Zaupanje prometnim podatkom v telefoniji

Matej Kovačič

Kazensko pravna šola 2012 | Čatež, november 2012

OPOZORILO:

Predstavljeni bodo rezultati več informacijsko-varnostnih raziskav iz področja telefonije, ki smo jih v letu 2012 izvedli varnostni raziskovalci Matej Kovačič, Jaka Hudoklin, Primož Bratanič in Klemen Rupnik.

Rezultati so bili predstavljeni v več člankih na spletnem portalu Slo-Tech.com (in povzeti v različnih slovenskih medijih) ter na nekaj strokovnih konferencah.

Pri izvajanju opisanih postopkov smo spoštovali veljavno zakonodajo, saj smo izvajali analizo izključno lastnih komunikacij in uporabljali lastno opremo..

Namen raziskav je bil opozoriti na varnostne ranljivosti v slovenskih telefonskih omrežjih z željo, da se varnostne ranljivosti odpravijo, posledično pa se poveča stopnja varnosti in zasebnosti uporabnikov mobilne in navadne telefonije.

Z raziskavami pa smo pokazali tudi na pomanjkljivosti pri sistemu hrambe prometnih podatkov (tim. *data retention*).

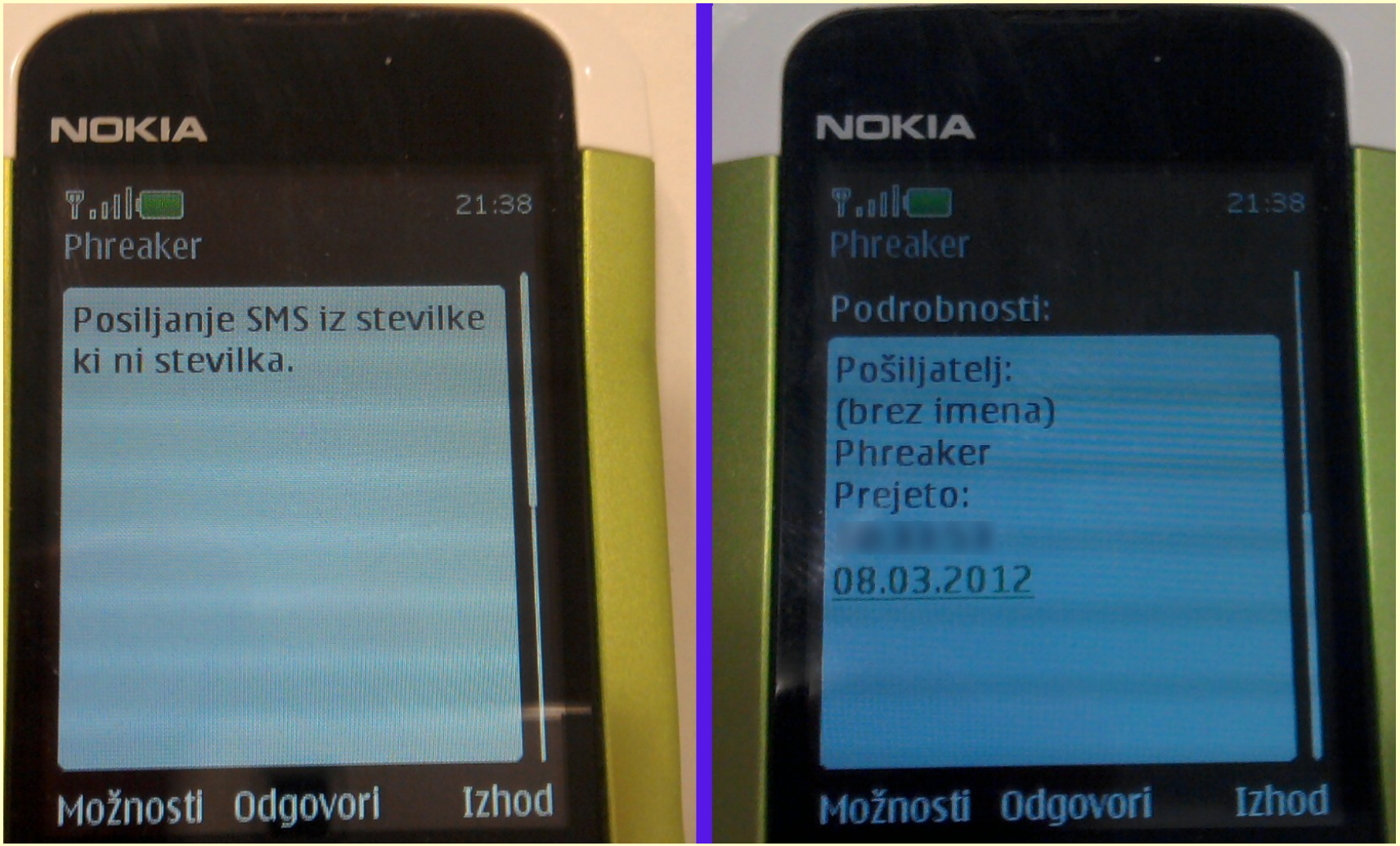
Po našem mnenju se postavlja tudi vprašanje zaupanja prometnim podatkom v kazenskem postopku oziroma se pod vprašaj postavlja njihova dokazna vrednost.

Pošiljanje SMS sporočil s spremenjeno klicno identifikacijo

Pošiljanje SMS sporočil “iz” poljubne številke

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

Pošiljanje SMS sporočil “iz” poljubne številke

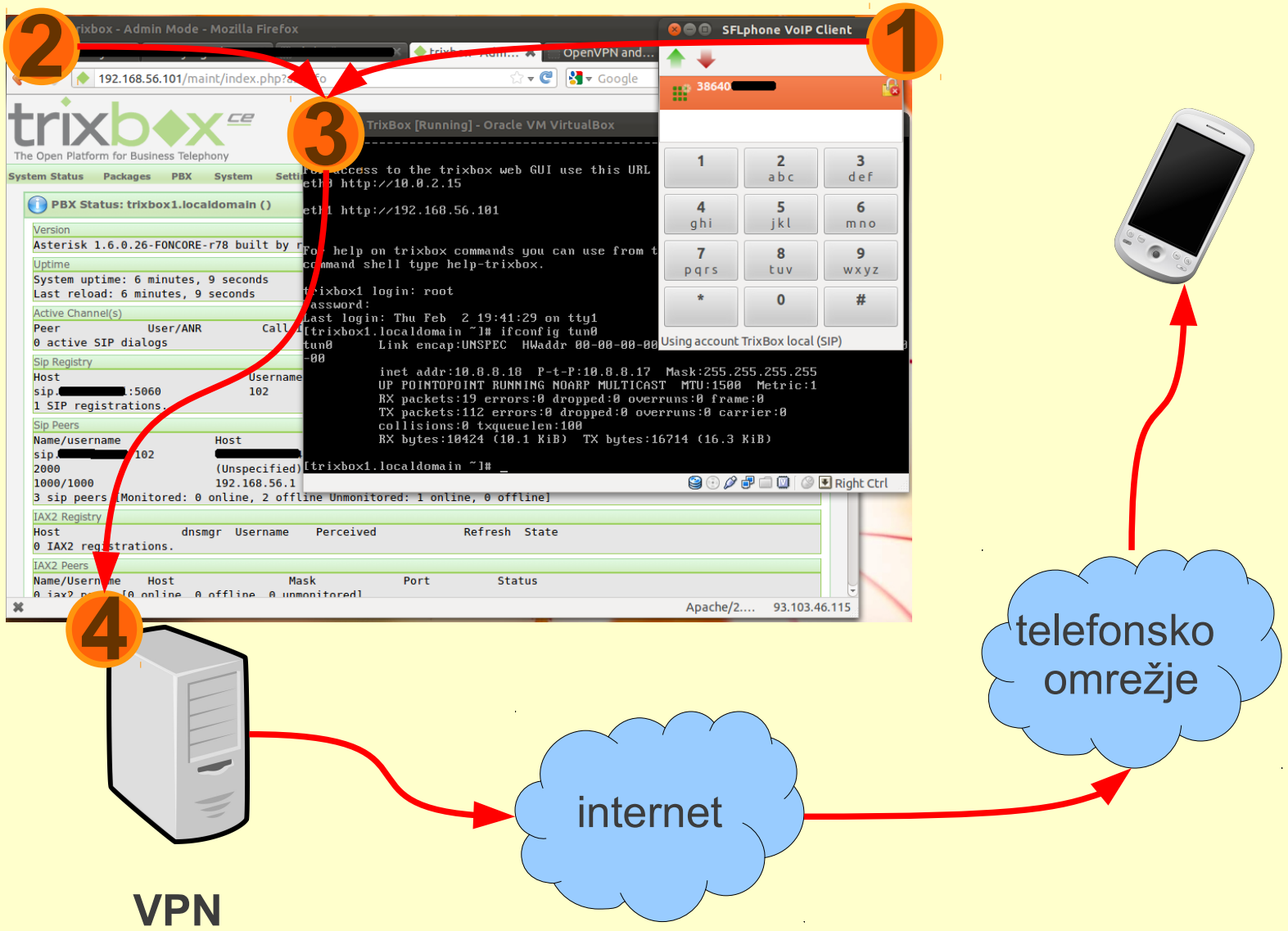


Klicanje s poljubno klicno identifikacijo

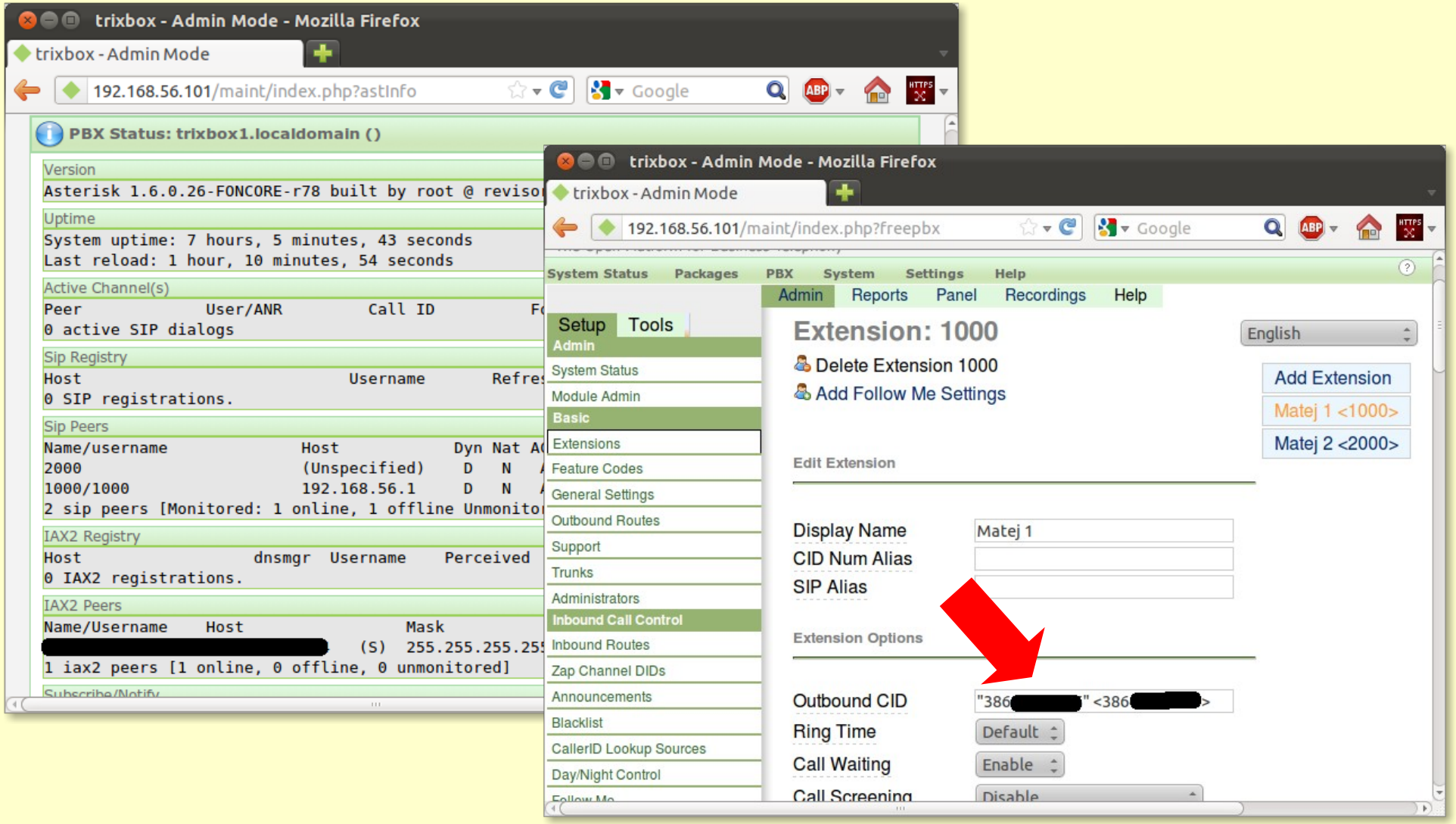
[kljub popravkom nekaterih operaterjev postopek v določenih okoliščinah še vedno deluje]

Klicanje s poljubno klicno identifikacijo

1: vzpostavitev infrastrukture



Klicanje s poljubno klicno identifikacijo
2: pogled v virtualno telefonsko centralo

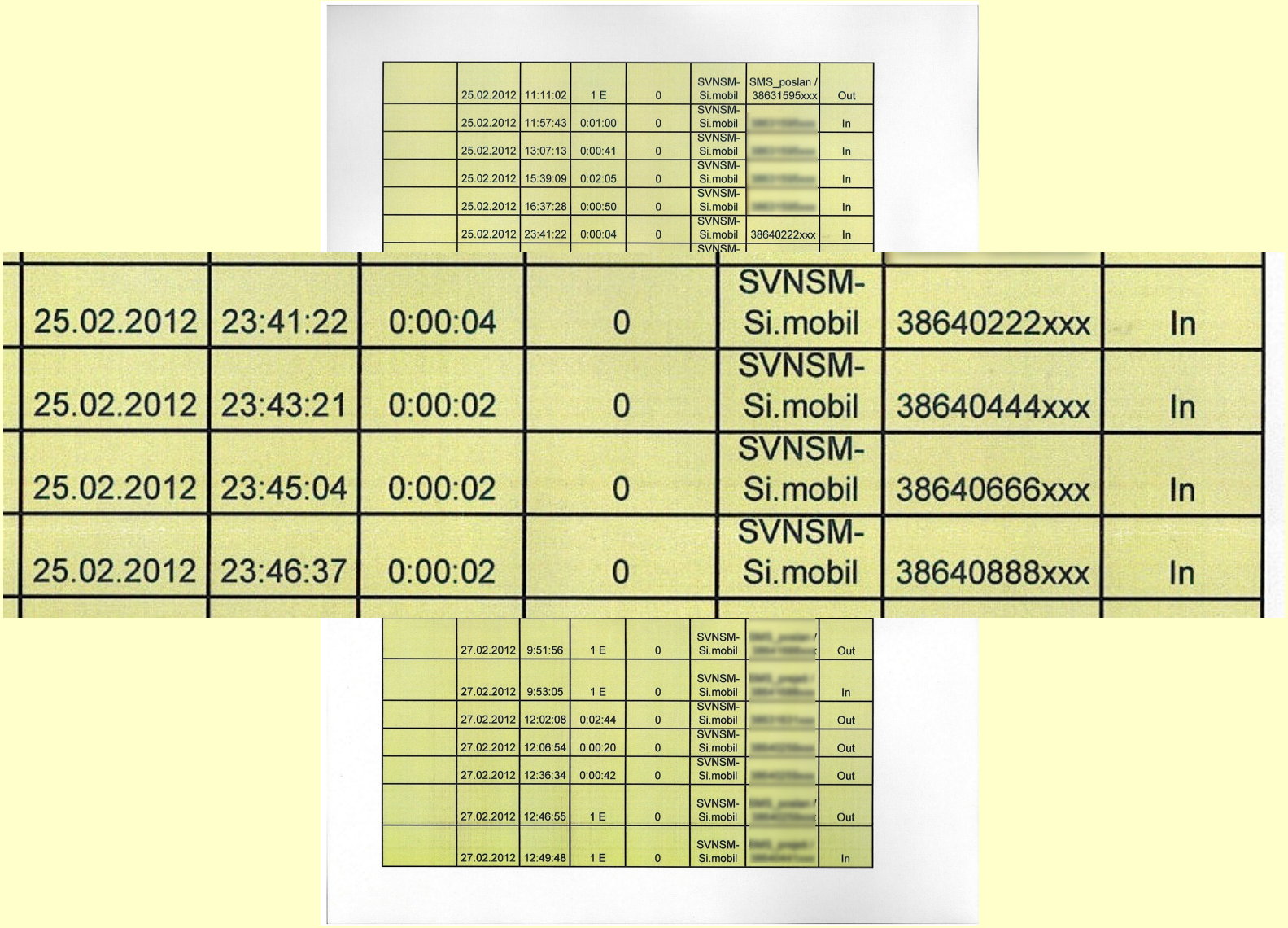


Klicanje s poljubno klicno identifikacijo

3: rezultat na telefonu

Klicanje s poljubno klicno identifikacijo

4: prometni podatki pri operaterju



	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

Varnost slovenskih GSM omrežij

Kaj točno smo naredili?
(in zakaj to ni nezakonito)

- Uporabljali smo atestirano opremo.
- Prestrezali smo **lastne** komunikacije:
  - na “broadcast kanalu” poslušamo (tehnična) sporočila omrežja telefonom. Sporočila pošilja omrežje **vsem** telefonom (tudi tistim, ki še niso povezani v omrežje);
  - našemu telefonu pošiljamo (tiha) SMS sporočila oz. ga kličemo;
  - na “broadcast kanalu” gledamo katera TMSI številka bo dobila SMS sporočilo oz. klic (TMSI lociramo statistično ter s pomočjo SABM (*Set Asynchronous Balance Mode*) sporočila, ki ga lahko zaznamo le v oddaljenosti 2m od telefona);

Kaj točno smo naredili?
(in zakaj to ni nezakonito)

- Prestrezali smo **lastne** komunikacije (*nadaljevanje*):
  - ko identificiramo (naš lasten) TMSI, počakamo na zahtevo za preklop na podatkovni kanal in ko do nje pride, zahtevi sledimo (preklopimo na podatkovni kanal, kjer naš telefon prejme šifrirane podatke – SMS sporočilo);
  - šifrirane podatke (vsebino SMS sporočila) poslane iz našega modema na naš telefon kriptoanaliziramo tako, da dobimo sejni šifrirni ključ Kc. Ta ključ se sicer nahaja v našem mobilnem telefonu (ne na SIM kartici, a izvira iz nje);
  - s pomočjo (našega) Kc (naše) podatke dešifriramo;
  - TMSI in Kc lahko z ustrezno programsko opremo pridobimo tudi iz mobilnega telefona, SIM kartice ne kloniramo, saj vsebuje samo Ki in ne Kc!

Kaj točno smo naredili?
(in zakaj to ni nezakonito)

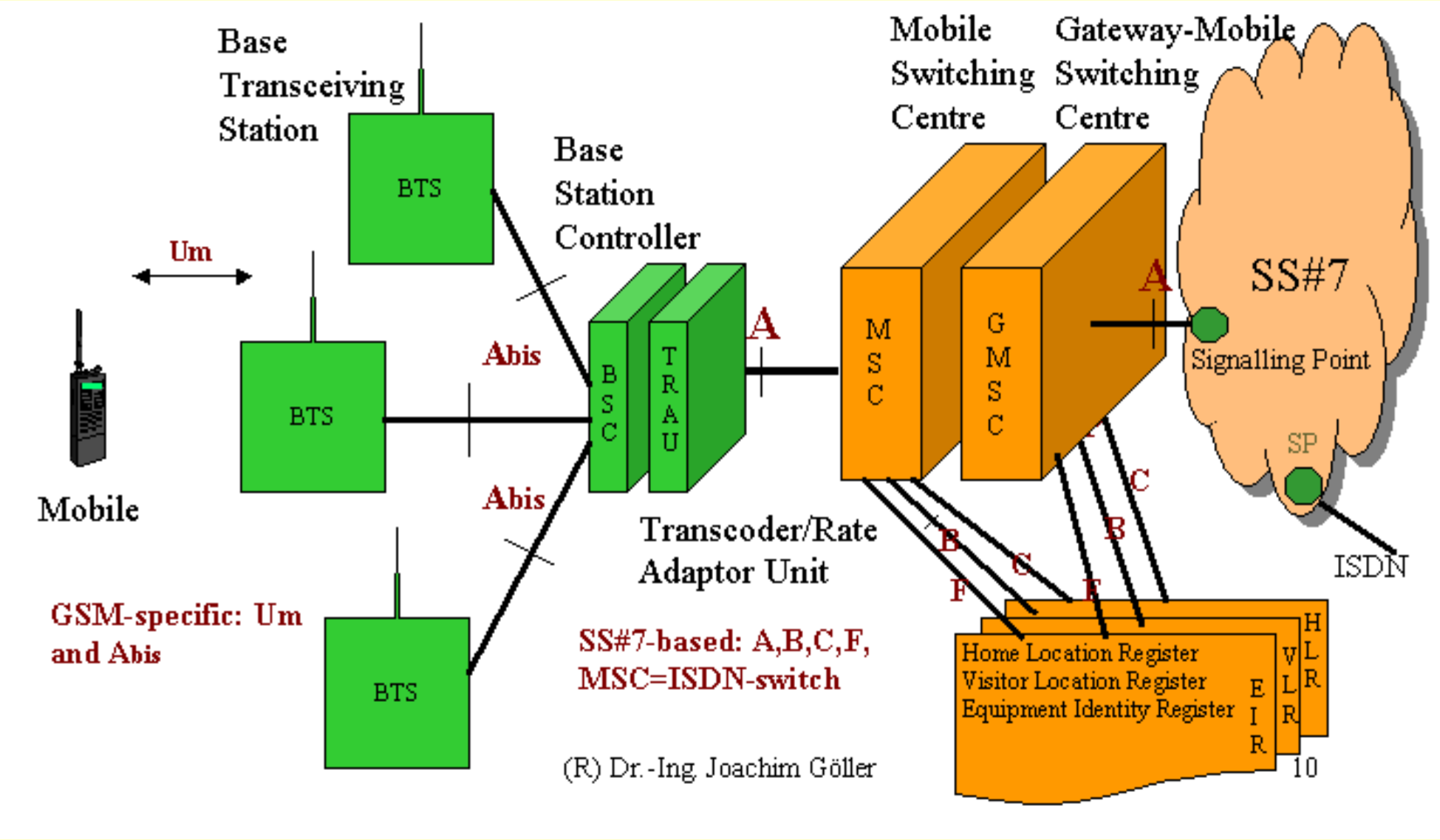
- Impersonacija - ponarejanje (lastne) mobilne identitete:
  - iz omrežja zajamemo naslednje identifikacijske podatke našega telefona: IMSI, TMSI, Kc, sekvenčno številko ključa. Gre za podatke našega lastnega mobilnega telefona.
  - te podatke prepišemo v naš drugi telefon in s tem telefonom opravimo klic v imenu našega prvega telefona.

Predzgodba

John Nevil Maskelyne
(1839 – 1917)

Kiberpipa
(2012)

Nekaj osnov o GSM



SIM kartica in mobilni aparat, IMSI, TMSI, A5/x, "broadcast kanali" in podatkovni kanali...

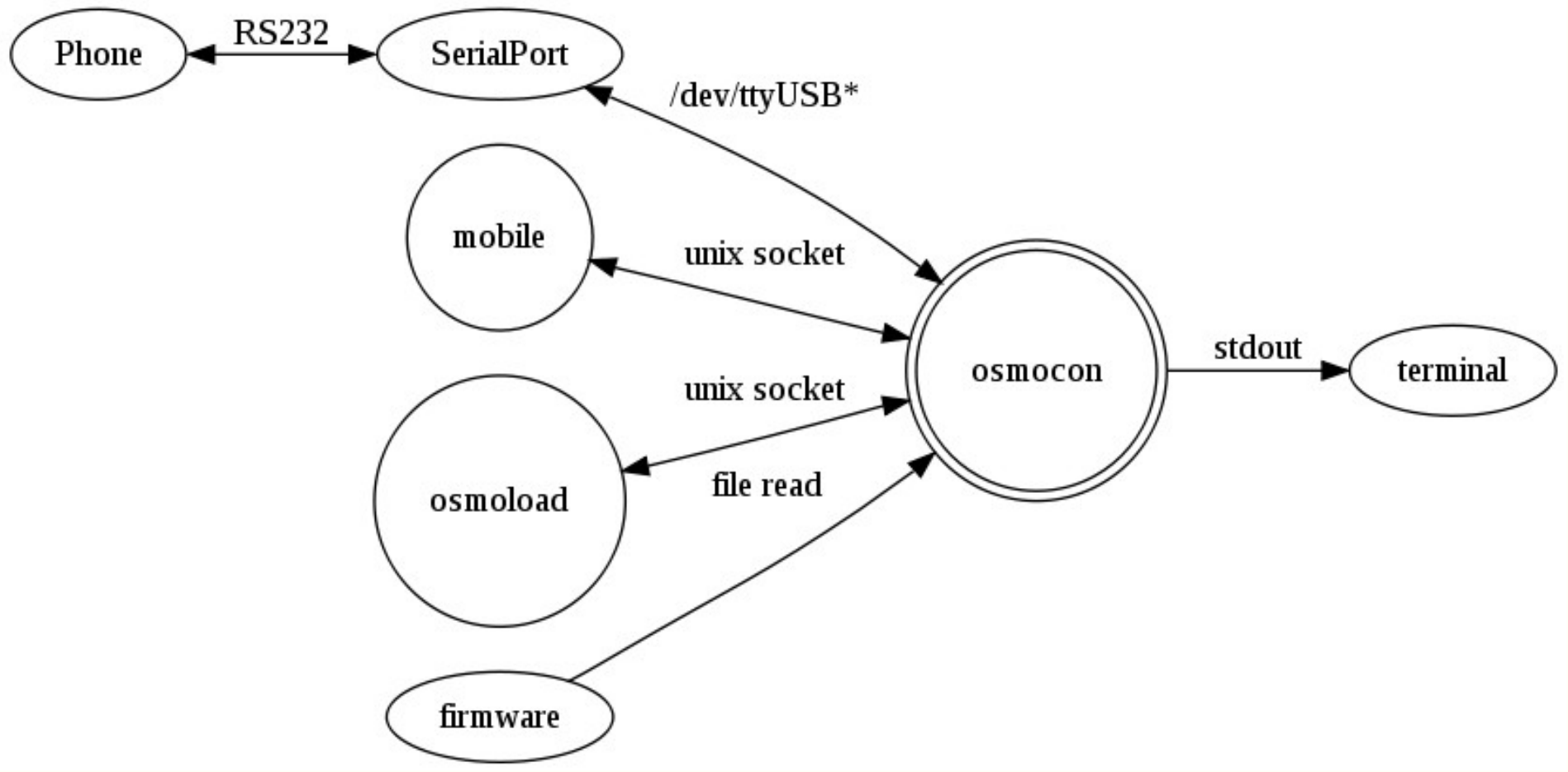
Shema GSM omrežja, vir: *www.gsmfordummies.com*.

OsmocomBB

Mobilni telefon s Calypso čipovjem...

Strojni del opreme lahko zajema tudi druge naprave, npr. RTL-SDR, USRP,...

...in OsmocomBB strojna programska oprema

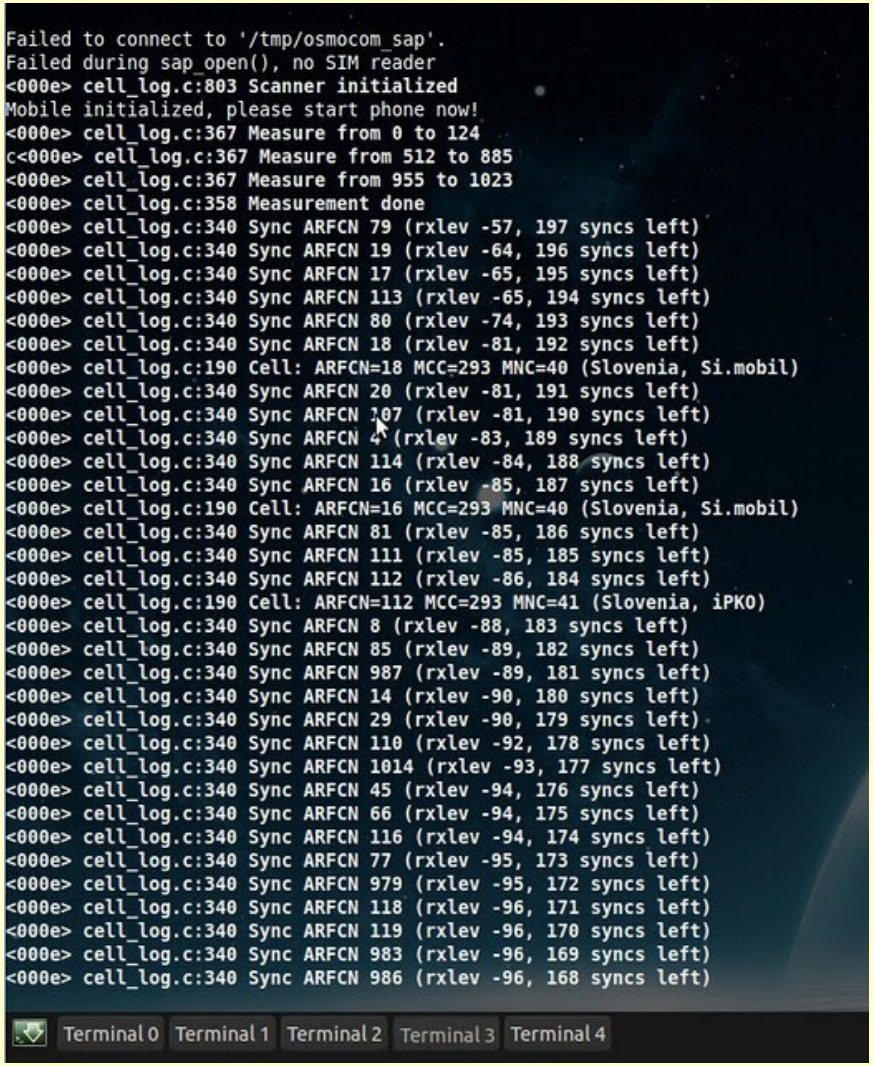


Zagon nalagalnika ROM (ang. *romloader*)

matej@cryptopia: ~/osmocom/osmocom-bb-raw/src/host/osmocon

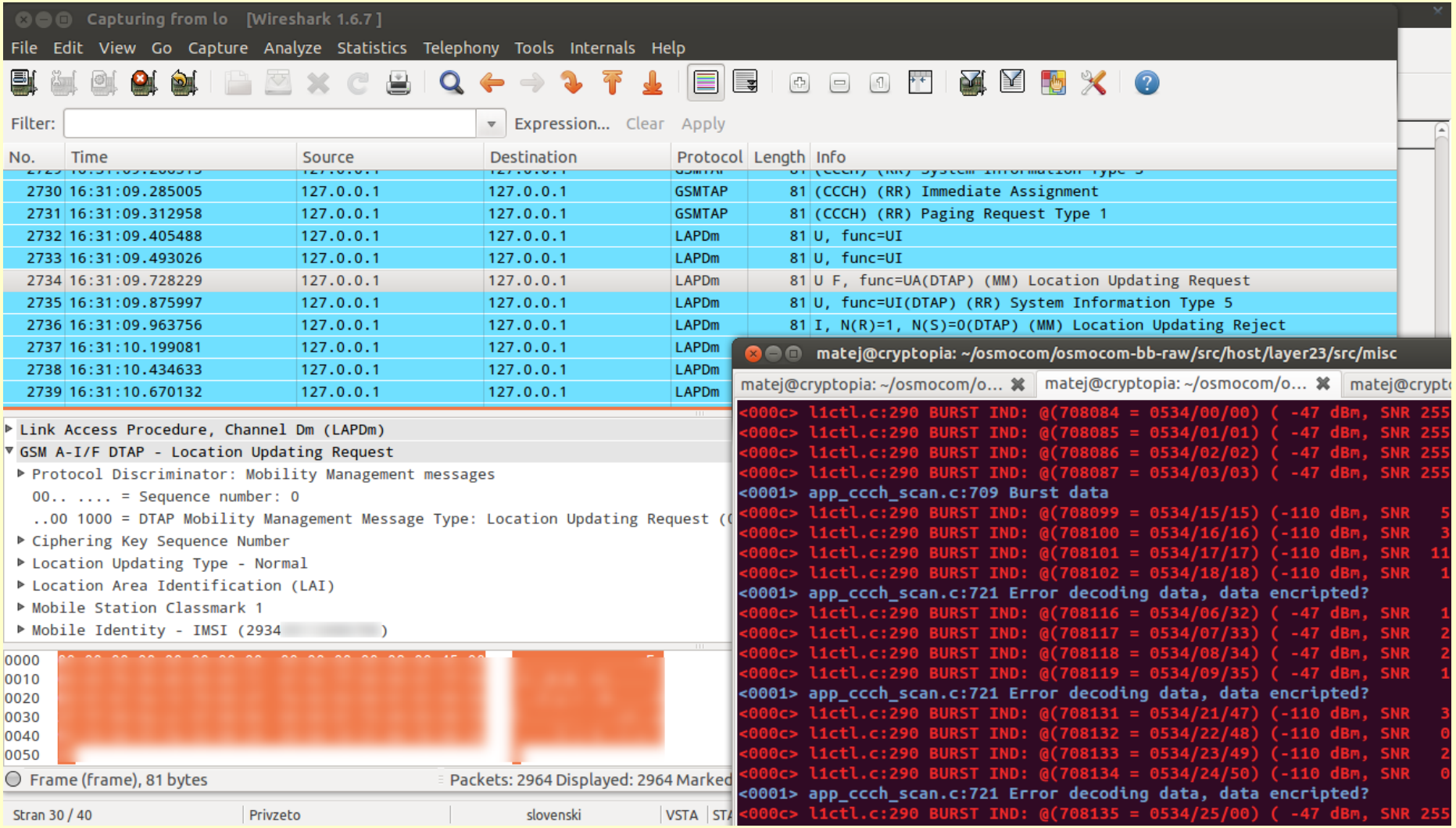
```
Die ID code: 7e540b2fc90393bb
======================================================================
REG_DPLL=0x2413
CNTL_ARM_CLK=0xf0a1
CNTL_CLK=0xff91
CNTL_RST=0xfff3
CNTL_ARM_DIV=0xfff9
======================================================================
Power up simcard:


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!
```

Pregled baznih postaj...



Pregled ARFCN-jev s programom *cell_log*.

Analiza GSM prometa...

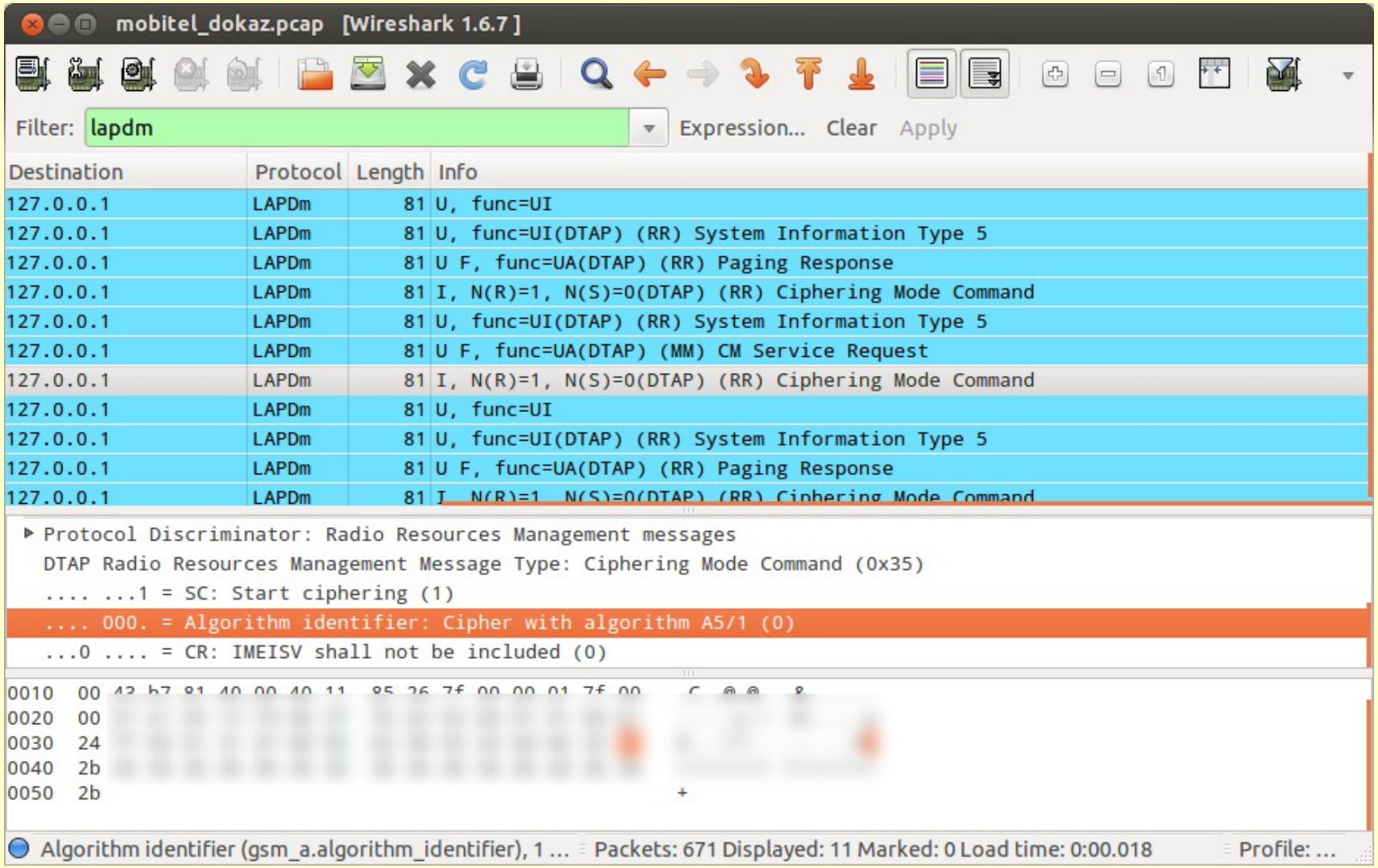


Analiza GSM prometa. Promet zajamemo s programom *ccch_scan* in ga prikažemo v aplikaciji Wireshark.

Varnostni pregled slovenskih GSM omrežij

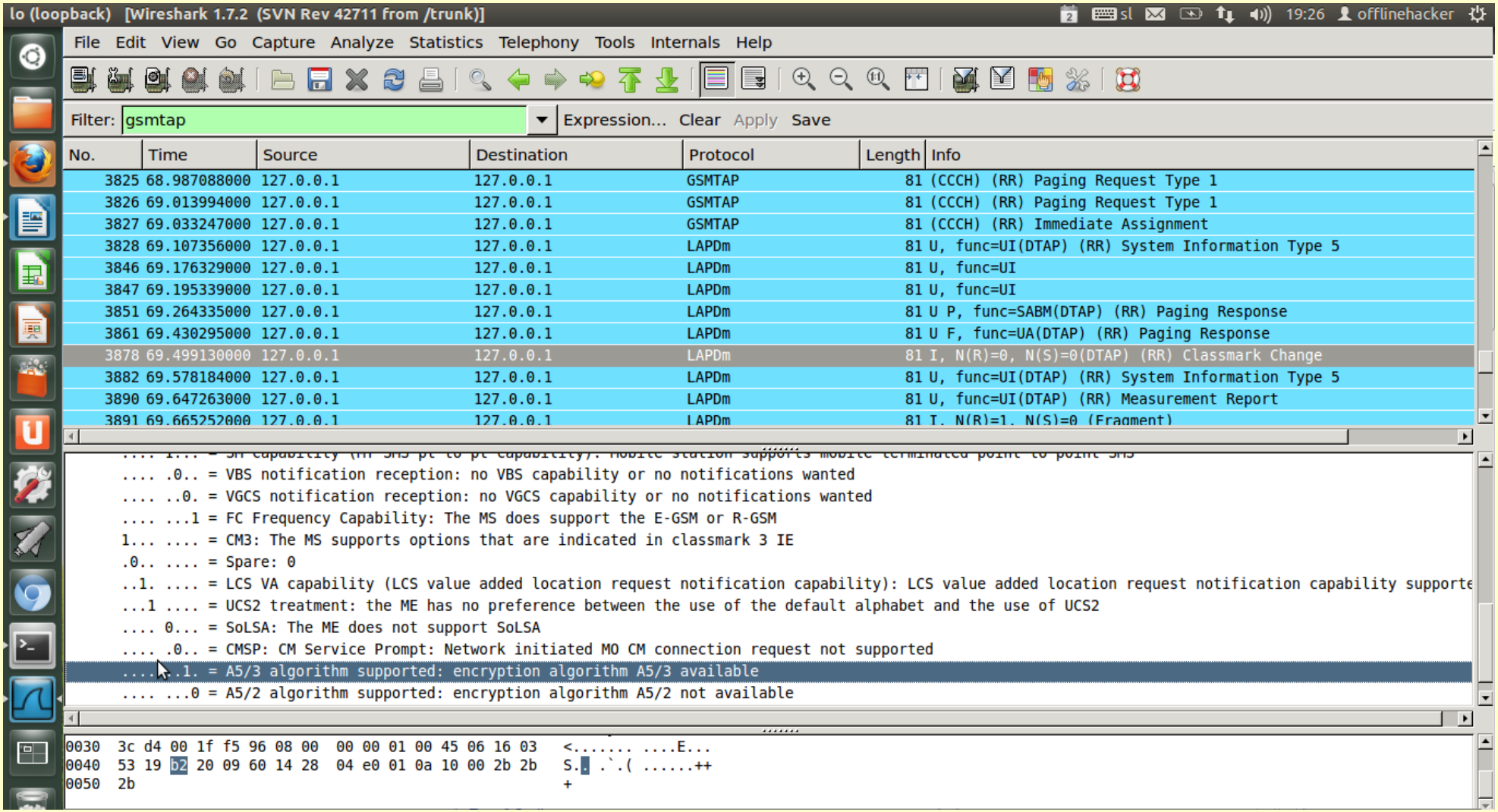
[nekatere opisane ranljivosti so bile po objavi člankov že odpravljene]

Uporaba šifriranja - Mobitel



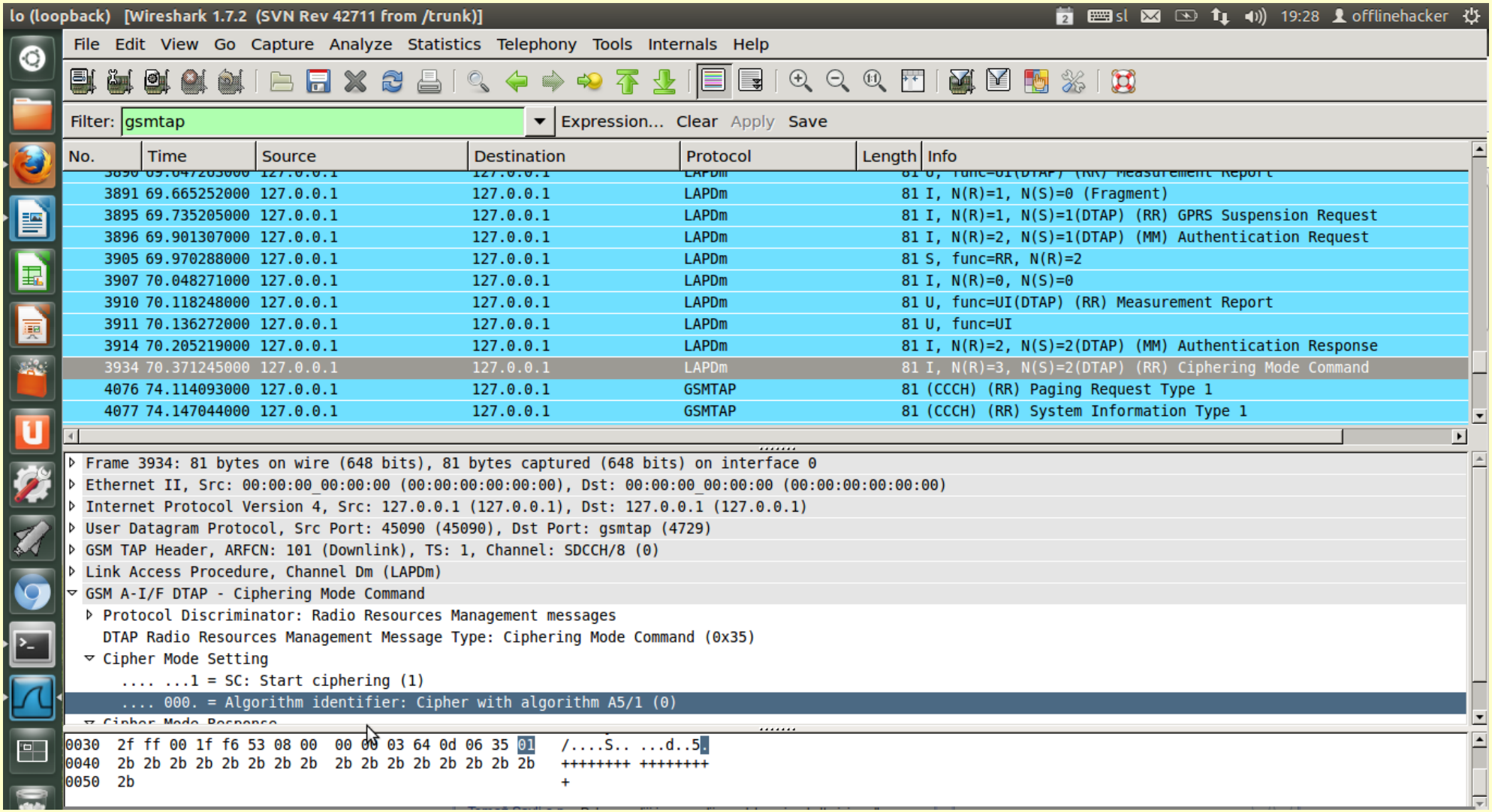
Mobitel je v času pregleda uporabljal šifriranje A5/1

Uporaba šifriranja - Mobitel



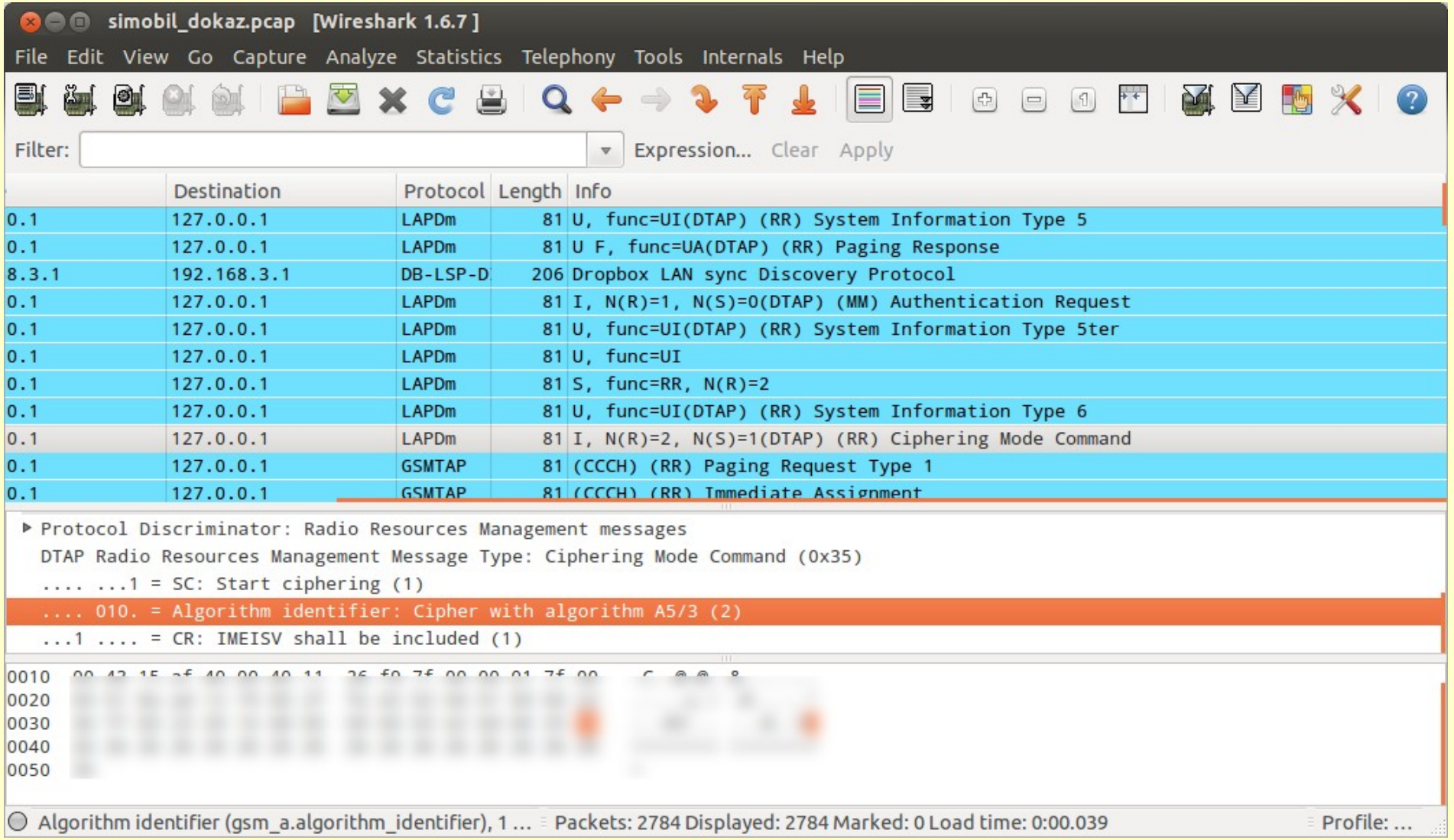
Če je mobilni telefon sporočil, da podpira A5/3...

Uporaba šifriranja - Mobitel



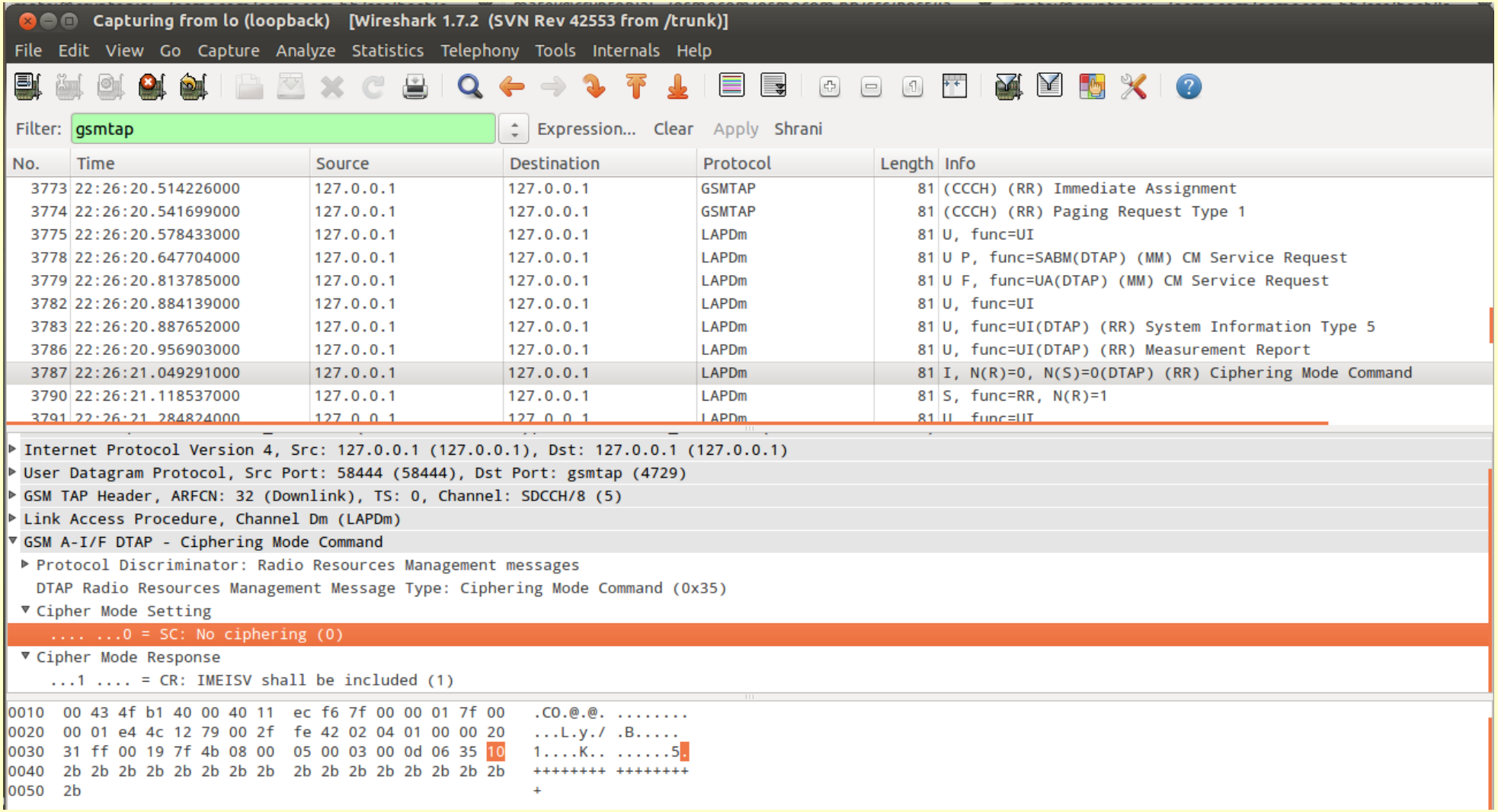
...je omrežje odgovorilo,da je na voljo samo A5/1.

Uporaba šifriranja - Simobil



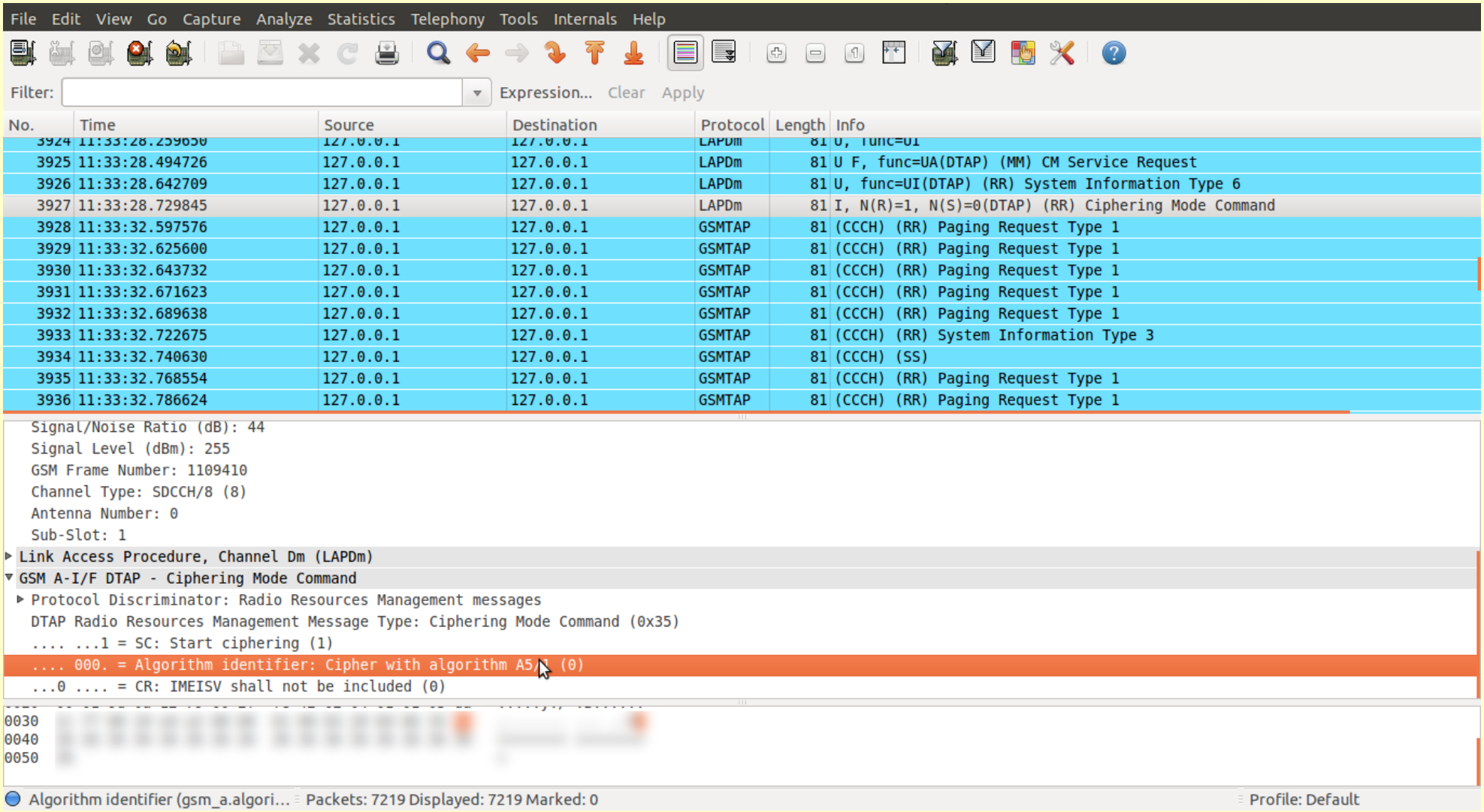
Simobil je v času pregleda uporabljal tudi A5/3...

Uporaba šifriranja - Simobil



...vendar pa je v času pregleda omogočal tudi uporabo A5/0.

Uporaba šifriranja - Tušmobil



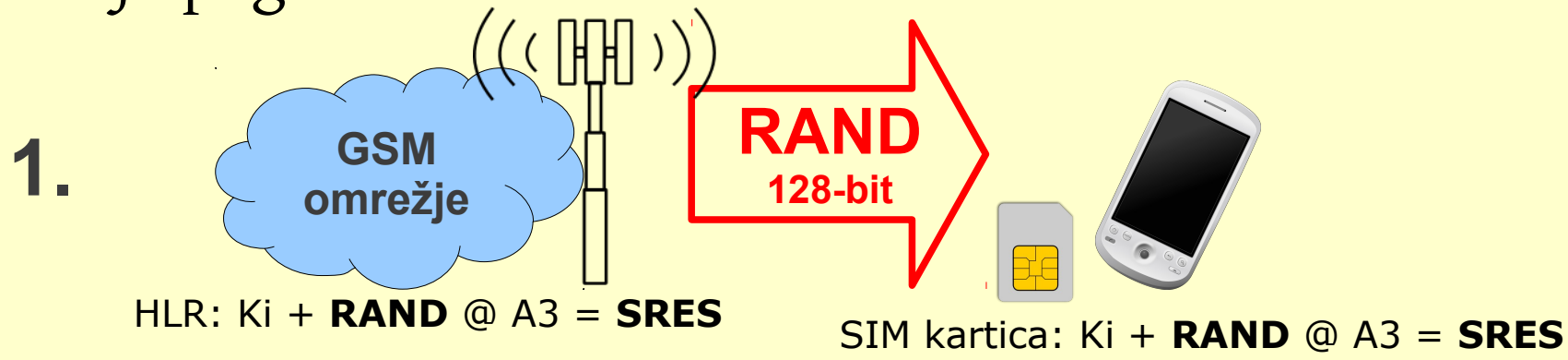
Tušmobil je v času pregleda uporabljal A5/1.

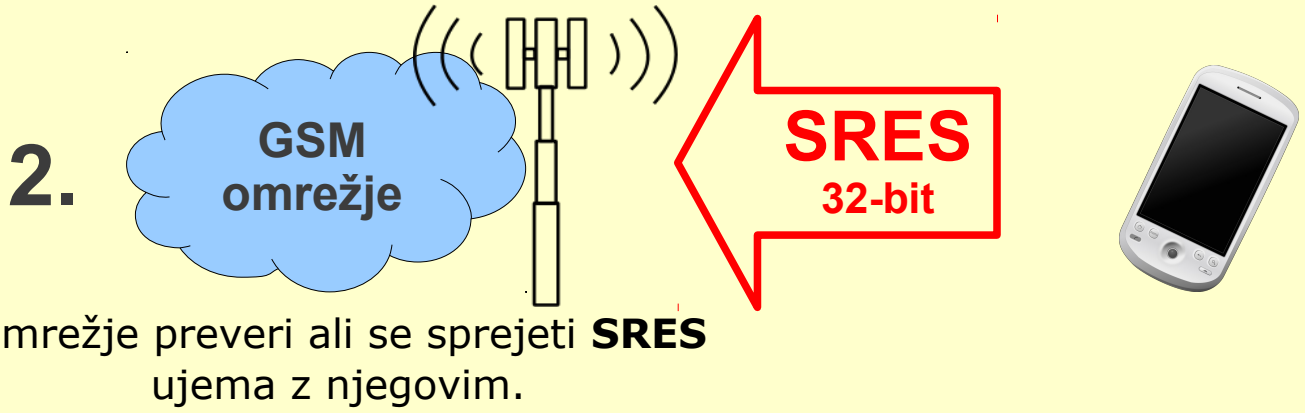
Kriptoanaliza sejnega šifrirnega ključa Kc
(brez posedovanja mobilnega telefona in/ali SIM kartice tarče)

[ranljivost je delovala v primeru A5/1 šifriranja brez naključnega zapolnjevanja]

Ustvarjanje sejnega ključa Kc

Šifrirni ključ **Ki** je shranjen v SIM kartici **in** HLR registru.
Na podlagi **Ki** se ustvari začasni, sejni ključ **Kc** s katerim se šifrirajo pogovori.





Ustvarjanje sejnega ključa Kc

3. Na vsaki strani se s pomočjo A8 ustvari sejni ključ Kc:

Ki + RAND @ A8 = **Kc**

4.

Če se SRES ujema, imata tako omrežje, kot telefon isti Kc. Ključ je s tem "izmenjan", čeprav se ne prenese preko omrežja. Šifriranje pogovorov poteka s Kc + A5/x. Po "zraku" se prenašajo samo šifrirani podatki.

Kriptoanaliza A5/1

teorija

VSEBINA PODATKOVEGA IZBRUHA V GSM

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

f(Kc)

"ENKRATNI" KLJUČ ZA ŠIFRIRANJE TOKA PODATKOV

D1	E8	02	BF	B7	A0	86	BB	37	E3	E3	E8	02

Kraken

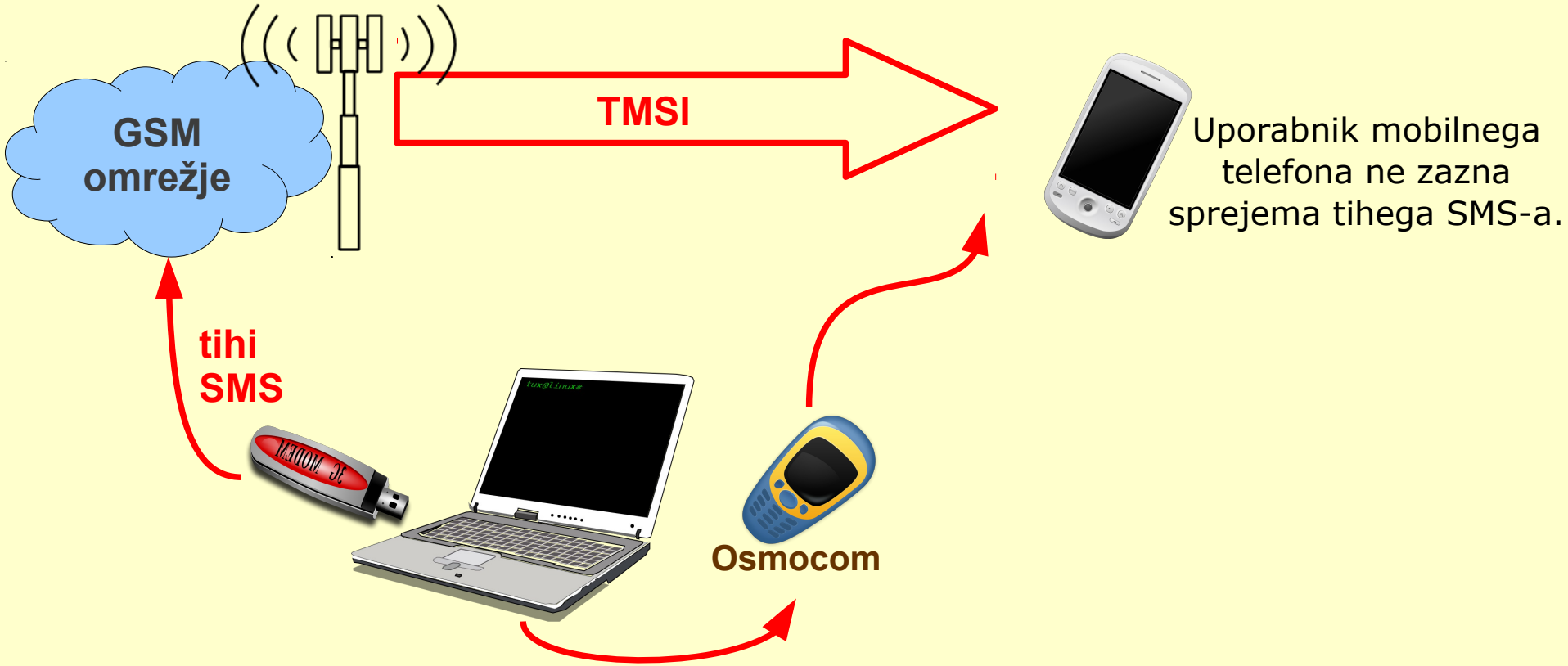
ŠIFRIRANO SPOROČILO (XOR)

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

Kc

Lociranje uporabnika v mobilnem omrežju

Na mobilno številko pričnemo pošiljati tihe SMS-e, hkrati na omrežju gledamo katera TMSI številka prejema šifrirane podatke.



Zajem in kriptoanaliza A5/1

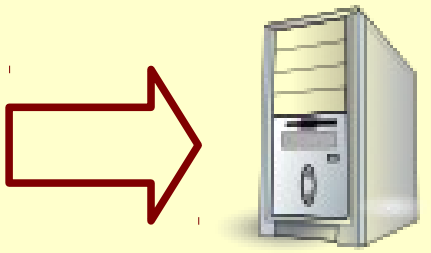
praksa

5.

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

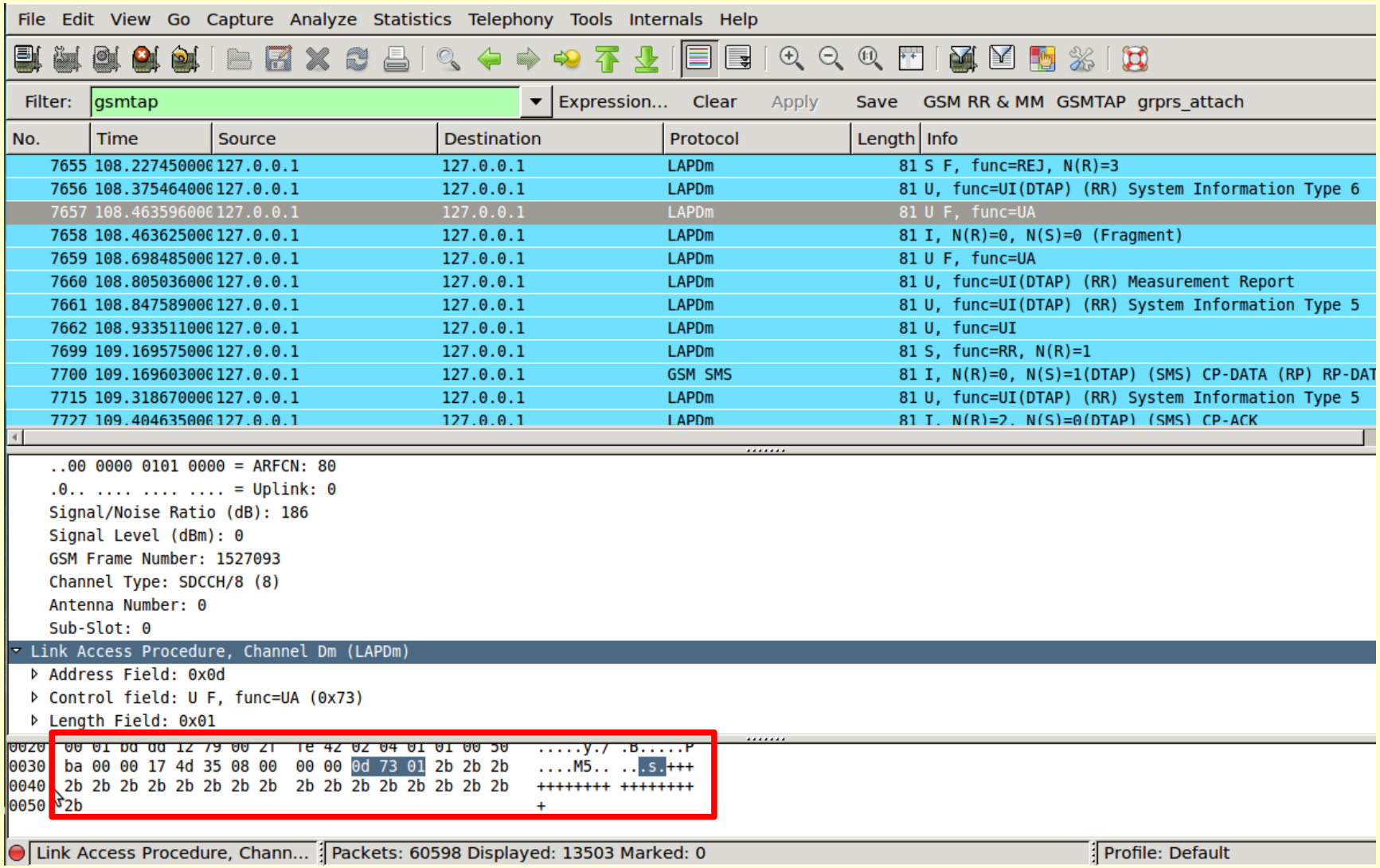
VSEBINA PODATKOVEGA IZBRUHA V GSM

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

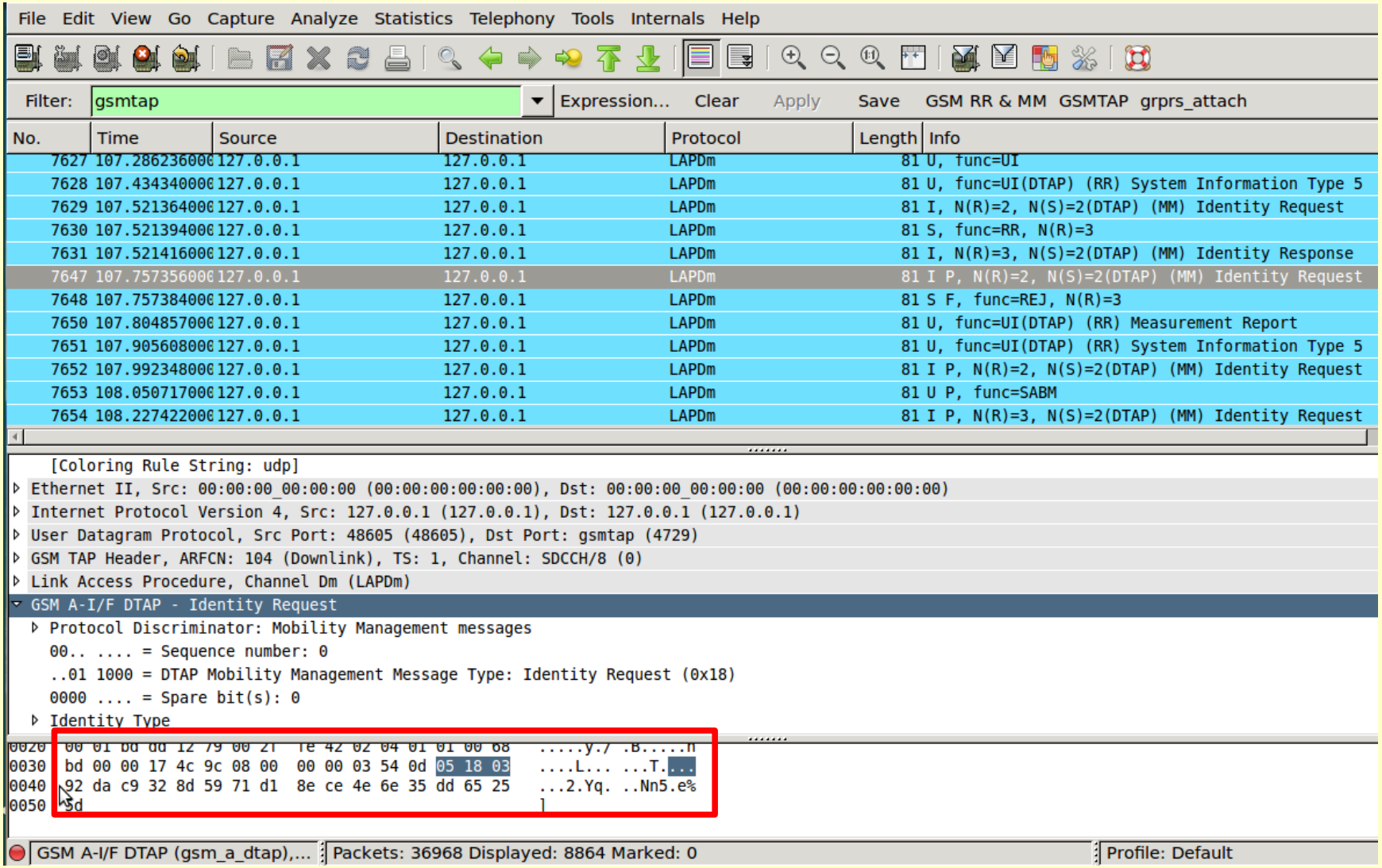


- Iz “zraka” pasivno zajamemo šifrirane podatkovne pakete.
- S pomočjo ugibanja vsebine podatkovnega izbruha (uganemo vsebino tim. polnila - ang. *padding bits*) izračunamo “enkratni” ključ za šifriranje toka podatkov.
- Sejni šifrirni ključ Kc nato rekonstruiramo s pomočjo kriptoanalize.
- V postopku ni potrebe po dostopu do SIM kartice, telefona ali omrežja.

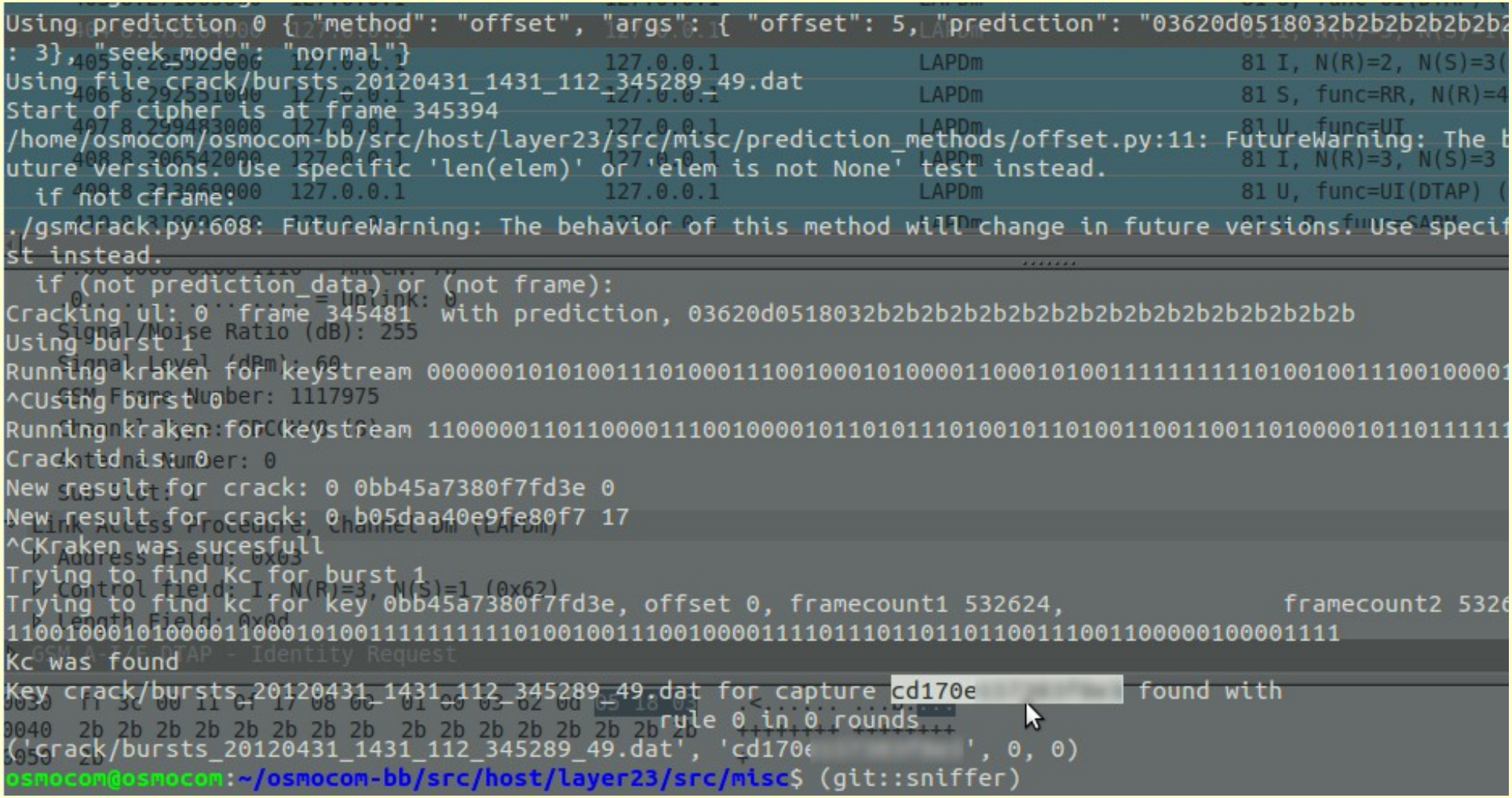
Navadno zapolnjevanje
(*non-random padding*)



Naključno zapolnjevanje
(*random padding*)

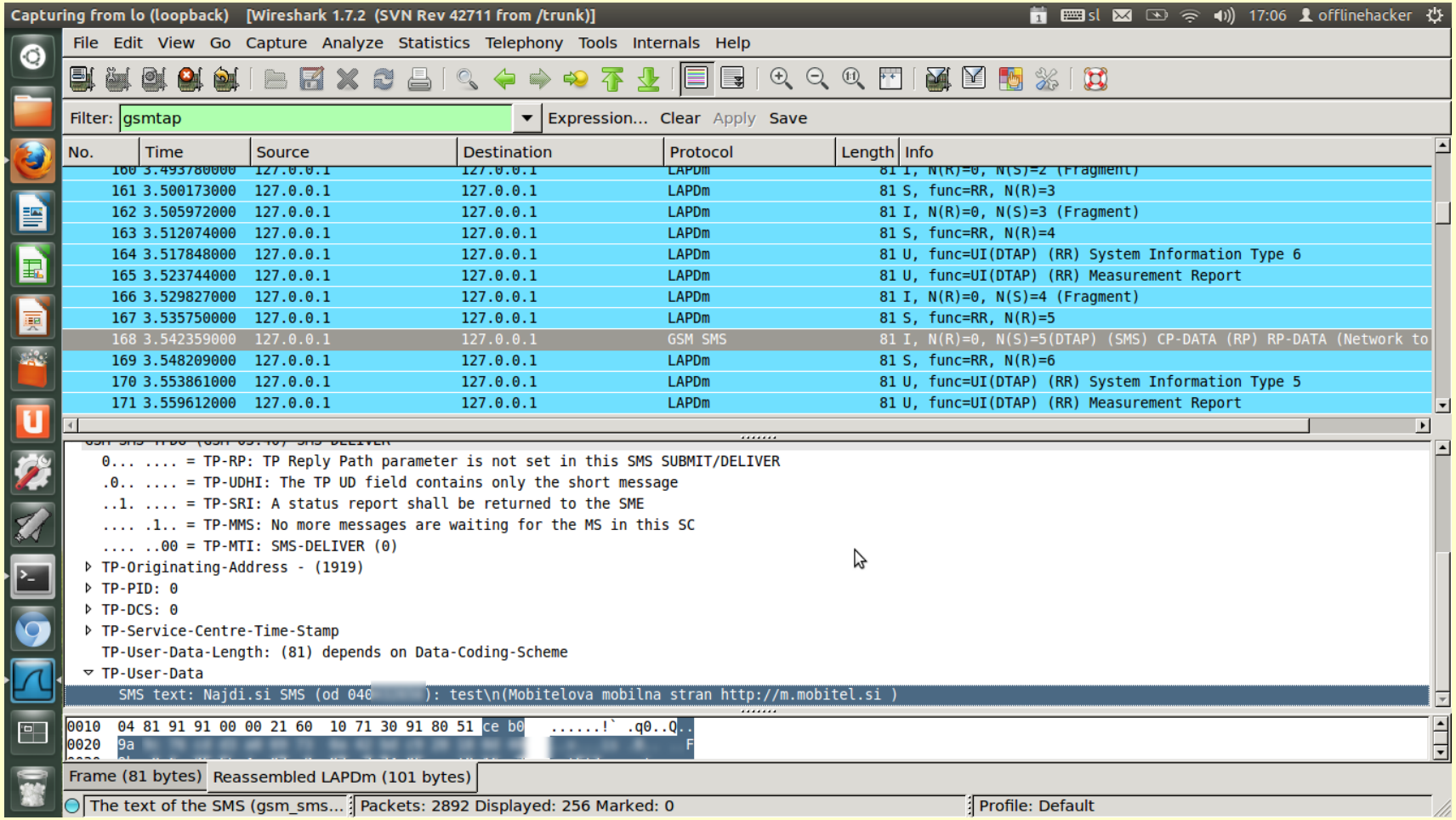


Razbijanje A5/1 sejnega šifrirnega ključa Kc v praksi



Razbijanje s pomočjo programa Kraken in predikcij, ki jih uporablja naš *gsmcrack.py*...

Razbijanje A5/1 sejnega šifrirnega ključa Kc v praksi



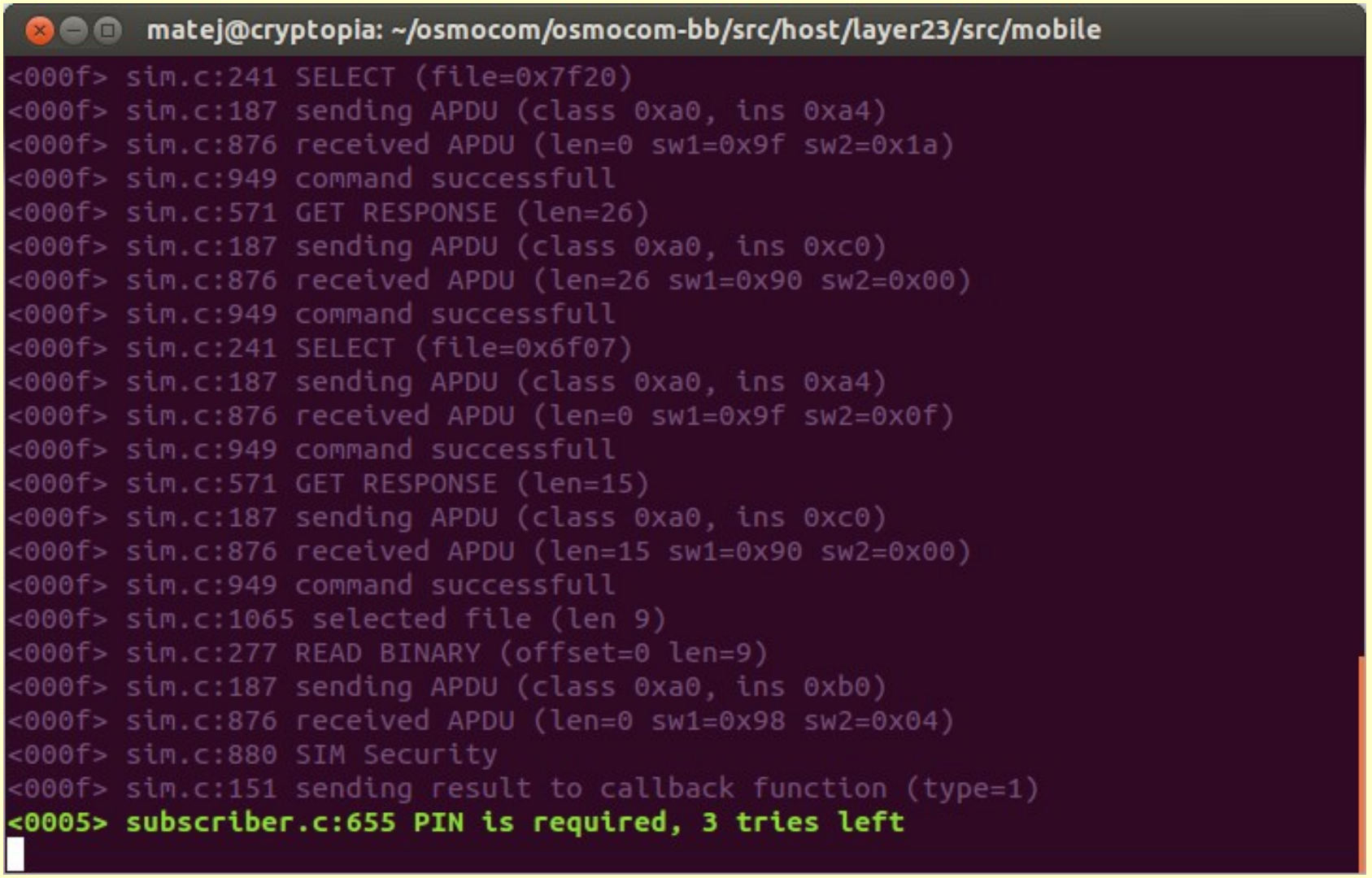
… in dešifrirano SMS sporočilo (prejeto preko 2G).
Program *gsmcrack.py* samodejno identificira TMSI številko na podlagi klicne številke (s pomočjo pošiljanja tihih SMS sporočil), ko imamo TMSI tarče pa aplikacija zna samodejno slediti telefonu na s strani bazne postaje dodeljeni kanal in posneti šifrirano sporočilo.

Ponarejanje mobilne identitete v GSM omrežju

(brez posedovanja mobilnega telefona in/ali SIM kartice tarče)

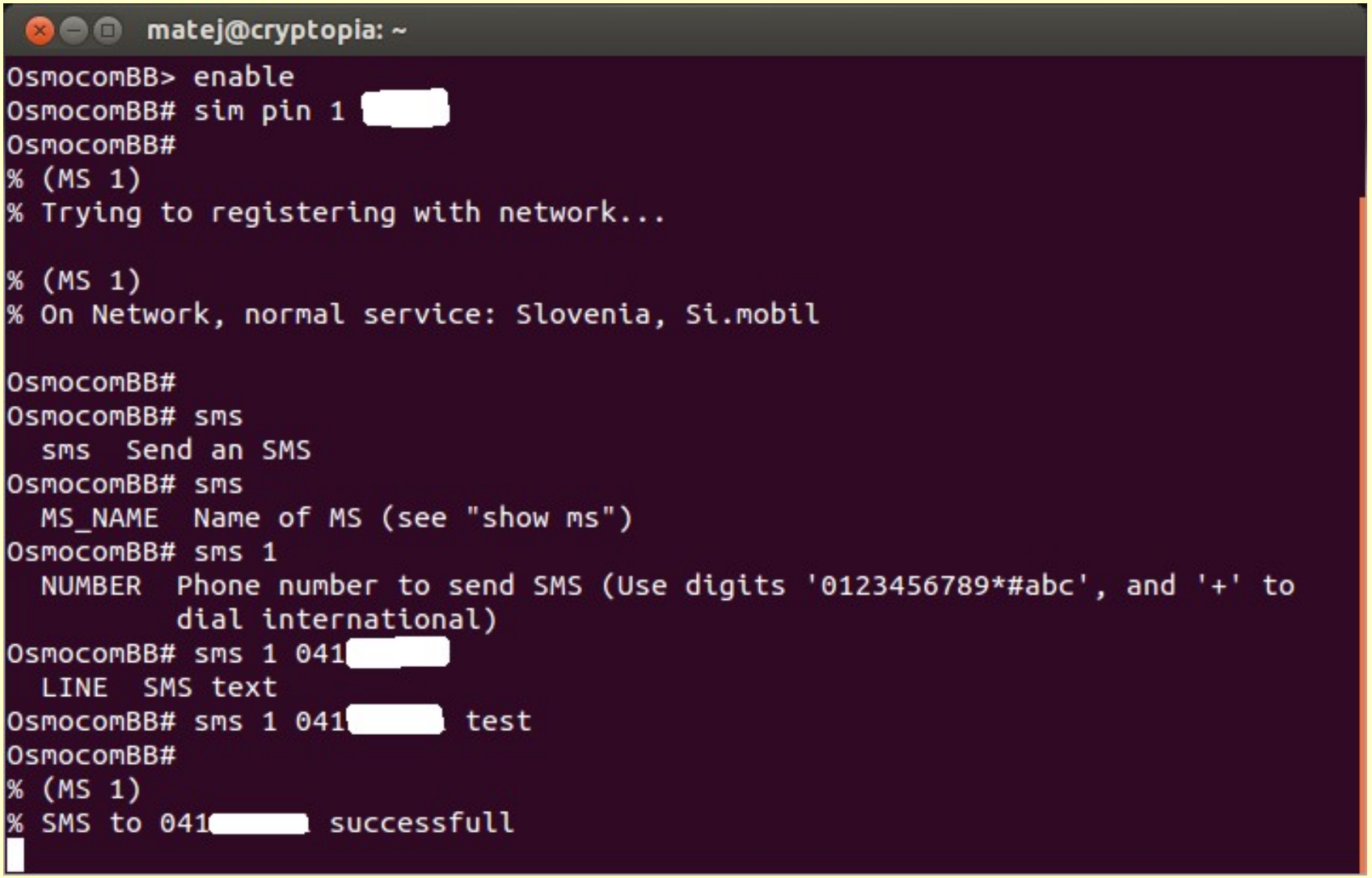
[ranljivosti so bile v večini slovenskih GSM omrežij odpravljene in postopek ne deluje več]

Aplikacija *mobile*



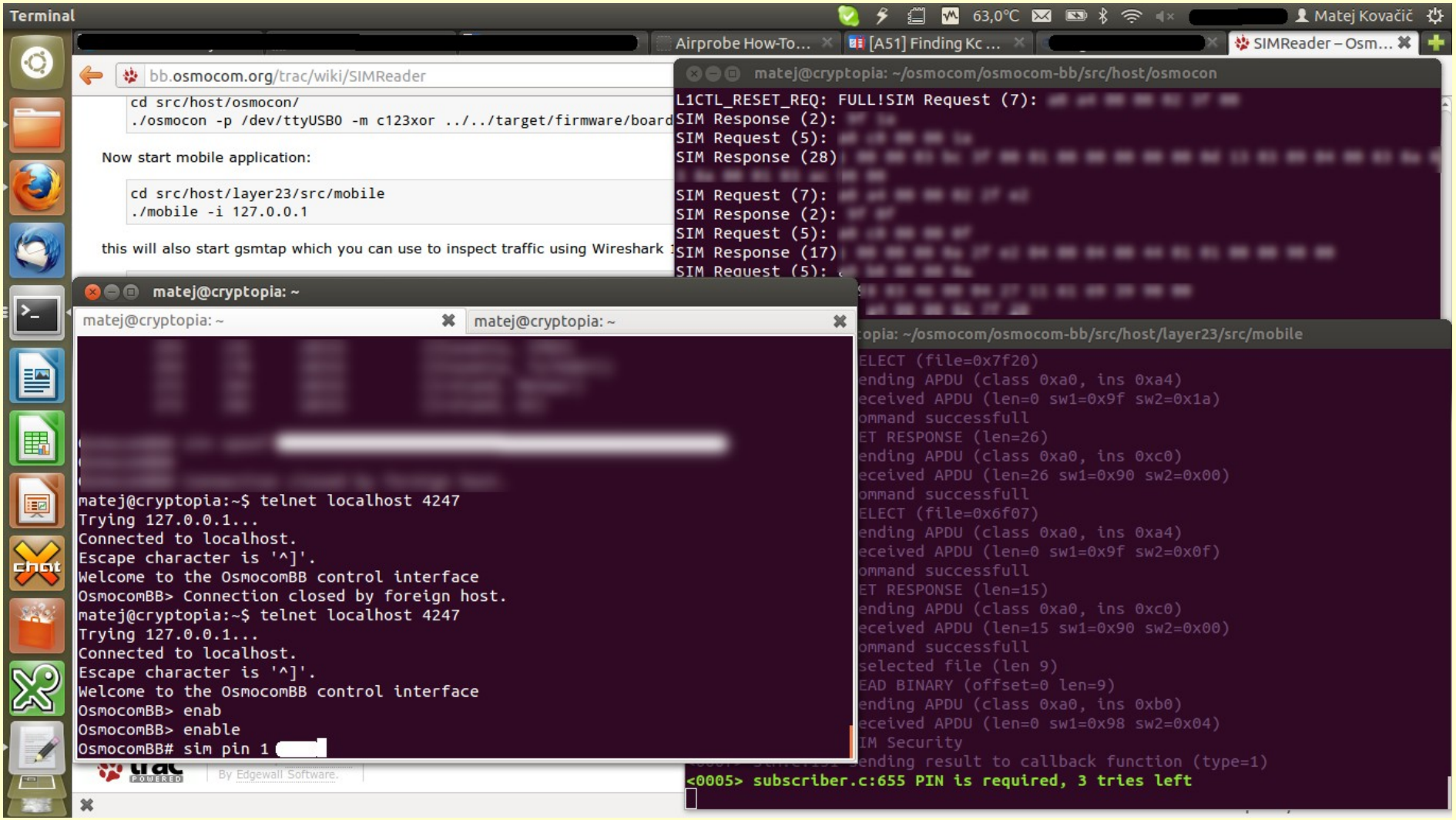
Aplikacija *mobile* omogoča klicanje ter pošiljanje in sprejemanje SMS sporočil na OsmocomBB mobilnih telefonih.

Aplikacija *mobile*



Pošiljanje SMS sporočila iz aplikacije *mobile*.

Aplikacija *mobile*



Uporaba aplikacije *mobile*. V ozadju Osmocom ROM nalagalnik, aplikacija *mobile* in (v ospredju) konzola aplikacije *mobile*.

Mobilna identiteta v mobilnem omrežju

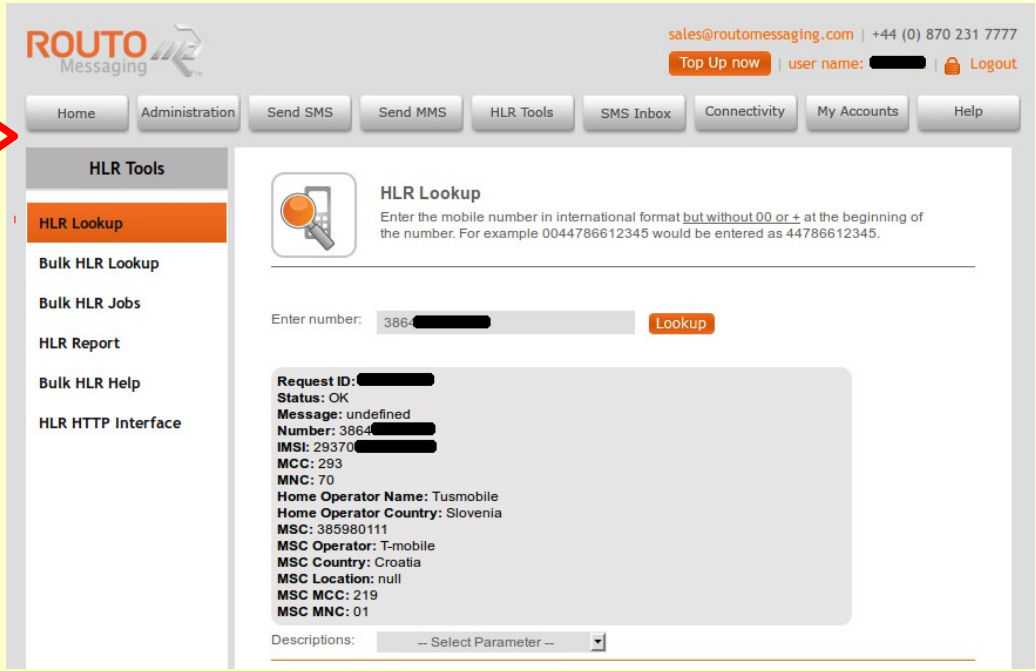
Uporabniki se v mobilnem omrežju ne identificirajo s telefonsko številko, pač pa z IMSI oziroma TMSI številko. Pomembna parametra sta tudi sejni šifrirni ključ Kc in sekvenčna številka ključa (*Key sequence number*).

Ponarejanje mobilne identitete

Če se Kc ne spreminja ob vsaki transakciji, je mogoče mobilno identiteto ponarediti. Najprej **identificiramo IMSI številko tarče...**

1.

HLR vpogled

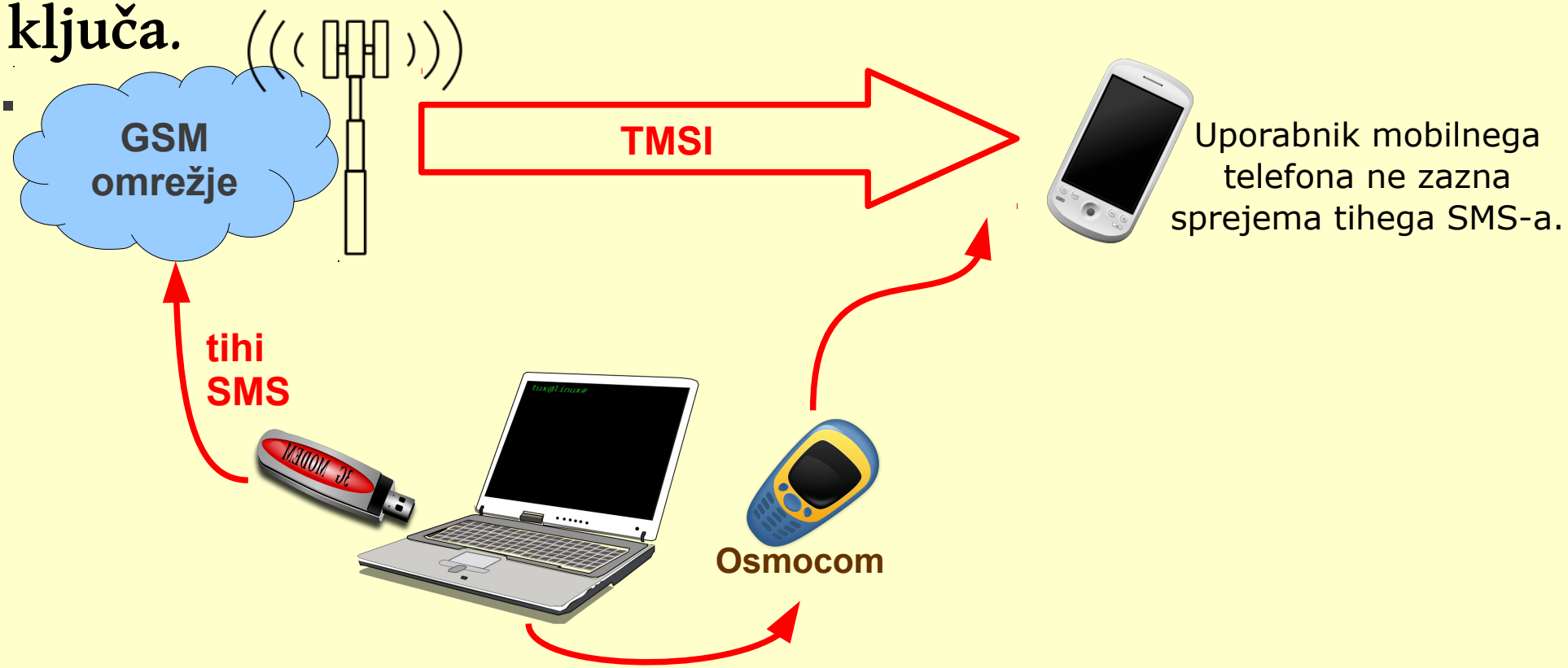


Preko spletne storitve za telefonsko številko izvedemo HLR vpogled in pridobimo IMSI številko.

Razkritje TMSI številke

S pošiljanjem tihih SMS sporočil na telefonsko številko tarče lociramo še njeno **TMSI številko**. Hkrati prestrežemo podatkovni paketek in **sekvenčno številko ključa**.

2.



Pridobitev Kc

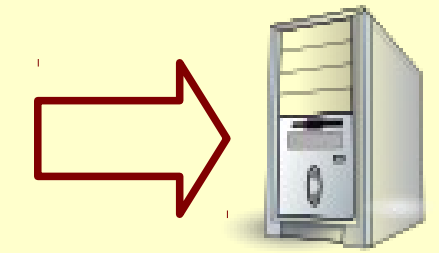
S pomočjo kriptoanalize **rekonstruiramo sejni šifrirni ključ Kc.** Sedaj imamo vse potrebne podatke...

3.

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

VSEBINA PODATKOVEGA IZBRUHA V GSM

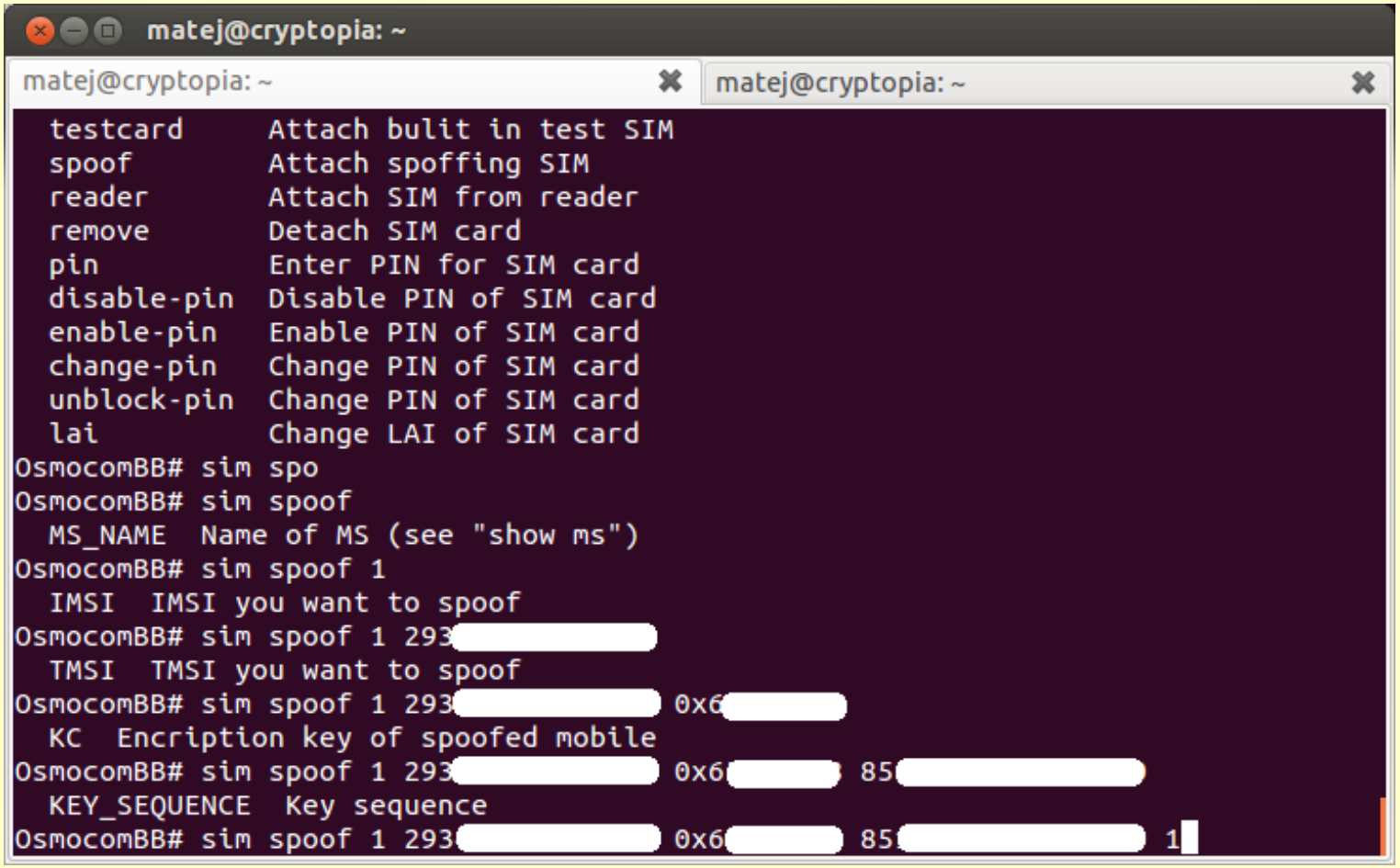
72	FE	BC	10	74	70	C4	2B	2B	2B	2B	2B	2B



Kraken

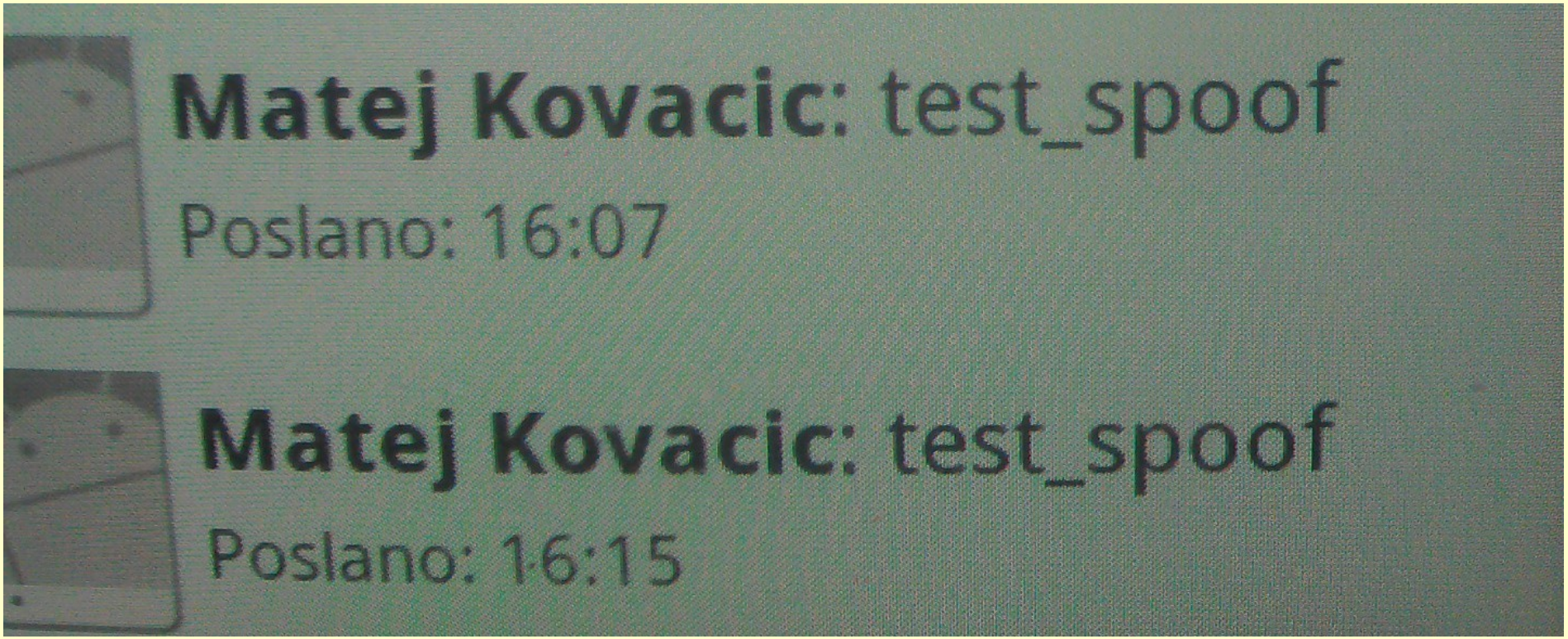
Kc

“SIM spoof”



Ponarejanje mobilne identitete z ukazom “sim spoof”. Za ponarejanje potrebujemo IMSI številko (SS7 vpogled), TMSI številko (zajem iz omrežja), šifrirni ključ (ga razbijemo) ter sekvenčno številko ključa (ang. *key sequence number* - zajem iz omrežja).
V omrežjih, ki uporabljajo A5/0 potrebujemo le TMSI in sekvenčno številko ključa.

Ponarejanje mobilne identitete



Dve SMS sporočili poslani s pomočjo ponarejene mobilne identitete.
Na podoben način je bilo mogoče ponarejati tudi glasovne klice.
[video]

Kaj to pomeni za obvezno hrambo prometnih podatkov?

Sodišča digitalne dokaze, zlasti računalniško generirane digitalne dokaze praviloma dojemajo kot zaupanja vredne same po sebi (*inherently trustworthy evidence*).

To ima posledice tudi na sam sodni postopek. Na (kazenskem) sodišču ima obramba pravico so soočenja s tožniki in navzkrižnega zaslišanja prič.

A kaj storiti, če je »priča« računalnik oz. programska oprema?

Sergey Bratus, Ashlyn Lembree in Anna Shubina. 2010.

Software on the Witness Stand: What Should It Take for Us to Trust It?

“Tudi Miran Kimovec z Mobitela, ki je naslednji stopil na prostor za pričanje, ni znal pojasniti, kako bi lahko nastali posnetki pogovora, ne da bi bil Reichov mobilni telefon prijavljen pri enem od slovenskih operaterjev. »Teoretično bi bilo možno, da je avstrijski državljan v Kranju ujel signal avstrijskega operaterja, praktično pa je skorajda nemogoče,« je povedal. Sojenje se bo še nadaljevalo.”

Gorenjski glas, 2. marec 2007,
<http://www.gorenjskiglas.si/novice/kronika/index.php?action=clanek&id=4329>

Ilustracija: (CC) SulphurSpoon @ DeviantArt

Vprašanja?