Varnost mobilne telefonije in zanesljivost prometnih podatkov

ter posledice tehnološkega razvoja za kazensko pravo

Matej Kovačič, Jaka Hudoklin, Primož Bratanič

Fakulteta za logistiko | Celje, december 2013

Varnost skozi transparentnost

- **Kerchoffsov zakon** pravi, da je dober šifrirni sistem varen, tudi če je o njem znano vse, razen šifrirnega ključa.
  - Zavrača načelo, da je mogoče varnost zagotoviti s skrivanjem (t. i. '*security through obscurity*').
  - Ne zahteva, da je šifrirni sistem javen, temveč le opozarja na to, da skrivnost ne zagotavlja varnosti, marveč jo v resnici lahko celo ogroža.
- Claude Shannon je postavil tim. Shannonovo maksimo, ki pravi, da sovražnik pozna šifrirni sistem.
- Eric S. Raymond pravi: "*Vsaka varnostna programska oprema, ki ne predpostavlja, da sovražnik poseduje izvorno kodo, je nevredna zaupanja; zatorej: nikoli ne zaupaj zaprti kodi.*".

Varnost skozi transparentnost

- Korist od javne objave šifrirnih algoritmov je predvsem v tem, da lahko drugi kriptologi algoritem ali zamisel ocenijo in kritično ovrednotijo.
- To pripomore k izboljšavi kakovosti in k hitrejšemu razvoju.
- Pri zaprtih sistemih je veliko večja verjetnost, da je v njih kakšna napaka, ki bi jo javni pregled verjetno odkril, avtorji pa bi s tem dobili možnost, da jo odpravijo.

Varnost skozi transparentnost

- *Ne spominjam se nobenega kriptografskega sistema, razvitega na skrivaj, v katerem ne bi, potem ko je bil razkrit javnosti, kriptografska skupnost našla napake.*
  --Bruce Schneier

- *But there's an old saying inside the NSA: "Attacks always get better; they never get worse."*
  --Bruce Schneier

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

Pri izvajanju opisanih postopkov smo uporabili atestirano opremo oz. izvajali analizo lastnih komunikacij, prav tako v slovenskih GSM omrežjih nismo povzročali kakršnihkoli motenj.

Pri izvajanju varnostnega pregleda nismo klonirali SIM kartice niti pridobili ali rekonstruirali Ki ključa.

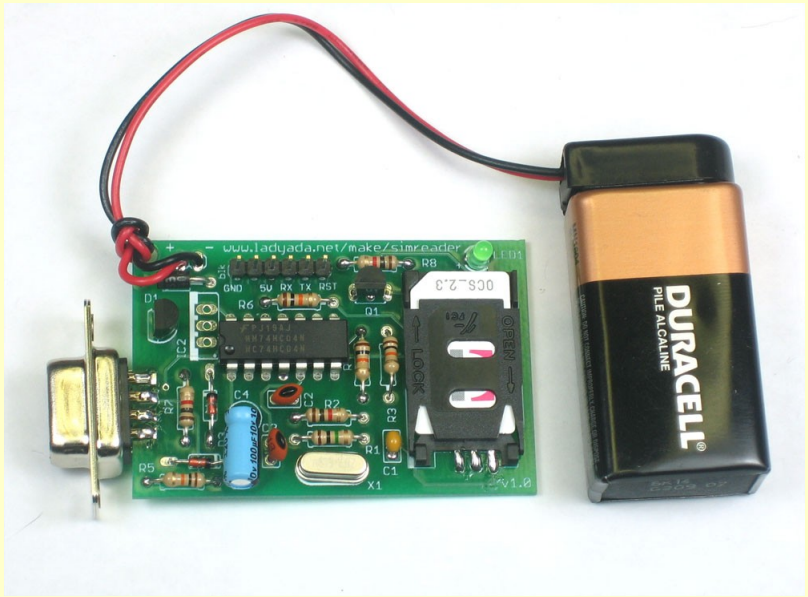
Namen raziskave je bil opozoriti na varnostne ranljivosti v slovenskih GSM omrežjih z željo, da se varnostne ranljivosti odpravijo, posledično pa se poveča stopnja varnosti in zasebnosti uporabnikov mobilne telefonije, ter z željo, da slovenski operaterji mobilne telefonije začnejo več vlagati v varnost omrežij in zaščito svojih uporabnikov.

Prav tako smo z raziskavo pokazali na pomanjkljivosti pri sistemu hrambe prometnih podatkov (tim. data retention) oziroma dokazno vrednost prometnih podatkov v kazenskem postopku postavili pod vprašaj.

Verodostojnost digitalnih podatkov na SIM kartici

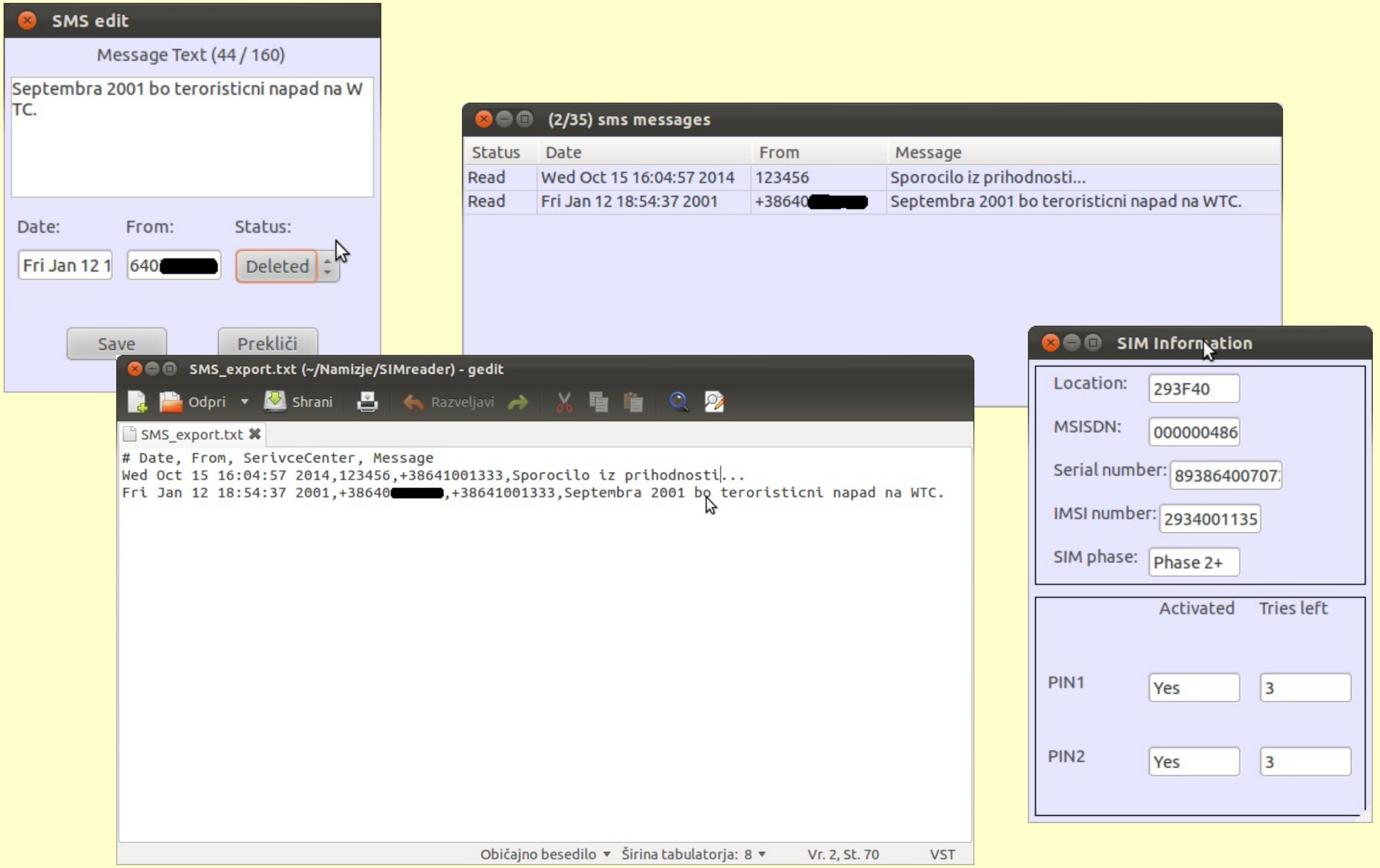
Podatki iz SIM kartice

1: čitalec SIM kartic



Podatki iz SIM kartice

2: spreminjanje vsebine in metapodatkov SMS sporočil na SIM kartici



Podatki iz SIM kartice

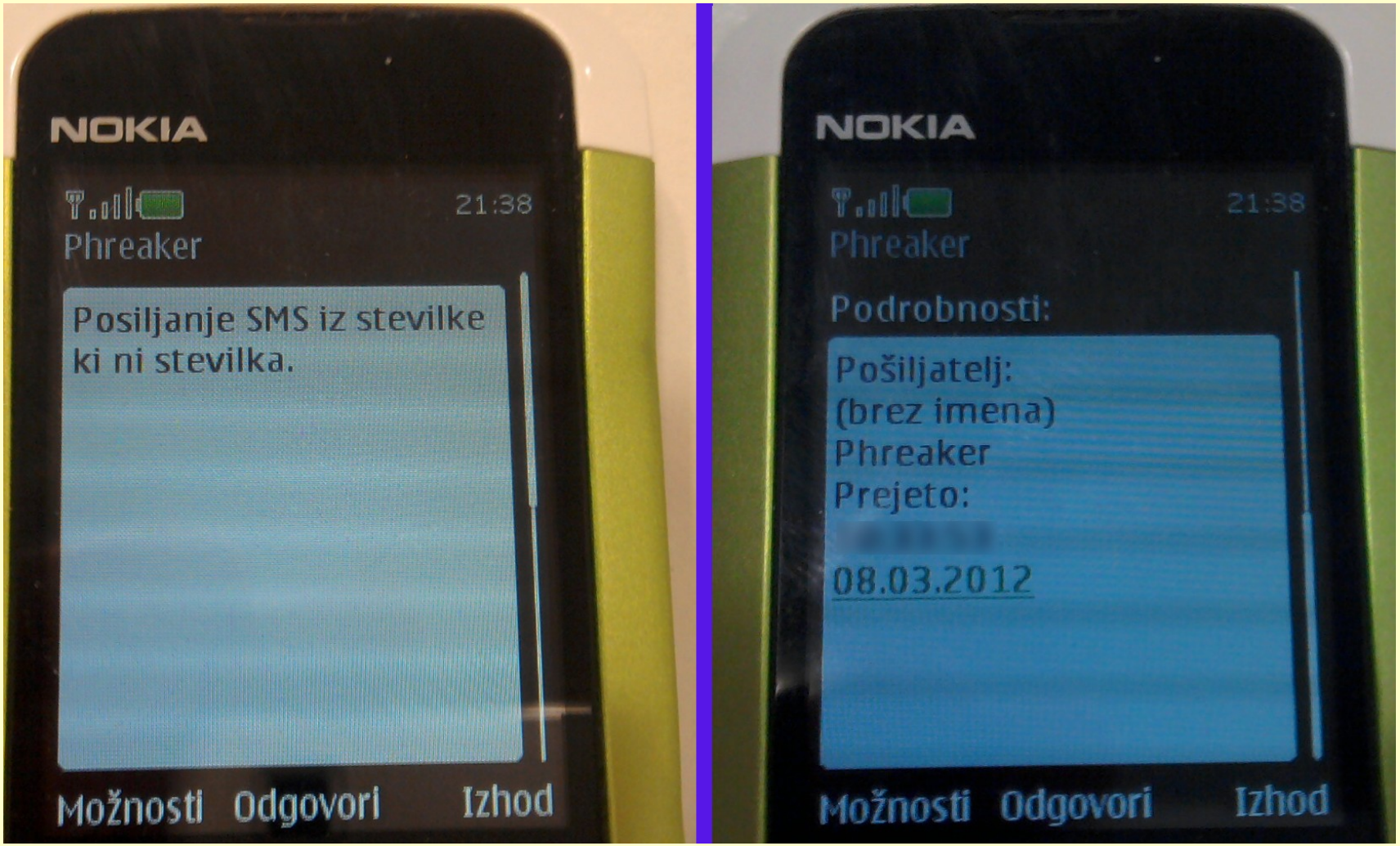
3: rezultat

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

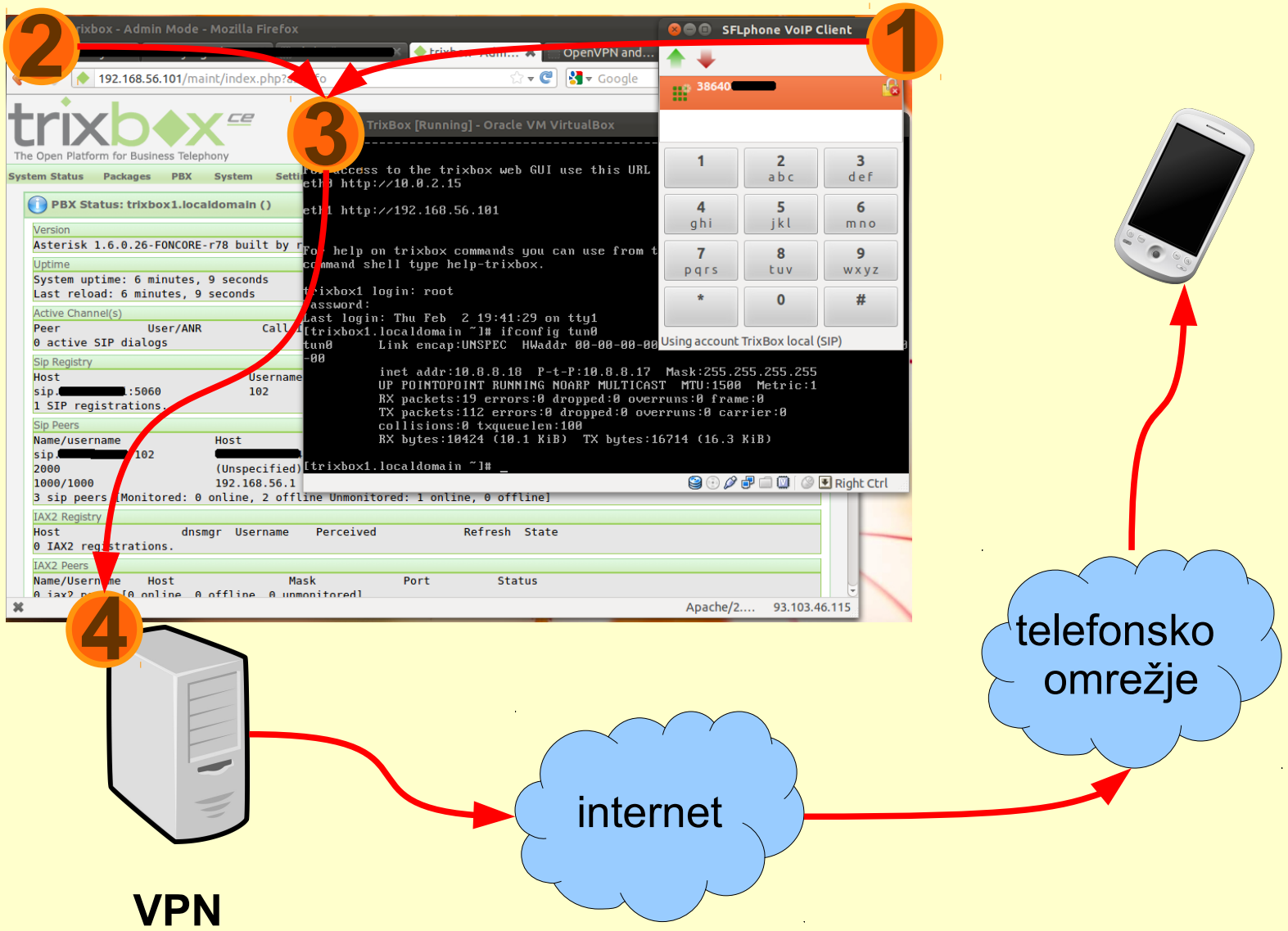


Klicanje s poljubno klicno identifikacijo

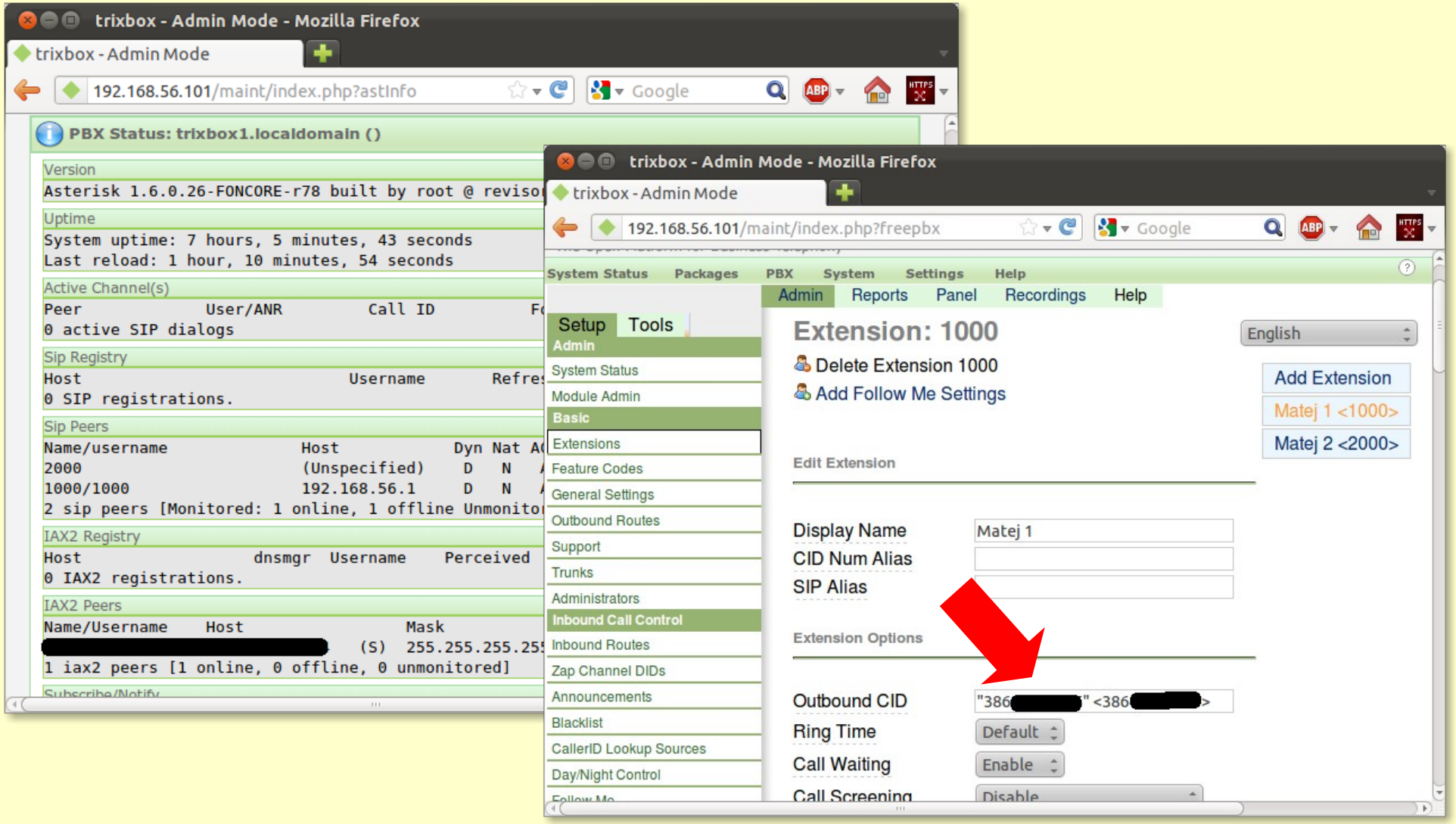
[kljub popravkom nekaterih operaterjev postopek v določenih okoliščinah še vedno deluje]

Klicanje s poljubno klicno identifikacijo

1: vzpostavitev infrastrukture



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

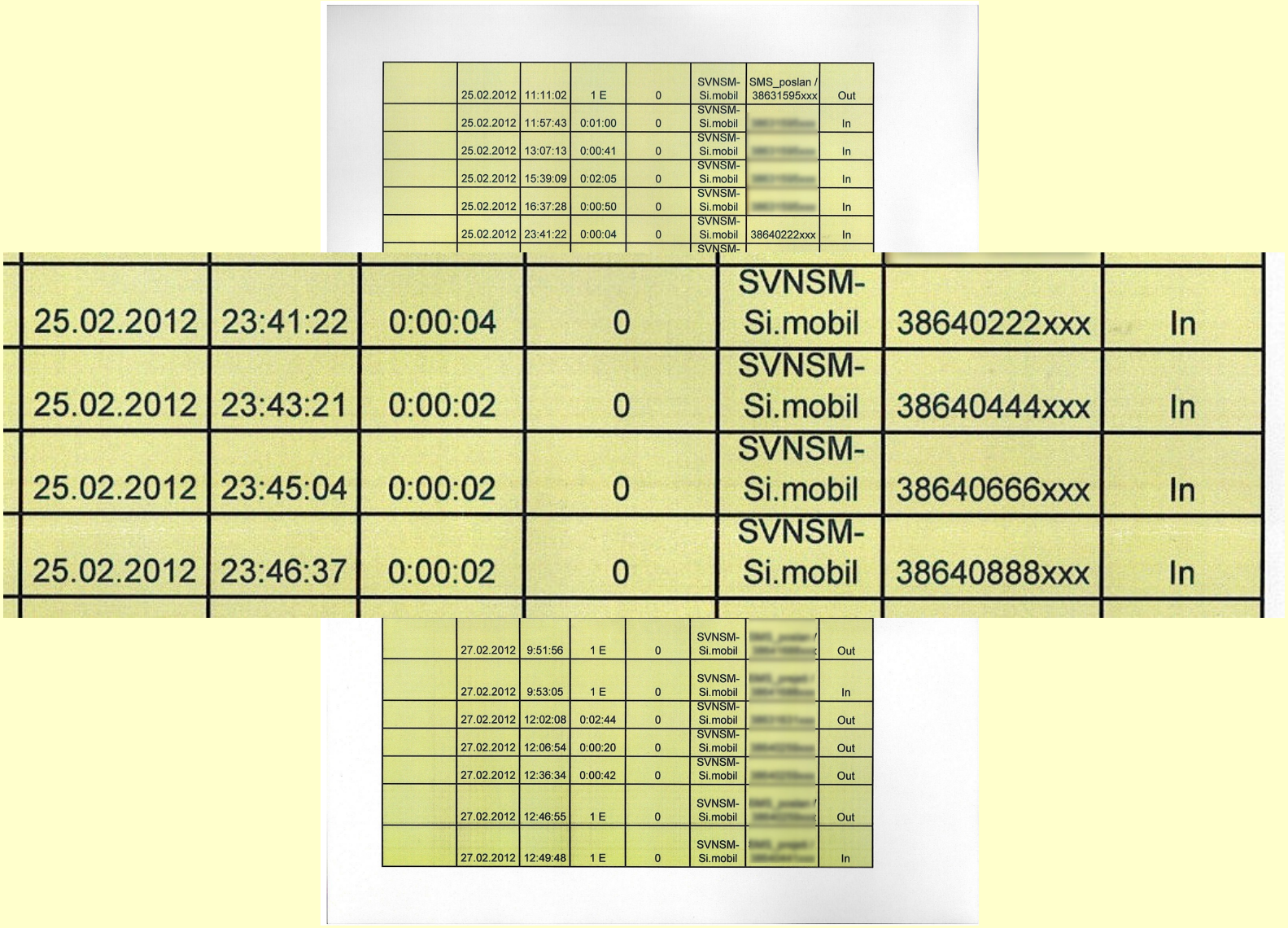


Klicanje s poljubno klicno identifikacijo

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

Praktične posledice :-)

GSM modul za odpiranje garažnih ali vhodnih vrat

Ponujamo vam uporabno napravo, ki z enostavnim telefonskim klicem odpre ali zapre avtomatizirana garažna ali vhodna vrata.

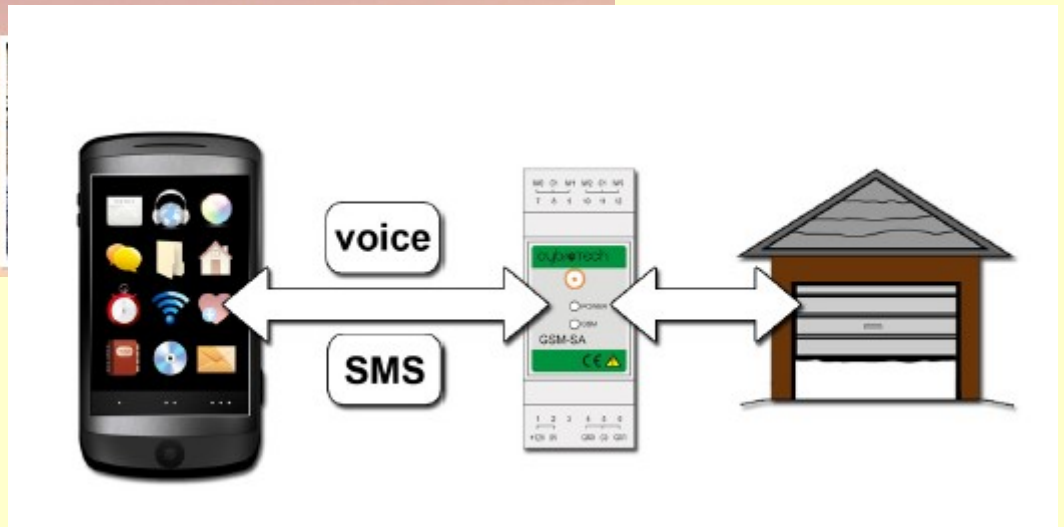
GSM modul je naprava, katero lahko avtorizirani uporabnik pokliče z namenom, da s hitrim klicem odpre ali zapre avtomatizirana vrata. Naprava prepozna največ pet določenih telefonskih številk, iz katerih se lahko na GSM modul pokliče in se s takim klicem sproži odprtje ali zaprtje vrat.

IKU d.o.o. vam nudi:

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

Uporaba GSM modula za odpiranje vrat:

na avtomatizirana garažna, vhodna ali druga vrata se namesti GSM modul, v katerega se zapiše do pet telefonskih (mobilnih) številk, s katerimi je možno s hitrim telefonskim klicem omenjena vrata odpreti ali zapreti. S tem načinom odpade uporaba daljinskih upravljalnikov oziroma dodatnih naprav in aparatov, ker predpostavljamo, da je mobilni telefon že »obvezna oprema« vseh ljudi.



Varnost slovenskih GSM omrežij

1.4 Ethical Considerations

During an ethical discussion the authors decided that operating within the legal framework had the highest priority. There was consensus on the fact that cracking somebody else's GSM traffic should not be performed. Here are some of the legal implications in Norway:

- GSM security research is allowed
- Receiving GSM traffic is (technically) allowed
- Decoding (e.g. cracking) your own GSM traffic is allowed
- Decoding somebody else's GSM traffic is illegal
- Setting up a BTS is allowed if you acquire a license. This is applied for through the Norwegian Post and Telecommunications Authority (NPT).

Decoding GSM. 2010. Magnus Glendrange, Kristian Hove in Espen Hvideberg, Norwegian University of Science and Technology, Department of Telematics.
<http://ntnu.diva-portal.org/smash/get/diva2:355716/FULLTEXT01>

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 do največ 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)

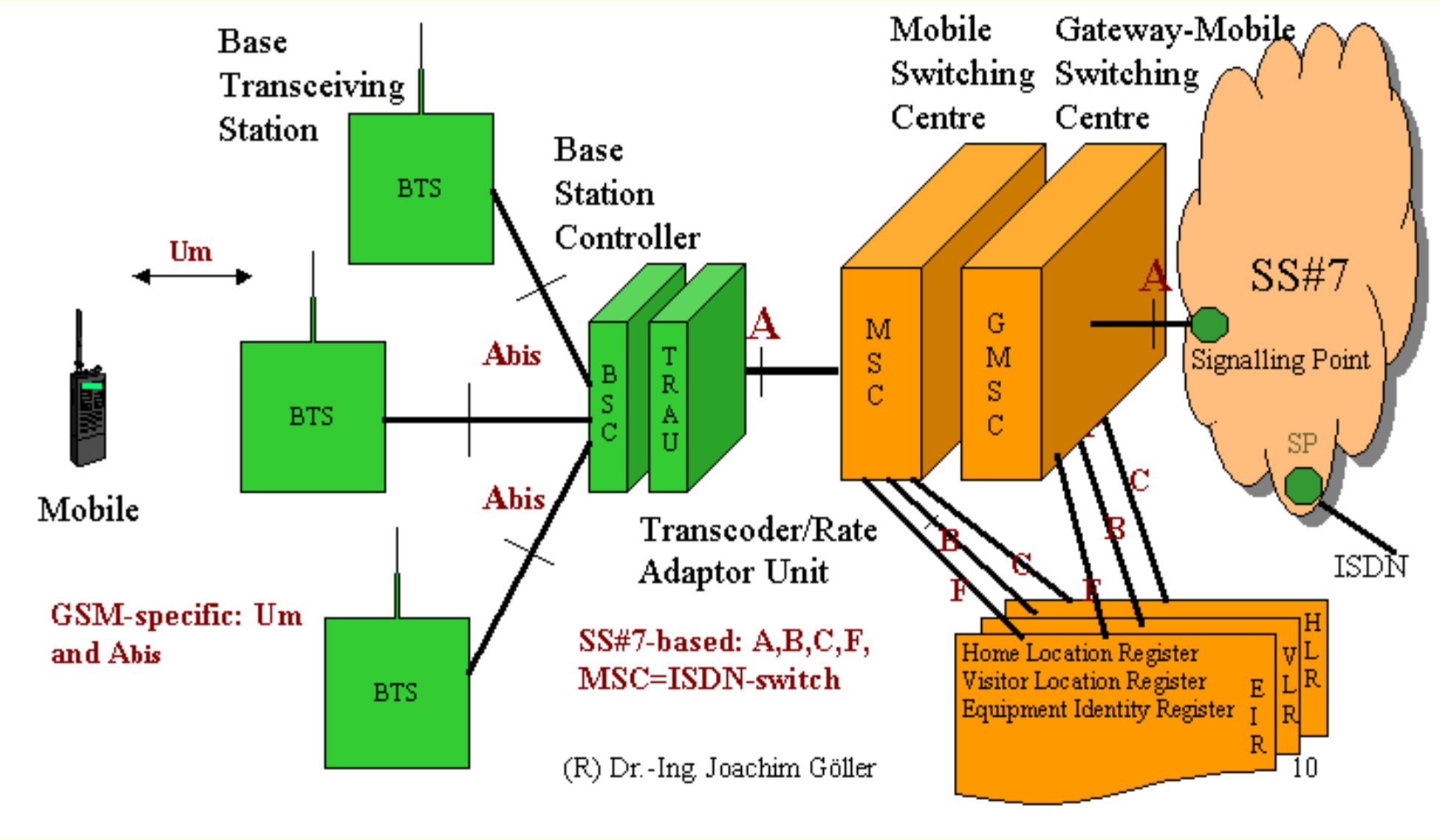
- Impersonacija - ponarejanje (lastne) mobilne identitete:
  - iz omrežja zajamemo naslednje identifikacijske podatke našega telefona: IMSI, TMSI, Kc, sekvenčno številko ključa. Gre za podatke našega lastnega mobilnega telefona.
  - te podatke prepišemo v naš drugi telefon in s tem telefonom opravimo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

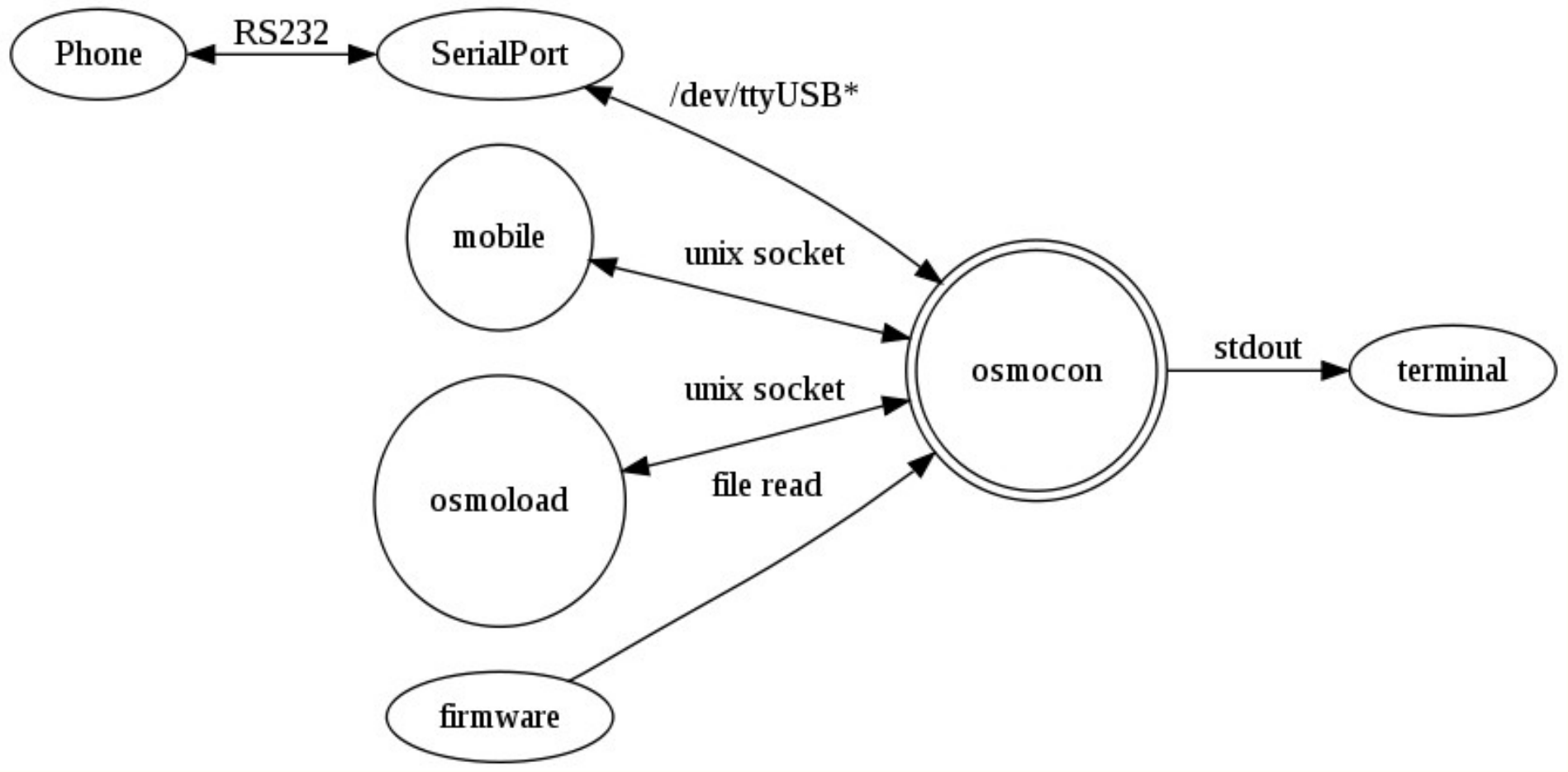
Shema GSM omrežja, vir: *www.gsmfordummies.com*.

OsmocomBB

Mobilni telefon s Calypso čipovjem...

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

...in OsmocomBB strojna programska oprema

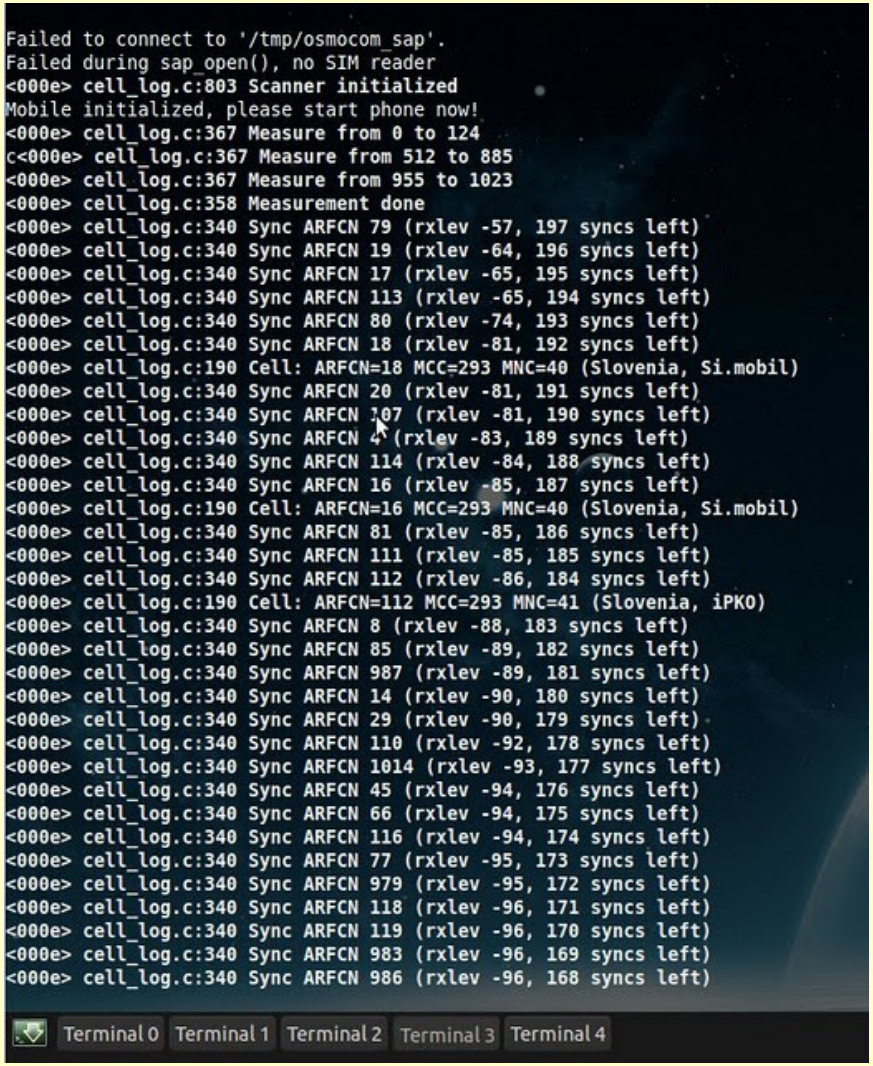


Zagon nalagalnika ROM (ang. *romloader*)

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

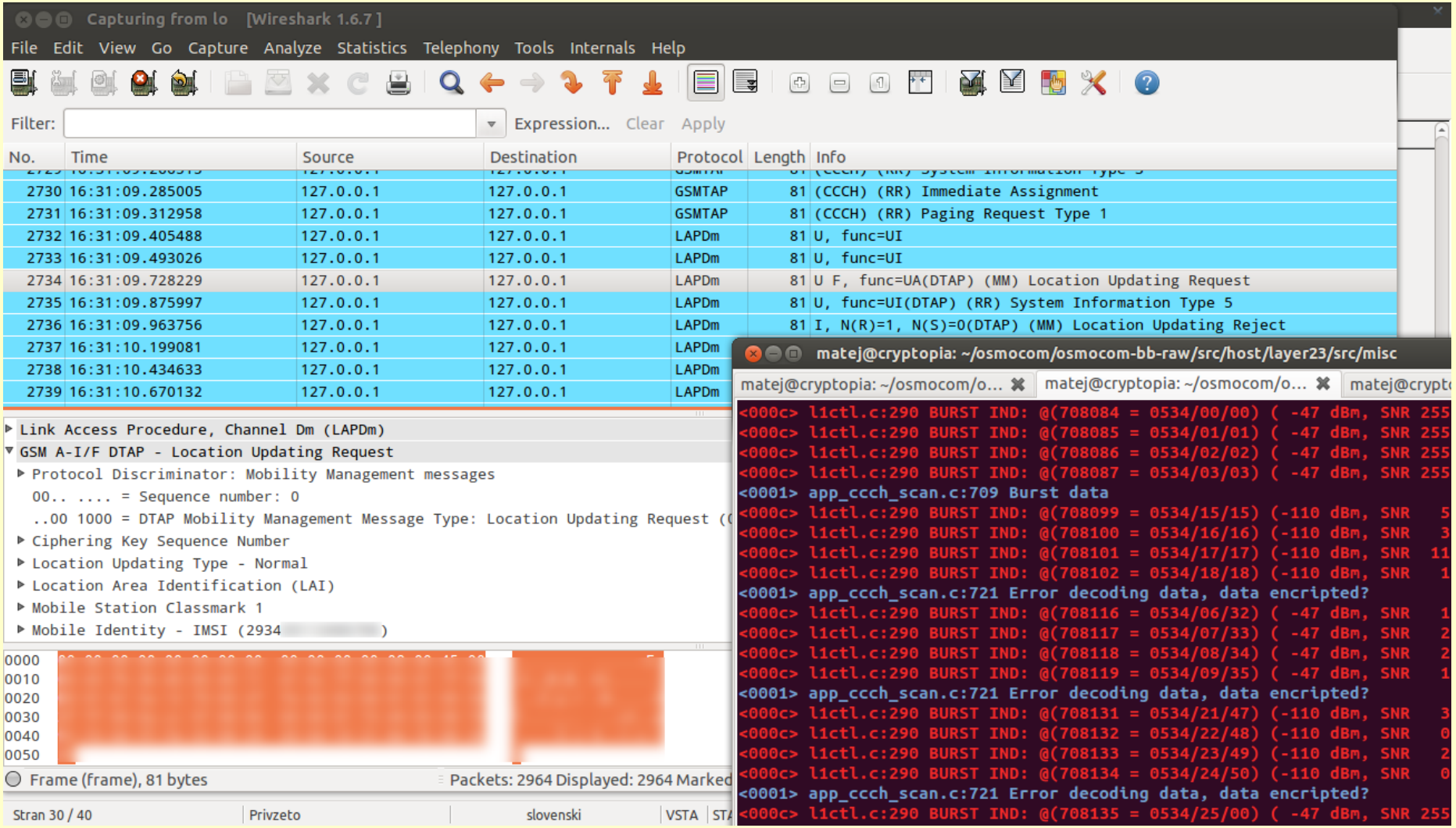
```
Die ID code: 7e540b2fc90393bb
======================================================================
REG_DPLL=0x2413
CNTL_ARM_CLK=0xf0a1
CNTL_CLK=0xff91
CNTL_RST=0xfff3
CNTL_ARM_DIV=0xfff9
======================================================================
Power up simcard:


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...

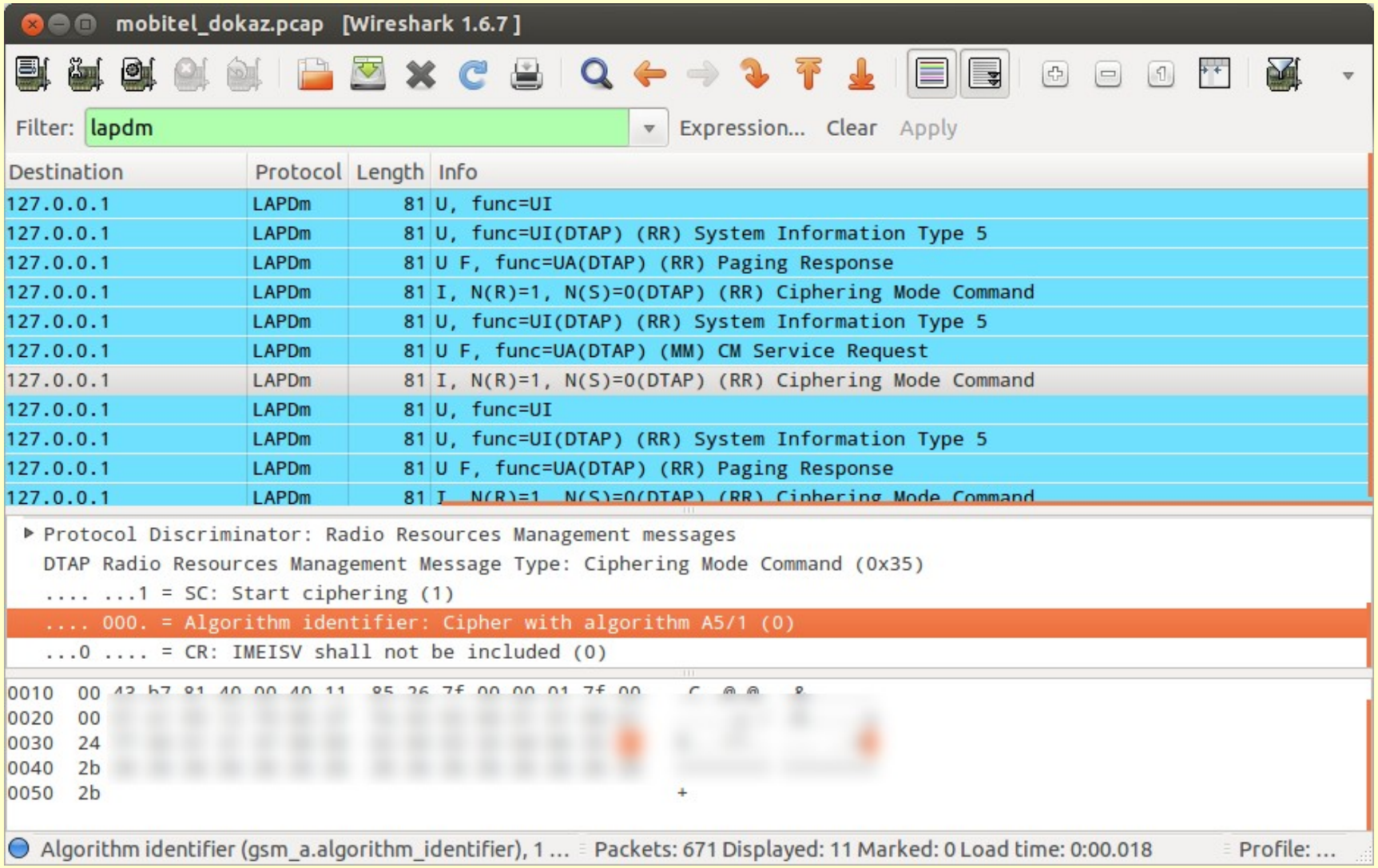


Analiza GSM prometa. Promet zajamemo s programom *ccch_scan* in ga prikažemo v aplikaciji Wireshark.

Varnostni pregled slovenskih GSM omrežij

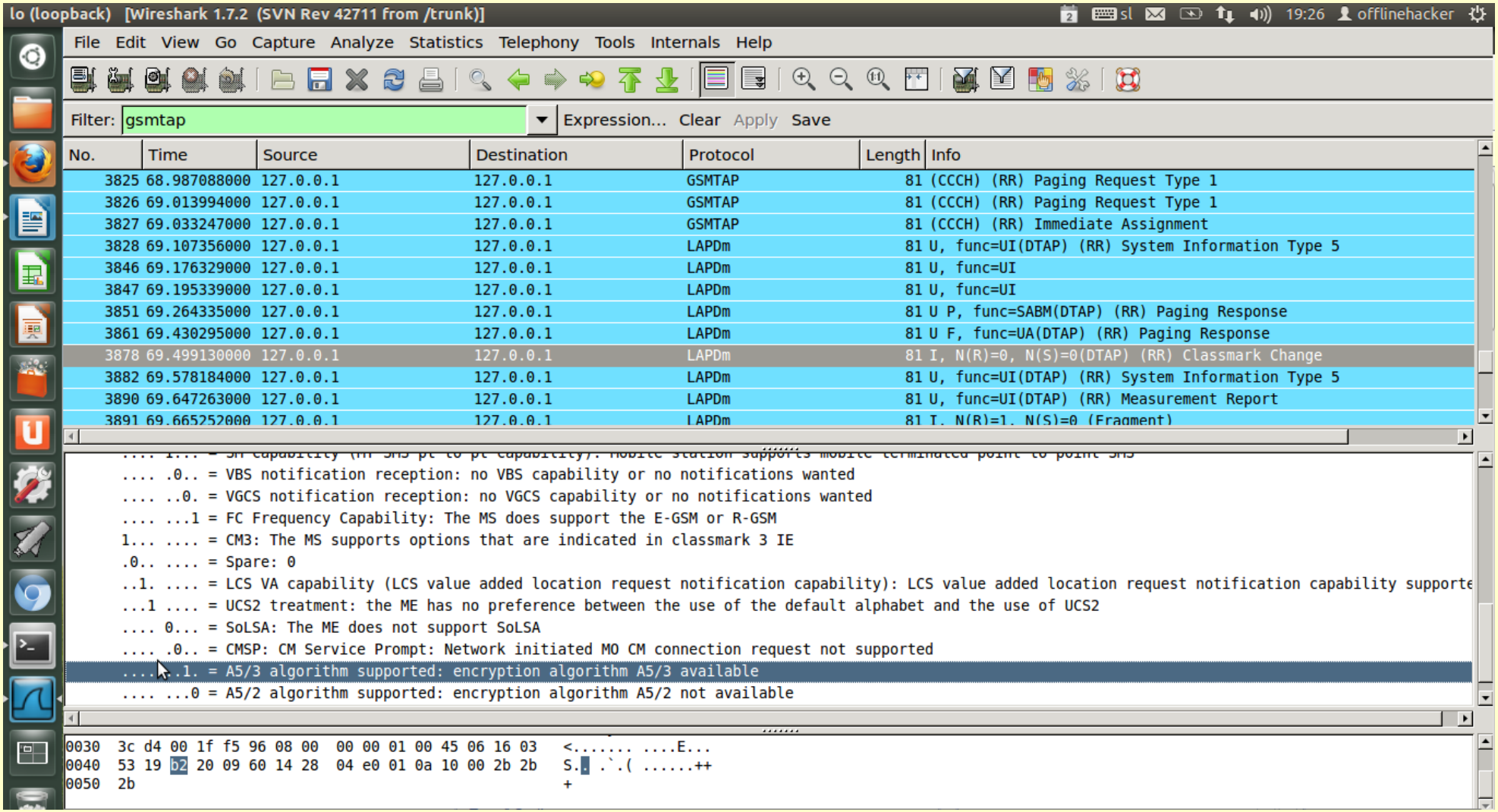
[nekatere opisane ranljivosti so bile po objavi člankov že odpravljene]

Uporaba šifriranja - Mobitel



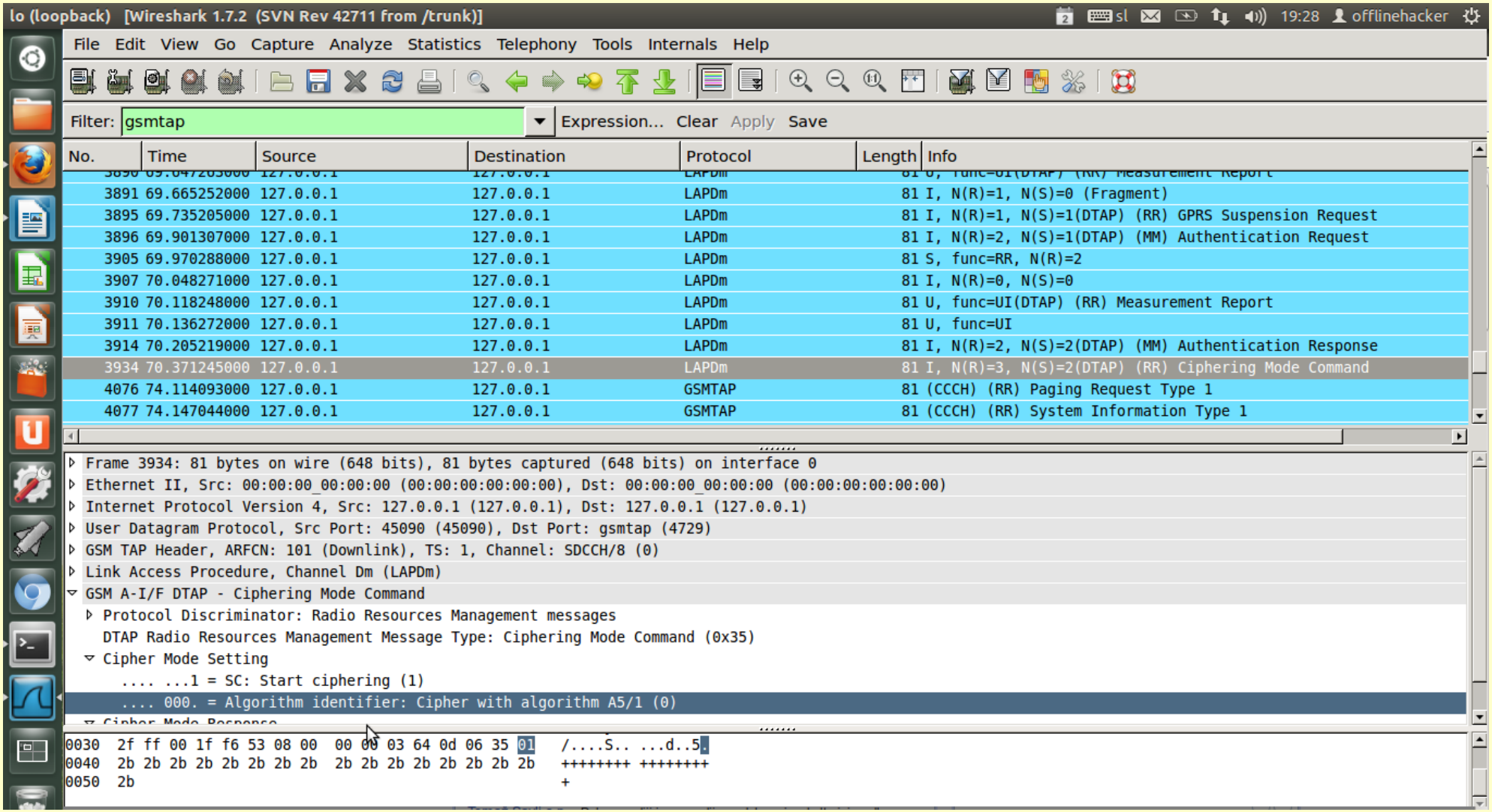
Mobitel je v času pregleda uporabljal šifriranje A5/1

Uporaba šifriranja - Mobitel



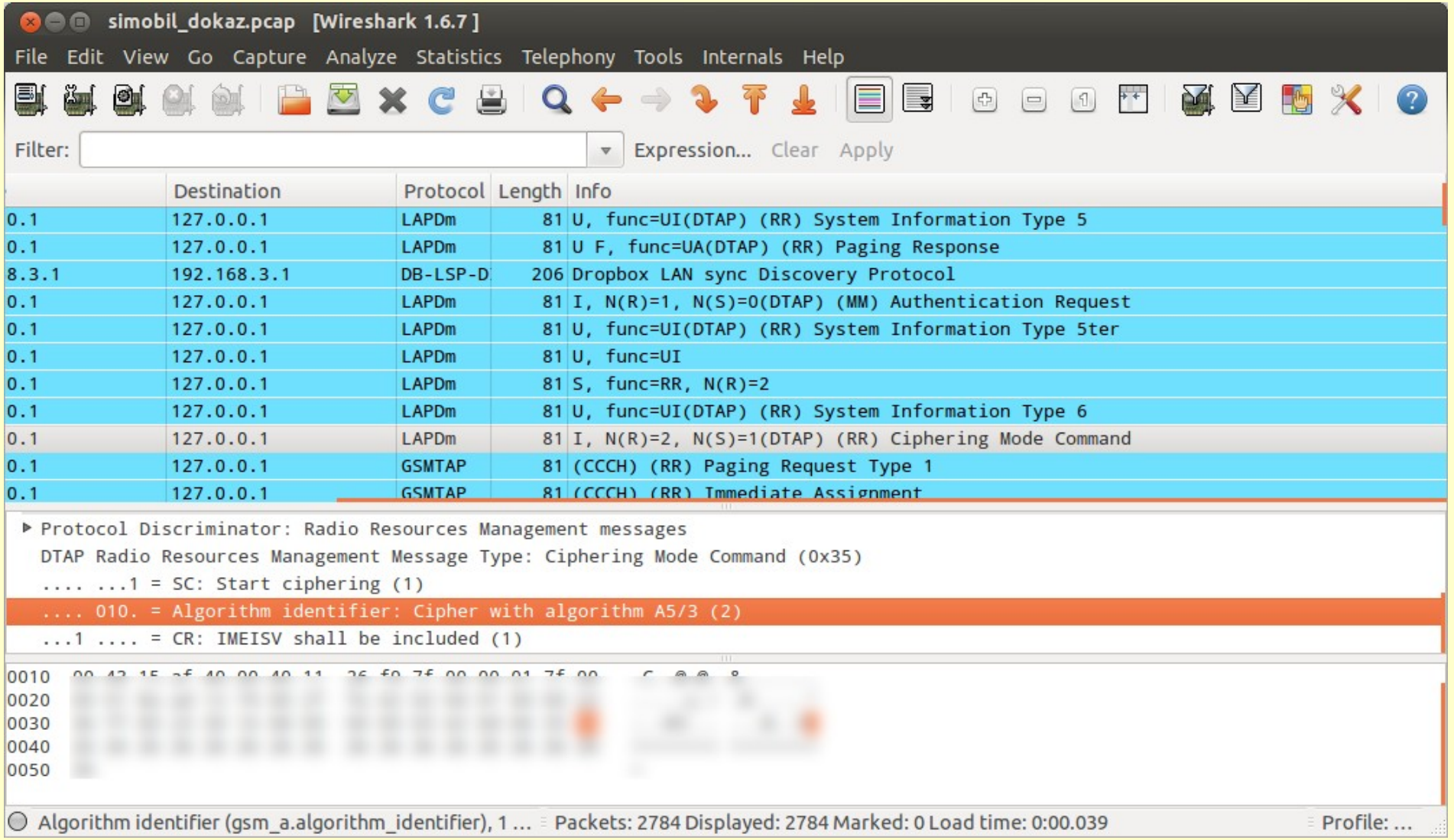
Če je mobilni telefon sporočil, da podpira A5/3...

Uporaba šifriranja - Mobitel



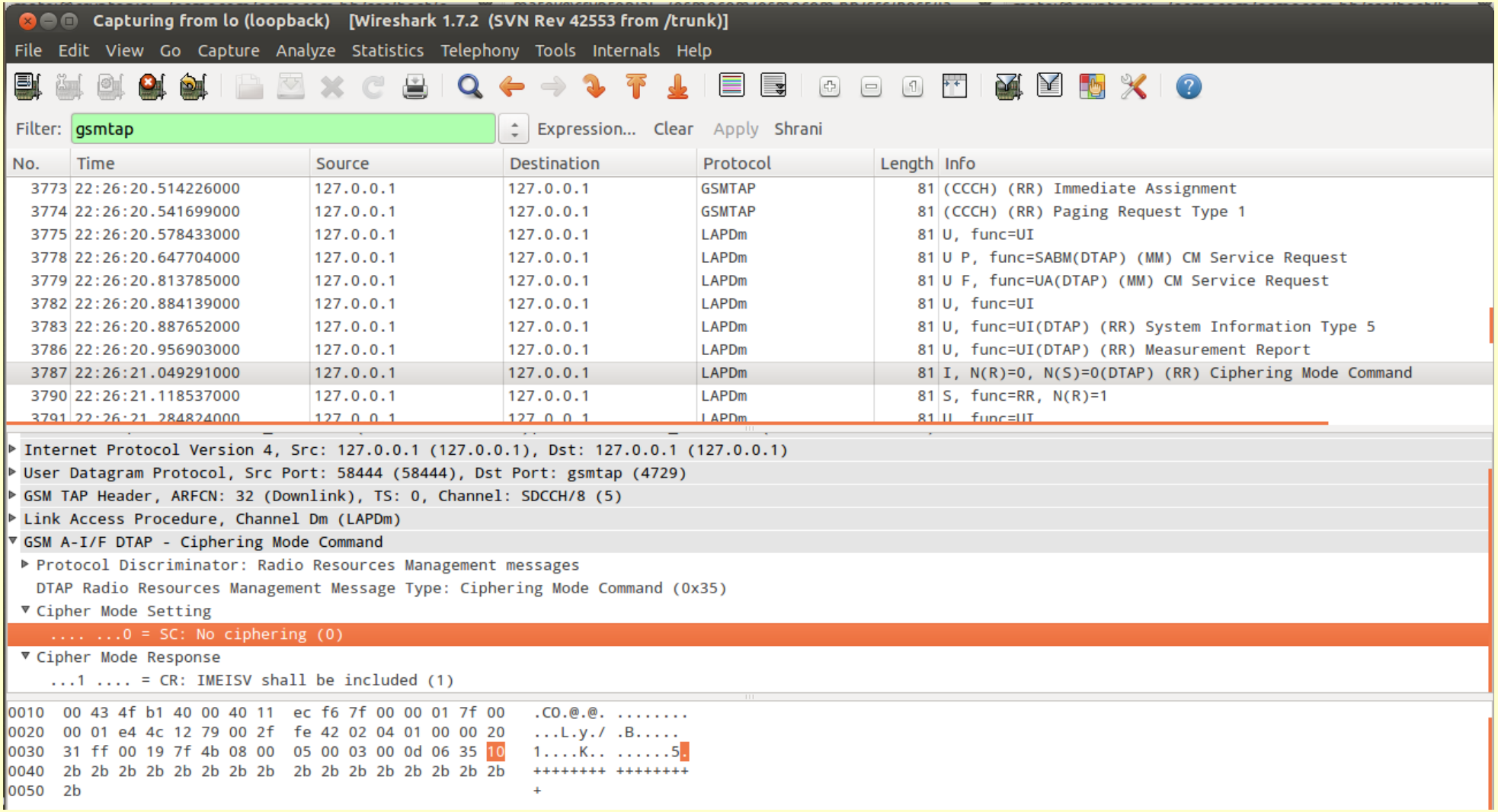
...je omrežje odgovorilo,da je na voljo samo A5/1.

Uporaba šifriranja - Simobil



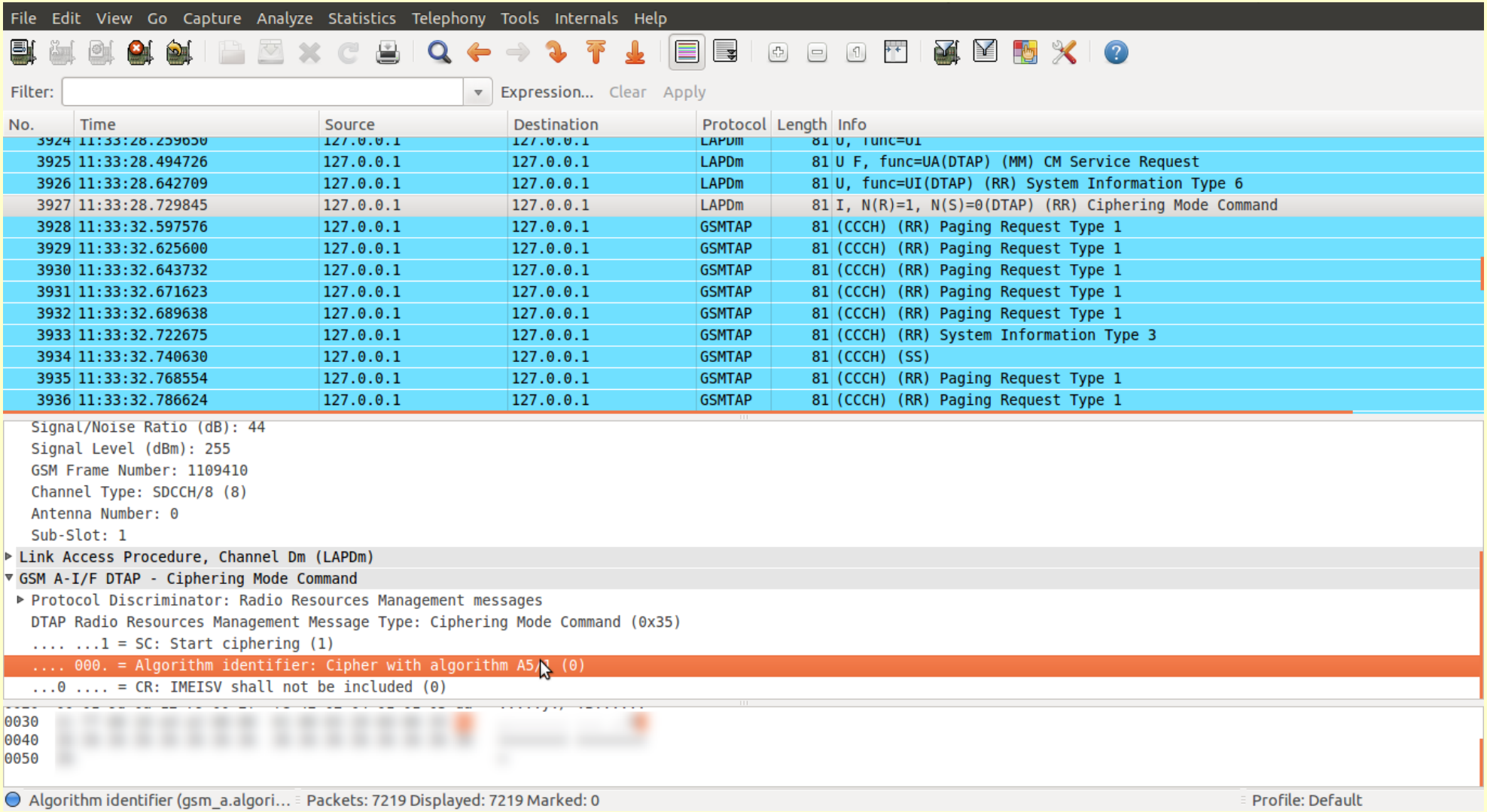
Simobil je v času pregleda uporabljal tudi A5/3...

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.

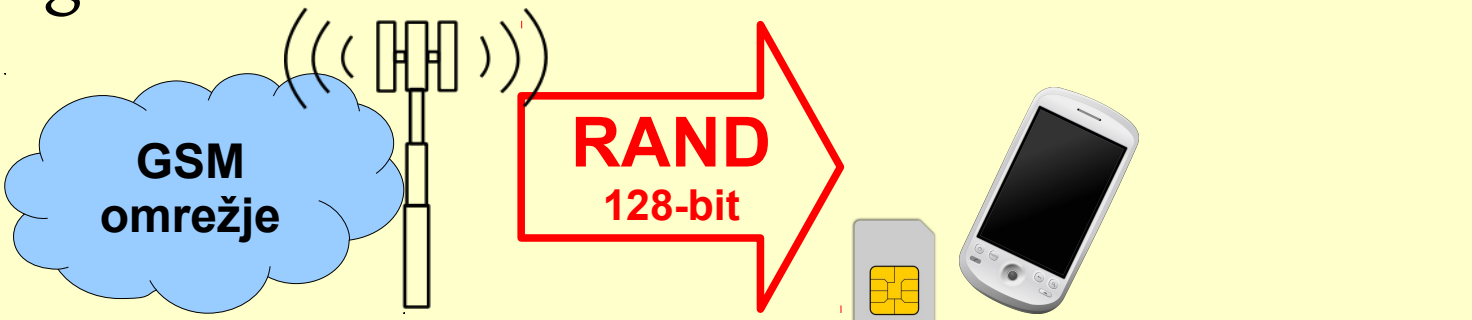
Kriptoanaliza sejnega šifrirnega ključa Kc
(brez posedovanja mobilnega telefona in/ali SIM kartice tarče)

[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.

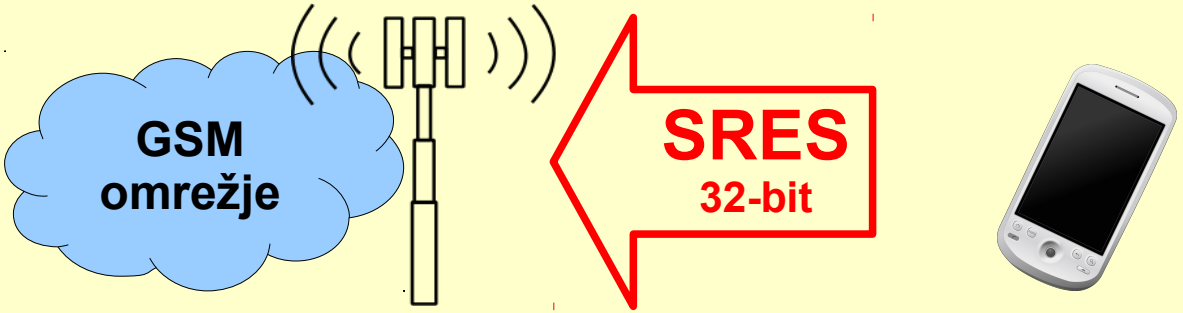
1.



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

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

2.



Omrežje preveri ali se sprejeti **SRES** ujema z njegovim.

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

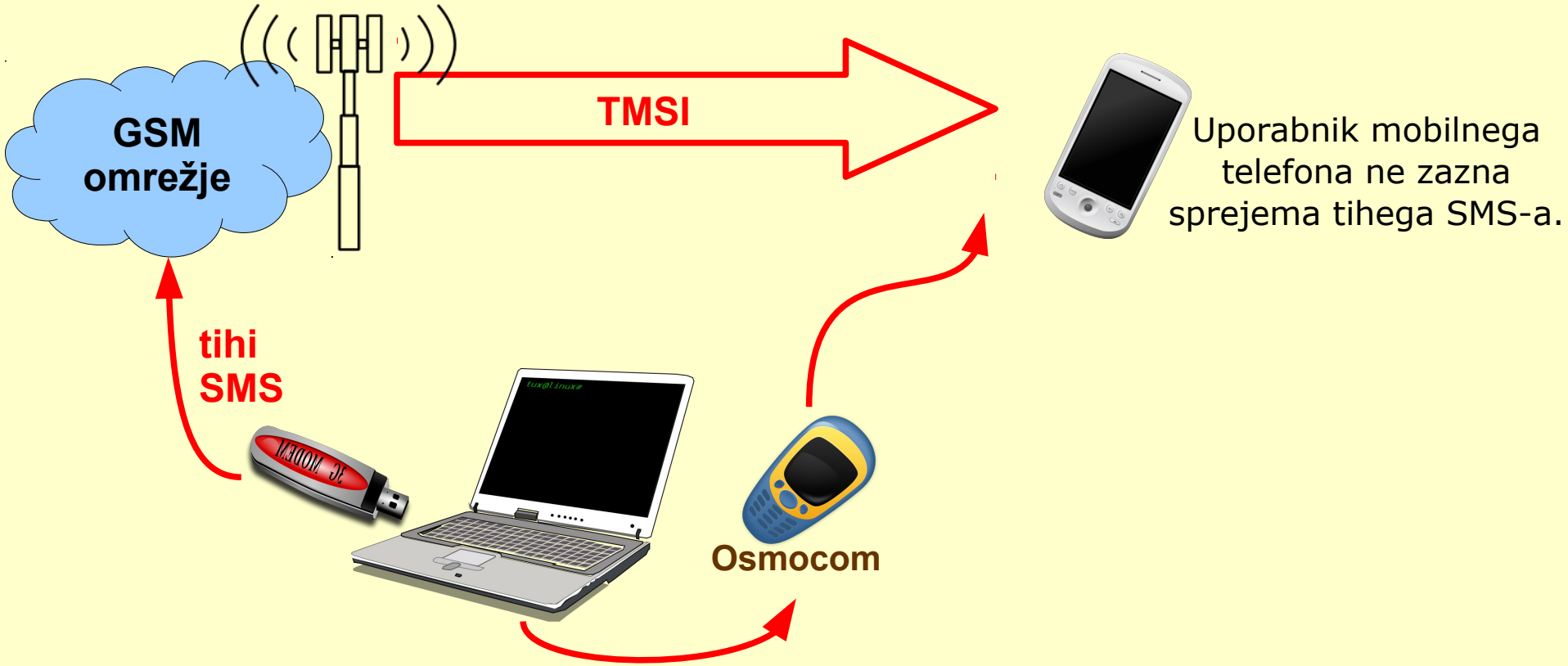
ŠIFRIRANO SPOROČILO (XOR)

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

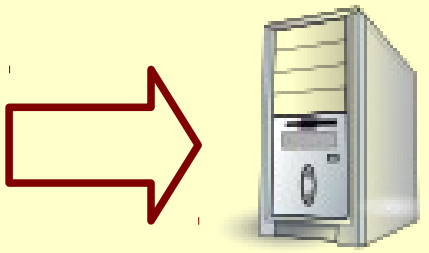
praksa

5.

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

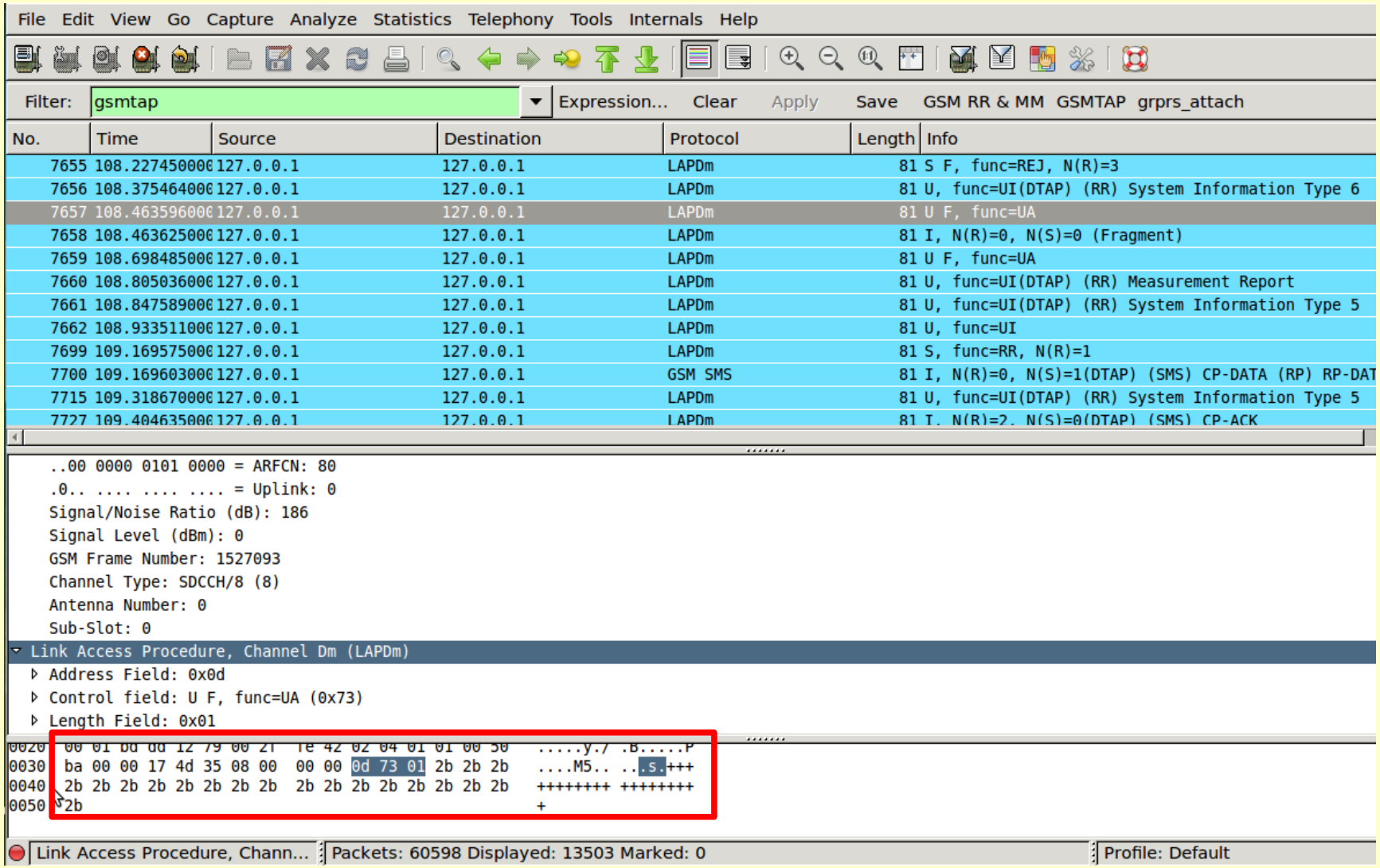
VSEBINA PODATKOVEGA IZBRUHA V GSM

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

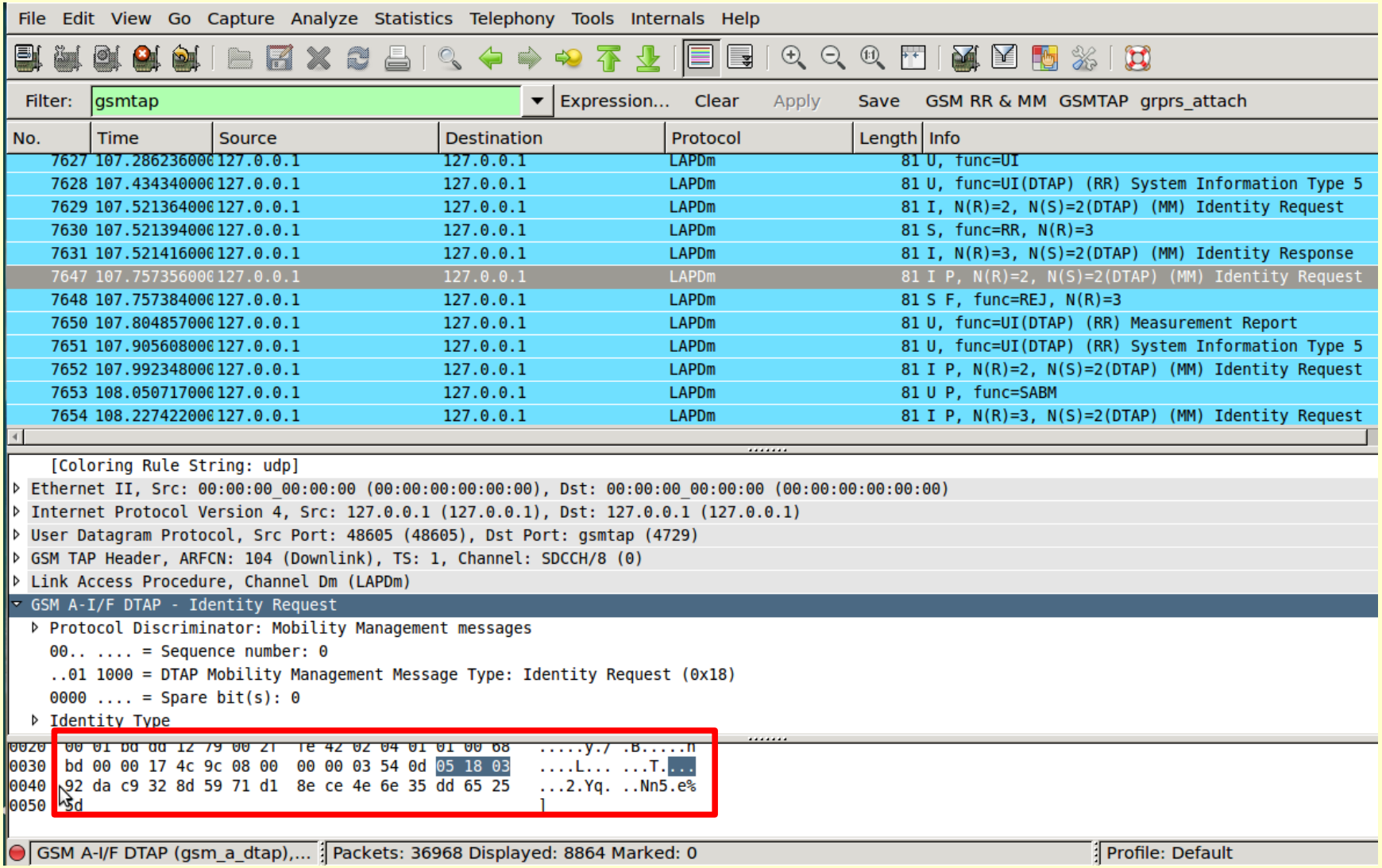


- Iz “zraka” pasivno zajamemo šifrirane podatkovne pakete.
- S pomočjo ugibanja vsebine podatkovnega izbruha (uganemo vsebino tim. polnila - ang. *padding bits*) izračunamo “enkratni” ključ za šifriranje toka podatkov.
- Sejni šifrirni ključ Kc nato rekonstruiramo s pomočjo kriptoanalize.
- V postopku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

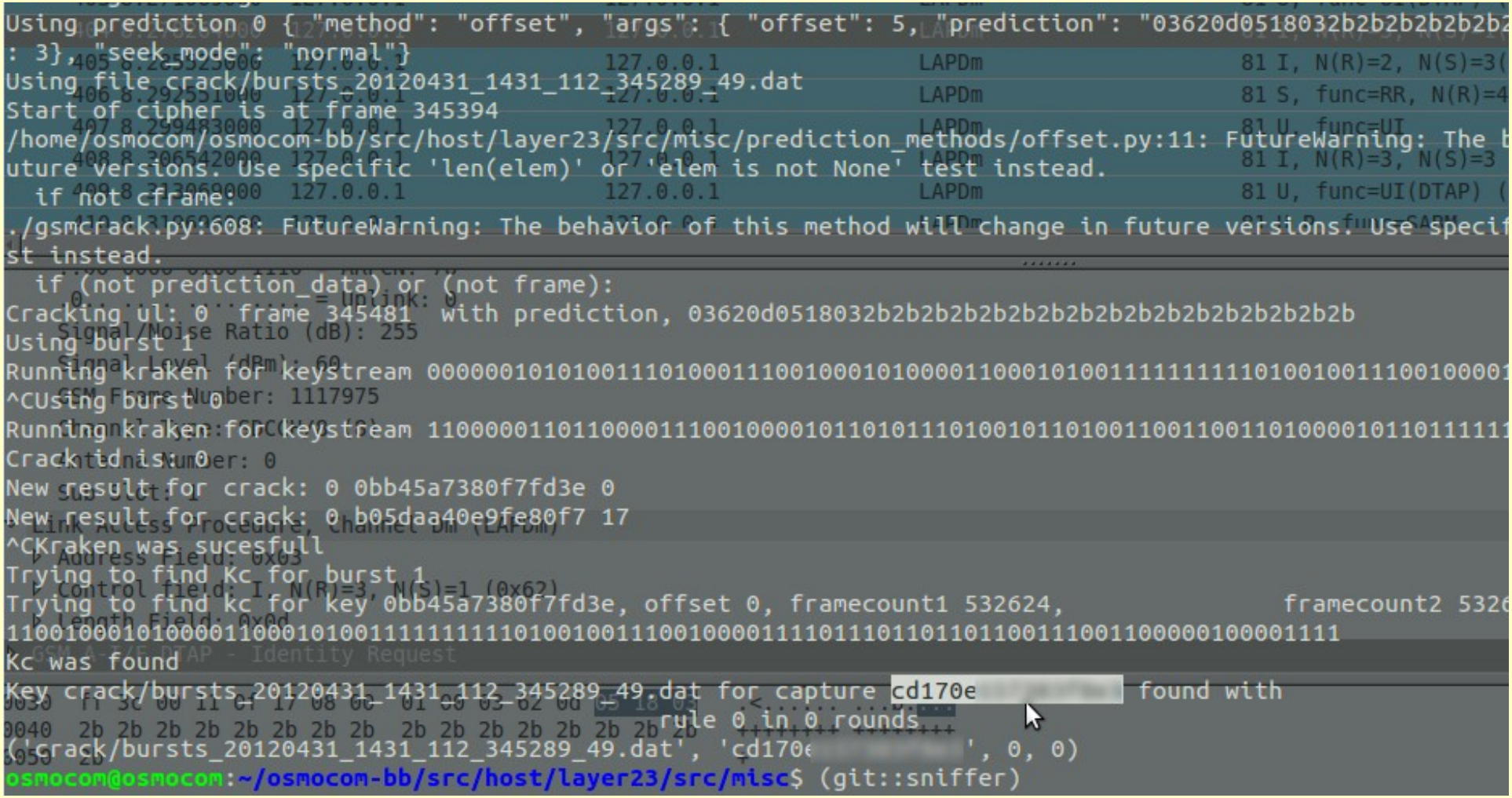
Navadno zapolnjevanje
(*non-random padding*)



Naključno zapolnjevanje
(*random padding*)

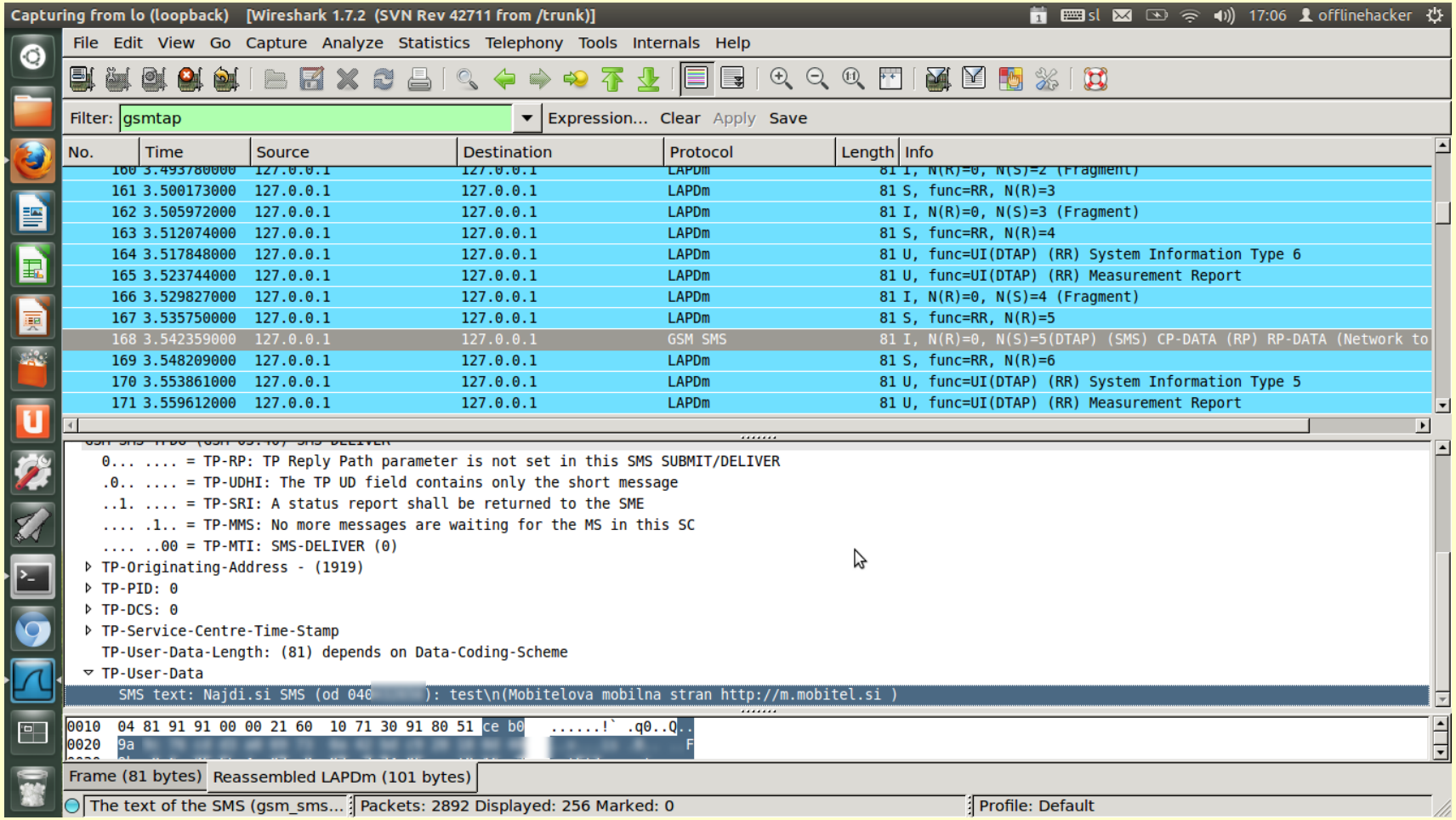


Razbijanje A5/1 sejnega šifrirnega ključa Kc v praksi



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

Razbijanje A5/1 sejnega šifrirnega ključa Kc v praksi



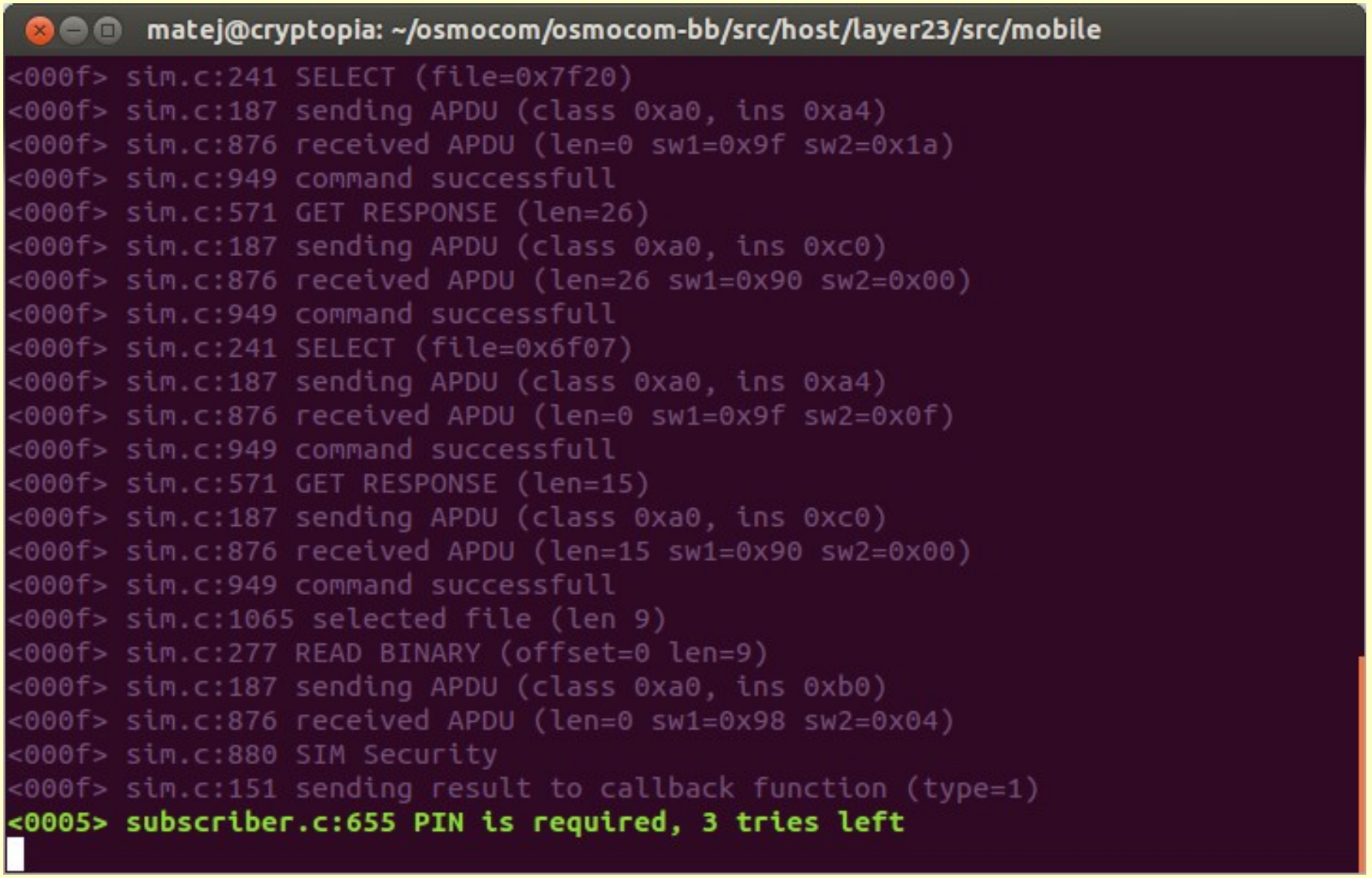
… in dešifrirano SMS sporočilo (prejeto preko 2G).
Program *gsmcrack.py* samodejno identificira TMSI številko na podlagi klicne številke (s pomočjo pošiljanja tihih SMS sporočil), ko imamo TMSI tarče pa aplikacija zna samodejno slediti telefonu na s strani bazne postaje dodeljeni kanal in posneti šifrirano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

Ponarejanje mobilne identitete v GSM omrežju

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

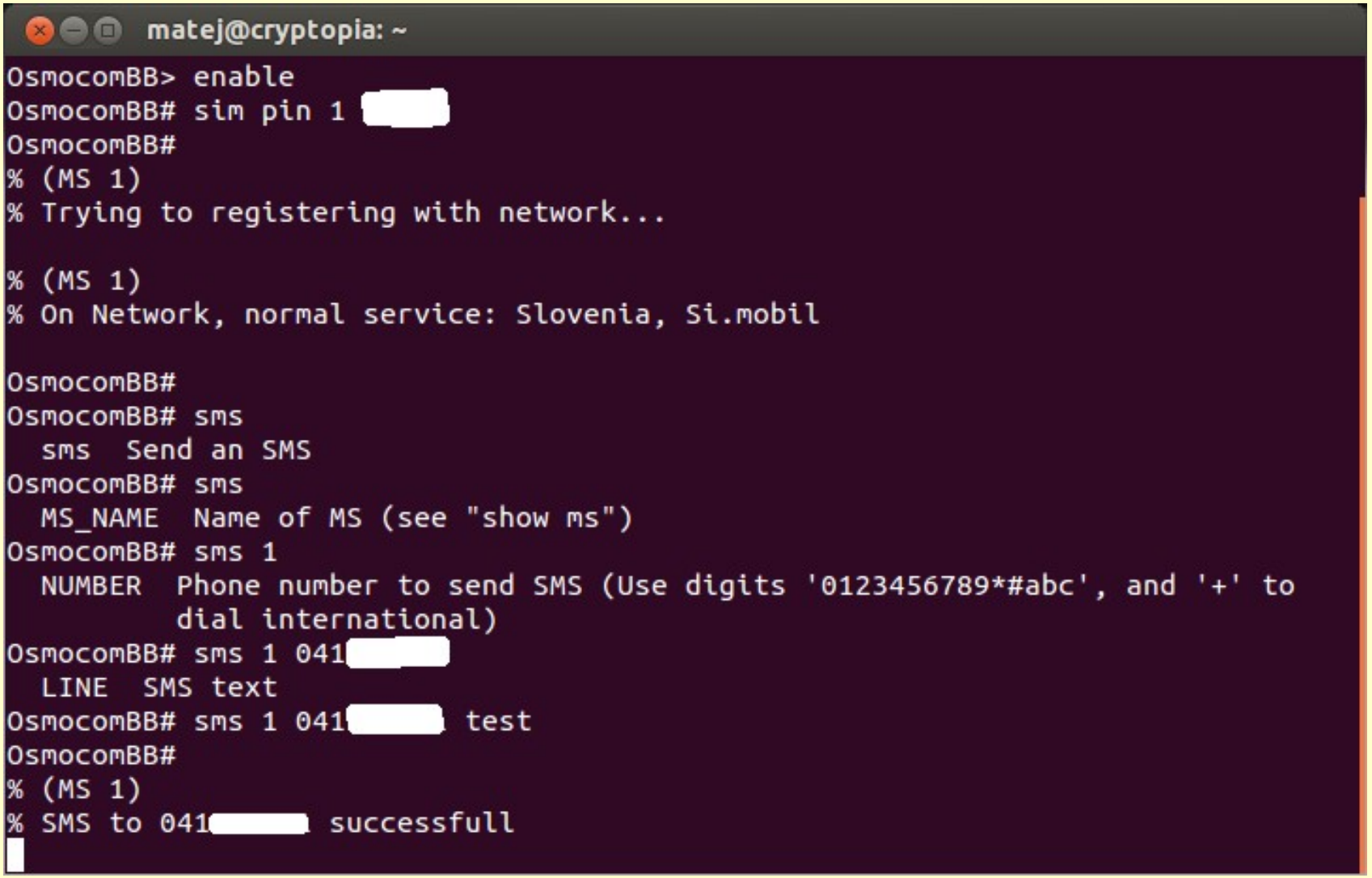
[ranljivosti so bile v večini slovenskih GSM omrežij odpravljene in postopek ne deluje več]

Aplikacija *mobile*



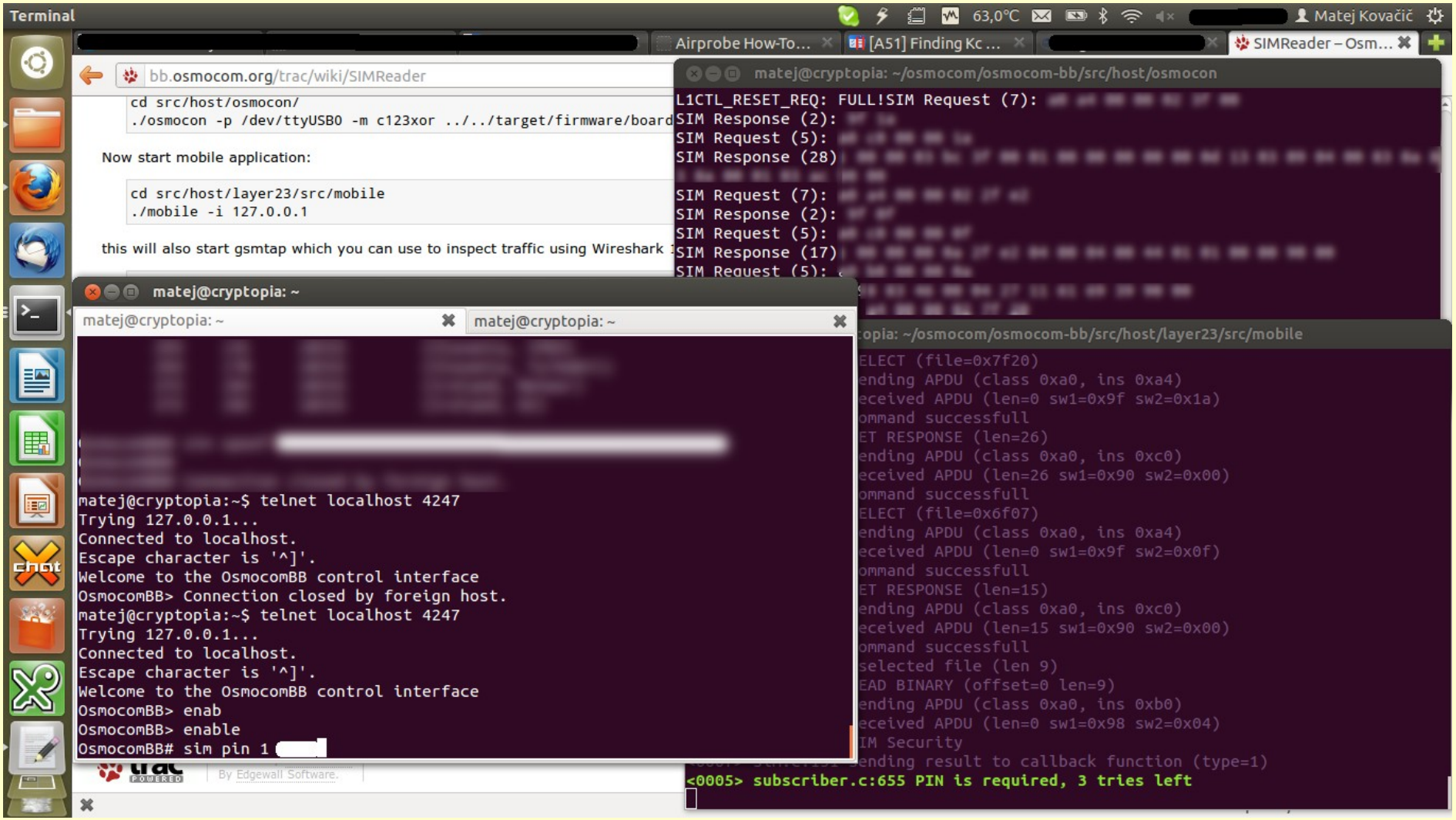
Aplikacija *mobile* omogoča klicanje ter pošiljanje in sprejemanje SMS sporočil na OsmocomBB mobilnih telefonih.

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*).

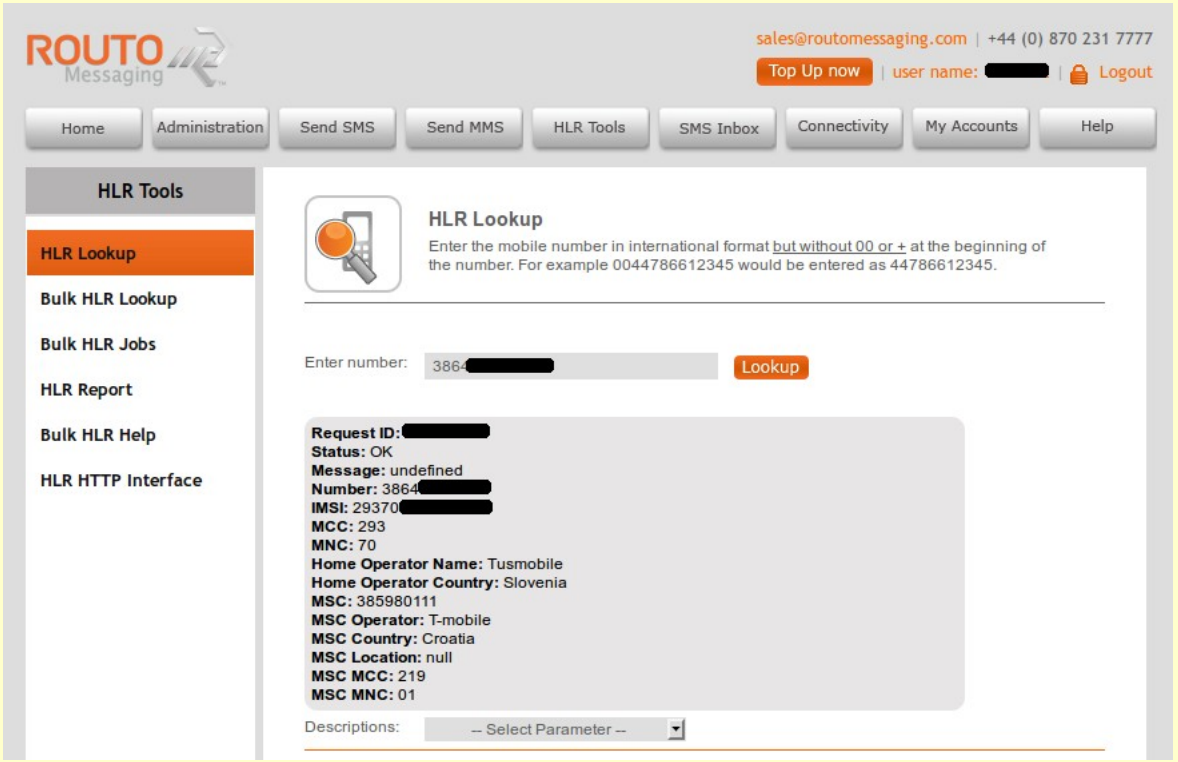
Ponarejanje mobilne identitete

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

1.

HLR vpogled

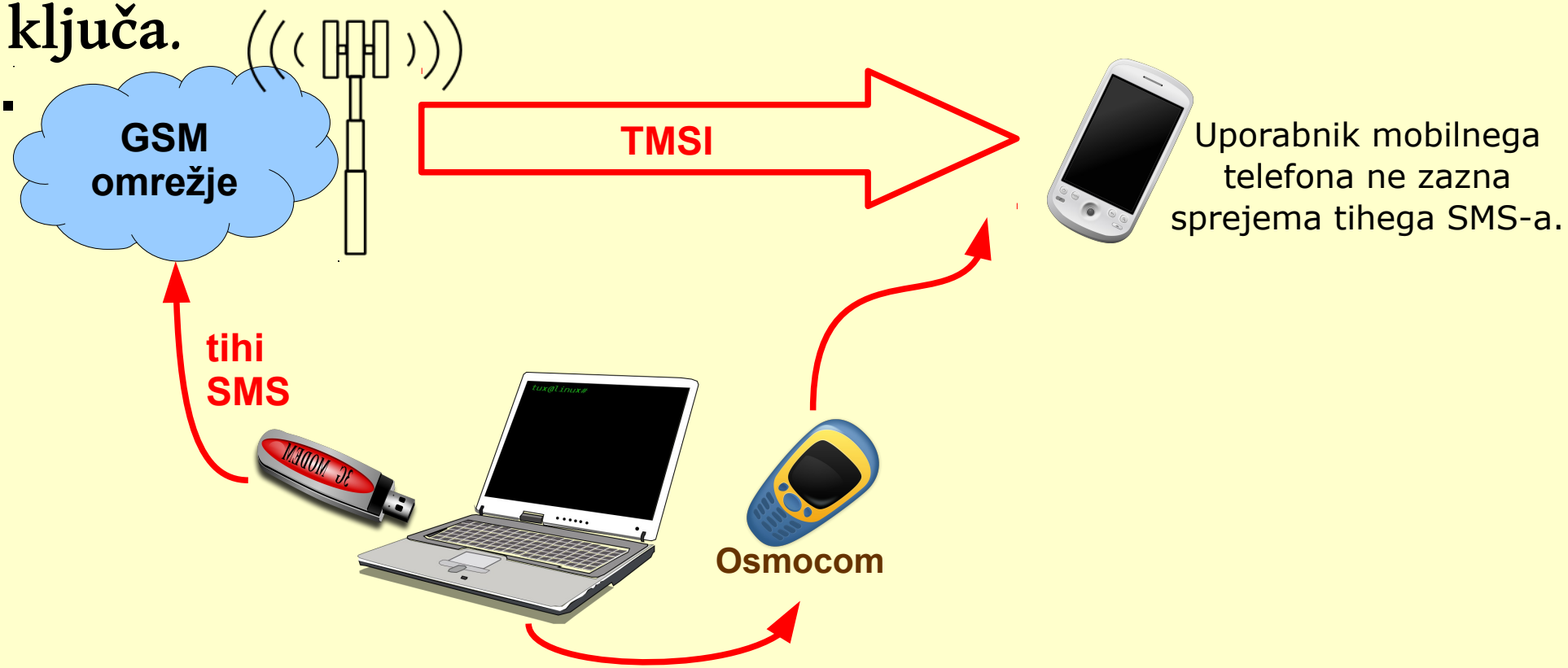
Preko spletne storitve za telefonsko številko izvedemo HLR vpogled in pridobimo IMSI številko.



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

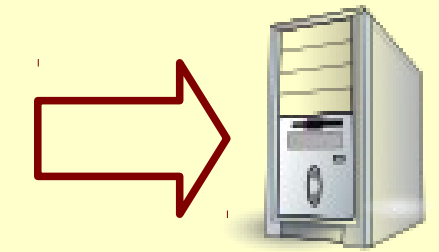
S pomočjo kriptoanalize **rekonstruiramo sejni šifrirni ključ Kc.** Sedaj imamo vse potrebne podatke...

3.

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

VSEBINA PODATKOVEGA IZBRUHA V GSM

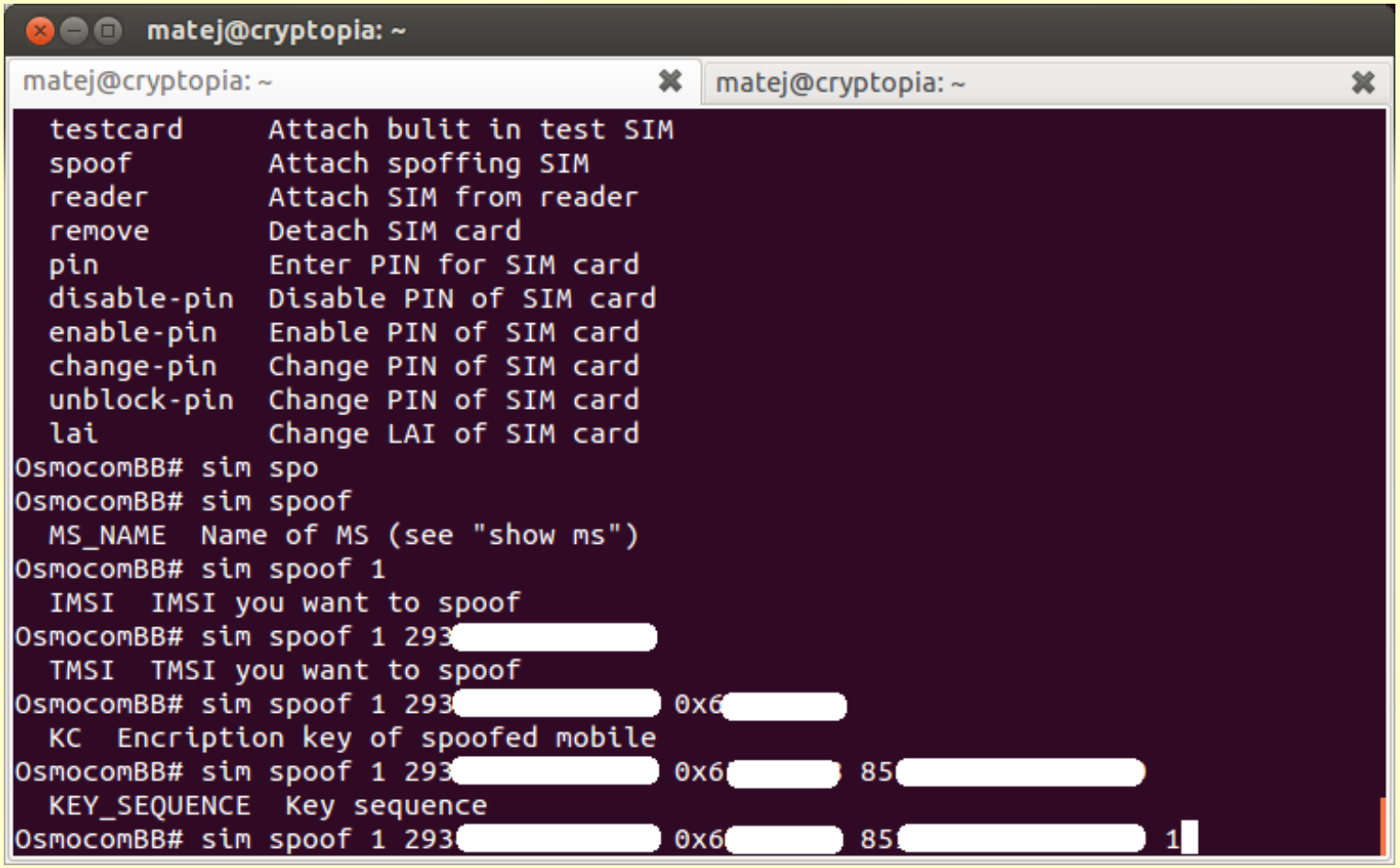
72	FE	BC	10	74	70	C4	2B	2B	2B	2B	2B	2B



Kraken

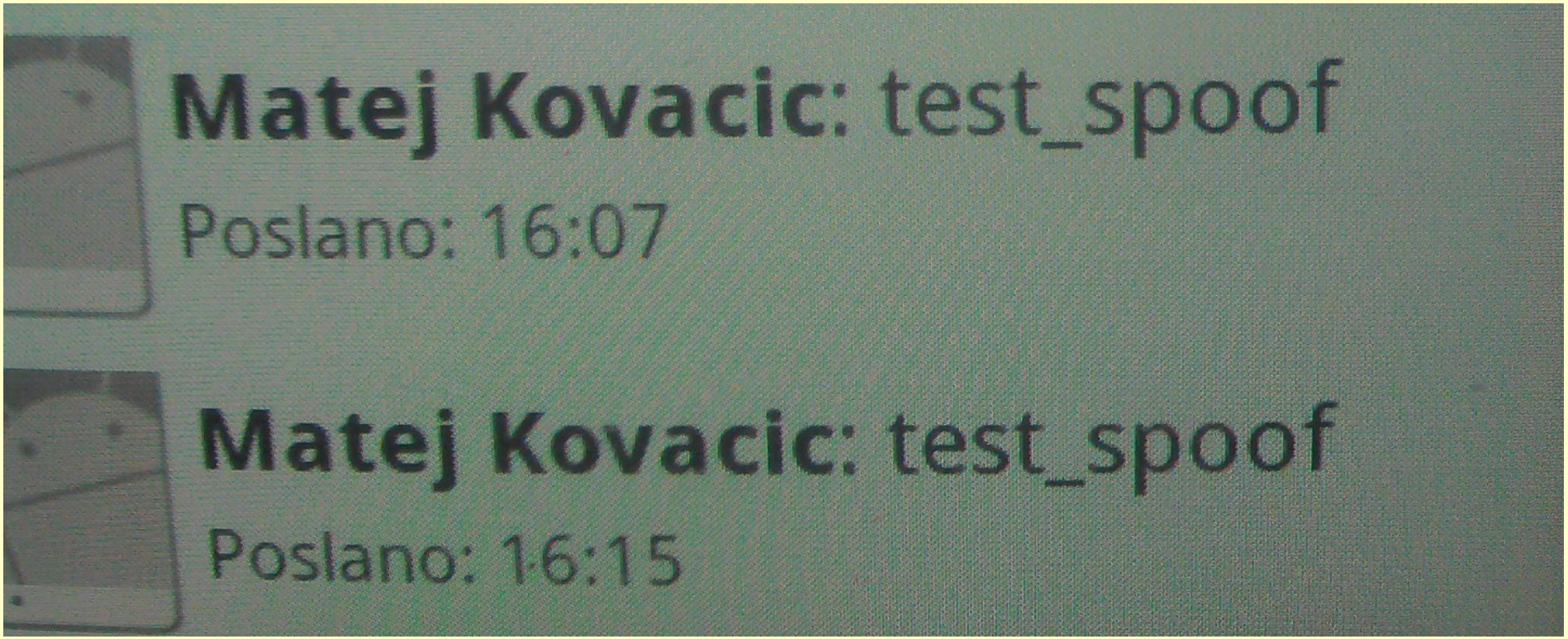
Kc

“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? In kaj za zvočne prisluhe telefonskih pogovorov?

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 do 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>

Operaterji so svoja omrežja nadgradili.
Smo sedaj varni?

Pravzaprav ne. Zakaj?

- Pošiljanje SMS sporočil s spremenjeno identifikacijo ter klicanje s spremenjeno identifikacijo je še vedno mogoče.
  - Z nekaj spretnosti so taki klici še vedno težko izsledljivi.
- Prestrezanje komunikacij je še vedno mogoče (kljub A5/3).
- Verjetno bi bilo še vedno mogoče izvajati ponarejanje mobilne identitete.

- V GSM omrežju obstajajo še nekatere druge ranljivosti.

- Na varnosti GSM tehnologije temelji tudi varnost nekaterih drugih rešitev.

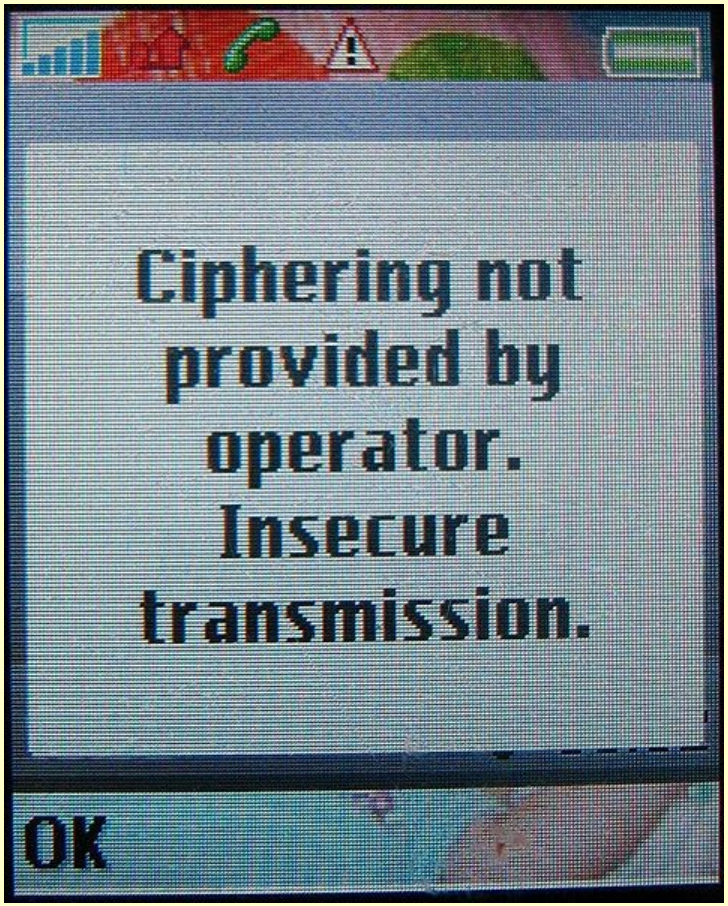
Problem: mobilno omrežje se ne avtenticira mobilnemu telefonu

- GSM omrežje je zasnovano tako, da se morajo mobilni telefoni avtenticirati omrežju. Vendar pa se po drugi strani mobilno omrežje **ne** avtenticira telefonu.
- Prevod: mobilni telefon ne ve v katero mobilno omrežje je povezan.

- Posledica: mogoč je napad s tim. "IMSI-catcherjem", posebno napravo, ki se v omrežju predstavi kot (lažna) bazna postaja. Ker mobilni telefon ne ve, da je ta bazna postaja lažna, se – če ima dober signal, in če uporabnik nima onemogočene samodejne izbire omrežja - poveže nanjo. Mogoči so tudi drugi napadi, s katerimi lažna bazna postaja mobilni telefon "prepriča", da se vedno poveže nanjo.

Problem: mobilno omrežje se ne avtenticira mobilnemu telefonu

- Ko je mobilni telefon povezan na lažno bazno postajo, mu le-ta lahko ukaže izklop šifriranja.
- Vendar pa GSM standard priporoča ("*should*") obveščanje uporabnika kadar komunikacija ni šifrirana (3GPP Rel.9 TS 33.102-920 "3G Security Architecture" 5.5.1 Visibility, ciphering indicator feature - 3GPP TS 22.101")



Problem: mobilno omrežje se ne avtenticira mobilnemu telefonu

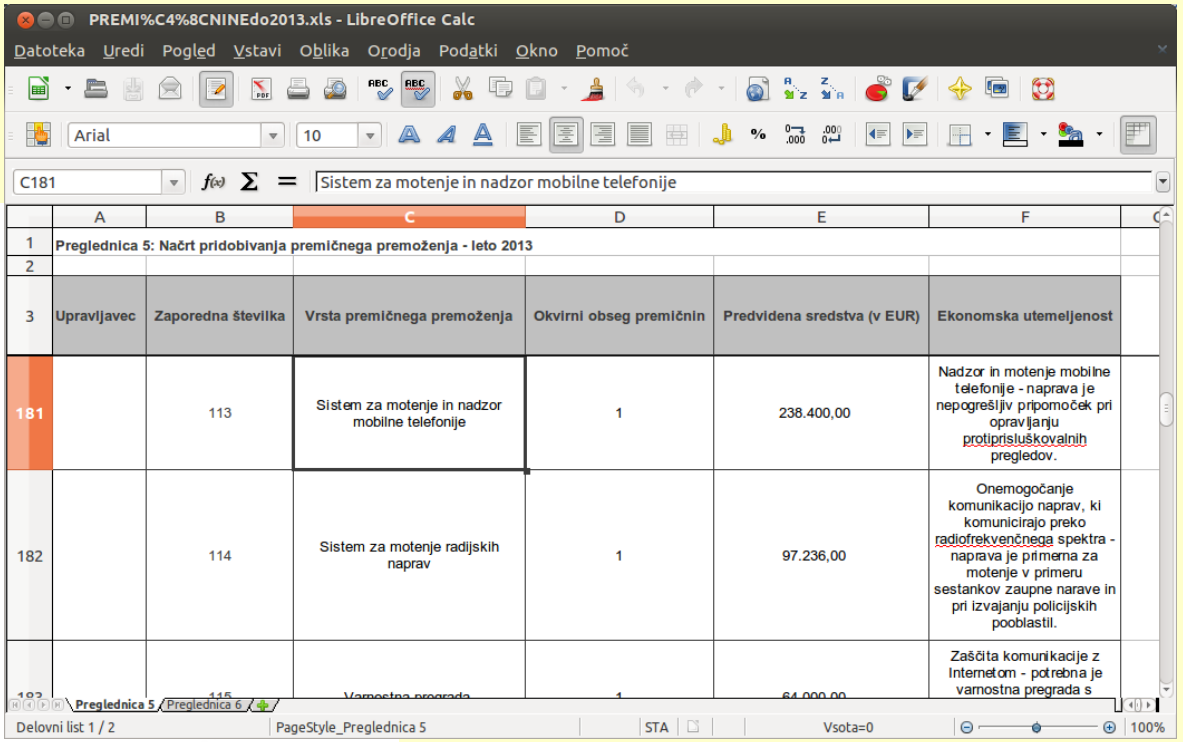
- Vendar pa se to obvestilo ne prikaže, če je tako nastavljeno na SIM kartici.

> The ciphering indicator feature may be disabled by the home network operator setting data in the SIM/USIM. If this feature is not disabled by the SIM, then whenever a connection is in place, which is, or becomes unenciphered, an indication shall be given to the user. Ciphering itself is unaffected by this feature, and the user can choose how to proceed;"
>
> ***3GPP TS 22.101 specification (R99 22.101-3.17.0), section 13, "Types of features of Ues"***

Problem: mobilno omrežje se ne avtenticira mobilnemu telefonu

Nekateri mobilni telefoni obvestilo izpišejo slabo vidno, nekateri pa ga sploh ne izpišejo.

IMSI Catcher lahko kupijo...



REPUBLIKA SLOVENIJA
MINISTRSTVO ZA NOTRANJE ZADEVE
Štefanova ulica 2, 1501 LJUBLJANA
Telefon: 01 428 40 00; telefaks: 01 428 47 33
E-pošta: gp.mnz@gov.si; http://www.mnz.gov.si

Številka: 029-34/2010/14 (2223-01)
Datum: 17 -06- 2010

MEDRESORSKA KOMISIJA
ZA IZDAJO SOGLASIJ ZA IZVEDBO
OBRAMBNIH IN ZAUPNIH NAROČIL

Ministrstvo za obrambo
Vojkova cesta 59
1000 Ljubljana

sekretar komisije

ZADEVA: **Vloga za soglasje k izvedbi naročila na podlagi Uredbe o obrambnih in zaupnih naročilih*[1]**

V skladu s 5. členom Uredbe o obrambnih in zaupnih naročilih (Uradni list RS, št. 80/07), ki določa, da mora naročnik za izvedbo naročila po navedeni uredbi predhodno pridobiti soglasje medresorske komisije, imenovane s strani Vlade Republike Slovenije, vas prosimo za soglasje k izvedbi sledečega zaupnega naročila:

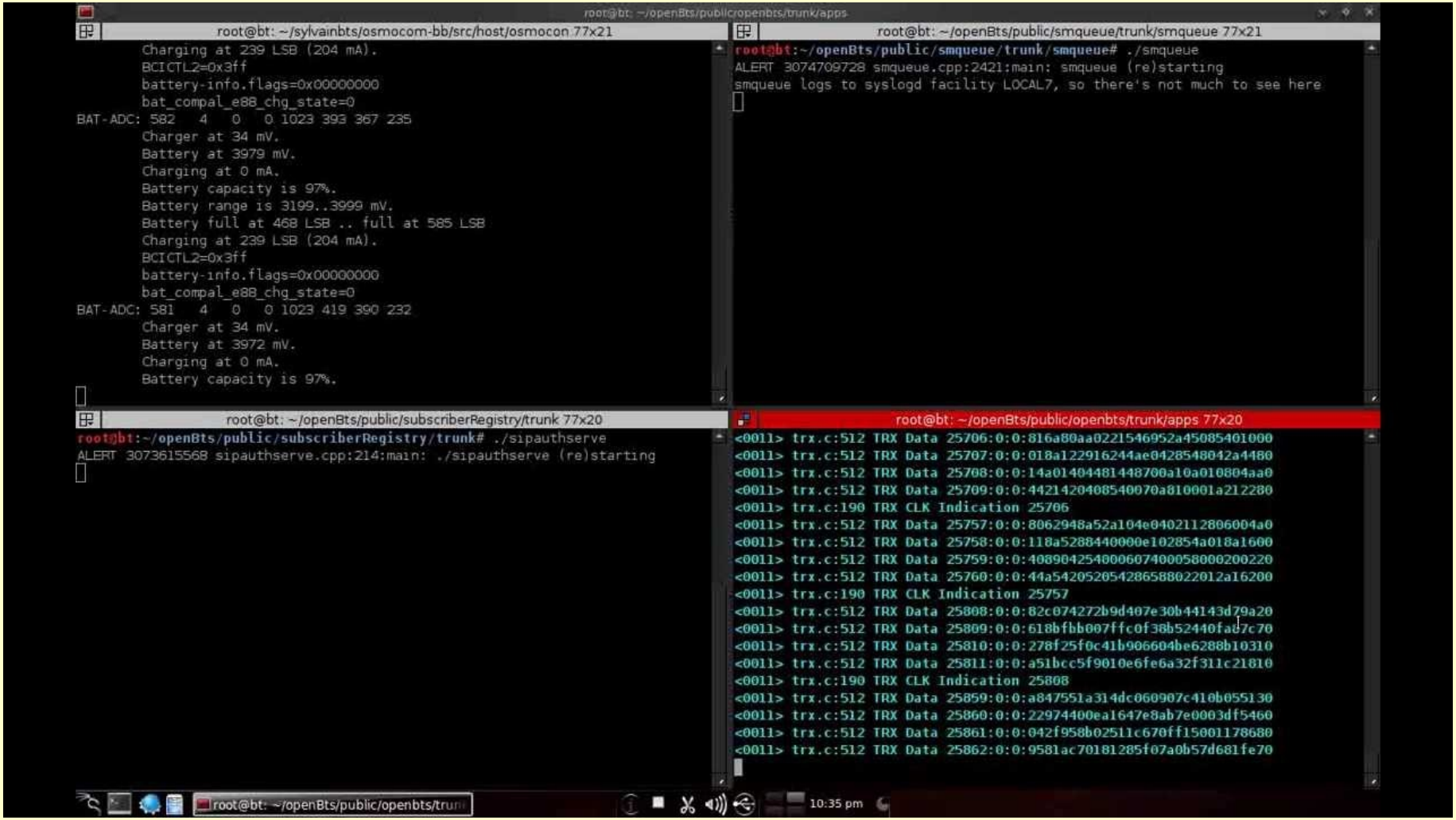
1. *Naziv ter naslov naročnika, ki bo izvedel naročilo po Uredbi o obrambnih in zaupnih naročilih:*

Ministrstvo za notranje zadeve, Policija, Štefanova 2, 1501 Ljubljana

2. *Predmet naročila:*

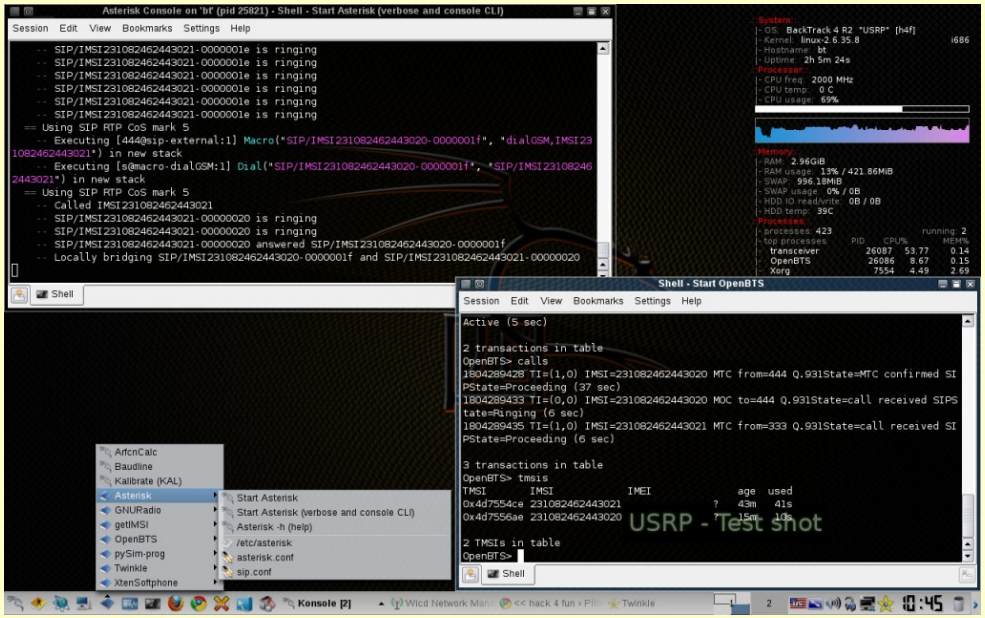
Nadgradnja sistema za [redacted]

...ali pa si ga izdelamo sami



Further hacks on the Calypso platform or How to turn a phone into a BTS, Sylvain Munaut, 29C3, 29. december 2012, <http://events.ccc.de/congress/2012/Fahrplan/events/5226.en.html>.

...ali pa si ga izdelamo sami



Vir in avtorstvo: prof. dr. ing. Andreas Steil, <http://www.fh-kl.de/~andreas.steil/Projekte/OpenBTS/>

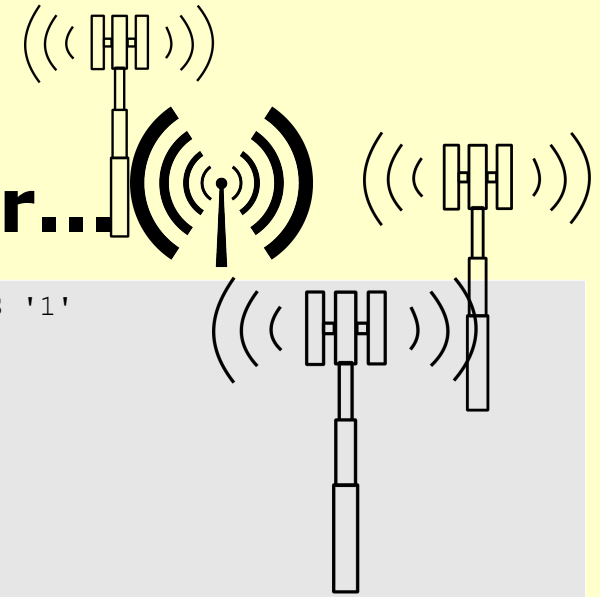
Ter:

BackTrack R2 USRP Test Shot, <http://www.serverfault.sk/2011/03/backtrack-r2-usrp-test-shot-rfx900/>.

...ali pa si ga izdelamo sami

Doug DePerry, Tom Ritter in Andrew Rahimi, Traffic Interception & Remote Mobile Phone Cloning with a Compromised CDMA Femtocell, BlackHat 2013, <https://www.defcon.org/images/defcon-21/dc-21-presentations/DePerry-Ritter/DEFCON-21-DePerry-Ritter-Femtocell-Updated.pdf>.

IMSI Catcher detektor...



matej@cryptopia: ~/catchercatcher/osmocom-bb/src/host/layer23/src/mobile

matej@cryptopia: ~/osmocom/osmoco... | matej@cryptopia: ~/catchercatcher/osr

```
    IMEI req:  0
    SilentSMS: 0

  status flag: GREEN

OsmocomBB# show catcher
Catcher status for MS '1'
  link establishment
    rach sent: 2
    paging:    0
    imm_ass:   1
    assign:    0
    handover:  0
    release:   1
    tune:      1
    failure:   0
    current:   0
    high pwr:  0.00
  cipher mode
    request:   1
    response:  1
    no cipher: 0
    no IMEISV: 0
    first alg: A5/1
    last alg:  A5/1
  cell monitoring
    camped:    0
    MCC:       293 (293, 0)
    MNC:       40 (40, 0)
    LAC:       [redacted]
    CID:       [redacted]
  data exchange
    IMSI req:  0
    IMEI req:  0
    SilentSMS: 0

  status flag: GREEN
```

```
Catcher status for MS '1'
  link establishment
    rach sent: 78
    paging:    1
    imm_ass:   0
    assign:    0
    handover:  0
    release:   0
    tune:      0
    failure:   0
    current:   1
    high pwr:  -
  cipher mode
    request:   0
    response:  0
    no cipher: 0
    no IMEISV: 0
    first alg: A5/0
    last alg:  A5/0
  cell monitoring
    camped:    0
    MCC:       293 (293, 0)
    MNC:       41 (41, 0)
    LAC:       11 (11, 0)
    CID:       10454 (103, 1)
  data exchange
    IMSI req:  0
    IMEI req:  0
    SilentSMS: 0

  status flag: RED
```

...pa obstaja samo za Osmocom telefone

(FemtoCatcher pa za Verizonove mobilnike).

Nekateri drugi napadi na mobilno telefonijo

- **Odklop mobilnega telefona iz omrežja:** napadalec, ki pozna IMSI in TMSI številko tarče, le-to lahko odklopi iz omrežja s pomočjo [redacted].

- **Prenehanje delovanja (izklop) omrežja**: če napadalec v manj kot [redacted] pošlje več [redacted] paketkov kot ima bazna postaja [redacted], omrežje preneha delovati. Gre za tim. [redacted] poplavljanje, posledica pa je prenehanje delovanja omrežja (tim. Denial Of Service napad).

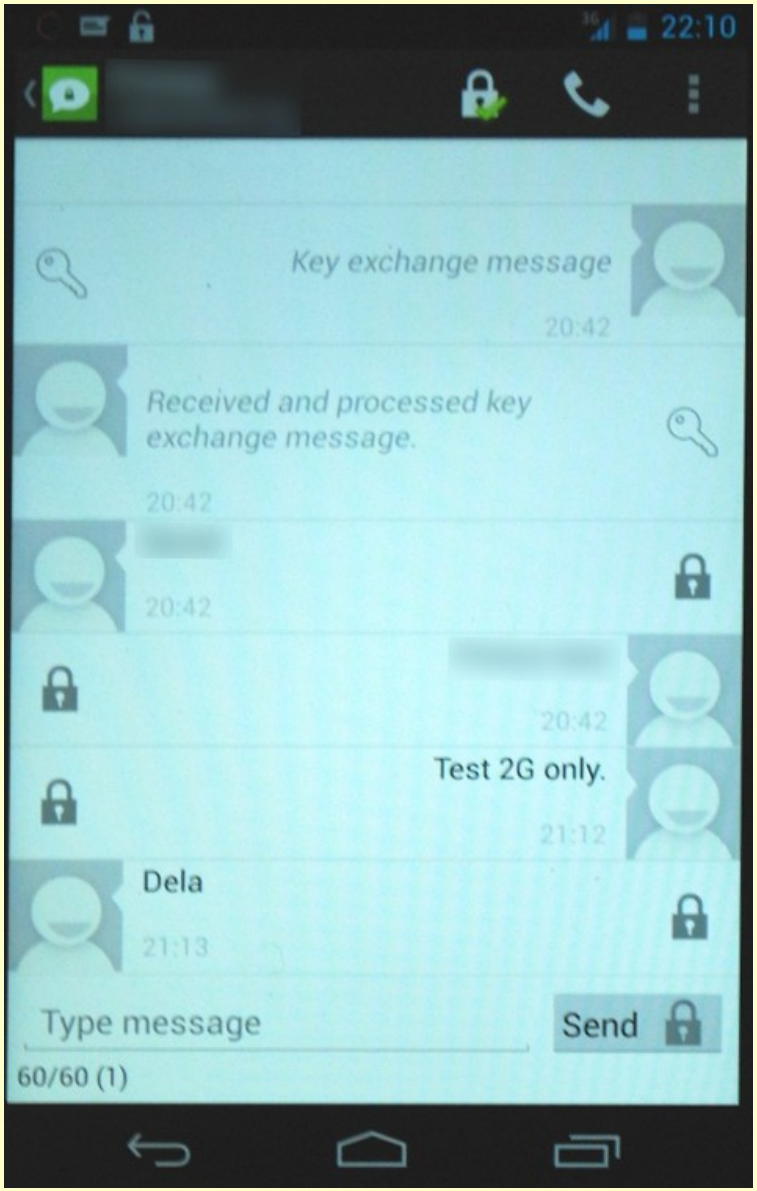
Rešitve?

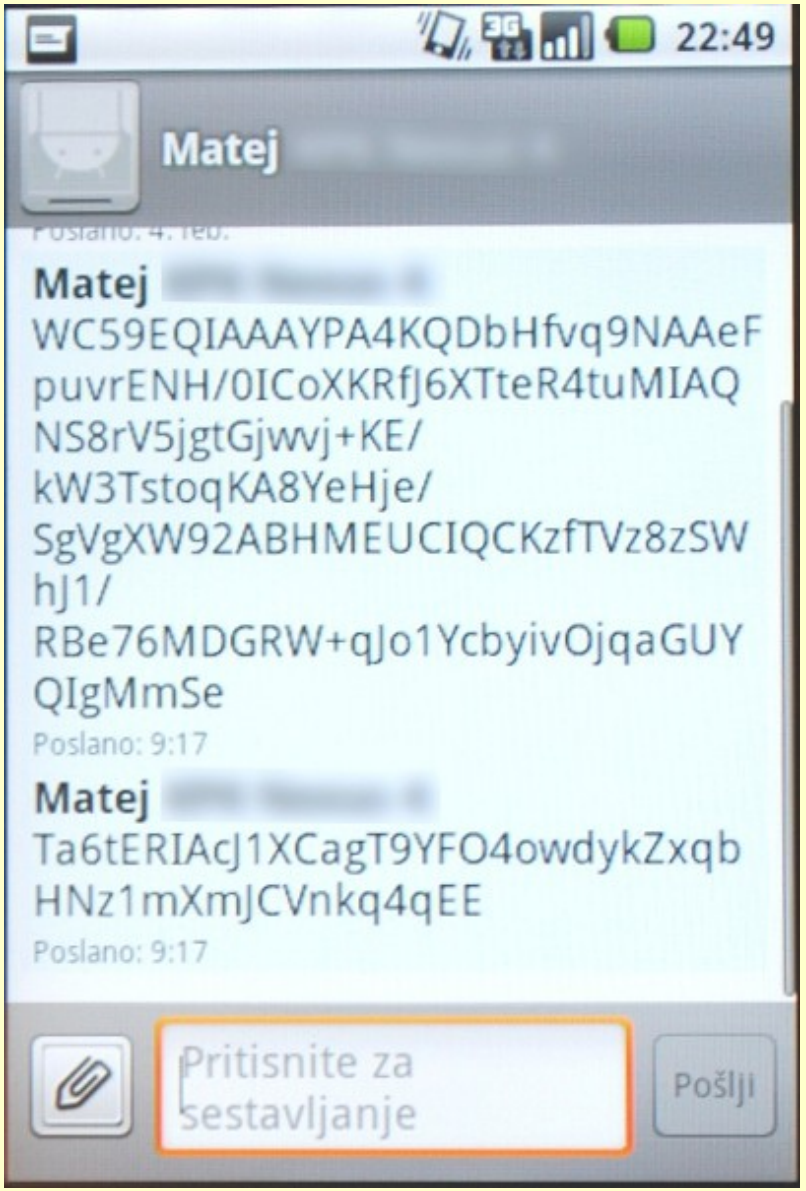
Šifrirane digitalne komunikacije

- Šifrirane digitalne komunikacije so že realnost!

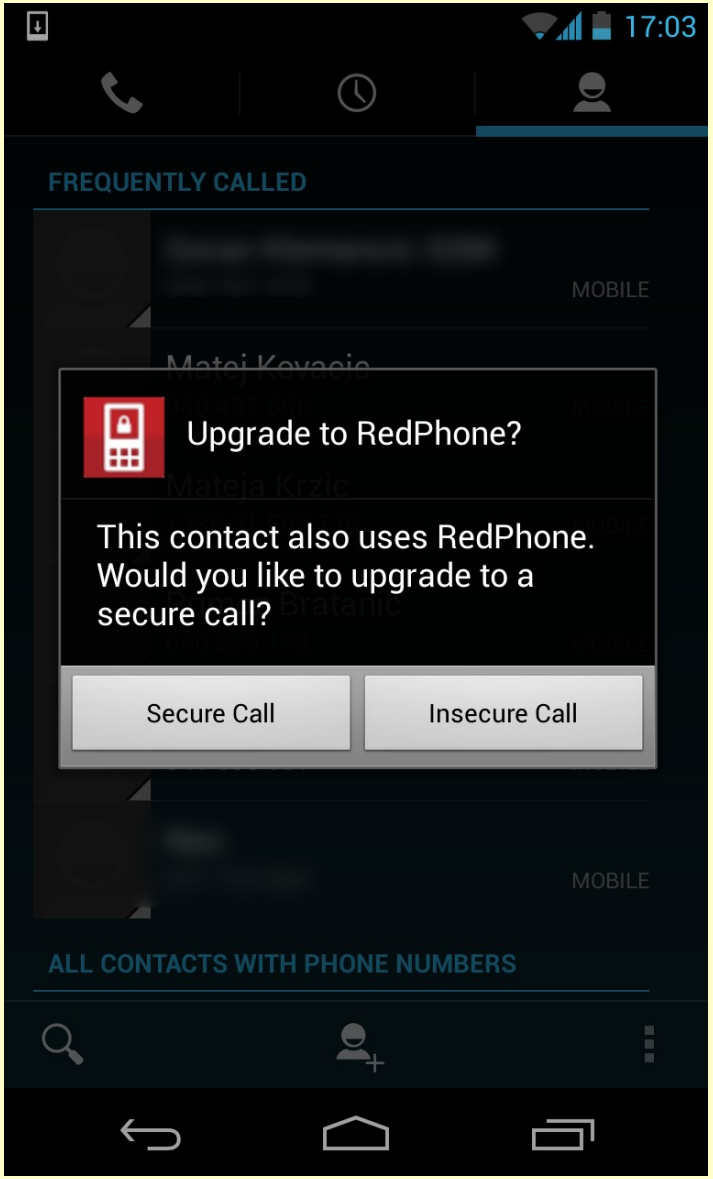
- Tehnologije so **prosto dostopne**.
- Omogočajo šifriranje vsebine komunikacij **od začetne do končne točke** (tim. *end-to-end*).
  - Posledica: prisluškovanje, tudi tim. zakonito **ni več mogoče.**
- Omogočajo praktično **nezlomljivo zaščito** (uporaba najsodobnejših šifrirnih mehanizmov) ob enostavni uporabi.
- Trend: skrivanje oz. **onemogočenje beleženja prometnih podatkov.**

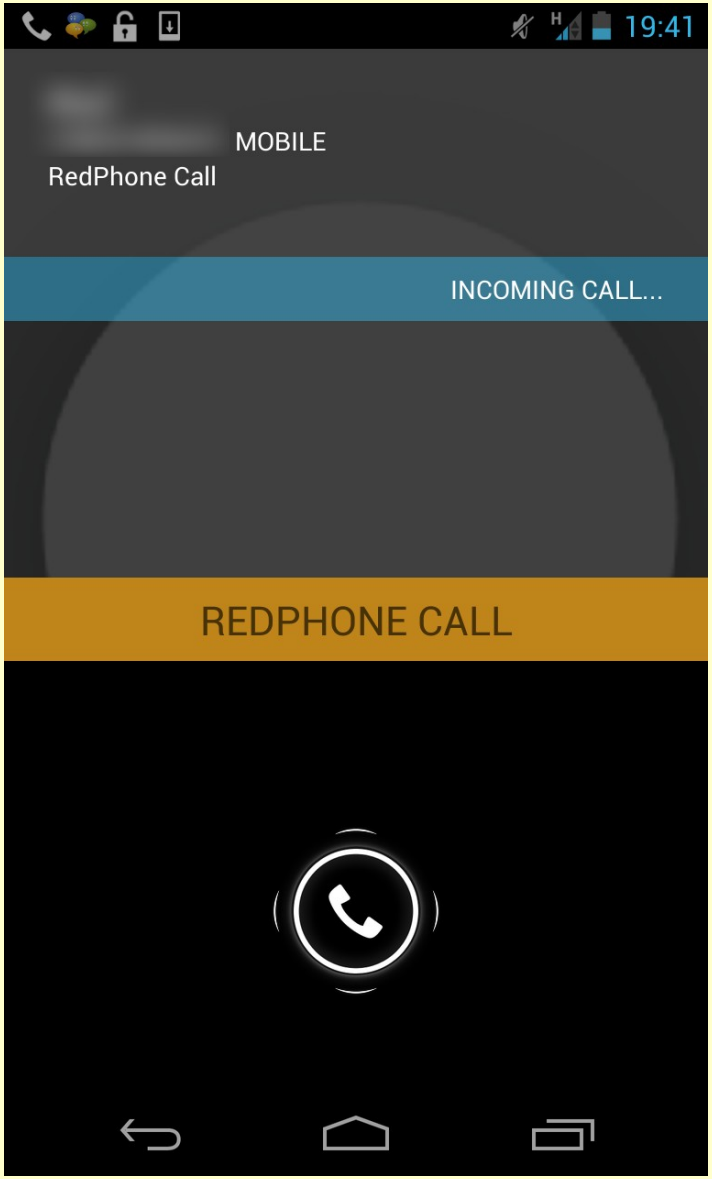
Šifrirana SMS sporočila: TextSecure



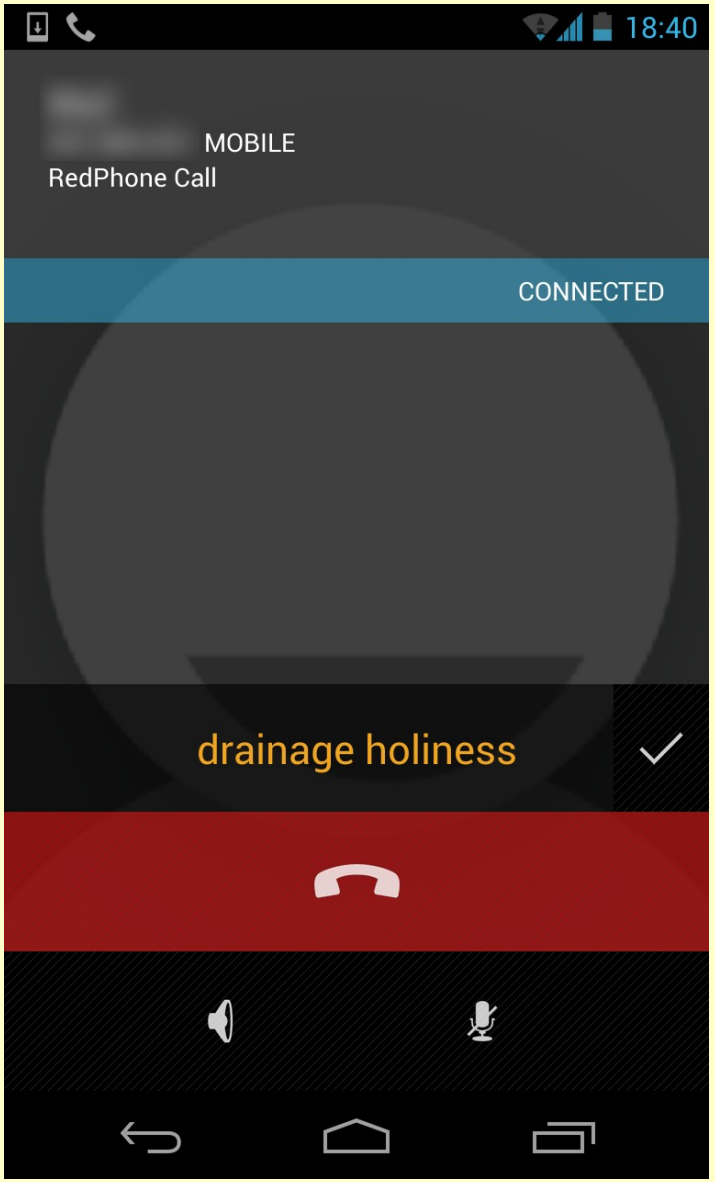


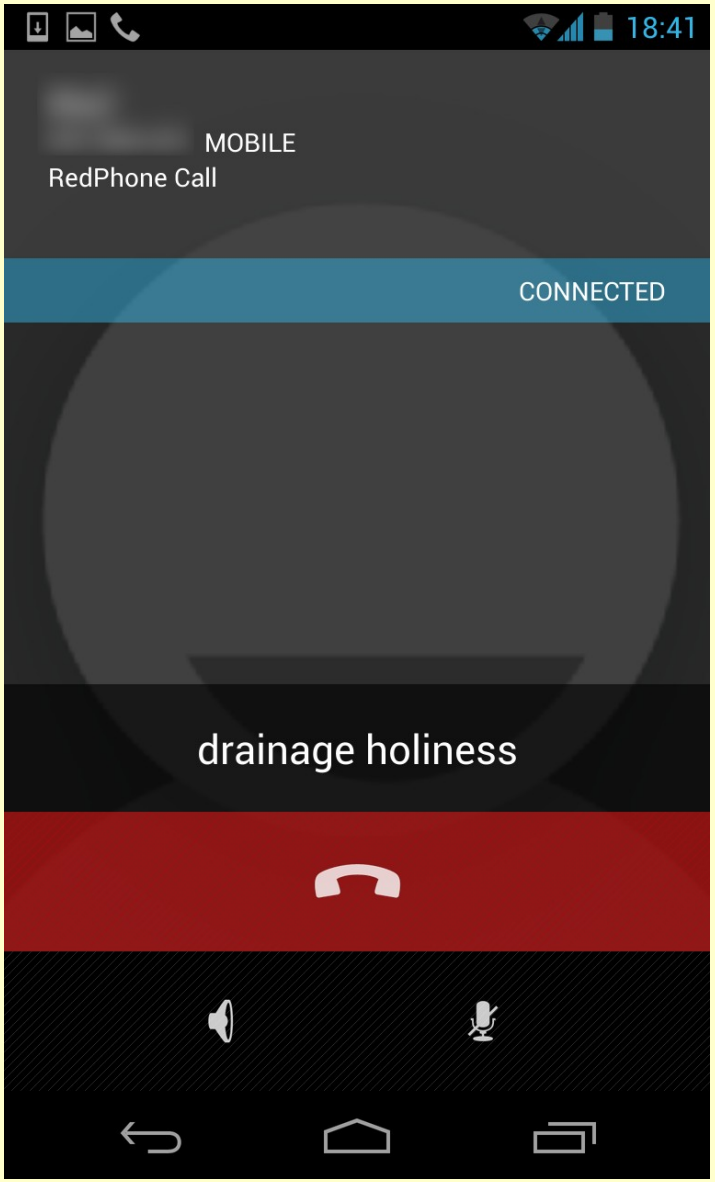
Šifrirani telefonski pogovori: RedPhone



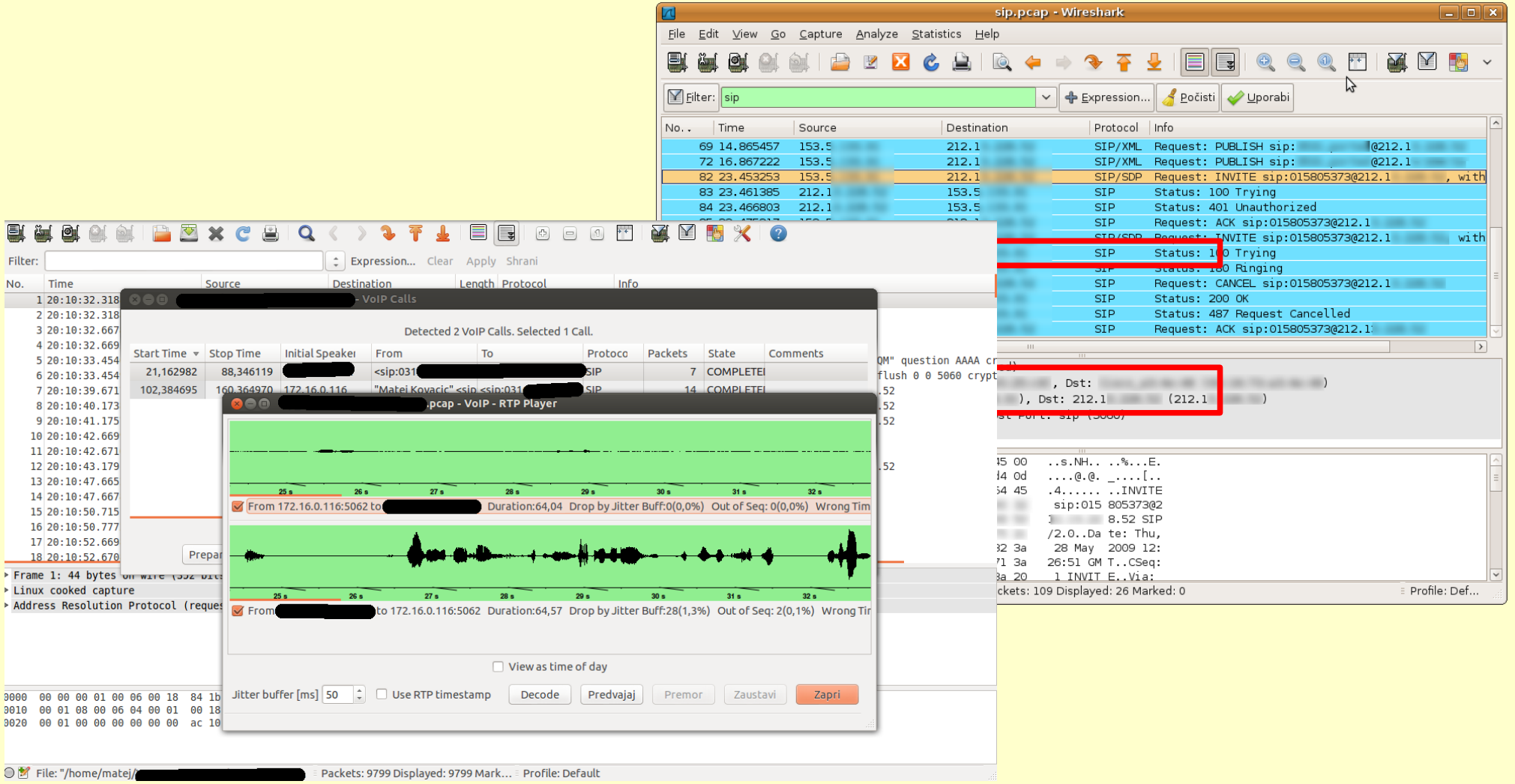


Šifrirani telefonski pogovori: RedPhone



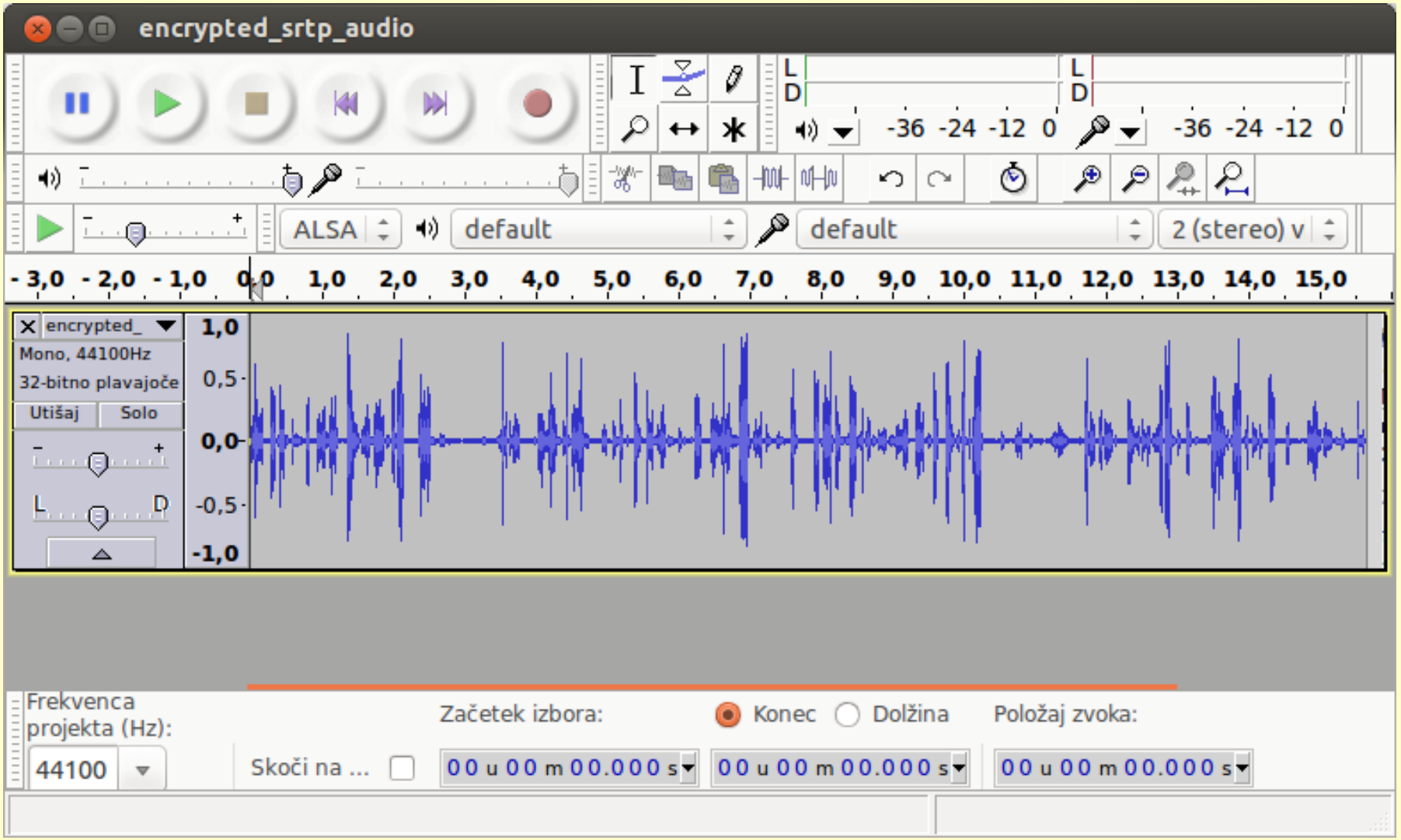


Kako je slišati nešifriran telefonski pogovor (IP telefonija)?



[Demo]

Kako je slišati šifriran telefonski pogovor?

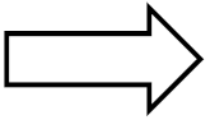


[Demo]

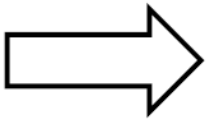
Prometni podatki RedPhone klicev

Analiza prometnih podatkov

datum in čas	Količina	Zarač. kol.	Destinacija	Storitev
1.6.2013 1:12	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 1:12	586 kB	590 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 3:12	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 3:12	629 kB	630 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 5:12	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 5:12	622 kB	630 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 7:12	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 7:13	492 kB	500 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 9:13	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 9:13	736 kB	740 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 11:13	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 11:13	16.276 kB	16.280 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 13:13	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 13:13	814 kB	820 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 15:13	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 15:14	845 kB	850 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 17:14	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 17:14	355 kB	360 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 18:24	11 kB	20 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 18:27	15 kB	20 kB	INTERNET	GPRS/UMTS prenos
1.6.2013 23:21	835 kB	840 kB	INTERNET	GPRS/UMTS prenos
2.6.2013 1:21	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
2.6.2013 1:22	786 kB	790 kB	INTERNET	GPRS/UMTS prenos
2.6.2013 3:22	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
2.6.2013 3:22	764 kB	770 kB	INTERNET	GPRS/UMTS prenos
2.6.2013 5:22	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
2.6.2013 5:23	834 kB	840 kB	INTERNET	GPRS/UMTS prenos
2.6.2013 7:23	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
2.6.2013 7:23	843 kB	850 kB	INTERNET	GPRS/UMTS prenos
2.6.2013 9:23	0 kB	0 kB	INTERNET	GPRS/UMTS prenos
2.6.2013 9:23	674 kB	680 kB	INTERNET	GPRS/UMTS prenos
2.6.2013 11:23	8 kB	10 kB	INTERNET	GPRS/UMTS prenos
2.6.2013 11:59	1 sms	1 sms	Slovenija4	SMS oddaja
2.6.2013 11:59	1 sms	1 sms	Slovenija4	SMS oddaja
2.6.2013 12:56	1 sms	1 sms	Slovenija5	SMS oddaja



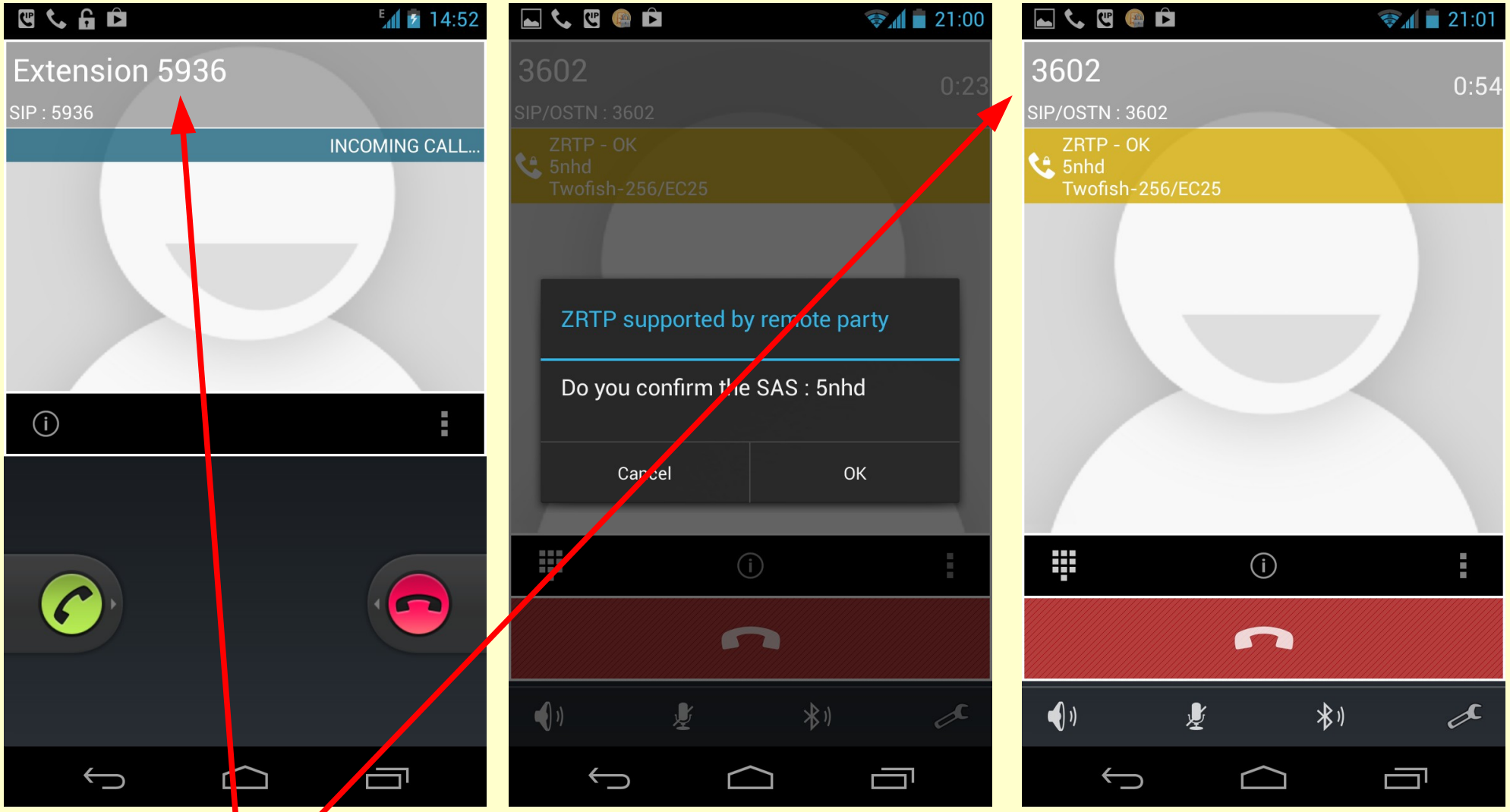
tip klica	klicana oseba	datum in čas	trajanje
RP klic	Nemčija	Jun 1, 2013 12:52:36 PM	37
RP klic	Nemčija	Jun 1, 2013 12:53:28 PM	23
RP klic	Nemčija	Jun 1, 2013 12:54:40 PM	22
RP klic	Nemčija	Jun 1, 2013 12:59:26 PM	17



tip klica	klicana oseba	datum in čas	trajanje
RP klic	Nemčija	Jun 1, 2013 5:59:51 PM	10
RP klic	Nemčija	Jun 1, 2013 6:21:14 PM	70

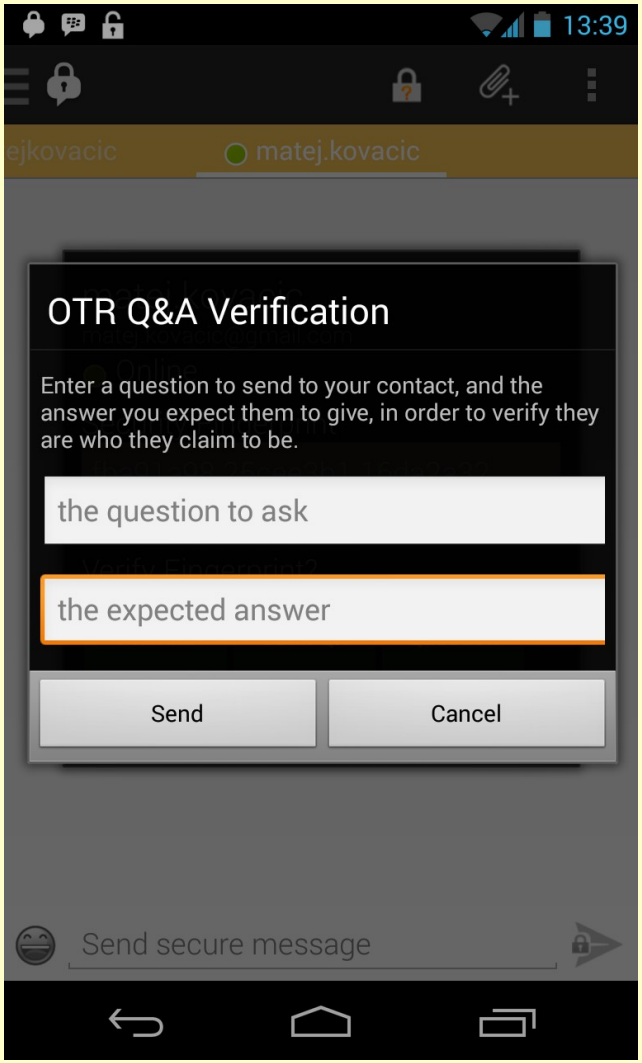
tip klica	klicana oseba	datum in čas	trajanje
RP klic	Slovenija3	Jun 2, 2013 10:47:14 AM	11
RP klic	Slovenija3	Jun 2, 2013 10:47:52 AM	64
RP klic	Slovenija3	Jun 2, 2013 10:49:03 AM	102
RP klic	Slovenija3	Jun 2, 2013 10:50:52 AM	70
RP klic	Slovenija4	Jun 2, 2013 11:59:36 AM	2
RP SMS	Slovenija4	Jun 2, 2013 12:38:11 PM	2
RP SMS	Slovenija5	Jun 2, 2013 12:56:06 PM	1

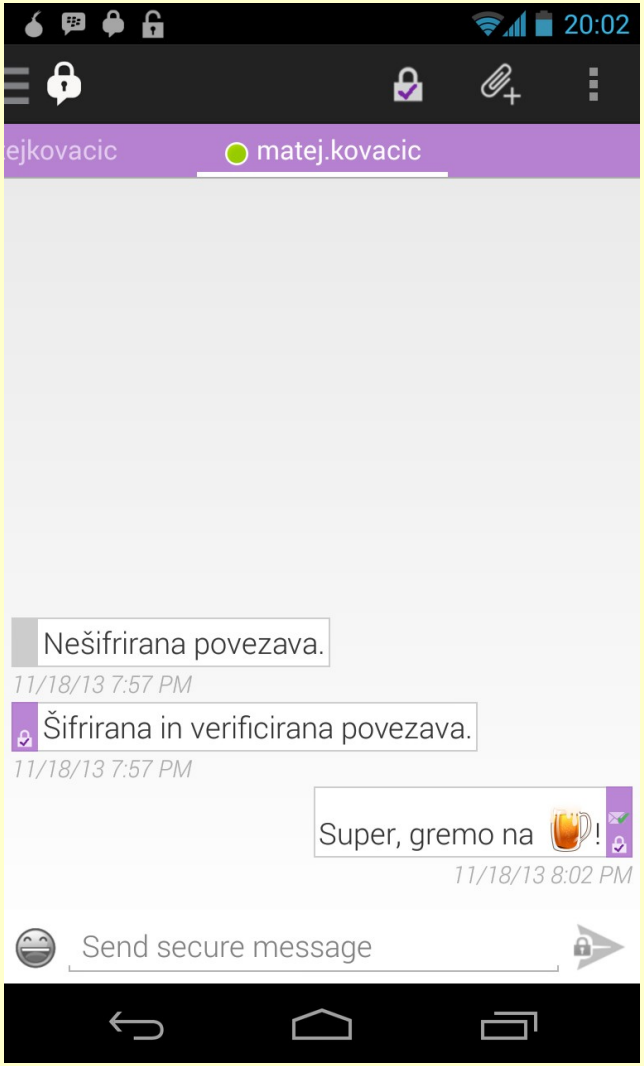
Šifrirana IP telefonija: CSipSimple

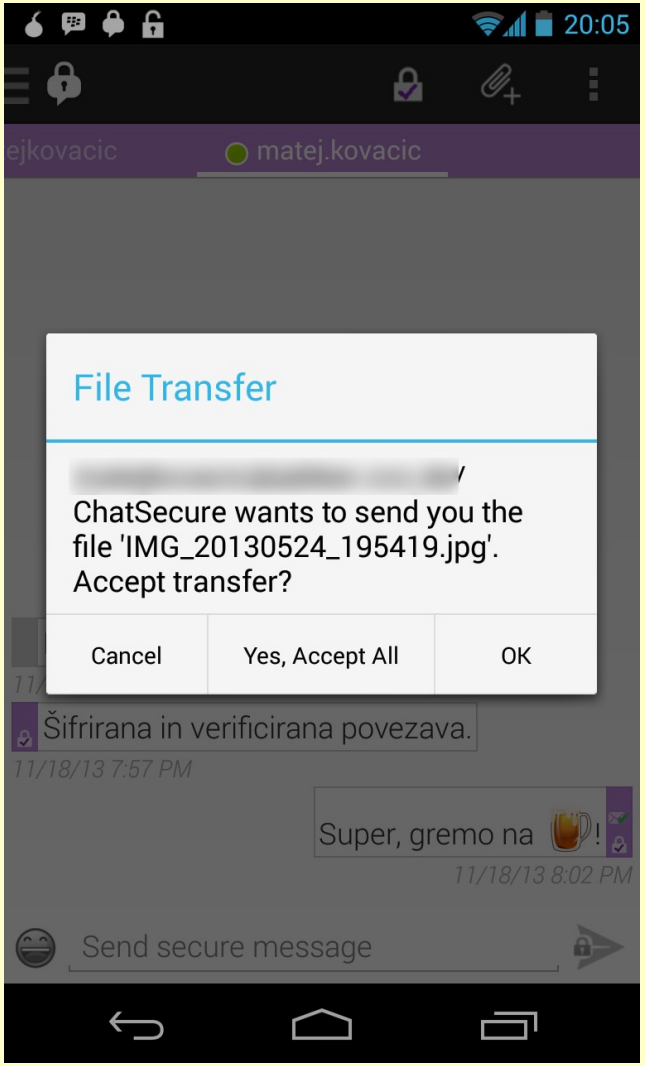


Prometni podatki?

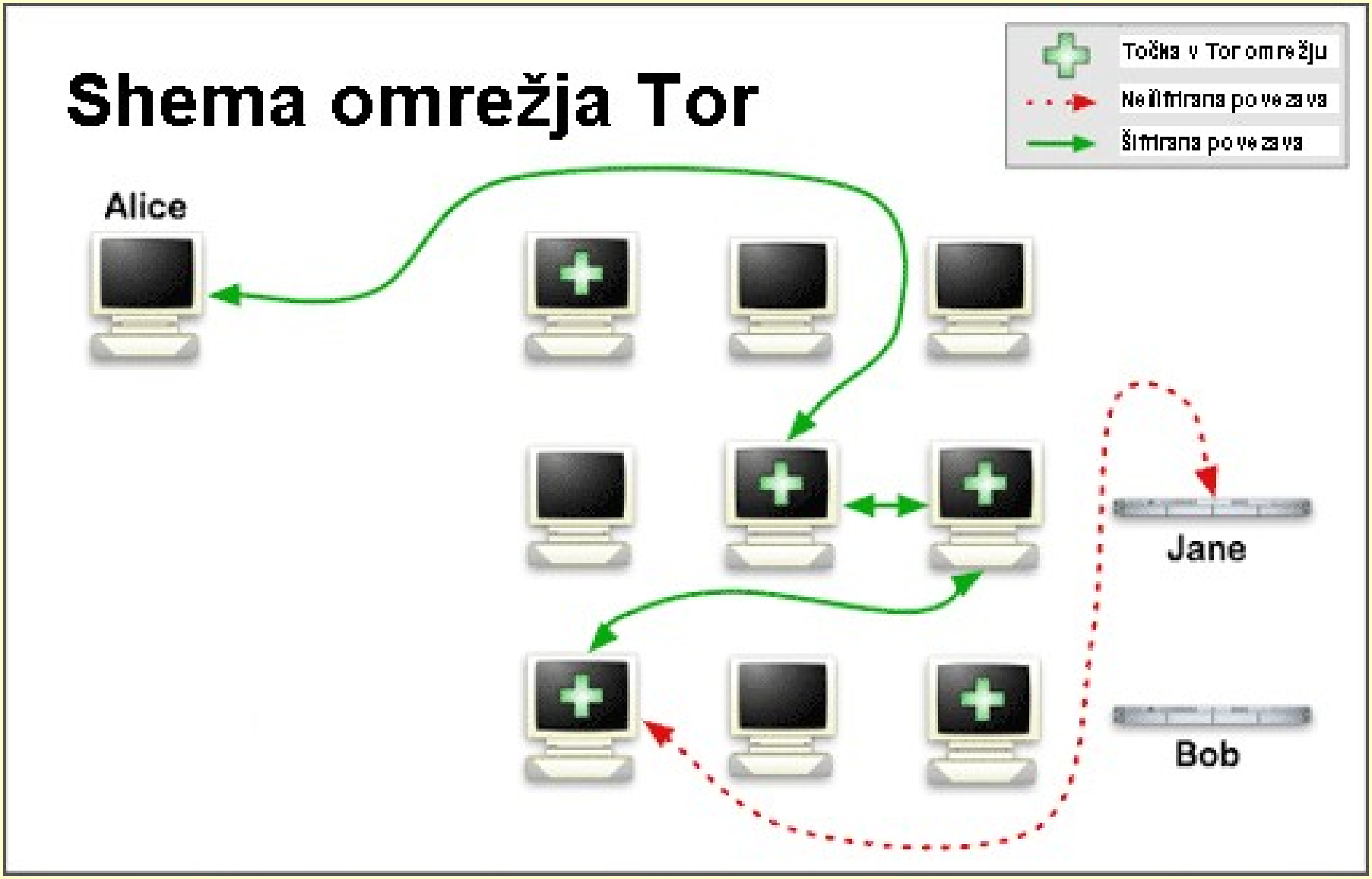
Šifrirana hipna sporočila: ChatSecure



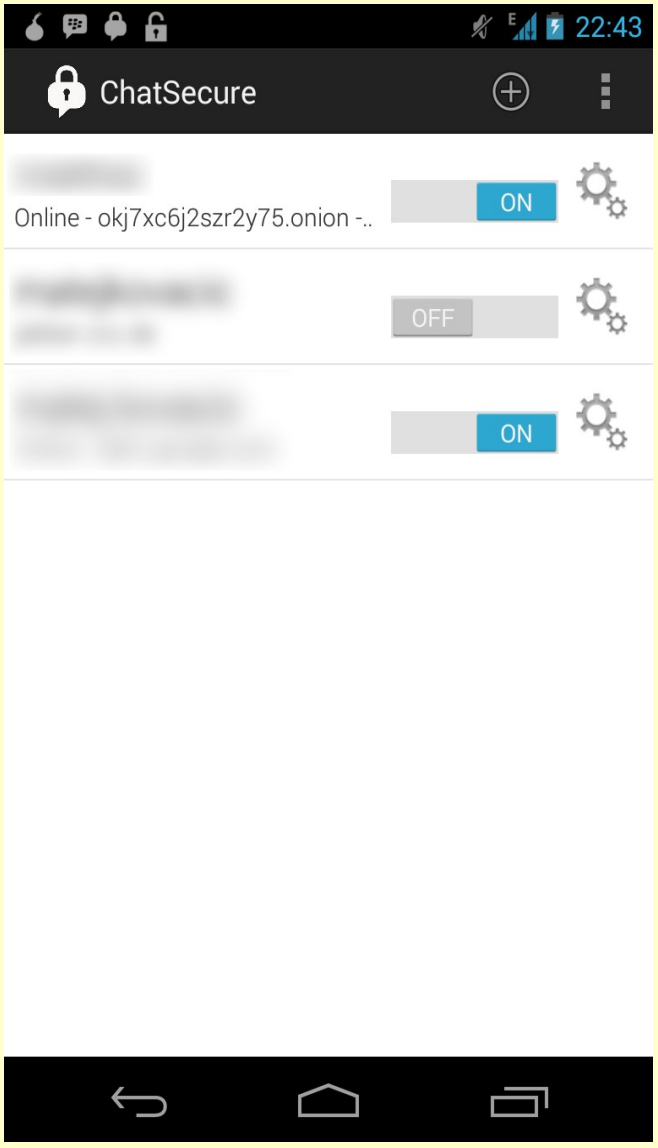




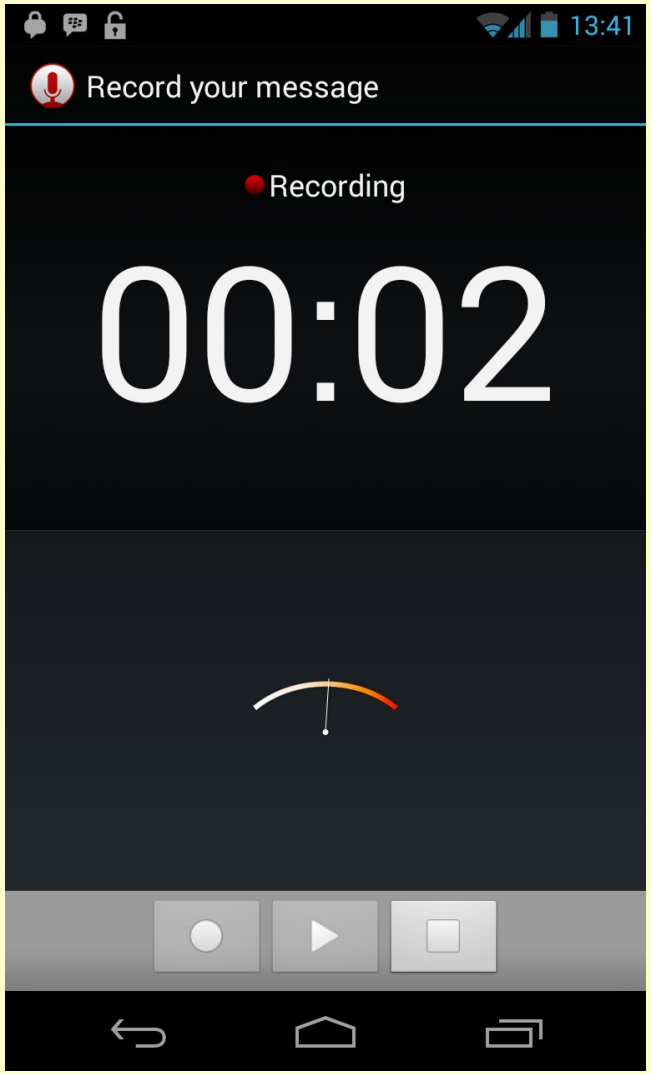
Anonimizacija...

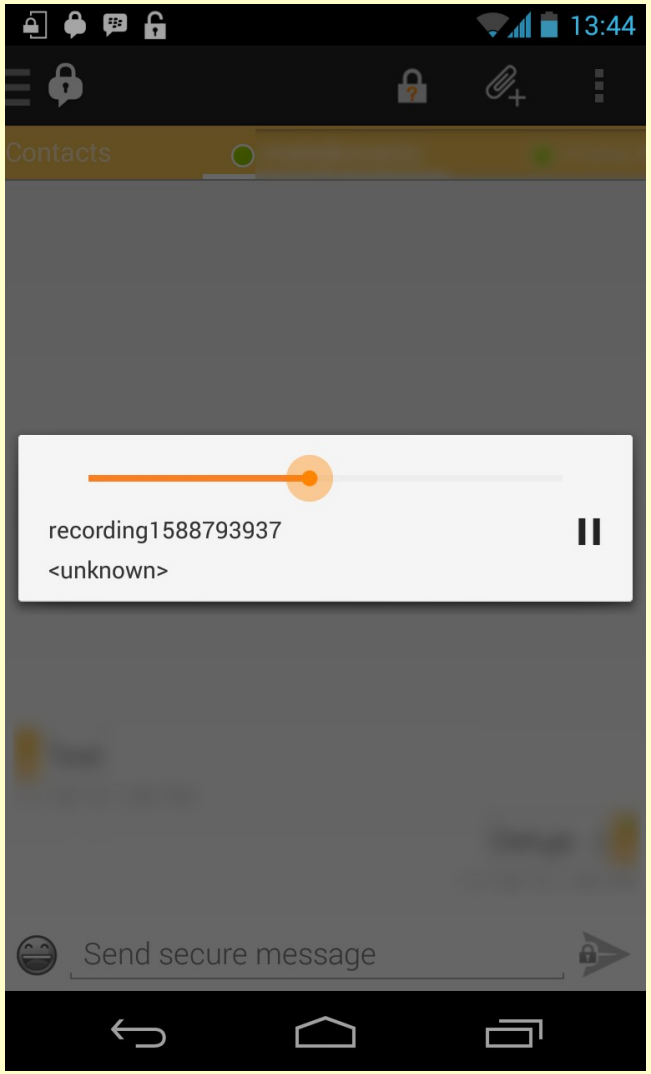


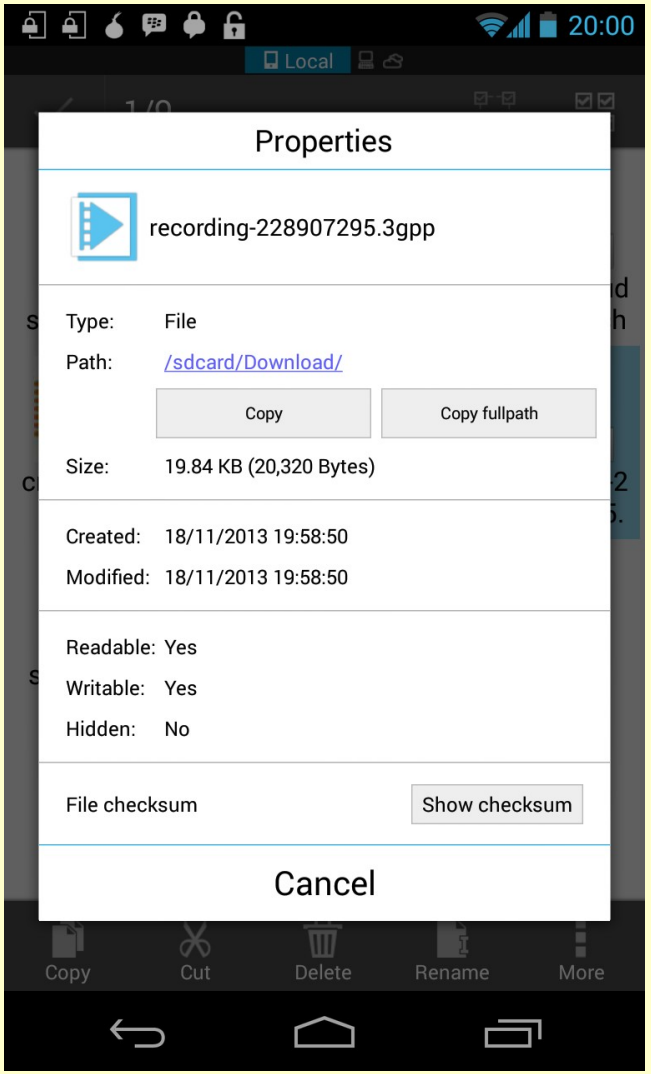
...zvočnih komunikacij na mobilnih telefonih



Zvočne komunikacije na mobilnih telefonih preko Tor omrežja







Pogled v (bližnjo) prihodnost...

- Trg pametnih telefonov se povečuje.
- Mobilna omrežja postajajo čedalje bolj zmogljiva.
- Mobilne naprave so čedalje bolj cenovno dostopne.
- VSE komunikacije se selijo na internet.
- Odprtokodne aplikacije za šifriranje komunikacij so brezplačne, interoperabilne in tečejo na različnih operacijskih sistemih.

- Bruce Schneier, Take Back the Internet:
  - "*To the engineers, I say this: we built the Internet, and some of us have helped to subvert it. Now, those of us who love liberty have to fix it.*"

Kaj razvoj tehnologije pomeni za preiskovanje kaznivih dejanj in kazensko pravo?

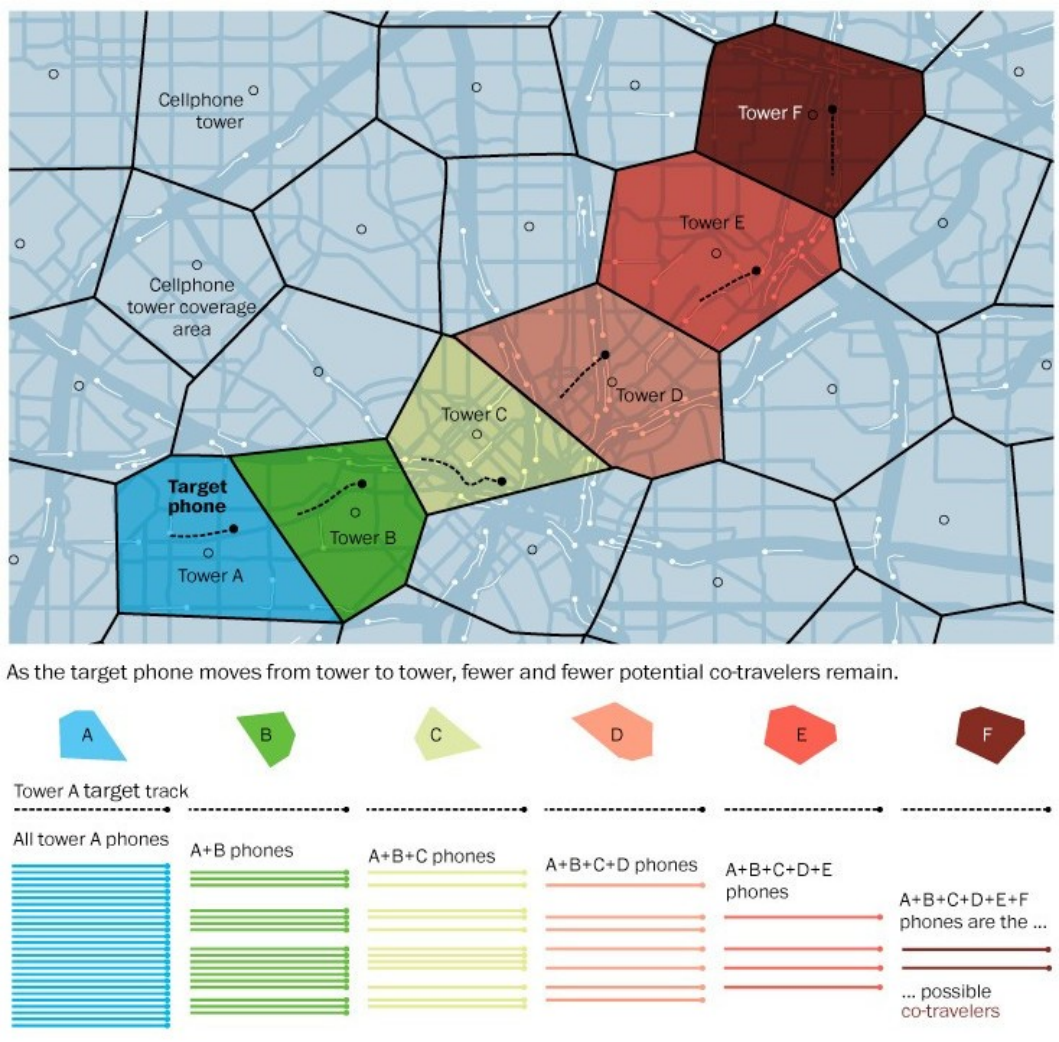
Smo sedaj varni...?

Lokacijska zasebnost

- *“Cell phones are 'Stalin's dream.'*
  Cell phones are tools of Big Brother. I'm not going to carry a tracking device that records where I go all the time, and I'm not going to carry a surveillance device that can be turned on to eavesdrop.”

--Richard Stallman

Lokacijska zasebnost



Vir in avtorstvo: Washington Post, NSA tracking cellphone locations worldwide, Snowden documents show, 4. december 2013, <http://apps.washingtonpost.com/g/page/national/how-the-nsa-is-tracking-people-right-now/634/>

Lokacijska zasebnost

- IMEI modifier
  [http://forum.xda-developers.com/showthread.php?t=1103766]
- MAC changer
  [http://www.openwiki.com/ow.asp?Changing+MAC+addresses+on+mobile+devices]
- IMSI... :-(

Koliko procesorjev ima vaš mobilni telefon?

- Poleg običajnega še procesor na SIM kartici ter na radijskem vmesniku...
- Napadi na radijski vmesnik mobilnega telefona (tim. *baseband processor*, ki je v telefonu **primarni** in na katerem teče *real-time OS*):
  - AT+S0=n: Hayes ukaz za vklop samodejnega odgovora, s katerim je mogoče vključiti mikrofon na mobilniku, izvesti pa ga je mogoče neopazno;
  - uničenje telefona,...
  - več: Ralf-Philipp Weinmann, University of Luxembourg: The Baseband Apocalypse.

BUSTED!

Vprašanja?

http://pravokator.si