

# NETWORK LICATER ANALYZER

**OS PROJE** 

My Journey in Network Monitoring and GUI Development

**JOHN NWEKE** 



## Introduction

## **Objective:**

- Develop a network traffic analyzer using Scapy and tcpdump.
- Implement a **GUI** using **Tkinter** for better usability.

## **Key Components:**

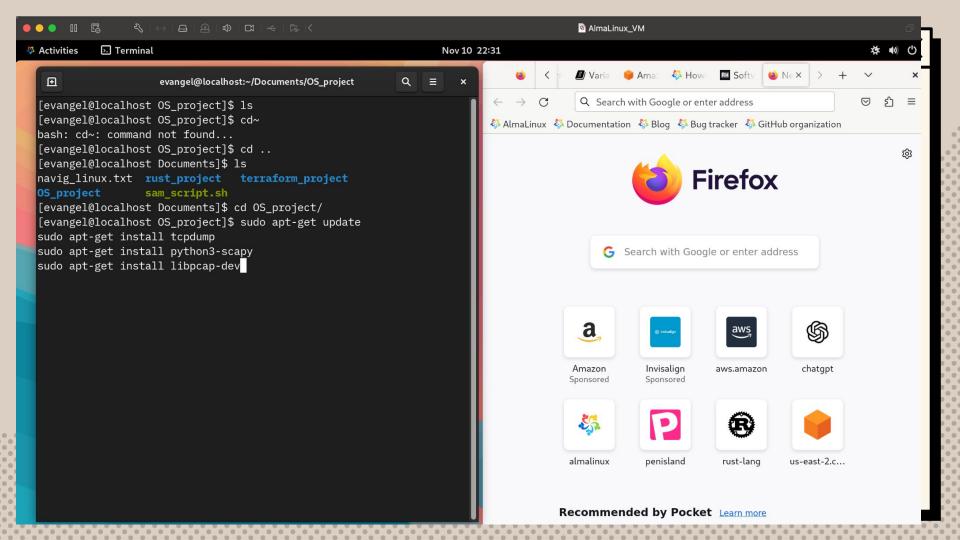
- Linux environment (AlmaLinux 9 fork of RHEL/CentOS)
- Python-based packet analysis



# **Initial Setup**

#### What I did:

- Installed required packages using `dnf`
- Faced errors due to missing network connectivity.



## **Network Challenges**

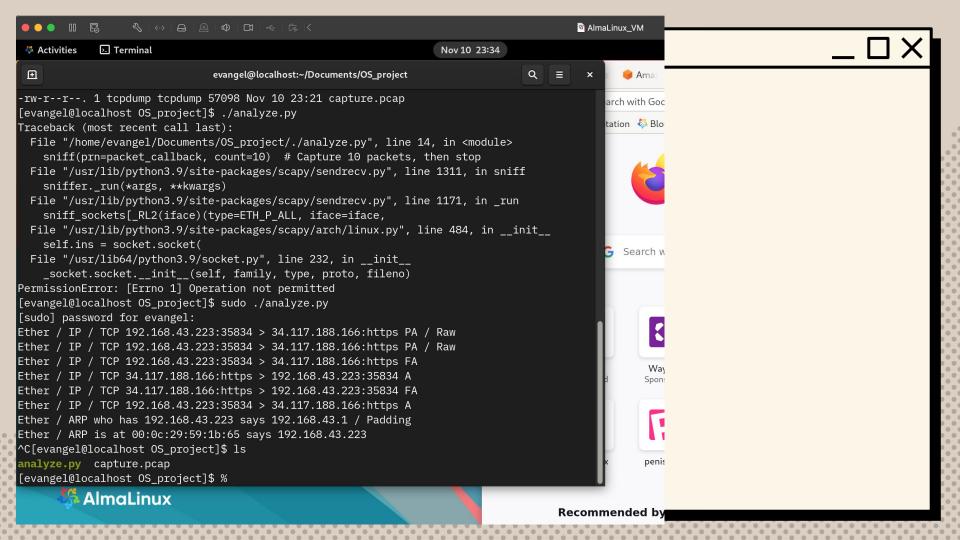
#### What I did:

- Error while downloading metadata for AlmaLinux repositories.
- Debugged using ping to check internet connectivity:

```
ping -c 4 8.8.8.8
```

### **Solution:**

- Switched from Towson Wi-Fi to mobile hotspot.
- Configured VM to use a bridged network adapter.





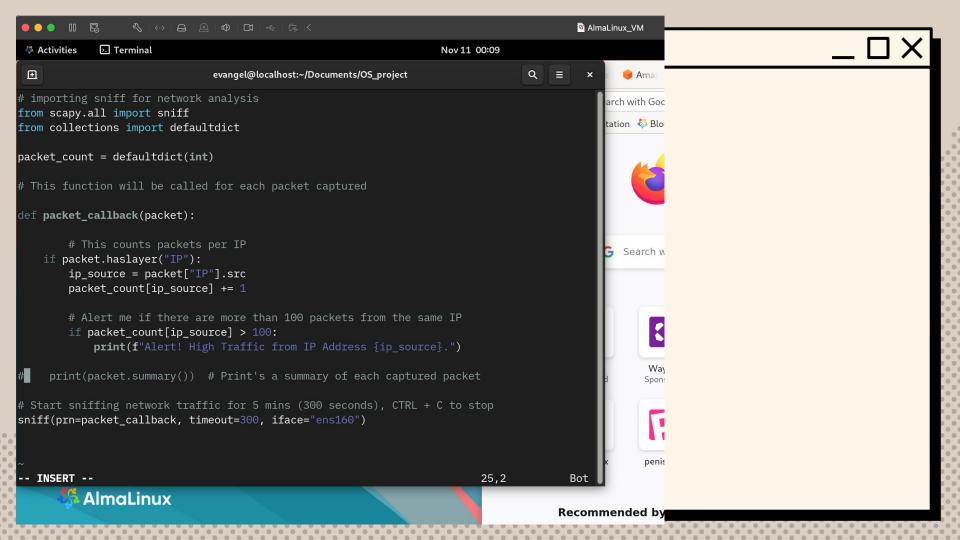
## **Dependency Challenges**

## **Challenge:**

- libpcap wasn't available by default.
- Pcap file is where raw, low-level network data is stored
   (Pcap = Packet Capture)

#### **Solution:**

- Enabled crb (CodeReady Builder/PowerTools) repository:
   sudo dnf config-manager --set-enabled crb
- Successfully installed libpcap.





# **Analyzing Traffic**

## **Using tcpdump:**

Captured network traffic and saved it to a pcap file
 sudo tcpdump -i any -w capture.pcap

## Packet Analysis with Scapy:

 Developed a Python script to analyze packets and log suspicious IP activity.



## **Interface Config**

#### **Identified Network Interfaces:**

Used ip link show to find active interfaces:

Loopback: lo

Ethernet: ens160

### **Optimization:**

Specified ens160 for monitoring.

Automated script execution with shebang and chmod +x:

```
[evangel@localhost OS project]$ cd ..
[evangel@localhost Documents]$ ls
navig_linux.txt OS_project rust_project sam_script.sh terraform_project
[evangel@localhost Documents]$ mkdir "OS project 2"
[evangel@localhost Documents]$ ls
navig linux.txt OS project OS project 2 rust project sam script.sh terraform pro
[evangel@localhost Documents]$ cd OS project 2/
[evangel@localhost OS project 2]$ ls
[evange]@localhost OS_project_2]$ touch network_analyzer.py
[evangel@localhost OS_project_2]$ vim network_analyzer.py
[evangel@localhost OS project 2]$ ls
network analyzer.py
[evangel@localhost OS_project_2]$ chmod +x network_analyzer.py
[evangel@localhost OS project 2]$ ls -tharl
total 4.0K
drwxr-xr-x. 6 evangel evangel 133 Dec 3 16:11 ...
-rwxr-xr-x. 1 evangel evangel 2.3K Dec 3 16:15 network analyzer.py
drwxr-xr-x. 2 evangel evangel 33 Dec 3 16:15
[evangel@localhost OS_project_2]$ %
```



## **Adding a GUI**

#### **Professor's Feedback:**

Requested GUI for user-friendly alerts, but AlmaLinux doesn't natively support GUIs.

#### **Solution:**

Had to Install GUI dependencies and integrate Tkinter.

Dependencies resolved.				
======================================	Architecture	Version	Repository	======== Size
===================================== nstalling:				
<b>python3-tkinter</b> pgrading:	x86_64	3.9.19-8.e19_5.1	appstream	309 k
python-unversioned-command	noarch	3.9.19-8.el9_5.1	appstream	9.0 k
python3	x86_64	3.9.19-8.el9_5.1	baseos	26 k
python3-libs	x86_64	3.9.19-8.el9_5.1	baseos	7.5 M
Installing dependencies:				
tk	x86_64	1:8.6.10-9.el9	appstream	1.6 M
ransaction Summary				
.=====================================	=======================================			=======
ransaction Summary		·		
Enstall 2 Packages Upgrade 3 Packages				=======
Enstall 2 Packages Upgrade 3 Packages  Total download size: 9.4 M  Total sok [y/N]: y  Downloading Packages:				
Enstall 2 Packages  Install 2 Packages  Ipgrade 3 Packages  Total download size: 9.4 M  Is this ok [y/N]: y  Iownloading Packages:  Install 2 Packages 2		n.rpm	 159 kB/s   9.0 kB	 
Install 2 Packages Install 2 Packages Ingrade 3 Packages  Total download size: 9.4 M Is this ok [y/N]: y Downloading Packages: [1/5): python-unversioned-command- [2/5): python3-3.9.19-8.el9_5.1.x8	6_64.rpm	n.rpm	294 kB/s   26 kB	00:00
Enstall 2 Packages  Install 2 Packages  Ipgrade 3 Packages  Total download size: 9.4 M  Is this ok [y/N]: y  It is pownloading Packages:  Install 2 Packages  Install	6_64.rpm	1. <b>r</b> pm	294 kB/s   26 kB 886 kB/s   309 kB	00:00 00:00
Install 2 Packages Install 2 Packages Ipgrade 3 Packages  Total download size: 9.4 M  Is this ok [y/N]: y	6_64.rpm 9_5.1.x86_64.rpm	n. <b>r</b> pm	294 kB/s   26 kB	00:00

```
F
                                                                                                               Q
                                                                                                                   evangel@localhost:~/Documents/OS project 2
Traceback (most recent call last):
  File "/home/evangel/Documents/OS_project_2/./network_analyzer.py", line 65, in <module>
    root = tk.Tk()
  File "/usr/lib64/python3.9/tkinter/ init .py", line 2270, in init
    self.tk = tkinter.create(screenName, baseName, className, interactive, wantobjects, useTk, sync, use)
 tkinter.TclError: no display name and no $DISPLAY environment variable
[evangel@localhost OS project 2]$ sudo dnf groupinstall "Server with GUI"
Last metadata expiration check: 0:05:11 ago on Tue 03 Dec 2024 04:19:02 PM EST.
Dependencies resolved.
Package
                                                 Architecture Version
                                                                                                   Repository
                                                                                                                     Size
Upgrading:
                                                 x86 64
                                                              1:1.48.10-2.el9 5.alma.1
                                                                                                   baseos
 NetworkManager-adsl
                                                 x86 64
                                                              1:1.48.10-2.el9 5.alma.1
                                                                                                   baseos
 NetworkManager-bluetooth
                                                 x86 64
                                                              1:1.48.10-2.el9 5.alma.1
                                                                                                   baseos
 NetworkManager-config-server
                                                 noarch
                                                              1:1.48.10-2.el9 5.alma.1
                                                                                                   baseos
 NetworkManager-libnm
                                                              1:1.48.10-2.el9 5.alma.1
                                                 x86_64
                                                                                                   baseos
 NetworkManager-team
                                                              1:1.48.10-2.el9 5.alma.1
                                                 x86 64
                                                                                                   baseos
```

2.3 M NetworkManager 34 k 61 k 20 k 1.8 M 40 k NetworkManager-tui 1:1.48.10-2.el9 5.alma.1 247 k x86 64 baseos NetworkManager-wifi 1:1.48.10-2.el9 5.alma.1 82 k x86 64 baseos NetworkManager-wwan x86 64 1:1.48.10-2.el9 5.alma.1 68 k baseos almalinux-gpg-keys x86 64 9.5-1.el9 9.5 k baseos almalinux-release x86 64 9.5-1.el9 baseos 20 k almalinux-repos x86 64 9.5-1.el9 9.6 k baseos alsa-lib 1.2.12-1.el9 504 k x86\_64 appstream alsa-ucm noarch 1.2.12-1.el9 150 k appstream



## **Virtual Machine Crashed**

Virtual Machine Crashed after installing GUI dependencies on AlmaLinux



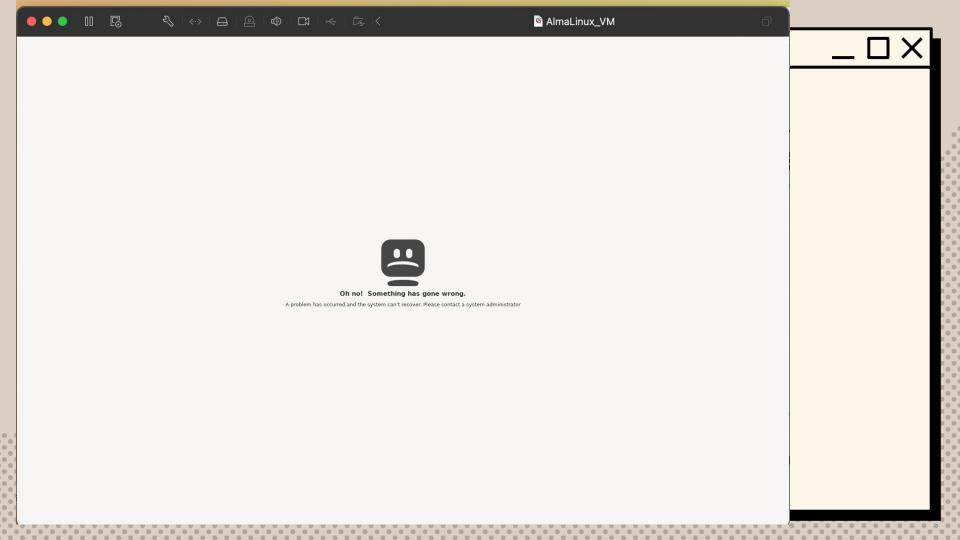








Didn't cuss tho





## Pivot to Use MacOS

Like any good Carnie says: "The Show must Go on."



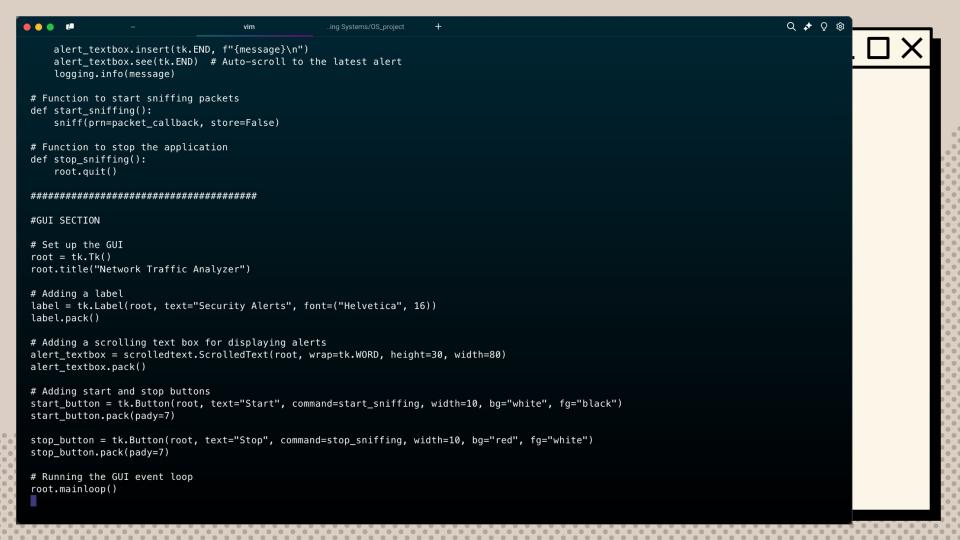
## **Final Solution**

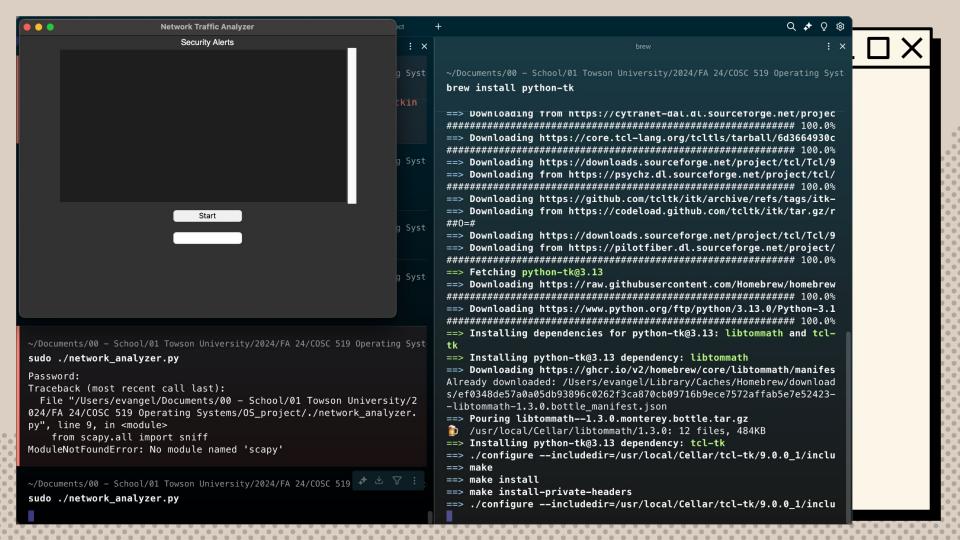
#### **Outcome:**

 Functional network analyzer with a responsive GUI on MacOS

## **Key Features:**

- Monitors traffic on ens160.
- Logs IPs with high traffic or port scans
- GUI displays real-time alerts
- Run on Mac OS instead of Linux





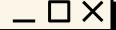


## **Future Improvements**

## **Ideas for Improvements**

- Add real-time traffic graphs using matplotlib.
- Implement email notifications for critical alerts.
- Enhance GUI with filtering options for different protocols.
- Optimize packet processing for large networks.





# NETWORK IRAFFIC ANALYZER

My Journey in Network Monitoring and GUI Development

**JOHN NWEKE**