# Pycket

## Network Sniffer

Technical Documentation

Alexis Le Dinh <le-dinh_a@epitech.eu>

Romain Zanchi <zanchi_r@epitech.eu>

Stéphane Mombuleau <mombul_s@epitech.eu>

## Abstract

**Pycket** is a light network sniffer.

The purpose of **pycket** is to capture and inspect incoming and outgoing packets on your network.

This documentation will cover (some of) the technical aspects of **pycket**.

## Dependencies

**Pycket** uses:

- Python 2.7.x
- PyQt4 (python-qt4)

## Main Program

**Pycket** allows you to capture, watch, inspect and forge packets on your networks. It runs on Linux and is developed in Python.

## GUI

**Pycket** uses Qt for its User Interface. More precisely, it uses PyQt4, the Python library for Qt.

## Capturing packets

To capture packets on the network, **Pycket** opens a socket on ETH_P_ALL which means that it will get access to every Ethernet packet.

*Socket.socket(socket.AF_PACKET, socket.SOCK_RAW, socket.ntohs(0x0003))*
*(0x0003 = ETH_P_ALL in C)*

We then read on the socket and capture every 65565 bytes in order to convert them to a packet structure.

## Extracting Images

To extract images from a .pcap file, **Pycket** opens it and tries to find every image headers in every TCP packet.

*Content-Type: image/jpeg*

For each image header, **pycket** retrieves the following bytes and puts them in a .jpeg file that will be potentially readable.

## Contact

Alexis Le Dinh <le-dinh_a@epitech.eu>

Romain Zanch <zanchi_r@epitech.eu>

Stéphane Mombuleau <mombul_s@epitech.eu>

Contribute : https://github.com/alexis-ld/pycket

Epitech – Novembre 2015