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
```

```
pip install dpkt
```

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

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
```