Location Tracking of WIFI Access Point and Bluetooth Devices

SP1 - Student Project

Hegnes, Bjørn Martin

Abstract

This report goes through the vulnerabilities of WIFI and Bluetooth in terms of privacy i.e. location tracking from 3rd parties without the user's knowledge. With the ever-increasing use of WIFI and Bluetooth devices in the daily life of the average citizen, many will own at least one device, if not several, which can be used as tracking devices.

The author wants to show that these technologies are vulnerable to tracking/surveillance without the individual's notice and online connection.

This report will show that it is possible to do not only tracking of a single individual but masstracking/surveillance of a large city as well, i.e Oslo.

This report is the culmination of 5 000 000 logged data points from MAC addresses and WiFi Access Points, which in turn

- generated repeated data points of specific devices that allowed the author to pinpoint movement patterns and habits of several device owners through Oslo, some with their full name on their devices.
- showed density of certain brands
- mapped encrypted and unencrypted WiFi networks in the covered area in Oslo

This was done in 12 days,a shoestring budget (3000 kr) and the technical knowledge about exploiting vulnerabilities in WiFi Access Points and Bluetooth.

The purpose of this report was to show the vulnerability of these technologies to tracking. All logged data and any identifier of any personal information have been deleted by the author after project end. No personal information is presented in this report, with exception of the preface where informed consent has been given.

Content

Preface

This is my final Course Project for the first year of Network and IT-Security at Noroff - School of technology and digital media.

Firstly, I would like to thank my two partners for supporting me through the project, especially in the first weeks of the data gathering period, which almost burned me out. And the brainstorming sessions with my brother.

Secondly, I would like to thank my teacher Mehdi Shadidi for the discussion that we had with another student about location tracking without the person being online. I took this as a challenge to prove to my fellow students that this was possible. He mentioned he used a Tile to find his keys in another setting. This Tile is a Bluetooth tracker device that you can attach to whatever you want. Below in Figure 0 is the result that I have presented for him about how I tracked him because of the keychain tracker, and allows me to present the data.

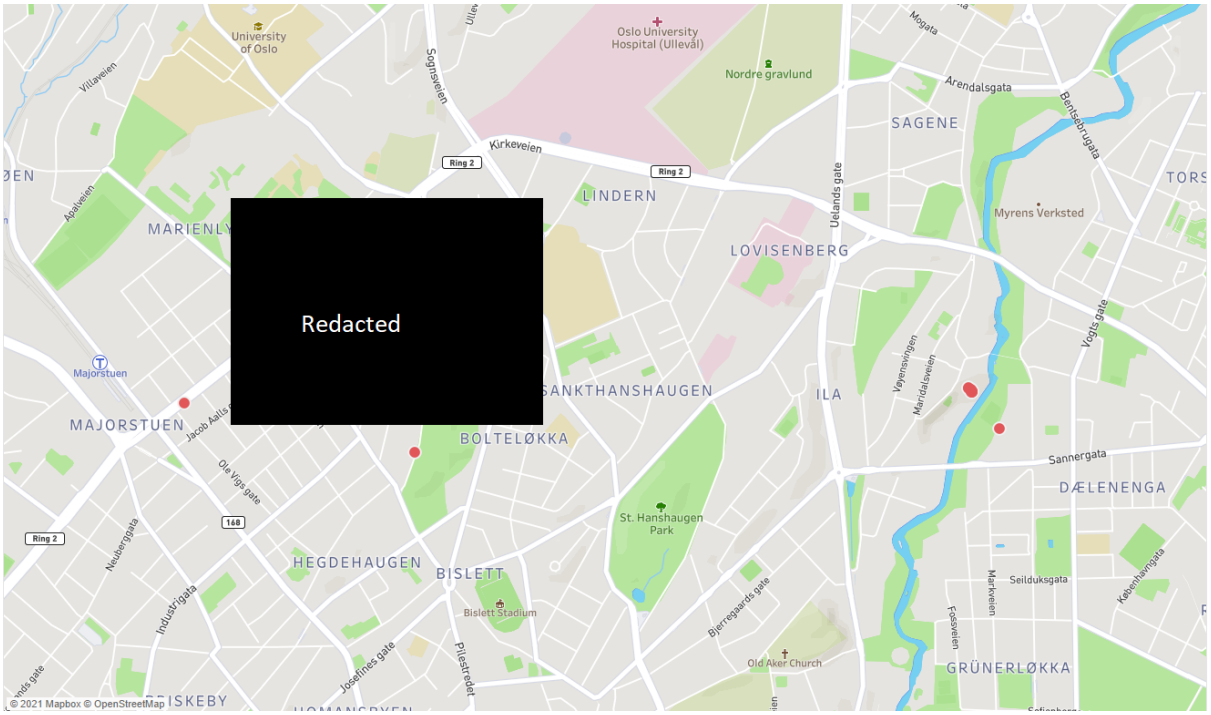


Figure 0. Gotcha. (Author, 2021).

1 - Introduction

In this report, the author will show how it was possible to location track the MAC address of WiFi Access Points and Bluetooth devices that people use in their daily lives without the knowledge of the user.

In the next part of the rapport, the author will explain what a MAC address is, with a visual explanation of what makes a MAC address as well as why a MAC address is unique in a technical explanation.

In the third part, the author will explain how the MAC address is broadcast from a WiFi Access Points and Bluetooth device. This will be explained with visual explanations as well as a technical explanation of what frames are being broadcasted from the wireless devices and where in the frame the MAC addresses are located.

In the fourth part, the author will write about what device has been used in the capture of the MAC address, with a brief tour of the different hardware chosen, and with an explanation of why it is used. In this part of the assignment, the author will also give a runthrough of the detailed configuration of the setup of the MAC address capture device as well as pictures of the device.

In the fifth part, the author will explain how and what data is passing from the raw data set and being present with a data visualization software called Tableau. The data points of the MAC address will be presented in a way that is shown as a colored dot with lines on a map over the location where it has been tracked. It will be a section of different devices and vehicles that has Bluetooth capability. In addition, there will be WiFi Access Points with no and outdated encryptions will be plotted to a map to visualize how many insecure networks there are. More detailed information on how to interpret the visualization will be given where necessary.

In the sixth part, the author will explain what the captured dataset can be used for, with examples of what has already been done by others in real life scenarios, what new methods are possible with examples of similar things done with other technologies. Furthermore, the author will provide an introduction to the inherent threats and dangers that comes with making a big dataset to location track wireless devices, also exemplified with scenarios and examples from real life events.

The last part is the summary of the whole report, as well as the authors' own thoughts and reflections about the student project.

2 - What is MAC

MAC stands for Media Access Control, this is a unique address that is hardware coded to a network interface card (NIC) (Ieee.org, 2021). This address consists of a 48-bit address and is represented by six octets. The first three octets of the MAC address are the OUI, this stands for Organizationally Unique Identifier and consists of a 24-bit number that identifies a vendor, manufacturer, or other organization globally. This OUI is given by the Institute of Electrical and Electronics Engineers (IEEE) Registration Authority to the vendor. The last three octets is a 24-bit value that is assigned by the owner or vendor of the OUI to form the address (Ieee.org, n.d.).

The results are shown below in figure 1, it starts with the OUI on the first three octets and a number that the manufacturer has never used with the OUI before. As a result, every MAC address is unique (Odom, 2014).

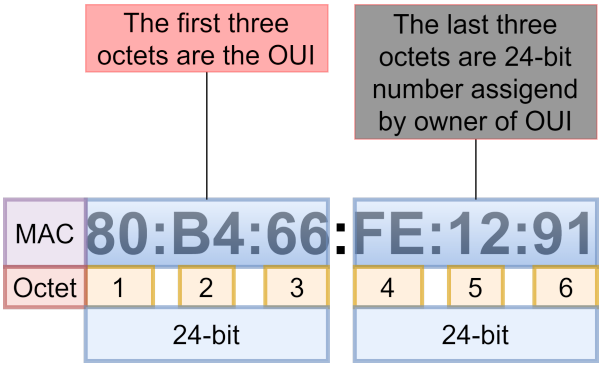


Figure 1. MAC address. (Author, 2021).

The MAC address is a hardware identification number that uniquely identifies each device on a network. The Mac address is manufactured into every network interface card (NIC) such as Ethernet card, WiFi-card, and Bluetooth card making it a physical unique address that cant be changed, unlike a Internet Protocol (IP) address that can be changed since it is a logical address (Techterms.com, 2020).

In the Open Systems Interconnection model (OSI model) a MAC address is in layer 2 also called the data link layer. It is on this layer the senders and the receivers MAC address are attracted to provide reliable transfer of data in between to nodes connected to a physical layer (Odom, 2014).

3 - Wireless MAC broadcast

In this part, the author will explain how a MAC address is broadcast wireless in a WiFi Access Point (AP) and Bluetooth Classic (BT), and Bluetooth Low Energy (BLE).

3.1 - WiFi Access Points

A WiFi Access Points uses the IEEE 802.11 standard, and in this standard, the Beacon frame consists of an 802.11 MAC header called Basic Service Set Identifiers (BSSID), body, and FCS.

The WiFi Access Points's Service set identifier (SSID) name Is not the unique address to the AP. It is the BSSID that has a unique layer 2 MAC address (Engeniustech.com, 2015)

The Beacon frames get broadcasted at certain intervals, and this is how the MAC address or BSSID of the WiFi Access Points gets broadcasted.

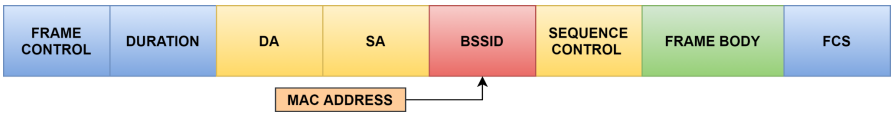


Figure 2. Beacon frame. (Author, 2021).

3.2 - Bluetooth

Bluetooth Classic (BT) uses the IEEE 802.15.1 frame standard and Bluetooth Low Energy (BLE) frame standard.

The IEEE 802.15.1 frame contains Physical Service Data Unit (PSDU) which consists of a MAC header, MAC frame body, payload, and frame check sequence(FCS). It is in the Sender ID under Mac Header where the MAC address is located.

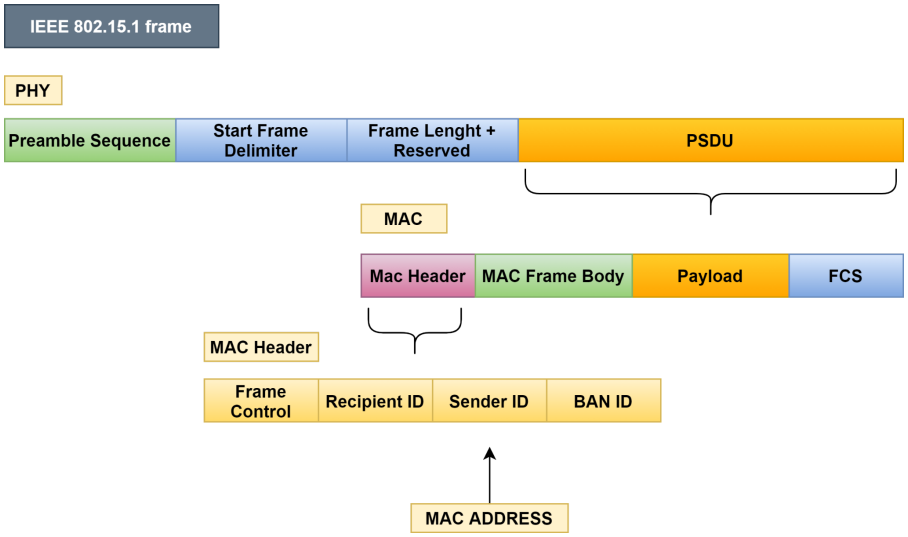


Figure 3. IEEE 802.15.1 frame. (Author, 2021).

The Bluetooth Low Energy (BLE) frame has only one packet format used for both data channel packets and advertising channel packets, In this standard, the MAC address gets sent from the device with a BLE packet, the MAC address is in the Advertising Channel Protocol data unit (PDU), it is in the Payload under Advertising (ADV) Address (Microchipdeveloper.com, 2021).

The ADV Address also called Broadcast address can be a public or random address, the public address is the physical MAC address of the device and random is the randomization of address to keep the device's privacy (Lindh, 2015).

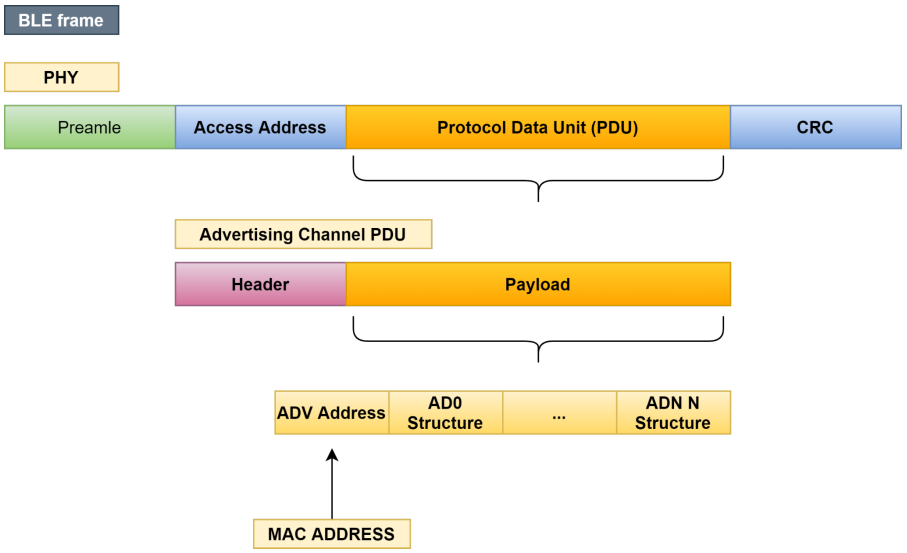


Figure 4. BLE frame. (Author, 2021).

4 - How to capture MAC addresses

In this section, the author will go through the setup of the hardware and software that was used to capture MAC addresses broadcasted from WiFi Access Points and Bluetooth devices for location tracking, step by step. The software that will be used to capture the MAC address is Kismet, his software is a intrusion detection system, wireless network detector for 802.11 and 802.15.1, and it is a sniffer. (Kali.org, 2014)

The device must be:

- Portable
- Have enough processing power to run Kismet..
- Be able to capture WiFi IEEE 802.11 signals broadcasted on 2.4 GHz, 5 GHz frequency band and Bluetooth IEEE 802.15.1 signals broadcasted on 2.402 GHz to 2.48 GHz frequency band.
- Have a USB GPS to get the location.
- Have storage for software(Kismet) that logs MAC addresses with a timestamp and GPS location and SSID.
- Have a reliable power bank that would last 24 hours minimum.

The device shown below in Figure 5 is fully assembled and meets all these criteria.

Figure 65 MAC capture device. (Author, 2021).

4.1 - Hardware

The Hardware chosen for this device in Figure 5 is the following:

Raspberry Pi 4 Model B 8GB is recommended as a good choice for a portable device because it is able to handle running Kismet in a moderate to a busy environment (Kismet, 2021)

DS3231 Mini Hardware clock, since the Raspberry Pi 4 does not come with an internal hardware clock and are relying on the Network Time Protocol, the author did chose to add a hardware clock to keep the time in case of the possibility of not having an internet connection (The Pi Hut, 2015).

SanDisk Micro SD-card 64 GB, was chosen so there will be no need to worry about storage.

Alfa Network AWUS1900, this network adapter was used since the author already had it from before. But in retrospect this specific adapter is not recommended due to unreliability.

LM1010 - Bluetooth v4.0 Dual Mode Long Range USB Adapter, was chosen since it is made for long-range communication and has an SMA connector with the support for external antennas with 9.8dBm power (LM Technologies, 2021). 800 meter unobstructed range, 100 meter range within city center

Omnidirectional wifi antenna 9 dBi. This antenna was chosen to be used with an LM1010 USB adapter to get a longer range.

Globalsat BU-353S4 GPS was chosen since this is one of the brands that are often used in wardriving (see section 4.5) projects that would work without soldering (Hackaday.io, 2021).

iiglo Powerbank 30000 mAh. This power bank was chosen because it will last 48 hours which leaves 1 day power charge in reserve if one forgets to recharge daily. And since the Raspberry Pi 4 needs a 15 watt 3A power supply, this will provide it through the USB-C connector on the power bank.

4.2 - Raspberry Pi Setup

In this section, the author will install and configure all of what is needed to make the capture device. The chosen Operating System (OS) to be installed on the Raspberry Pi 4 is Raspberry Pi OS Lite, this is a lightweight OS without a desktop or GUI and is recommended to be used since it is stable and developed specifically for the Raspberry Pi. This is downloaded directly from the official website (The Raspberry Pi Foundation, 2021).

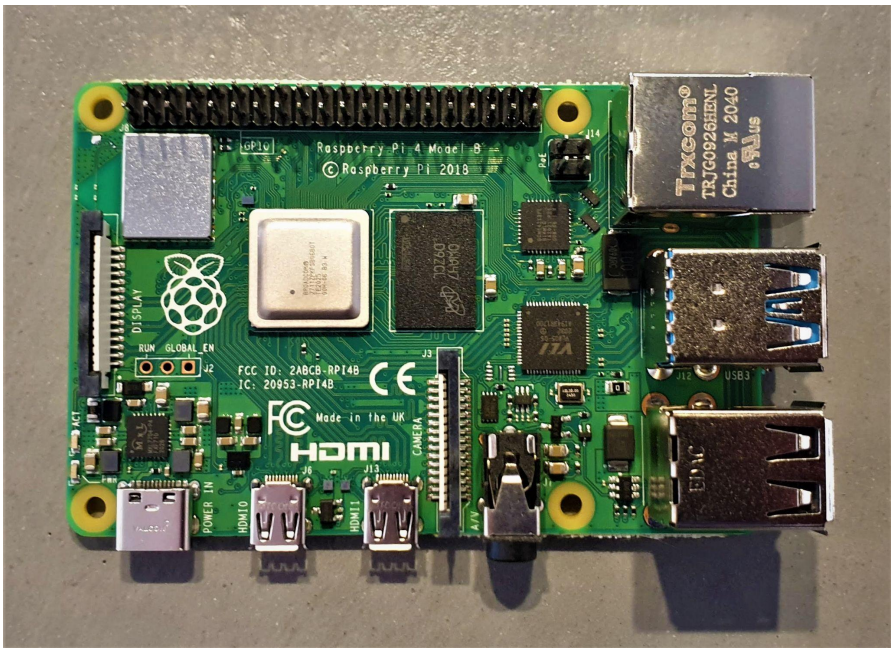


Figure 6. Raspberry Pi 4. (Author, 2021).

To install the OS on the Raspberry Pi it is needed to use a computer and the Raspberry Pi Image software to install the OS onto the microSD-card. The software was also downloadable from the official website. Choose the image, and microSD-card as storage and press write.

Figure 7. Raspberry Pi OS installer. (Author, 2021).

Then it is needed to make an SSH file without any extension or contains any information, this makes it possible to SSH the device without needing to connect it to a monitor or keyboard. This file is placed in the **x:\boot** partition on the micro SD card.

To configure the WiFi to connect to the smartphone hotspot, it needs to place a file **wpa_supplicant.conf** with the configuration below in the **x:\boot** partition on the micro SD card.

```
country=US # Your 2-digit country code
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=netdev
network={
    ssid="YOUR_NETWORK_NAME"
    psk="YOUR_PASSWORD"
    key_mgmt=WPA-PSK
}
```

After that, it was needed to change the password, configure the keyboard layout, the timezone and upgrade the OS by using these commands.

Change Password

```
passwd
```

Upgrade the system

```
sudo apt-get update
sudo apt-get upgrade
```

Set timezone and keyboard

```
sudo raspi-config
```

As explained in 4.1 it is needed to install the hardware clock, since the raspberry pi does not have an internal hardware clock, the hardware clock is DS3231 Mini modul. Place the DS3231 mini on the GPIO as shown in figure

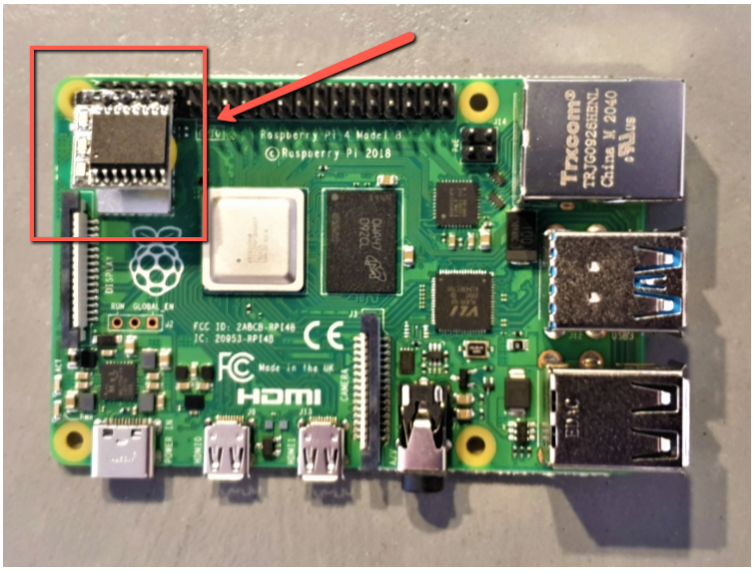


Figure 8. DS3231 mini on the GPIO. (Author, 2021).

then run

```
sudo raspi-config
```

Then chose Interfacing options and press enter

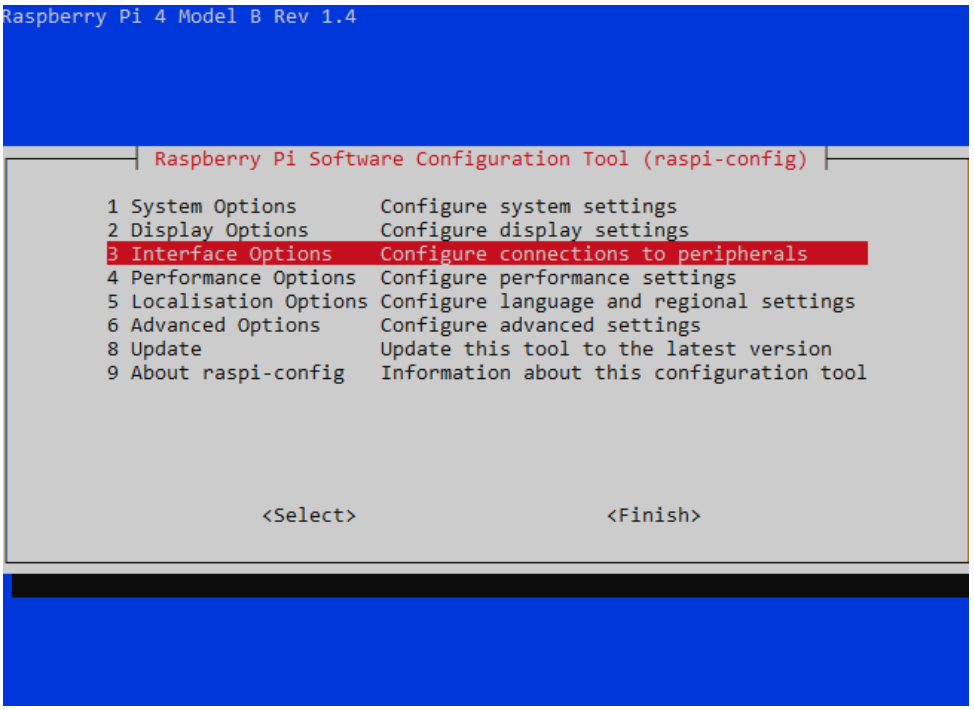


Figure 9. Raspi-config. (Author, 2021).

Then choose I2C and press enter.

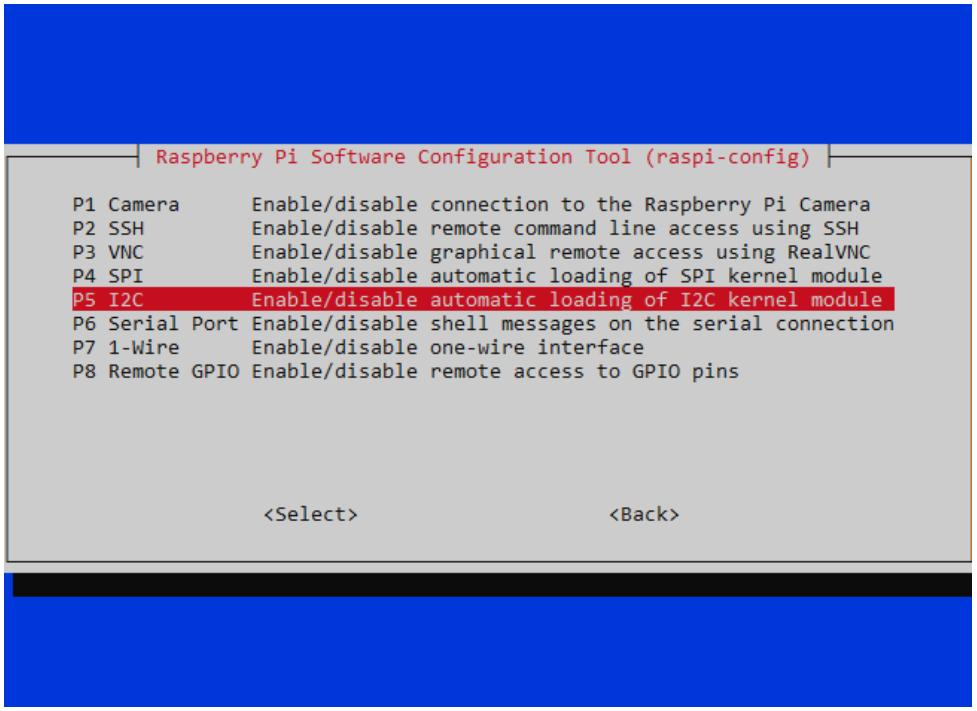


Figure 10. Interface options submenu. (Author, 2021).

Enable ARM I2C Interface.

Reboot by using

```
sudo reboot
```

Install Python SMBUS and I2C

```
sudo apt-get install python-smbus i2c-tools
```

Now it is needed to edit the config.txt in /boot to make the Raspberry Pi use the hardware clock. navigate to **/boot**

Then run

```
sudo nano config.txt
```

Add the config for the ds3231 mini and save.

```
dtoverlay=i2c-rtc,ds3231
```

Reboot by using

```
sudo reboot
```

Remove the fake hardware clock which is already installed.

```
sudo apt-get -y remove fake-hwclocksudo update-rc.d -f fake-hwclock
remove
```

Enable the hardware clock by edit hwclock-set

```
sudo nano /lib/udev/hwclock-set
```

Place **#** in front of the text that is shown in the code box below, and save.

```
#if [ -e /run/systemd/system ] ; then
#
#   exit 0
#
#fi
```

Then it is needed to check if the date and time are right by using the command date, if it is not right connect the Raspberry Pi to the internet.

```
date
```

Write the date to the hardware clock.

```
sudo hwclock -w
```

Afterward, use the command below to read the time on the hardware clock

```
sudo hwclock -r
```

To prevent SSH sessions from being terminated and being able to resume the session a utility called screen is used (Linuxize, 2018).

```
sudo apt-get install screen
```

Then the GPS program GPSD is installed to get the GPS location data from the USB GPS device, this service is monitoring available GPS data available I on TCP port 2947 (Gitlab.io, 2021).

```
sudo apt-get install gpsd gpsd-clients
```

Disable the systemd service the GPSD installed

```
sudo systemctl stop gpsd.socket
sudo systemctl disable gpsd.socket
```

The next step is to install the driver for Alfa Network AWUS1900, to install the drivers it is needed to have git to download from Github, dkms and update the kernel.

Install git and dkms

```
sudo apt-get install git
sudo apt install dkms
```

Update kernel

```
sudo apt-get install raspberrypi-kernel-headers
```

Install driver rtl1900ac

```
git clone https://github.com/aircrack-ng/rtl8814au.git

cd rtl8814au

sed -i 's/CONFIG_PLATFORM_I386_PC = y/CONFIG_PLATFORM_I386_PC = n/g'
Makefile

sed -i 's/CONFIG_PLATFORM_ARM_RPI = n/CONFIG_PLATFORM_ARM_RPI = y/g'
Makefile

export ARCH=arm
sed -i 's/^MAKE="/MAKE="ARCH=arm\ /' dkms.conf
```

```
sudo make dkms_install
```

Then it is time to install the software to capture all of the MAC addresses, this program is called Kismet.

```
wget -O - https://www.kismetwireless.net/repos/kismet-release.gpg.key |
sudo apt-key add -

echo 'deb https://www.kismetwireless.net/repos/apt/release/buster buster
main' | sudo tee /etc/apt/sources.list.d/kismet.list

sudo apt update
sudo apt install kismet
```

Enable GPS in kismet by configure the kismet.conf

```
sudo nano /etc/kismet/kismet.conf
```

Uncheck **#** / delete **#** infront of

```
gps=gpsd:host=localhost,port=2947,reconnect=true
```

4.4 - Start Capture

In this section, the author will show how the data is captured with the Raspberry Pi.

To start it is needed to start to enable WiFi Hotspot on the smartphone, power on the Raspberry Pi, use SSH app to connect to the Raspberry Pi

When the SSH session is established it is needed to run the screen command to prevent the SSH session from being terminated when the smartphone is disconnected and be able to reconnect the SSH session using the screen -r command.

Start Screen

```
screen
```

Start GPS

```
sudo gpsd /dev/ttyUSB0 -F /var/run/gpsd.sock
```

Start Kismet with the **-p** option to choose the path to save the captured data.

```
sudo kismet -p /home/pi/wardrive
```

Then it is needed to navigate to the Kismet WebUI and set the login and password, this is something that has to be done the first time using Kismet. This is the Raspberry Pi IP address with port 2501.

```
http://192.168.43.194:2501/
```

After that, the author chose to enable the data source hci0 and wlan1 to capture data and have wlan0 reserved for connecting the raspberry pi to the smartphone, and have the possibility to use SSH and the KIsmet WebUI when needed.

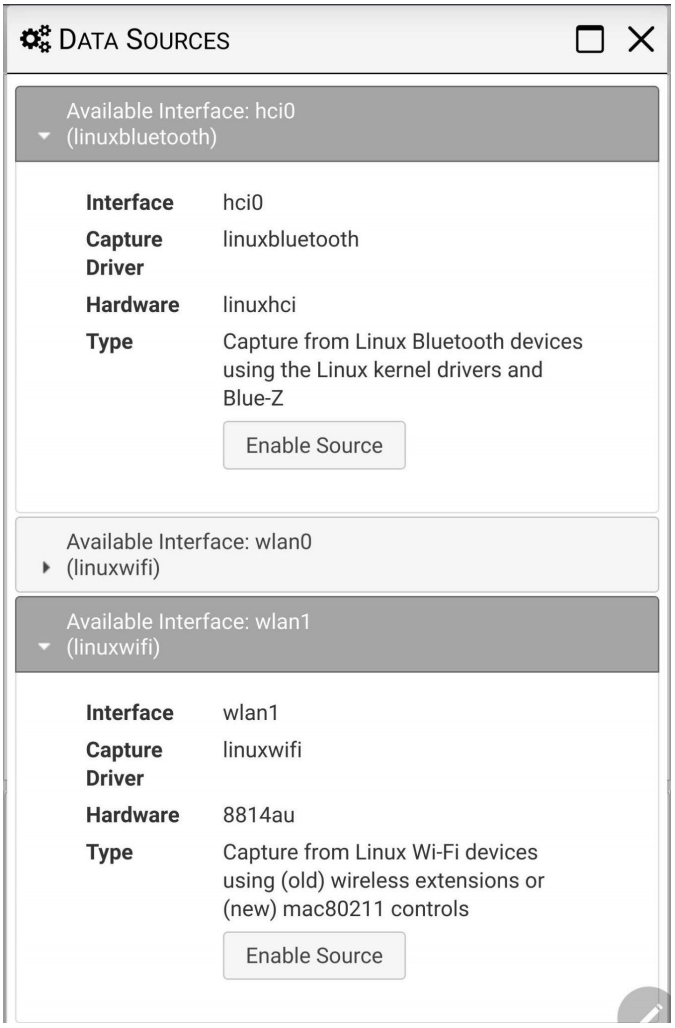


Figure 11. Kismet WebUI - datasource. (Author, 2021)

4.5 - Operation Wardrive 07.04.2021-19.04.2021

Operation Wardrive was the nickname the author called the period of data gathering. It is derived from word wardriving.

Wardriving is the act of searching for wireless networks, usually driving a vehicle to discover and logg the wireless networks using a laptop or smartphone with a proper software to log the information about the wireless network with its GPS location. (Hurley and Ebrary, 2004, p.19) The term comes from Wardailing that was introduced to the general public through the cult classic WarGames in 1983.(Hurley and Ebrary, 2004, p.18)

Wardriving is not trying to get unauthorized access to wireless networks (hacking), while wardriving may be seen as logging publicly available information. The information gathered over a longer span can track the movement of an individual's habits and can therefore identify who the MAC address belongs to, for this reason MAC address is considered personal data.

In this project, no car was used, only a regular bike and the author's own two legs. Twelve days (07.04.2021-19.04.2021) were allocated to “Operation Wardrive”, which consisted of moving through different parts of Oslo city within Ring 3 and covering as much area as possible in twelve days. The result is below in Figure 12, this is the data from gps logged from 12 days of moving around in Oslo.

The entire route was 300 km and coupled with a tracking range of the system, 100 meter, that resulted in 30km^2 having been tracked and logged by the authors device .

As a comparison, Oslo excluding Marka, is 154 km^2.

This method coveredthe equivalent of 1/5th of Oslo’s total surface area.

See Figure 12 for the whole rute the author did cover, it is the raw data gpx files from 12 days that have been combined to visualise how much the city has been covered.

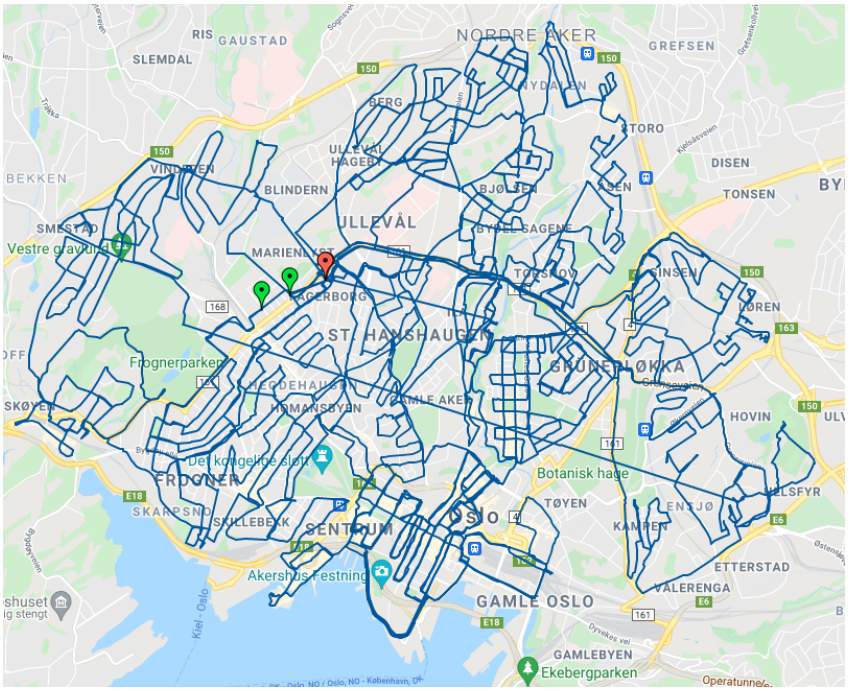


Figure 12.Operation Wardriving In Oslo. (Author, 2021).

To make it more manageable and have a structure during wardriving, the author divided up the city in parts as shown in Figure 13. This made it easier planning the routes to avoid passing through the one area more than necessary.

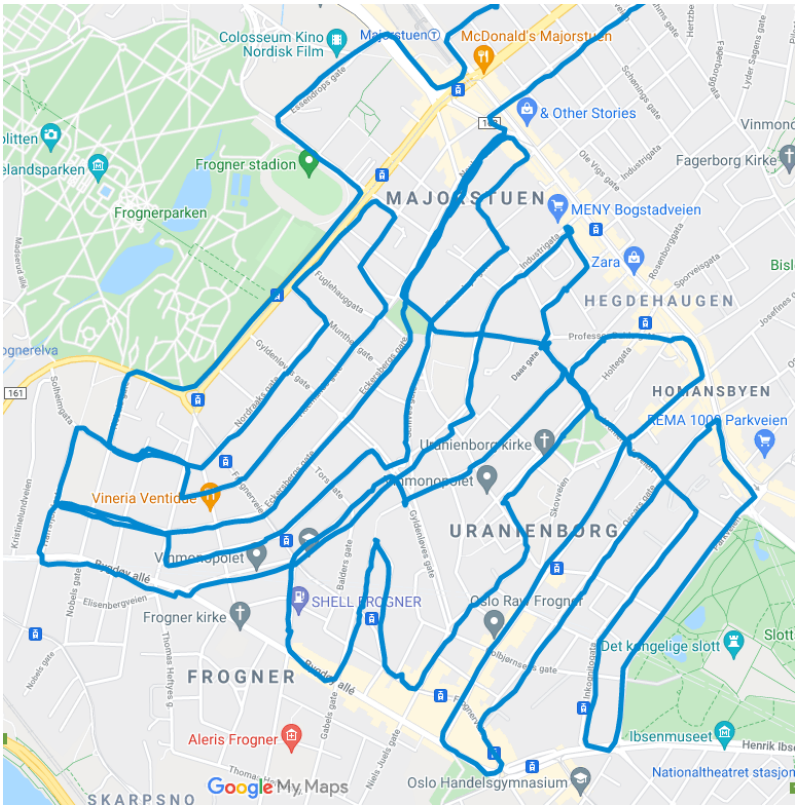


Figure 13. Wardriving Section. (Author, 2021).

After twelve days and 300km (30 km^2), the author accumulated 6GB of data. It may contain every information there is about the captured device, such as connected clients to a WiFi Access Points, captured packages, MAC, SSID, Handshakes, and more.

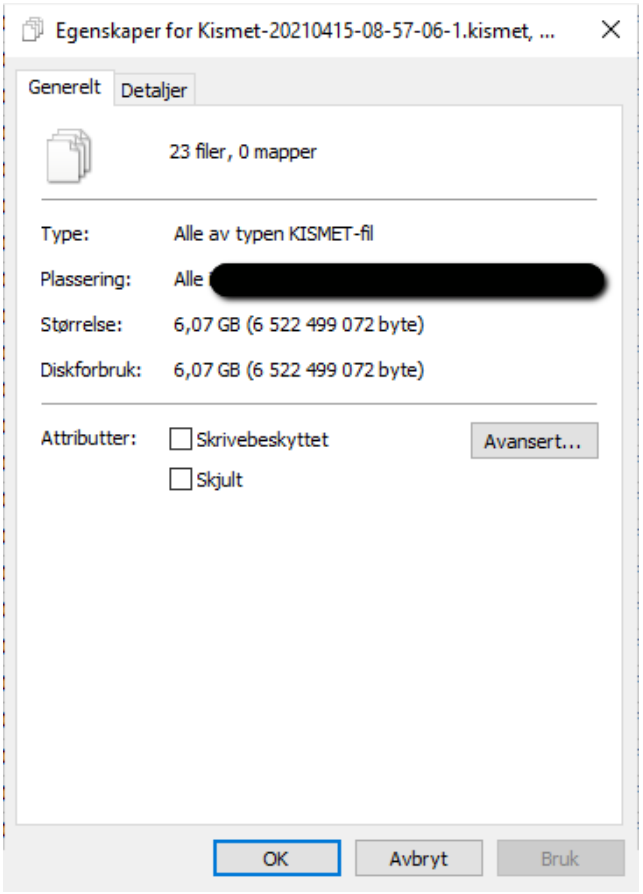


Figure 14. Accumulated data. (Author, 2021).

5 - Data Visualisation

In this section the author will present the date with the use of the data visualisation software called Tableau. The data visualised here will be the data captured during wardriving through Oslo plus a separate dataset that the author has captured with its smartphone 5 months prior to “Operation Wardrive”. This dataset can be seen in the figures that show tracked data outside of Oslo.

Figure 15. Raw data to Tableau. (Author, 2021).

The selected data that will be parsing from the raw kismet data file from each device captured will be the following MAC, SSID, AuthMode, FirstSeen, Channel, RSSI, CurrentLatitude, CurrentLongitude, AltitudeMeters, Accuracy Meters, Type. This data will be exported as a ***.csv** file that will have all of the mentioned above as columns and all of the devices as rows as shown in Figure 16 below.

	A	B	C	D	E	F	G	H	I	J	K
1	MAC	SSID	AuthMode	FirstSeen	Channe	RSSI	CurrentLatitude	CurrentLong	AltitudeMet	AccuracyMeters	Type
2	A0:39:EE:	[redacted]	[WPA2-PSK-CCMP][ESS]	09.04.2021 10:57	36	-89	59.9373092651	10.72280502	14.024000	0	WIFI
3	44:AD:B1		[WPA2-PSK-CCMP][ESS]	09.04.2021 10:57	100	-86	59.9373092651	10.72280502	14.024000	0	WIFI
4	80:F5:03:		[WPA2-PSK-CCMP][ESS]	09.04.2021 10:58	36	-87	59.9373092651	10.72280502	14.024000	0	WIFI
5	CC:40:D0		[WPA2-PSK-CCMP][ESS]	09.04.2021 10:58	36	-89	59.9373092651	10.72280502	14.024000	0	WIFI
6	4C:9E:FF:		[WPA2-PSK-CCMP][ESS]	09.04.2021 10:58	100	-91	59.9373092651	10.72280502	14.024000	0	WIFI
7	28:28:5D:		[WPA2-PSK-CCMP][ESS]	09.04.2021 10:57	60	-77	59.9373092651	10.72280502	14.024000	0	WIFI
8	28:9E:FC:		[WPA2-PSK-CCMP][ESS]	09.04.2021 10:58	60	-86	59.9373092651	10.72280502	14.024000	0	WIFI
9	40:B0:76:		[WPA2-PSK-CCMP][ESS]	09.04.2021 10:58	60	-89	59.9373092651	10.72280502	14.024000	0	WIFI
10	28:28:5D:		[WPA2-PSK-CCMP][ESS]	09.04.2021 10:57	64	-79	59.9373092651	10.72280502	14.024000	0	WIFI

Figure 16. Parsed data. (Author, 2021).

The MAC data will be visualised with a colored dot on a map, and if the MAC has several data points there will be drawn a line in between them to see the movement as shown in Figure 17.

5.1 - BT: Vehicle

In figure 17 and 18, are all of the vehicles with the SSID that are identifiable as a Car brand such as Tesla, Volswagen, Audi and so on that have a smart device with Bluetooth. Also older cars were able to be tracked also, because of the PURE Highway DAB that many car owners have installed in their car to get DAB radio, this also has a Bluetooth capability that makes it possible to track. In addition, Figure 17 shows how a bus that the author was on also was tracked because of the bus Garmin DriveSmart GPS has Bluetooth capability.

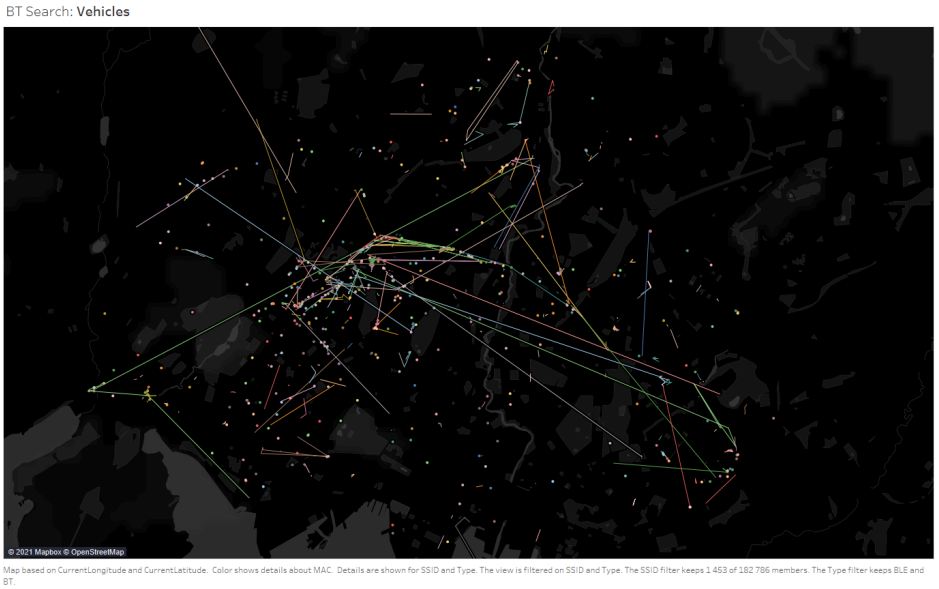


Figure 17. Vehicles in Oslo. (Author, 2021).

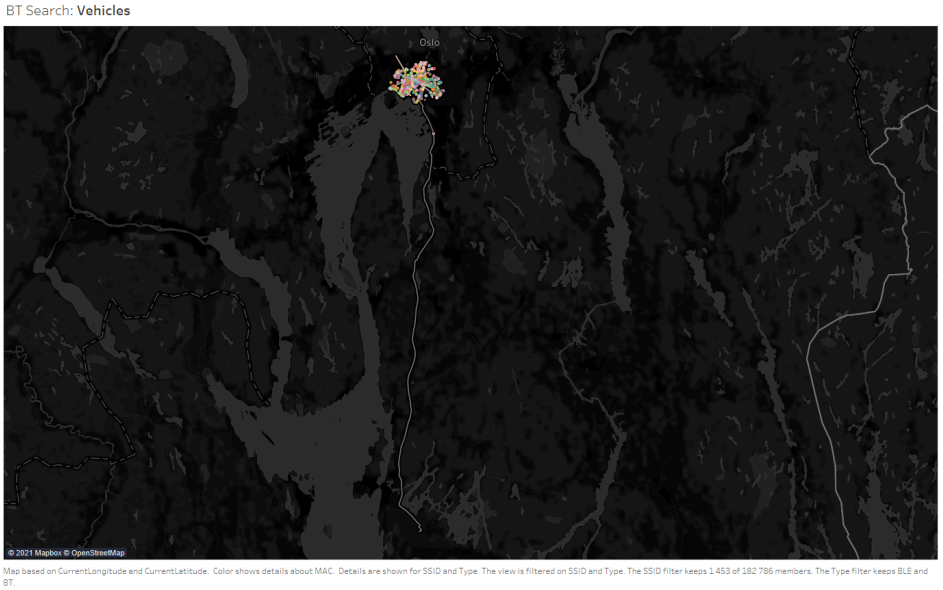


Figure 18. Vehicles in Oslo and Østfold. (Author, 2021).

5.2 - BT: Smartphones

In Figure 19 and 20 are the Smartphones in Oslo that were tracked. It shows that devices are tracked by their SSID suchs as iPhone, Note 9, Huawei p20, and the devices that have several data points will be matched by their MAC address to form a line to show the devices movement. Many of the smartphones may not show up due to SSID being something else, not broadcasting or the use of MAC randomization. MAC randomization is for increasing the user privacy and prevents tracking technologies to connect several data points to one MAC address and monitoring movements (Android Open Source Project, 2021).

Figure 19. Smartphones in Oslo. (Author, 2021).

Figure 20. Smartphones in Oslo and Østfold. (Author, 2021).

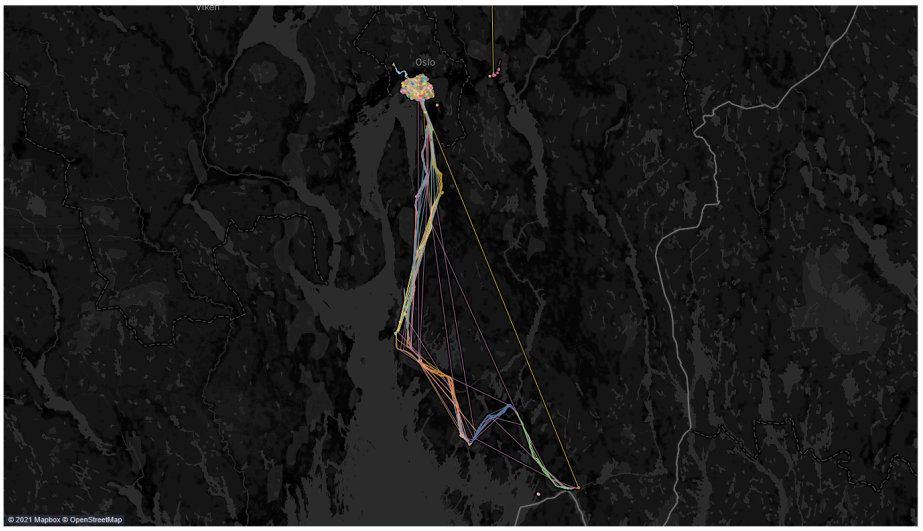
5.3 - BT: Headset

When filtering SSID for everything that is a Bluetooth headset such as: Beoplay, Bose, Jabra and more the result as shown in figure 21 to 24. It shows how the author has tracked a user of a Bluetooth headset over a long distance. By the look of it, it seems that it is easier to track movements of individuals by their headset rather than their smartphones, and another reason for this possibly being the best way to track to track a individual is since headset do not use MAC randomization, see figure 19 and 20 for comparison.

Figure 21. Headset in Oslo. (Author, 2021).

Figure 22. Headset in Oslo zoomed out. (Author, 2021).

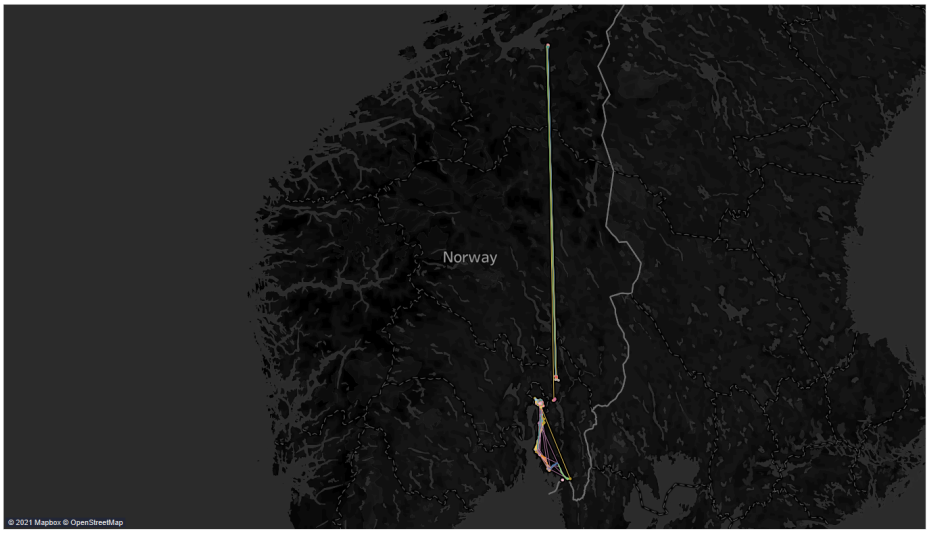
BT: Headset



Map based on CurrentLongitude and CurrentLatitude. Color shows details about MAC. Details are shown for SSID, Type and AccuracyMeters. The view is filtered on SSID and Type. The SSID filter keeps 863 of 182 786 members. The Type filter keeps BLE and BT.

Figure 23. Headset in Oslo and Østfold. (Author, 2021).

BT: Headset



Map based on CurrentLongitude and CurrentLatitude. Color shows details about MAC. Details are shown for SSID, Type and AccuracyMeters. The view is filtered on SSID and Type. The SSID filter keeps 863 of 182 786 members. The Type filter keeps BLE and BT.

Figure 24. Headset in Norway. (Author, 2021).

5.4 - BT: Wearable Technology

With the increase of wearable technology such as fitness trackers that monitor the individual's health statistics and smart watches, it shows how they can be tracked because of the bluetooth capability of wearable technology. Below in figure 25 to 27 shows SSID that has Honor watch, Huawei band, Huawei watch, vîvoactive and all of the model names of activity trackers and smart watches.

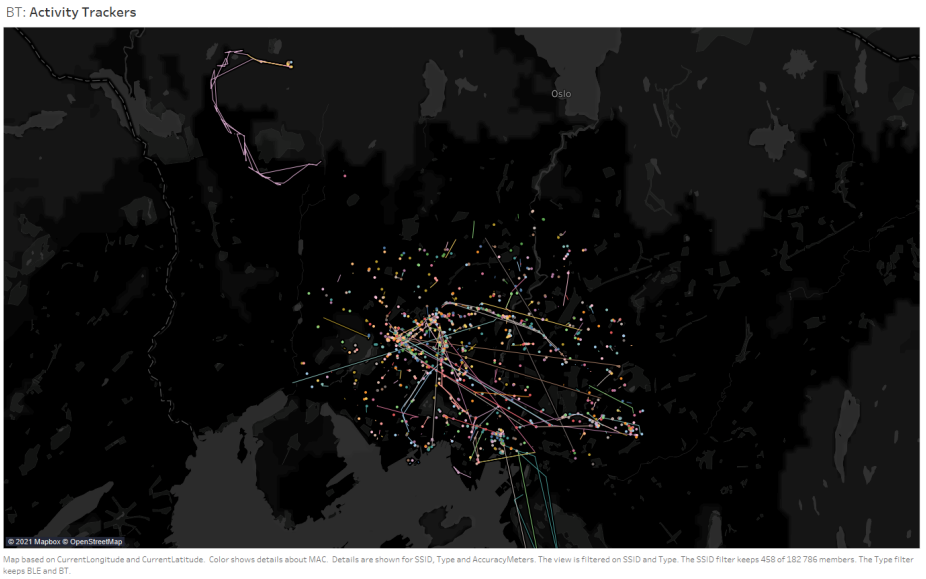


Figure 25. Activity trackers in Oslo. (Author, 2021).

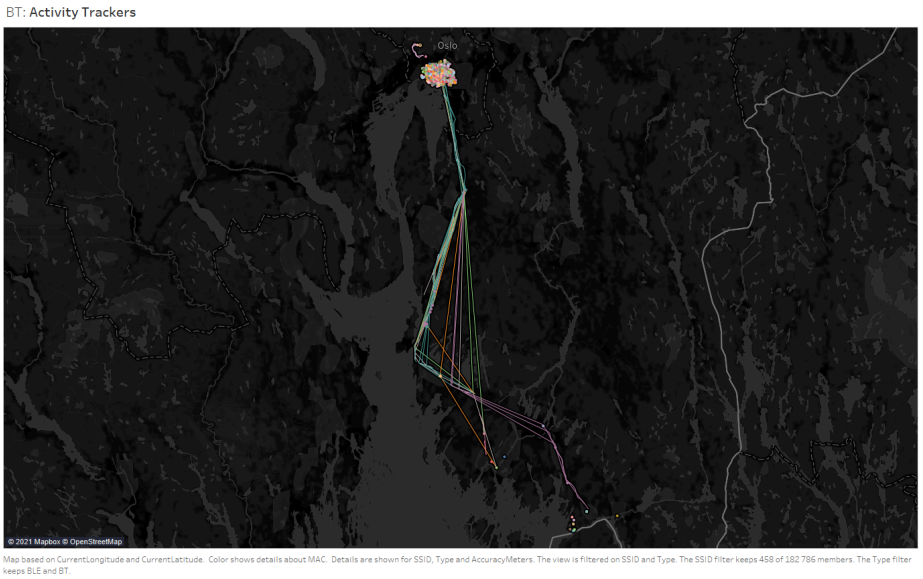


Figure 26. Activity trackers in Oslo and Østfold. (Author, 2021).

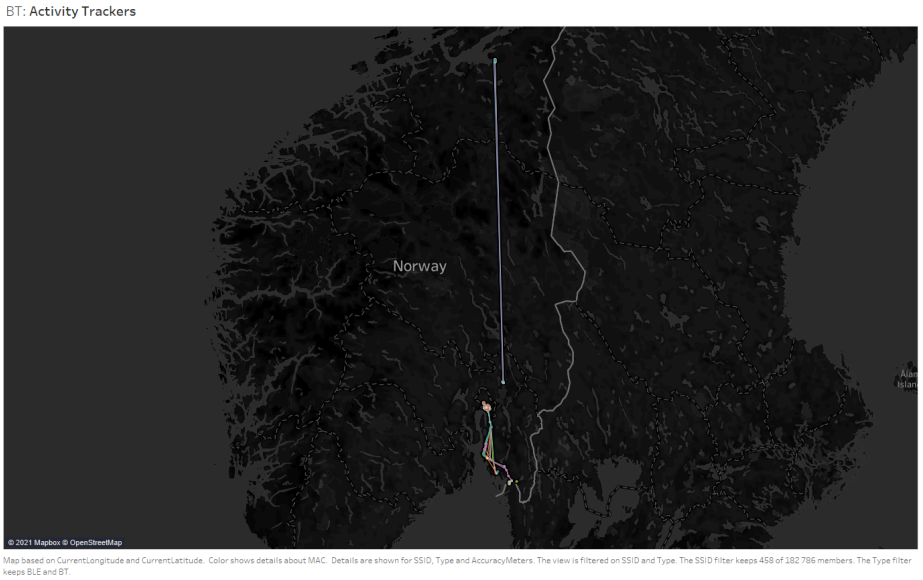


Figure 27. Activity trackers in Norway. (Author, 2021).

5.5 - BT: Real-time tracking terminal

There are also findings of real-time tracking terminal plugs on cars, as the information on the website say it is often used for courier delivery service, car rental and leasing. But one should not rule out the possibility that it also can be a tracking device unknown to the customer. See section 6

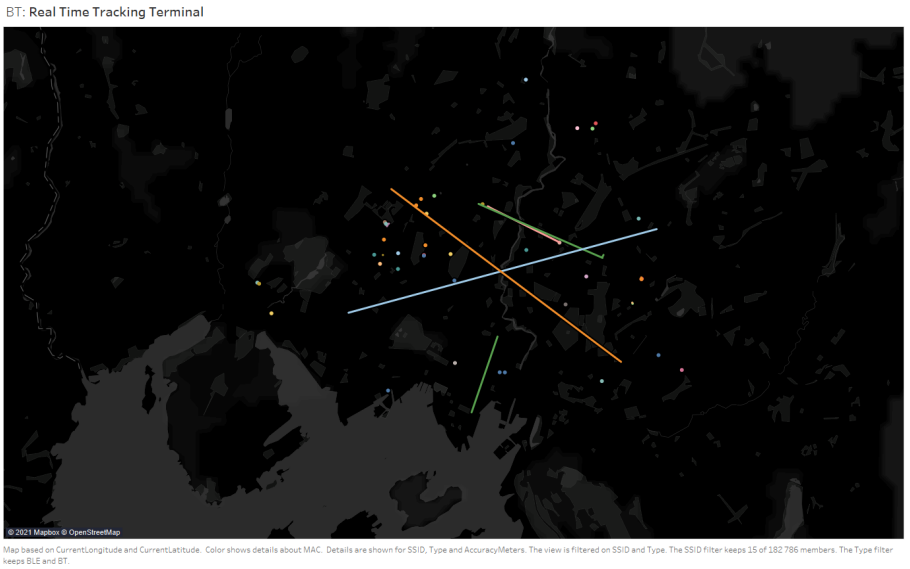


Figure 28. Real-time tracking terminal plugs in Oslo. (Author, 2021).

5.6 - BT: TV’s

It is also possible to track TVs, the figure 29 shows geographically what brand model and type of TV is popular in that area. see section 6 .

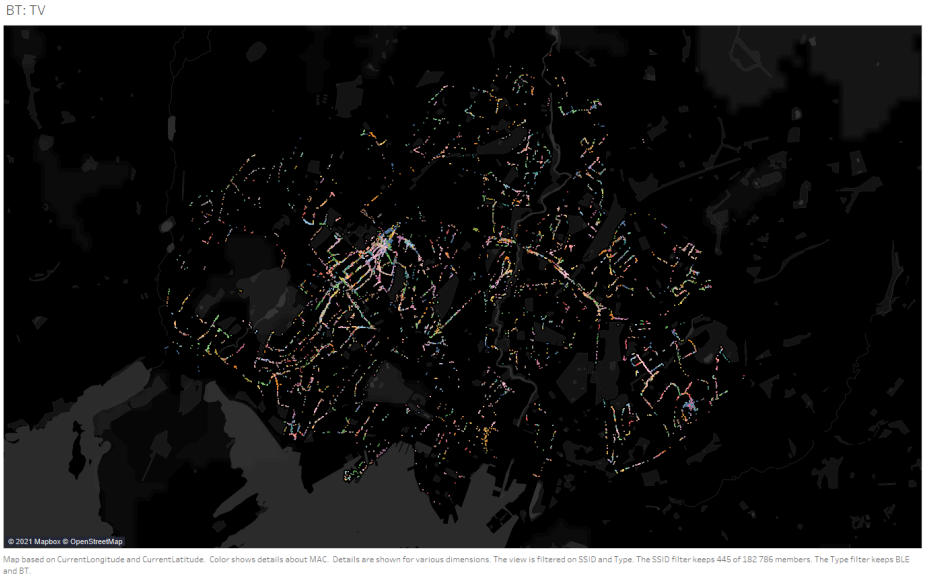


Figure 29. TV’s in Oslo. (Author, 2021).

5.7 - WiFi Access Points encryption

The total scanned and logged WiFi Access Points in Oslo is 2 917 870, 5.84% do not have encryption enabled, 0.25% have WEP, 0.13% have RSN, 7.78% have WPA and 86.40% have WPA2 enabled. In total 13.60% have no or outdated encryption.

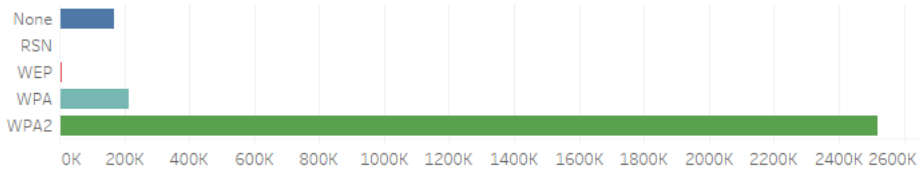


Figure 30. Encryption Protocol usage. (Author, 2021).

5.8 - WiFi: No Encryption

As shown below in Figure 31, although 5% does not sound like much the visual explanation of the date shows there is an unsecured network at every street the author has moved through with the tracking device.

Figure 31. Open networks in Oslo. (Author, 2021).

5.9 - WiFi: WEP

And even 0.25% of the WiFi Access Points have Wired Equivalent Privacy (WEP) , that's still 7155 networks that have very weak security. By using the aircrack-ng tool it is possible to crack the WEP keys in minutes (Bitforestinfo.com, 2017). The different attacks are FMS, KoreK, Chopchop, and PTW. The PTW attack only needs about 35 000 to 40 000 packets to have a success rate of 50% to crack the WiFi network, the amount of packages can easily be collected in the span of 60 seconds (Tews and Beck, 2020). There is found one business that uses this outdated encryption.

Figure 32. WEP networks in Oslo. (Author, 2021).

5.10 - WiFi: WPA

While WPA is more secure than WEP it is still an outdated encryption that should not be used. Since it is vulnerable to Key Reinstallation Attack (KRACK), this attack involves in reusing a one-time key that is given during the four-way handshake when connecting to the WiFi network, this is possible since that the attackers force the AP to install the same encryption key (Lomas, 2017) And makes the attacker able to decrypt all of the date the victim's smartphones, laptops, and tablets that transmits (Krackattacks.com, 2017). This means that a lot of personal details or classified information can be exposed. In the dataset, there are two Accounting Firms found to be using the WPA encryption for their WiFi networks.

Figure 33. WPA networks in Oslo. (Author, 2021).

6 - What can the dataset be used for?

Section 4 and 5 showed how easy it was to mass-collect data of a whole city in a small amount of time with what can be assumed to be quite little effort compared to other intelligence gathering methods.

Tracking technology is already in use by businesses in public spaces to gather data, as the data can be used for their commercial interest. These public spaces include shopping centers, shops, streets, public transportation and entertainment venues.(Datatilsynet, 2016.)

There are already companies that use tracking technology to make an estimate for the waiting time in an airport security line. For example, in the Helsinki airport they are using a queuing time measurement system that is based on Bluetooth, where they captures the Bluetooth MAC address from passengers' smartphones (Finavia.fi, 2017). Oslo Airport is using WiFi tracking to calculate the waiting time in the security queue, in the way that they use WiFi access points before and after the security desk to calculate the average time the individuals are moving in between them (Datatilsynet, 2016.)

Bluetooth tracking has also been used to calculate how many there are in the line at the traffic light by counting how many signals or MAC addresses there are from the smartphones. By changing traffic lights depending on signal density, the aim is to keep traffic flow more efficient than a system that changes traffic lights on fixed time intervals.The system can also calculate how long time the travel time between two or more sensors, as well as how much of the traffic either turn left or right (Roald Ramsdal, 2013)

In Norway, road development company Nye Veier (New Roads), have started to register the passing of Bluetooth MAC address for several sections on public roads Nye Veier will use the the information gathering system CitySense to collect and and analyse the traffic, it will be used to analyse the average travel time from hour to hour and from day to day (Bjørn Atle Gildestad, 2020).

In Sweden Västerås CitySamverkan, the company Bumbee Labs was using WiFi tracking to map the movements of individuals. The Purpose was to collect the MAC address to make a statistic of how many people were visiting the city core (admin, 2015) (Datatilsynet, 2016.).

In Enschede, Netherlands, there were several sensors set up to collect WiFi MAC addresses to track individuals and see what movement they had around the city, to analyse where they used most of the time and how often they did return (Themayor, 2018).

In stores, there are Bluetooth beacons that broadcast one-way messages to smartphones that are nearby, one of the beacons is called iBeacon. Some of the features of this beacon it can welcome customers, provide directions inside of the store, provide promotion and ongoing offers when walking past the beacon. (Beaconstac, 2013) This will work as long as the individual has installed an app on the phone that recognizes the beacons. Companies that specialise in location data encourage app developers to give them personal information, such as email address, name and MAC address (Kwet, 2021).

And with the use of a ESP8266 microchip it is possible to make a tracking device that will notify the user when a device is nearby for the cost of 10 NOK. Which can give the user a notification if the individual that is being tracked is at a location or not (Kody, 2018).

Another example is the ability to use geolocation mapping of the MAC address for devices to find out how many devices there are of a brand, such as TV's. In the figure 29 in section 5.6 the author mapped all of the smart tv's that were in the range of MAC capture devices, this was possible since all of the new smart TV's have Bluetooth capability. Using this method makes it possible to see the device density of brands, this method may be faster and more accurate than using surveys to get the same result.

This method of MAC address location tracking can be used to find stolen smartphones, laptops, smart TV, desktop, broadband router, smart refrigerators or any other device that broadcasts a MAC address. In Iowa the police officer David Schwindt has developed the sniffing software Latent analysis of 802.11 Network Traffic (L8NT), this software was made to help the police to find stolen electronic devices. How it works is that the sender ID is stripped from the MAC Header in the PDSU (see section 3.2) and compared to the MAC address that is in the L8NT database, if the MAC address is not in the database it will be ignored. If there is a coalition with a MAC address located in the database there will be a notification (Khandelwal, 2015). The limitation in L8NT is that it wont detect devices have their wireless ability turned off or if the device is turned off, furthermore the owners of the devices have to know how to find their MAC address. Still there are advantages to using this method than using tracking software since it software is easily deleted when the device is factory reset and a MAC address is a physical address that won't change(Hermiston, 2015).

But this technology can also be used in a malevolent way. MAC tracking can be used by anyone, this comes in addition to the use of GPS trackers in terms of location tracking. As a mechanic in Australia did find out during a routine service of the car, it turns out the ex boyfriend did install a GPS tracker underneath her car (NewsComAu, 2021). As for the most common hiding place for such trackers are underside of the vehicle, under the hood of the hood of the, and the diagnostic port. The diagnostic port/OBD II is a good place to see if the vehicle has a tracking device, see figure 34 (Gpstechnologies.com, 2021).

Figure 34. ODBII port. (derek, 2021).

In figure 28 located in section 5.5, show the use of a GPS tracking device that is connected to a diagnostic port. This device is called Teltonika Vehicle Tracker, it is advertised as plug and track real time tracking terminal. It is small and easy to plug into the diagnostic port on the vehicle and it has GNSS, GSM and Bluetooth connectivity. And is made to location track remote vehicles such as, fleet management, car rental and for personal cars. (Dallinger, 2018).

The examples above about the GPS tracking of an ex-girlfriend is one of the unwanted forms of location tracking of MAC addresses that can be used for. By having more and more electronic devices that broadcast a MAC address, it can be used to track down individuals that are in the address confidentiality program. This program allows individuals that are victims of stalking, sexualt assult, domestic violence or other crimes able to get a confidential address to keep their real address hidden (Merlino, 2019). As for an example, if the perpetrator has a MAC address for the smart TV or WiFI Access point, and these devices are not changed it is possible to pinpoint where the individual lives.

After the leaking of highly confidential NSA documents by the whistleblower Edward Snowden in the USA, there were a lot of different surveillance programs that the public and even the Congress did not know about (Burrough, Ellison and Andrews, 2014). One of the capabilities of one of the NSA surveillance programs, was the ability to location track every movement of the population of a city by tracking their MAC address, this is the unique address that all devices have, this was mentioned in section 2 (Bamford, 2020).

Due to the strict data protection and privacy laws in Norway, it is unlikely this type of surveillance program is done by a government agency of the Norwegian state. The Norwegian Data Protection Authority (DPA) is an independent body and public authority that is setup to protect individual right to privacy.

The DPA have made guidelines for the use of this tracking technology based on WiFi and Bluetooth. Guidelines statestracking can only occur after consent is given from the individual, it has to be made clear how the tracking is done, who is tracking and the purpose of the tracking and if the tracking involves physical movements of the individual(Datatilsynet, 2016.).

Before starting tracking, a clearly defined purpose of the collected data is necessary. The collected data can only be used for this purpose and not for other intentions/purposes. Collecting more personal data that is necessary and relevant is also unlawful. The user collecting tracking information must have oversight on how the data is processed, and can not share the information to others without the consent of the individual (Datatilsynet, 2016.)
.
Locations where tracking technologies can disclose a person's personal health, political views, religious beliefs and sexual orientations are not allowed by law. For physical tracking of a location, it is needed to have information near the tracker to state that the location is being tracked by who, why and the purpose of the data gathering. And lastly DPA must be notified if location tracking technologies are being used in a certain location (Datatilsynet, 2016.).

However, a clearly defined purpose might still be not enough to avoid less savory use of tracked devices.

Example:
If a location has location tracking where the purpose is counting the different types of smartphones that go through that area and the tracking period is over a time period, any device that goes through that area repeatedly will give off data points. With enough data points, a pattern may become apparent for example when a specific device shows up repeatedly in the tracked area. (AP NEWS, 2021).

While DPA guidelines state that collected data can only be used for one clearly defined purpose, possible patterns emerging from single device data points may reveal movement patterns and habits of the device owner, or if scaled up, the movement patterns of the device owners in an area.

This is one of the reasons why MAC addresses are classified as personal data by Datatilsynet (Datatilsynet, 2016.).

Tracking technologies can be also used by foreign government agencies on Norwegian soil, to find out compromised information about an individual by tracking them in controversial locations that may be used for blackmail purposes. For example, it has been stated by the Norwegian Police Security Service (PST) that the Russian military intelligence agency GRU, was likely behind the cyber breach that affected the Norwegian parliament's email system in 2020. (Olsen, 2021). PST states more specifically that the hacker group called Fancy Bear, which is a part of GRU, was behind the targeted attack against the Parliament which in turn was a part of a much bigger operation from Fancy Bear. The Parliament was part of an attack that targeted more than ten state-owned and private companies that were tried to be compromised (Tormod Strand, Gundersen and Mjaaland, 2020)

Regarding WiFi Access points, since they are stationary, the logged data is more used in the ability to track down stolen routers or individuals' new home rather than location tracking. It may still be of interest to commercial businesses if they want to track router brand quantity/density or broadband providers.

Hackers can use the wardriving method to map all of the unsecure, improperly configured WiFi access points with outdated encryption as shown in figure 32 to 34 in section 5.7 to 5.10. These figures show where to get access to unsecured networks. These unsecured networks are "gold mines" for criminals since this access to the network to steal sensitive and confidential data from home and enterprise networks.(Legezo, 2016). Digital criminal activity performed on these unsecured networks may implicate or harm innocent individuals.

One of the attacks that can be used is packet sniffing. This is a type of attack where the attacker monitors the client communication with the endpoint to a service, server or website. Packet sniffing is used to monitor and analyse the packet flow on the network as well as to the internet to check the network's capacity, monitoring bandwidth as well as increasing efficiencies (Software Reviews, Opinions, and Tips - DNSstuff, 2019). The sniffing attack, also called a man-in-the middle attack, will capture all of the package sent back and forth from the client and the destination. (NordVPN, 2020)

If the services the individual is using is unencrypted the information that can be sniffed by the hacker are the following: Email, what pages the individual is browsing, what apps are on a smartphone, getting a individual's username and password, banking information or transaction information, FTP and telnet password, router configuration, chat messages, information that can be used with identity theft and DNS traffic (Greycampus.com, 2013). If the traffic is encrypted in the case of a websites are using Secure Socket Layer SSL in HTTPS thee it is not possible to see what the content is, it only possible to see what services are being used and what websites they are connected but not the content (Kody, 2019).

The Seattle Police has investigated a criminal hacker group that was wardriving around the city looking for WiFi networks of companies that did use the unsecure WEP encryption (see section 5.9) and making a list of locations with the. After finding company WiFi networks with the vulnerable WEP encryption, the hacker group started cracking the encryption to get into the business network and install credit card-stealing programs. The hacker group did this activity from 2005 to 2007 and stole up to 130 million credit card numbers before getting caught and convicted. (PCWorld, 2011)

7 - Conclusion

First of all, the hardware chosen to make the MAC capture device was a little flawed, even though there was a lot of good data captured with the device. The issues the author ran into was that there was some time the device went into a looping disconnected and reconnected with the WiFi adapter. Resultinly, the author had to move through the same place twice in the affected areas. This has to do with the fact that the hardware chosen was,as one of the admin on Kismet support discord channel wrote, “one of the worst possible devices, 8814au is even worse than the 8812au”. KIsmet hardware webpage says that 8812au is one of the adapters that should be avoided due to driver issues. If this data gathering process would be conducted again, another adapter would have been chosen.

Wardriving without the use of a car should be planned with the most energy efficient route and necessary amount of rest between rounds to make sure the user does not get exhausted due to lack of recovery. The author did take into consideration to have a good route plan before wardriving each day, but due to the weather there was a lot of headwind halfway into the wardriving weeks which made the routes more labor intensive.

After the wardriving was completed, the raw data was parsed to a format that made it possible to list every device onto a map to have a visual interface and to present it in an aesthetically pleasing way with colored dots to indicate the different MAC address and lines between them when having several data points. This was a much easier way to find data that correlates rather than doing it manually and going through excel files with five million lines with info about the device with GPS coordinates and plotting them onto a map.

The visualized data for the Bluetooth devices showed something interesting that there were not that many smartphones captured. This can be a result from that the SSID was not broadcasted, empty or the device used MAC randomization. The data shown was filtered with SSID, and not by OUI vendors. If the data was categorized by the OUI vendors of smartphones it could be a better way to show all of the smartphones in the dataset, but this is not possible with the software being used.

What is interesting about the dataset is that the best example for location tracking of movements are not vehicles, smartphones or even activity trackers - but headsets that do not have MAC randomization, which may make it easier to track the movements of an individual headset rather than the individual's smartphone.

For the WiFi Access Point in the captured dataset, it is a surprisingly high number of how many wireless networks are unsecure. There was found a business still using WEP encryption and two accounting firms using WPA encryption, both of these encryption protocols are considered as outdated and easy to crack fast and are high targets for criminals. As an accounting firm which administers financial data for their customers, this vulnerability could serve as a serious threat to their business.

As discussed in section 6, the potential uses of logged/tracked data from MAC and WiFi addresses are substantial, ranging from commercial use cases such as traffic light control, to tracking down stolen electronic devices that broadcast MAC addresses, tracking down an individual, and to espionage.

The tracking and logging was done without informed consent from the public, as the author wanted to show how easy it is to do. This to prove that while government guidelines may affect commercial interests, less savory individuals not necessarily affected by the same commercial regulations may choose to ignore them and just go ahead.

In hindsight after data gathering and data preparation, it is scaringly easy. Looking at the data, it is even easier to identify people than one could assume, as many chose to use their full name as identifiers on their devices. It is the author's opinion that this is a tech area where many do not know about these vulnerabilities or how to avoid them, or even downright choose to ignore them.

As the gathered data show (section 5) and with events talked about (section 6), there is so much information that modern devices transmit that unless one were to take a definitive stance and actively start masking themselves, you will be tracked.

Due to the given limitations of this assignment, the author has limited the scope of this research to be what has already been presented in this paper. If the author would continue this work based on the findings in this paper in another assignment, it would be possible to go more in depth on data gathering, to do more qualitative studies with individual awareness on the issue, or to do further research on which measures could be taken to minimise or avoid these types of risk. However, in this paper the conclusion is that they do exist and there have been given examples on how data can be gathered, as well as how it can be both used, and misused.

The author has himself started to adjust his devices, with having generic names on the devices that blend in with the crowd, turning off wireless capabilities when not needed and using wired headset.

8 - References

admin (2015). *Wi-fi tracking illegal in Swedish cities | ScandinavianRetail.com*. [online] Scandinavianretail.se. Available at: http://scandinavianretail.se/wi-fi-tracking-illegal-in-swedish-cities/ [Accessed 26 May 2021].

AP NEWS. (2021). *Dutch city fined for Wi-Fi tracking says it will appeal*. [online] Available at: https://apnews.com/article/europe-wi-fi-data-privacy-technology-1c631129617e8f031be97ff2e6163cef [Accessed 27 May 2021].

Bamford, J. (2020). *Edward Snowden: The Untold Story*. [online] Wired. Available at: https://www.wired.com/2014/08/edward-snowden/ [Accessed 3 May 2021].

Beaconstac (2013). *What is iBeacon? How does Apple iBeacon technology work?* [online] Beaconstac. Available at: https://www.beaconstac.com/apple-ibeacon-technology [Accessed 27 May 2021].

Bitforestinfo.com. (2017). *Crack WEP Password Using Kali Linux And Aircrack-ng - Bitforestinfo*. [online] Available at: https://www.bitforestinfo.com/blog/07/23/crack-wep-password-using-kali-linux-and.html [Accessed 25 May 2021].

Bjørn Atle Gildestad (2020). *Vegselskapet Nye Veier registrerer mobiltelefonen din*. [online] NRK. Available at: https://www.nrk.no/norge/vegselskapet-nye-veier-registrerer-mobiltelefonen-din-1.15133464 [Accessed 26 May 2021].

Burrough, B., Ellison, S. and Andrews, S. (2014). *Snowden Speaks: A Vanity Fair Special Report*. [online] Vanity Fair. Available at: https://www.vanityfair.com/news/politics/2014/05/edward-snowden-politics-interview [Accessed 28 May 2021].

Dallinger, S. (2018). *Plug & Track Real-Time Tracking Terminal*. [online] VARIA Group - Import & Export, Training, Distribution, Consulting. Available at: https://www.varia.org/en/portfolio-view/plug-track-real-time-tracking-terminal/ [Accessed 28 May 2021].

Datatilsynet (2016). *Tracking in Public Spaces.* [online] . Available at: https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/rettigheter-og-plikter/rapporter/sporing-i-det-offentlige-rom_eng_web.pdf.

derek (2021). OBD Port Location (With Pictures!). [online] CarMD. Available at: https://www.carmd.com/obd-port-location/ [Accessed 30 May 2021].

Engeniustech.com. (2015). *EnGenius Technologies*. [online] Available at: https://www.engeniustech.com/wi-fi-beacon-frames-simplified/ [Accessed 5 May 2021].

Finavia.fi. (2017). *Estimated waiting time for security control | Finavia*. [online] Available at: https://www.finavia.fi/en/airports/helsinki-airport/airport/terminals/security-control-waiting-time [Accessed 26 May 2021].

Gitlab.io. (2021). *GPSd — Put your GPS on the net!* [online] Available at: https://gpsd.gitlab.io/gpsd/ [Accessed 30 May 2021].

Gpstechnologies.com (2021). *How To Find a Hidden GPS Tracking Device on Your Car*. [online] Gpstechnologies.com. Available at: https://gpstechnologies.com/2018/09/how-to-find-a-hidden-gps-tracking-device-on-your-car/ [Accessed 28 May 2021].

Greycampus.com. (2013). *Greycampus*. [online] Available at: https://www.greycampus.com/blog/information-security/what-is-a-sniffing-attack-and-how-can-you-defend-it [Accessed 29 May 2021].

Hackaday.io. (2021). *YAAWP (Yet Another Automated Wardriving Project)*. [online] Available at: https://hackaday.io/project/176358-yaawp-yet-another-automated-wardriving-project [Accessed 21 May 2021].

Hermiston, L. (2015). *Iowa City officer develops software to find stolen Wi-Fi-enabled devices*. [online] @gazettedotcom. Available at: https://www.thegazette.com/news/iowa-city-officer-develops-software-to-find-stolen-wi-fi-enabled-devices/ [Accessed 27 May 2021].

Hurley, C. and Ebrary, I. (2004). *WarDriving : drive, detect, defend: a guide to wireless security*. Rockland, Ma: Syngress Publishing, p.18.

Hurley, C. and Ebrary, I. (2004). *WarDriving : drive, detect, defend: a guide to wireless security*. Rockland, Ma: Syngress Publishing, p.19.

Ieee.org. (2021). *IEEE SA - MAC Infographic*. [online] Available at: https://standards.ieee.org/products-services/regauth/mac.html [Accessed 4 May 2021].

Ieee.org (n.d.). *Standard Group MAC Addresses Standard Group MAC Addresses: A Tutorial Guide*. [online] *Ieee.org*. Available at: https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/tutorials/macgrp.pdf.

Khandelwal, S. (2015). *The Hacker News*. [online] The Hacker News. Available at: https://thehackernews.com/2015/09/track-stolen-devices.html [Accessed 27 May 2021].

Kismet. (2021). *Hardware*. [online] Available at: https://www.kismetwireless.net/hardware/ [Accessed 21 May 2021].

Kody (2019). *How to Spy on Traffic from a Smartphone with Wireshark*. [online] WonderHowTo. Available at: https://null-byte.wonderhowto.com/how-to/spy-traffic-from-smartphone-with-wireshark-0198549/ [Accessed 29 May 2021].

Kody (2018). *How to Detect When a Device Is Nearby with the ESP8266 Friend Detector*. [online] WonderHowTo. Available at: https://web.archive.org/web/20210304100329/https://null-byte.wonderhowto.com/how-to/detect-when-device-is-nearby-with-esp8266-friend-detector-0188642/ [Accessed 30 May 2021].

Krackattacks.com. (2017). *KRACK Attacks: Breaking WPA2*. [online] Available at: https://www.krackattacks.com/ [Accessed 25 May 2021].

Kwet, M. (2021). Opinion | In Stores, Secret Bluetooth Surveillance Tracks Your Every Move. *The New York Times*. [online] Available at: https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html [Accessed 27 May 2021].

Legezo, D. (2016). *Research on unsecured Wi-Fi networks across the world*. [online] Securelist.com. Available at: https://securelist.com/research-on-unsecured-wi-fi-networks-across-the-world/76733/ [Accessed 29 May 2021].

Lindh, J. (2015). *Bluetooth ® low energy Beacons Bluetooth ® low energy Beacons*. [online]. Available at: https://www.ti.com/lit/an/swra475a/swra475a.pdf?ts=1621584293009&ref_url=https%253A%252F%252Fwww.startpage.com%252F. [Accessed 20 May 2021].

LM Technologies. (2021). *Bluetooth® v4.0 Dual Mode Long Range USB Adapter - LM1010 - Bluetooth and WiFi Modules and Adapters - LM Technologies*. [online] Available at: https://www.lm-technologies.com/product/bluetooth-v4-0-dual-mode-long-range-usb-adapter-lm1010/ [Accessed 21 May 2021].

Lomas, A. (2017). *Your wireless network is NOT secure - WPA Vulnerability*. [online] Creativefolks.com.au. Available at: https://www.creativefolks.com.au/news/your-wireless-network-is-not-secure-wpa-vulnerability [Accessed 25 May 2021].

Linuxize (2018). *How To Use Linux Screen*. [online] Linuxize.com. Available at: https://linuxize.com/post/how-to-use-linux-screen/ [Accessed 10 May 2021].

Merlino, V. (2019). *Queens Daily Eagle*. [online] Queens Daily Eagle. Available at: https://queenseagle.com/all/law-enables-sex-assault-stalking-and-trafficking-survivors-to-conceal-their-addresses [Accessed 28 May 2021].

Microchipdeveloper.com. (2021). *Bluetooth® Low Energy Packet Types - Developer Help*. [online] Available at: https://microchipdeveloper.com/wireless:ble-link-layer-packet-types [Accessed 20 May 2021].

Negus, C., 2015. *Linux Bible Ed. 9*. John Wiley & Sons, p.349.

NewsComAu. (2021). *Mechanic finds tracking device during woman's routine car service*. [online] Available at: https://www.news.com.au/lifestyle/relationships/mechanic-finds-tracking-device-during-womans-routine-car-service/news-story/51147c1d14c8d128cae801881af690cd [Accessed 28 May 2021].

NordVPN. (2020). *What is a sniffing attack? | NordVPN*. [online] Available at: https://nordvpn.com/no/blog/sniffing-attack/ [Accessed 29 May 2021].

Odom, W., 2014. *Cisco CCENT/CCNA ICND1 100-101*. Madrid: Pearson Educación, p.27.

Odom, W., 2014. *Cisco CCENT/CCNA ICND1 100-101*. Madrid: Pearson Educación, p.46.

Olsen, J.M. (2021). *Norway intel: Russians likely behind parliament hacking*. [online] AP NEWS. Available at: https://apnews.com/article/denmark-europe-military-intelligence-hacking-norway-fd69246508dc8621821afab5d0eace09 [Accessed 25 May 2021].

PCWorld. (2011). *Seattle Police Say "wardrivers" Are Hitting Small Businesses*. [online] Available at: https://www.pcworld.com/article/226086/article.html [Accessed 29 May 2021].

Roald Ramsdal (2013). *Styrer trafikklys med bilistenes bluetooth*. [online] Tu.no. Available at: https://www.tu.no/artikler/styrer-trafikklys-med-bilistenes-bluetooth/234320 [Accessed 26 May 2021].

Software Reviews, Opinions, and Tips - DNSstuff. (2019). *10 Best Packet Sniffers - Comparison and Tips - DNSstuff*. [online] Available at: https://www.dnsstuff.com/packet-sniffers [Accessed 29 May 2021].

Techterms.com. (2020). *MAC Address*. [online] Available at: https://techterms.com/definition/macaddress [Accessed 3 May 2021].

Tews, E. and Beck, M. (2020). *Practical attacks against WEP and WPA | Proceedings of the second ACM conference on Wireless network security.* [online] Acm.org. Available at: https://dl.acm.org/doi/pdf/10.1145/1514274.1514286 [Accessed 25 May 2021].

The Raspberry Pi Foundation (2021). *Operating system images – Raspberry Pi*. [online] Raspberry Pi. Available at: https://www.raspberrypi.org/software/operating-systems/ [Accessed 7 May 2021].

The Pi Hut (2015). *Adding a Real Time Clock to your Raspberry Pi*. [online] The Pi Hut. Available at: https://thepihut.com/blogs/raspberry-pi-tutorials/17209332-adding-a-real-time-clock-to-your-raspberry-pi [Accessed 21 May 2021].

Themayor (2018). *Find out why in Enschede Wi-Fi sensors track the location of the citizens and visitors*. [online] Themayor.eu. Available at: https://www.themayor.eu/en/a/view/find-out-why-in-enschede-wi-fi-sensors-track-the-location-of-the-citizens-and-visitors-1311 [Accessed 26 May 2021].

Tormod Strand, Gundersen, M. and Mjaaland, O. (2020). *Stortinget ikke alene: Massivt hackerangrep mot Norge*. [online] NRK. Available at: https://www.nrk.no/norge/stortinget-ikke-alene_-massivt-hackerangrep-mot-norge-1.15277734 [Accessed 29 May 2021].