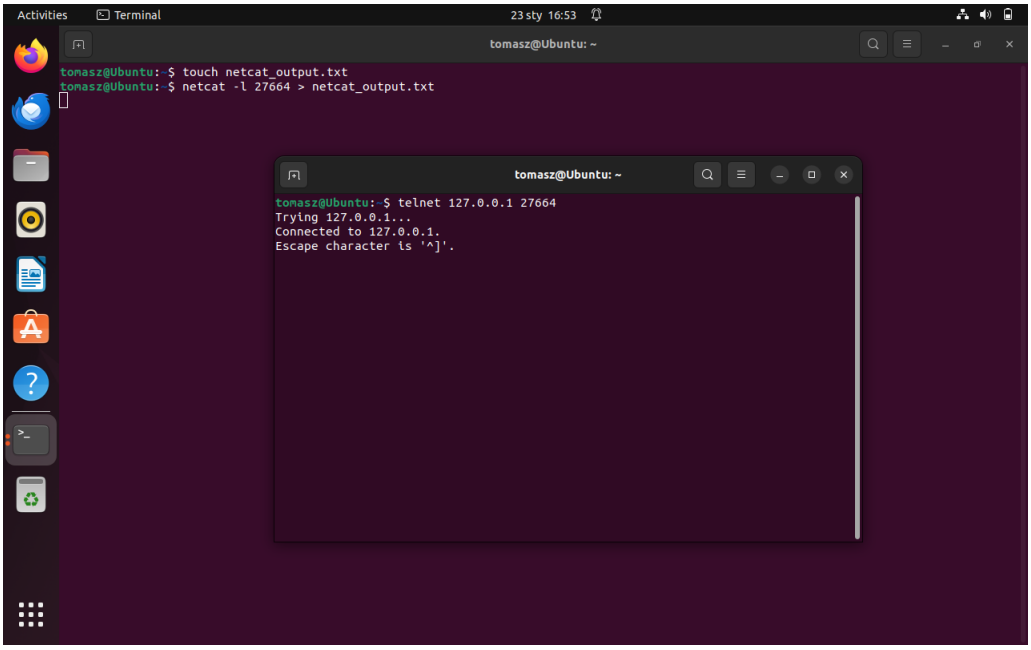


Figure 5: Starting telnet connection

## 2.4 Redirecting output

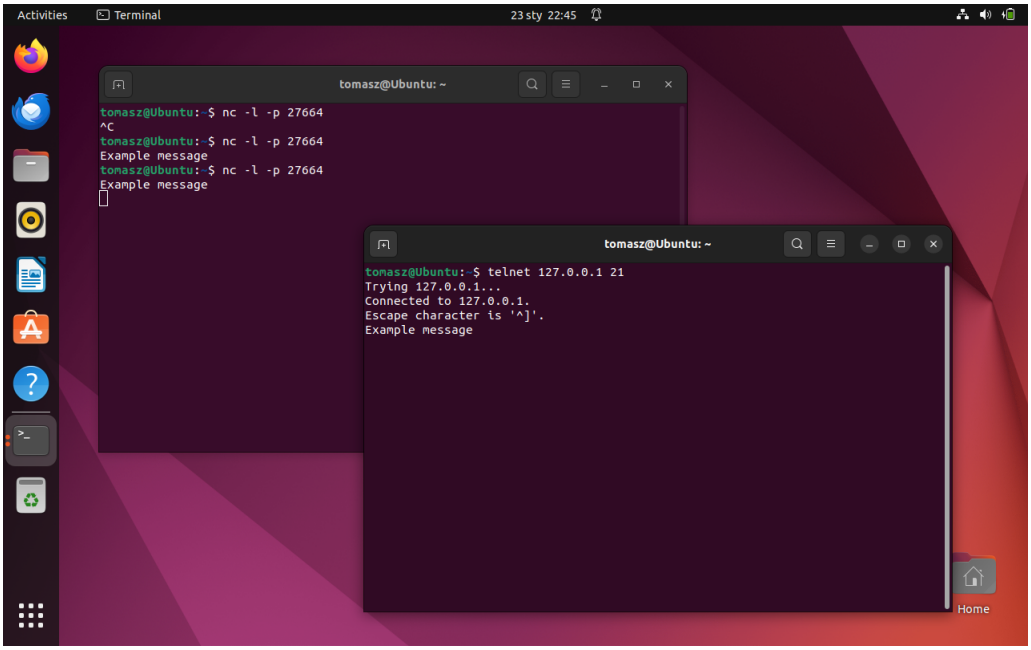


Figure 6: Redirecting output from 21th port to port 27644

# 3 Output

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

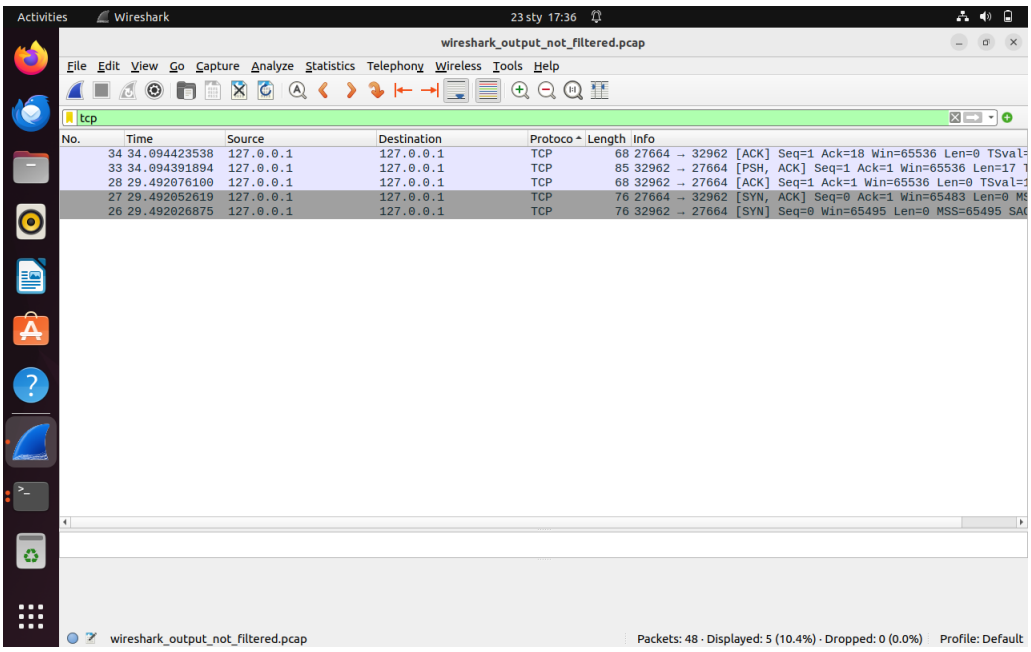


Figure 7: Filtered Wireshark output

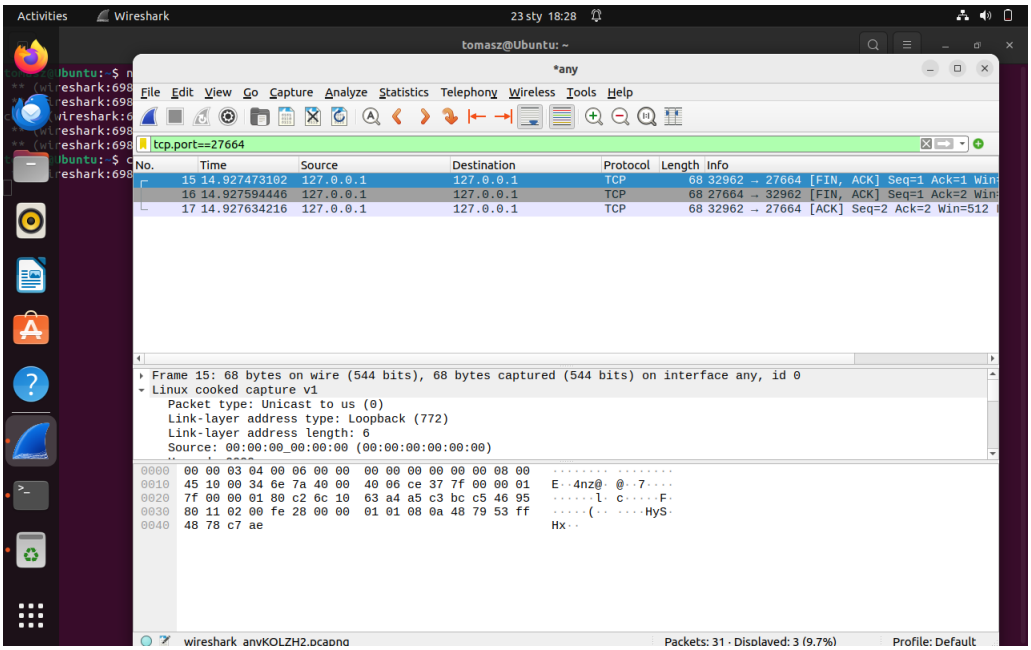


Figure 8: Filtered Wireshark output, end

## 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 receing packet with data
- At the end message with FIN and ACK flags are send

## 3.2 Output with redirecting

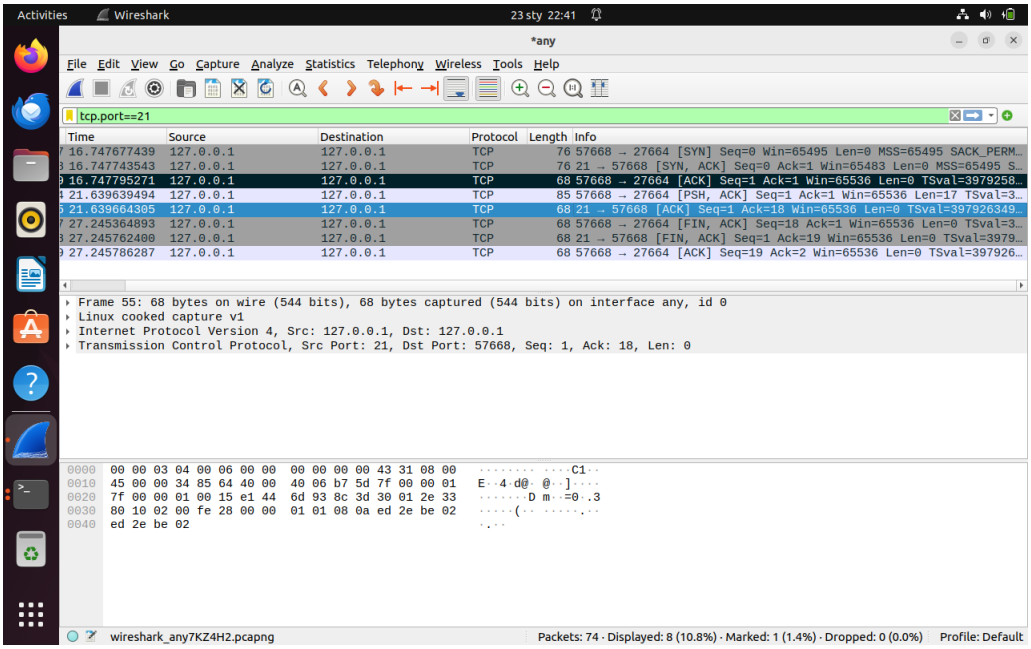


Figure 9: Filtered output of wireshark with port redirection