analysis_pcap_tcp.py

Libraries:

sys

datetime

from dpkt:

- dpkt
- dpkt.utils

Requirements:

```
pip install dpkt
```

Usage:

Use command line arguments to query a domain:

```
python3 analysis_pcap_tcp.py foo.pcap
```

Output:

```
Flow #1
SRC IP: 130.245.145.12
PORT  : 43498
DST IP: 128.208.2.198
PORT  : 80
Window: 42340

Total Packets: 11106
Throughput: 627798 (bytes/sec)

Flow #1 Transactions
type            flag         seq         ack         window     time

snd -> rev      PUSH,ACK     705669103   1921750144  3          2017-02-17 19:56:33.607655

rev -> snd      ACK          1921750144  705669127   3          2017-02-17 19:56:33.680429

snd -> rev      ACK          705669127   1921750144  3          2017-02-17 19:56:33.607996

rev -> snd      ACK          1921750144  705670575   3          2017-02-17 19:56:33.680644
```