Phonebusters

Kako varni so v resnici mobilni telefoni?

Matej Kovačič

Institut
"Jožef Stefan"
Ljubljana, Slovenija

OPOZORILO:
“kidz, don't try this at home”

Pri izvajanju varnostnih analiz je potrebno paziti na spoštovanje zakonodaje, izogibati se je potrebno povzročanju motenj na omrežju.

Prestrezanje tujih komunikacij je kaznivo.

Vdiranje v tuje sisteme in omrežja je kaznivo.

Oddajanje v nelicenciranem delu radijskega spektra je kaznivo.

Nevil Maskelyne (1863-1924)

Problem avtentikacije

Mobilna telefonija nima vgrajenih ustreznih mehanizmov overovitve.

Klicatelj oz. pošiljatelj SMS sporočila je "overjen" zgolj s svojo mobilno številko.

Rezultat: močno je ponarejanje klicne identitete!

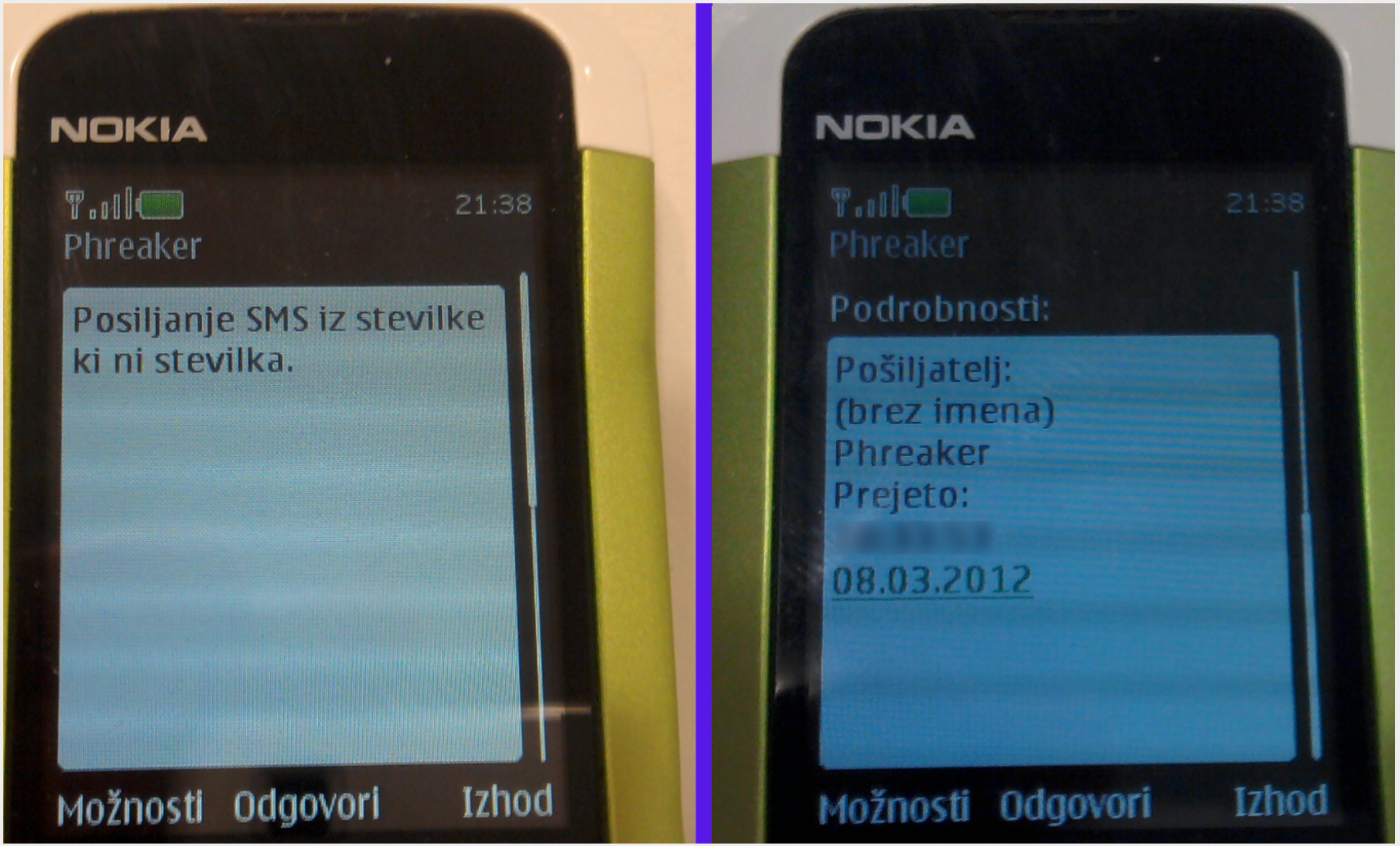
Overovitveni mehanizmi so pomanjkljivi tudi med operaterji.

Rezultat: mogoči so številni napadi na SS7 infrastrukturo!

Mobilno omrežje se ne avtenticira mobilnemu telefonu.

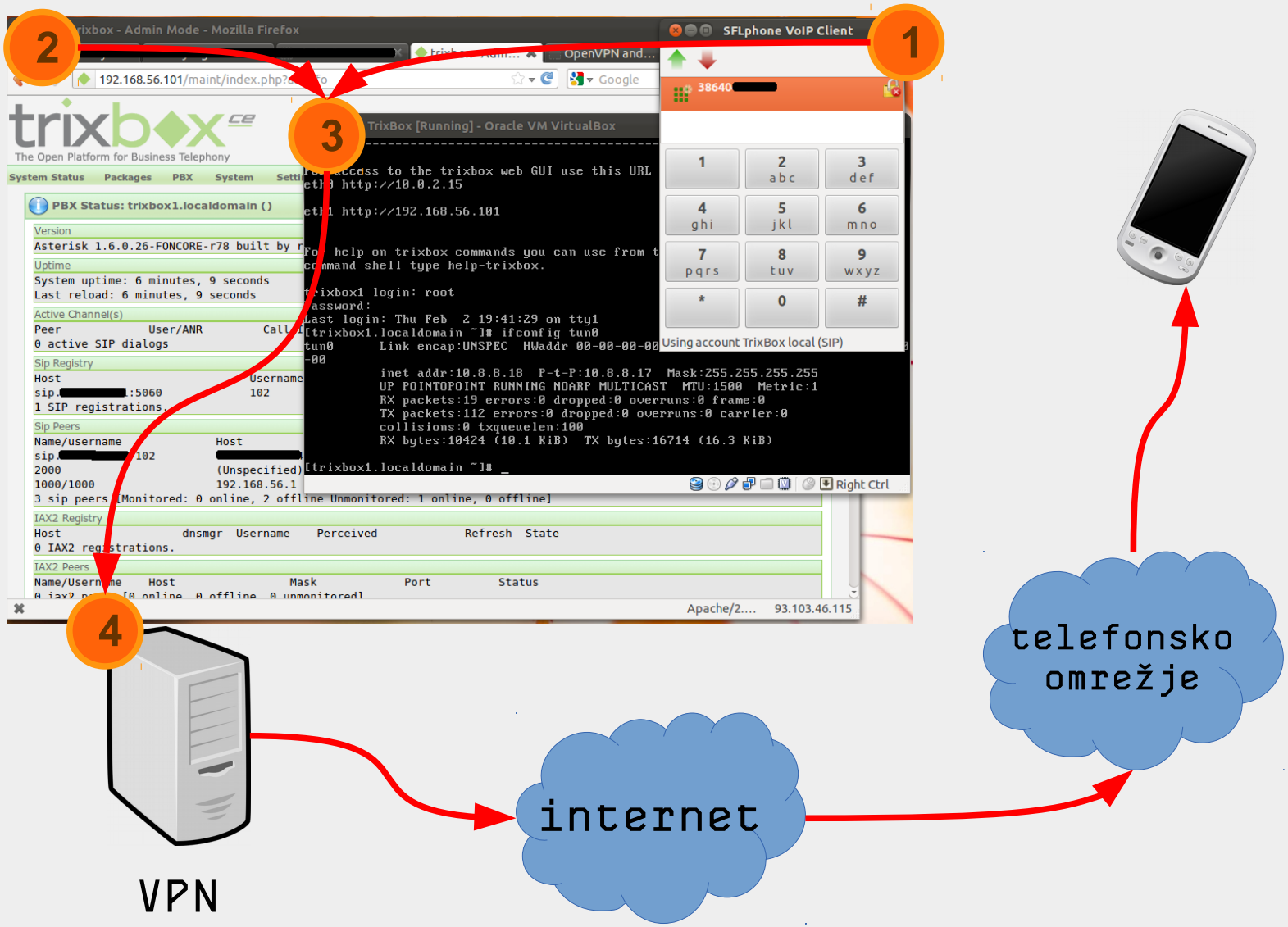
Rezultat: mogoče je uporabiti lažne bazne postaje (IMSI lovilce)!

Pošiljanje SMS sporočil z lažno identifikacijo

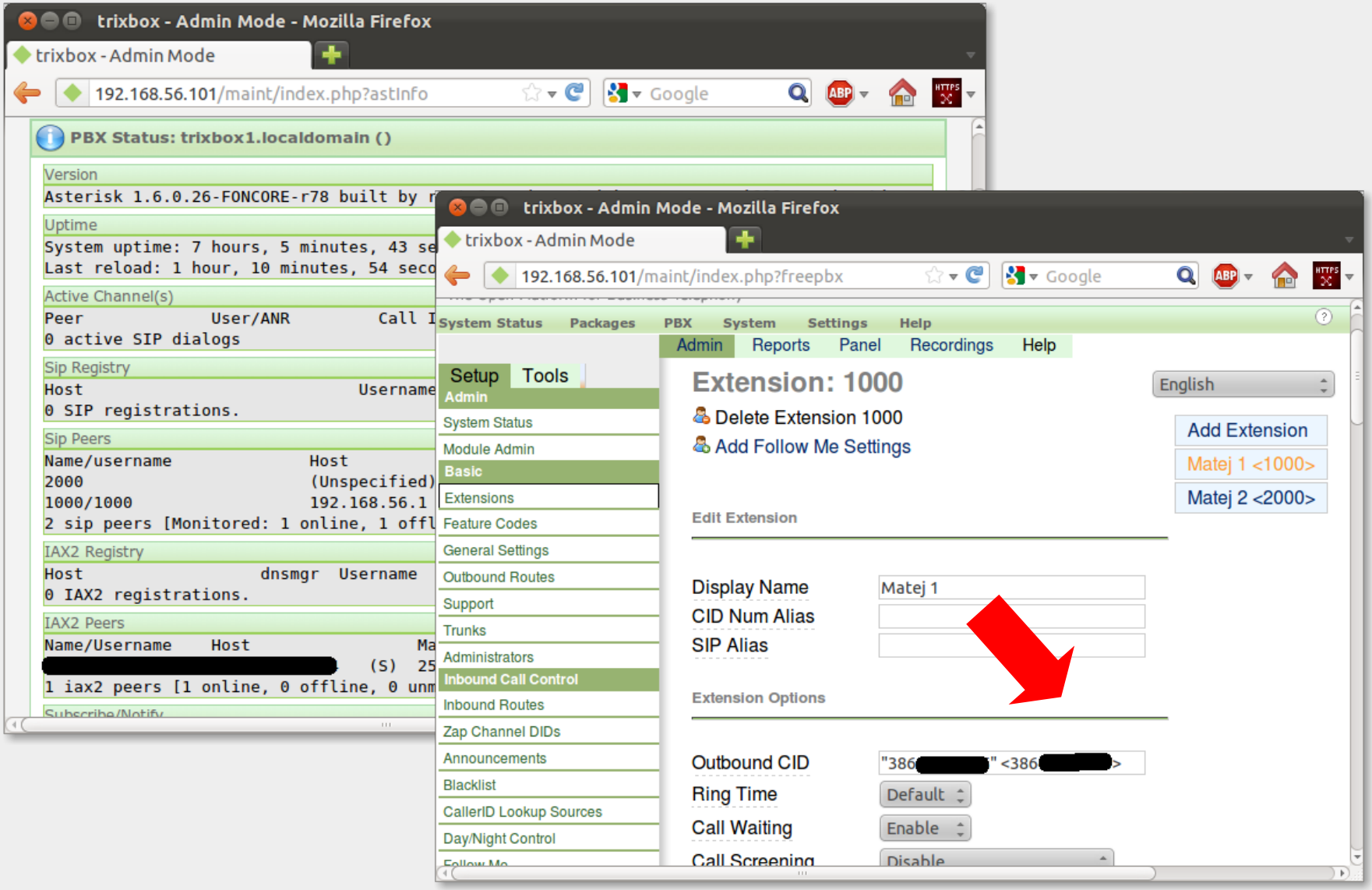


<http://provider.com/sms/json?username=xxxxxxxx&password=xxxxxxxxx&from=Phreaker&to=38631123456&text=Posiljanje%20SMS%20iz%20stevilke%20ki%20ni%20stevilka.>

Lažna klicna identifikacija

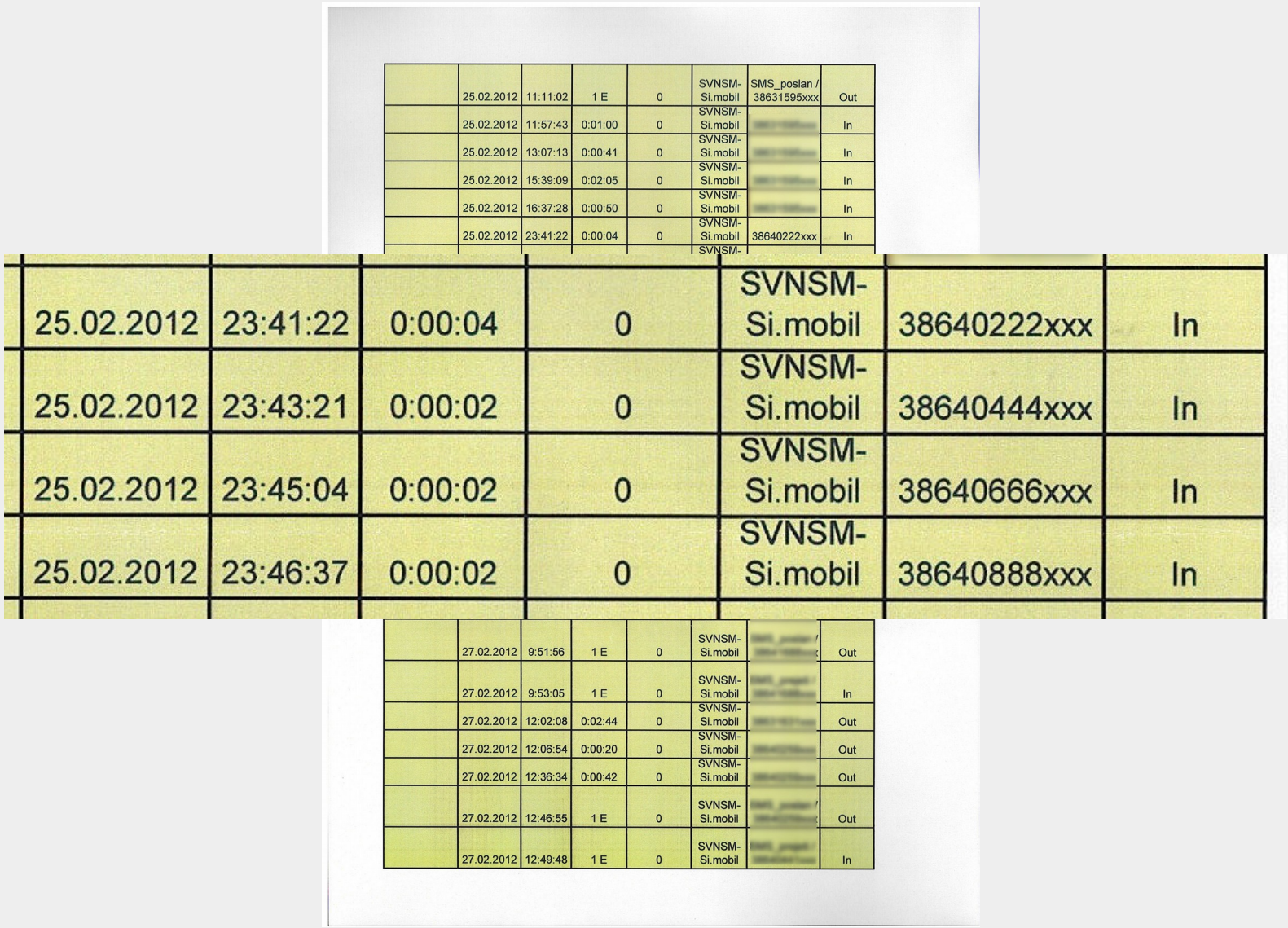


Lažna klicna identifikacija



Lažna klicna identifikacija

Lažna klicna identifikacija



	25.02.2012	11:11:02	1 E	0	SVNSM-Si.mobil	SMS_poslan / 38631595xxx	Out
	25.02.2012	11:57:43	0:01:00	0	SVNSM-Si.mobil		In
	25.02.2012	13:07:13	0:00:41	0	SVNSM-Si.mobil		In
	25.02.2012	15:39:09	0:02:05	0	SVNSM-Si.mobil		In
	25.02.2012	16:37:28	0:00:50	0	SVNSM-Si.mobil		In
	25.02.2012	23:41:22	0:00:04	0	SVNSM-Si.mobil	38640222xxx	In
	25.02.2012	23:43:21	0:00:02	0	SVNSM-Si.mobil	38640444xxx	In
	25.02.2012	23:45:04	0:00:02	0	SVNSM-Si.mobil	38640666xxx	In
	25.02.2012	23:46:37	0:00:02	0	SVNSM-Si.mobil	38640888xxx	In
	27.02.2012	9:51:56	1 E	0	SVNSM-Si.mobil		Out
	27.02.2012	9:53:05	1 E	0	SVNSM-Si.mobil		In
	27.02.2012	12:02:08	0:02:44	0	SVNSM-Si.mobil		Out
	27.02.2012	12:06:54	0:00:20	0	SVNSM-Si.mobil		Out
	27.02.2012	12:36:34	0:00:42	0	SVNSM-Si.mobil		Out
	27.02.2012	12:46:55	1 E	0	SVNSM-Si.mobil		Out
	27.02.2012	12:49:48	1 E	0	SVNSM-Si.mobil		In

Praktična "uporaba" :-)

GSM modul za odpiranje garažnih ali vhodnih vrat

Ponujamo vam uporabno napravo, ki z enostavnim telefonskim
garažna ali vhodna vrata.

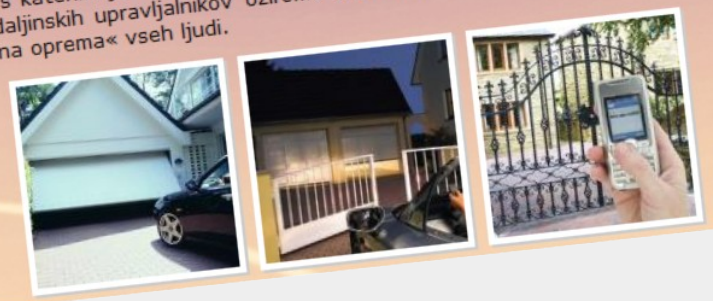
GSM modul je naprava, katero lahko avtorizirani uporabnik pokliče z
avtomatizirana vrata. Naprava prepozna največ pet določenih telefons
pokliče in se s takim klicem sproži odprtje ali zaprtje vrat.

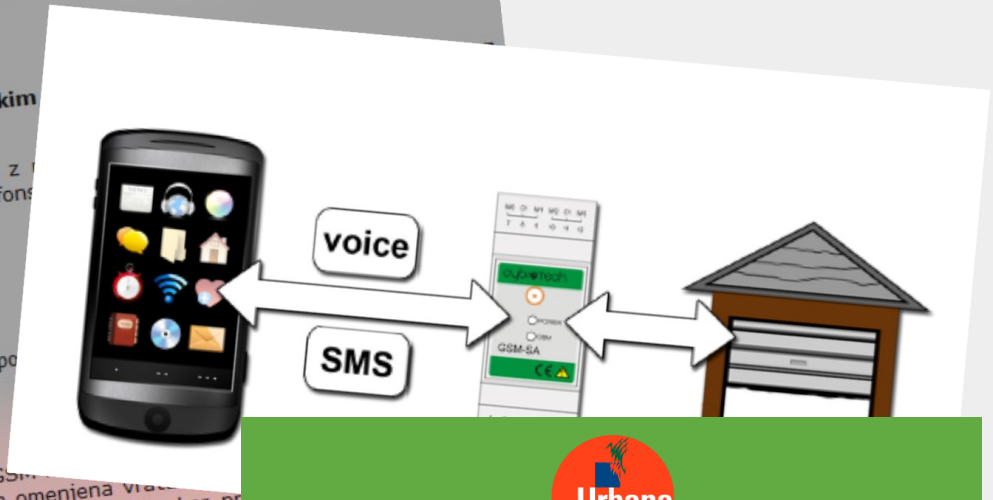
IKU d.o.o. vam nudi:

- dobavo paketa z navodili za uporabo,
- montažo na dogovorjena mesta (pokličite nas in poslali vam bomo po

Uporaba GSM modula za odpiranje vrat:

na avtomatizirana garažna, vhodna ali druga vrata se namesti GS
(mobilnih) številk, s katerimi je možno s hitrim telefonskim klicem omenjena vra
odpade uporaba daljinskih upravljalnikov oziroma dodatnih naprav in aparatov, ker pr
telefon že »obvezna oprema« vseh ljudi.





Urbana

SMS PARKING

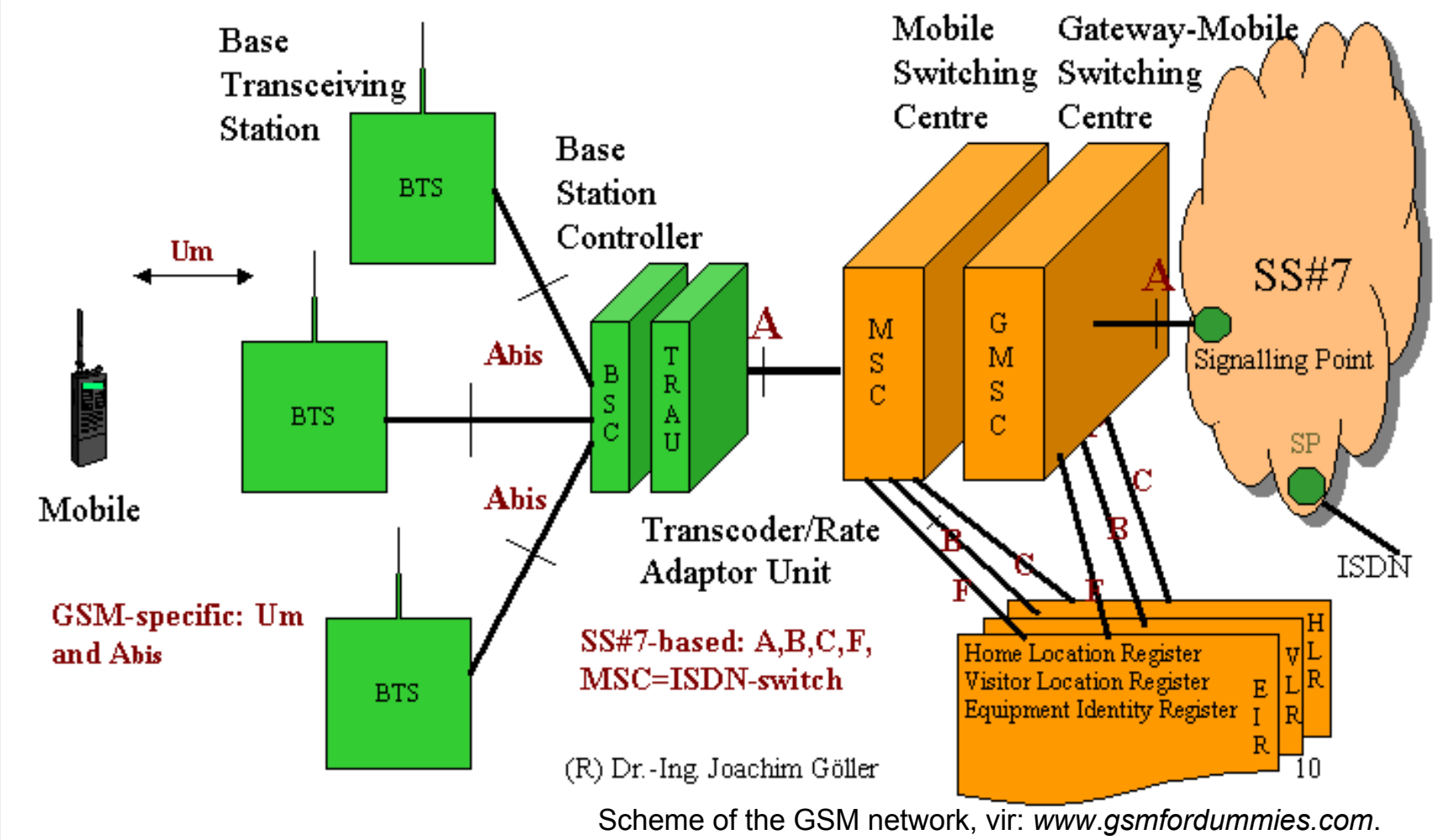
PLAČILO PARKIRNINE:

1. Na številko **041 20 20 10** pošljite SMS s cono, številko registrske tablice vozila in časom parkiranja s presledki za vozilo za katero želite plačati parkirnino.
   Primer plačila parkirnine v coni B1 za 2 uri: **B1 LJ1234 2**
2. Prejeli boste brezplačno povratno SMS sporočilo, ki velja kot dokazilo o plačilu parkirnine. Plača se vsaka začeta ura.

REGISTRACIJA / POLNITEV RAČUNA:

Polnitev URBANA SMS Parking računa se lahko izvede na vseh Urbanomatih ali prodajnih mestih za polnitev in prodajo kartice Urbana (TIC, Kiosk DELO prodaja, Trafika 3 DVA, Pošta Slovenije, Petrol, Mercator, Spar, itd.). Registracija računa se izvede samodejno ob prvi polnitvi.

Nekaj osnov o GSM tehnologiji



Scheme of the GSM network, vir: *www.gsmfordummies.com*.

SIM kartica in mobilna naprava, IMSI, TMSI, A5/x, "broadcast channels" in podatkovni kanali...

Zajemanje signala včasih...

1 Uporaba mobilnih telefonov s Calypso čipovjem...

```
Failed to connect to '/tmp/osmocom_sap'.
Failed during sap_open(), no SIM reader
<000e> cell_log.c:803 Scanner initialized
Mobile initialized, please start phone now!
<000e> cell_log.c:367 Measure from 0 to 124
c<000e> cell_log.c:367 Measure from 512 to 885
<000e> cell_log.c:367 Measure from 955 to 1023
<000e> cell_log.c:358 Measurement done
<000e> cell_log.c:340 Sync ARFCN 79 (rxlev -57, 197 syncs left)
<000e> cell_log.c:340 Sync ARFCN 19 (rxlev -64, 196 syncs left)
<000e> cell_log.c:340 Sync ARFCN 17 (rxlev -65, 195 syncs left)
<000e> cell_log.c:340 Sync ARFCN 113 (rxlev -65, 194 syncs left)
<000e> cell_log.c:340 Sync ARFCN 80 (rxlev -74, 193 syncs left)
<000e> cell_log.c:340 Sync ARFCN 18 (rxlev -81, 192 syncs left)
<000e> cell_log.c:190 Cell: ARFCN=18 MCC=293 MNC=40 (Slovenia, Si.mobil)
<000e> cell_log.c:340 Sync ARFCN 20 (rxlev -81, 191 syncs left)
<000e> cell_log.c:340 Sync ARFCN 107 (rxlev -81, 190 syncs left)
<000e> cell_log.c:340 Sync ARFCN 4 (rxlev -83, 189 syncs left)
<000e> cell_log.c:340 Sync ARFCN 114 (rxlev -84, 188 syncs left)
<000e> cell_log.c:340 Sync ARFCN 16 (rxlev -85, 187 syncs left)
<000e> cell_log.c:190 Cell: ARFCN=16 MCC=293 MNC=40 (Slovenia, Si.mobil)
<000e> cell_log.c:340 Sync ARFCN 81 (rxlev -85, 186 syncs left)
<000e> cell_log.c:340 Sync ARFCN 111 (rxlev -85, 185 syncs left)
<000e> cell_log.c:340 Sync ARFCN 112 (rxlev -86, 184 syncs left)
<000e> cell_log.c:190 Cell: ARFCN=112 MCC=293 MNC=41 (Slovenia, iPKO)
<000e> cell_log.c:340 Sync ARFCN 8 (rxlev -88, 183 syncs left)
<000e> cell_log.c:340 Sync ARFCN 85 (rxlev -89, 182 syncs left)
<000e> cell_log.c:340 Sync ARFCN 987 (rxlev -89, 181 syncs left)
<000e> cell_log.c:340 Sync ARFCN 14 (rxlev -90, 180 syncs left)
<000e> cell_log.c:340 Sync ARFCN 29 (rxlev -90, 179 syncs left)
<000e> cell_log.c:340 Sync ARFCN 110 (rxlev -92, 178 syncs left)
<000e> cell_log.c:340 Sync ARFCN 1014 (rxlev -93, 177 syncs left)
<000e> cell_log.c:340 Sync ARFCN 45 (rxlev -94, 176 syncs left)
<000e> cell_log.c:340 Sync ARFCN 66 (rxlev -94, 175 syncs left)
<000e> cell_log.c:340 Sync ARFCN 116 (rxlev -94, 174 syncs left)
<000e> cell_log.c:340 Sync ARFCN 77 (rxlev -95, 173 syncs left)
<000e> cell_log.c:340 Sync ARFCN 979 (rxlev -95, 172 syncs left)
<000e> cell_log.c:340 Sync ARFCN 118 (rxlev -96, 171 syncs left)
<000e> cell_log.c:340 Sync ARFCN 119 (rxlev -96, 170 syncs left)
<000e> cell_log.c:340 Sync ARFCN 983 (rxlev -96, 169 syncs left)
<000e> cell_log.c:340 Sync ARFCN 986 (rxlev -96, 168 syncs left)
Terminal 0  Terminal 1  Terminal 2  Terminal 3  Terminal 4
```

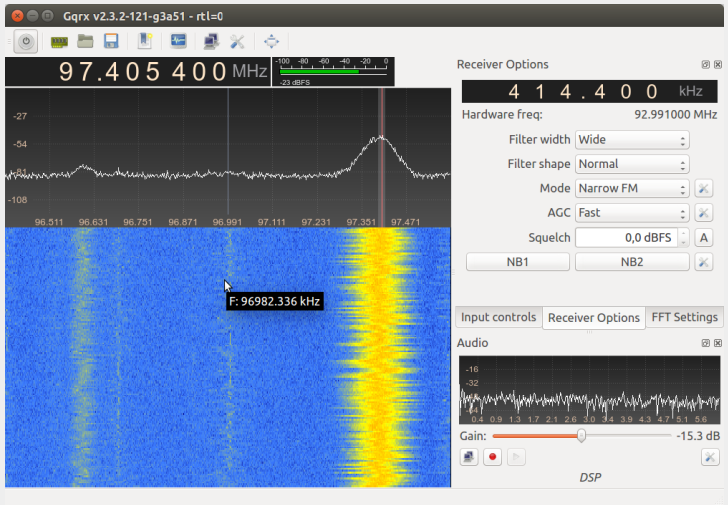
```
matej@cryptopia: ~/osmocom/osmocom-bb-raw/src/host/osmocon
Die ID code: 7e540b2fc90393bb
================================================================================
REG_DPLL=0x2413
CNTL_ARM_CLK=0xf0a1
CNTL_CLK=0xff91
CNTL_RST=0xfff3
CNTL_ARM_DIV=0xfff9
================================================================================
Power up simcard:


THIS FIRMWARE WAS COMPILED WITHOUT TX SUPPORT!!!
Assert DSP into Reset
Releasing DSP from Reset
Installing DSP sniff patch
Setting some dsp_api.ndb values
Setting API NDB parameters
DSP Download Status: 0x0001
DSP API Version: 0x0000 0x0000
Finishing download phase
DSP Download Status: 0x0002
DSP API Version: 0x3606 0x0000
LOST 3901!
LOST 3750!
```

2 Povezava telefona in računalnika s posebnim kablom in nalaganje spremenjenega ROM-a...

3 Poganjanje aplikacij za zajem in analizo.

Zajemanje signala danes...

DVB-T naprava (z Elonics 4000 čipom; ~20 EUR).

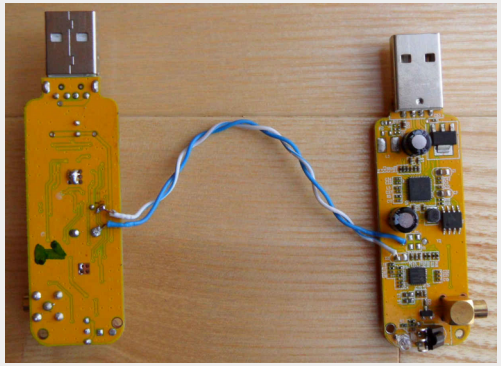


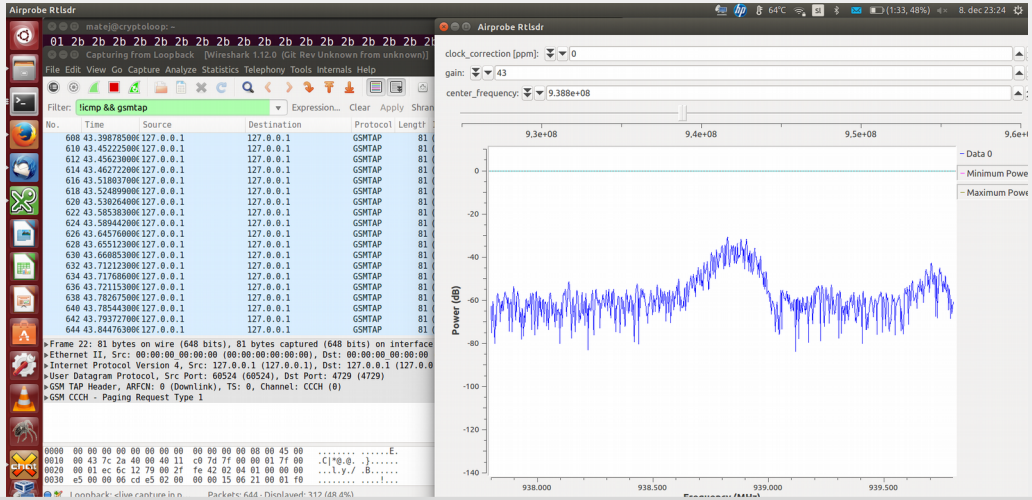
gr-gsm

Orodje za zajem in analizo GSM signalov.

```
grgsm_livemon -p 35 -f 938.8M
```

```
wireshark -k -Y '!icmp && gsmtap' -i lo
```

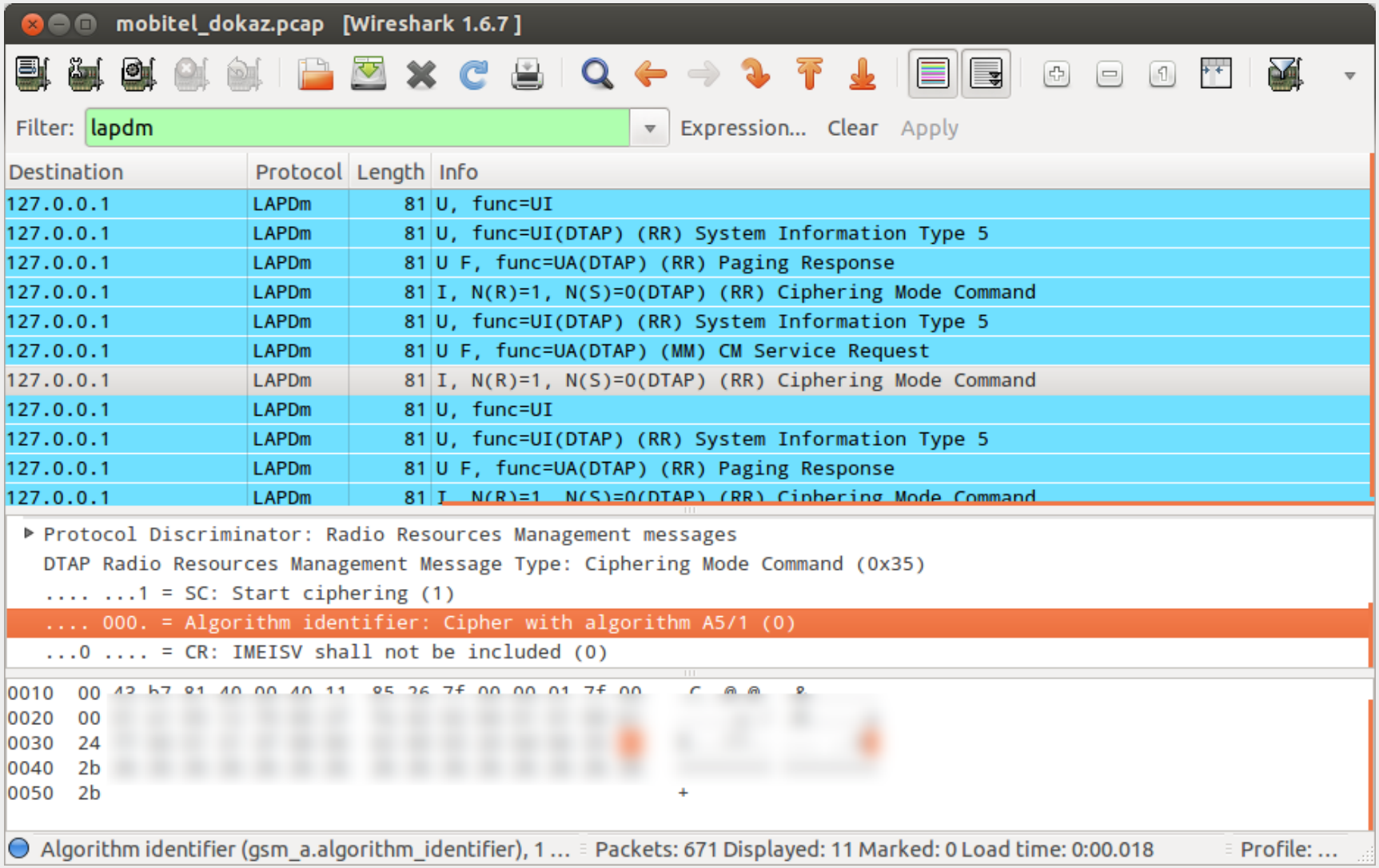





```
grgsm_scanner -p 35
```

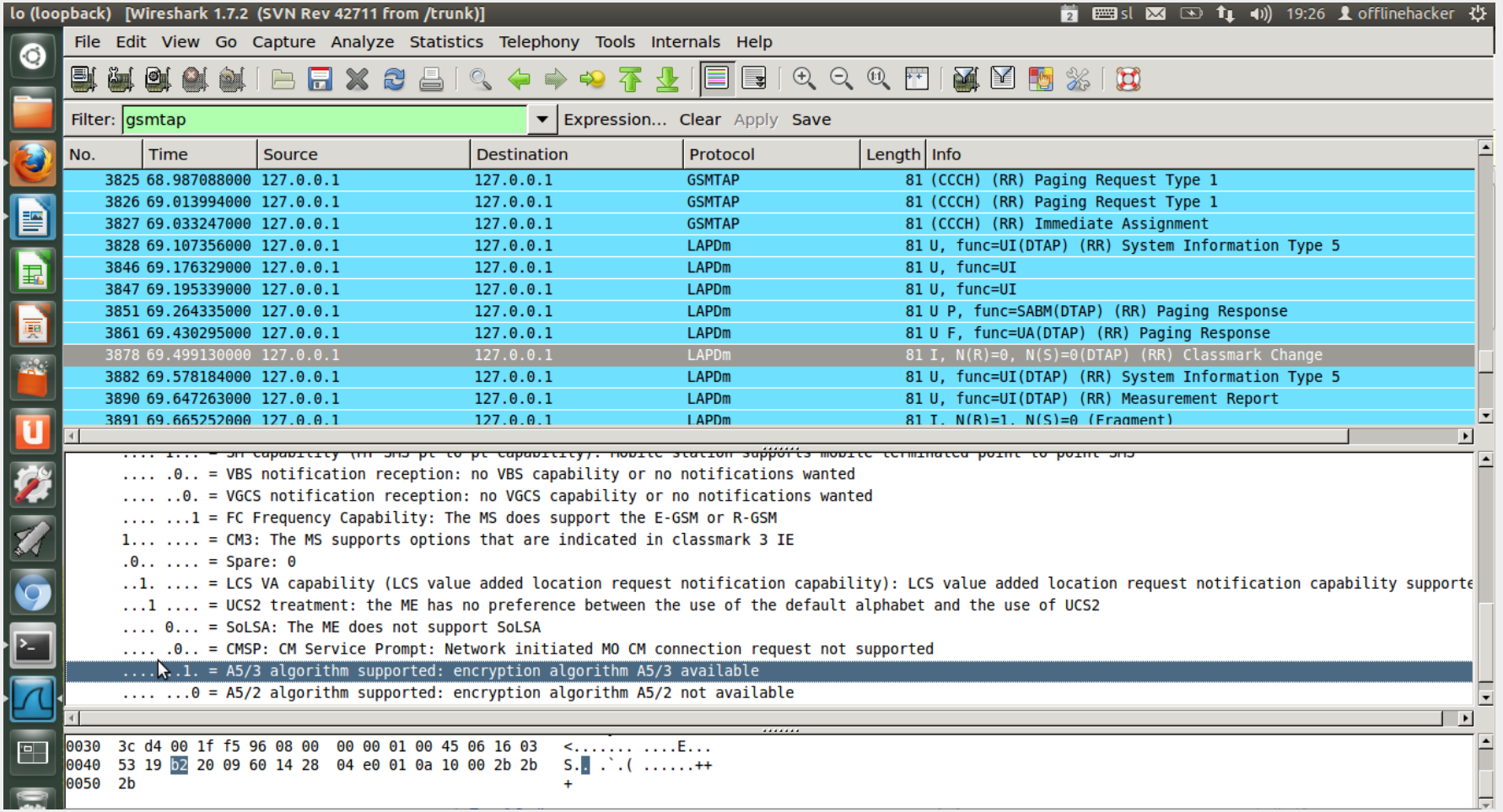
```
linux; GNU C++ version 4.9.1; Boost_105500; UHD_003.007.003-0-unknown


ARFCN:   18, Freq:  938.6M, CID:     0, LAC:   100, MCC: 293, MNC:  40, Pwr: -35
ARFCN:   24, Freq:  939.8M, CID:  1313, LAC:   100, MCC: 293, MNC:  40, Pwr: -33
ARFCN:   26, Freq:  940.2M, CID:   501, LAC:   100, MCC: 293, MNC:  40, Pwr: -27
ARFCN:  124, Freq:  959.8M, CID:     0, LAC:     0, MCC:   0, MNC:   0, Pwr: -29
```

Varnostna analiza GSM v letu 2012



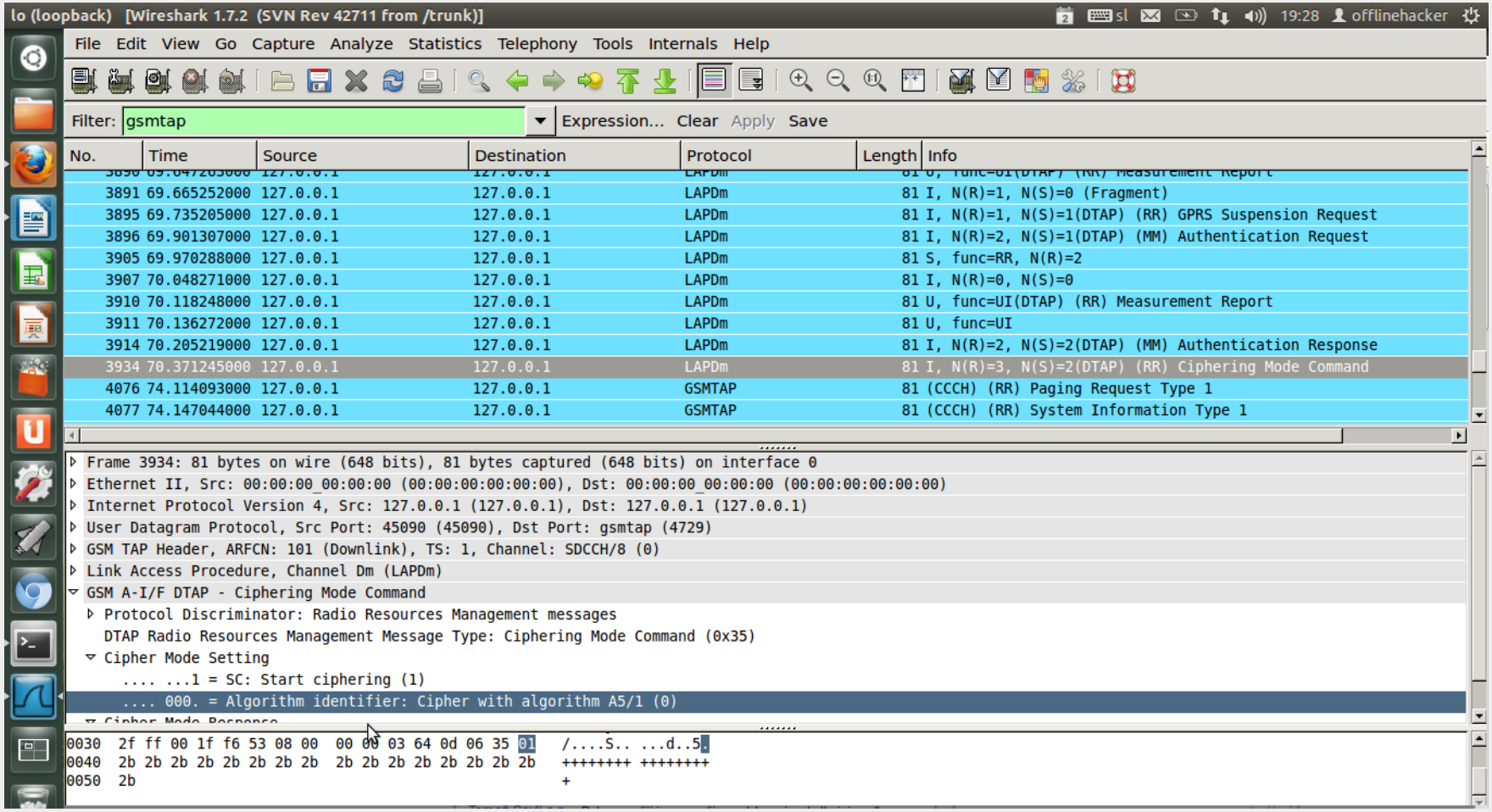
Nekateri operaterji so uporabljali šifrirni algoritem A5/1...

Varnostna analiza GSM v letu 2012



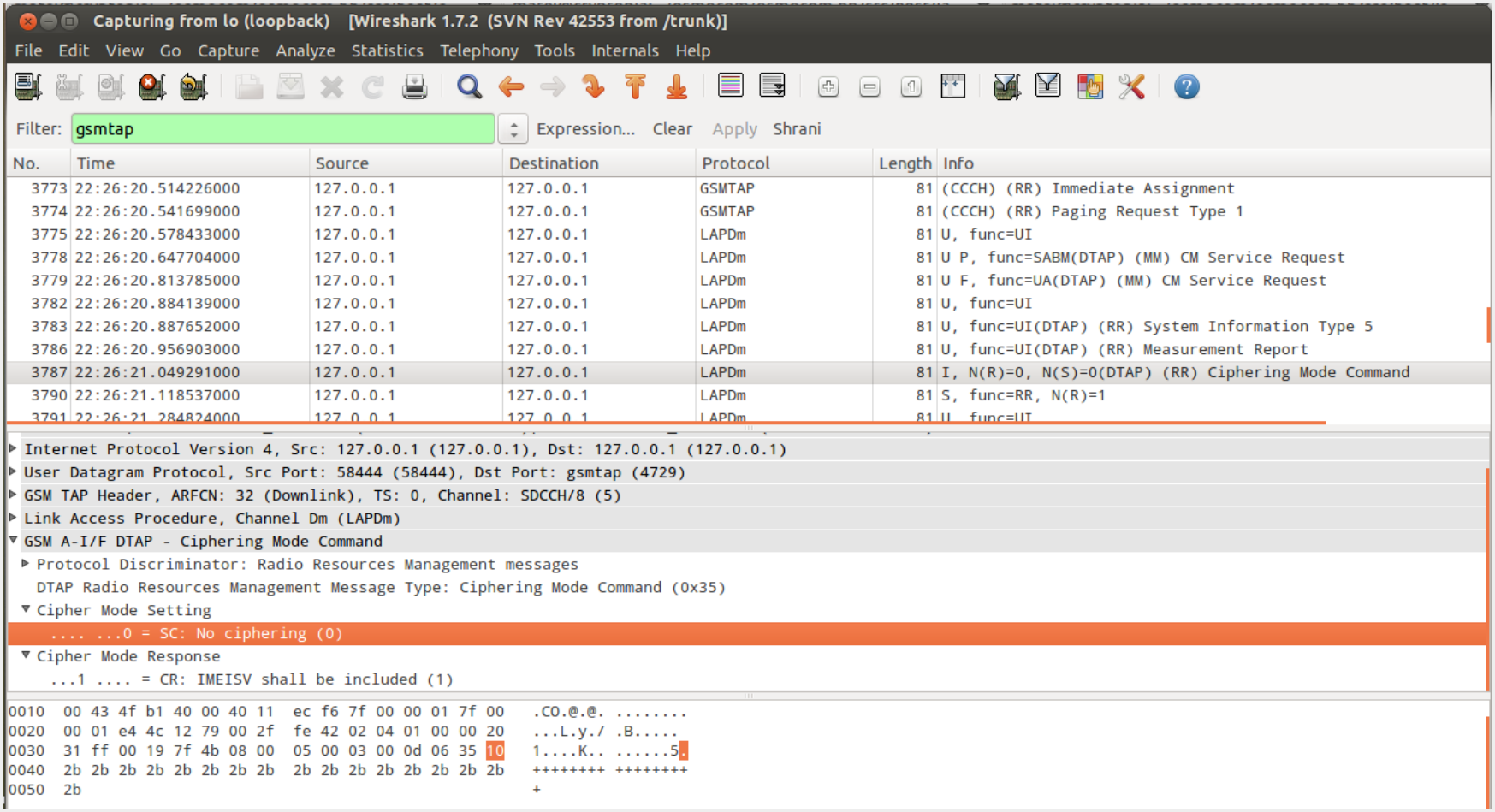
Če je mobilni telefon rekel, da podpira A5/3...

Varnostna analiza GSM v letu 2012



...je omrežje odvrnilo, da podpira samo A5/1.

Varnostna analiza GSM v letu 2012

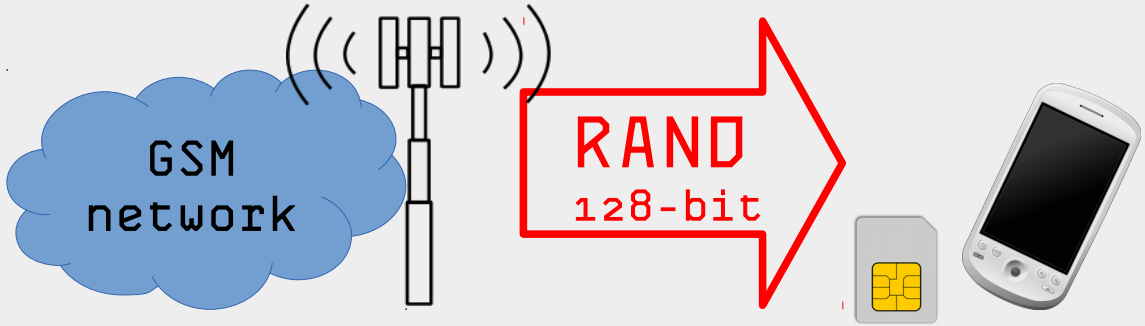


V enem omrežju je bilo mogoče celo izključiti šifriranje...

GSM šifriranje

Šifrirni ključ ***Ki*** je shranjen na SIM kartici in v HLR registru. Sejni šifrirni ključ ***Kc*** se izračuna s pomočjo ***Ki*** in se uporablja za šifriranje SMS iz govorne komunikacije.

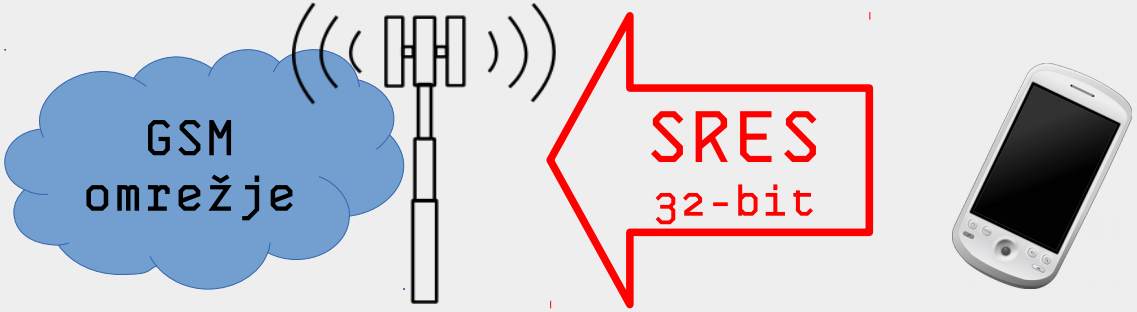
1.



HLR: Ki + **RAND** @ A3 = **SRES**

SIM kartica: Ki + **RAND** @ A3 = **SRES**

2.



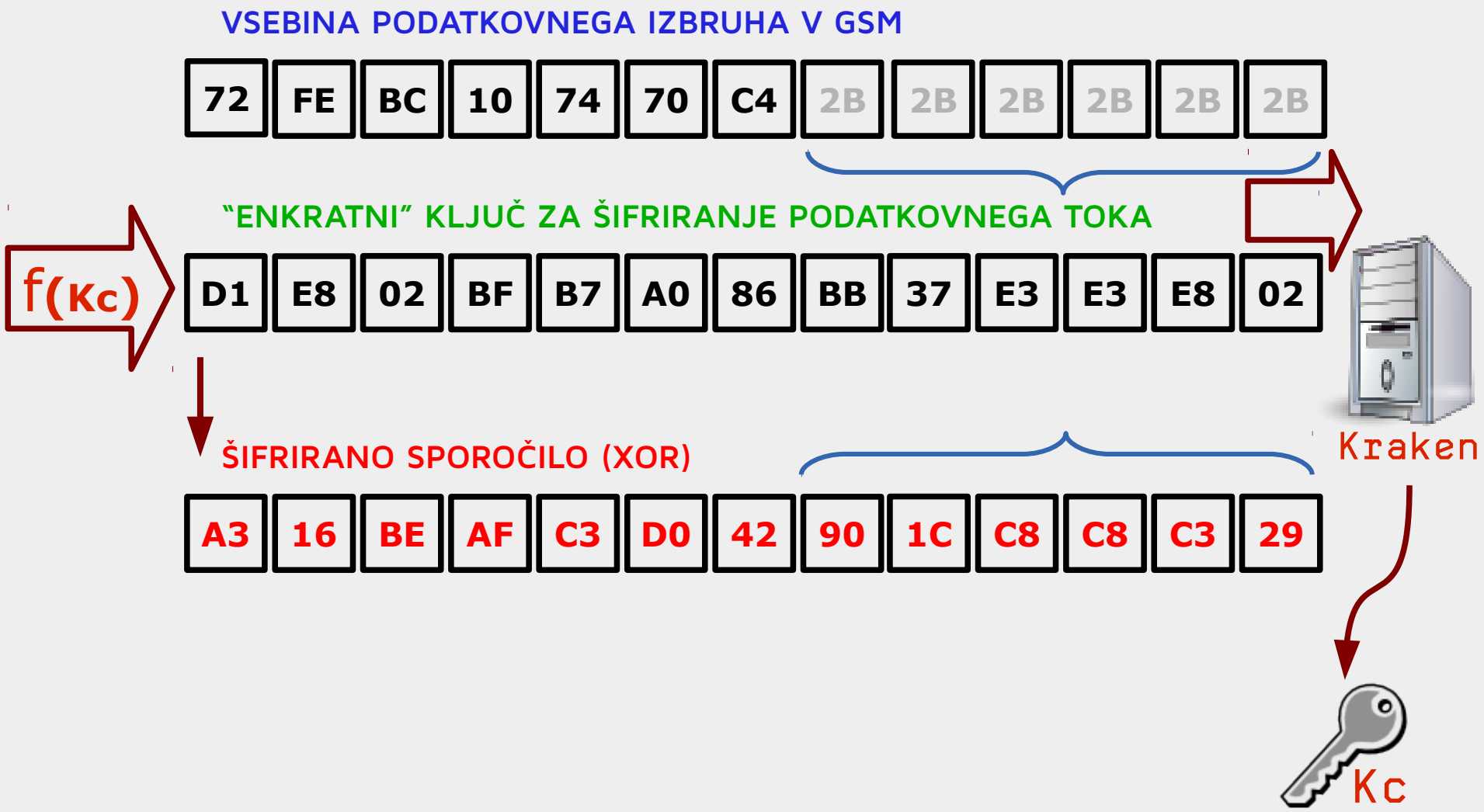
GSM šifriranje

3. Na obeh straneh se izračuna Kc (z uporabo algoritma A8):
Ki + RAND @ A8 = **Kc**

4.

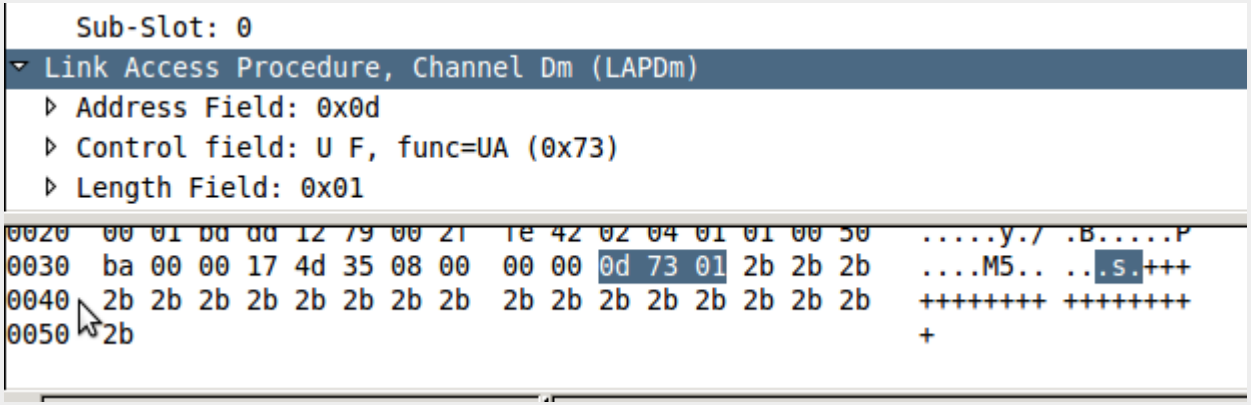
Če je SRES na obeh straneh enak, imata omrežje in mobilni telefon enak Kc. To pomeni, da je sejni ključ »izmenjan« ne da bi bil prenesen čez omrežje. Zdaj se podatki šifrirajo z Kc + A5/x. »Po zraku« se prenašajo samo šifrirani podatki.

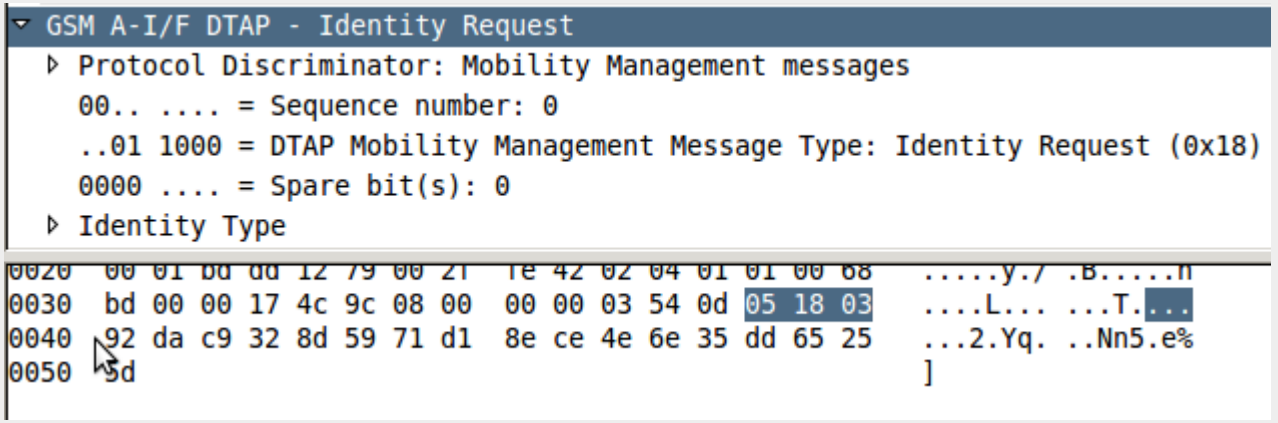
Kriptoanaliza GSM komunikacije



Nakljućno vs. nenakljućno bitno zapolnjevanje

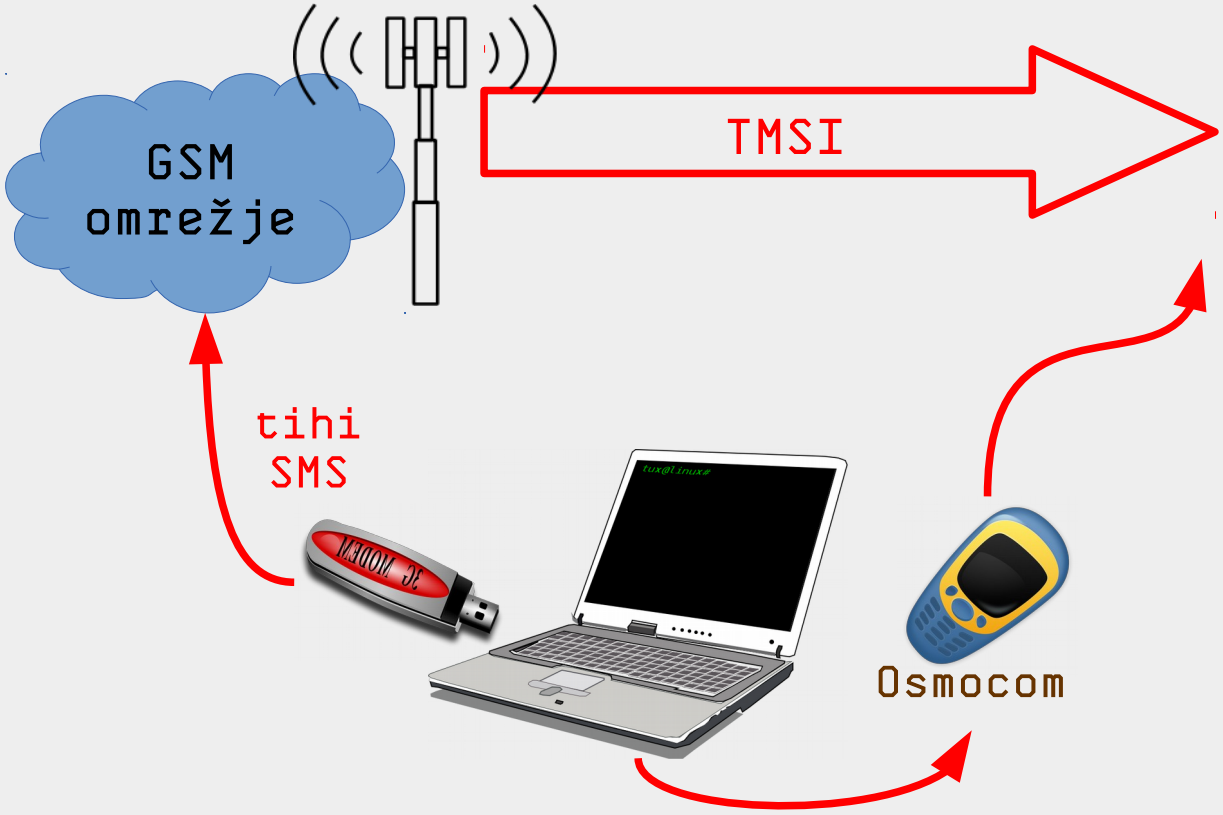
(*Random padding* vs. *non-random padding*)





Lociranje uporabnika v mobilnem omrežju

Na mobilno številko pričnemo pošiljati tihe SMS. Hkrati na omrežju opazujemo katera TMSI številka prejema (šifrirane) podatke.



Mobilni telefon ne prikaže tihega SMS sporočila.

Kriptoanaliza v praksi

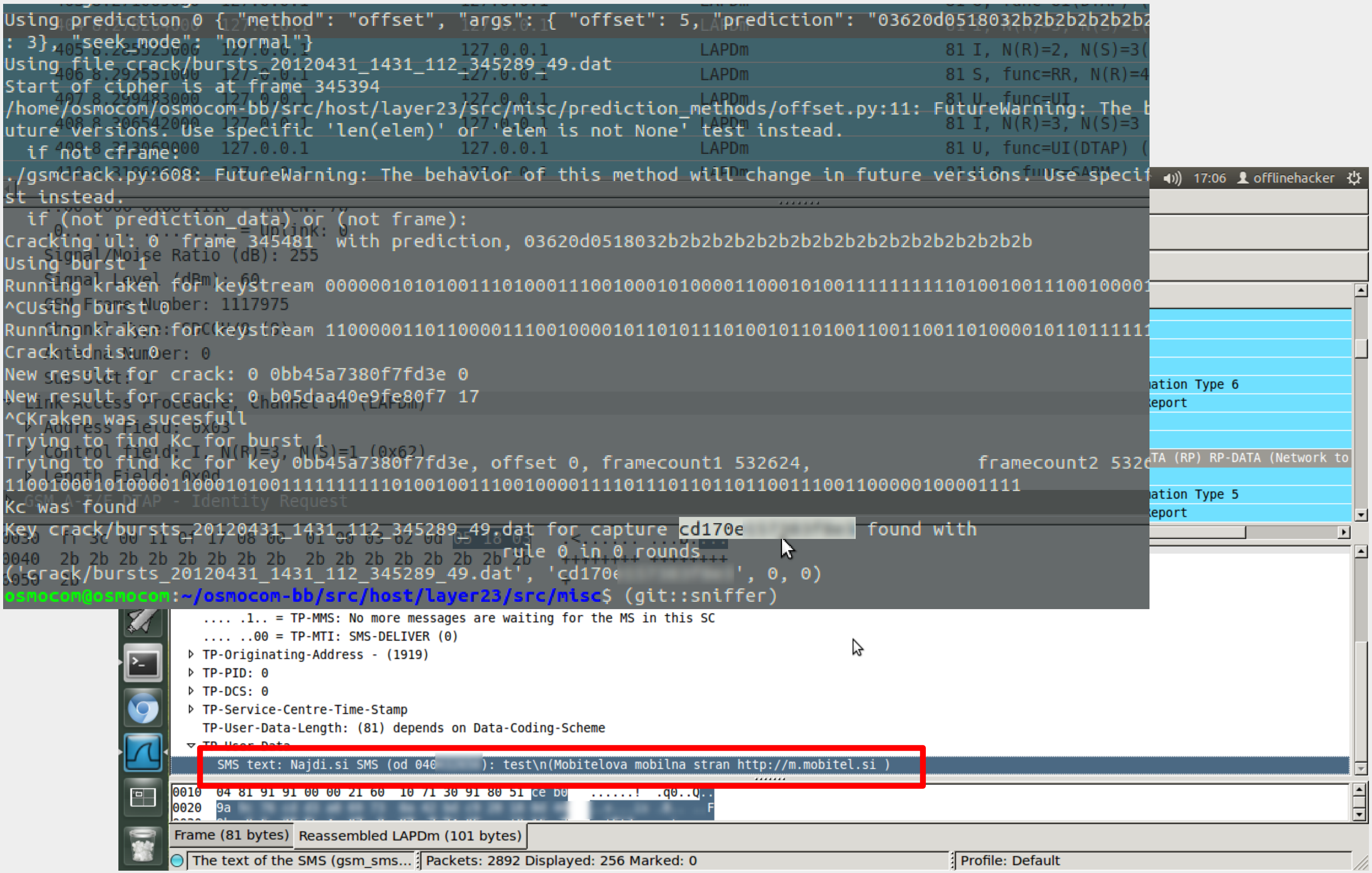
A3	16	BE	AF	C3	D0	42	90	1C	C8	C8	C3	29

VSEBINA PODATKOVNEGA IZBRUHA V GSM

72	FE	BC	10	74	70	C4	2B	2B	2B	2B	2B	2B

- »Iz zraka« pasivno zajamemo šifrirane podatkovne pakete.
- Z ugibanjem vsebine GSM izbruha (ugibanjem zapolnitvenih bitov) izračunamo »enkratni« šifrirni ključ.
- S pomočjo kriptoanalize rekonstruiramo sejni ključ Kc.
- V procesu ne potrebujemo fizičnega dostopa ne do SIM kartice, ne do mobilnega telefona niti do mobilnega omrežja!

Kriptoanaliza v praksi

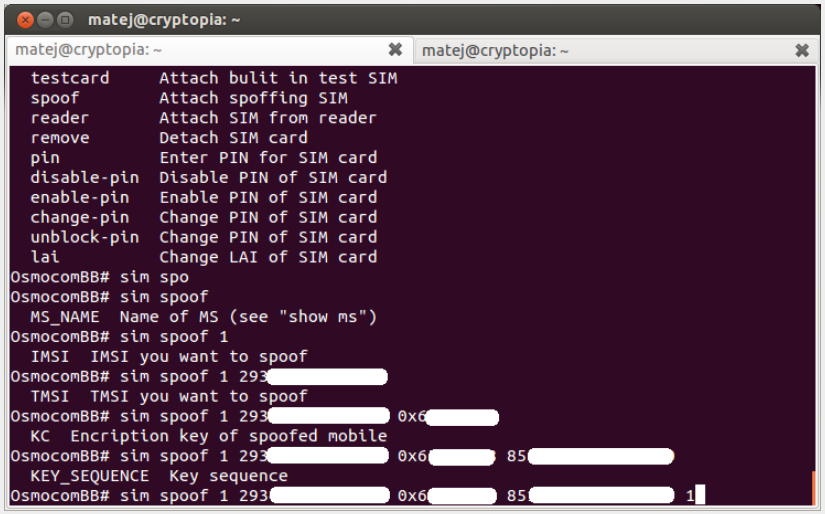


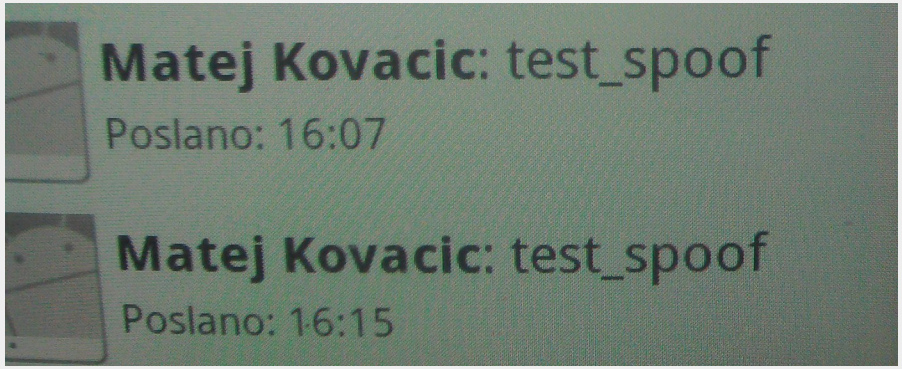
Ponarejanje mobilne *identitete*

Za ponarejanje mobilne **identitete** potrebujemo:

- IMSI številka (jo pridobimo z SS7 vpogledom),
- TMSI številka (jo zajamemo iz omrežja),
- sejni šifrirni ključ (ga pridobimo s kriptoanalizo),
- zaporedna številka ključa (ang. *key sequence number* – jo zajamemo iz omrežja).

Če omrežje uporablja A5/0, potrebujemo samo TMSI in zaporedno številko ključa – kriptoanaliza ni potrebna!

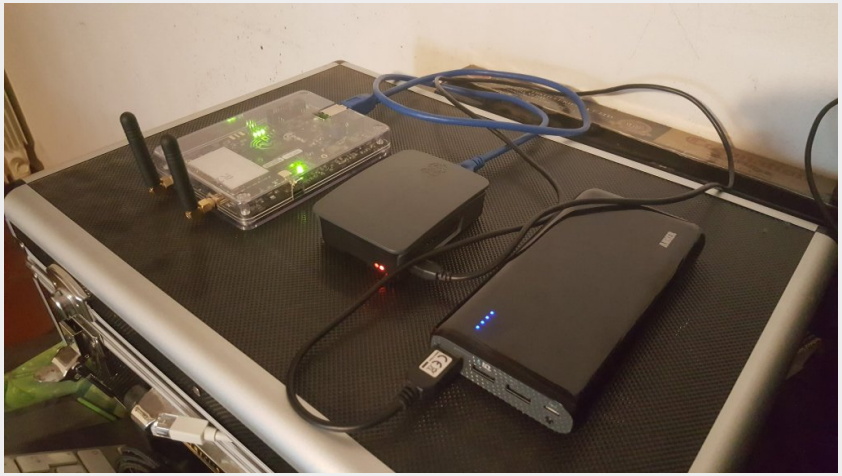


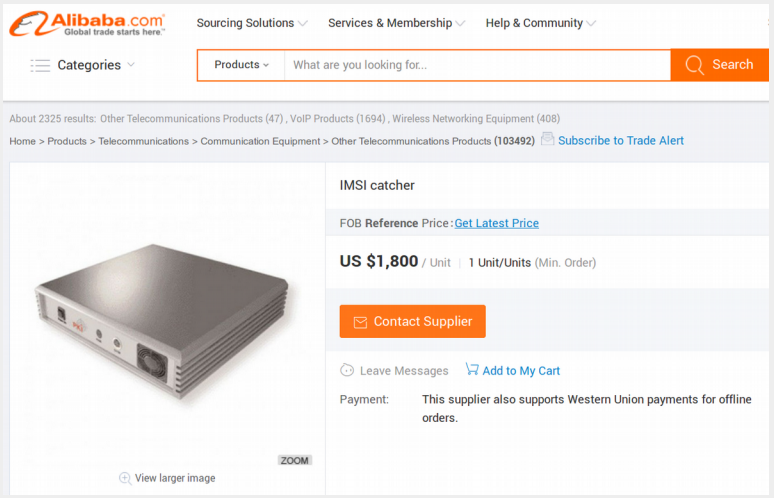


Dve SMS sporočili poslani z lažno mobilno identiteto.

Lovilci IMSI številk

V osnovi so to lažne bazne postaje.





IMSI lovilci – kako delujejo?

Najprej se lažno predstavijo kot legitimna bazna postaja nekega omrežja.

Nato mobilnim telefonom v bližini sporočijo lažno LAC kodo (*Location Area Code*).

Zdaj mobilni telefoni kontaktirajo IMSI lovilec (z tim. *Location Update* proceduro), a s svojo TMSI številko.

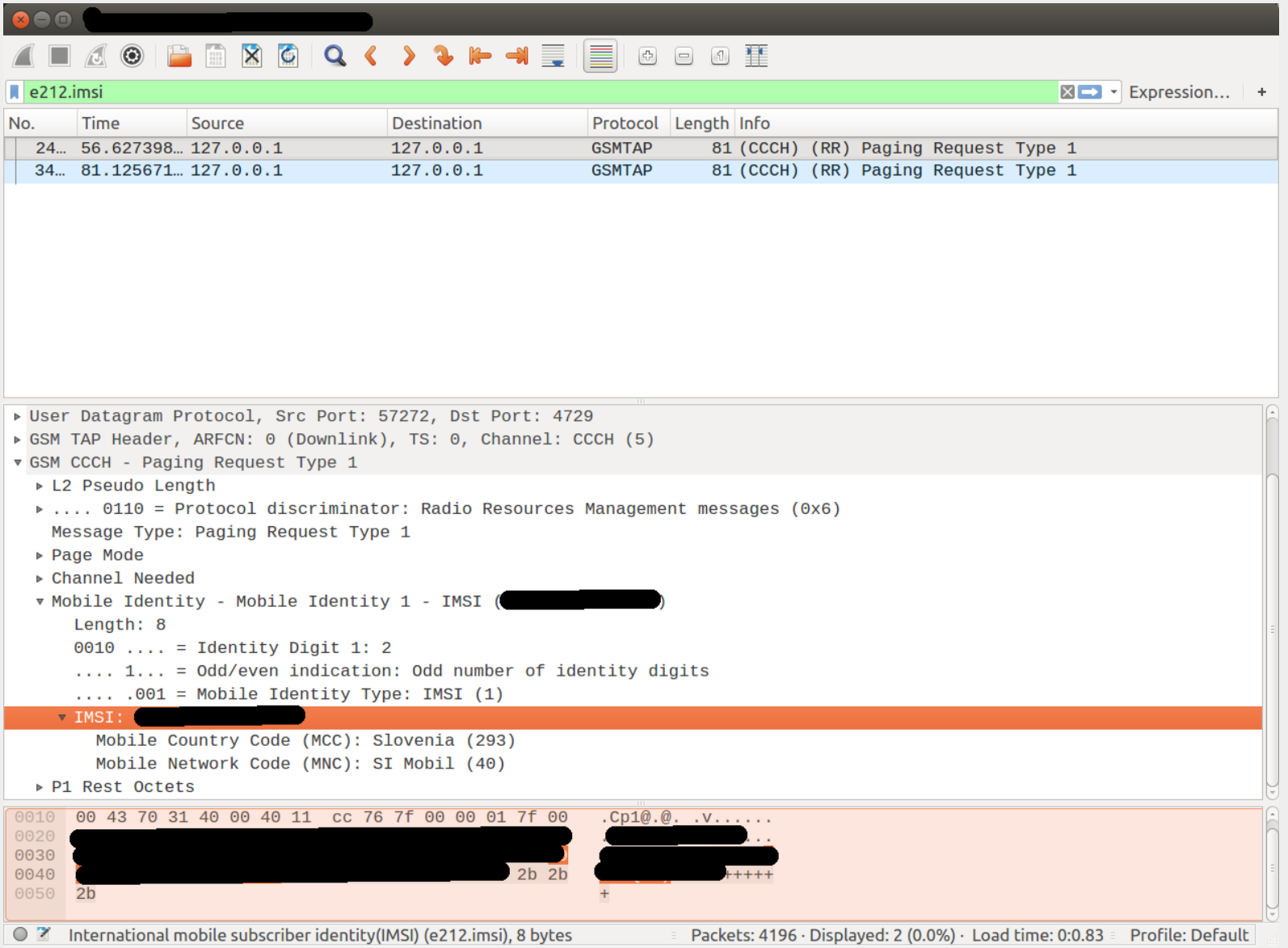
IMSI lovilec se zdaj zlaže, da je TMSI številka potekla in zahteva ponovno avtentikacijo (tim. *re-authentication*).

Mobilni telefoni zdaj lovilcu javijo svoji IMSI in IMEI številki.

IMSI lovilec zdaj reče, da ne more sprejeti telefona (*Location Update Reject*) in ga preusmeri nazaj k izvornemu omrežju.

Ali pa tudi ne... v tem primeru lovilci s telefonom lahko počnejo še marsikaj...

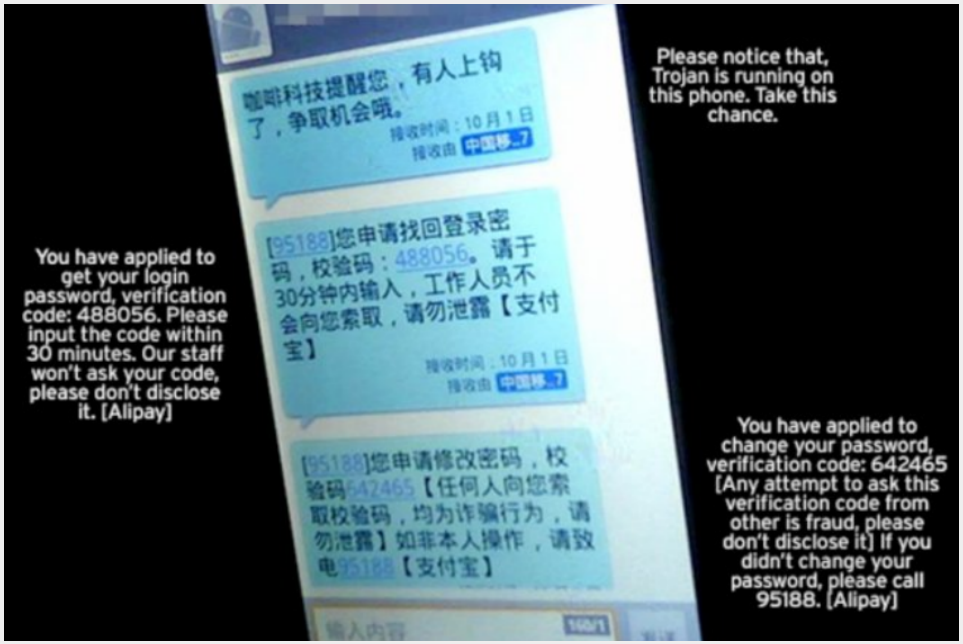
IMSI lovilci – jih lahko zaznamo?



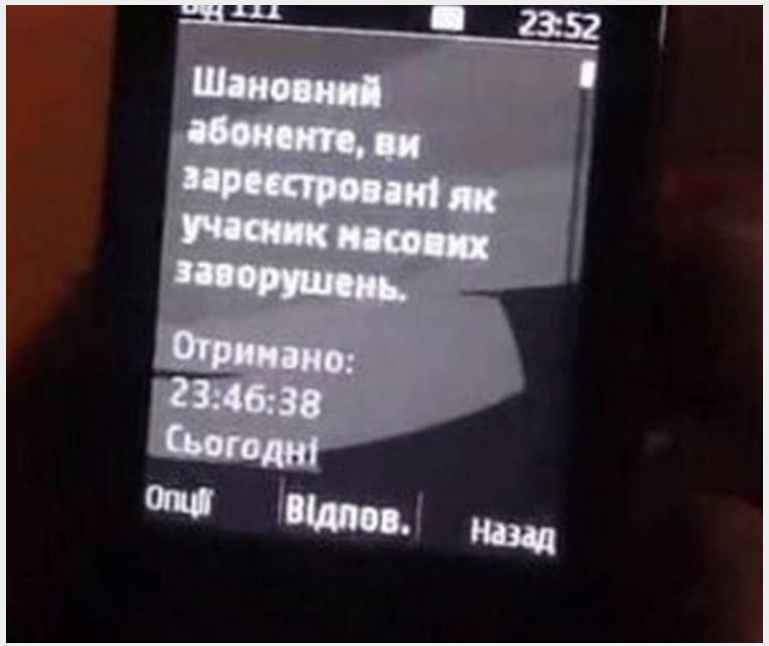
IMSI lovilci – kaj zmorejo?

IMSI lovilci lahko:

- **razkrijejo lokacijo** mobilnega telefona,
- mobilnemu telefonu ponudijo omrežno povezljivost in izvedejo **napad s posrednikom** (tim. **MITM napad**),
- pokličejo telefon ali mu pošljejo SMS **mimo omrežja**.



Kitajska SMS SPAM sporočila.

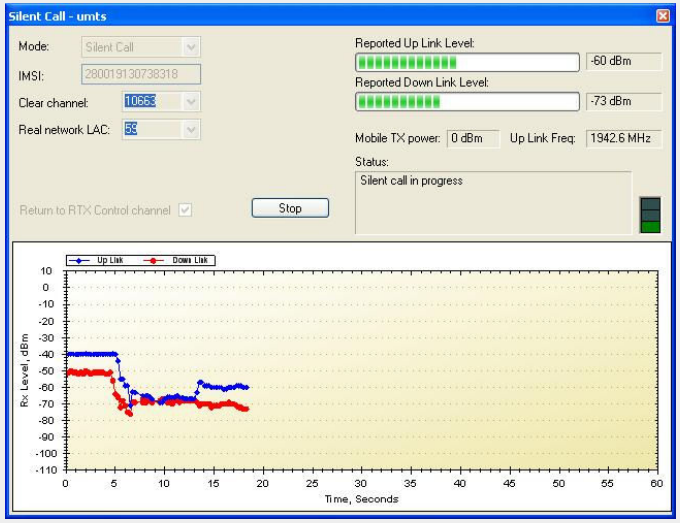


Ukrajina – sporočilo protestnikom.

IMSI lovilci – kaj zmorejo?

IMSI lovilci lahko tudi:

- **izolirajo** mobilni telefon od omrežja,
- mobilni telefon **začasno onemogočijo** (tako, da je potreben ponovni zagon) ali mu hitro **izpraznijo baterijo**,
- izvedejo **tihi klic**, kar omogoča prisluškovanje okolici telefona,
- na daljavo **namestijo zlonamerno programsko opremo** (tim. *baseband attack*).



UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- X

IN THE MATTER OF AN APPLICATION OF :
THE UNITED STATES OF AMERICA FOR
AUTHORIZATION TO CONTINUE TO :
INTERCEPT ORAL COMMUNICATIONS
OCCURRING AT (i) THE SEATING AREA :
INSIDE BRUNELLO TRATTORIA, 227 EAST
MAIN STREET, NEW ROCHELLE, NEW YORK :
10801; (ii) THE SEATING AREA INSIDE
MARIO'S RESTAURANT, 2342 ARTHUR :
AVENUE, BRONX, NEW YORK 10458;
(iii) THE SEATING AREA INSIDE :
AGOSTINO'S RESTAURANT, 969 BOSTON
POST ROAD, NEW ROCHELLE, NEW YORK :
10801; AND (iv) THE SEATING AREA
INSIDE THE MARINA RESTAURANT, WRIGHT :
ISLAND MARINA, 290 DRAKE AVENUE, NEW

APPLICATION FOR AN
ORDER AUTHORIZING THE
INTERCEPTION OF ORAL
COMMUNICATIONS

Nekateri SS7 napadi

Signalling System #7 je protokol za izmenjavo podatkov med telefonskimi operaterji.

SS7 omogoča dostop do Home Location Registra, Visitor Location Registra in Mobile Switching Centra...

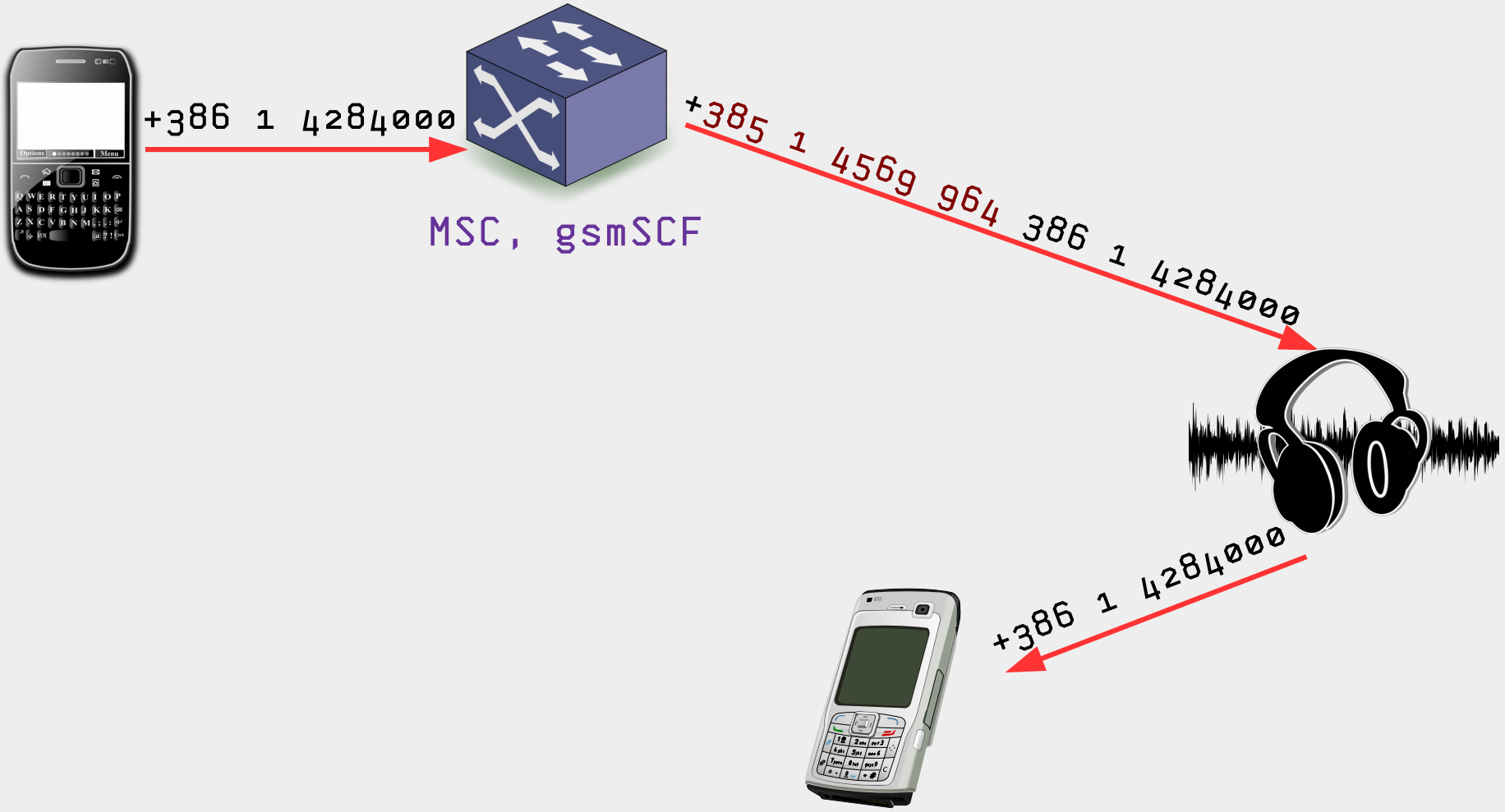
Vendar pa je avtentikacija v SS7 pomanjkljiva. Zato je z zlorabo SS7 mogočih nekaj zanimivih napadov...

Legitimna uporaba: CAMEL (*Customised Applications for Mobile networks Enhanced Logic*):

- Uporabnik gostuje v tujem omrežju.
- Uporabnikov HLR pove gostujočemu VLR, naj MSC pred vsakim klicem, ki ga želi opraviti uporabnik, kontaktira gsmSCF (*GSM Service Control Function*) v domačem omrežju in vpraša kaj naj stori s klicem.
- Če uporabnik kliče "lokalno številko", gsmSCF številko prepiše v mednarodni format (+386...) in sporoči MSCju naj pokliče to številko.

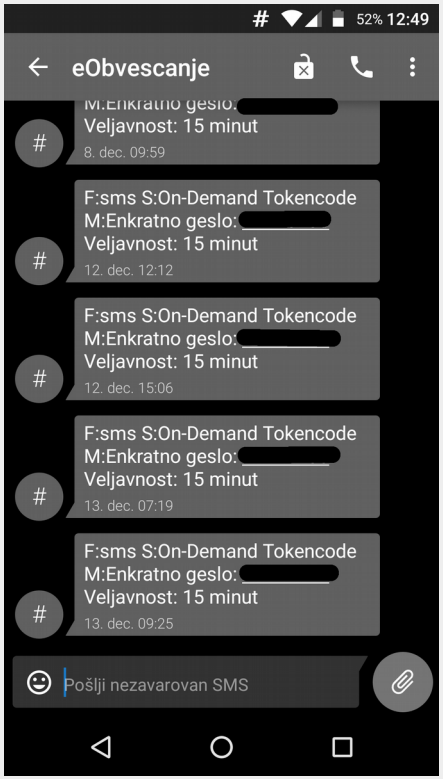
Primer: preusmerjanje odhodnih klicev

gsmSCF funkcijo pa je mogoče tudi zlorabiti...



Primer: preusmerjanje dohodnih klicev

Napadalec se pretvarja, da uporabnik gostuje v njegovem omrežju... Od te točke dalje so vsi dohodni klici in SMS sporočila preusmerjeni k napadalcu.



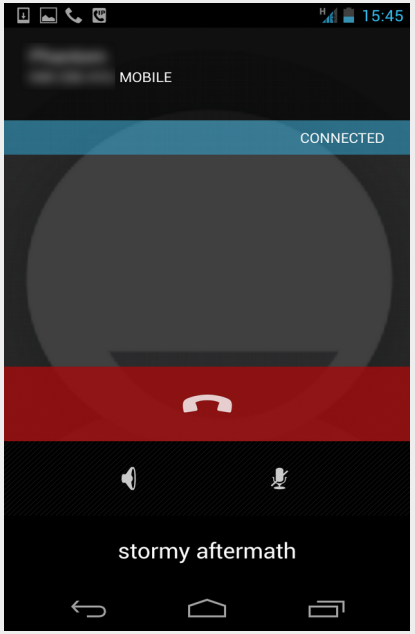
Zdaj se žrtev želi prijaviti v bančni račun. Ker uporablja dvofaktorsko avtentikacijo, ji banka pošlje SMS sporočilo z mTAN dostopno kodo...

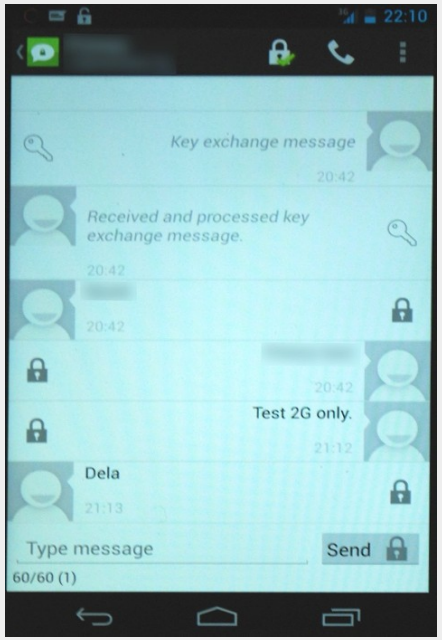
Ali pa se žrtev želi prijaviti v interno omrežje slovenske vlade... :-)

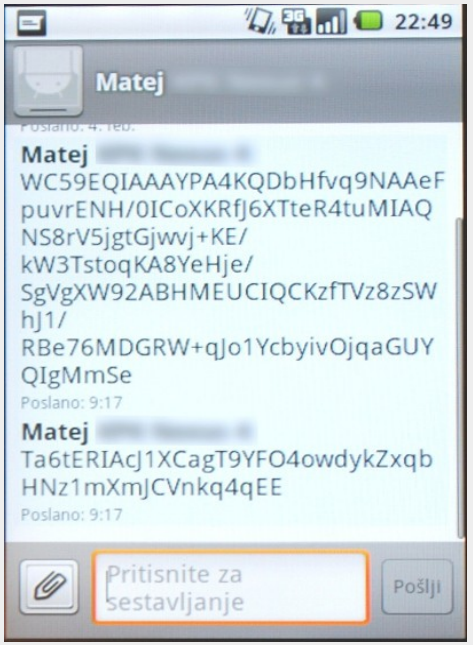

BUSTED!

Zaščita

Šifriranje mobilnih komunikacij

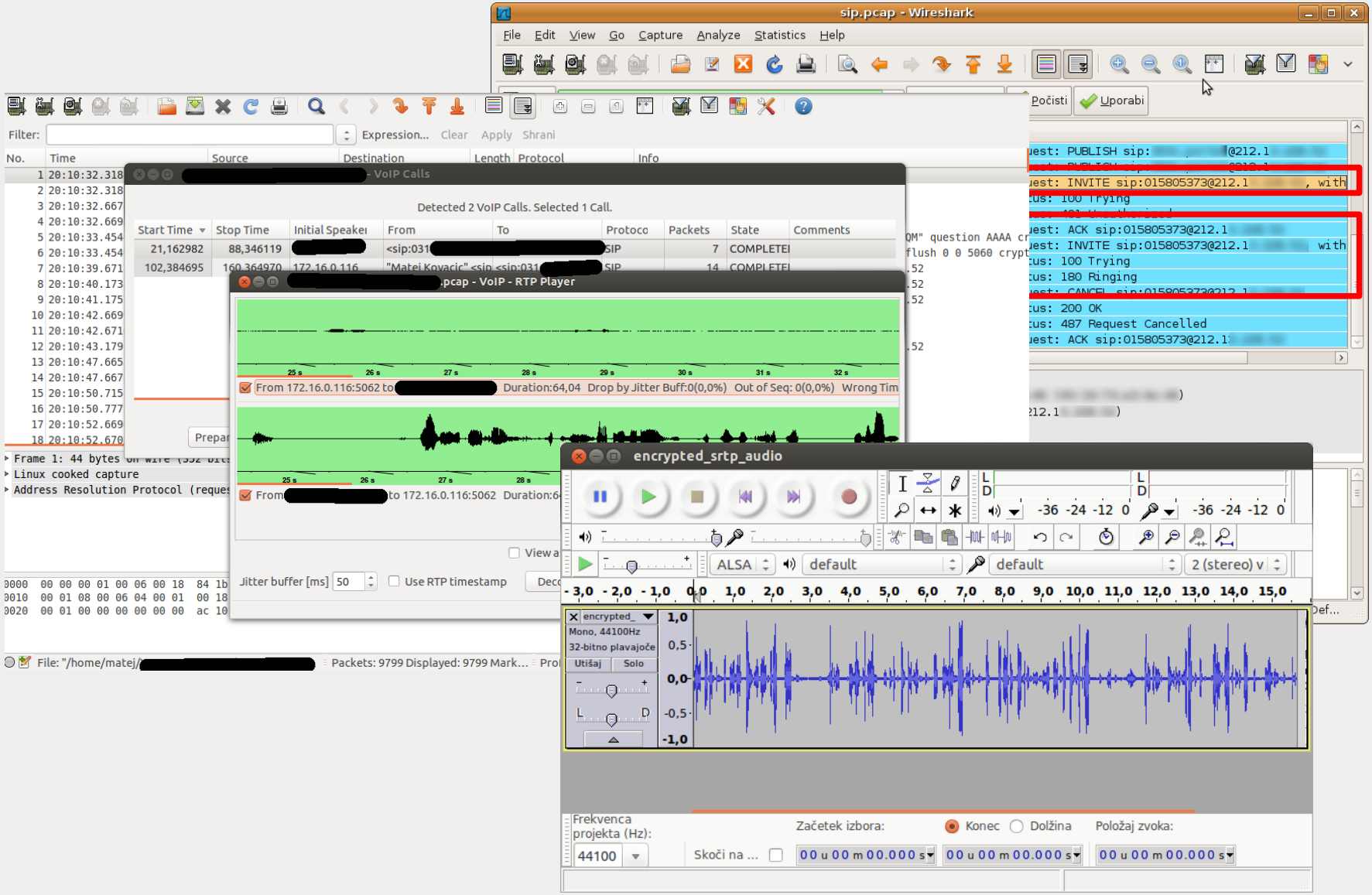






Rešitev: uporaba podatkovnega prenosa in šifriranje komunikacij na nivoju aplikacij.

Nešifriran in šifriran telefonski klic



Aplikacija Signal

Za šifriranje mobilnih komunikacij obstaja več aplikacij.

Ena izmed boljših je aplikacija Signal, podjetja Open Whisper Systems. Na tehnični ravni uporablja:

- močne šifrirne algoritme,
- poudarjeno zaupnost (*perferct forward secrecy* ter *future secrecy*),
- zaznavanje napadov s posrednikom (MITM napadov),
- šifriranje od začetne do končne točke (tim. »end-to-end« šifriranje),
- podporo asinhroni komunikaciji,
- šifrirno lokalno shrambo sporočil.

Tehnična rešitev **preprečuje** prisluškovanje na omrežju ter s strani operaterja.

Aplikacija Signal

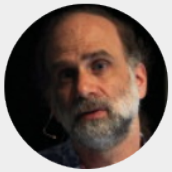
Uporabniški vidik:

- enostavna za uporabo,
- brezplačna,

“After reading the code, I literally discovered a line of drool running down my face. It’s really nice.

— **Matt Green**, Cryptographer, Johns Hopkins University

- odprtokodna,
- aplikacija je bila varnostno preverjena.



“I am regularly impressed with the thought and care put into both the security and the usability of this app. It's my first choice for an encrypted conversation.

— **Bruce Schneier**, internationally renowned security technologist

“Signal is the most scalable encryption tool we have. It is free and peer reviewed. I encourage people to use it everyday.

— **Laura Poitras**, Oscar winning filmmaker and journalist

Aplikacija Signal

Na strežnikih se beleži minimalno število prometnih podatkov.

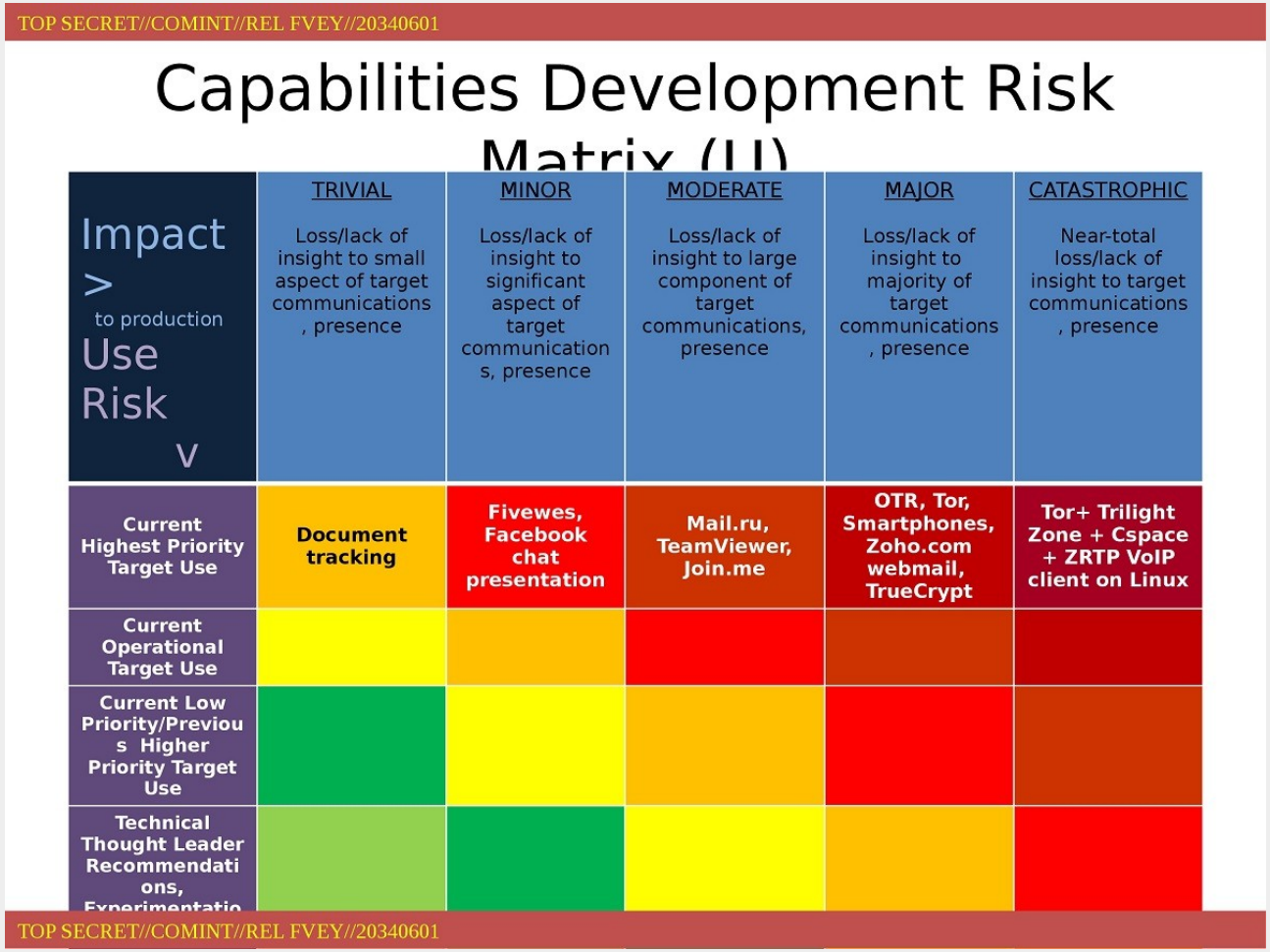
Attachment A

Account	Information
[redacted]	N/A
[redacted]	Last connection date: [redacted] Unix millis Account created: [redacted] Unix millis

Mogoča je dodatna anonimizacija:

- uporaba OWS posredniškega strežnika,
- registracija "nepovezane telefonske številke",
- teoretično: uporaba preko Tor omrežja,
- aplikacija vsebuje tudi tehnologije za zaobid cenzure (tim. *domain fronting*).

Tehnologijo »priporoča« celo NSA! :-)



Things become "catastrophic" for the NSA at level five - when, for example, a subject uses a combination of Tor, another anonymization service, the instant messaging system CSpace and a system for Internet telephony (voice over IP) called ZRTP. This type of combination results in a "near-total loss/lack of insight to target communications, presence," the NSA document states. (Der Spiegel)

Signal protokol

Pri Open Whisper Systems so v letu 2013 razvili kriptografski protokol Signal.

Trenutno je protokol implementiran v:

- *Facebook Messenger* (od julija 2015) – mesečno ima okrog milijardo uporabnikov,
- *WhatsApp* (od aprila 2016) – ima več kot milijardo registriranih uporabnikov,
- *Google Alo* (od septembra 2016) – od oktobra 2016 je Google Alo privzeta aplikacija za sporočila na Pixel mobilnih telefonih,
- *Viber* (od maja 2015) – implementiran samo delno – ima več kot 100 milijonov mesečno aktivnih uporabnikov.

Vseeno pa je aplikacija Signal še zdaleč najbolj varna rešitev.

Anonimnost mobilnih komunikacij

Uporaba anonimizacijskih tehnologij povečuje latenco. Zato realnočasovna (govorna) komunikacija ni mogoča!

Vendar pa Signal podpira pošiljanje zvočnih sporočil. Pošiljati jih je mogoče preko omrežja Tor.

V skupinskih pogovorih jih je mogoče uporabiti kot popolnoma anonimnen PTT ("push-to-talk") sistem.

Nekateri razvijajo tudi rešitve, ki omogočajo visoko anonimnost in celo ne potrebujejo centralne infrastrukture. Primeri:

- **Ring** je VoIP odjemalec, ki podpira decentralizirano komunikacijo, anonimne identitete P2P iskanje in P2P povezave.
- **Briar** (še v razvoju) je aplikacija za pošiljanje šifriranih sporočil in izmenjavo preko forumov, uporablja P2P povezovanje, ne potrebuje internetne povezave (!) in ne uporablja oblačnih rešitev.

Zaključek

Šifriranje komunikacij postaja v zadnjih letih čedalje bolj razširjeno.

Uporaba močnega šifriranja je postala enostavna.

Povprečnemu uporabniku je treba biti čedalje manj proaktiven glede varnosti – varnostne posodobitve se nameščajo samodejno, rešitve imajo že vgrajene varnostne mehanizme,....

Podjetja čedalje več pozornosti namenjajo implementaciji varnostnih rešitev, varnostnemu testiranju, itd..

Tudi zakonodaja zahteva implementacijo varnostnih rešitev.

Težave še vedno ostajajo, zlastni na nivoju strojne opreme in strojne programske opreme, a se stanje izboljšuje.

Prisluškovanje postaja čedalje težje in čedalje dražje.

Anonimnost: kako sploh odkriti pravo tarčo???

Vprašanja?

Matej Kovačič
matej.kovacic@ijs.si

https://pravokator.si