Network Traffic Analysis with Wireshark

Created by Hasan Williams

Overview:

In this project, I set up and used Wireshark to capture and analyze network traffic on a virtual machine. The process involved updating the system, installing Wireshark, configuring it, and performing a detailed analysis of network traffic.

Process:

System Update and Wireshark Installation

System Update

- **Command**: `sudo apt update`
- **Purpose**: I used this command to refresh package lists for upgrades and new installations.

Wireshark Installation

- **Command**: `sudo apt install wireshark`
- **Result**: After running the command, I confirmed that Wireshark was updated to the newest version.

Launching Wireshark

- **Command**: `wireshark`
- **Purpose**: This command allowed me to start the Wireshark application.

Wireshark Configuration and Packet Capture

Configuration

- **Capture Options**: I selected `enp0s3` as the network interface for capturing traffic.
- **Promiscuous Mode**: I enabled this option to capture all packets on the network.

Permission Configuration

- **Reconfiguration**: I ran `sudo dpkg-reconfigure wireshark-common` to allow non-superusers, including myself, to capture packets.
- **User Group**: I added my user to the "wireshark" group using the command `sudo usermod -a -G wireshark hasan`.
- **New Group Session**: To apply the changes, I used the `newgrp wireshark` command.

Packet Capture and Analysis

Capture Start

- I initiated packet capture on the `enp0s3` interface.

Filter Usage

- I applied filters like `http`, `ip.addr`, and `tcp.port` to focus on specific types of traffic.

Packet Inspection

- I analyzed protocols such as TCP and ICMP in detail.

Statistics and Conversations

- **Protocol Hierarchy**: I reviewed the distribution of protocols in the traffic.
- **Conversations and Endpoints**: I examined the communication between different network devices.

Technologies and Tools Used

- **Ubuntu**: I used this operating system for the virtual machine.
- **Wireshark**: This was my primary tool for analyzing network protocols.
- **APT**: I used this for managing software installations.
- **VirtualBox**: I utilized VirtualBox as my virtualization platform.

Key Skills Acquired

- I developed proficiency in configuring Wireshark for packet capture.
- I gained a deeper understanding of network protocols and traffic analysis.
- I learned how to manage Linux user permissions and groups effectively.

Lessons Learned

- I realized the importance of user permissions when performing network analysis.
- I learned how to use Wireshark filters to focus on specific traffic types.
- I became skilled at analyzing traffic to identify communication patterns.

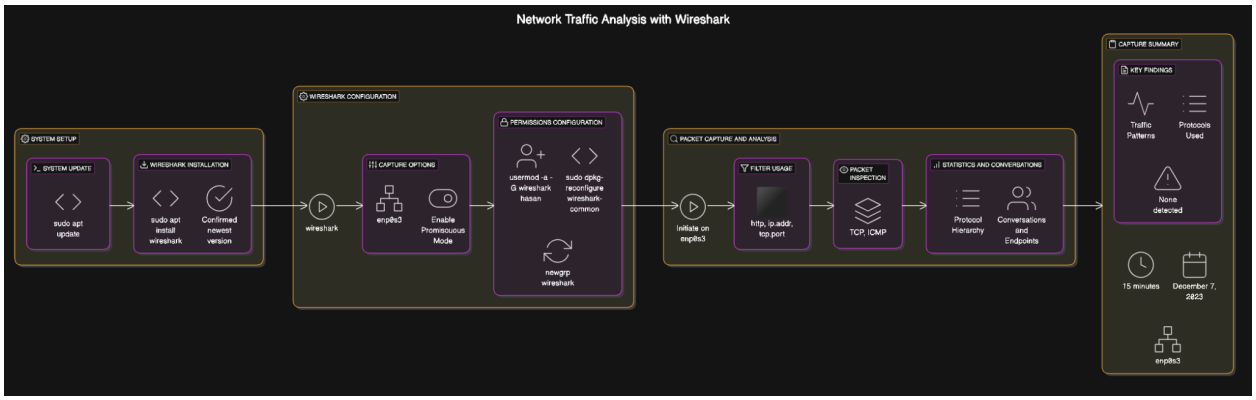
Capture Summary

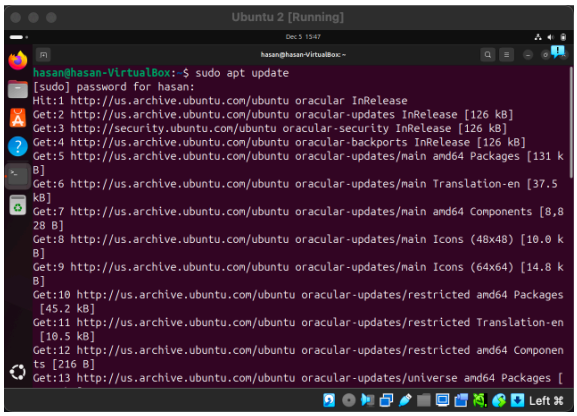
- **Date and Time**: I conducted the capture on December 7, 2023.
- **Duration**: The capture lasted approximately 15 minutes.
- **Network Interface Used**: I used the `enp0s3` network interface.

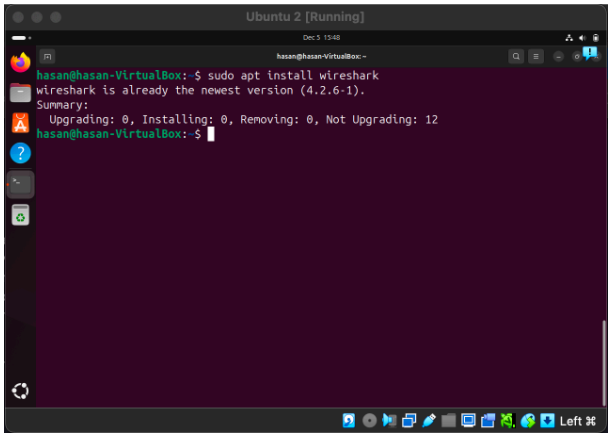
Key Findings

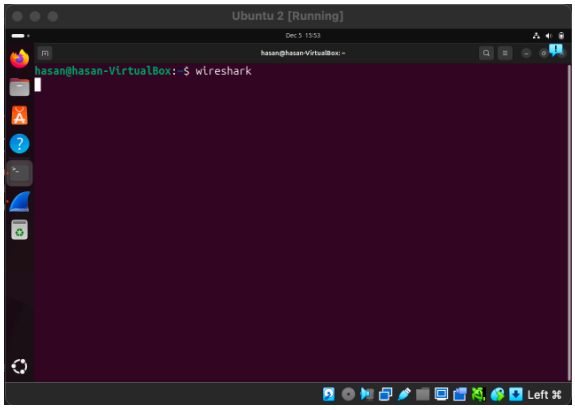
- **Traffic Patterns**: I observed standard query responses and TCP communications.
- **Protocols Used**: There was notable use of ICMPv6, MDNS, and HTTP protocols.
- **Suspicious Activity**: I did not detect any suspicious activity during the capture.

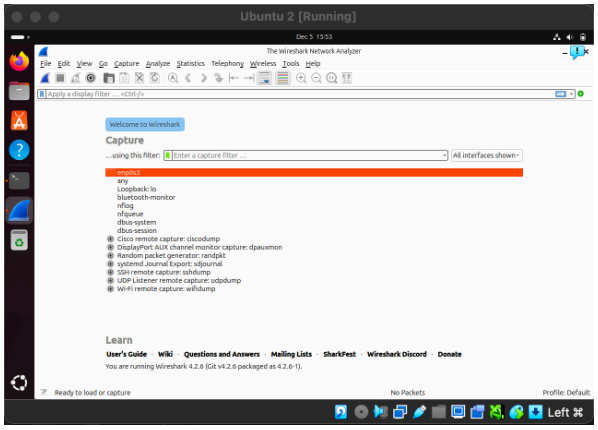
This documentation summarizes my work on network traffic analysis using Wireshark. It highlights the steps I followed, the skills I acquired, and the key findings from my analysis.

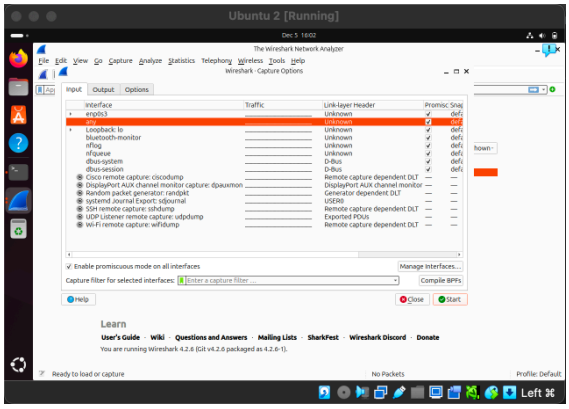


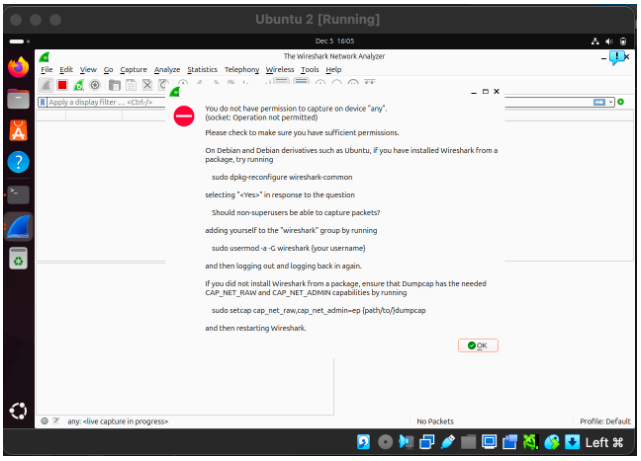


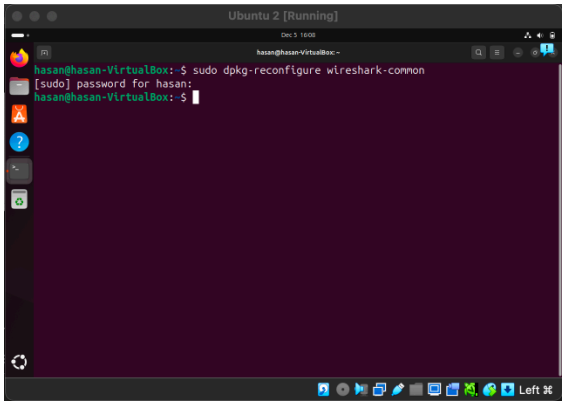


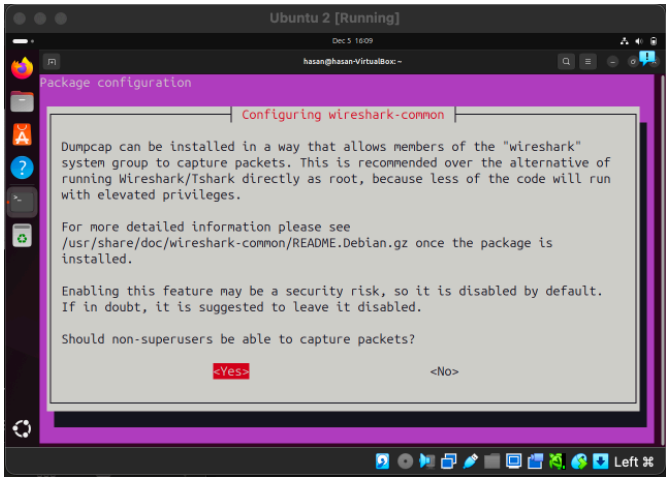


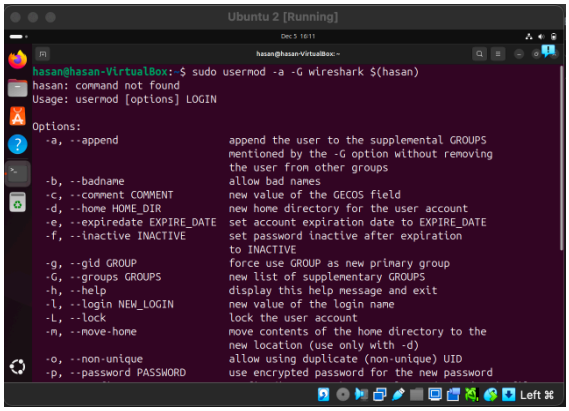


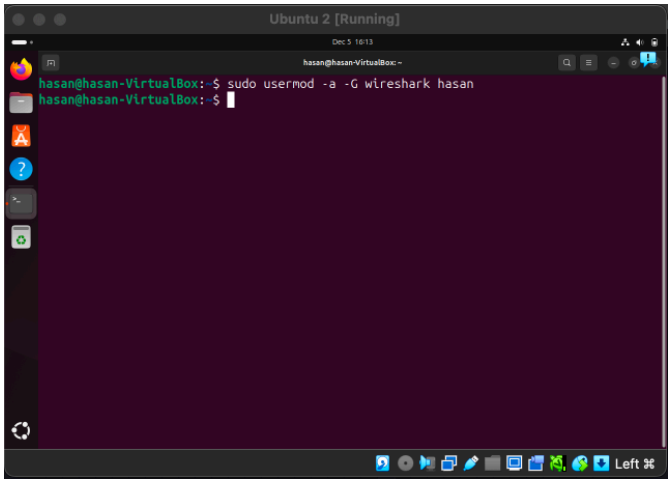

Ubuntu 2 [Running]
The Wireshark Network Analyzer
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

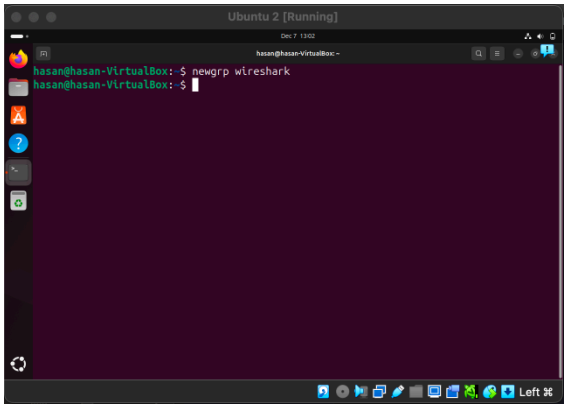

Ubuntu 2 [Running]
The Wireshark Network Analyzer
You do not have permission to capture on device "any".
(socket: Operation not permitted)
Please check to make sure you have sufficient permissions.
On Debian and Debian derivatives such as Ubuntu, if you have installed Wireshark from a package, try running
sudo dpkg-reconfigure wireshark-common
selecting "<Yes>" in response to the question
Should non-superusers be able to capture packets?
adding yourself to the "wireshark" group by running
sudo usermod -a -G wireshark {your username}
and then logging out and logging back in again.
If you did not install Wireshark from a package, ensure that Dumpcap has the needed CAP_NET_RAW and CAP_NET_ADMIN capabilities by running
sudo setcap cap_net_raw,cap_net_admin=ep {path/to}/dumpcap
and then restarting Wireshark.
OK

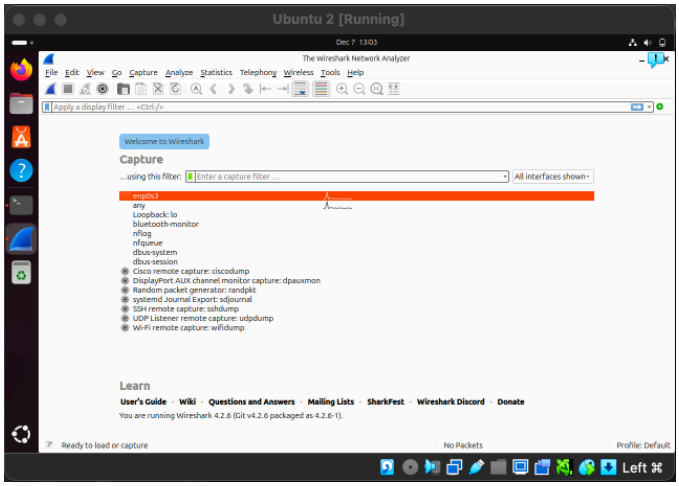

Ubuntu 2 [Running]
hasan@hasan-VirtualBox:~$ sudo dpkg-reconfigure wireshark-common
[sudo] password for hasan:
hasan@hasan-VirtualBox:~$

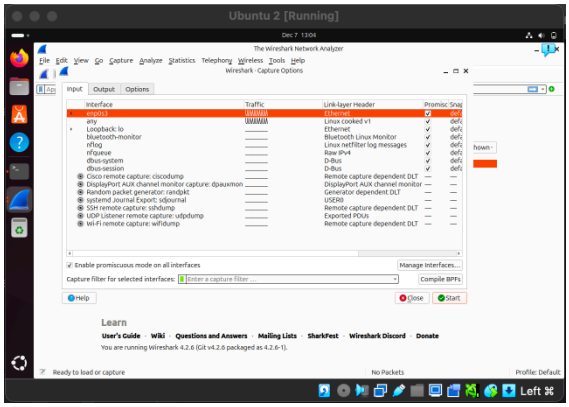

Ubuntu 2 [Running]
Package configuration
Configuring wireshark-common
Dumpcap can be installed in a way that allows members of the "wireshark" system group to capture packets. This is recommended over the alternative of running Wireshark/Tshark directly as root, because less of the code will run with elevated privileges.
For more detailed information please see /usr/share/doc/wireshark-common/README.Debian.gz once the package is installed.
Enabling this feature may be a security risk, so it is disabled by default. If in doubt, it is suggested to leave it disabled.
Should non-superusers be able to capture packets?
<Yes>
<No>

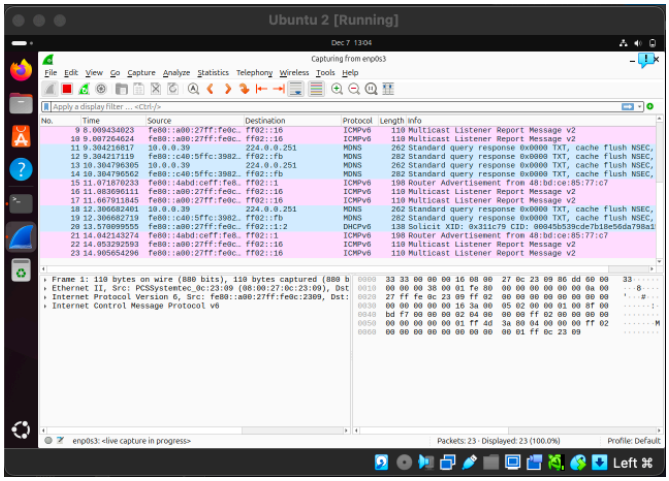

Ubuntu 2 [Running]
hasan@hasan-VirtualBox:~$ sudo usermod -a -G wireshark $(hasan)
hasan: command not found
Usage: usermod [options] LOGIN
Options:
-a, --append append the user to the supplemental GROUPS
-b, --badname allow bad names
-c, --comment COMMENT new value of the GECOS field
-d, --home HOME_DIR new home directory for the user account
-e, --expiredate EXPIRE_DATE set account expiration date to EXPIRE_DATE
-f, --inactive INACTIVE set password inactive after expiration
-g, --gid GROUP force use GROUP as new primary group
-G, --groups GROUPS new list of supplementary GROUPS
-h, --help display this help message and exit
-l, --login NEW_LOGIN new value of the login name
-L, --lock lock the user account
-m, --move-home move contents of the home directory to the
-o, --non-unique allow using duplicate (non-unique) UID
-p, --password PASSWORD use encrypted password for the new password

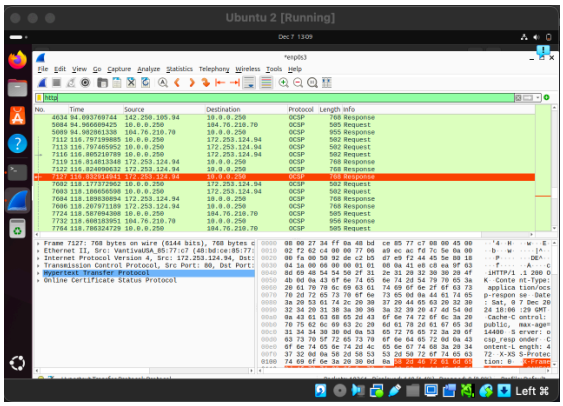

Ubuntu 2 [Running]
hasan@hasan-VirtualBox:~$ sudo usermod -a -G wireshark hasan
hasan@hasan-VirtualBox:~$

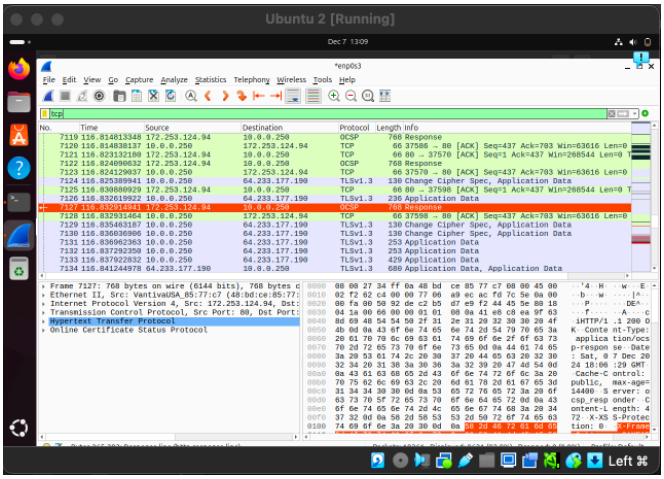

Ubuntu 2 [Running]
hasan@hasan-VirtualBox:~$ newgrp wireshark
hasan@hasan-VirtualBox:~$

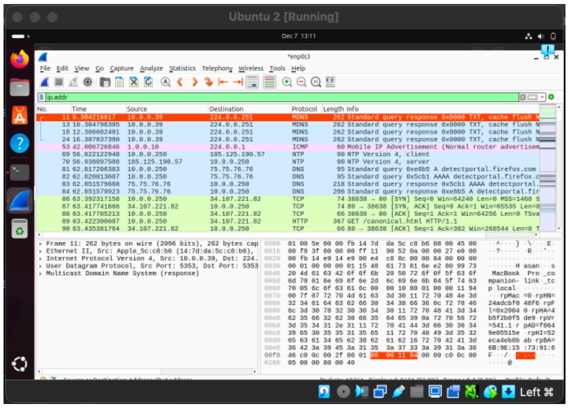

Ubuntu 2 [Running]
The Wireshark Network Analyzer
Welcome to Wireshark
Capture
Learn

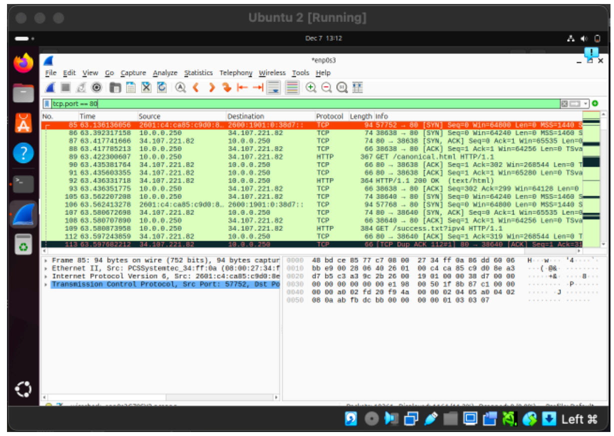

Ubuntu 2 [Running]
Wireshark · Capture Options
Learn

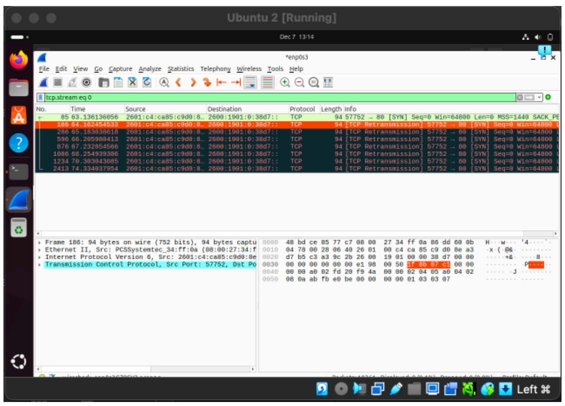

Ubuntu 2 [Running]
Capturing from enp0s3

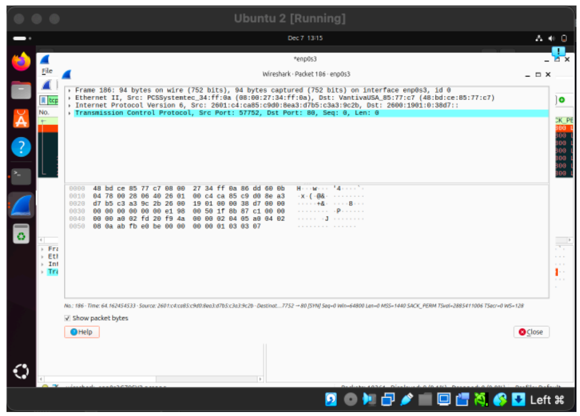

Ubuntu 2 [Running]

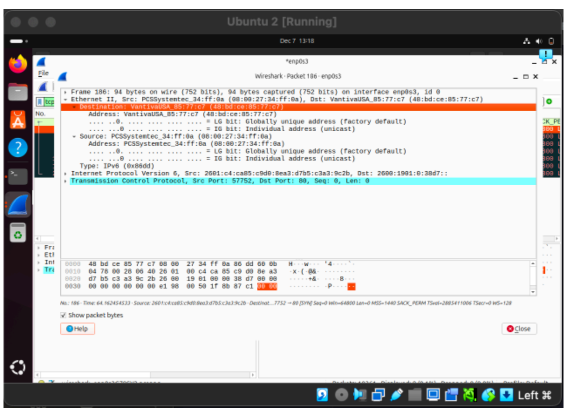

Ubuntu 2 [Running]

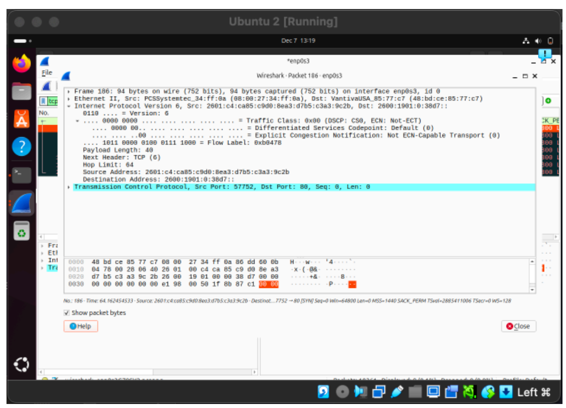

Ubuntu 2 [Running]

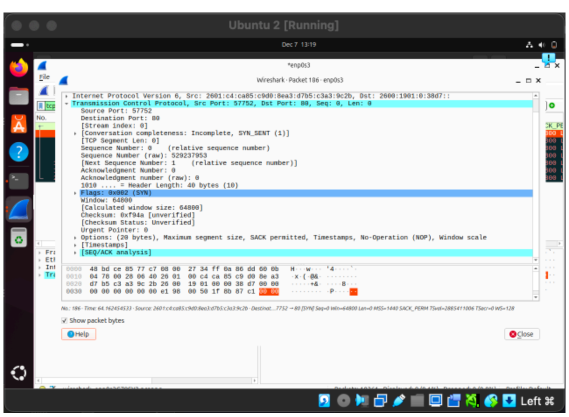

Ubuntu 2 [Running]

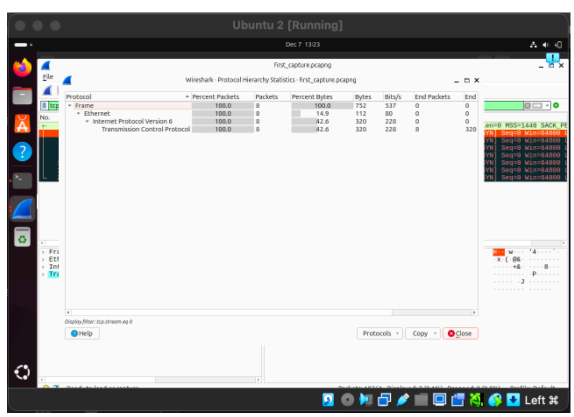

Ubuntu 2 [Running]

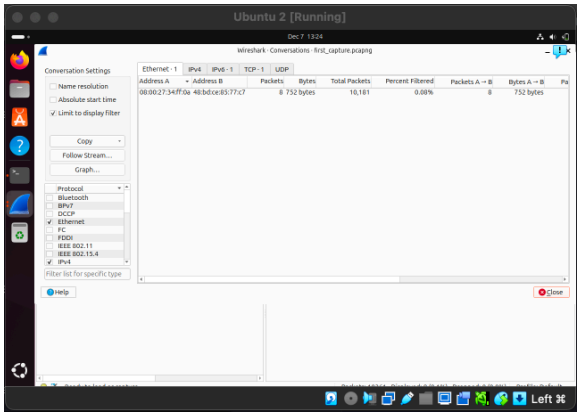

Ubuntu 2 [Running]

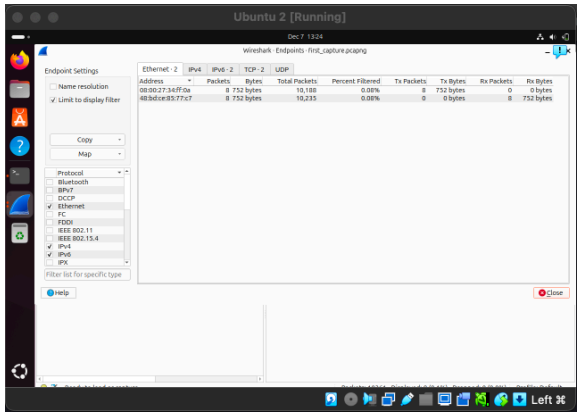

Ubuntu 2 [Running]

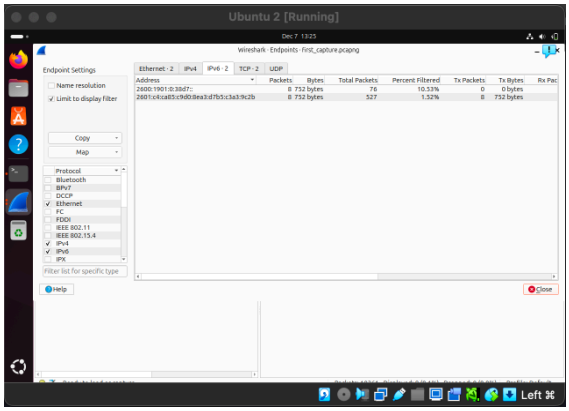

Ubuntu 2 [Running]

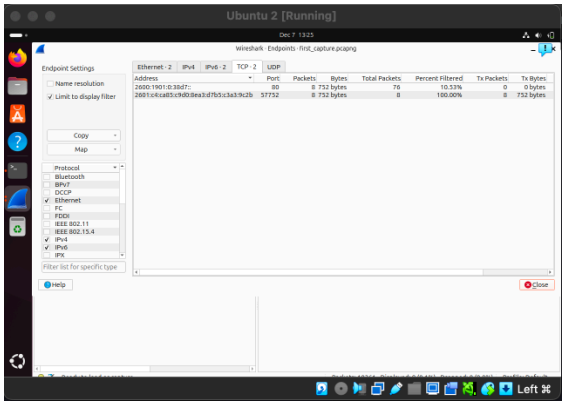

Ubuntu 2 [Running]


Ubuntu 2 [Running]


Ubuntu 2 [Running]
Wireshark · Conversations · first_capture.pcapng
Left ⌘


Ubuntu 2 [Running]
Wireshark · Endpoints · first_capture.pcapng
Left ⌘


Ubuntu 2 [Running]
Wireshark · Endpoints · first_capture.pcapng
Left ⌘


Ubuntu 2 [Running]
Wireshark · Endpoints · first_capture.pcapng
Left ⌘