WARDRIVING

Antwerpen in kaart

De zoektocht naar beveiligde en onbeveiligde wifi-netwerken in een grootstad

Peter Van de Putte, Daan Maes

Inhoud

Wat is wardriving 2

Belgische wetgeving 2

Europese wetgeving 2

Technologie 3

- Kismet 3
- Gps 3
- Wifi Antenne 3
- Google Maps 3

Werkwijze 4

- gps 4
- Kismet 4
- Onze sessie 5
- Verwerking data 5
- In kaart brengen 6

Verslag 7

- Gevonden netwerken 7
- Encryptiemethoden 7
- Channels 9
- SSID 10

Wat is wardriving

Wardriving is het opzoek gaan naar wifi-netwerken, dit door middel van rond te rijden met een wagen die met speciale apparatuur is uitgerust. Deze apparatuur registreert alle gevonden informatie over de draadloze netwerken die kunnen worden gevonden. Onder meer Google heeft wardriving toegepast, de wagen die de beelden maakte voor Google Street View registreerde tegelijkertijd alle draadloze netwerken in de omgeving.

Belgische wetgeving

Het vaststellen of een Wi-Fi-netwerk aanwezig is, zonder zich toegang tot het netwerk te verschaffen, is niet strafbaar. Alles hangt er natuurlijk vanaf wat je met deze informatie gaat doen.

De Belgische wet zegt sinds het jaar 2000 dat het verboden is om zomaar te surfen op andermans wifi-netwerk, ook als dit onbeveiligd is en zelfs als je laptop of telefoon automatisch verbinding maakt, is het strafbaar. Voor een beveiligde verbinding is het uiteraard meteen strafbaar als je erop inbreekt, aangezien je het dan sowieso moedwillig doet. Voor een onbeveiligde verbinding echter is het moeilijker te bepalen of je nu echt een misdaad hebt begaan of niet. Je kan namelijk per ongeluk verbonden worden met een onbeveiligde wifi-verbinding, wat een misdrijf is. Maar je kan ook, zoals vaak in koffiebars of bedrijfskantines gebeurt, de toegangscode van een vergrendeld WiFi-netwerk verkrijgen, dan heb je natuurlijk toestemming en ben je niet in fout. Als je deze moedwillig gebruikt voor bijvoorbeeld iets te hacken ben je natuurlijk strafbaar voor deze feiten, maar niet voor het inbreken in een netwerk.

Personen die zich niet houden aan bovenstaande regels, riskeren een celstraf van drie maanden tot een jaar en tot 125.000 euro boete.

Europese wetgeving

In andere Europese landen en in de VS bestaan vergelijkbare wetgevingen.

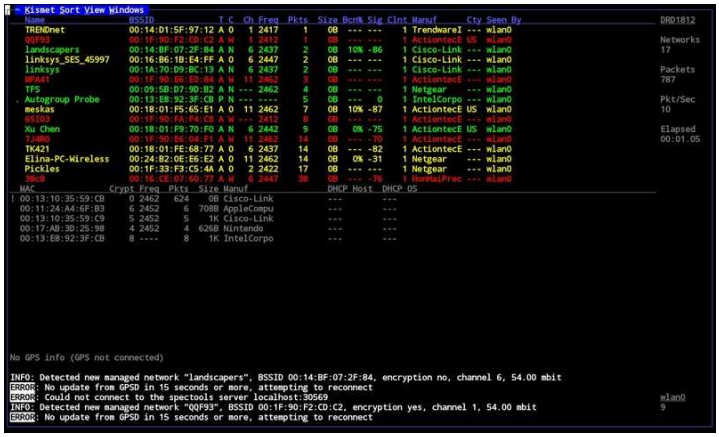
Op politiek niveau bestaat er binnen de EU wel wat discussie over: moet zoiets echt strafbaar zijn, of is de grens pas overschreden als je de toegang tot een beveiligd netwerk kraakt? Voorlopig blijft het allemaal taboe

Technologie

Kismet

Voor dit project zullen we gebruik maken van kismet. Kismet is een applicatie op het linux-kali besturingssysteem dat op zoek gaat naar alle wifinetwerken in de buurt en hiervan het volgende opslaat:

- Encryptiemethode
- SSID
- BSSID
- Channel
- Verbonden mac-adressen
- Locatie



Gps

We hebben ook nog een gps-tracking toegevoegd aan Kismet door middel van een android-gsm die gps kan ontvangen. Dit doen we door de daemon gpsd te gebruiken. Deze daemon neemt de gps-locatie van de gsm via usb en stuurt deze door naar kismet, die deze locatie koppelt aan de op dat moment gevonden netwerk. Elk netwerk staat dus opgeslagen samen met de locatie waar het netwerk gevonden werd.

Wifi Antenne

We zullen ook gebruik maken van een aparte WiFi-antenne, deze is veel krachtiger dan de ingebouwde antenne van de laptop waardoor we meerdere netwerken kunnen detecteren en er meer in kaart kunnen brengen.

Een standaard ingebouwde antenne heeft ongeveer een versterking van 2dBi. Door deze standaard antenne te vervangen door een exemplaar met 5dBi vergroten we ons bereik dus aanzienlijk.

Google Maps

De data van Kismet wordt opgeslagen in een netxml-file. Deze moeten we via het terminalvenster van Kali omzetten naar een kml-file, welke we rechtstreeks in google maps kunnen plaatsen. Hier zal dan elk WiFi-netwerk weergegeven worden als een punt, en wanneer we hierop klikken wordt al de opgeslagen informatie over het netwerk weergegeven.

Werkwijze

gps

Eerst moeten we onze gps zien te koppelen aan de computer.

Hier hebben we da app BlueNMEA voor nodig. Dit is een Android applicatie die de locatie van de het toestel doorstuurt via TCP in NMEA formaat. Het toestel moet ook in USB Debugging Mode staan en de GPS natuurlijk ingeschakeld.

Om de gsm te herkennen en de locatie te weten moeten we de Android-sdk, gpsd, en gpsd-clients installeren. Dit kan met het volgende commando:

Apt-get install android-sdk gpsd gpsd-clients

Via “Android” in het terminalvenster komen we in de Android-sdk manager. Hier moeten we nog de nodige SDK build tools en juiste API installeren.

De volgende stap is de TCP poort 4352 van de Android gsm te forwarden naar de laptop.

Commando: adb forward tcp:4352 tcp:4352

Nu moet enkel nog GPSD luisteren naar de poort 4352:

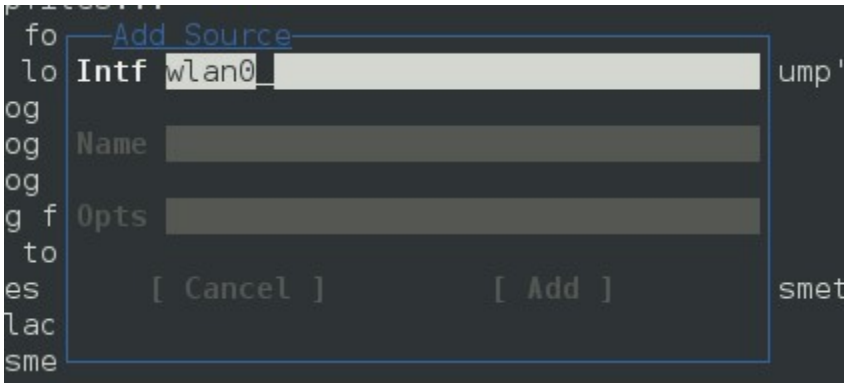
Gpsd –N –n –D5 tcp://localhost:4352

Kismet

Nu kunnen we Kismet starten. (Terminalvenster→”Kismet”)

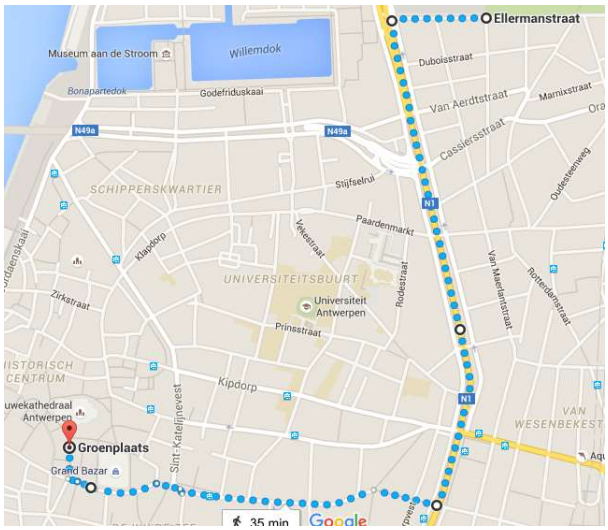
Kismet zal automatisch gpsd gebruiken voor het bepalen van de locatie.

Als laatste stap moeten we nog instellen welke wifi-adapter er gebruikt moet worden. Deze kunnen we vinden door ‘iwconfig’ te runnen in een terminalvenster.



Eens we op Add klikken zal kismet beginnen te scannen naar netwerken en kunnen we dus gaan wardriven !

Onze sessie



Voor onze sessie zijn we vanuit de AP-hogeschool (campus Ellermanstraat) vertrokken, over de Italielei richting Meir, dit omdat zich daar veel winkels bevinden die wel eens netwerken kunne gebruiken die niet beveiligd zijn. Zo hebben we heel de Meir doorgewandeld tot aan de Groenplaats en hebben we hier nog een cirkel gewandeld langs alle gebouwen om deze nog in kaart te brengen. In het totaal hebben ongeveer 4000 netwerken gevonden.

Verwerking data

De data die door Kismet wordt gevonden wordt opgeslagen in een .netxml file. Deze data moet worden omgevormd naar een .kml file zodat we deze kunnen gebruiken in Google Maps voor een visuele weergave.

Dit doen we door de data van de .netxml file in de giskismet database te zetten. Dit kan met het volgende commando:

Giskismet –x BESTAND.netxml

Met de volgende querie kunnen we dan deze data opslaan in een .kml file:

giskismet -q "SELECT * FROM WIRELESS" -o output.kml.

In kaart brengen

Om de gevonden informatie in kaart te brengen maken we zoals eerder vermeld gebruik van Google Maps. Deze kan enkel Kml files in beeld brengen met een maximum van 2000 punten.

De data is voor iedereen toegankelijk:

https://www.google.com/maps/d/edit?mid=z91pBwm5cRJ4.kTjo-STITUy0&usp=sharing

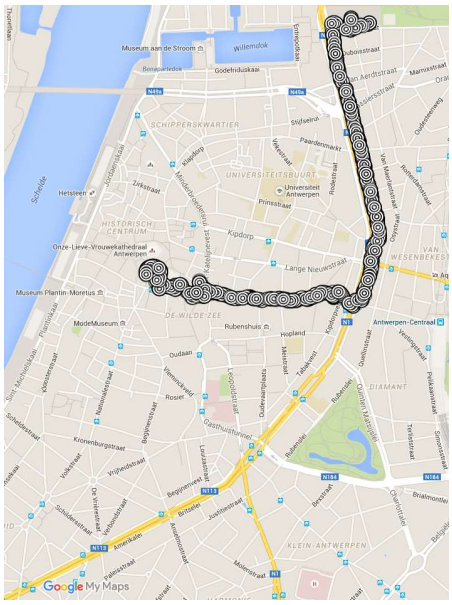
Hiernaast een weergave van het google-maps-bestand, waarin we 2000 (het maximum) van de gevonden netwerken hebben geplaatst op hun gevonden locatie. Als we een netwerk selecteren kunnen we alle informatie van het netwerk zien, inclusief SSID, encryptiemethoden, aangesloten MAC Address, BSSID, en het channel waar het netwerk op werkt.

Verslag

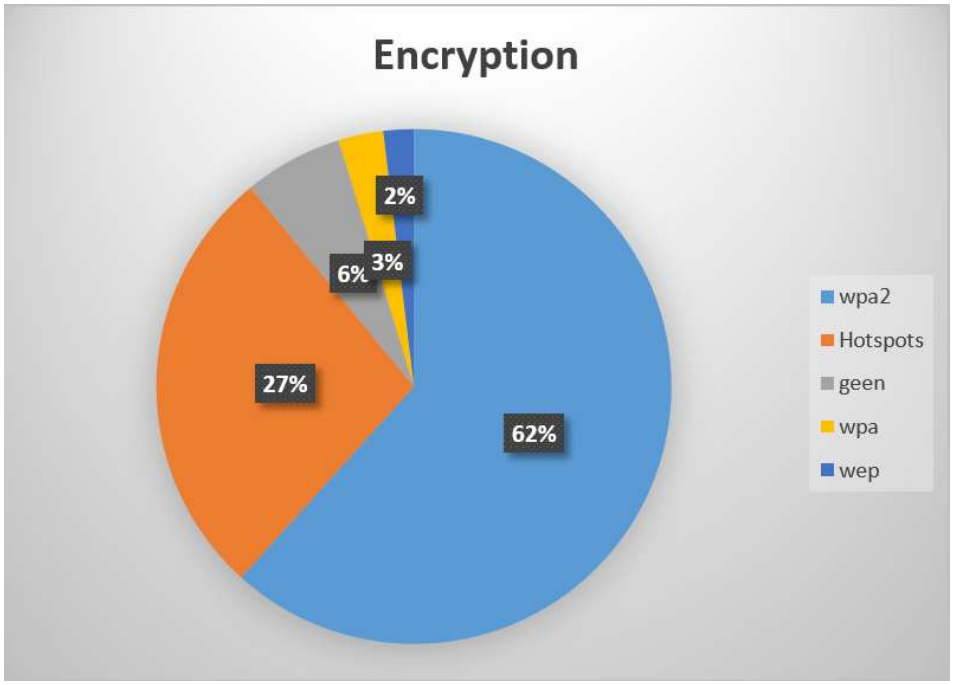
Gevonden netwerken

In totaal hebben we 3829 netwerken gevonden over een afstand van 2.7 kilometer.

Dat zijn bijna 1.5 netwerken per meter die er in Antwerpen kunnen worden gevonden.



Encryptiemethoden



De meest voorkomende encryptiemethode is WPA2(62%), wat ook de meest veilige methode is.

WPA1(3%) en WEP(2%) zijn minder veilig en representeren dus een kleiner deel van de encryptiemethoden.

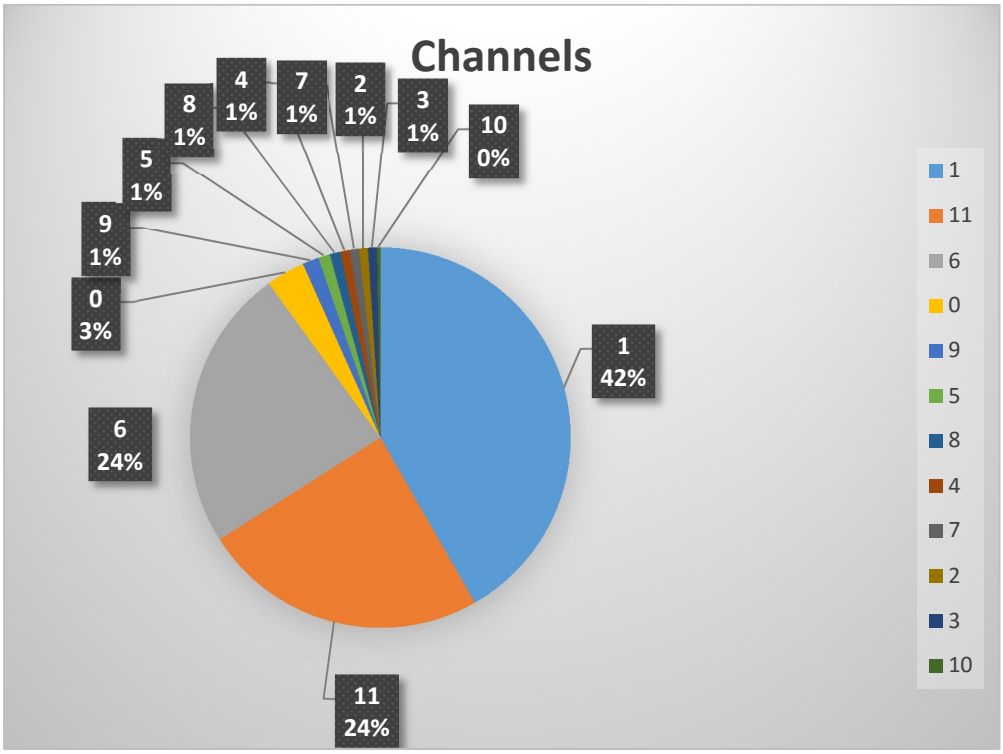
6% van alle netwerken heeft geen encryptiemethode en staat dus open voor alle mensen die toegang willen tot het netwerk en eventueel verkeerde dingen willen doen. Als we dit toetsen aan onze gevonden netwerken per meter, komen we uit op ongeveer 1 onbeveiligd netwerk per 20 meter in Antwerpen.

Hotspots(27%) maken tegenwoordig een groot deel uit van alle netwerken. Er wordt geen beveiligingssleutel toegepast maar gebruikers moeten zich meestal wel registreren alvorens het netwerk optimaal te kunnen gebruiken.

Onder deze hotspots vallen onder anderen:

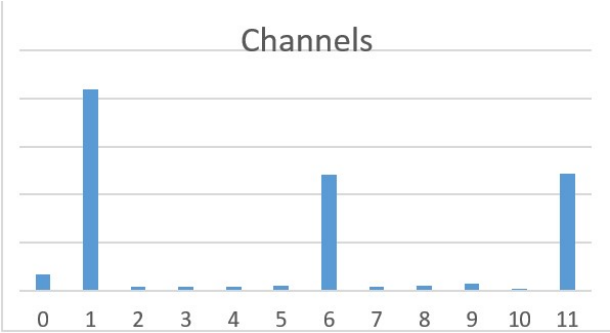
PROXIMUS_FON, Colombus-net, hhonors-public, TelenetHomespot, hhonors, Antwerpport en telentehotspot.

Channels



De minste netwerken werken op channel 10. Hier werken amper 0.3% van alle netwerken op.

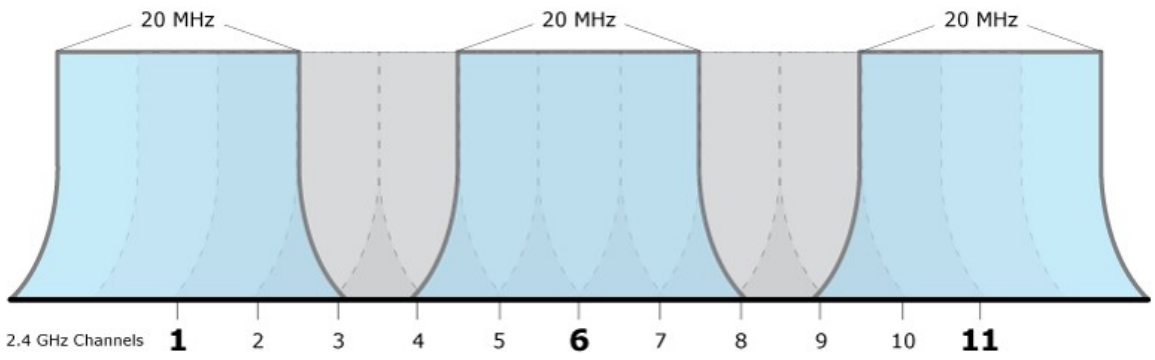
Bijna de helft van alle wifinetwerken werken op channel 1. Samen met channel 11(24%) en channel 6(24%) zijn ze verantwoordelijk voor 90 van de channels die gebuikt worden. Buiten deze drie worden er dus amper andere channels gebruikt.



Hoe komt dit ?

Slecht bereik of een langzame WiFi verbinding kan veroorzaak worden door storing in je WiFi netwerk. De 3 meest voorkomende oorzaken van deze storing zijn: draadloze netwerken die op hetzelfde kanaal uitzenden, de router van de buren die op een overlappend kanaal uitzendt en storing op 2.4 GHz van iets dat geen WiFi signaal uitzendt.

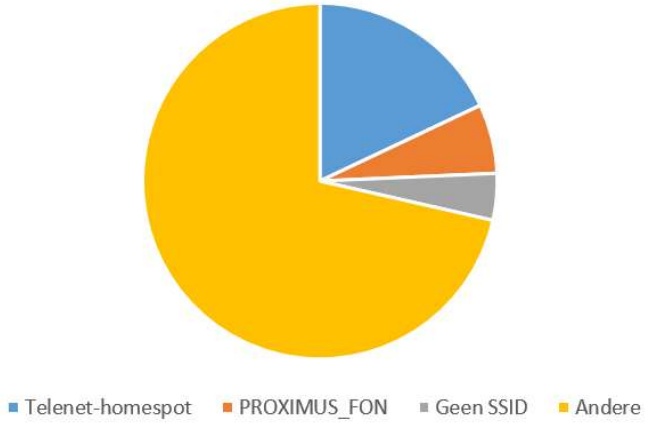
Kanaal 1, 6 of 11 zijn de beste WiFi kanalen omdat deze elkaar niet overlappen. Het is dan ook mogelijk om meerdere signalen naast elkaar op de 2.4 GHz band te versturen, omdat deze 100 MHz breed is en een kanaal een spectrum van 20 MHz gebruikt.



Indien er meerdere draadloze netwerken in de buurt zijn, is het vaak beter om hetzelfde kanaal (bij voorkeur 1, 6 of 11) te gebruiken, dan een overlappend kanaal. In dit geval is het het beste, het kanaal dat het minst gebruikt wordt bij de sterkste netwerken te gebruiken.

Met het gratis programma inSSIDer kun je bijvoorbeeld zien welke netwerken in de buurt zijn, hoe sterk het signaal is en op welk kanaal deze uitzendt en hier desnoods uit concluderen dat je beter van kanaal kan veranderen.

SSID



Als we kijken naar de SSIDs van de netwerken valt het op dat 18 procent van alle netwerken in Antwerpen een Telenethomspot is en 6 procent een PROXIMUS_FON netwerk.

Daarnaast zijn er ook een goede 4 procent van de netwerken die hun SSID niet tonen. Waarvan nog eens 22 procent van deze netwerken geen encryptie methode gebruikt. Toch even onderstrepen dat het verbergen van je SSID geen volwaardige maatregel is tegen indringers. Zo is het redelijk effectief tegen personen, die niet gericht zoeken naar het netwerk van een specifiek bedrijf. Maar een vastberaden hacker heeft dit zo gevonden.

Ook heeft het verbergen van een SSID vaak een omgekeerd effect. Zo zal een hacker die een netwerk vindt zonder SSID, dit netwerk eerder gaan aanvallen dan één met SSID. Dit omdat het verbergen van de SSID kan gelinkt worden aan het verbergen van gevoelige informatie. Laat dat nu eenmaal de hoofdreden zijn dan de hackers toeslagen.