Varnost komunikacij
1. del

Varnost GSM telefonije in zanesljivost prometnih podatkov

Matej Kovačič, Jaka Hudoklin, Primož Bratanič

(CC) 2012, 2013

Kiberpipa – predavanja na temo varnosti mobilne telefonije | Ljubljana, november 2013

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.

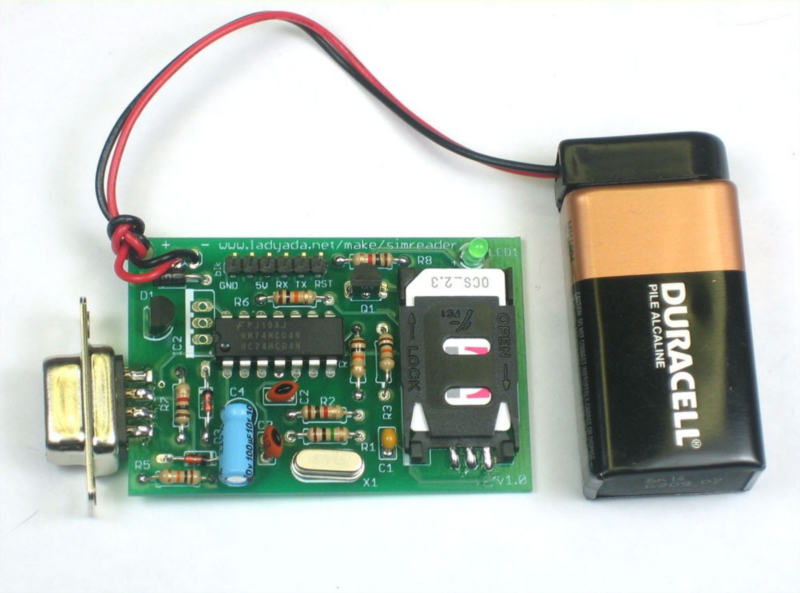
Namen raziskave je bil opozoriti na varnostne ranljivosti v slovenskih GSM omrežjih z željo, da se varnostne ranljivosti odpravijo, posledično pa se poveča stopnja varnosti in zasebnosti uporabnikov mobilne telefonije, ter z željo, da slovenski operaterji mobilne telefonije začnejo več vlagati v varnost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

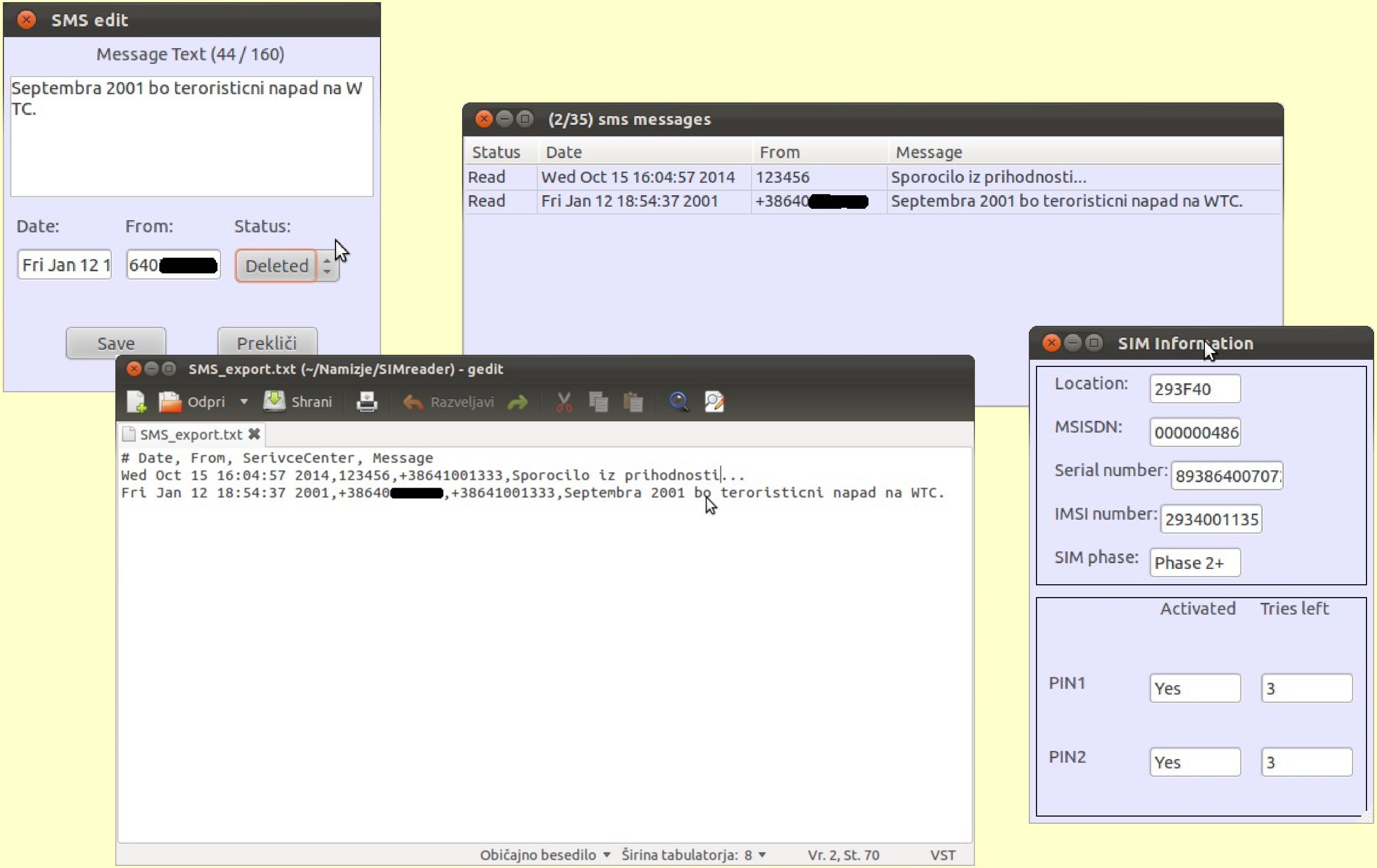
Podatki iz SIM kartice

1: čitalec SIM kartic



Podatki iz SIM kartice

2: spreminjanje vsebine in metapodatkov SMS sporočil na SIM kartici



Septembra 2001 bo teroristicni napad na W
TC.

Date:	From:	Status:
Fri Jan 12 1	640[redacted]	Deleted

Status	Date	From	Message
Read	Wed Oct 15 16:04:57 2014	123456	Sporocilo iz prihodnosti...
Read	Fri Jan 12 18:54:37 2001	+38640[redacted]	Septembra 2001 bo teroristicni napad na WTC.

```
# Date, From, SerivceCenter, Message
Wed Oct 15 16:04:57 2014,123456,+38641001333,Sporocilo iz prihodnosti...
Fri Jan 12 18:54:37 2001,+38640[redacted],+38641001333,Septembra 2001 bo teroristicni napad na WTC.
```

Location: 293F40

MSISDN: 000000486

Serial number: 89386400707

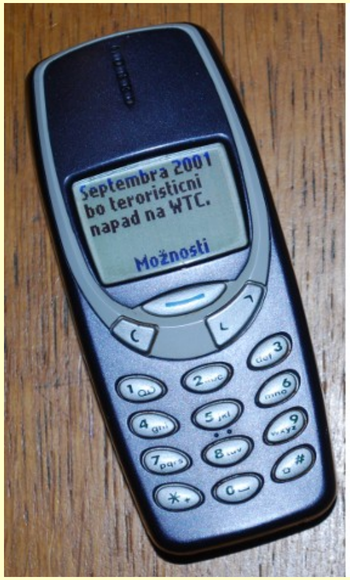
IMSI number: 2934001135

SIM phase: Phase 2+

	Activated	Tries left
PIN1	Yes	3
PIN2	Yes	3

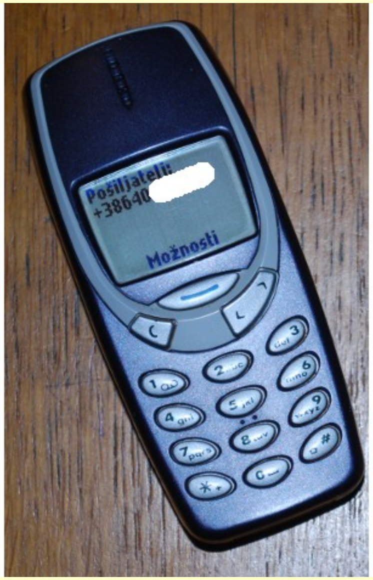
Podatki iz SIM kartice

3: rezultat



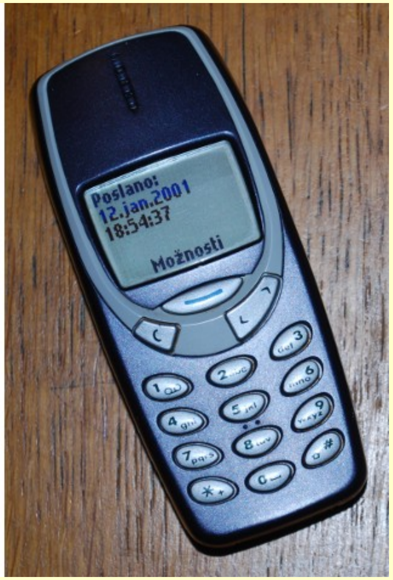
Septembra 2001
bo teroristicni
napad na WTC.

Možnosti



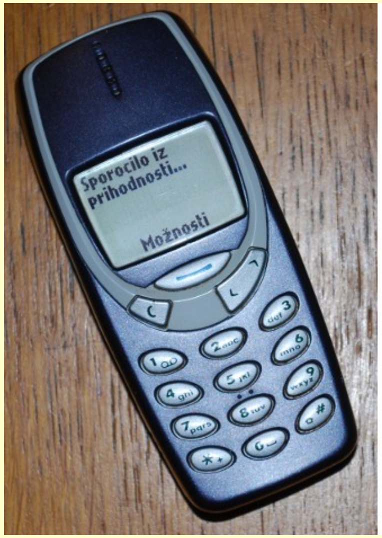
Pošiljatelj:
+38640[redacted]

Možnosti



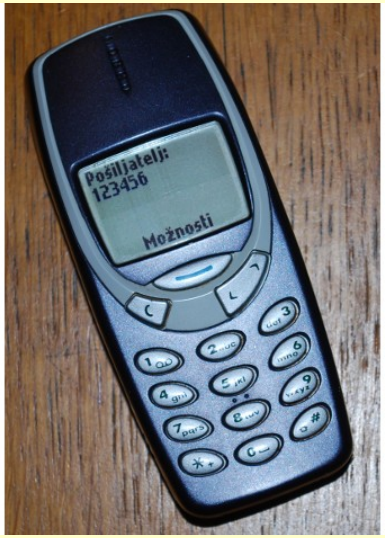
Poslano:
12.jan.2001
18:54:37

Možnosti



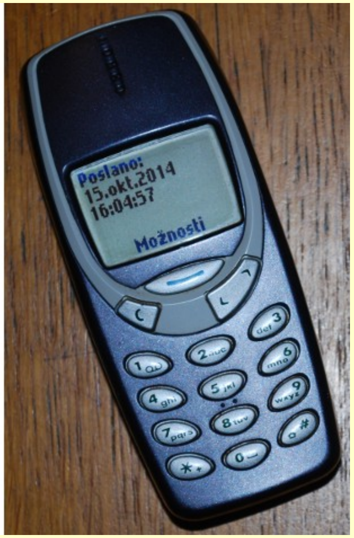
Sporocilo iz
prihodnosti...

Možnosti



Pošiljatelj:
123456

Možnosti



Poslano:
15.okt.2014
16:04:57

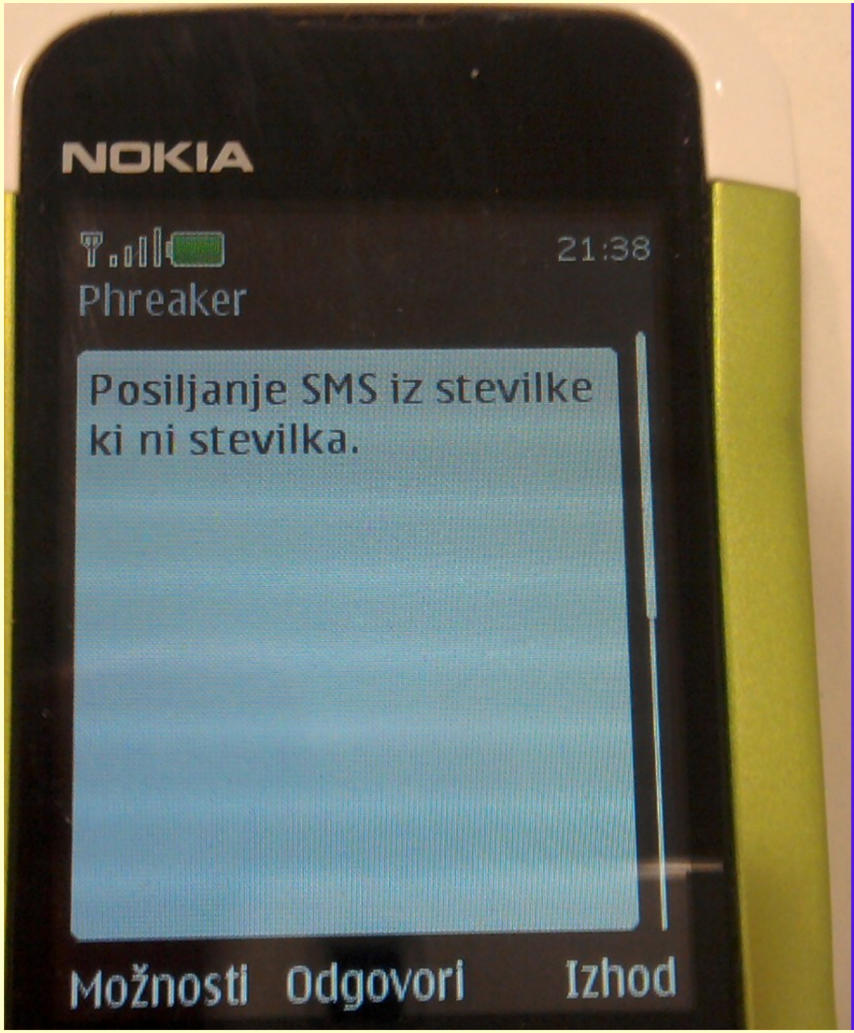
Možnosti

Pošiljanje SMS sporočil s spremenjeno klicno identifikacijo

Pošiljanje SMS sporočil “iz” poljubne številke

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

Pošiljanje SMS sporočil “iz” poljubne številke

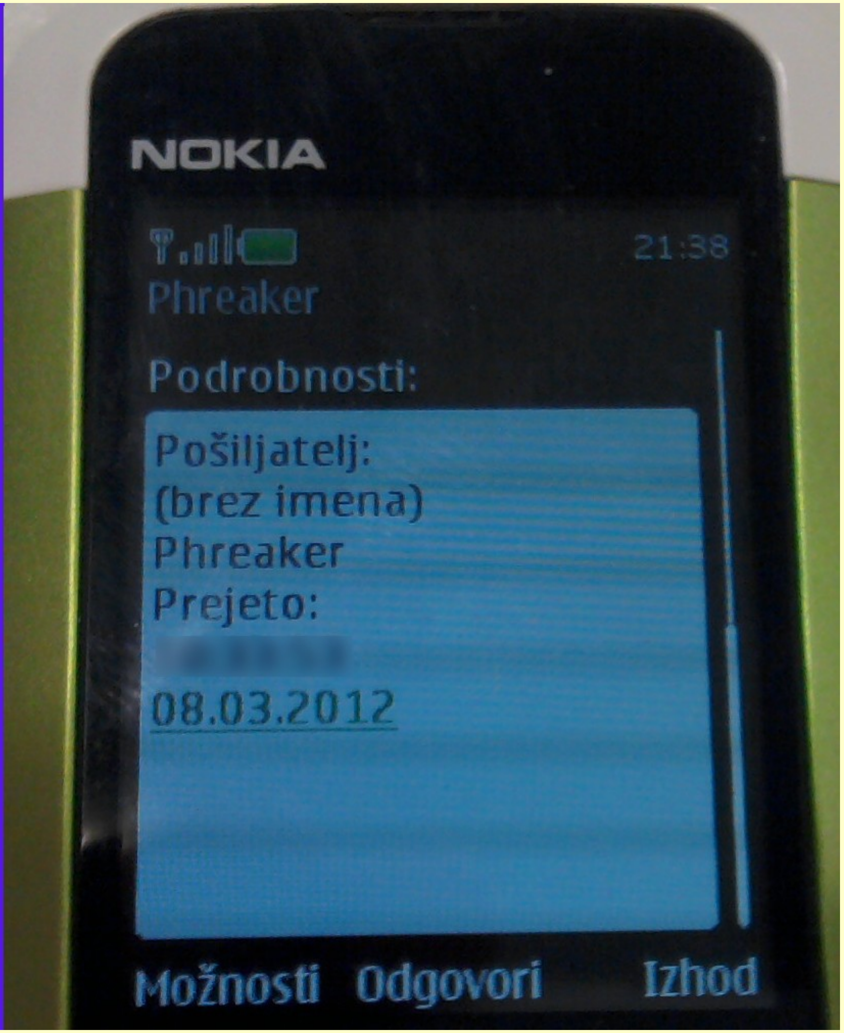


21:38

Phreaker

Posiljanje SMS iz stevilke ki ni stevilka.

Možnosti Odgovori Izhod



21:38

Phreaker

Podrobnosti:

Pošiljatelj:
(brez imena)
Phreaker
Prejeto:
[redacted]
08.03.2012

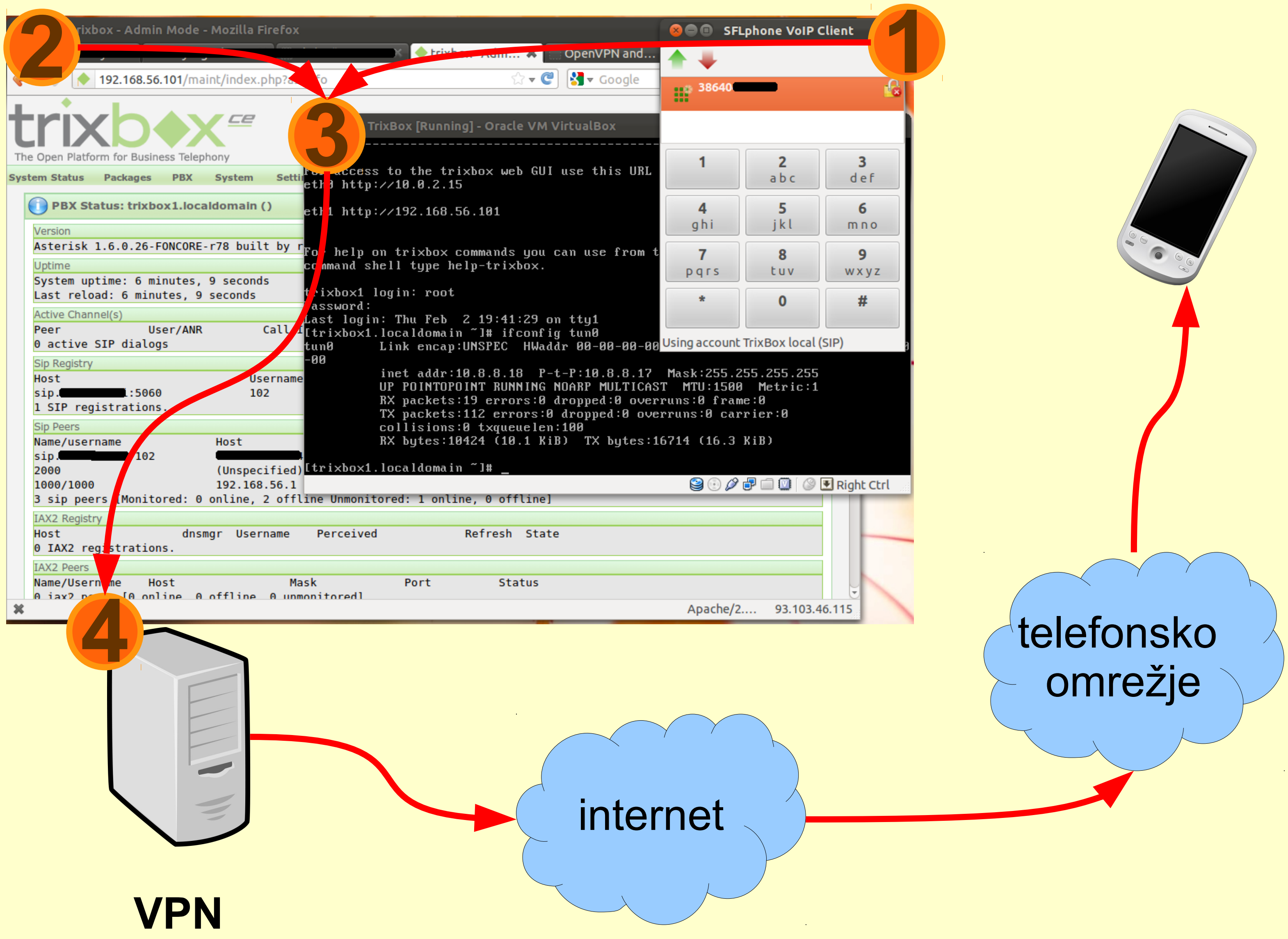
Možnosti Odgovori Izhod

Klicanje s poljubno klicno identifikacijo

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

Klicanje s poljubno klicno identifikacijo

1: vzpostavitev infrastrukture



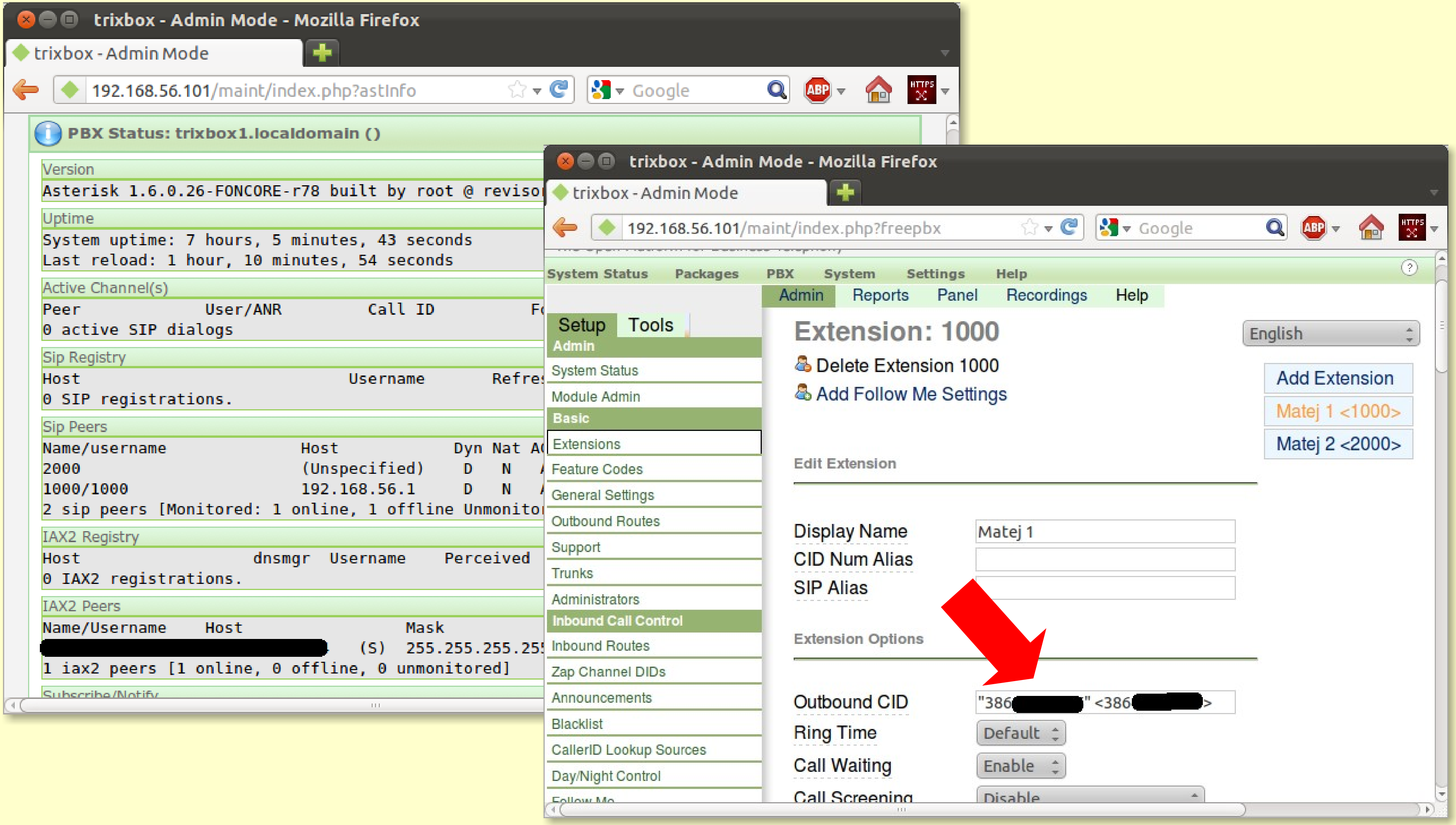
PBX Status: trixbox1.localdomain ()

```
Version
Asterisk 1.6.0.26-FONCORE-r78 built by r
Uptime
System uptime: 6 minutes, 9 seconds
Last reload: 6 minutes, 9 seconds
Active Channel(s)
Peer                User/ANR          Call I
0 active SIP dialogs
Sip Registry
Host                                  Username
sip.[redacted]:5060                   102
1 SIP registrations.
Sip Peers
Name/username              Host
sip.[redacted]102          [redacted]
2000                       (Unspecified)
1000/1000                  192.168.56.1
3 sip peers [Monitored: 0 online, 2 offline Unmonitored: 1 online, 0 offline]
IAX2 Registry
Host                dnsmgr  Username    Perceived            Refresh  State
0 IAX2 registrations.
IAX2 Peers
Name/Username    Host                Mask            Port          Status
0 iax2 p     [0 online  0 offline  0 unmonitored]
```

```
--------------------------------------------------
For access to the trixbox web GUI use this URL
eth0 http://10.0.2.15

eth1 http://192.168.56.101


For help on trixbox commands you can use from t
command shell type help-trixbox.

trixbox1 login: root
Password:
Last login: Thu Feb  2 19:41:29 on tty1
[trixbox1.localdomain ~]# ifconfig tun0
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00
-00
          inet addr:10.8.8.18  P-t-P:10.8.8.17  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:19 errors:0 dropped:0 overruns:0 frame:0
          TX packets:112 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:10424 (10.1 KiB)  TX bytes:16714 (16.3 KiB)

[trixbox1.localdomain ~]# _
```

Klicanje s poljubno klicno identifikacijo

2: pogled v virtualno telefonsko centralo



trixbox - Admin Mode - Mozilla Firefox
trixbox - Admin Mode
192.168.56.101/maint/index.php?astInfo
Google

PBX Status: trixbox1.localdomain ()

```
Version
Asterisk 1.6.0.26-FONCORE-r78 built by root @ reviso
Uptime
System uptime: 7 hours, 5 minutes, 43 seconds
Last reload: 1 hour, 10 minutes, 54 seconds
Active Channel(s)
Peer              User/ANR          Call ID          F
0 active SIP dialogs
Sip Registry
Host                            Username       Refre
0 SIP registrations.
Sip Peers
Name/username             Host             Dyn Nat A
2000                      (Unspecified)     D   N   
1000/1000                 192.168.56.1      D   N   
2 sip peers [Monitored: 1 online, 1 offline Unmonito
IAX2 Registry
Host              dnsmgr  Username     Perceived
0 IAX2 registrations.
IAX2 Peers
Name/Username     Host                  Mask
[redacted]                          (S)  255.255.255.25
1 iax2 peers [1 online, 0 offline, 0 unmonitored]
Subscribe/Notify
```

Extension: 1000

Delete Extension 1000

Add Follow Me Settings

Edit Extension

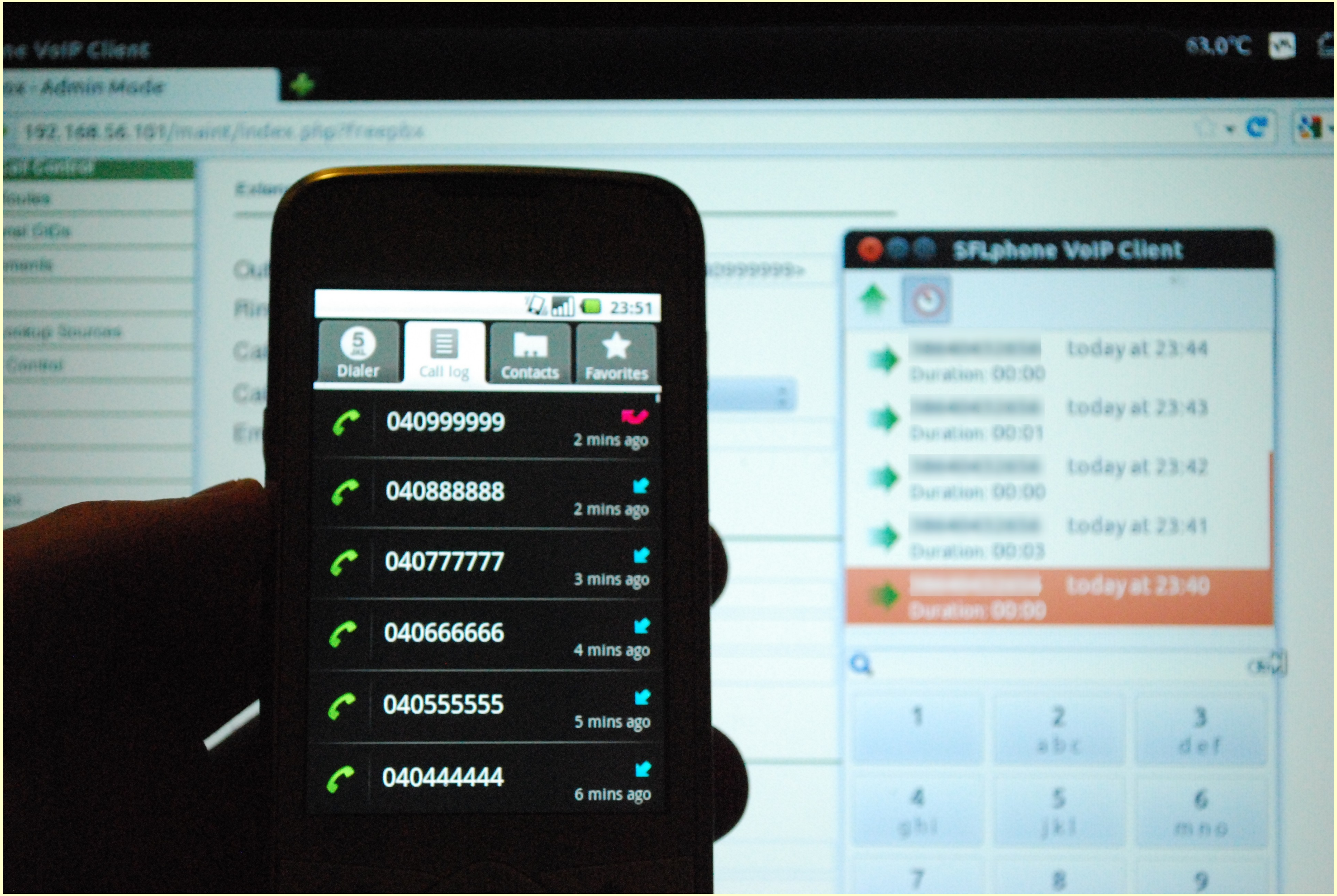
Display Name	Matej 1
CID Num Alias	
SIP Alias	

Extension Options

Outbound CID	"386[redacted]" <386[redacted]>
Ring Time	Default
Call Waiting	Enable
Call Screening	Disable

Klicanje s poljubno klicno identifikacijo

3: rezultat na telefonu

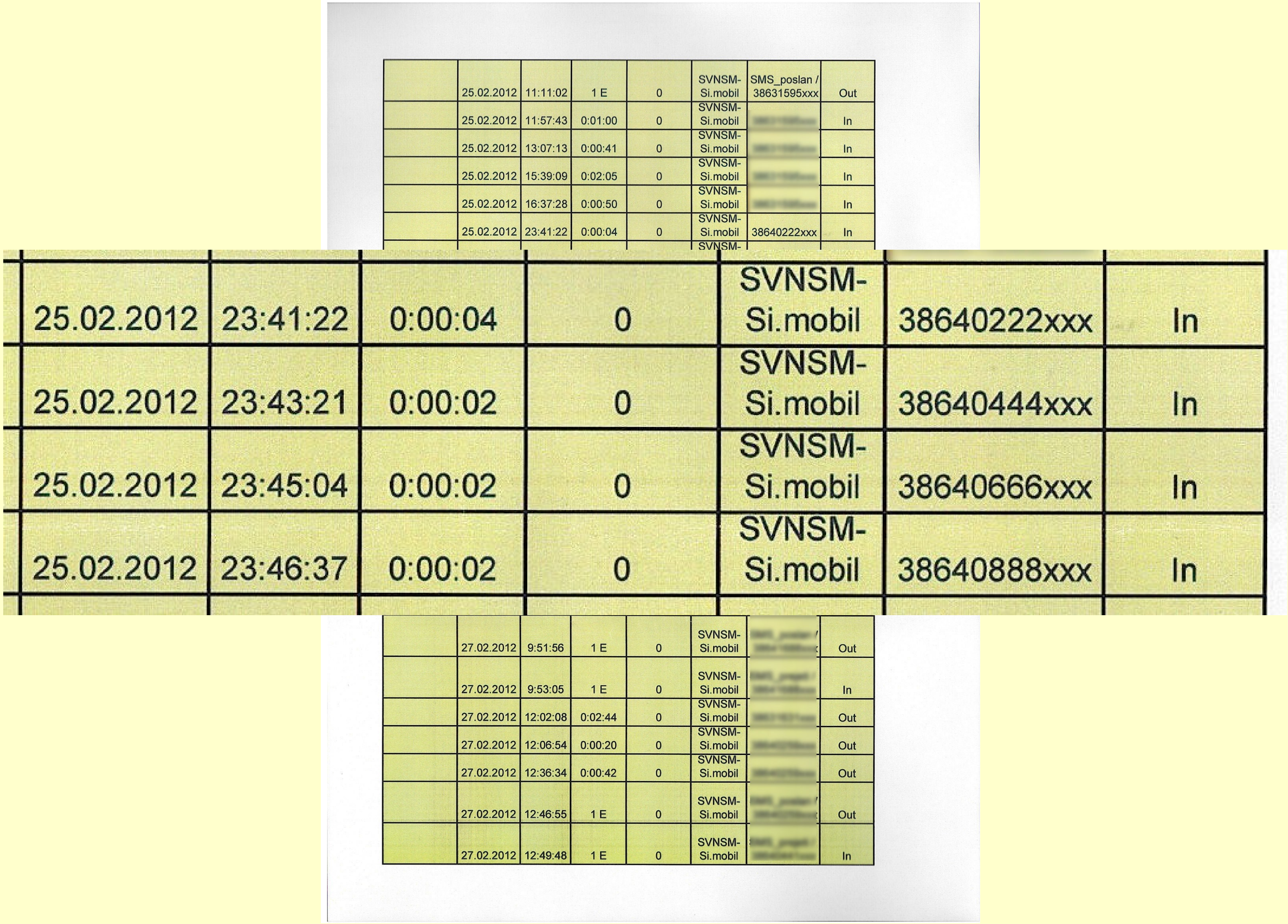


040999999 2 mins ago
040888888 2 mins ago
040777777 3 mins ago
040666666 4 mins ago
040555555 5 mins ago
040444444 6 mins ago

today at 23:44 Duration: 00:00
today at 23:43 Duration: 00:01
today at 23:42 Duration: 00:00
today at 23:41 Duration: 00:03
today at 23:40 Duration: 00:00

Klicanje s poljubno klicno identifikacijo

4: prometni podatki pri operaterju

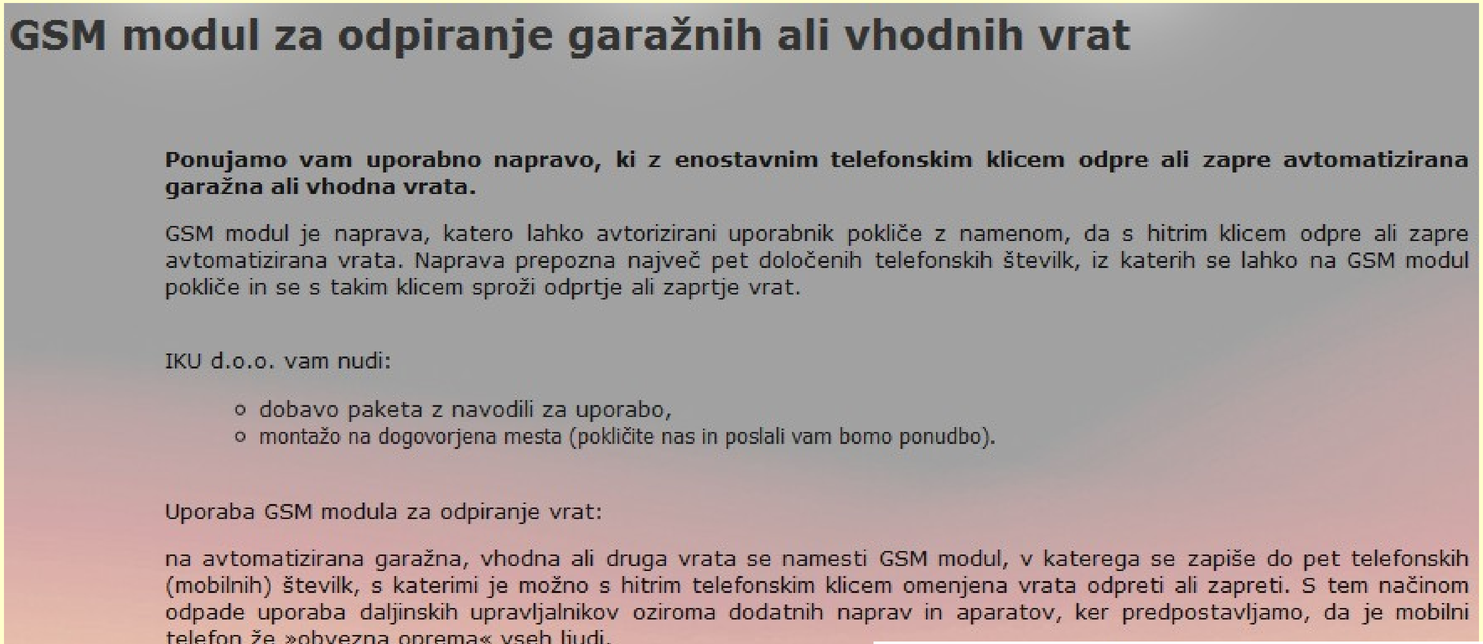


	25.02.2012	11:11:02	1 E	0	SVNSM-Si.mobil	SMS_poslan / 38631595xxx	Out
	25.02.2012	11:57:43	0:01:00	0	SVNSM-Si.mobil	[redacted]	In
	25.02.2012	13:07:13	0:00:41	0	SVNSM-Si.mobil	[redacted]	In
	25.02.2012	15:39:09	0:02:05	0	SVNSM-Si.mobil	[redacted]	In
	25.02.2012	16:37:28	0:00:50	0	SVNSM-Si.mobil	[redacted]	In
	25.02.2012	23:41:22	0:00:04	0	SVNSM-Si.mobil	38640222xxx	In
					SVNSM-		

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	[redacted]	Out
	27.02.2012	9:53:05	1 E	0	SVNSM-Si.mobil	[redacted]	In
	27.02.2012	12:02:08	0:02:44	0	SVNSM-Si.mobil	[redacted]	Out
	27.02.2012	12:06:54	0:00:20	0	SVNSM-Si.mobil	[redacted]	Out
	27.02.2012	12:36:34	0:00:42	0	SVNSM-Si.mobil	[redacted]	Out
	27.02.2012	12:46:55	1 E	0	SVNSM-Si.mobil	[redacted]	Out
	27.02.2012	12:49:48	1 E	0	SVNSM-Si.mobil	[redacted]	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.

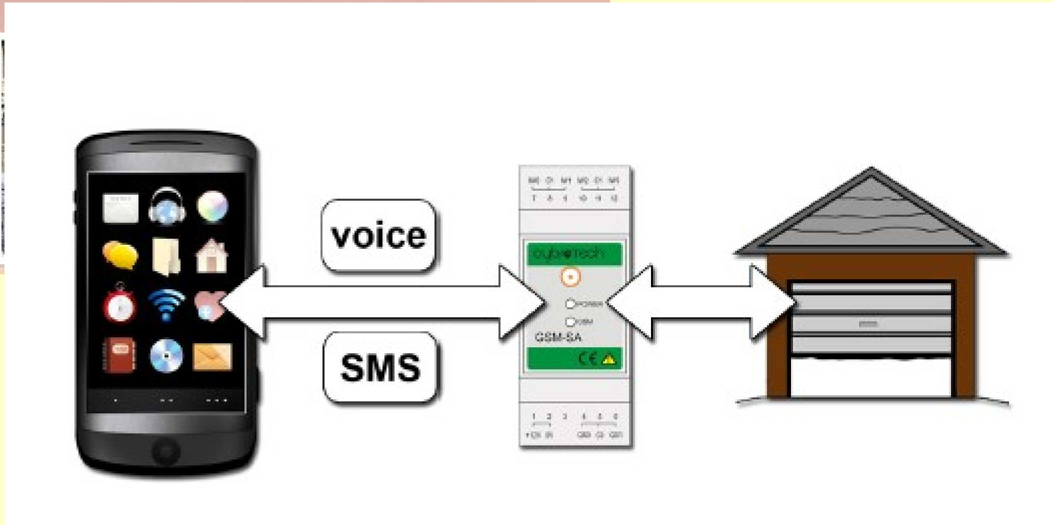
GSM modul je naprava, katero lahko avtorizirani uporabnik pokliče z namenom, da s hitrim klicem odpre ali zapre avtomatizirana vrata. Naprava prepozna največ pet določenih telefonskih številk, iz katerih se lahko na GSM modul pokliče in se s takim klicem sproži odprtje ali zaprtje vrat.

IKU d.o.o. vam nudi:

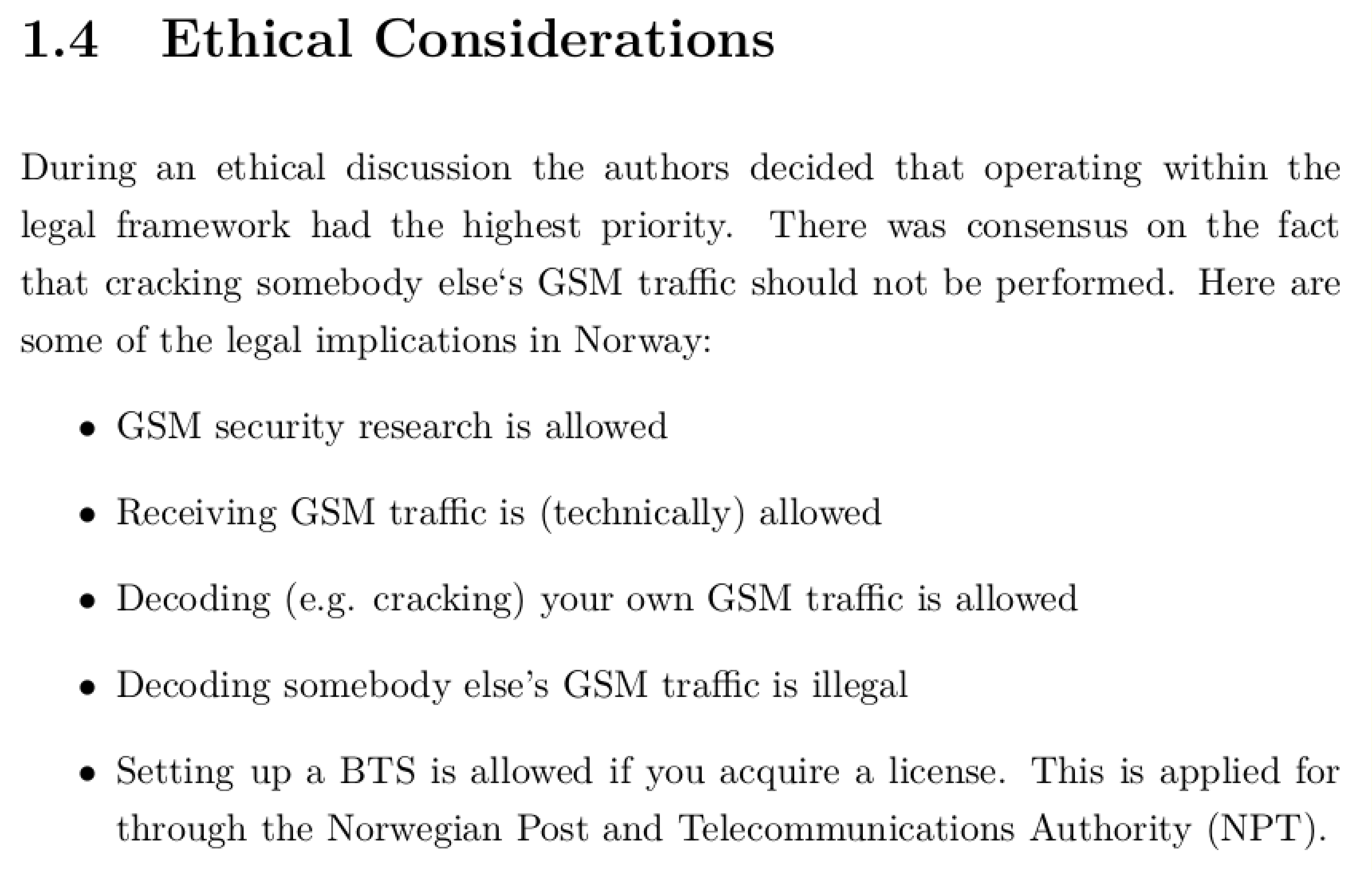
- dobavo paketa z navodili za uporabo,
- montažo na dogovorjena mesta (pokličite nas in poslali vam bomo ponudbo).

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);
  - <u>našemu telefonu</u> 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);

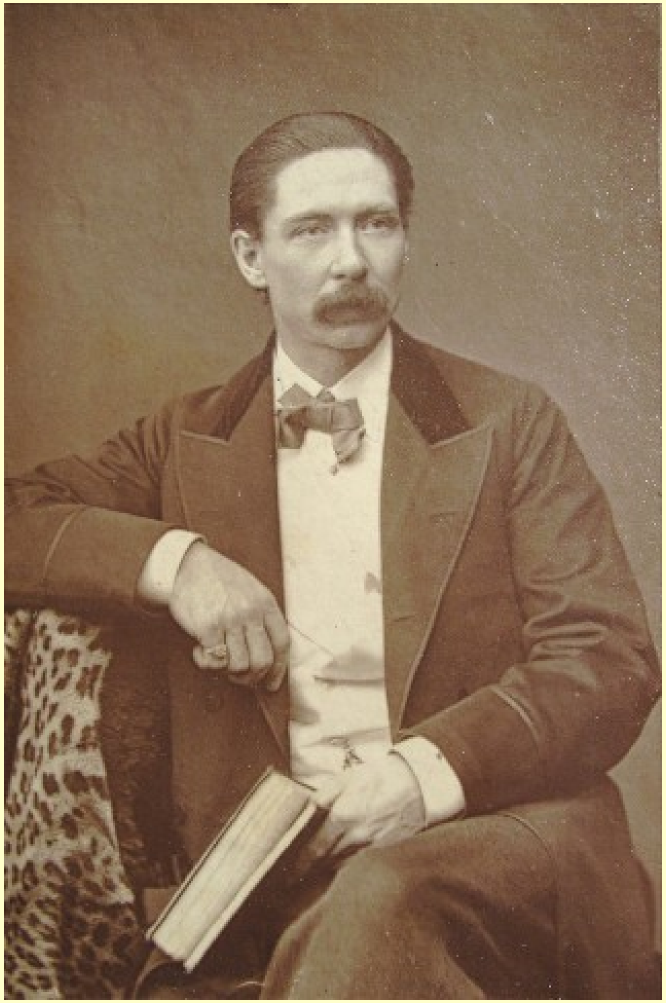
Kaj točno smo naredili?
(in zakaj to ni nezakonito)

- 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!

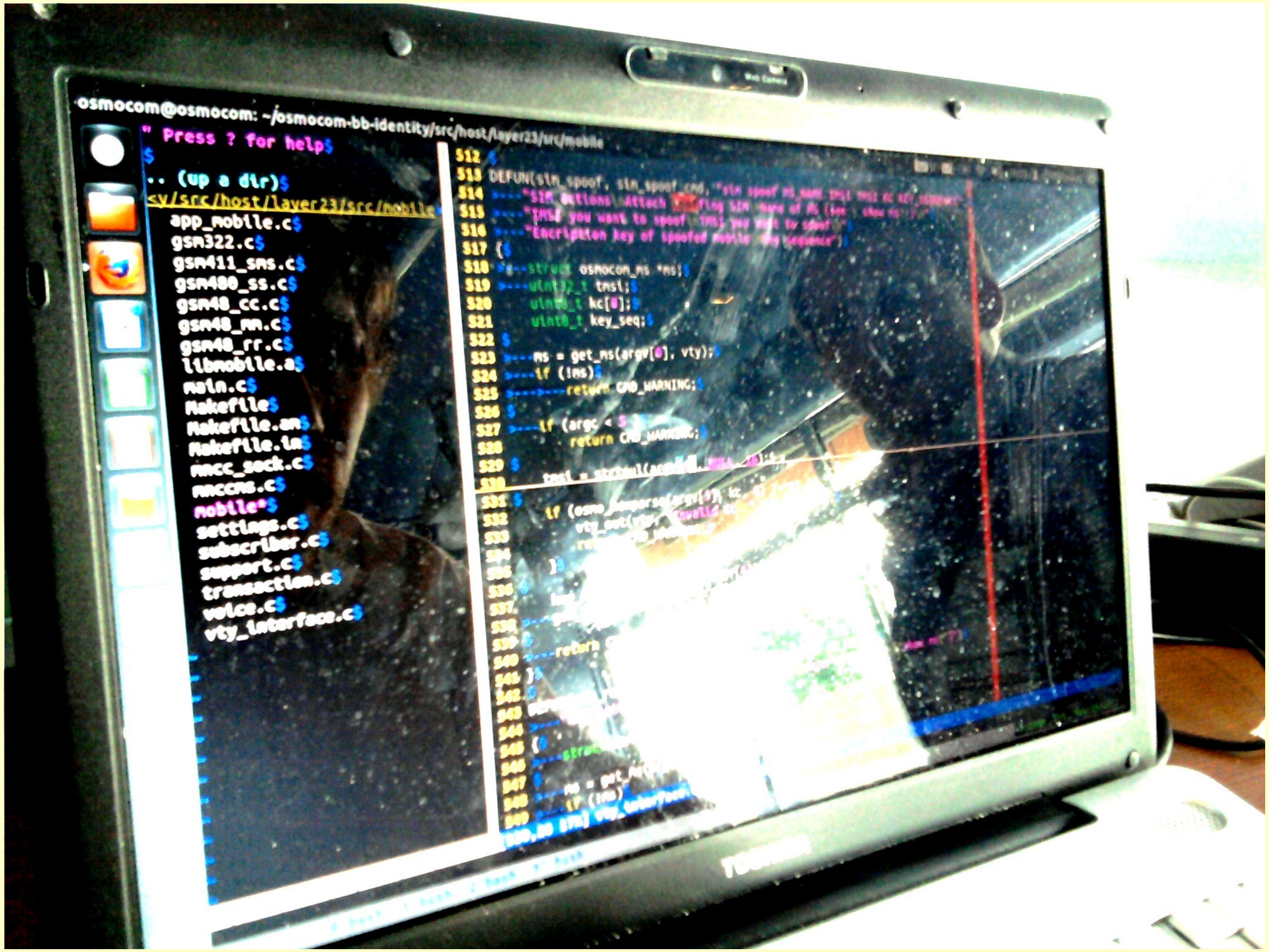
Kaj točno smo naredili?
(in zakaj to ni nezakonito)

- 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



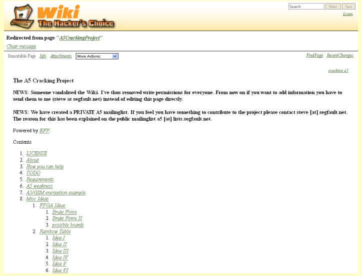
John Nevil Maskelyne
(1839 – 1917)



```
osmocom@osmocom: ~/osmocom-bb-identity/src/host/layer23/src/mobile
" Press ? for help

.. (up a dir)
<y/src/host/layer23/src/mobile
  app_mobile.c
  gsm322.c
  gsm411_sms.c
  gsm480_ss.c
  gsm48_cc.c
  gsm48_mm.c
  gsm48_rr.c
  libmobile.a
  main.c
  Makefile
  Makefile.am
  Makefile.in
  mncc_sock.c
  mnccms.c
  mobile*
  settings.c
  subscriber.c
  support.c
  transaction.c
  voice.c
  vty_interface.c
```

```

DEFUN(sim_spoof, sim_spoof_cmd, "sim spoof [illegible]
	"SIM actions\nAttach [illegible]
	"IMSI you want to spoof\nIMSI you want to spoof"
	"Encription key of spoofed mobile [illegible] sequence")
{
	struct osmocom_ms *ms;
	uint32_t tmsi;
	uint8_t kc[8];
	uint8_t key_seq;

	ms = get_ms(argv[0], vty);
	if (!ms)
		return CMD_WARNING;

	if (argc < 5 )
		return CMD_WARNING;

	tmsi = strtoul(argv[illegible]

	if (osmo_hexparse(argv[3], kc, [illegible]
		vty_out(vty, "Invalid Kc [illegible]
		return [illegible]
	}
```

Kiberpipa
(2012)



Redirected from page "A5CrackingProject"

Clear message

The A5 Cracking Project

NEWS: Someone vandalised the Wiki. I've thus removed write permissions for everyone. From now on if you want to add information you have to send them to me (steve at segfault.net) instead of editing this page directly.

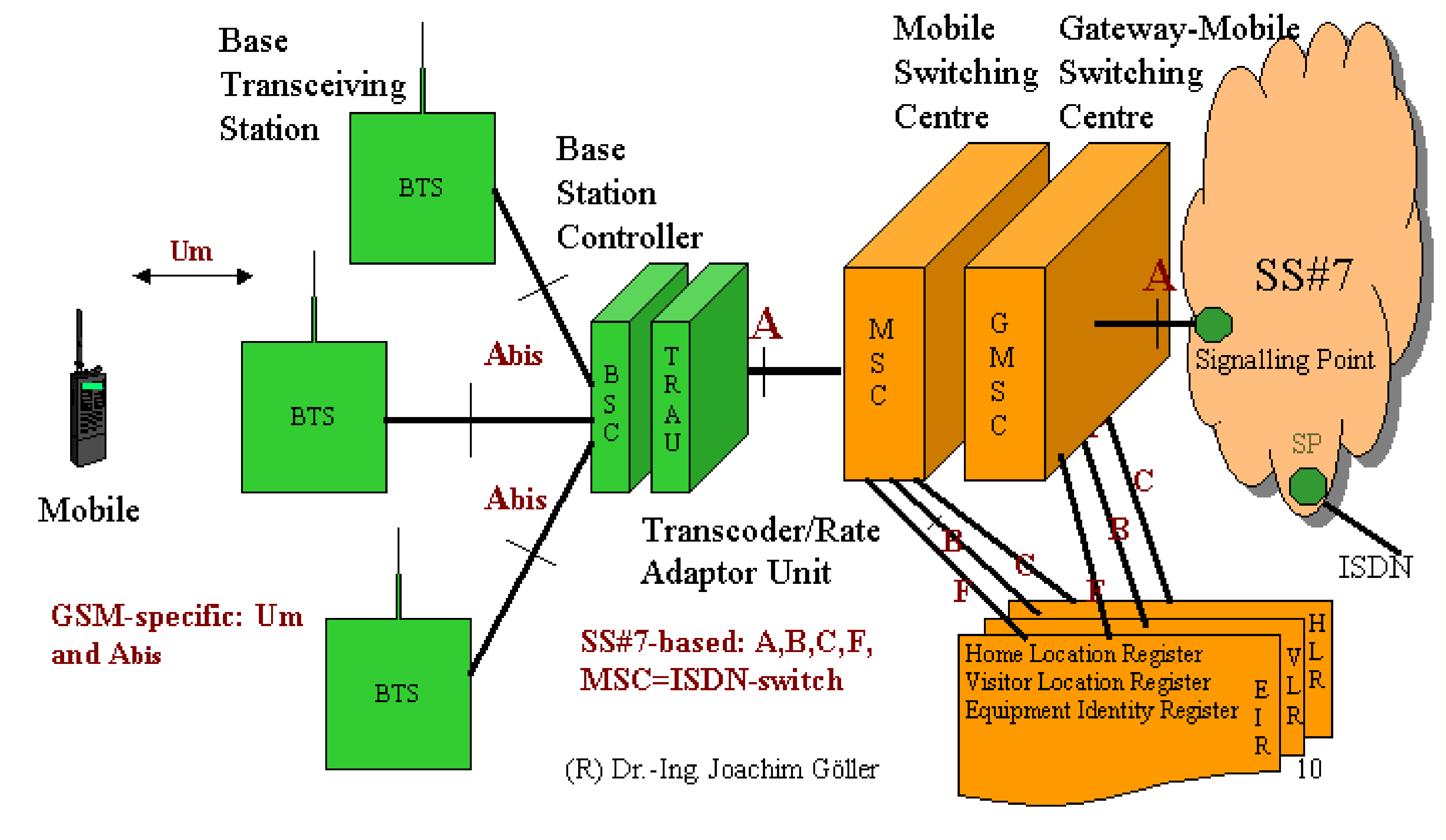
NEWS: We have created a PRIVATE A5 mailinglist. If you feel you have something to contribute to the project please contact steve [at] segfault.net. The reason for this has been explained on the public mailinglist a5 [at] lists.segfault.net.

Powered by EFF.

Contents

1. LICENSE
2. About
3. How you can help
4. TODO
5. Requirements
6. A5 weakness
7. A5/GSM encryption example
8. Misc Ideas
    1. FPGA Ideas
        1. Brute Force
        2. Brute Force II
        3. possible boards
    2. Rainbow Table
        1. Idea I
        2. Idea II
        3. Idea III
        4. Idea IV
        5. Idea V
        6. Idea VI

Nekaj osnov o GSM



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

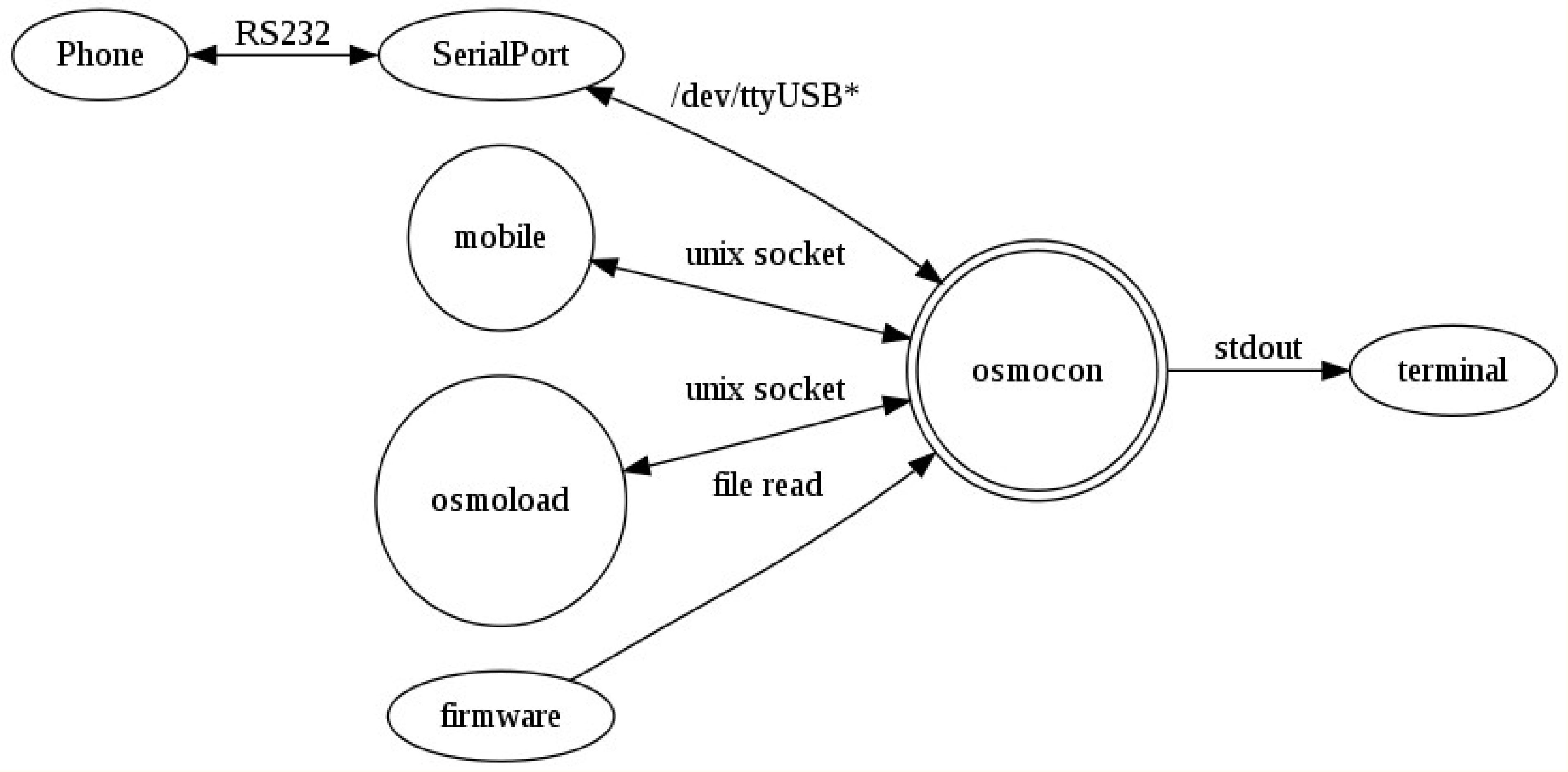
Shema GSM omrežja, vir: *www.gsmfordummies.com*.

OsmocomBB

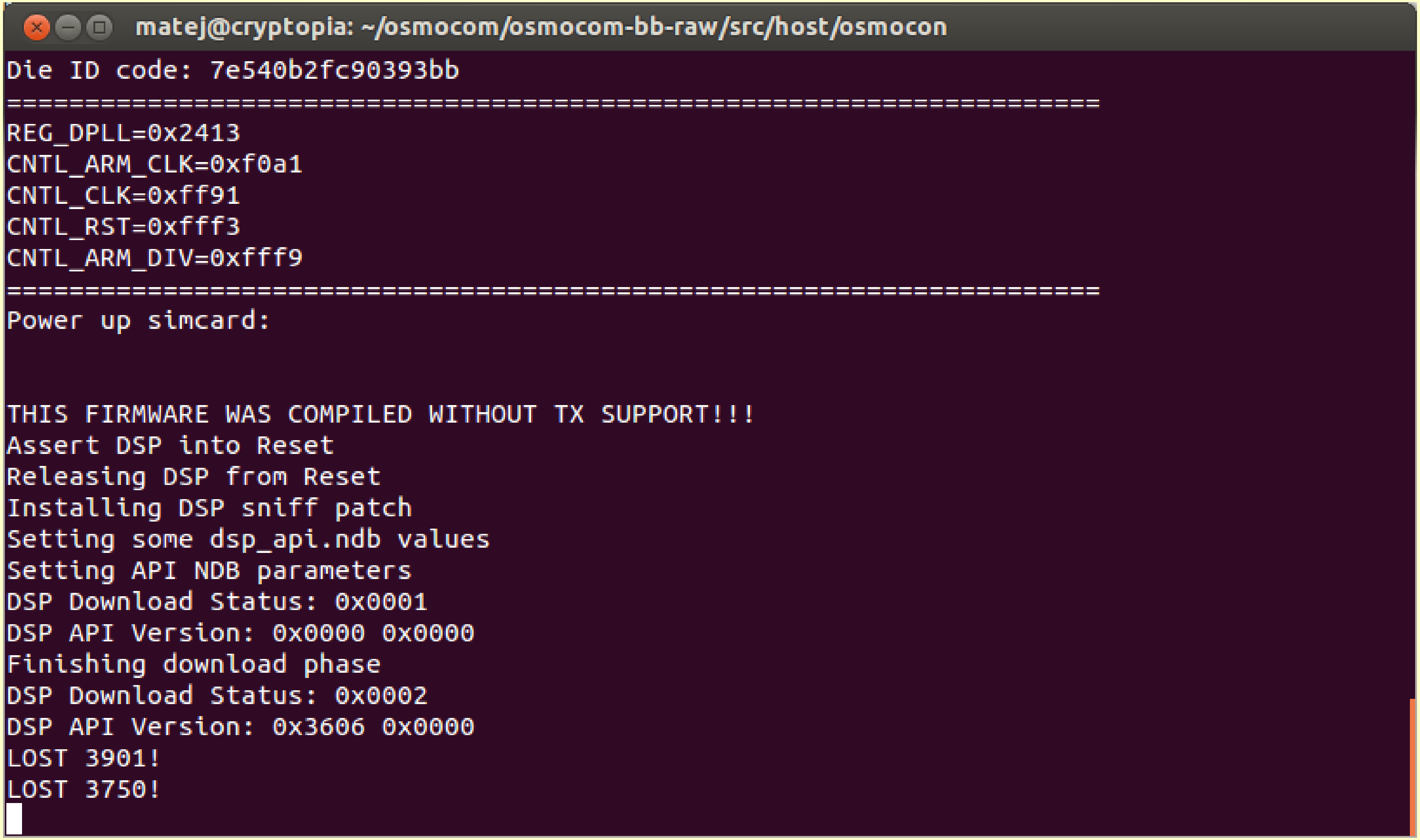
Mobilni telefon s Calypso čipovjem...

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

...in OsmocomBB strojna programska oprema

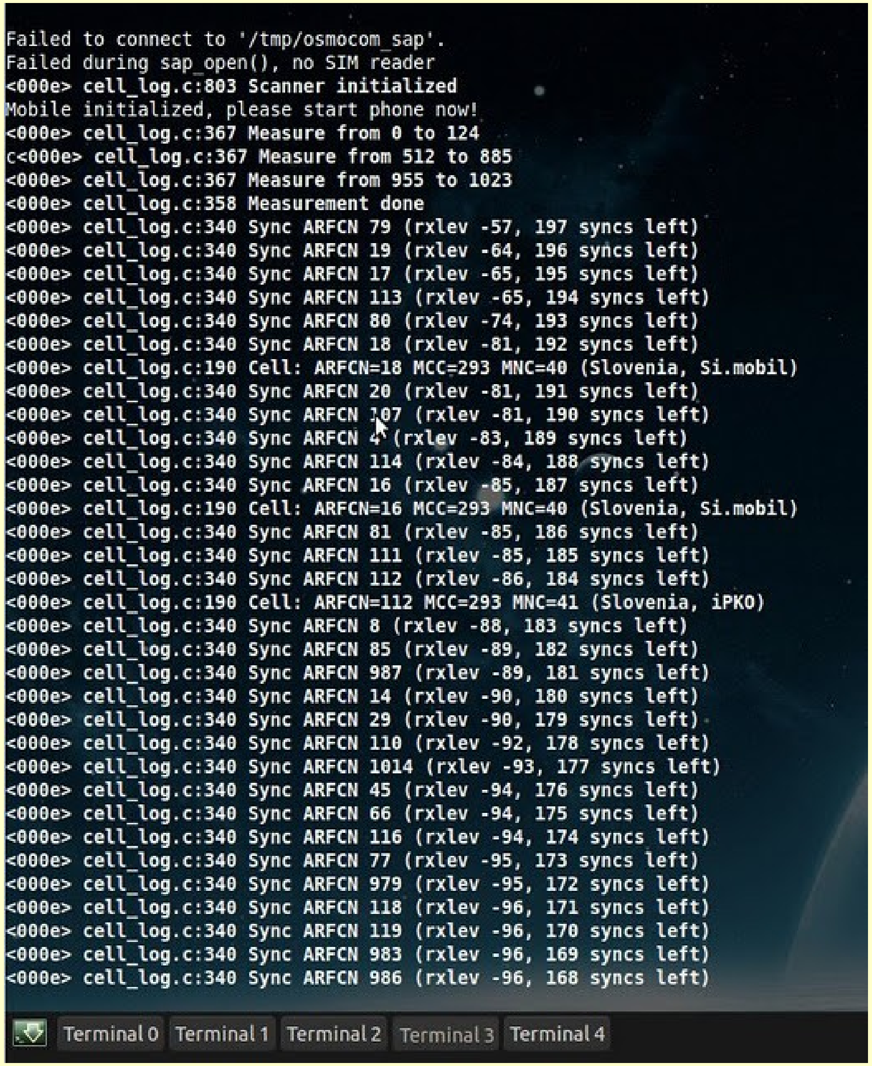


Zagon nalagalnika ROM (ang. *romloader*)



```
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!
```

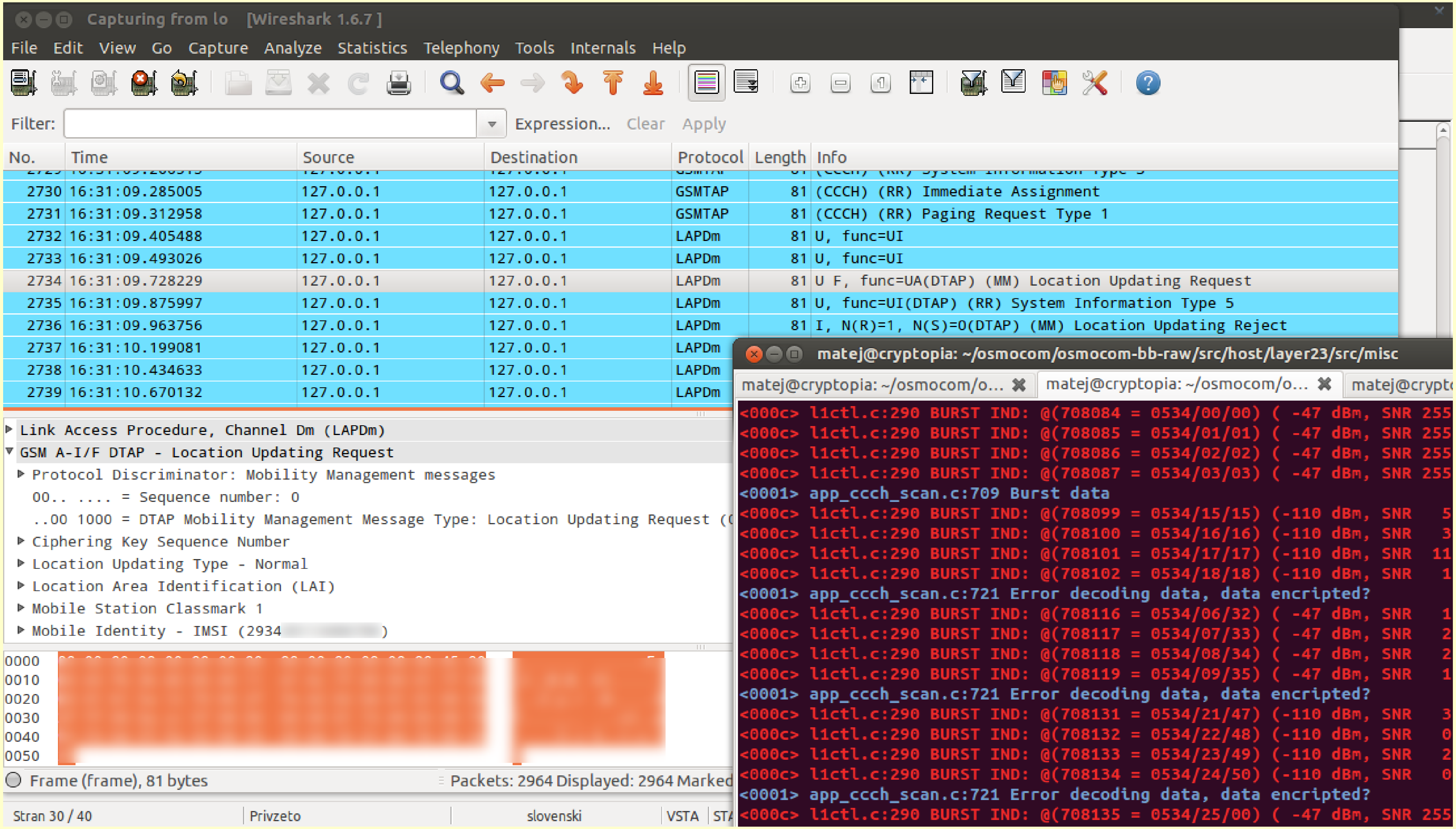
Pregled baznih postaj...



```
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)
```

Pregled ARFCN-jev s programom *cell_log*.

Analiza GSM prometa...



Capturing from lo [Wireshark 1.6.7]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

```
No.  Time             Source      Destination  Protocol  Length  Info
2730 16:31:09.285005  127.0.0.1   127.0.0.1    GSMTAP        81  (CCCH) (RR) Immediate Assignment
2731 16:31:09.312958  127.0.0.1   127.0.0.1    GSMTAP        81  (CCCH) (RR) Paging Request Type 1
2732 16:31:09.405488  127.0.0.1   127.0.0.1    LAPDm         81  U, func=UI
2733 16:31:09.493026  127.0.0.1   127.0.0.1    LAPDm         81  U, func=UI
2734 16:31:09.728229  127.0.0.1   127.0.0.1    LAPDm         81  U F, func=UA(DTAP) (MM) Location Updating Request
2735 16:31:09.875997  127.0.0.1   127.0.0.1    LAPDm         81  U, func=UI(DTAP) (RR) System Information Type 5
2736 16:31:09.963756  127.0.0.1   127.0.0.1    LAPDm         81  I, N(R)=1, N(S)=0(DTAP) (MM) Location Updating Reject
2737 16:31:10.199081  127.0.0.1   127.0.0.1    LAPDm
2738 16:31:10.434633  127.0.0.1   127.0.0.1    LAPDm
2739 16:31:10.670132  127.0.0.1   127.0.0.1    LAPDm
```

```
▶ Link Access Procedure, Channel Dm (LAPDm)
▼ GSM A-I/F DTAP - Location Updating Request
  ▶ Protocol Discriminator: Mobility Management messages
    00.. .... = Sequence number: 0
    ..00 1000 = DTAP Mobility Management Message Type: Location Updating Request ((
  ▶ Ciphering Key Sequence Number
  ▶ Location Updating Type - Normal
  ▶ Location Area Identification (LAI)
  ▶ Mobile Station Classmark 1
  ▶ Mobile Identity - IMSI (2934[redacted])
```

```
0000 [redacted]
0010
0020
0030
0040
0050
```

Frame (frame), 81 bytes
Packets: 2964 Displayed: 2964 Marked
Stran 30 / 40
Privzeto
slovenski
VSTA
STA
matej@cryptopia: ~/osmocom/osmocom-bb-raw/src/host/layer23/src/misc
matej@cryptopia: ~/osmocom/o...
matej@cryptopia: ~/osmocom/o...
matej@crypto

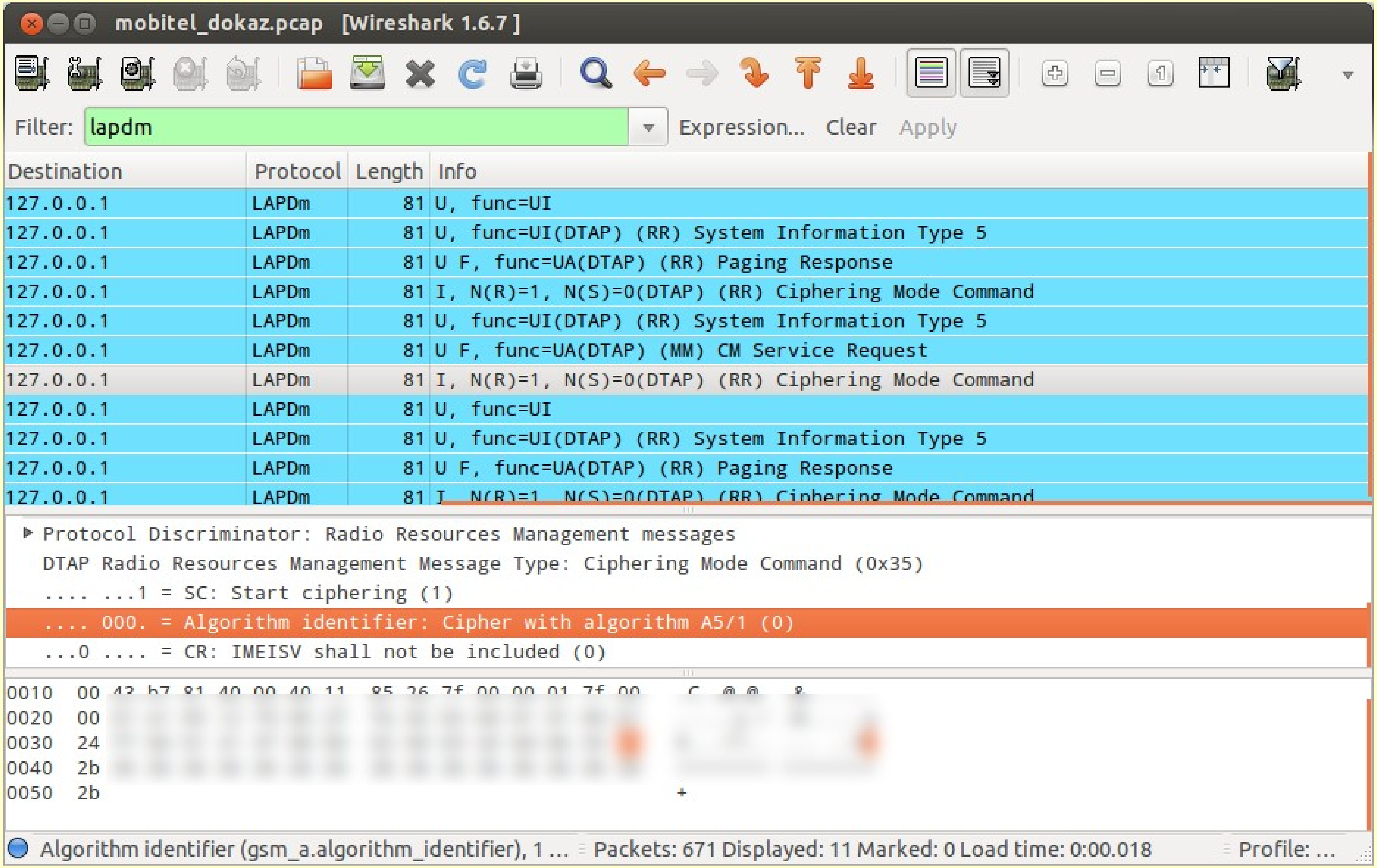
```
<000c> l1ctl.c:290 BURST IND: @(708084 = 0534/00/00) ( -47 dBm, SNR 255
<000c> l1ctl.c:290 BURST IND: @(708085 = 0534/01/01) ( -47 dBm, SNR 255
<000c> l1ctl.c:290 BURST IND: @(708086 = 0534/02/02) ( -47 dBm, SNR 255
<000c> l1ctl.c:290 BURST IND: @(708087 = 0534/03/03) ( -47 dBm, SNR 255
<0001> app_ccch_scan.c:709 Burst data
<000c> l1ctl.c:290 BURST IND: @(708099 = 0534/15/15) (-110 dBm, SNR   5
<000c> l1ctl.c:290 BURST IND: @(708100 = 0534/16/16) (-110 dBm, SNR   3
<000c> l1ctl.c:290 BURST IND: @(708101 = 0534/17/17) (-110 dBm, SNR  11
<000c> l1ctl.c:290 BURST IND: @(708102 = 0534/18/18) (-110 dBm, SNR   1
<0001> app_ccch_scan.c:721 Error decoding data, data encripted?
<000c> l1ctl.c:290 BURST IND: @(708116 = 0534/06/32) ( -47 dBm, SNR   1
<000c> l1ctl.c:290 BURST IND: @(708117 = 0534/07/33) ( -47 dBm, SNR   2
<000c> l1ctl.c:290 BURST IND: @(708118 = 0534/08/34) ( -47 dBm, SNR   2
<000c> l1ctl.c:290 BURST IND: @(708119 = 0534/09/35) ( -47 dBm, SNR   1
<0001> app_ccch_scan.c:721 Error decoding data, data encripted?
<000c> l1ctl.c:290 BURST IND: @(708131 = 0534/21/47) (-110 dBm, SNR   3
<000c> l1ctl.c:290 BURST IND: @(708132 = 0534/22/48) (-110 dBm, SNR   0
<000c> l1ctl.c:290 BURST IND: @(708133 = 0534/23/49) (-110 dBm, SNR   2
<000c> l1ctl.c:290 BURST IND: @(708134 = 0534/24/50) (-110 dBm, SNR   0
<0001> app_ccch_scan.c:721 Error decoding data, data encripted?
<000c> l1ctl.c:290 BURST IND: @(708135 = 0534/25/00) ( -47 dBm, SNR 255
```

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



```
Destination   Protocol  Length  Info
127.0.0.1     LAPDm         81  U, func=UI
127.0.0.1     LAPDm         81  U, func=UI(DTAP) (RR) System Information Type 5
127.0.0.1     LAPDm         81  U F, func=UA(DTAP) (RR) Paging Response
127.0.0.1     LAPDm         81  I, N(R)=1, N(S)=0(DTAP) (RR) Ciphering Mode Command
127.0.0.1     LAPDm         81  U, func=UI(DTAP) (RR) System Information Type 5
127.0.0.1     LAPDm         81  U F, func=UA(DTAP) (MM) CM Service Request
127.0.0.1     LAPDm         81  I, N(R)=1, N(S)=0(DTAP) (RR) Ciphering Mode Command
127.0.0.1     LAPDm         81  U, func=UI
127.0.0.1     LAPDm         81  U, func=UI(DTAP) (RR) System Information Type 5
127.0.0.1     LAPDm         81  U F, func=UA(DTAP) (RR) Paging Response
127.0.0.1     LAPDm         81  I, N(R)=1, N(S)=0(DTAP) (RR) Ciphering Mode Command
```

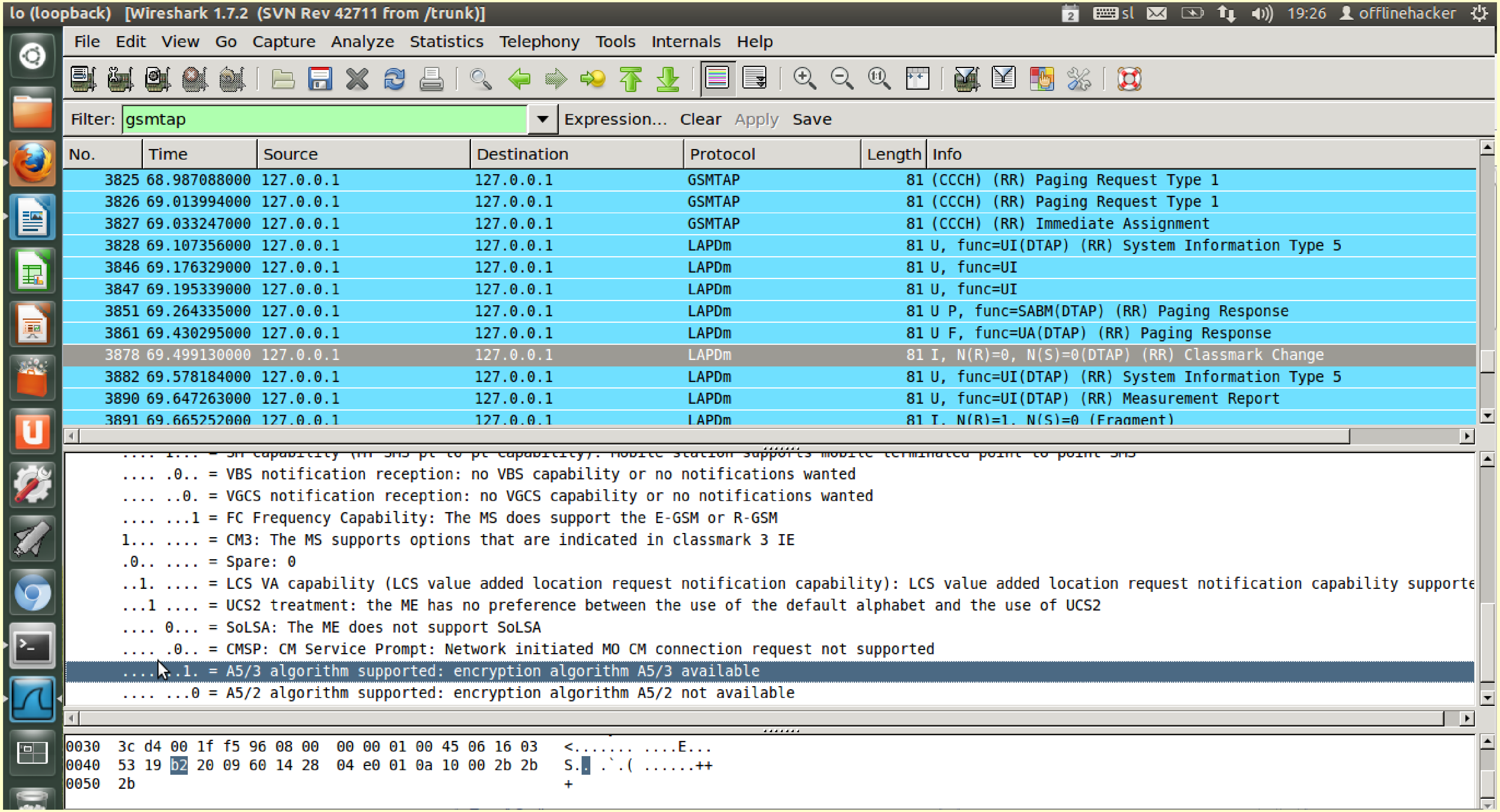
```
▶ Protocol Discriminator: Radio Resources Management messages
  DTAP Radio Resources Management Message Type: Ciphering Mode Command (0x35)
  .... ...1 = SC: Start ciphering (1)
  .... 000. = Algorithm identifier: Cipher with algorithm A5/1 (0)
  ...0 .... = CR: IMEISV shall not be included (0)
```

```
0010   00 [redacted]
0020   00
0030   24
0040   2b
0050   2b                                              +
```

Algorithm identifier (gsm_a.algorithm_identifier), 1 ... Packets: 671 Displayed: 11 Marked: 0 Load time: 0:00.018 Profile: ...

Mobitel je v času pregleda uporabljal šifriranje A5/1

Uporaba šifriranja - Mobitel



Filter: gsmtap

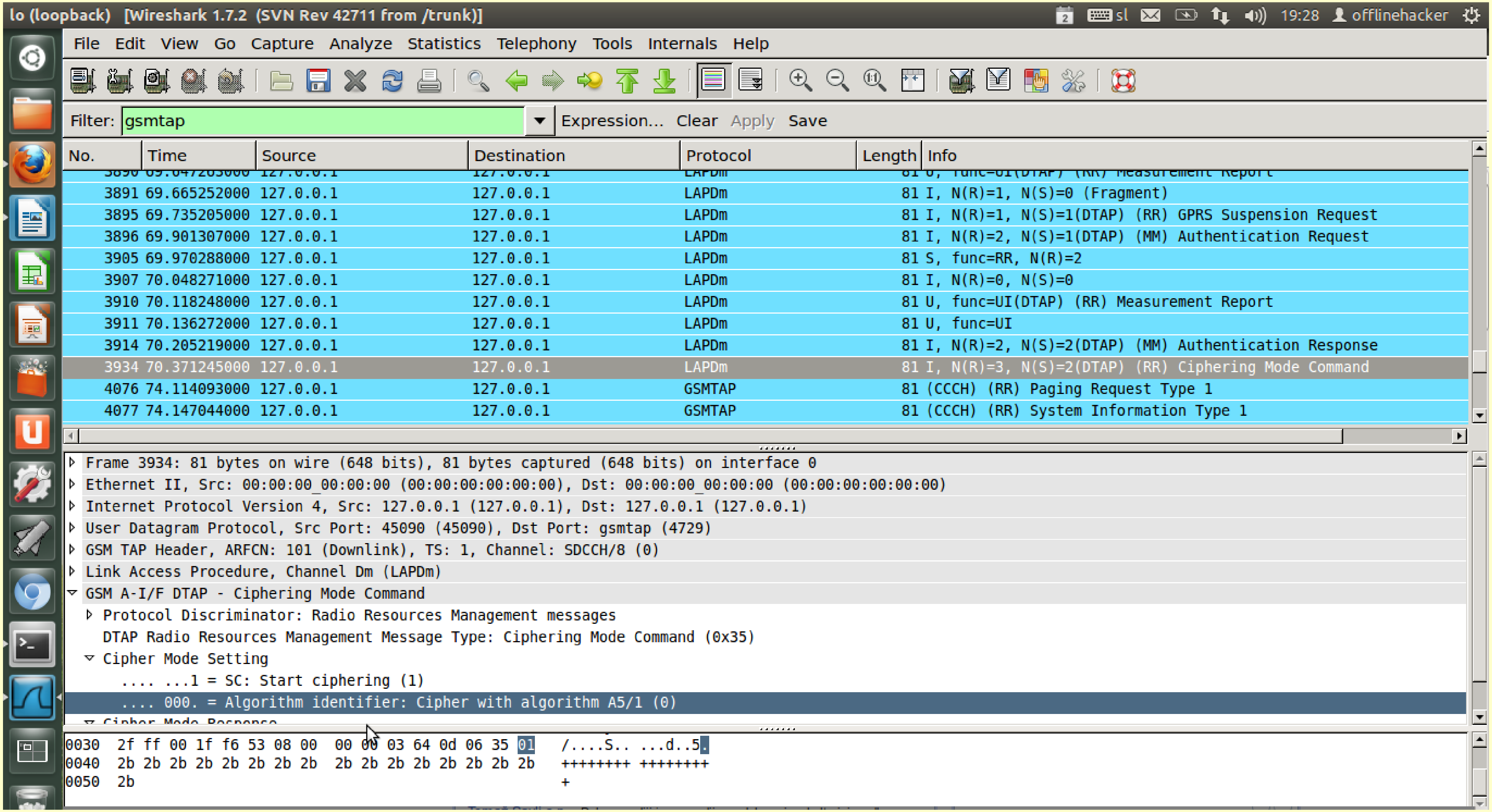
```
No.   Time          Source      Destination  Protocol  Length Info
 3825 68.987088000  127.0.0.1   127.0.0.1    GSMTAP    81 (CCCH) (RR) Paging Request Type 1
 3826 69.013994000  127.0.0.1   127.0.0.1    GSMTAP    81 (CCCH) (RR) Paging Request Type 1
 3827 69.033247000  127.0.0.1   127.0.0.1    GSMTAP    81 (CCCH) (RR) Immediate Assignment
 3828 69.107356000  127.0.0.1   127.0.0.1    LAPDm     81 U, func=UI(DTAP) (RR) System Information Type 5
 3846 69.176329000  127.0.0.1   127.0.0.1    LAPDm     81 U, func=UI
 3847 69.195339000  127.0.0.1   127.0.0.1    LAPDm     81 U, func=UI
 3851 69.264335000  127.0.0.1   127.0.0.1    LAPDm     81 U P, func=SABM(DTAP) (RR) Paging Response
 3861 69.430295000  127.0.0.1   127.0.0.1    LAPDm     81 U F, func=UA(DTAP) (RR) Paging Response
 3878 69.499130000  127.0.0.1   127.0.0.1    LAPDm     81 I, N(R)=0, N(S)=0(DTAP) (RR) Classmark Change
 3882 69.578184000  127.0.0.1   127.0.0.1    LAPDm     81 U, func=UI(DTAP) (RR) System Information Type 5
 3890 69.647263000  127.0.0.1   127.0.0.1    LAPDm     81 U, func=UI(DTAP) (RR) Measurement Report
 3891 69.665252000  127.0.0.1   127.0.0.1    LAPDm     81 I, N(R)=1, N(S)=0 (Fragment)
```

```
    .... 1... = SM capability (MT SMS pt to pt capability): Mobile station supports mobile terminated point to point SMS
    .... .0.. = VBS notification reception: no VBS capability or no notifications wanted
    .... ..0. = VGCS notification reception: no VGCS capability or no notifications wanted
    .... ...1 = FC Frequency Capability: The MS does support the E-GSM or R-GSM
    1... .... = CM3: The MS supports options that are indicated in classmark 3 IE
    .0.. .... = Spare: 0
    ..1. .... = LCS VA capability (LCS value added location request notification capability): LCS value added location request notification capability supporte
    ...1 .... = UCS2 treatment: the ME has no preference between the use of the default alphabet and the use of UCS2
    .... 0... = SoLSA: The ME does not support SoLSA
    .... .0.. = CMSP: CM Service Prompt: Network initiated MO CM connection request not supported
    .... ..1. = A5/3 algorithm supported: encryption algorithm A5/3 available
    .... ...0 = A5/2 algorithm supported: encryption algorithm A5/2 not available
```

```
0030  3c d4 00 1f f5 96 08 00  00 00 01 00 45 06 16 03   <....... ....E...
0040  53 19 b2 20 09 60 14 28  04 e0 01 0a 10 00 2b 2b   S.. .`.( ......++
0050  2b                                                 +
```

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

Uporaba šifriranja - Mobitel


lo (loopback) [Wireshark 1.7.2 (SVN Rev 42711 from /trunk)]
sl
19:28
offlinehacker
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: gsmtap

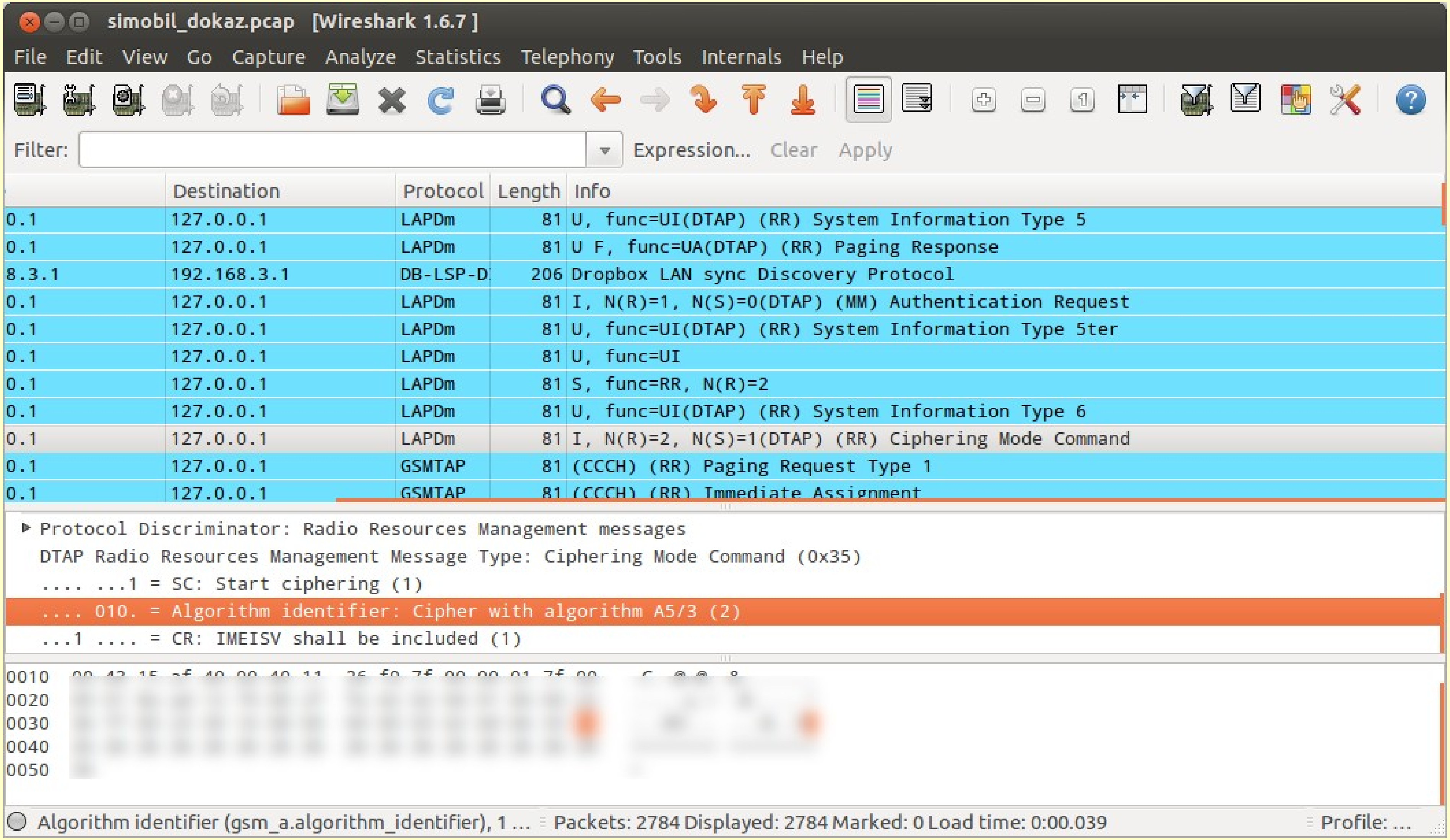
```
No.   Time          Source      Destination  Protocol  Length Info
 3890 69.647263000 127.0.0.1   127.0.0.1    LAPDm     81 U, func=UI(DTAP) (RR) Measurement Report
 3891 69.665252000 127.0.0.1   127.0.0.1    LAPDm     81 I, N(R)=1, N(S)=0 (Fragment)
 3895 69.735205000 127.0.0.1   127.0.0.1    LAPDm     81 I, N(R)=1, N(S)=1(DTAP) (RR) GPRS Suspension Request
 3896 69.901307000 127.0.0.1   127.0.0.1    LAPDm     81 I, N(R)=2, N(S)=1(DTAP) (MM) Authentication Request
 3905 69.970288000 127.0.0.1   127.0.0.1    LAPDm     81 S, func=RR, N(R)=2
 3907 70.048271000 127.0.0.1   127.0.0.1    LAPDm     81 I, N(R)=0, N(S)=0
 3910 70.118248000 127.0.0.1   127.0.0.1    LAPDm     81 U, func=UI(DTAP) (RR) Measurement Report
 3911 70.136272000 127.0.0.1   127.0.0.1    LAPDm     81 U, func=UI
 3914 70.205219000 127.0.0.1   127.0.0.1    LAPDm     81 I, N(R)=2, N(S)=2(DTAP) (MM) Authentication Response
 3934 70.371245000 127.0.0.1   127.0.0.1    LAPDm     81 I, N(R)=3, N(S)=2(DTAP) (RR) Ciphering Mode Command
 4076 74.114093000 127.0.0.1   127.0.0.1    GSMTAP    81 (CCCH) (RR) Paging Request Type 1
 4077 74.147044000 127.0.0.1   127.0.0.1    GSMTAP    81 (CCCH) (RR) System Information Type 1
```

```
▷ Frame 3934: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
▷ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▷ Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
▷ User Datagram Protocol, Src Port: 45090 (45090), Dst Port: gsmtap (4729)
▷ GSM TAP Header, ARFCN: 101 (Downlink), TS: 1, Channel: SDCCH/8 (0)
▷ Link Access Procedure, Channel Dm (LAPDm)
▽ GSM A-I/F DTAP - Ciphering Mode Command
  ▷ Protocol Discriminator: Radio Resources Management messages
    DTAP Radio Resources Management Message Type: Ciphering Mode Command (0x35)
  ▽ Cipher Mode Setting
      .... ...1 = SC: Start ciphering (1)
      .... 000. = Algorithm identifier: Cipher with algorithm A5/1 (0)
  ▽ Cipher Mode Response
```

```
0030  2f ff 00 1f f6 53 08 00  00 00 03 64 0d 06 35 01   /....S.. ...d..5.
0040  2b 2b 2b 2b 2b 2b 2b 2b  2b 2b 2b 2b 2b 2b 2b 2b   ++++++++ ++++++++
0050  2b                                                  +
```

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

Uporaba šifriranja - Simobil



simobil_dokaz.pcap [Wireshark 1.6.7]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

```
         Destination    Protocol  Length Info
0.1      127.0.0.1      LAPDm         81 U, func=UI(DTAP) (RR) System Information Type 5
0.1      127.0.0.1      LAPDm         81 U F, func=UA(DTAP) (RR) Paging Response
8.3.1    192.168.3.1    DB-LSP-DI    206 Dropbox LAN sync Discovery Protocol
0.1      127.0.0.1      LAPDm         81 I, N(R)=1, N(S)=0(DTAP) (MM) Authentication Request
0.1      127.0.0.1      LAPDm         81 U, func=UI(DTAP) (RR) System Information Type 5ter
0.1      127.0.0.1      LAPDm         81 U, func=UI
0.1      127.0.0.1      LAPDm         81 S, func=RR, N(R)=2
0.1      127.0.0.1      LAPDm         81 U, func=UI(DTAP) (RR) System Information Type 6
0.1      127.0.0.1      LAPDm         81 I, N(R)=2, N(S)=1(DTAP) (RR) Ciphering Mode Command
0.1      127.0.0.1      GSMTAP        81 (CCCH) (RR) Paging Request Type 1
0.1      127.0.0.1      GSMTAP        81 (CCCH) (RR) Immediate Assignment
```

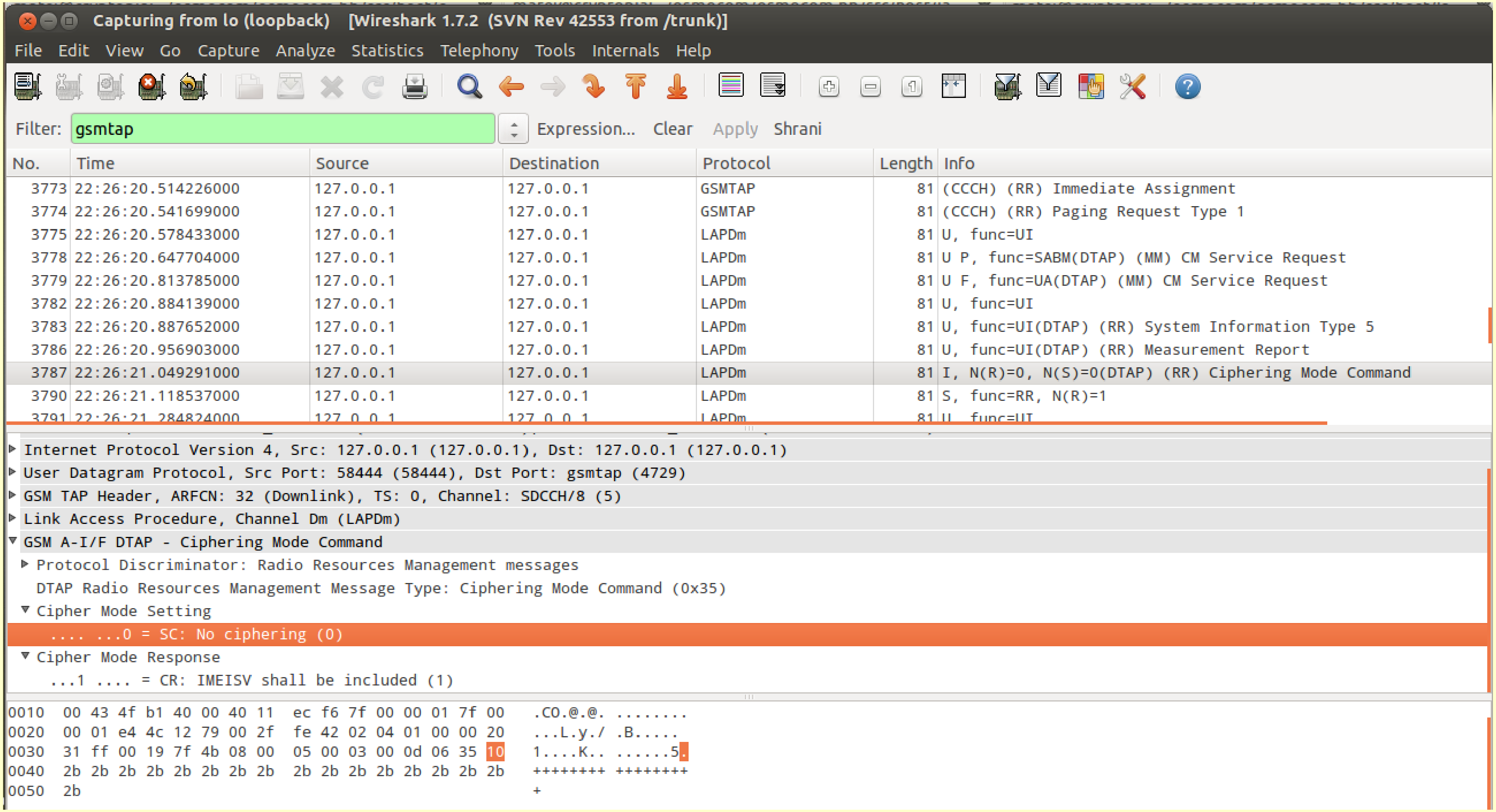
```
▶ Protocol Discriminator: Radio Resources Management messages
  DTAP Radio Resources Management Message Type: Ciphering Mode Command (0x35)
  .... ...1 = SC: Start ciphering (1)
  .... 010. = Algorithm identifier: Cipher with algorithm A5/3 (2)
  ...1 .... = CR: IMEISV shall be included (1)
```

```
0010  [redacted]
0020
0030
0040
0050
```

```
○ Algorithm identifier (gsm_a.algorithm_identifier), 1 ... Packets: 2784 Displayed: 2784 Marked: 0 Load time: 0:00.039   Profile: ...
```

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

Uporaba šifriranja - Simobil


Capturing from lo (loopback)   [Wireshark 1.7.2 (SVN Rev 42553 from /trunk)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Shrani

Filter: gsmtap

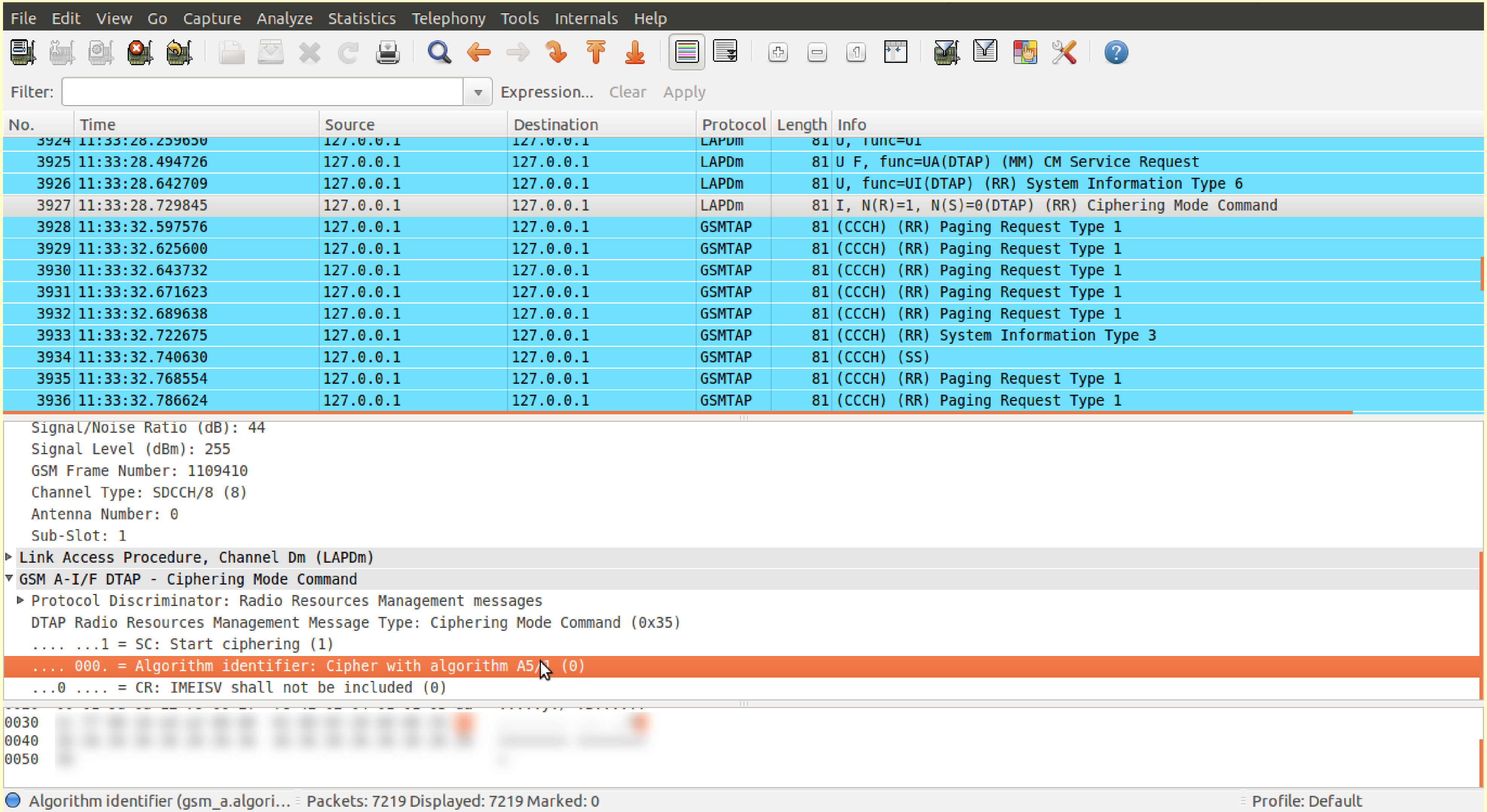
```
No.   Time                Source      Destination  Protocol  Length Info
 3773 22:26:20.514226000  127.0.0.1   127.0.0.1    GSMTAP        81 (CCCH) (RR) Immediate Assignment
 3774 22:26:20.541699000  127.0.0.1   127.0.0.1    GSMTAP        81 (CCCH) (RR) Paging Request Type 1
 3775 22:26:20.578433000  127.0.0.1   127.0.0.1    LAPDm         81 U, func=UI
 3778 22:26:20.647704000  127.0.0.1   127.0.0.1    LAPDm         81 U P, func=SABM(DTAP) (MM) CM Service Request
 3779 22:26:20.813785000  127.0.0.1   127.0.0.1    LAPDm         81 U F, func=UA(DTAP) (MM) CM Service Request
 3782 22:26:20.884139000  127.0.0.1   127.0.0.1    LAPDm         81 U, func=UI
 3783 22:26:20.887652000  127.0.0.1   127.0.0.1    LAPDm         81 U, func=UI(DTAP) (RR) System Information Type 5
 3786 22:26:20.956903000  127.0.0.1   127.0.0.1    LAPDm         81 U, func=UI(DTAP) (RR) Measurement Report
 3787 22:26:21.049291000  127.0.0.1   127.0.0.1    LAPDm         81 I, N(R)=0, N(S)=0(DTAP) (RR) Ciphering Mode Command
 3790 22:26:21.118537000  127.0.0.1   127.0.0.1    LAPDm         81 S, func=RR, N(R)=1
 3791 22:26:21.284824000  127.0.0.1   127.0.0.1    LAPDm         81 U, func=UI
```

```
▶ Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
▶ User Datagram Protocol, Src Port: 58444 (58444), Dst Port: gsmtap (4729)
▶ GSM TAP Header, ARFCN: 32 (Downlink), TS: 0, Channel: SDCCH/8 (5)
▶ Link Access Procedure, Channel Dm (LAPDm)
▼ GSM A-I/F DTAP - Ciphering Mode Command
  ▶ Protocol Discriminator: Radio Resources Management messages
    DTAP Radio Resources Management Message Type: Ciphering Mode Command (0x35)
  ▼ Cipher Mode Setting
      .... ...0 = SC: No ciphering (0)
  ▼ Cipher Mode Response
      ...1 .... = CR: IMEISV shall be included (1)
```

```
0010  00 43 4f b1 40 00 40 11  ec f6 7f 00 00 01 7f 00   .CO.@.@. ........
0020  00 01 e4 4c 12 79 00 2f  fe 42 02 04 01 00 00 20   ...L.y./ .B.....
0030  31 ff 00 19 7f 4b 08 00  05 00 03 00 0d 06 35 10   1....K.. ......5.
0040  2b 2b 2b 2b 2b 2b 2b 2b  2b 2b 2b 2b 2b 2b 2b 2b   ++++++++ ++++++++
0050  2b                                                 +
```

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

Uporaba šifriranja - Tušmobil


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

```
No.  Time             Source     Destination Protocol Length Info
3924 11:33:28.259650  127.0.0.1  127.0.0.1   LAPDm    81 U, func=UI
3925 11:33:28.494726  127.0.0.1  127.0.0.1   LAPDm    81 U F, func=UA(DTAP) (MM) CM Service Request
3926 11:33:28.642709  127.0.0.1  127.0.0.1   LAPDm    81 U, func=UI(DTAP) (RR) System Information Type 6
3927 11:33:28.729845  127.0.0.1  127.0.0.1   LAPDm    81 I, N(R)=1, N(S)=0(DTAP) (RR) Ciphering Mode Command
3928 11:33:32.597576  127.0.0.1  127.0.0.1   GSMTAP   81 (CCCH) (RR) Paging Request Type 1
3929 11:33:32.625600  127.0.0.1  127.0.0.1   GSMTAP   81 (CCCH) (RR) Paging Request Type 1
3930 11:33:32.643732  127.0.0.1  127.0.0.1   GSMTAP   81 (CCCH) (RR) Paging Request Type 1
3931 11:33:32.671623  127.0.0.1  127.0.0.1   GSMTAP   81 (CCCH) (RR) Paging Request Type 1
3932 11:33:32.689638  127.0.0.1  127.0.0.1   GSMTAP   81 (CCCH) (RR) Paging Request Type 1
3933 11:33:32.722675  127.0.0.1  127.0.0.1   GSMTAP   81 (CCCH) (RR) System Information Type 3
3934 11:33:32.740630  127.0.0.1  127.0.0.1   GSMTAP   81 (CCCH) (SS)
3935 11:33:32.768554  127.0.0.1  127.0.0.1   GSMTAP   81 (CCCH) (RR) Paging Request Type 1
3936 11:33:32.786624  127.0.0.1  127.0.0.1   GSMTAP   81 (CCCH) (RR) Paging Request Type 1
```

```
  Signal/Noise Ratio (dB): 44
  Signal Level (dBm): 255
  GSM Frame Number: 1109410
  Channel Type: SDCCH/8 (8)
  Antenna Number: 0
  Sub-Slot: 1
▸ Link Access Procedure, Channel Dm (LAPDm)
▾ GSM A-I/F DTAP - Ciphering Mode Command
 ▸ Protocol Discriminator: Radio Resources Management messages
  DTAP Radio Resources Management Message Type: Ciphering Mode Command (0x35)
  .... ...1 = SC: Start ciphering (1)
  .... 000. = Algorithm identifier: Cipher with algorithm A5/1 (0)
  ...0 .... = CR: IMEISV shall not be included (0)
```

```
0030  [redacted]
0040
0050
```

Algorithm identifier (gsm_a.algori... Packets: 7219 Displayed: 7219 Marked: 0 Profile: Default

Tušmobil je v času pregleda uporabljal A5/1.

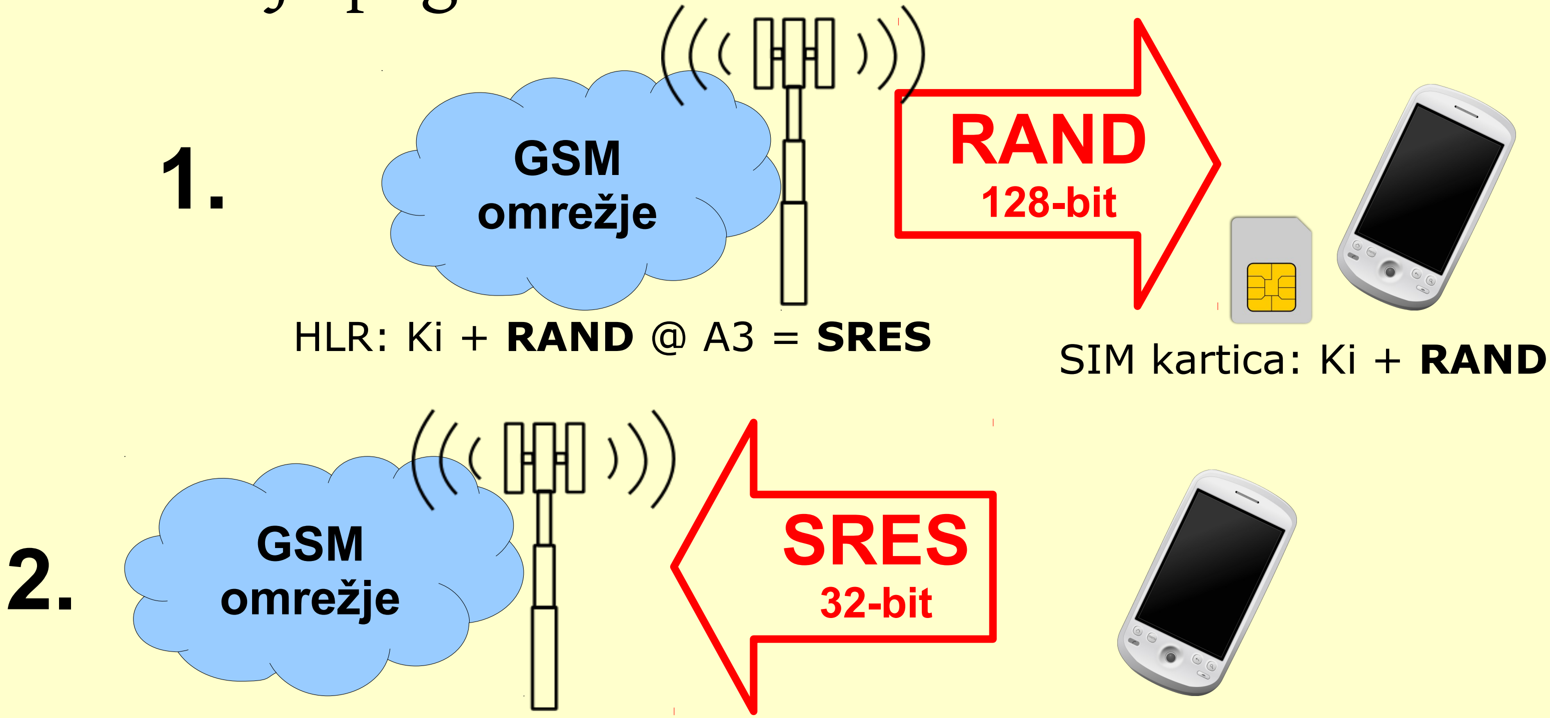
Kriptoanaliza sejnega šifrirnega ključa Kc

(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.



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

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

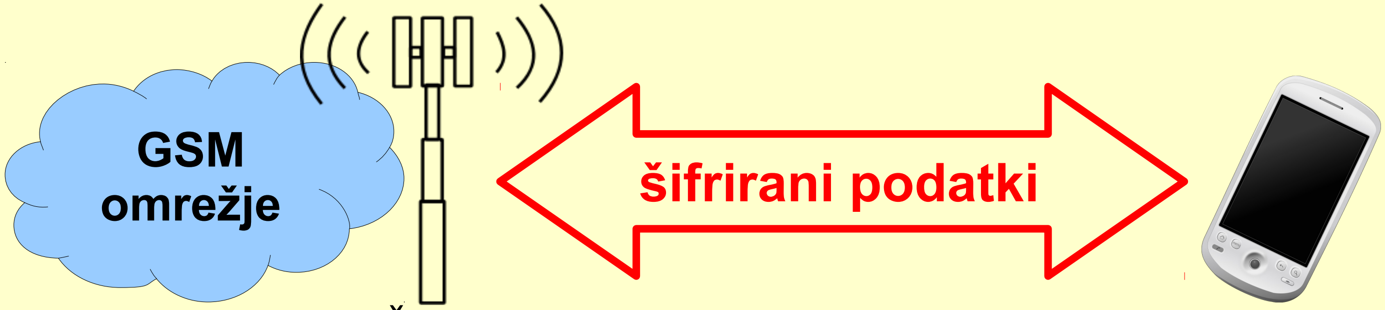
Omrežje preveri ali se sprejeti **SRES** ujema z njegovim.

Ustvarjanje sejnega ključa Kc

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

Ki + RAND @ A8 = **Kc**

4.



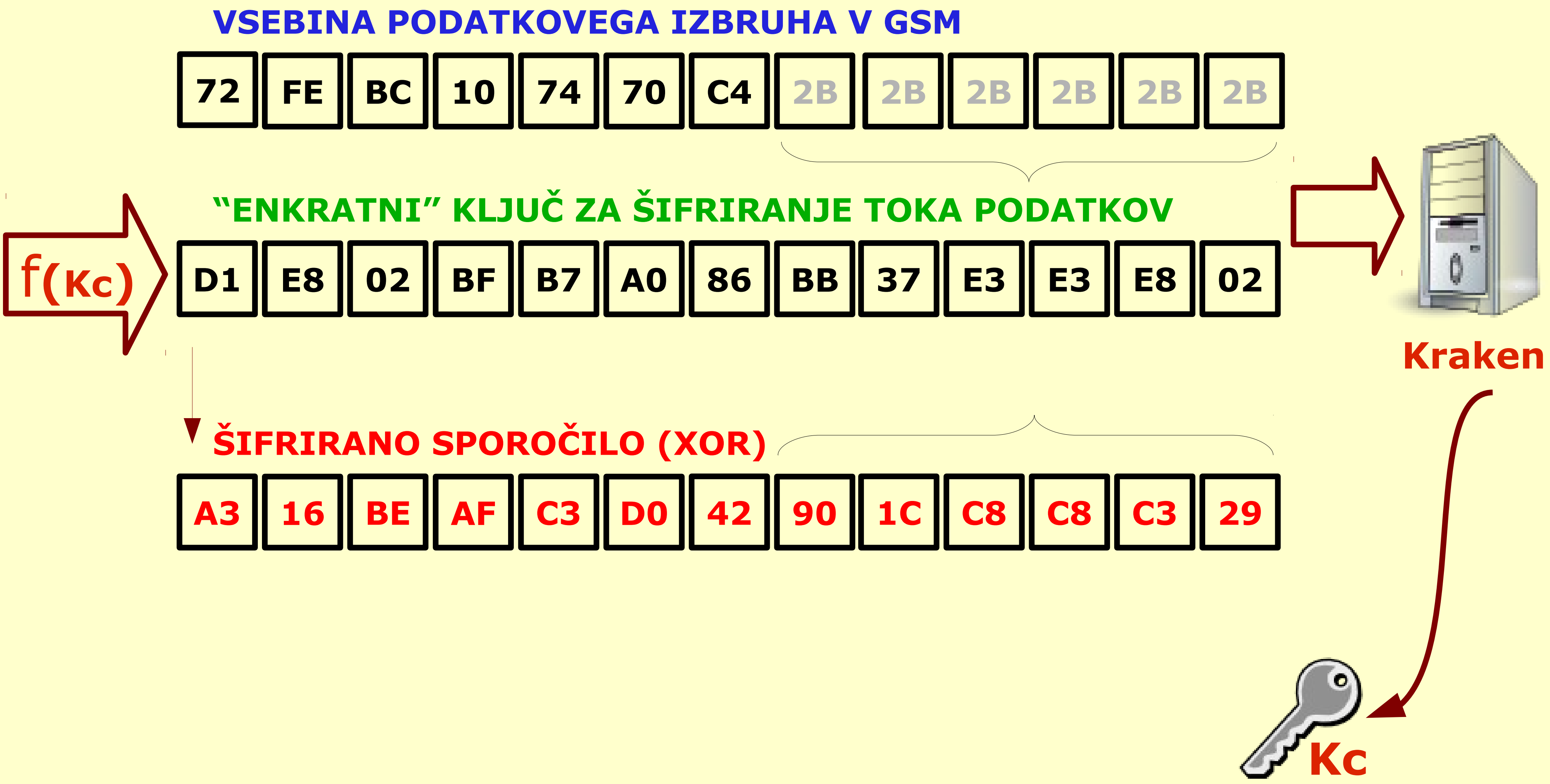
GSM omrežje

šifrirani podatki

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

“ENKRATNI” KLJUČ ZA ŠIFRIRANJE TOKA PODATKOV

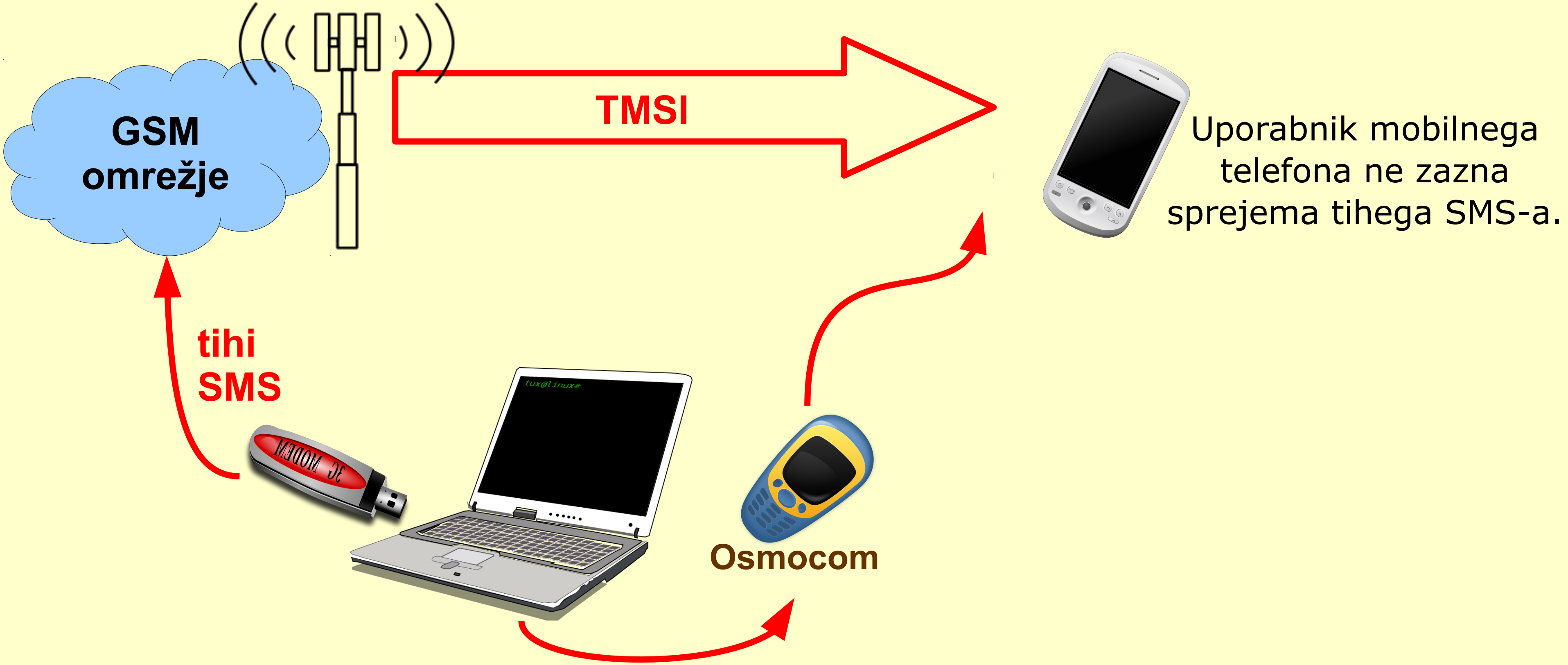
D1	E8	02	BF	B7	A0	86	BB	37	E3	E3	E8	02

ŠIFRIRANO SPOROČILO (XOR)

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

Lociranje uporabnika v mobilnem omrežju

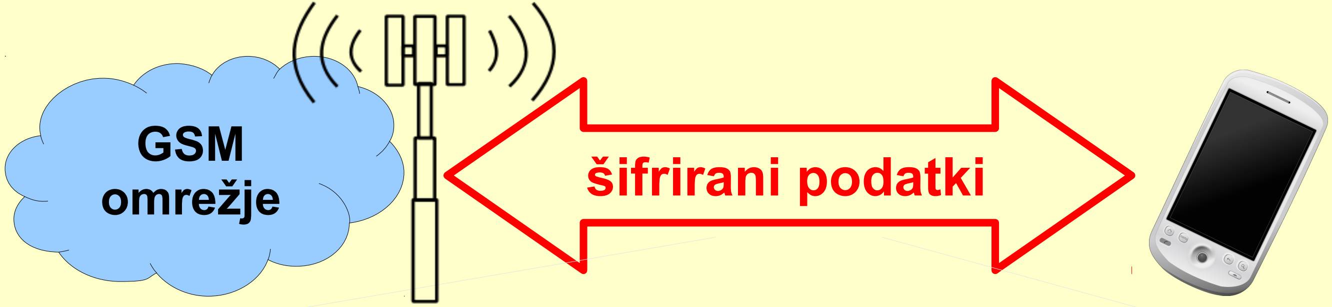
Na mobilno številko pričnemo pošiljati tihe SMS-e, hkrati na omrežju gledamo katera TMSI številka prejema šifrirane podatke.


GSM omrežje
TMSI
Uporabnik mobilnega telefona ne zazna sprejema tihega SMS-a.
tihi SMS
3G MODEM
tux@linux#
Osmocom

Zajem in kriptoanaliza A5/1

praksa

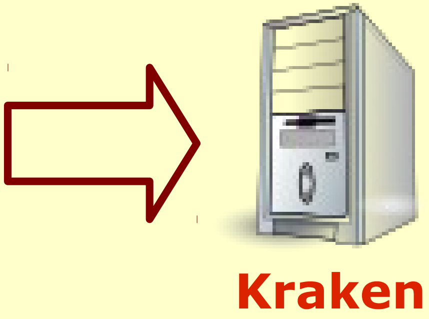
5.

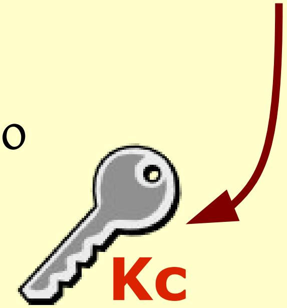


A3	16	BE	AF	C3	D0	42	90	1C	C8	C8	C3	29

VSEBINA PODATKOVEGA IZBRUHA V GSM

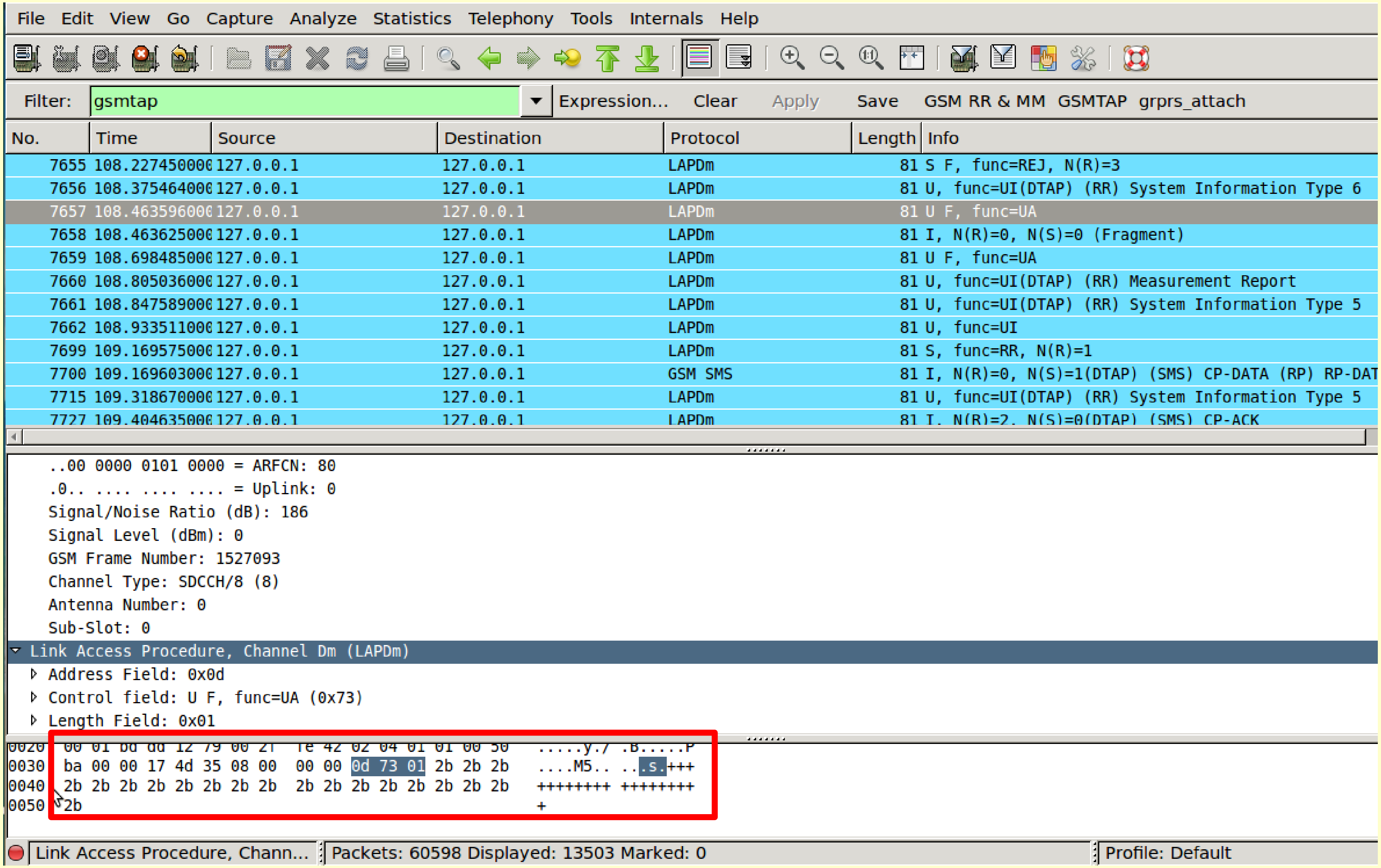
72	FE	BC	10	74	70	C4	2B	2B	2B	2B	2B	2B





- 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*)



Filter: gsmtap

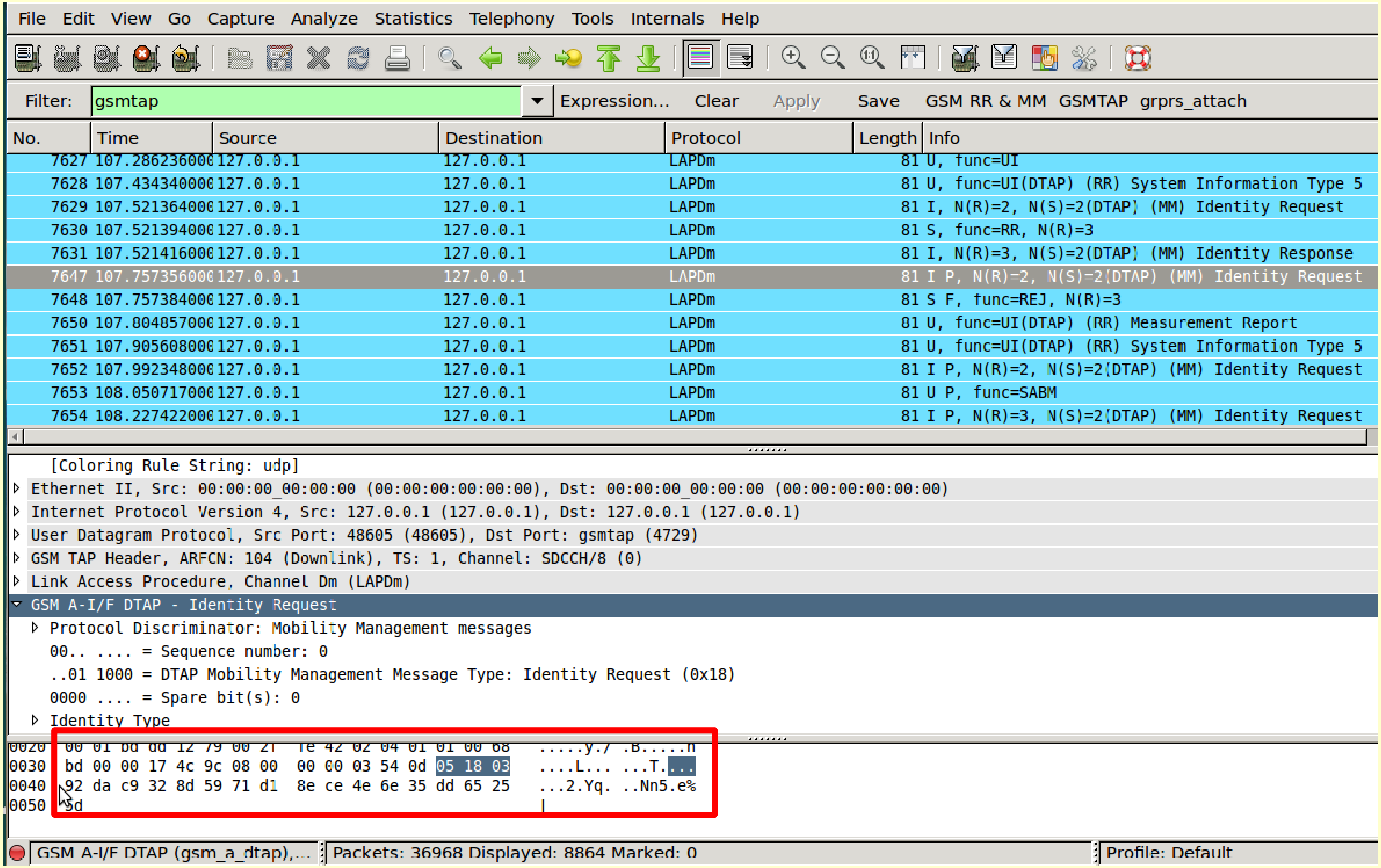
No.	Time	Source	Destination	Protocol	Length	Info
7655	108.22745000	127.0.0.1	127.0.0.1	LAPDm	81	S F, func=REJ, N(R)=3
7656	108.37546400	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) System Information Type 6
7657	108.46359600	127.0.0.1	127.0.0.1	LAPDm	81	U F, func=UA
7658	108.46362500	127.0.0.1	127.0.0.1	LAPDm	81	I, N(R)=0, N(S)=0 (Fragment)
7659	108.69848500	127.0.0.1	127.0.0.1	LAPDm	81	U F, func=UA
7660	108.80503600	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) Measurement Report
7661	108.84758900	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) System Information Type 5
7662	108.93351100	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI
7699	109.16957500	127.0.0.1	127.0.0.1	LAPDm	81	S, func=RR, N(R)=1
7700	109.16960300	127.0.0.1	127.0.0.1	GSM SMS	81	I, N(R)=0, N(S)=1(DTAP) (SMS) CP-DATA (RP) RP-DAT
7715	109.31867000	127.0.0.1	127.0.0.1	LAPDm	81	U, func=UI(DTAP) (RR) System Information Type 5
7727	109.40463500	127.0.0.1	127.0.0.1	LAPDm	81	I, N(R)=2, N(S)=0(DTAP) (SMS) CP-ACK

```
    ..00 0000 0101 0000 = ARFCN: 80
    .0.. .... .... .... = Uplink: 0
    Signal/Noise Ratio (dB): 186
    Signal Level (dBm): 0
    GSM Frame Number: 1527093
    Channel Type: SDCCH/8 (8)
    Antenna Number: 0
    Sub-Slot: 0
▿ Link Access Procedure, Channel Dm (LAPDm)
  ▹ Address Field: 0x0d
  ▹ Control field: U F, func=UA (0x73)
  ▹ Length Field: 0x01
```

```
0020  00 01 bd dd 12 79 00 2f  fe 42 02 04 01 01 00 50   .....y./ .B.....P
0030  ba 00 00 17 4d 35 08 00  00 00 0d 73 01 2b 2b 2b   ....M5.. ...s.+++
0040  2b 2b 2b 2b 2b 2b 2b 2b  2b 2b 2b 2b 2b 2b 2b 2b   ++++++++ ++++++++
0050  2b                                                 +
```

● Link Access Procedure, Chann... | Packets: 60598 Displayed: 13503 Marked: 0 | Profile: Default

Naključno zapolnjevanje
(*random padding*)


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: gsmtap
Expression... Clear Apply Save GSM RR & MM GSMTAP grprs_attach

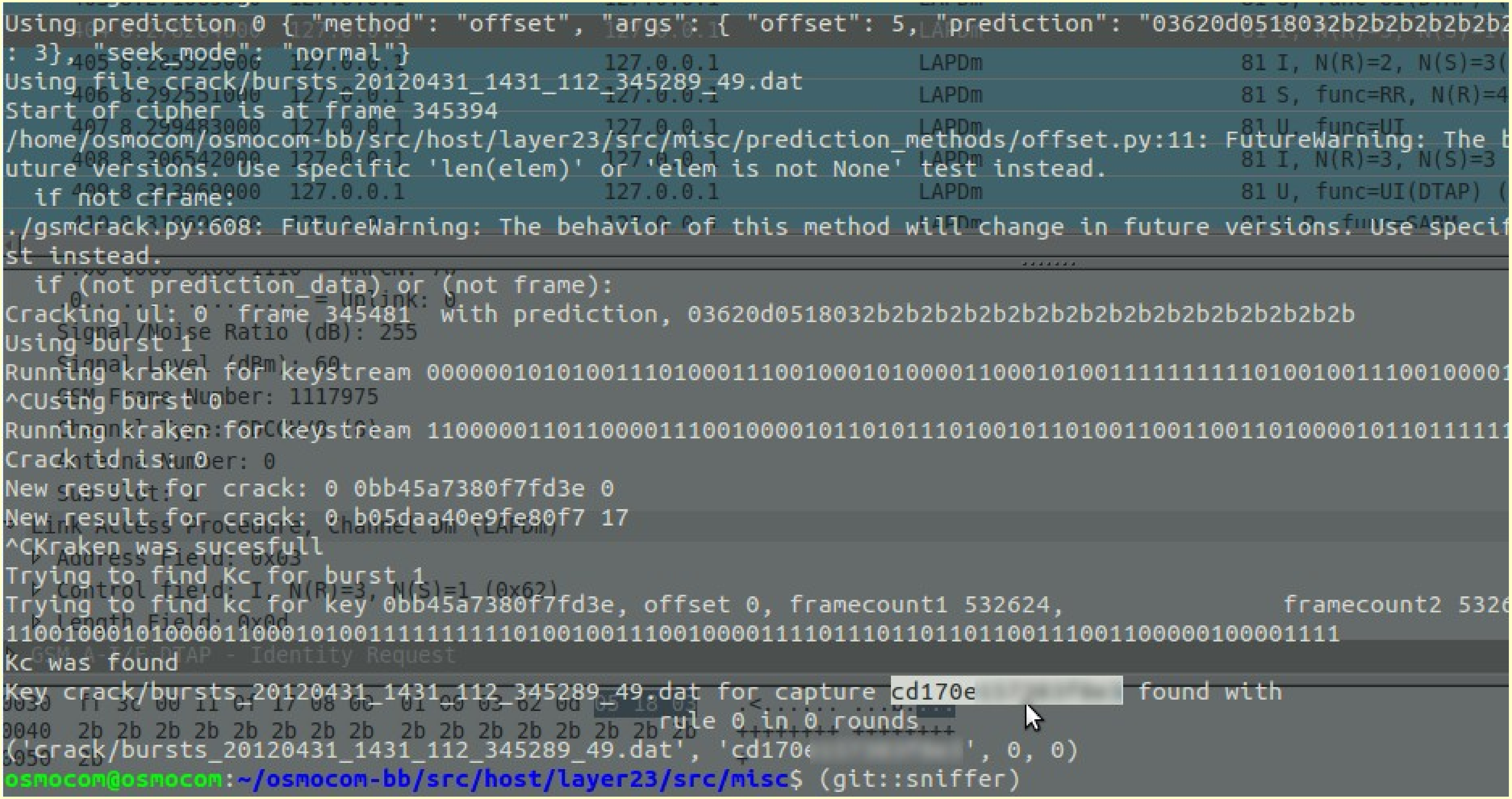
```
No.    Time            Source      Destination  Protocol  Length Info
  7627 107.286236000 127.0.0.1   127.0.0.1    LAPDm        81 U, func=UI
  7628 107.434340000 127.0.0.1   127.0.0.1    LAPDm        81 U, func=UI(DTAP) (RR) System Information Type 5
  7629 107.521364000 127.0.0.1   127.0.0.1    LAPDm        81 I, N(R)=2, N(S)=2(DTAP) (MM) Identity Request
  7630 107.521394000 127.0.0.1   127.0.0.1    LAPDm        81 S, func=RR, N(R)=3
  7631 107.521416000 127.0.0.1   127.0.0.1    LAPDm        81 I, N(R)=3, N(S)=2(DTAP) (MM) Identity Response
  7647 107.757356000 127.0.0.1   127.0.0.1    LAPDm        81 I P, N(R)=2, N(S)=2(DTAP) (MM) Identity Request
  7648 107.757384000 127.0.0.1   127.0.0.1    LAPDm        81 S F, func=REJ, N(R)=3
  7650 107.804857000 127.0.0.1   127.0.0.1    LAPDm        81 U, func=UI(DTAP) (RR) Measurement Report
  7651 107.905608000 127.0.0.1   127.0.0.1    LAPDm        81 U, func=UI(DTAP) (RR) System Information Type 5
  7652 107.992348000 127.0.0.1   127.0.0.1    LAPDm        81 I P, N(R)=2, N(S)=2(DTAP) (MM) Identity Request
  7653 108.050717000 127.0.0.1   127.0.0.1    LAPDm        81 U P, func=SABM
  7654 108.227422000 127.0.0.1   127.0.0.1    LAPDm        81 I P, N(R)=3, N(S)=2(DTAP) (MM) Identity Request
```

```
    [Coloring Rule String: udp]
▷ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▷ Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
▷ User Datagram Protocol, Src Port: 48605 (48605), Dst Port: gsmtap (4729)
▷ GSM TAP Header, ARFCN: 104 (Downlink), TS: 1, Channel: SDCCH/8 (0)
▷ Link Access Procedure, Channel Dm (LAPDm)
▽ GSM A-I/F DTAP - Identity Request
  ▷ Protocol Discriminator: Mobility Management messages
    00.. .... = Sequence number: 0
    ..01 1000 = DTAP Mobility Management Message Type: Identity Request (0x18)
    0000 .... = Spare bit(s): 0
  ▷ Identity Type
```

```
0020  00 01 bd dd 12 79 00 2f  fe 42 02 04 01 01 00 68   .....y./ .B.....h
0030  bd 00 00 17 4c 9c 08 00  00 00 03 54 0d 05 18 03   ....L... ...T....
0040  92 da c9 32 8d 59 71 d1  8e ce 4e 6e 35 dd 65 25   ...2.Yq. ..Nn5.e%
0050  5d                                                 ]
```

GSM A-I/F DTAP (gsm_a_dtap),... Packets: 36968 Displayed: 8864 Marked: 0 Profile: Default

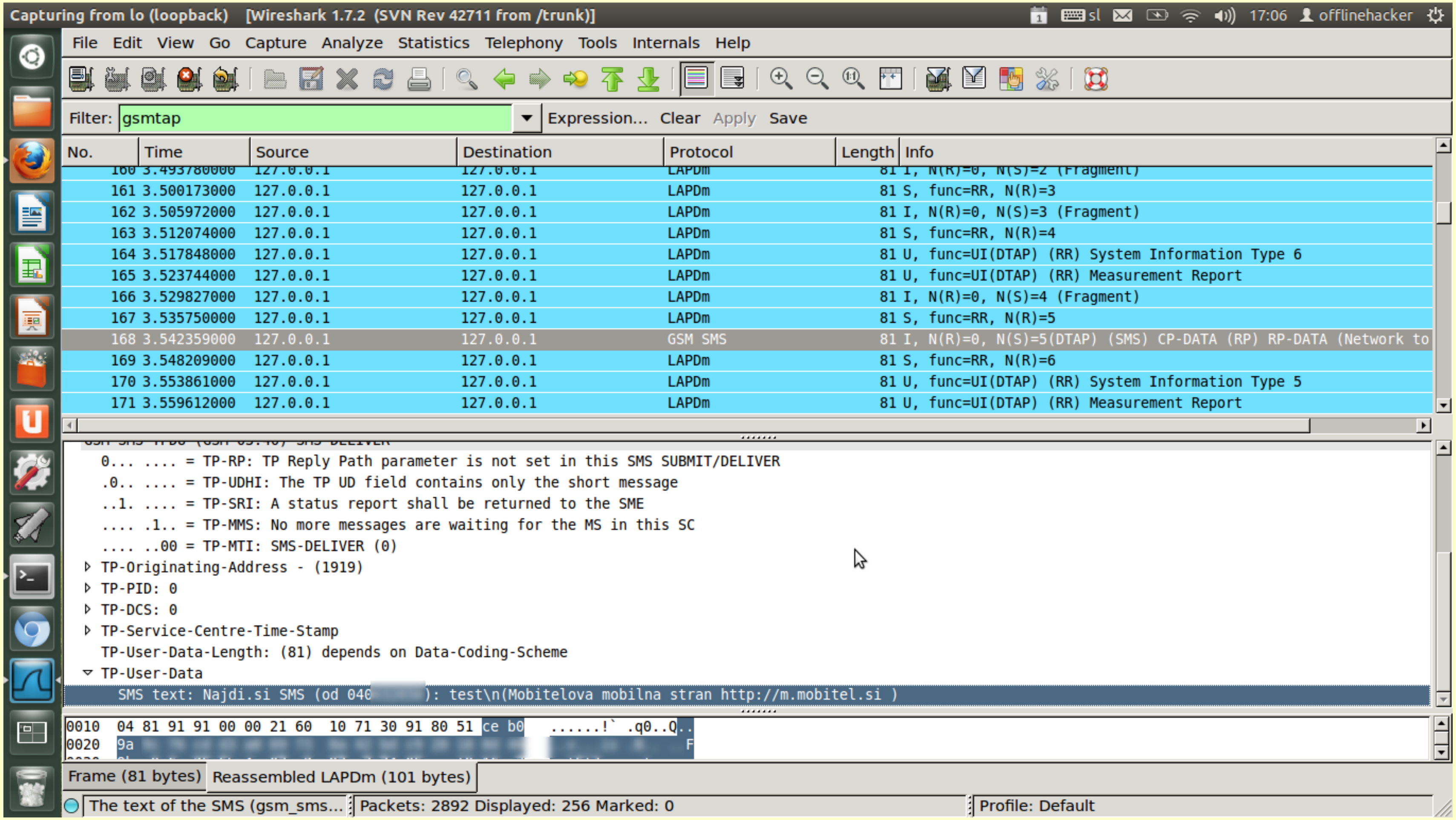
Razbijanje A5/1 sejnega šifrirnega ključa Kc v praksi



```
Using prediction 0 { "method": "offset", "args": { "offset": 5, "prediction": "03620d0518032b2b2b2b2b2
: 3}, "seek_mode": "normal"}
Using file crack/bursts_20120431_1431_112_345289_49.dat
Start of cipher is at frame 345394
/home/osmocom/osmocom-bb/src/host/layer23/src/misc/prediction_methods/offset.py:11: FutureWarning: The b
uture versions. Use specific 'len(elem)' or 'elem is not None' test instead.
  if not cframe:
./gsmcrack.py:608: FutureWarning: The behavior of this method will change in future versions. Use specif
st instead.
  if (not prediction_data) or (not frame):
Cracking ul: 0  frame 345481  with prediction, 03620d0518032b2b2b2b2b2b2b2b2b2b2b2b2b2b
Using burst 1
Running kraken for keystream 00000101010011101000111001000101000011000101001111111110100100111001000001
^CUsing burst 0
Running kraken for keystream 11000001101100001110010000101101011101001011010011001100110100001011011111
Crack id is: 0
New result for crack: 0 0bb45a7380f7fd3e 0
New result for crack: 0 b05daa40e9fe80f7 17
^CKraken was sucesfull
Trying to find Kc for burst 1
Trying to find kc for key 0bb45a7380f7fd3e, offset 0, framecount1 532624,            framecount2 5326
1100100010100001100010100111111111101001001110010000111101110110110110011100110000010000111l
Kc was found
Key crack/bursts_20120431_1431_112_345289_49.dat for capture cd170e[redacted] found with
                                                 rule 0 in 0 rounds
('crack/bursts_20120431_1431_112_345289_49.dat', 'cd170e[redacted]', 0, 0)
osmocom@osmocom:~/osmocom-bb/src/host/layer23/src/misc$ (git::sniffer)
```

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

Razbijanje A5/1 sejnega šifrirnega ključa Kc v praksi


Capturing from lo (loopback) [Wireshark 1.7.2 (SVN Rev 42711 from /trunk)]
sl
17:06
offlinehacker
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: gsmtap
Expression... Clear Apply Save
Frame (81 bytes)
Reassembled LAPDm (101 bytes)
The text of the SMS (gsm_sms...
Packets: 2892 Displayed: 256 Marked: 0
Profile: Default

```
No.  Time         Source      Destination  Protocol  Length Info
 160 3.493780000  127.0.0.1   127.0.0.1    LAPDm         81 I, N(R)=0, N(S)=2 (Fragment)
 161 3.500173000  127.0.0.1   127.0.0.1    LAPDm         81 S, func=RR, N(R)=3
 162 3.505972000  127.0.0.1   127.0.0.1    LAPDm         81 I, N(R)=0, N(S)=3 (Fragment)
 163 3.512074000  127.0.0.1   127.0.0.1    LAPDm         81 S, func=RR, N(R)=4
 164 3.517848000  127.0.0.1   127.0.0.1    LAPDm         81 U, func=UI(DTAP) (RR) System Information Type 6
 165 3.523744000  127.0.0.1   127.0.0.1    LAPDm         81 U, func=UI(DTAP) (RR) Measurement Report
 166 3.529827000  127.0.0.1   127.0.0.1    LAPDm         81 I, N(R)=0, N(S)=4 (Fragment)
 167 3.535750000  127.0.0.1   127.0.0.1    LAPDm         81 S, func=RR, N(R)=5
 168 3.542359000  127.0.0.1   127.0.0.1    GSM SMS       81 I, N(R)=0, N(S)=5(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to
 169 3.548209000  127.0.0.1   127.0.0.1    LAPDm         81 S, func=RR, N(R)=6
 170 3.553861000  127.0.0.1   127.0.0.1    LAPDm         81 U, func=UI(DTAP) (RR) System Information Type 5
 171 3.559612000  127.0.0.1   127.0.0.1    LAPDm         81 U, func=UI(DTAP) (RR) Measurement Report
```

```
  0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
  .0.. .... = TP-UDHI: The TP UD field contains only the short message
  ..1. .... = TP-SRI: A status report shall be returned to the SME
  .... .1.. = TP-MMS: No more messages are waiting for the MS in this SC
  .... ..00 = TP-MTI: SMS-DELIVER (0)
▷ TP-Originating-Address - (1919)
▷ TP-PID: 0
▷ TP-DCS: 0
▷ TP-Service-Centre-Time-Stamp
  TP-User-Data-Length: (81) depends on Data-Coding-Scheme
▽ TP-User-Data
    SMS text: Najdi.si SMS (od 040[redacted]): test\n(Mobitelova mobilna stran http://m.mobitel.si )
```

```
0010  04 81 91 91 00 00 21 60  10 71 30 91 80 51 ce b0   ......!` .q0..Q..
0020  9a [redacted]                                       F
```

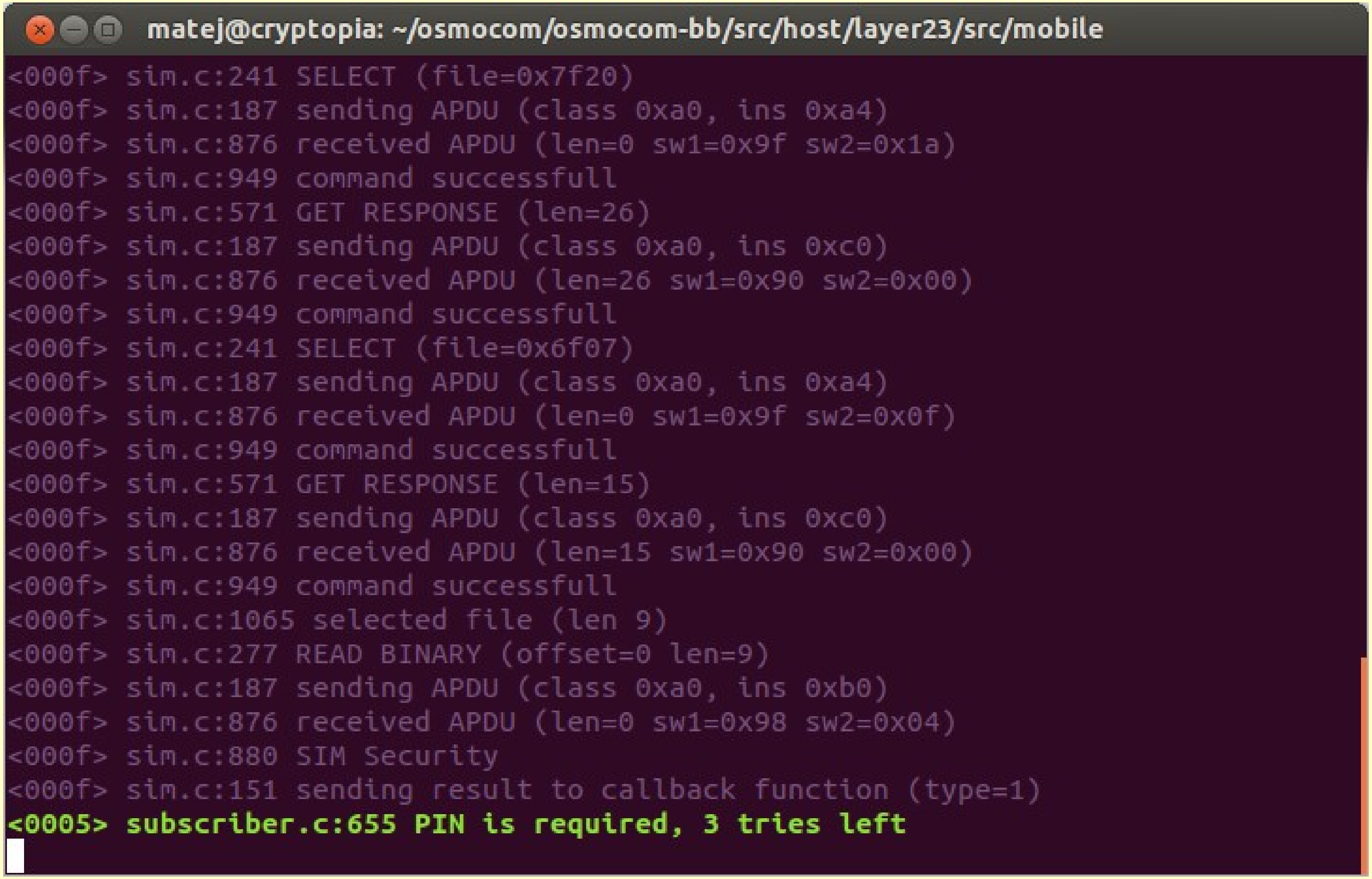
… in dešifrirano SMS sporočilo (prejeto preko 2G).
Program *gsmcrack.py* samodejno identificira TMSI številko na podlagi klicne številke (s pomočjo pošiljanja tihih SMS sporočil), ko imamo TMSI tarče pa aplikacija zna samodejno slediti telefonu na s strani bazne postaje dodeljeni kanal in posneti šifrirano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

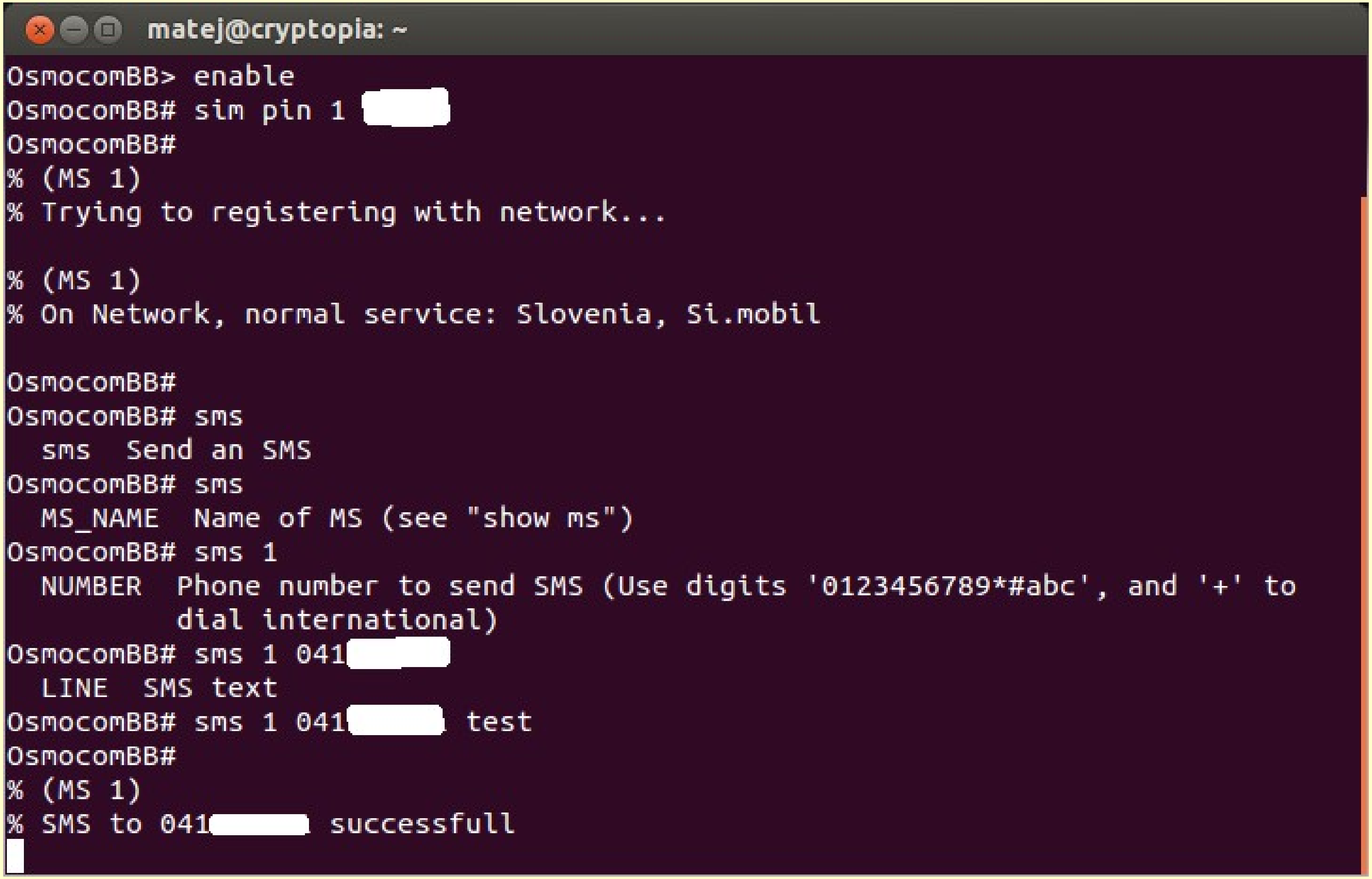


matej@cryptopia: ~/osmocom/osmocom-bb/src/host/layer23/src/mobile

```
<000f> sim.c:241 SELECT (file=0x7f20)
<000f> sim.c:187 sending APDU (class 0xa0, ins 0xa4)
<000f> sim.c:876 received APDU (len=0 sw1=0x9f sw2=0x1a)
<000f> sim.c:949 command successfull
<000f> sim.c:571 GET RESPONSE (len=26)
<000f> sim.c:187 sending APDU (class 0xa0, ins 0xc0)
<000f> sim.c:876 received APDU (len=26 sw1=0x90 sw2=0x00)
<000f> sim.c:949 command successfull
<000f> sim.c:241 SELECT (file=0x6f07)
<000f> sim.c:187 sending APDU (class 0xa0, ins 0xa4)
<000f> sim.c:876 received APDU (len=0 sw1=0x9f sw2=0x0f)
<000f> sim.c:949 command successfull
<000f> sim.c:571 GET RESPONSE (len=15)
<000f> sim.c:187 sending APDU (class 0xa0, ins 0xc0)
<000f> sim.c:876 received APDU (len=15 sw1=0x90 sw2=0x00)
<000f> sim.c:949 command successfull
<000f> sim.c:1065 selected file (len 9)
<000f> sim.c:277 READ BINARY (offset=0 len=9)
<000f> sim.c:187 sending APDU (class 0xa0, ins 0xb0)
<000f> sim.c:876 received APDU (len=0 sw1=0x98 sw2=0x04)
<000f> sim.c:880 SIM Security
<000f> sim.c:151 sending result to callback function (type=1)
<0005> subscriber.c:655 PIN is required, 3 tries left
```

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

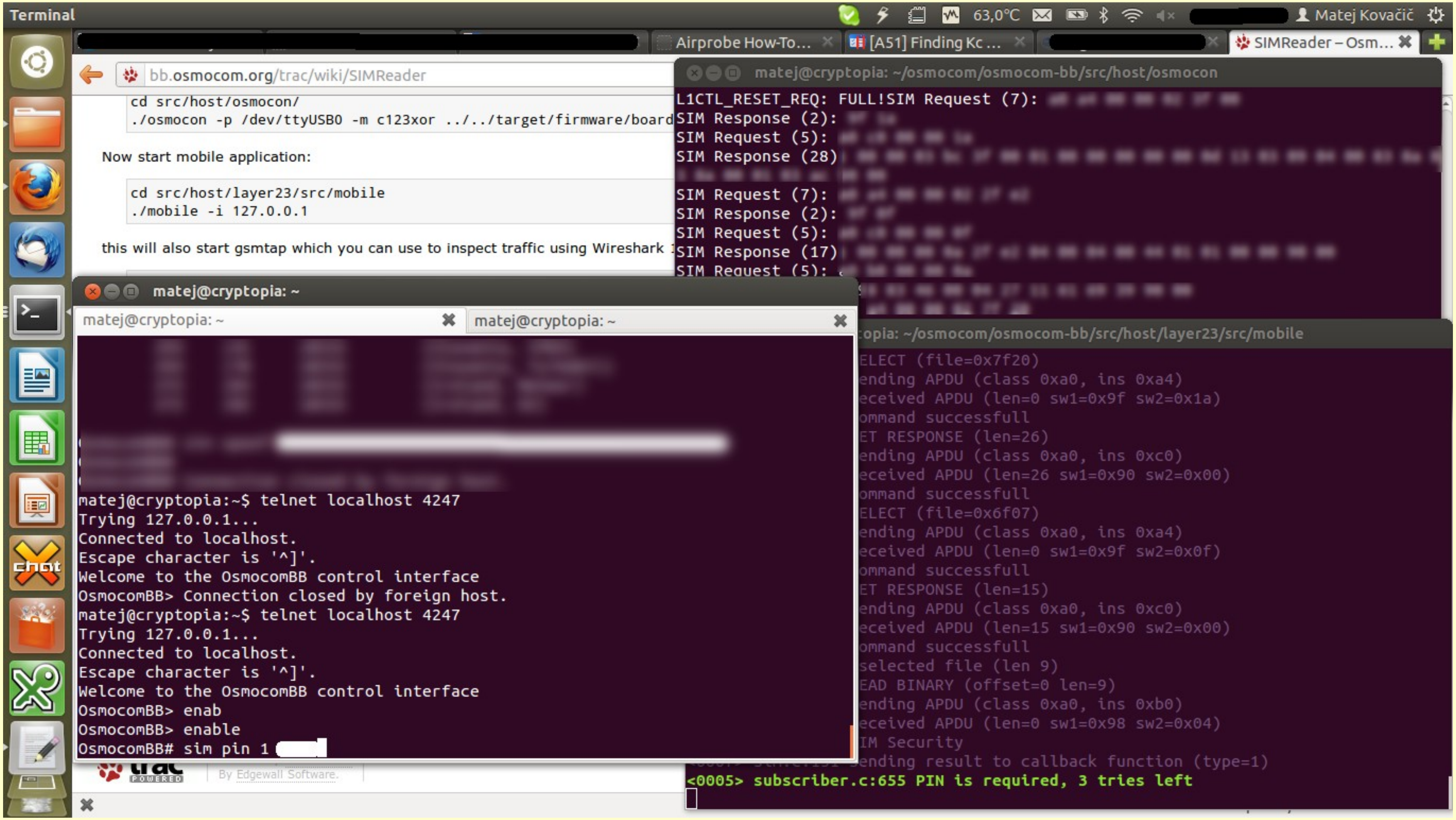
Aplikacija *mobile*



```
OsmocomBB> enable
OsmocomBB# sim pin 1 [redacted]
OsmocomBB#
% (MS 1)
% Trying to registering with network...

% (MS 1)
% On Network, normal service: Slovenia, Si.mobil

OsmocomBB#
OsmocomBB# sms
  sms  Send an SMS
OsmocomBB# sms
  MS_NAME  Name of MS (see "show ms")
OsmocomBB# sms 1
  NUMBER  Phone number to send SMS (Use digits '0123456789*#abc', and '+' to
          dial international)
OsmocomBB# sms 1 041[redacted]
  LINE  SMS text
OsmocomBB# sms 1 041[redacted] test
OsmocomBB#
% (MS 1)
% SMS to 041[redacted] successfull
```

Pošiljanje SMS sporočila iz aplikacije *mobile*.

Aplikacija *mobile*



```
cd src/host/osmocon/
./osmocon -p /dev/ttyUSB0 -m c123xor ../../target/firmware/board
```

Now start mobile application:

```
cd src/host/layer23/src/mobile
./mobile -i 127.0.0.1
```

this will also start gsmtap which you can use to inspect traffic using Wireshark

```
L1CTL_RESET_REQ: FULL!SIM Request (7): [redacted]
SIM Response (2): [redacted]
SIM Request (5): [redacted]
SIM Response (28) [redacted]
SIM Request (7): [redacted]
SIM Response (2): [redacted]
SIM Request (5): [redacted]
SIM Response (17) [redacted]
SIM Request (5): [redacted]
```

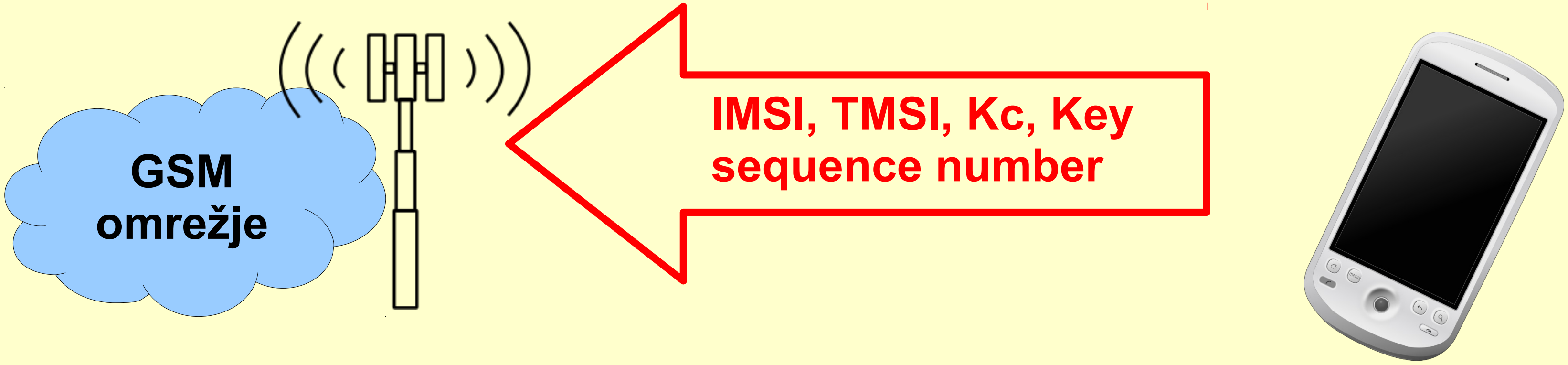
```
[redacted]
matej@cryptopia:~$ telnet localhost 4247
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Welcome to the OsmocomBB control interface
OsmocomBB> Connection closed by foreign host.
matej@cryptopia:~$ telnet localhost 4247
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Welcome to the OsmocomBB control interface
OsmocomBB> enab
OsmocomBB> enable
OsmocomBB# sim pin 1 [redacted]
```

```
ELECT (file=0x7f20)
ending APDU (class 0xa0, ins 0xa4)
eceived APDU (len=0 sw1=0x9f sw2=0x1a)
ommand successfull
ET RESPONSE (len=26)
ending APDU (class 0xa0, ins 0xc0)
eceived APDU (len=26 sw1=0x90 sw2=0x00)
ommand successfull
ELECT (file=0x6f07)
ending APDU (class 0xa0, ins 0xa4)
eceived APDU (len=0 sw1=0x9f sw2=0x0f)
ommand successfull
ET RESPONSE (len=15)
ending APDU (class 0xa0, ins 0xc0)
eceived APDU (len=15 sw1=0x90 sw2=0x00)
ommand successfull
selected file (len 9)
EAD BINARY (offset=0 len=9)
ending APDU (class 0xa0, ins 0xb0)
eceived APDU (len=0 sw1=0x98 sw2=0x04)
IM Security
ending result to callback function (type=1)
<0005> subscriber.c:655 PIN is required, 3 tries left
```

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*).



GSM omrežje

IMSI, TMSI, Kc, Key sequence number

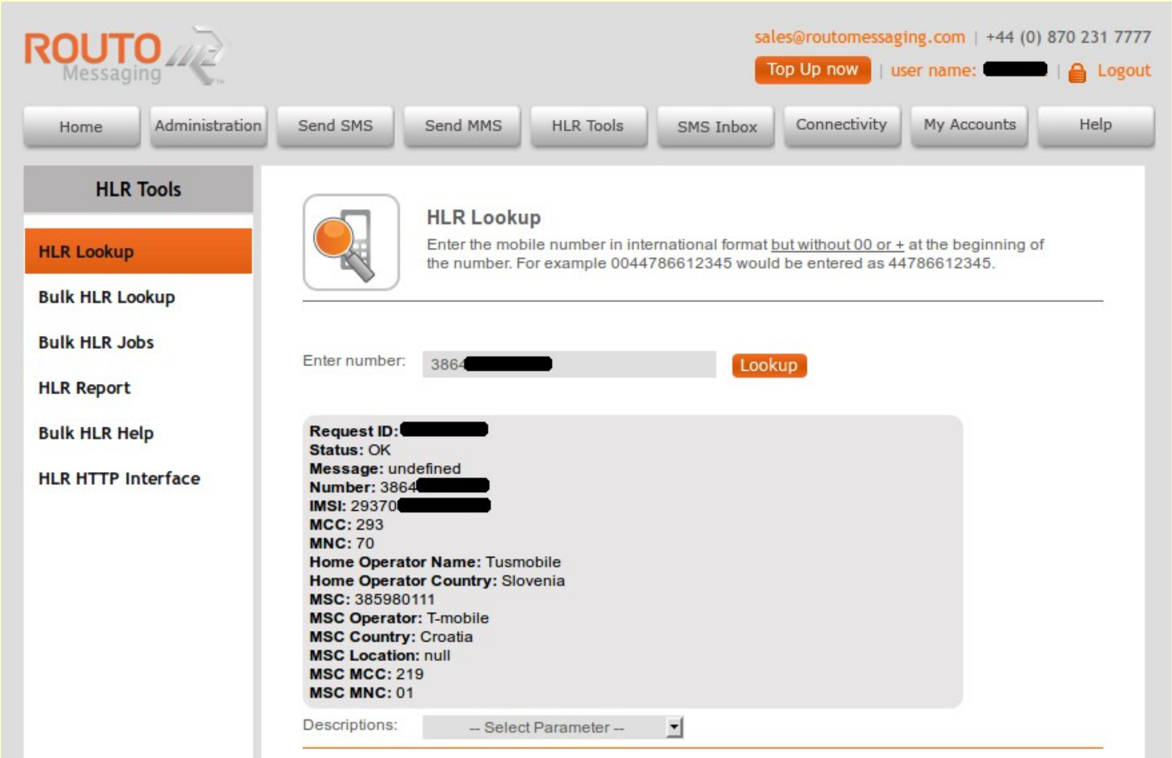
Ponarejanje mobilne identitete

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.



HLR Lookup

Enter the mobile number in international format but without 00 or + at the beginning of the number. For example 0044786612345 would be entered as 44786612345.

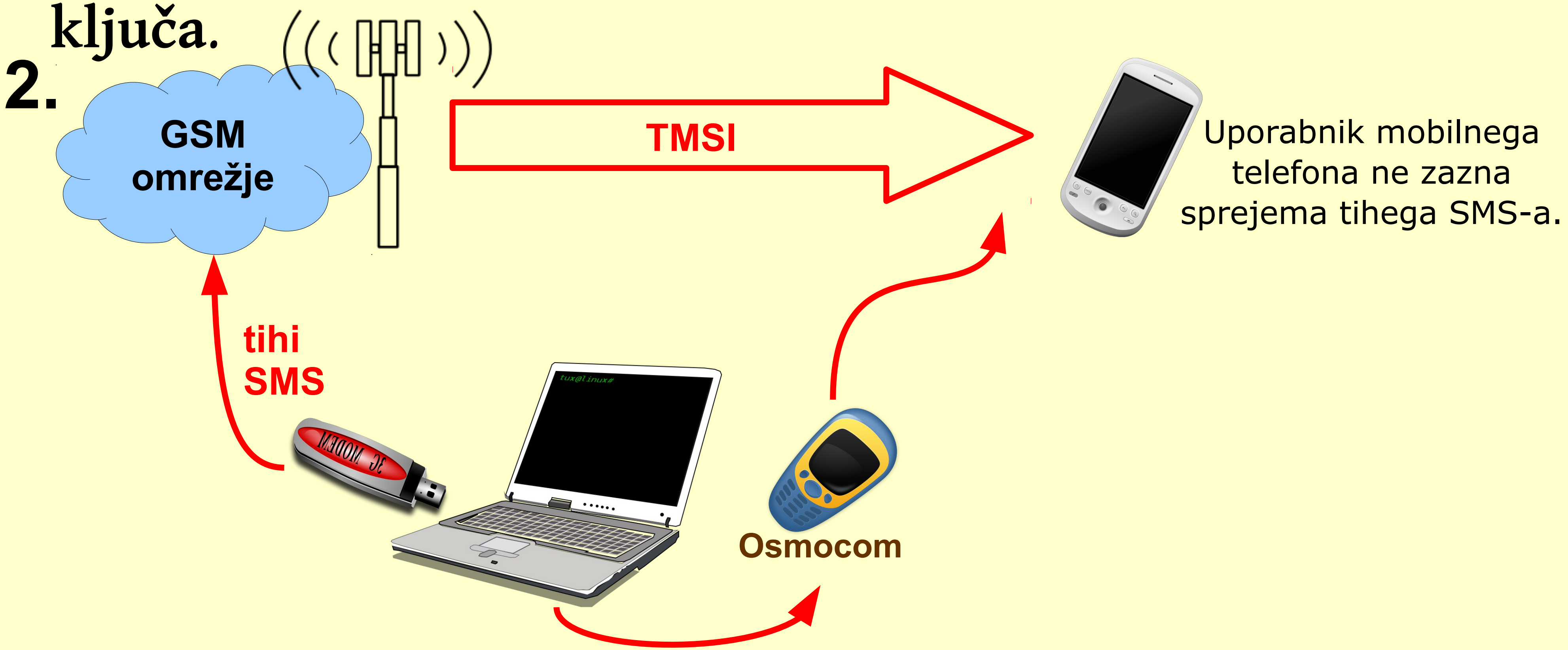
Enter number: 3864[redacted] Lookup

Request ID: [redacted]
Status: OK
Message: undefined
Number: 3864[redacted]
IMSI: 29370[redacted]
MCC: 293
MNC: 70
Home Operator Name: Tusmobile
Home Operator Country: Slovenia
MSC: 385980111
MSC Operator: T-mobile
MSC Country: Croatia
MSC Location: null
MSC MCC: 219
MSC MNC: 01

Descriptions: -- Select Parameter --

Razkritje TMSI številke

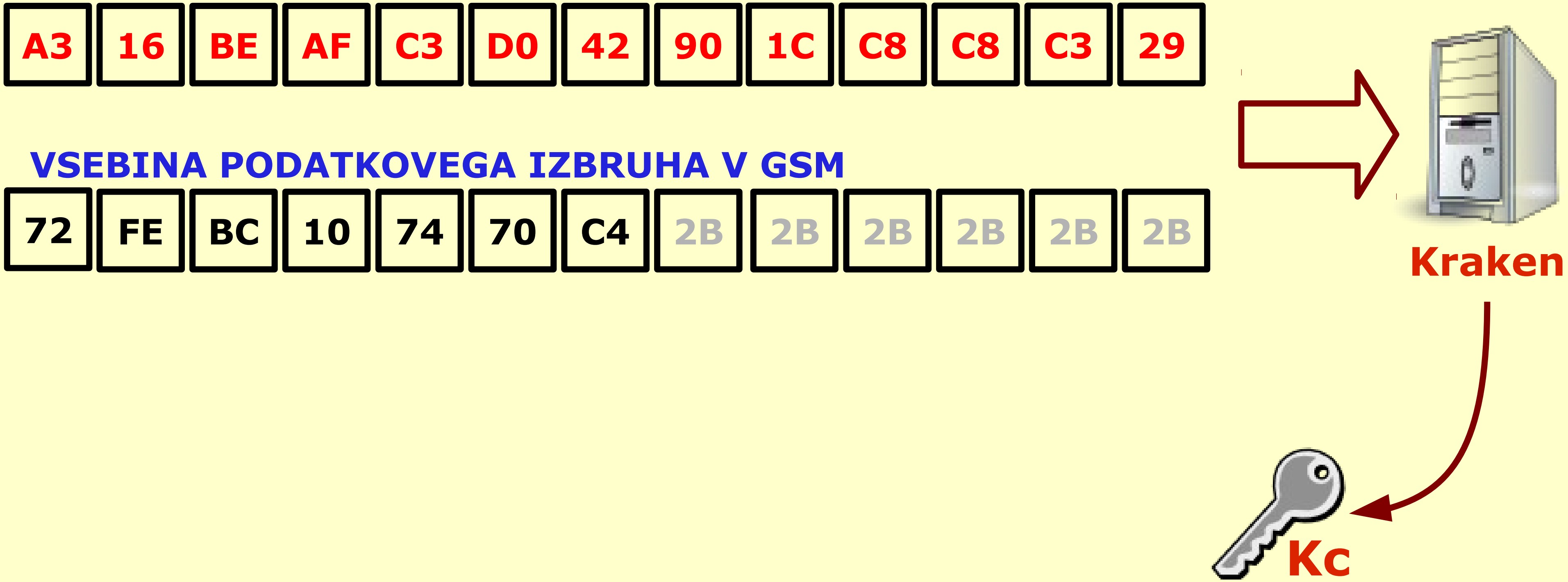
S pošiljanjem tihih SMS sporočil na telefonsko številko tarče lociramo še njeno **TMSI številko.** Hkrati prestrežemo podatkovni paketek in **sekvenčno številko ključa.**


2.
GSM
omrežje
TMSI
Uporabnik mobilnega telefona ne zazna sprejema tihega SMS-a.
tihi
SMS
3G MODEM
tux@linux#
Osmocom

Pridobitev Kc

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

3.

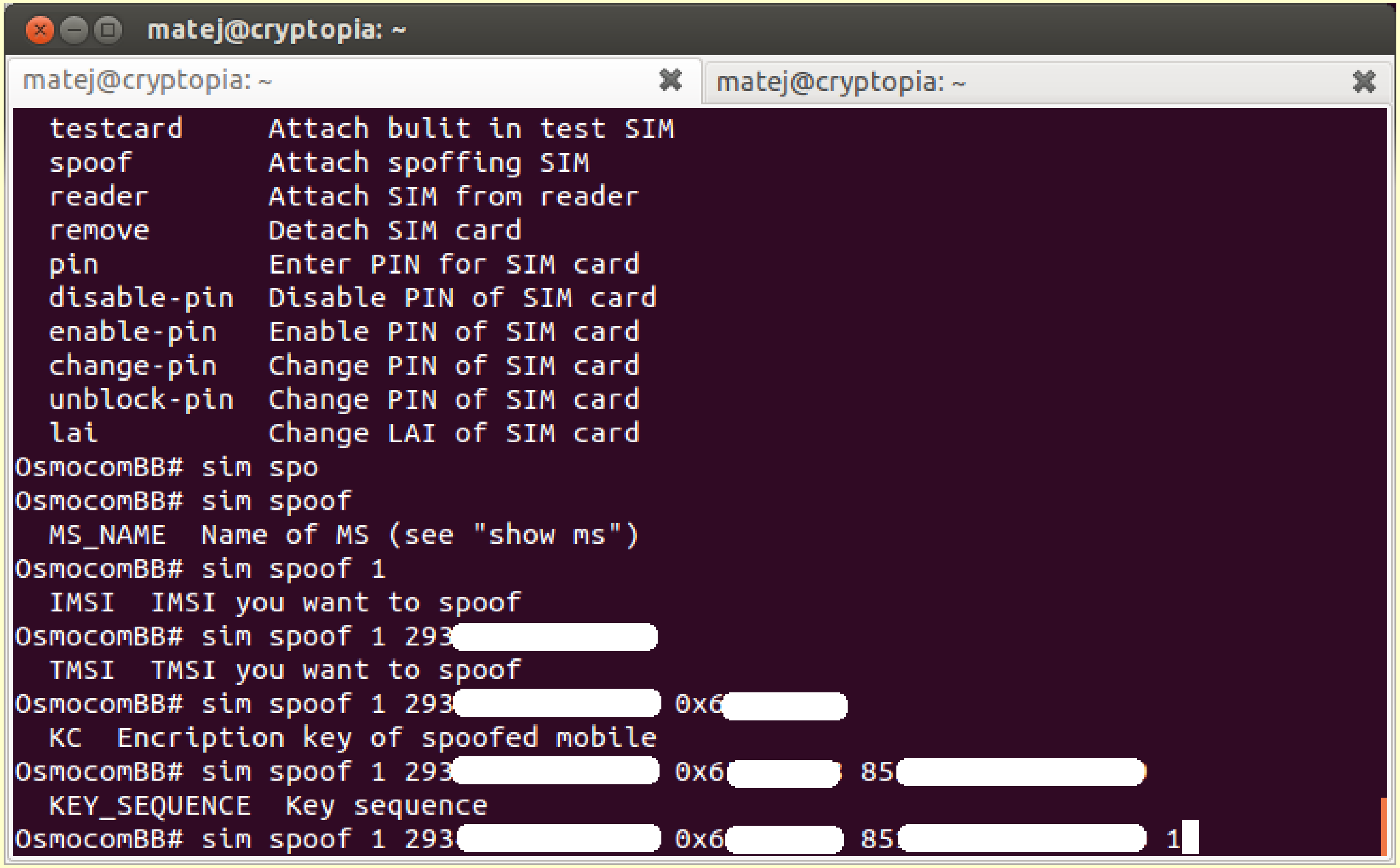


A3 16 BE AF C3 D0 42 90 1C C8 C8 C3 29

VSEBINA PODATKOVEGA IZBRUHA V GSM

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

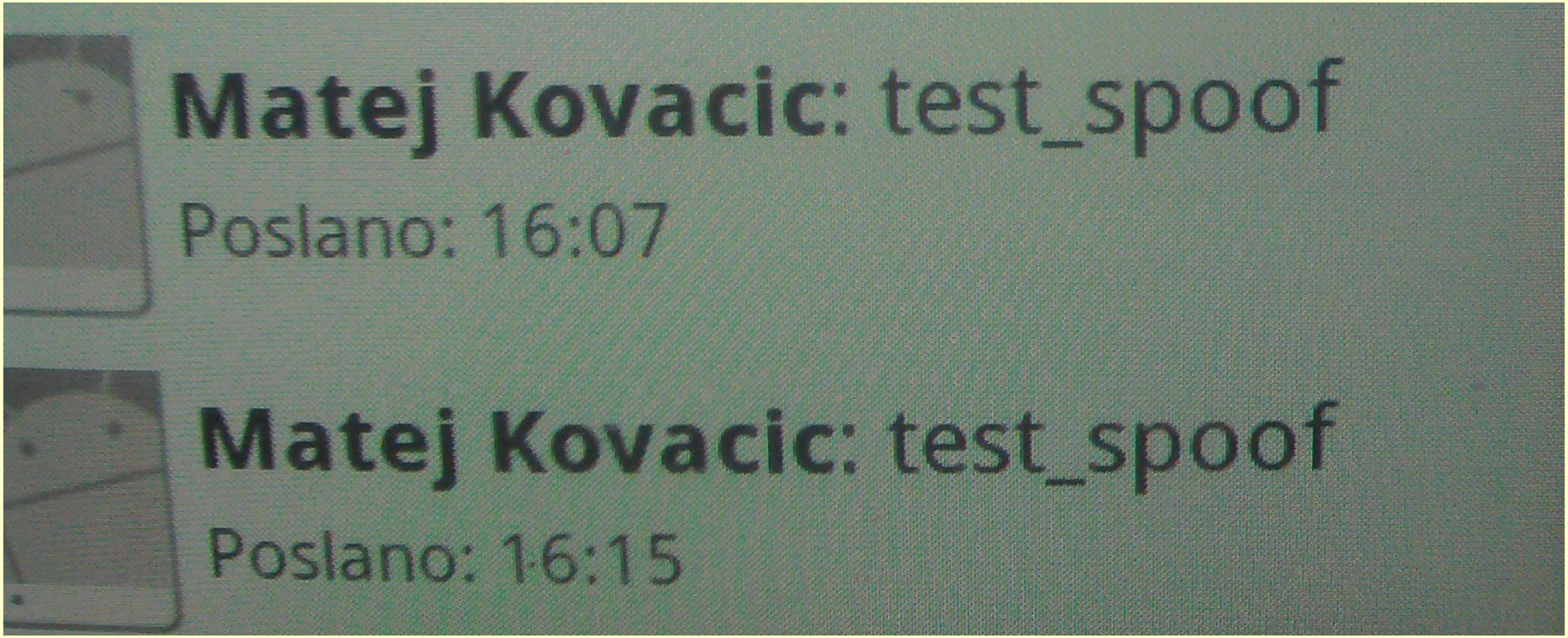
“SIM spoof”



```
  testcard      Attach bulit in test SIM
  spoof         Attach spoffing SIM
  reader        Attach SIM from reader
  remove        Detach SIM card
  pin           Enter PIN for SIM card
  disable-pin   Disable PIN of SIM card
  enable-pin    Enable PIN of SIM card
  change-pin    Change PIN of SIM card
  unblock-pin   Change PIN of SIM card
  lai           Change LAI of SIM card
OsmocomBB# sim spo
OsmocomBB# sim spoof
  MS_NAME   Name of MS (see "show ms")
OsmocomBB# sim spoof 1
  IMSI   IMSI you want to spoof
OsmocomBB# sim spoof 1 293[redacted]
  TMSI   TMSI you want to spoof
OsmocomBB# sim spoof 1 293[redacted] 0x6[redacted]
  KC  Encription key of spoofed mobile
OsmocomBB# sim spoof 1 293[redacted] 0x6[redacted] 85[redacted]
  KEY_SEQUENCE  Key sequence
OsmocomBB# sim spoof 1 293[redacted] 0x6[redacted] 85[redacted] 1
```

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



Matej Kovacic: test_spoof

Poslano: 16:07

Matej Kovacic: test_spoof

Poslano: 16:15

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.

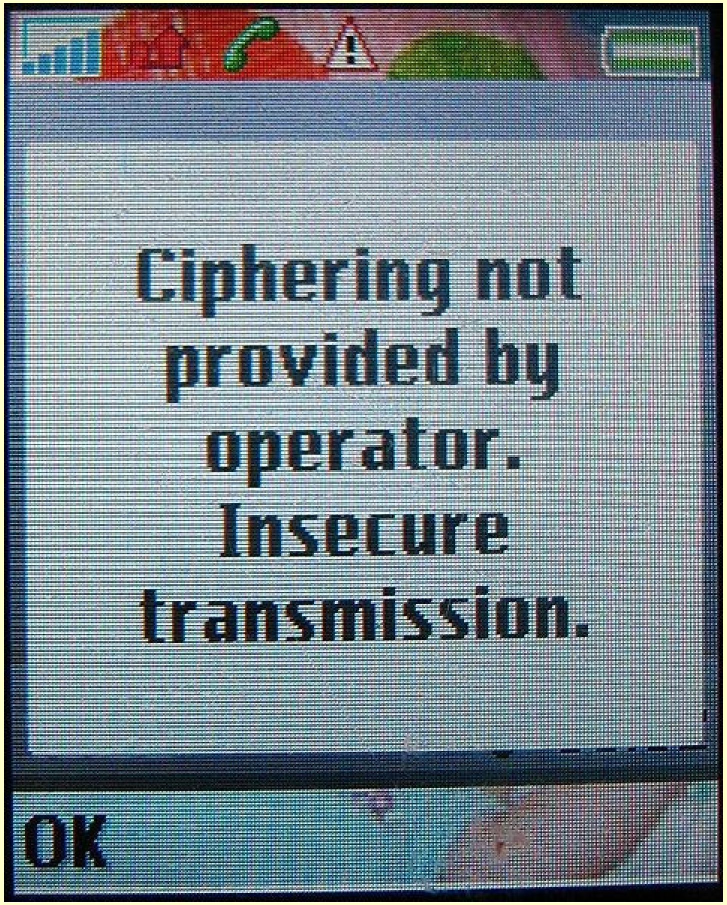
Problem: mobilno omrežje se ne avtenticira mobilnemu telefonu

- 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")



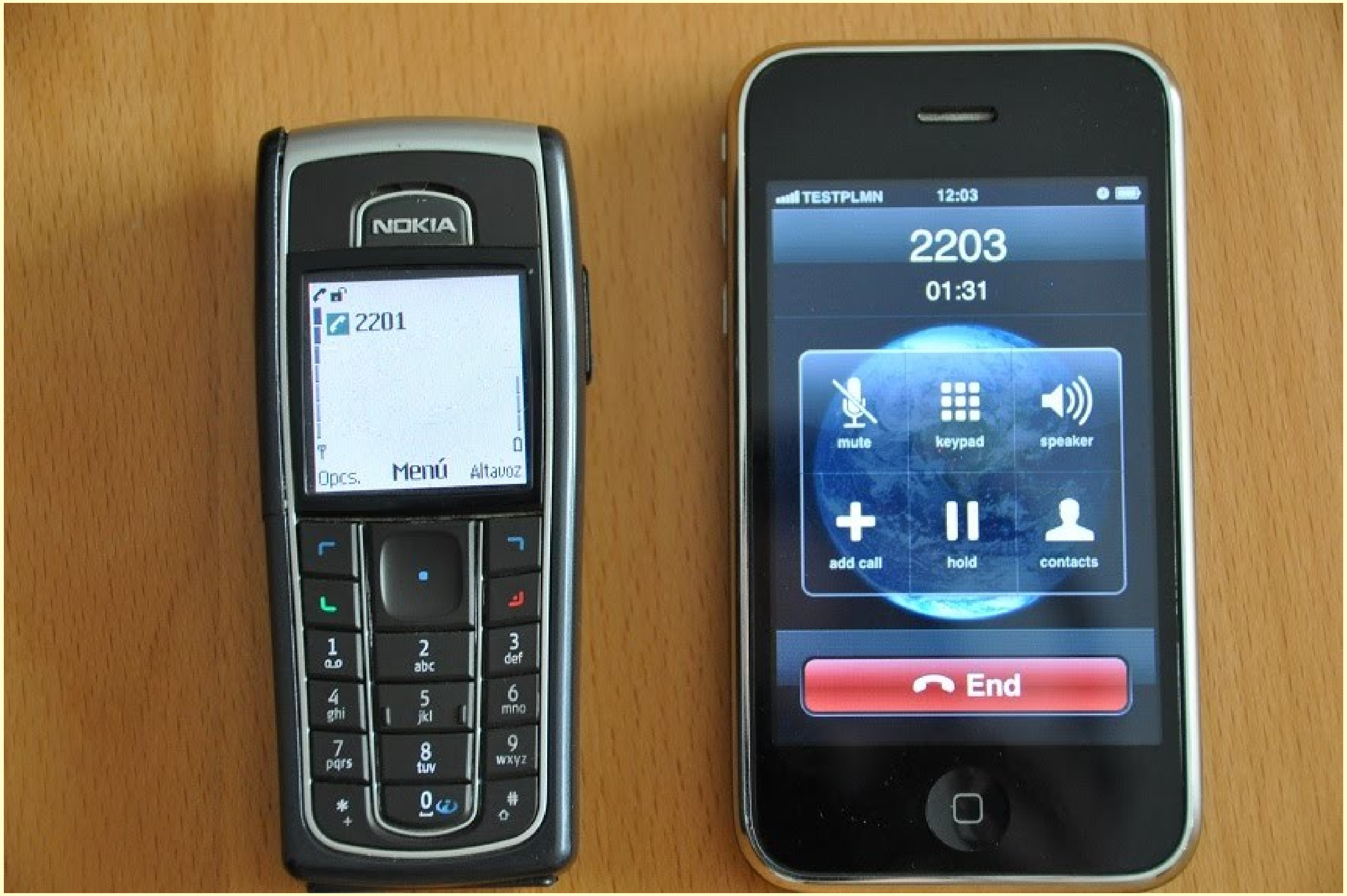
Ciphering not provided by operator. Insecure transmission.

Problem: mobilno omrežje se ne avtenticira mobilnemu telefonu

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

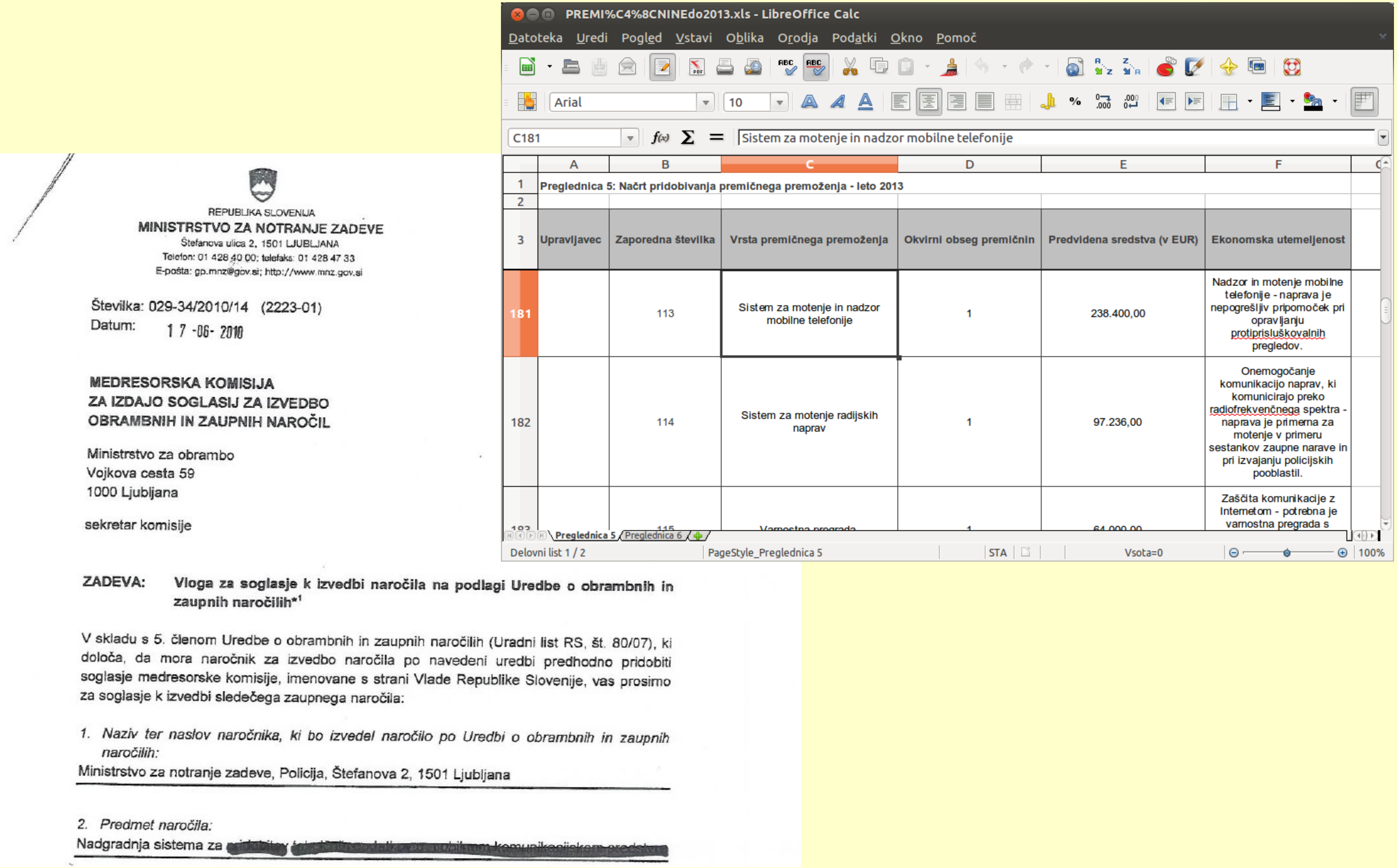
> The ciphering indicator feature may be disabled by the home network operator setting data in the SIM/USIM. If this feature is not disabled by the SIM, then whenever a connection is in place, which is, or becomes unenciphered, an indication shall be given to the user. Ciphering itself is unaffected 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…



PREMI%C4%8CNINEdo2013.xls - LibreOffice Calc
Datoteka Uredi Pogled Vstavi Oblika Orodja Podatki Okno Pomoč
Arial
10
Delovni list 1 / 2
PageStyle_Preglednica 5
STA
Vsota=0
100%
Preglednica 5
Preglednica 6

C181 | Sistem za motenje in nadzor mobilne telefonije

	A	B	C	D	E	F
1	Preglednica 5: Načrt pridobivanja premičnega premoženja - leto 2013					
2						
3	Upravljavec	Zaporedna številka	Vrsta premičnega premoženja	Okvirni obseg premičnin	Predvidena sredstva (v EUR)	Ekonomska utemeljenost
181		113	Sistem za motenje in nadzor mobilne telefonije	1	238.400,00	Nadzor in motenje mobilne telefonije - naprava je nepogrešljiv pripomoček pri opravljanju protiprisluškovalnih pregledov.
182		114	Sistem za motenje radijskih naprav	1	97.236,00	Onemogočanje komunikacijo naprav, ki komunicirajo preko radiofrekvenčnega spektra - naprava je primerna za motenje v primeru sestankov zaupne narave in pri izvajanju policijskih pooblastil.
183		115	Varnostna pregrada	1	64.000,00	Zaščita komunikacije z Internetom - potrebna je varnostna pregrada s

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: 1 7 -06- 2010

**MEDRESORSKA KOMISIJA
ZA IZDAJO SOGLASIJ ZA IZVEDBO
OBRAMBNIH IN ZAUPNIH NAROČIL**

Ministrstvo za obrambo
Vojkova cesta 59
1000 Ljubljana

sekretar komisije

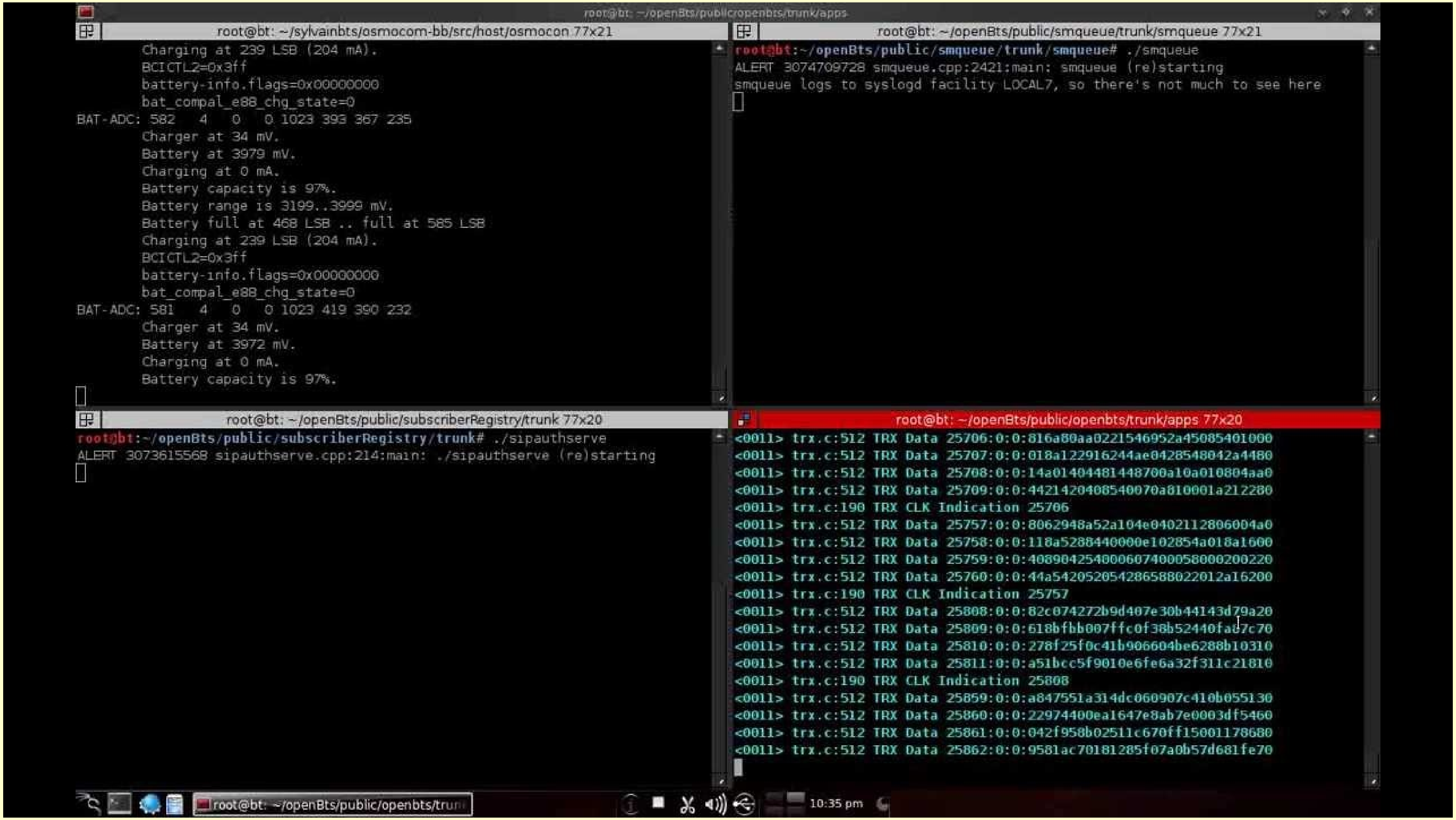
ZADEVA: **Vloga za soglasje k izvedbi naročila na podlagi Uredbe o obrambnih in zaupnih naročilih***[1]

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



root@bt: ~/openBts/public/openbts/trunk/apps

root@bt: ~/sylvainbts/osmocom-bb/src/host/osmocon 77x21

```
        Charging at 239 LSB (204 mA).
        BCICTL2=0x3ff
        battery-info.flags=0x00000000
        bat_compal_e88_chg_state=0
BAT-ADC: 582   4   0   0 1023 393 367 235
        Charger at 34 mV.
        Battery at 3979 mV.
        Charging at 0 mA.
        Battery capacity is 97%.
        Battery range is 3199..3999 mV.
        Battery full at 468 LSB .. full at 585 LSB
        Charging at 239 LSB (204 mA).
        BCICTL2=0x3ff
        battery-info.flags=0x00000000
        bat_compal_e88_chg_state=0
BAT-ADC: 581   4   0   0 1023 419 390 232
        Charger at 34 mV.
        Battery at 3972 mV.
        Charging at 0 mA.
        Battery capacity is 97%.
```

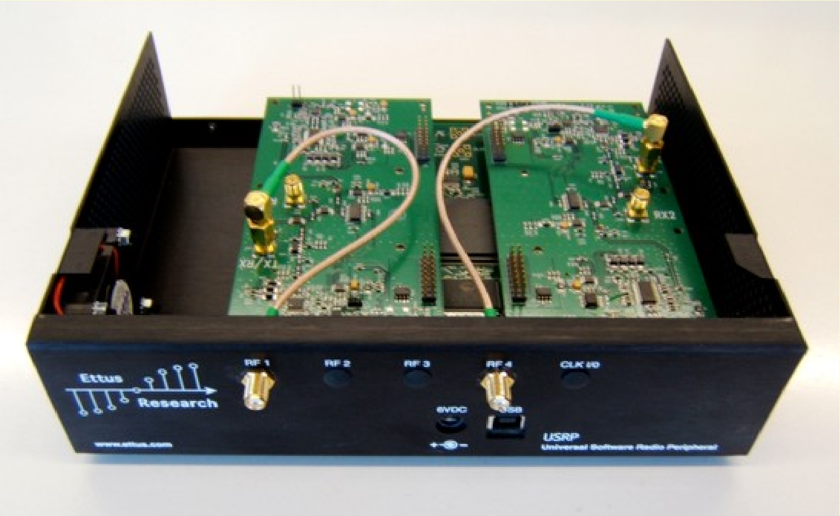
```
root@bt:~/openBts/public/smqueue/trunk/smqueue# ./smqueue
ALERT 3074709728 smqueue.cpp:2421:main: smqueue (re)starting
smqueue logs to syslogd facility LOCAL7, so there's not much to see here
```

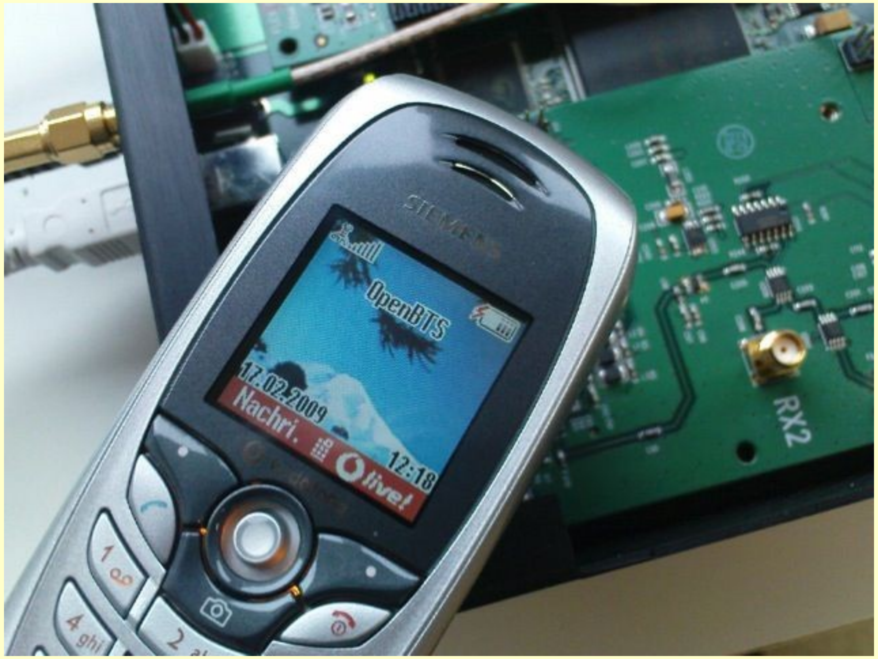
```
root@bt:~/openBts/public/subscriberRegistry/trunk# ./sipauthserve
ALERT 3073615568 sipauthserve.cpp:214:main: ./sipauthserve (re)starting
```

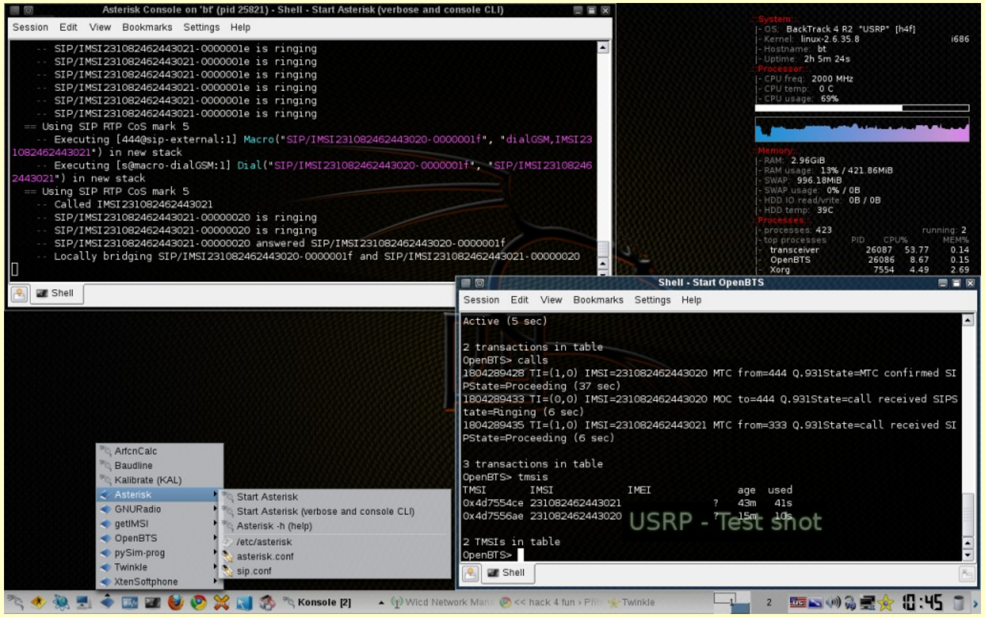
```
<0011> trx.c:512 TRX Data 25706:0:0:816a80aa0221546952a45085401000
<0011> trx.c:512 TRX Data 25707:0:0:018a122916244ae0428548042a4480
<0011> trx.c:512 TRX Data 25708:0:0:14a01404481448700a10a010804aa0
<0011> trx.c:512 TRX Data 25709:0:0:4421420408540070a810001a212280
<0011> trx.c:190 TRX CLK Indication 25706
<0011> trx.c:512 TRX Data 25757:0:0:8062948a52a104e0402112806004a0
<0011> trx.c:512 TRX Data 25758:0:0:118a5288440000e102854a018a1600
<0011> trx.c:512 TRX Data 25759:0:0:408904254000607400058000200220
<0011> trx.c:512 TRX Data 25760:0:0:44a542052054286588022012a16200
<0011> trx.c:190 TRX CLK Indication 25757
<0011> trx.c:512 TRX Data 25808:0:0:82c074272b9d407e30b44143d79a20
<0011> trx.c:512 TRX Data 25809:0:0:618bfbb007ffc0f38b52440fa87c70
<0011> trx.c:512 TRX Data 25810:0:0:278f25f0c41b906604be6288b10310
<0011> trx.c:512 TRX Data 25811:0:0:a51bcc5f9010e6fe6a32f311c21810
<0011> trx.c:190 TRX CLK Indication 25808
<0011> trx.c:512 TRX Data 25859:0:0:a847551a314dc060907c410b055130
<0011> trx.c:512 TRX Data 25860:0:0:22974400ea1647e8ab7e0003df5460
<0011> trx.c:512 TRX Data 25861:0:0:042f958b02511c670ff15001178680
<0011> trx.c:512 TRX Data 25862:0:0:9581ac70181285f07a0b57d681fe70
```

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







```
    -- SIP/IMSI231082462443021-0000001e is ringing
    -- SIP/IMSI231082462443021-0000001e is ringing
    -- SIP/IMSI231082462443021-0000001e is ringing
    -- SIP/IMSI231082462443021-0000001e is ringing
    -- SIP/IMSI231082462443021-0000001e is ringing
    -- SIP/IMSI231082462443021-0000001e is ringing
  == Using SIP RTP CoS mark 5
    -- Executing [444@sip-external:1] Macro("SIP/IMSI231082462443020-0000001f", "dialGSM,IMSI23
1082462443021") in new stack
    -- Executing [s@macro-dialGSM:1] Dial("SIP/IMSI231082462443020-0000001f", "SIP/IMSI23108246
2443021") in new stack
  == Using SIP RTP CoS mark 5
    -- Called IMSI231082462443021
    -- SIP/IMSI231082462443021-00000020 is ringing
    -- SIP/IMSI231082462443021-00000020 is ringing
    -- SIP/IMSI231082462443021-00000020 answered SIP/IMSI231082462443020-0000001f
    -- Locally bridging SIP/IMSI231082462443020-0000001f and SIP/IMSI231082462443021-00000020
```

```
::System::
|- OS:  BackTrack 4 R2  "USRP"  [h4f]
|- Kernel:  linux-2.6.35.8                 i686
|- Hostname:  bt
|- Uptime:  2h 5m 24s
::Processor::
|- CPU freq:  2000 MHz
|- CPU temp:  0 C
|- CPU usage:  69%
::Memory::
|- RAM:  2.96GiB
|- RAM usage:  13% / 421.86MiB
|- SWAP:  996.18MiB
|- SWAP usage:  0% / 0B
|- HDD IO read/write:  0B / 0B
|- HDD temp:  39C
::Processes::
|- processes: 423                 running: 2
|- top processes      PID    CPU%      MEM%
|-  transceiver      26087   53.77     0.14
|-  OpenBTS          26086    8.67     0.15
|-  Xorg              7554    4.49     2.69
```

```
Active (5 sec)

2 transactions in table
OpenBTS> calls
1804289428 TI=(1,0) IMSI=231082462443020 MTC from=444 Q.931State=MTC confirmed SI
PState=Proceeding (37 sec)
1804289433 TI=(0,0) IMSI=231082462443020 MOC to=444 Q.931State=call received SIPS
tate=Ringing (6 sec)
1804289435 TI=(1,0) IMSI=231082462443021 MTC from=333 Q.931State=call received SI
PState=Proceeding (6 sec)

3 transactions in table
OpenBTS> tmsis
TMSI       IMSI            IMEI            age  used
0x4d7554ce 231082462443021              ?  43m   41s
0x4d7556ae 231082462443020              ?  15m   10s

2 TMSIs in table
OpenBTS>
```

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

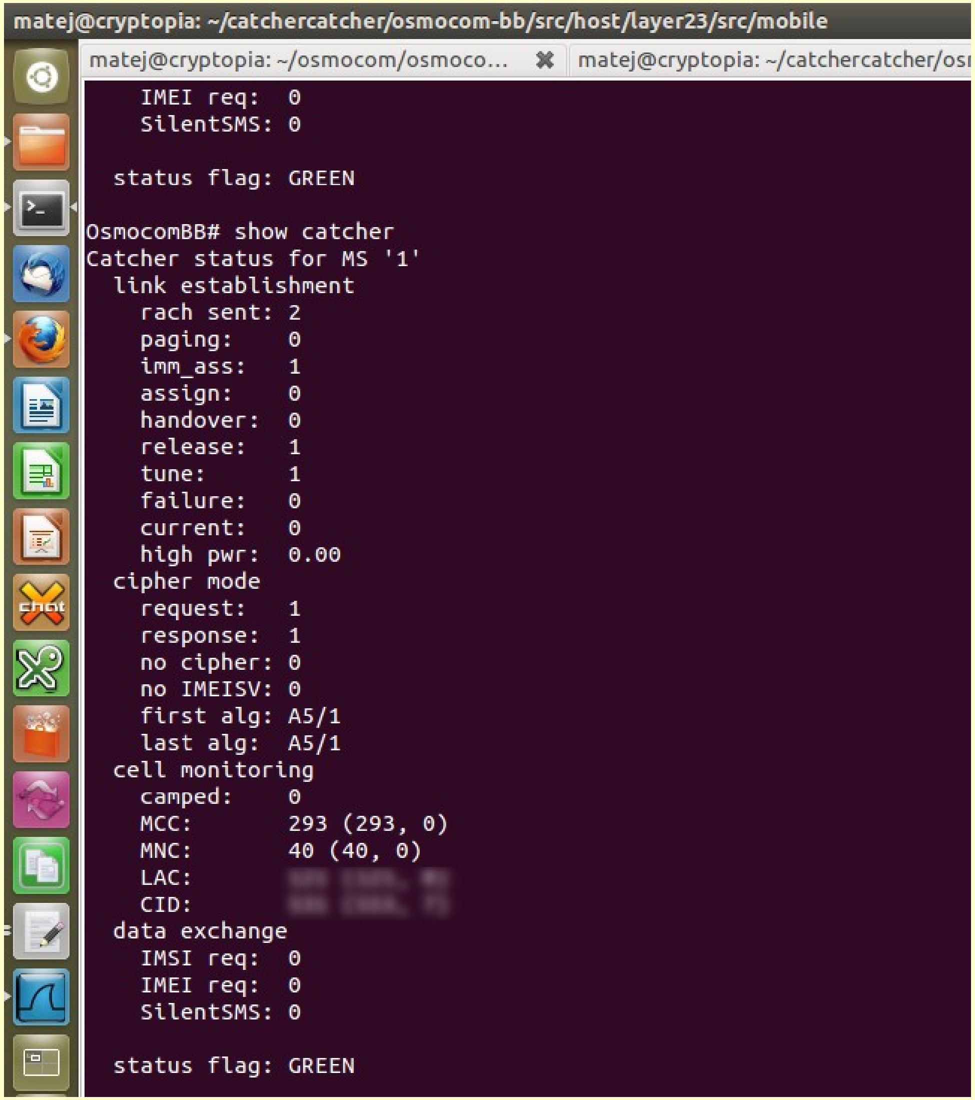
Ter:

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/osı

```
    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).

BUSTED!

Ilustracija: (CC) SulphurSpoon @ DeviantArt

Vprašanja?

Vabljeni še na predavanji:

Varnost internetne (VoIP) telefonije (15. november 2013)

Na predavanju se bomo seznanili z osnovami VoIP telefonije ter si ogledali kako je mogoče prestrezati VoIP komunikacije. Prikazan bo konkreten primer varnostne analize VoIP omrežja.

Rešitve za zaščito mobilnih komunikacij (13. december 2013)

Na predavanju bodo predstavljene rešitve za zaščito mobilnih komunikacij. Ogledali si bomo kako šifrirati svoja SMS/tekstovna sporočila in telefonske pogovore, kako skriti svoje prometne podatke ter kakšne so možnosti za povsem anonimno komuniciranje.