# Python3.11 site-packages

C:\Users\IGS\AppData\Roaming\Python\Python311\site-packages

# Download Dshell

git clone <https://github.com/USArmyResearchLab/Dshell>;

# Create a Python virtual env for Dshell to avoid conflicting modules

cd ./Dshell;

virtualenv venv\_dshell;

# Directory will have venv\_dshell come up

A screenshot of a computer

Description automatically generated

# Get into virtual environment (Linux)

source venv\_dshell/bin/activate

A black screen with white text

Description automatically generated

# Get into virtual environment (windows)

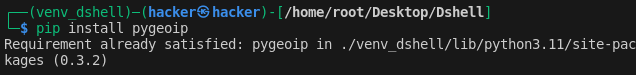
source venv\_dshell/Scripts/activate;

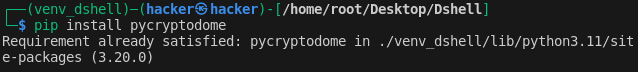
A black background with yellow and green text

Description automatically generated

# Install dependencies in venv\_dshell

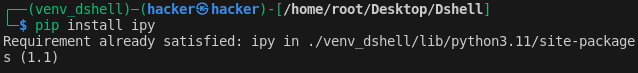
pip install pygeoip pycryptodome dpkt ipy pypcap;

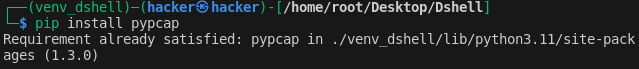




A black screen with white text

Description automatically generated





# If need to exit virtual env

deactivate;

# Exit virtual environment && Use decode.py

cd Dshell/dshell;

python3 decode.py;

A screenshot of a computer

Description automatically generated

python3 decode.py -l;

A screenshot of a computer screen

Description automatically generated

# Using decoders

A white text with black text

Description automatically generated

python3 Dshell/dshell/decode.py -l;

A screenshot of a computer

Description automatically generated

python3 Dshell/dshell/decode.py -d <decoder> <path/to/pcap>;

# Test using bitcoin decoder

python3 decode.py -d bitcoin;

A screenshot of a computer program

Description automatically generated

# Try using ether decoder

A computer screen shot of a black screen

Description automatically generated

# Use wireShark to capture some traffic in your network

start => stop

A screenshot of a computer

Description automatically generated

File => Save As =>

A screenshot of a computer program

Description automatically generated

network-test.pcapng

A screenshot of a computer

Description automatically generated

# Use IP decoder to decode network traffic

python3 decode.py -d ip ./data/network-test.pcapng;

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

You can try out other decoders too :D