analysis\_pcap\_tcp – README

analysis\_pcap\_tcp is a version of TCPDump. The analysis\_pcap\_tcp parses a pcap file and finds all the packets in the TCP.

## Installation

The analysis\_pcap\_tcp function requires Python 3.8.1, which can be obtained from python.org In order to check the version on your system, enter the terminal:

Python --version

The following imports were used

import struct

import dpkt

import sys

For the import dpkt it requires the installation of dpkt. In your terminal type:

pip install dpkt

## Running the tests

After unzipping the folder, go to the terminal (command prompt). Change the directory to the folder where the “analysis\_pcap\_tcp.py” python file is located. Once the terminal is in that folder, you can call ‘python analysis\_pcap\_tcp.py filename.pcap’. The filename.pcap has to be in the folder where the “analysis\_pcap\_tcp.py” is located. In addition, that file has to be a pcap file for it to analysis correctly.

python analysis\_pcap\_tcp.py assignment2.pcap