

Pycket

Network Sniffer

User 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 covers the installation process and presents the features.

Requirements

Pycket requires python-2.7 and python-qt4 to run.

Installation

To install **pycket**, run:

```
sudo dpkg -i python-pycket_1.0.0-1_all.deb
```

Usage

```
python mainGUI.py
```

Features

pycket comes with a handful of features:

- **Capture:** Capture incoming and outgoing packets on your network
- **Filter:** Search through live traffic
- **Forging:** Forge packets
- **Export to .pcap file:** Export your capture to a formatted .pcap file
- **Import .pcap file**
- **Watch list:** Add IPs to a watch list and get notified of incoming traffic from those IPs (packets will be highlighted in red)
- **Trigger:** Get notified when an IP has been seen a lot in a short period of time (packets will be highlighted in orange)
- **Extract images:** Extract images (jpeg) from previously captured packets (.pcap file)

Contact

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

Romain Zanchi <zanchi_r@epitech.eu>

Stéphane Mombuleau <mombul_s@epitech.eu>

<https://github.com/alexis-ld/pycket>