TASK 1

BASIC NETWORK SNIFFER

Build a network sniffer in Python that captures and analyzes network traffic.

A Network Packet Sniffer developed in Python 3. Packets are disassembled as they arrive at a given network interface controller and their information is displayed on the screen.

A network packet sniffer was created, which is solely focused on gathering, managing, and examining network traffic. The user has the option to choose which interface to use to record traffic, how many packets to sniff, and how long the sniffer should run (how long to record packets). The user inputs the file name because the application will record the traffic data it records in a text file. The user-selected protocol is used by the 'packet_log' function to filter the packets and save them in the log file. Every detail of the traffic passing via the interface will be included in the data saved in the file.

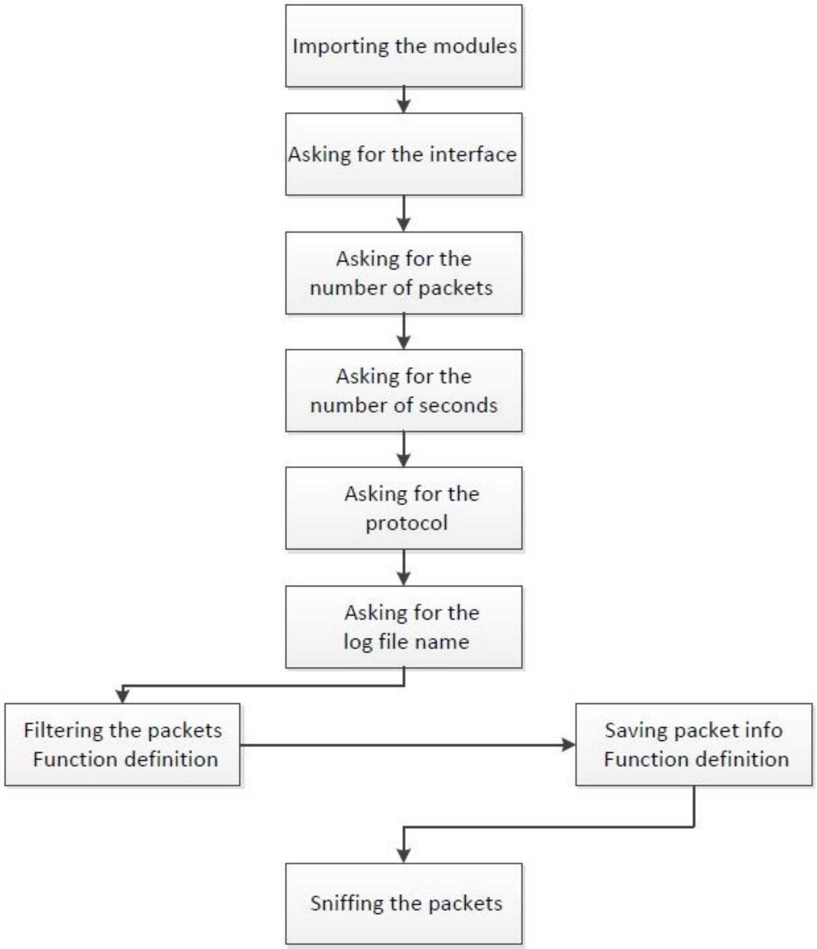

Importing the modules
Asking for the interface
Asking for the number of packets
Asking for the number of seconds
Asking for the protocol
Asking for the log file name
Filtering the packets Function definition
Saving packet info Function definition
Sniffing the packets

Figure: Logical Flow Diagram

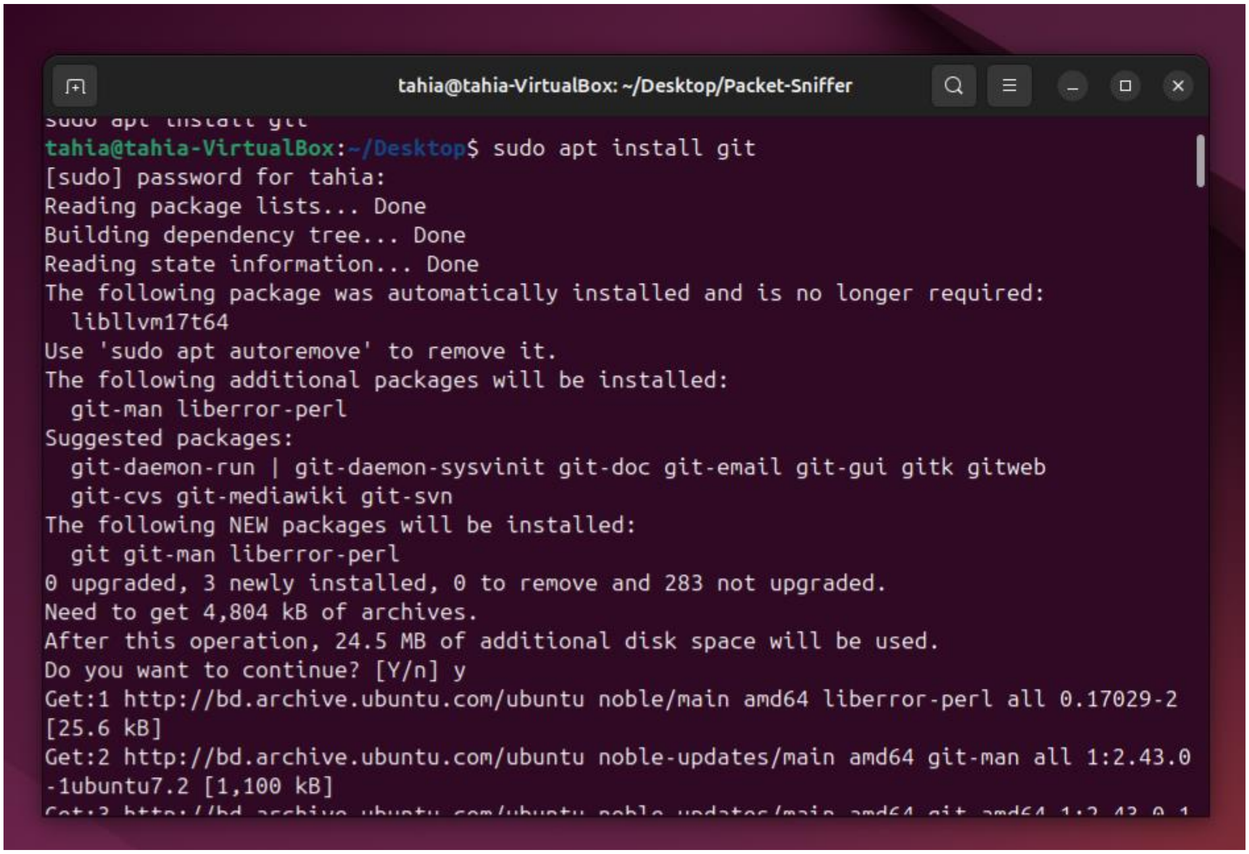
Running the Application

I. Development Mode

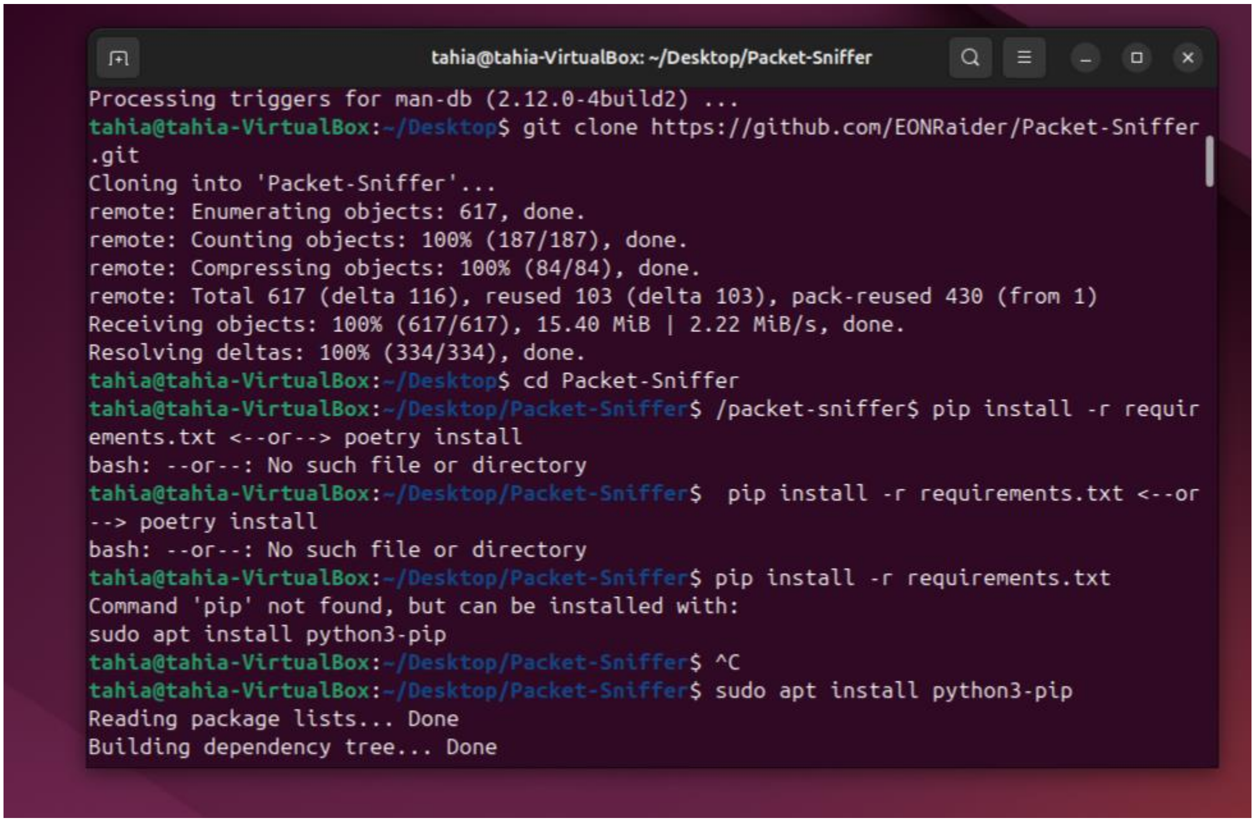
Simply clone this repository with git clone, install the dependencies and execute the sniffer.py file.

```
user@host:~$ git clone https://github.com/EONRaider/Packet-Sniffer.git

user@host:~$ cd Packet-Sniffer

user@host:~/packet-sniffer$ pip install -r requirements.txt <--or--> poetry install

user@host:~/packet-sniffer$ sudo python3 packet_sniffer/sniffer.py
```

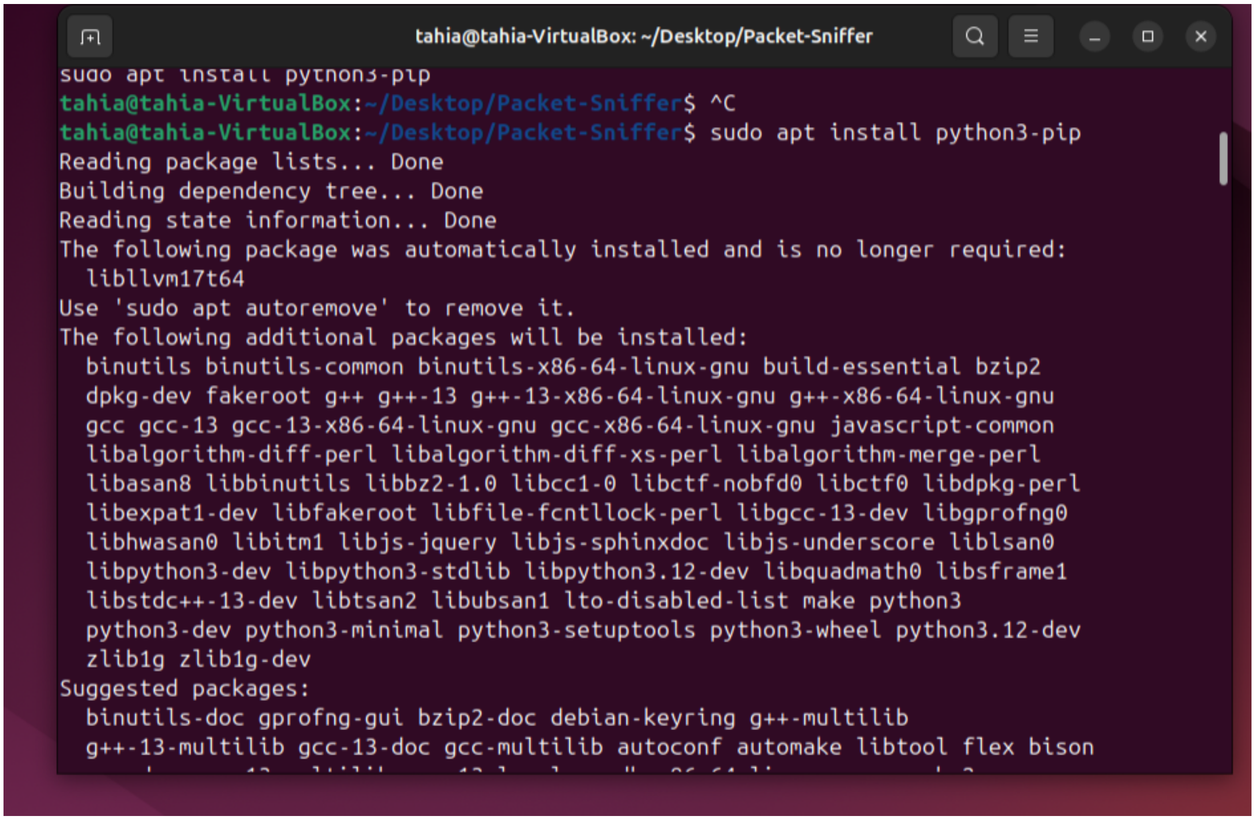
The sudo command is required due to the use of socket.SOCK_RAW, which needs administrative privileges to run on GNU/Linux.



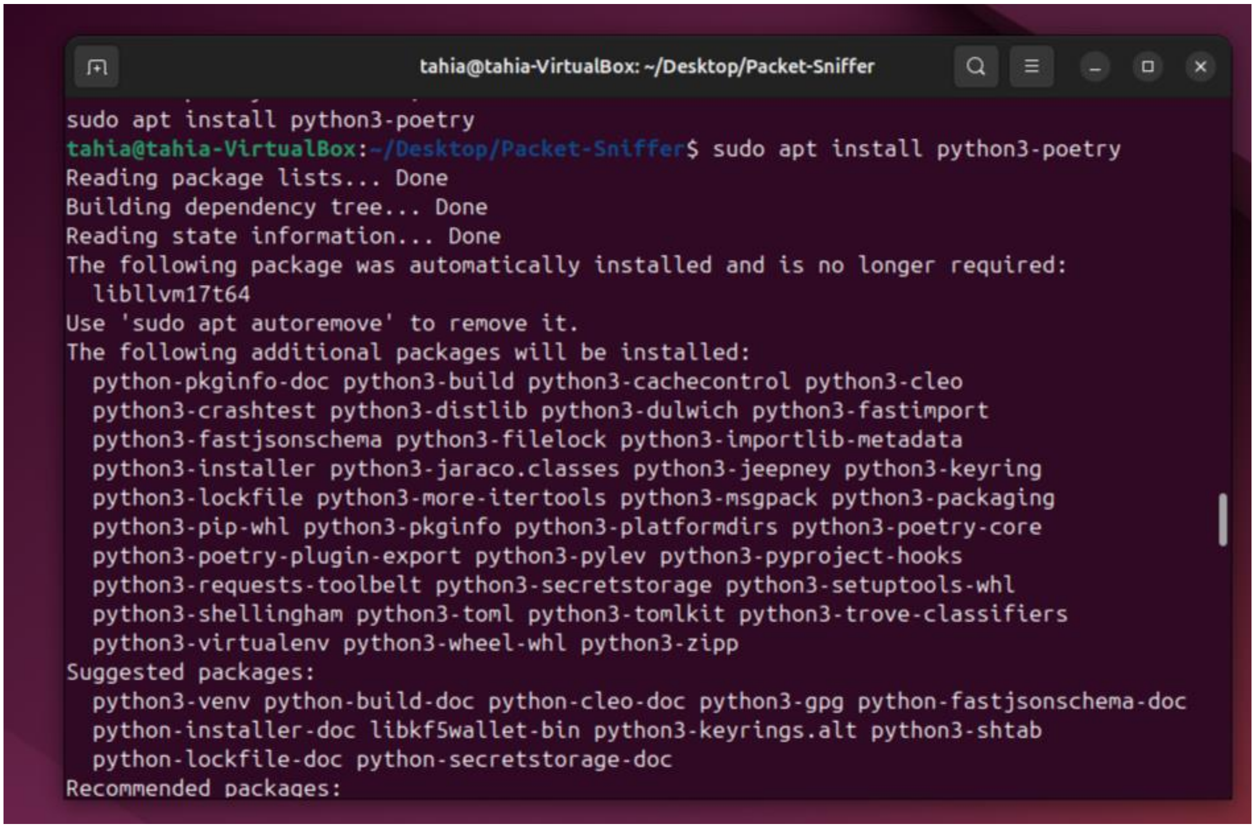
```
sudo apt install git
tahia@tahia-VirtualBox:~/Desktop$ sudo apt install git
[sudo] password for tahia:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  libllvm17t64
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  git-man liberror-perl
Suggested packages:
  git-daemon-run | git-daemon-sysvinit git-doc git-email git-gui gitk gitweb
  git-cvs git-mediawiki git-svn
The following NEW packages will be installed:
  git git-man liberror-perl
0 upgraded, 3 newly installed, 0 to remove and 283 not upgraded.
Need to get 4,804 kB of archives.
After this operation, 24.5 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://bd.archive.ubuntu.com/ubuntu noble/main amd64 liberror-perl all 0.17029-2
[25.6 kB]
Get:2 http://bd.archive.ubuntu.com/ubuntu noble-updates/main amd64 git-man all 1:2.43.0
-1ubuntu7.2 [1,100 kB]
Get:3 http://bd.archive.ubuntu.com/ubuntu noble-updates/main amd64 git amd64 1:2.43.0-1
```



```
Processing triggers for man-db (2.12.0-4build2) ...
tahia@tahia-VirtualBox:~/Desktop$ git clone https://github.com/EONRaider/Packet-Sniffer
.git
Cloning into 'Packet-Sniffer'...
remote: Enumerating objects: 617, done.
remote: Counting objects: 100% (187/187), done.
remote: Compressing objects: 100% (84/84), done.
remote: Total 617 (delta 116), reused 103 (delta 103), pack-reused 430 (from 1)
Receiving objects: 100% (617/617), 15.40 MiB | 2.22 MiB/s, done.
Resolving deltas: 100% (334/334), done.
tahia@tahia-VirtualBox:~/Desktop$ cd Packet-Sniffer
tahia@tahia-VirtualBox:~/Desktop/Packet-Sniffer$ /packet-sniffer$ pip install -r requir
ements.txt <--or--> poetry install
bash: --or--: No such file or directory
tahia@tahia-VirtualBox:~/Desktop/Packet-Sniffer$  pip install -r requirements.txt <--or
--> poetry install
bash: --or--: No such file or directory
tahia@tahia-VirtualBox:~/Desktop/Packet-Sniffer$ pip install -r requirements.txt
Command 'pip' not found, but can be installed with:
sudo apt install python3-pip
tahia@tahia-VirtualBox:~/Desktop/Packet-Sniffer$ ^C
tahia@tahia-VirtualBox:~/Desktop/Packet-Sniffer$ sudo apt install python3-pip
Reading package lists... Done
Building dependency tree... Done
```

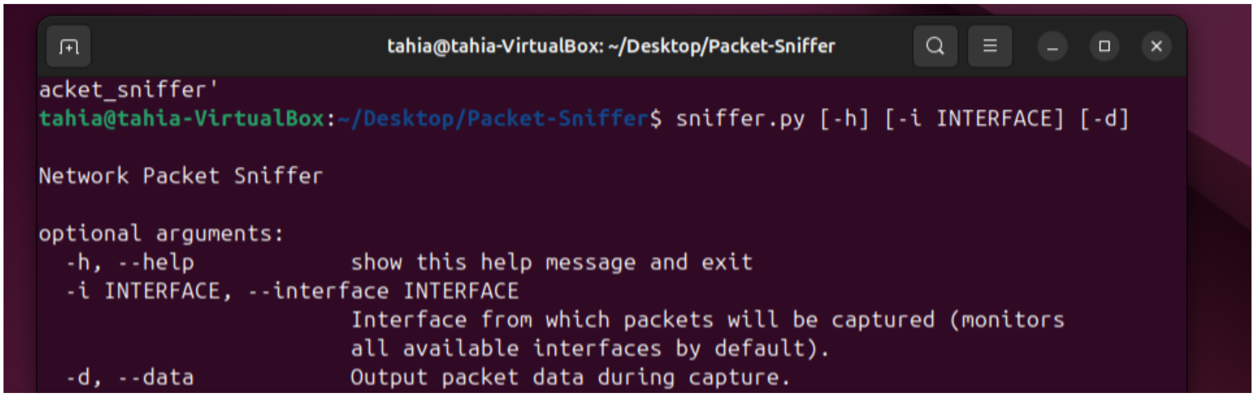


```
sudo apt install python3-pip
tahia@tahia-VirtualBox:~/Desktop/Packet-Sniffer$ ^C
tahia@tahia-VirtualBox:~/Desktop/Packet-Sniffer$ sudo apt install python3-pip
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  libllvm17t64
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu build-essential bzip2
  dpkg-dev fakeroot g++ g++-13 g++-13-x86-64-linux-gnu g++-x86-64-linux-gnu
  gcc gcc-13 gcc-13-x86-64-linux-gnu gcc-x86-64-linux-gnu javascript-common
  libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl
  libasan8 libbinutils libbz2-1.0 libcc1-0 libctf-nobfd0 libctf0 libdpkg-perl
  libexpat1-dev libfakeroot libfile-fcntllock-perl libgcc-13-dev libgprofng0
  libhwasan0 libitm1 libjs-jquery libjs-sphinxdoc libjs-underscore liblsan0
  libpython3-dev libpython3-stdlib libpython3.12-dev libquadmath0 libsframe1
  libstdc++-13-dev libtsan2 libubsan1 lto-disabled-list make python3
  python3-dev python3-minimal python3-setuptools python3-wheel python3.12-dev
  zlib1g zlib1g-dev
Suggested packages:
  binutils-doc gprofng-gui bzip2-doc debian-keyring g++-multilib
  g++-13-multilib gcc-13-doc gcc-multilib autoconf automake libtool flex bison
```



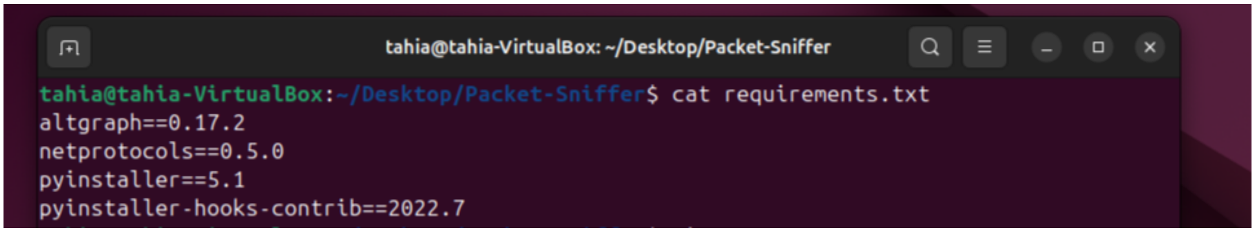
```
sudo apt install python3-poetry
tahia@tahia-VirtualBox:~/Desktop/Packet-Sniffer$ sudo apt install python3-poetry
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  libllvm17t64
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  python-pkginfo-doc python3-build python3-cachecontrol python3-cleo
  python3-crashtest python3-distlib python3-dulwich python3-fastimport
  python3-fastjsonschema python3-filelock python3-importlib-metadata
  python3-installer python3-jaraco.classes python3-jeepney python3-keyring
  python3-lockfile python3-more-itertools python3-msgpack python3-packaging
  python3-pip-whl python3-pkginfo python3-platformdirs python3-poetry-core
  python3-poetry-plugin-export python3-pylev python3-pyproject-hooks
  python3-requests-toolbelt python3-secretstorage python3-setuptools-whl
  python3-shellingham python3-toml python3-tomlkit python3-trove-classifiers
  python3-virtualenv python3-wheel-whl python3-zipp
Suggested packages:
  python3-venv python-build-doc python-cleo-doc python3-gpg python-fastjsonschema-doc
  python-installer-doc libkf5wallet-bin python3-keyrings.alt python3-shtab
  python-lockfile-doc python-secretstorage-doc
Recommended packages:
```

Usage



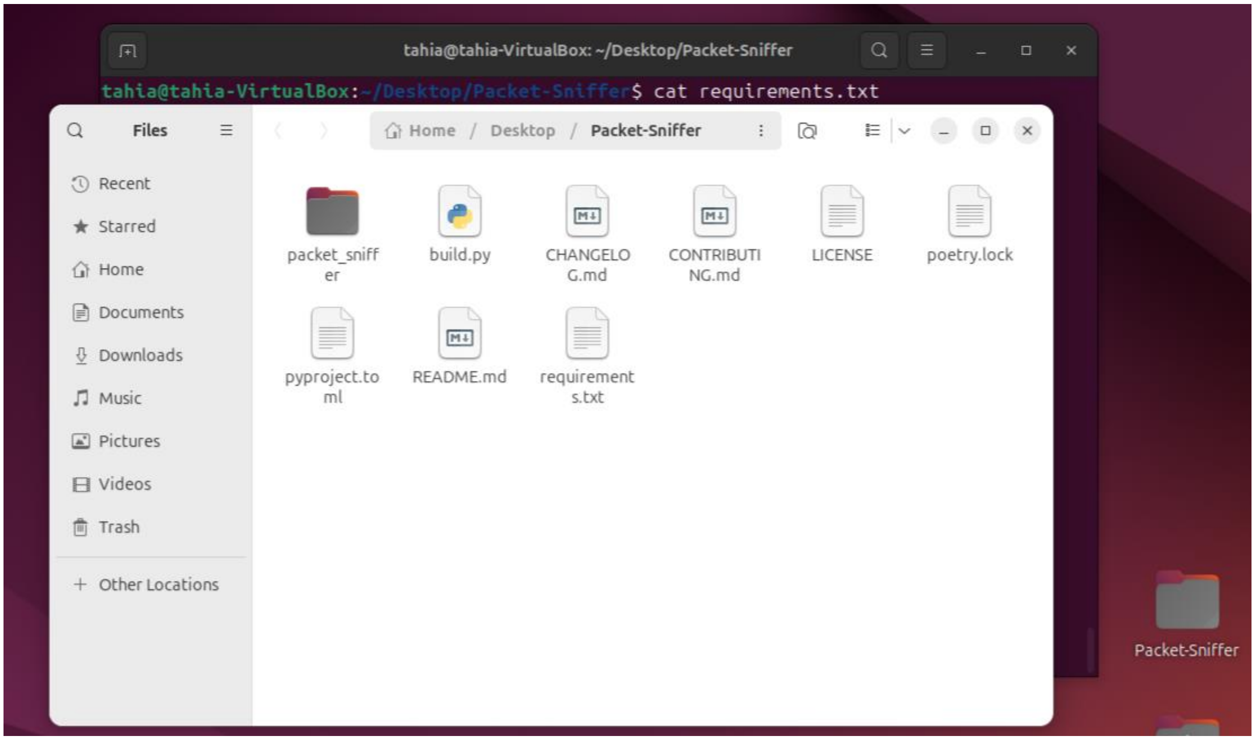
```
acket_sniffer'
tahia@tahia-VirtualBox:~/Desktop/Packet-Sniffer$ sniffer.py [-h] [-i INTERFACE] [-d]

Network Packet Sniffer

optional arguments:
  -h, --help            show this help message and exit
  -i INTERFACE, --interface INTERFACE
                        Interface from which packets will be captured (monitors
                        all available interfaces by default).
  -d, --data            Output packet data during capture.
```

Application Execution



```
tahia@tahia-VirtualBox:~/Desktop/Packet-Sniffer$ cat requirements.txt
altgraph==0.17.2
netprotocols==0.5.0
pyinstaller==5.1
pyinstaller-hooks-contrib==2022.7
```

Generated Files



```
tahia@tahia-VirtualBox:~/Desktop/Packet-Sniffer$ cat requirements.txt
```