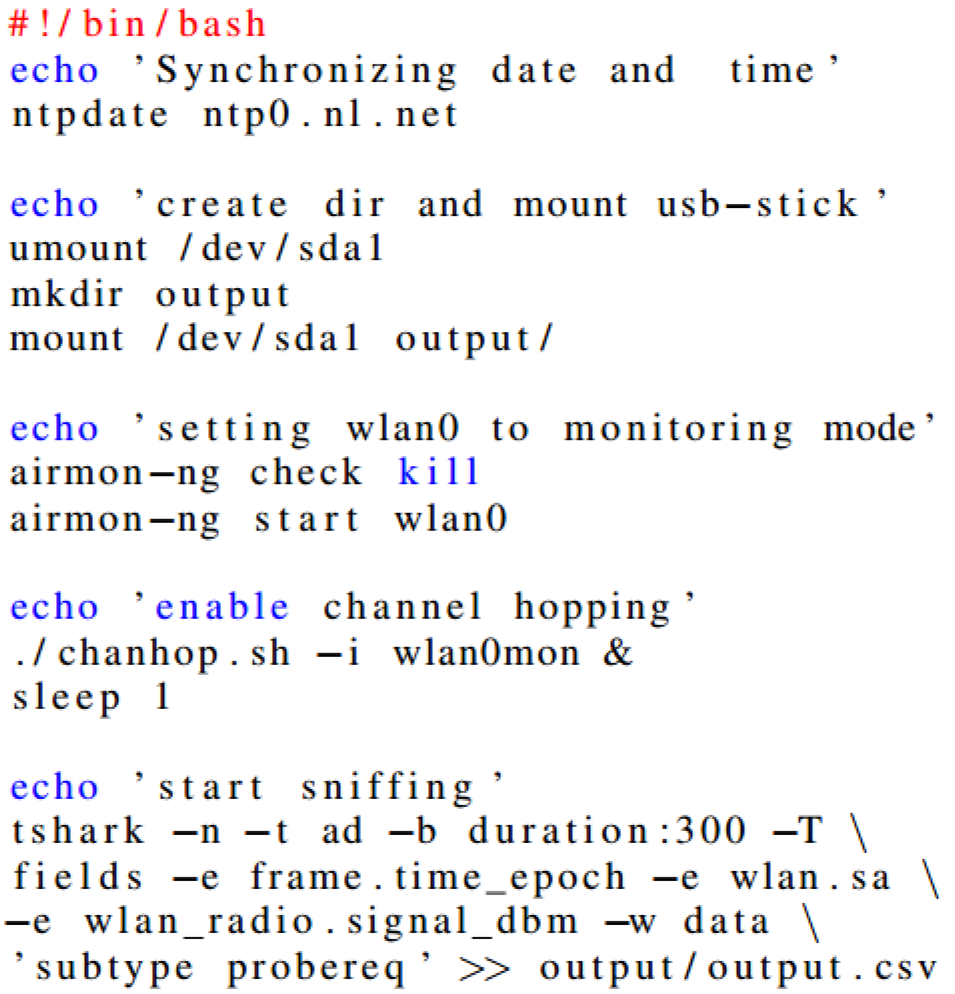
MAC activity tracker

N.Hokke

J. Brouwer

Method

- Probe request
- Hardware
  - Pi 3
- Software
  - Kali Linux
  - Tshark
  - Python
- Location?



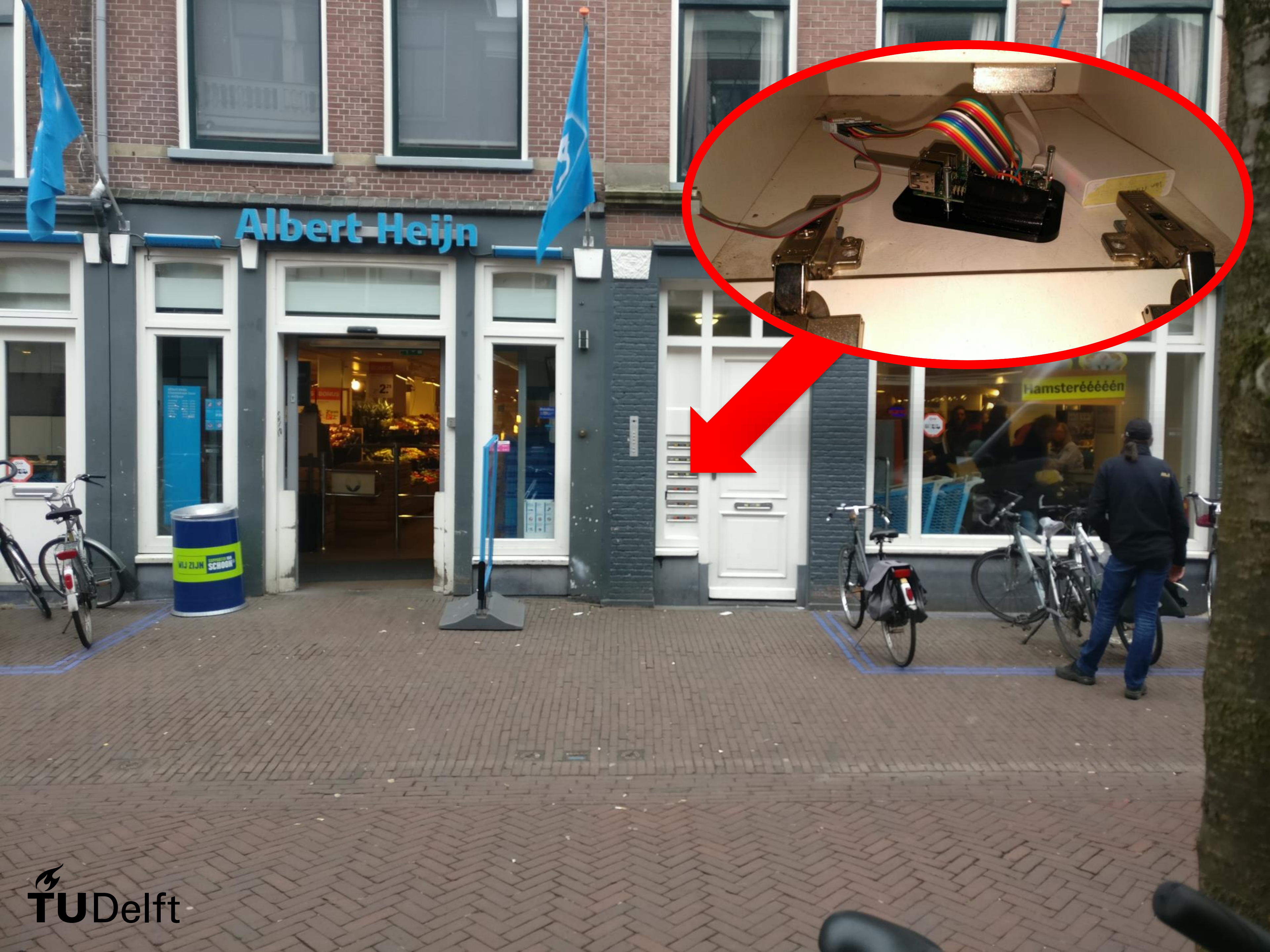
```
#!/bin/bash
echo 'Synchronizing date and  time'
ntpdate ntp0.nl.net

echo 'create dir and mount usb-stick'
umount /dev/sda1
mkdir output
mount /dev/sda1 output/

echo 'setting wlan0 to monitoring mode'
airmon-ng check kill
airmon-ng start wlan0

echo 'enable channel hopping'
./chanhop.sh -i wlan0mon &
sleep 1

echo 'start sniffing'
tshark -n -t ad -b duration:300 -T \
fields -e frame.time_epoch -e wlan.sa \
-e wlan_radio.signal_dbm -w data \
'subtype probereq' >> output/output.csv
```

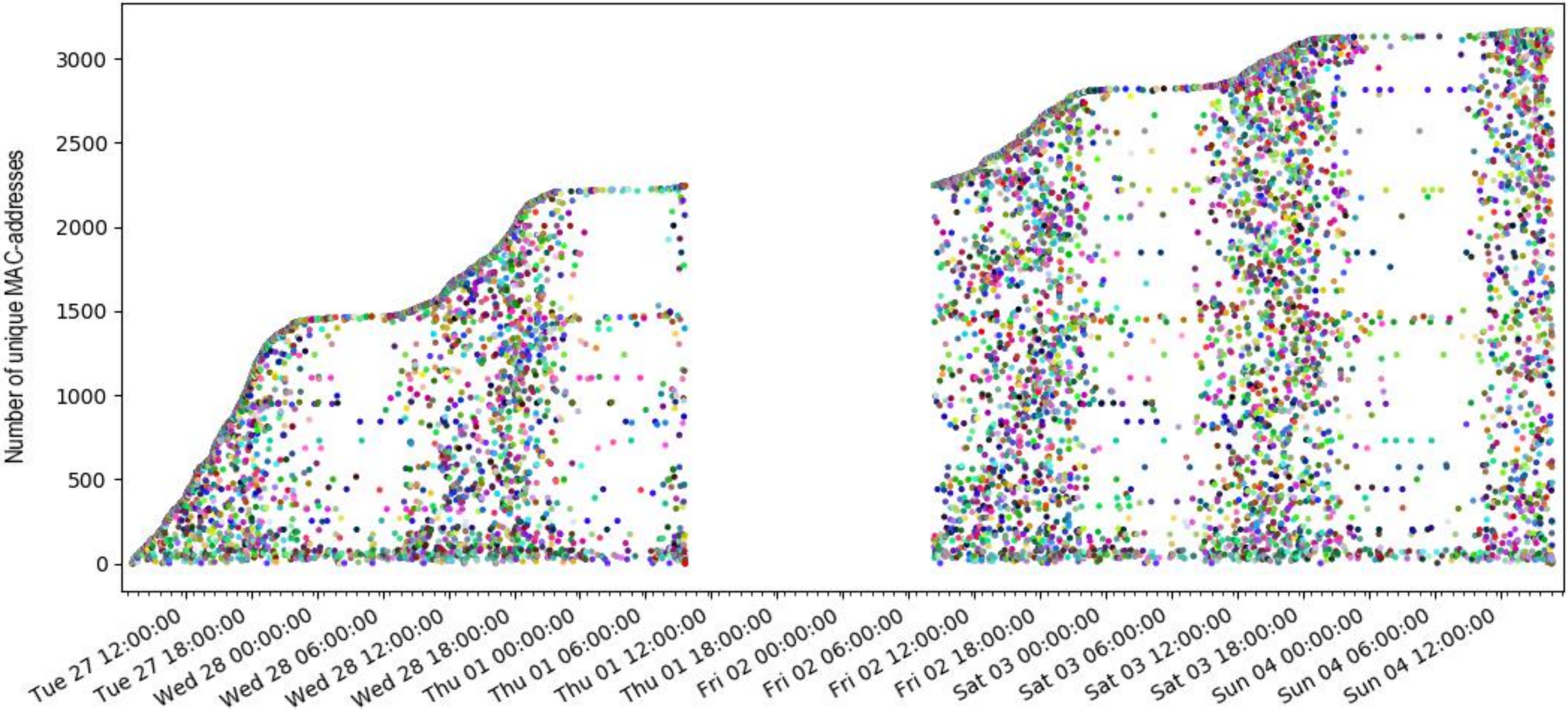


TU Delft

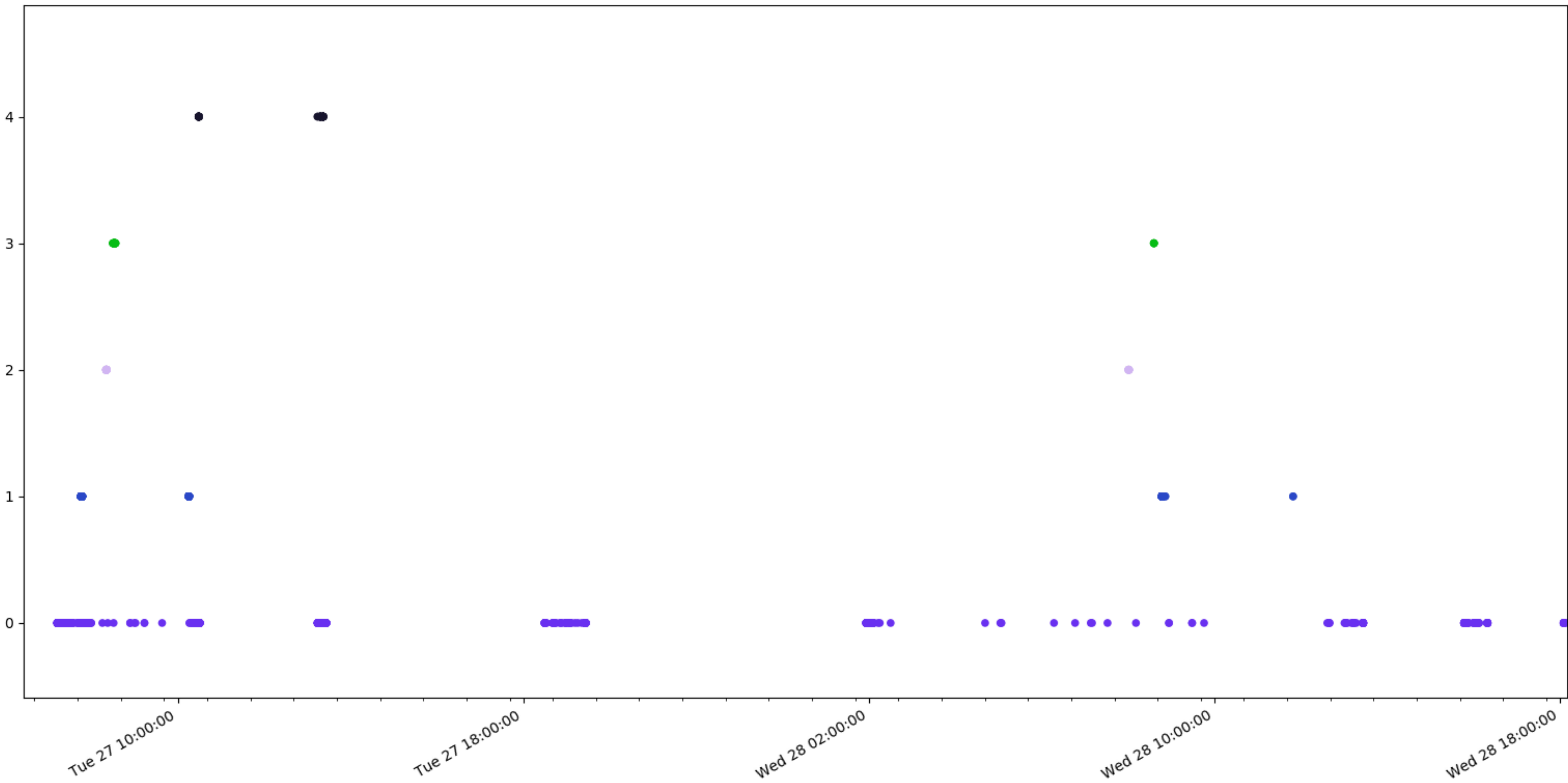
Results

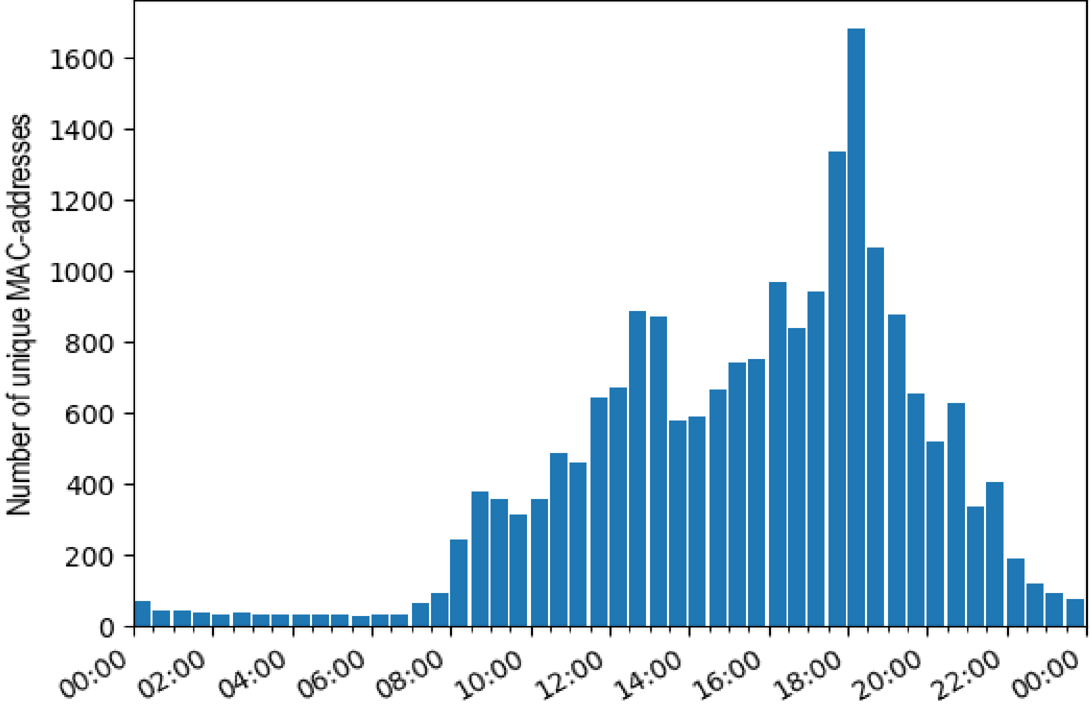
- Preprocessing
  - 1.182.393 probe requests
  - 91.626 unique mac addresses
- Python
  - Delete singletons
  - Filter based on interval or MAC
- Visualization
  - MAC occurrences over time
  - Number of unique MAC over time
  - Market share by vendor ID

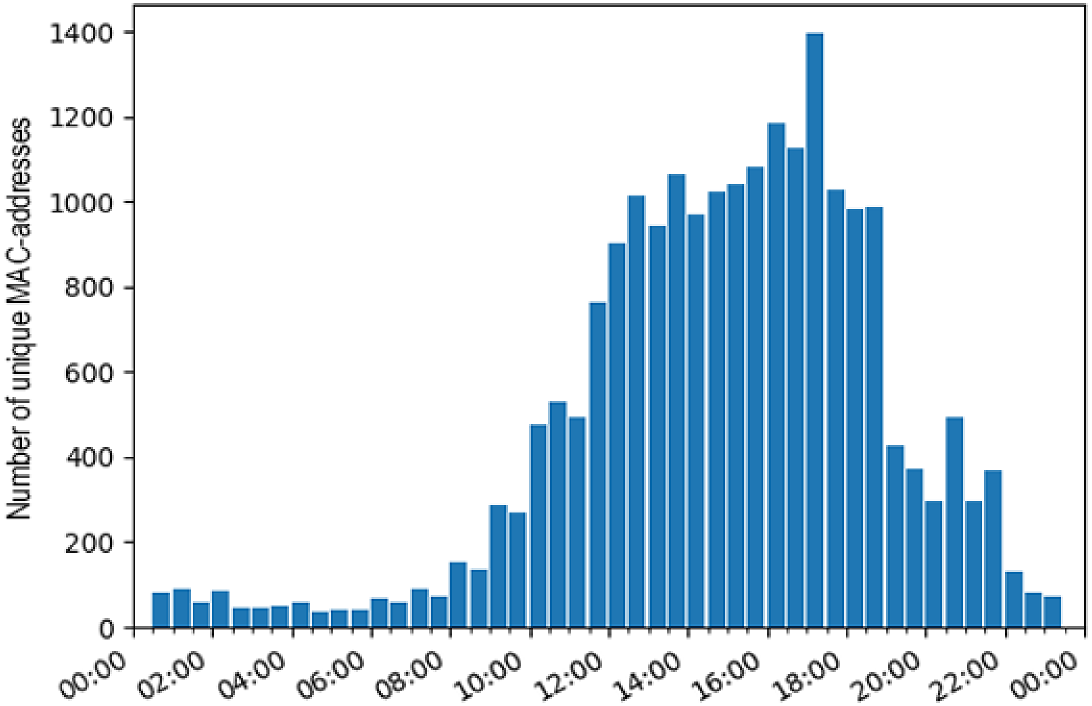
MAC occurrences over time



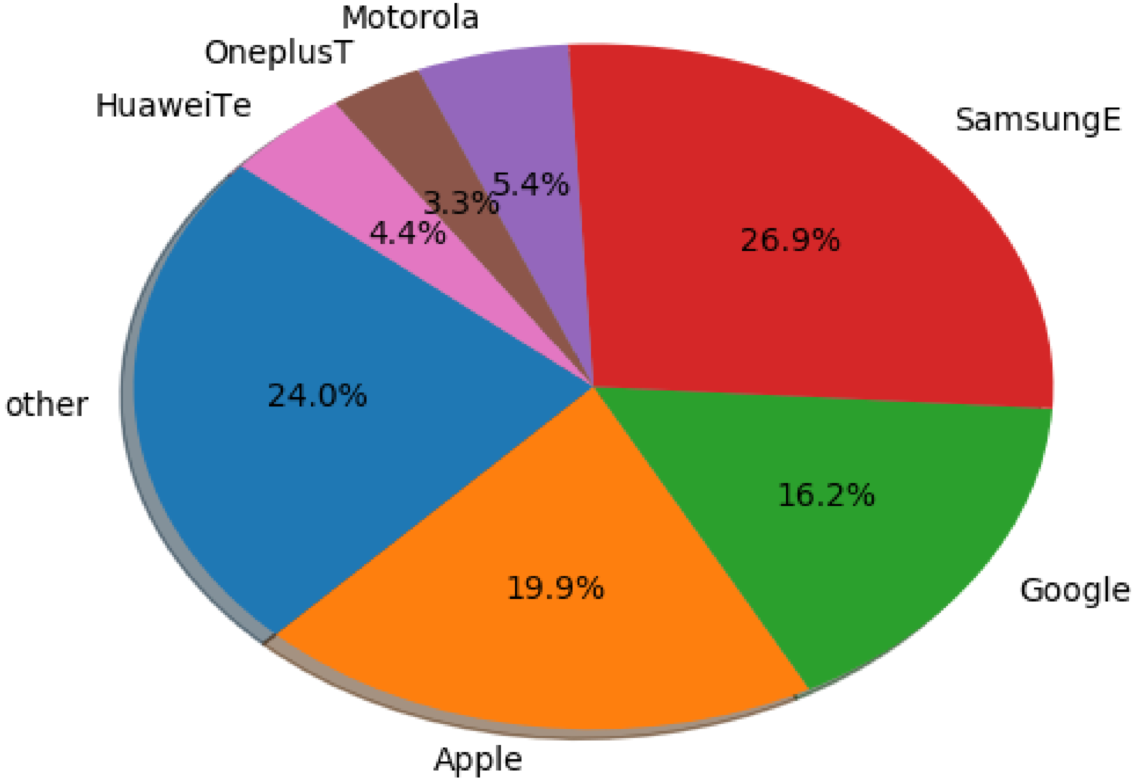
MAC occurrences over time




Number of unique MAC-addresses
0
200
400
600
800
1000
1200
1400
1600
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
00:00


Number of unique MAC-addresses
0
200
400
600
800
1000
1200
1400
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
00:00

Results


Motorola
OneplusT
HuaweiTe
SamsungE
5.4%
3.3%
4.4%
26.9%
other
24.0%
16.2%
19.9%
Google
Apple

QUESTIONS?

https://github.com/NielsHokke/MAC_Tracker