Varnost slovenskih GSM omrežij

Jaka Hudoklin, Matej Kovačič, Klemen Rupnik

Predavanje na konferenci Vitel, 15. junija 2012

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

Pri izvajanju varnostnega pregleda smo uporabili lastno opremo oz. izvajali analizo lastnih komunikacij, prav tako v slovenskih GSM omrežjih nismo povzročali kakršnihkoli motenj.

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

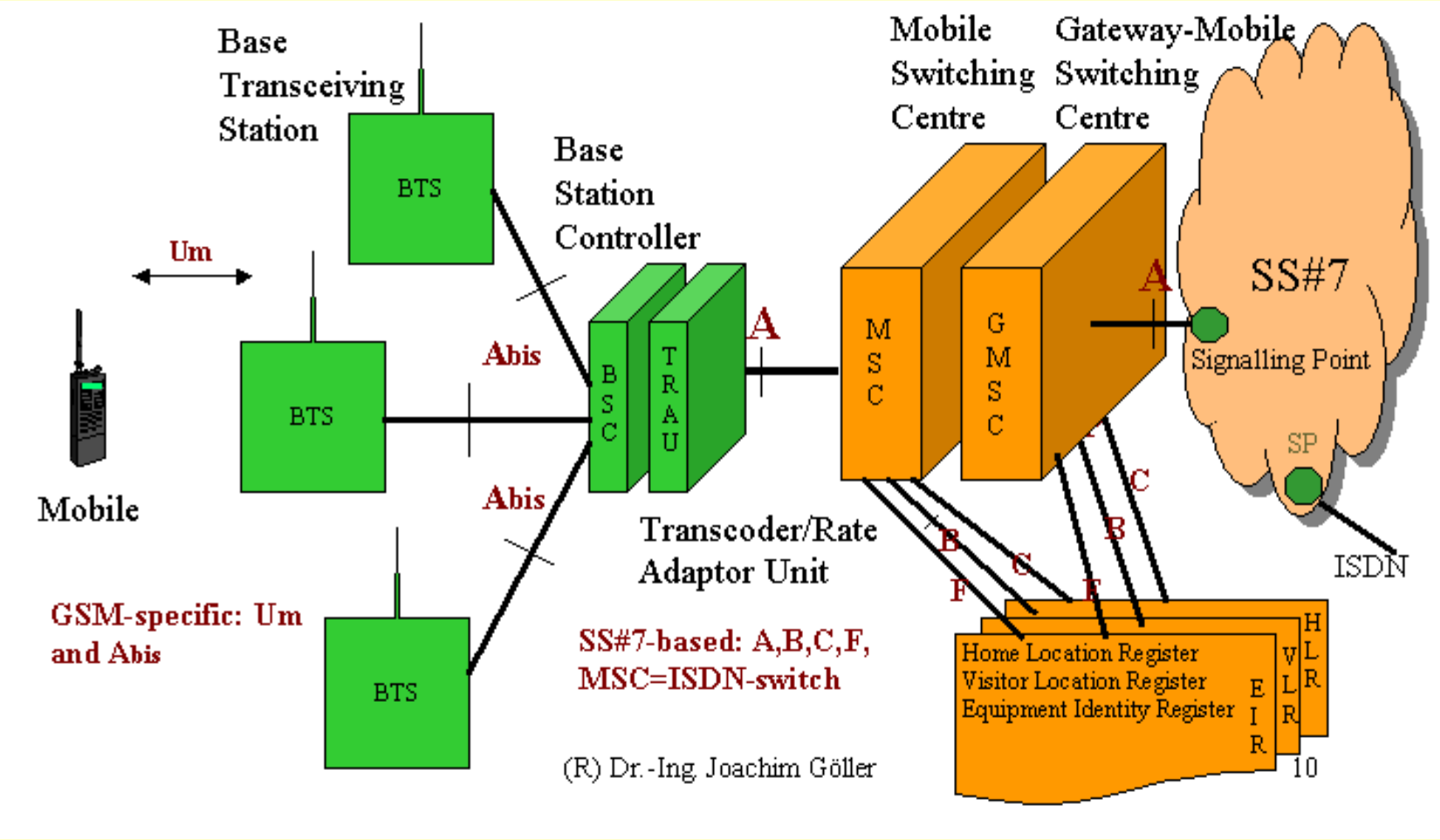
Predzgodba

John Nevil Maskelyne (1839 – 1917)

Nokia 3310

A5 Buster

Nekaj osnov o GSM



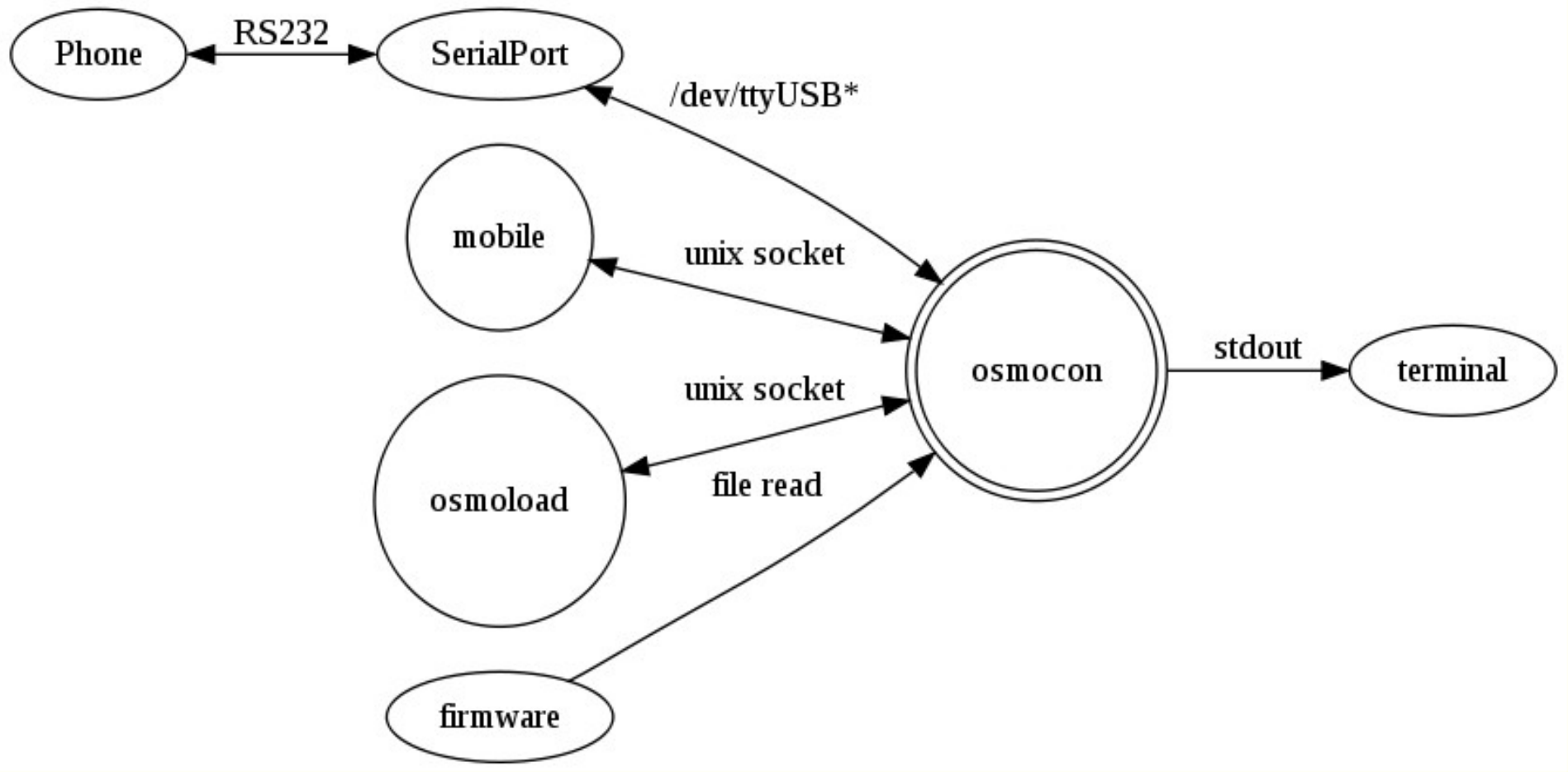
SIM kartica in mobilni aparat, IMSI, TMSI, A5/x, kanali...

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

OsmocomBB

Mobilni telefon s Calypso čipovjem...

...in OsmocomBB strojna programska oprema

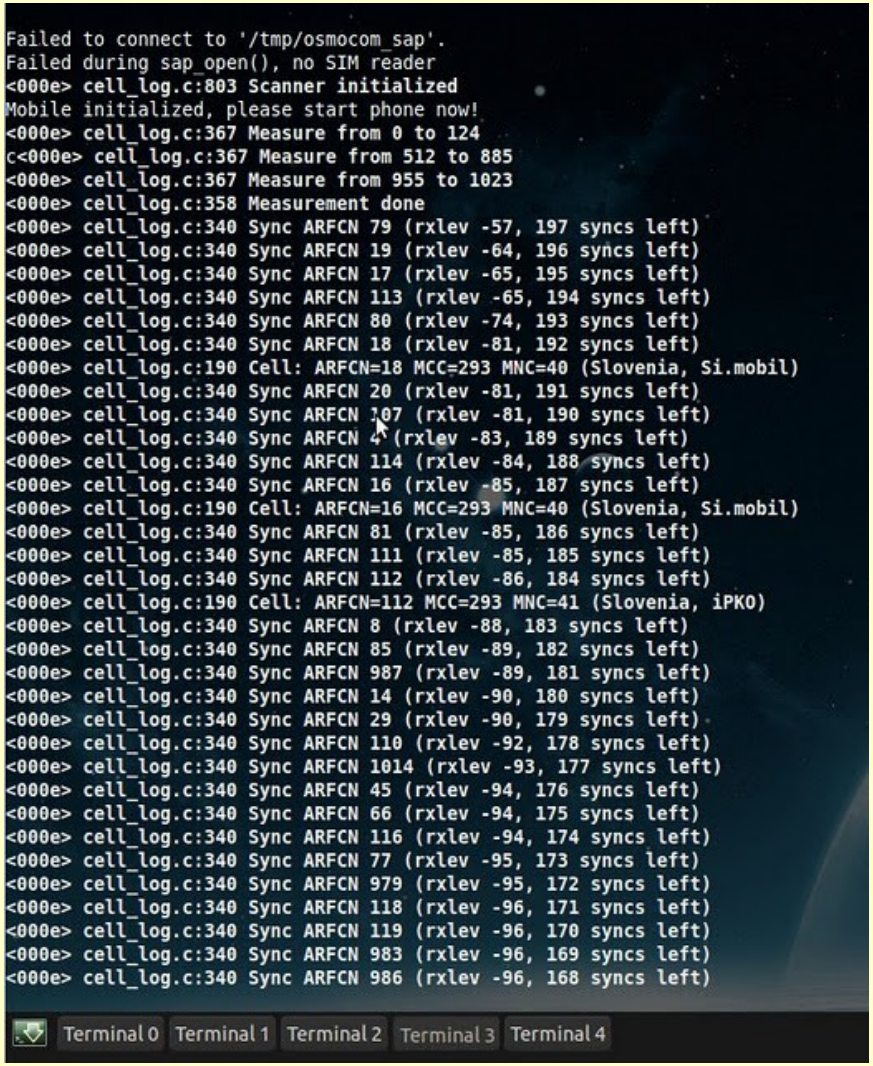


Zagon nalagalnika ROM (ang. *romloader*)

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

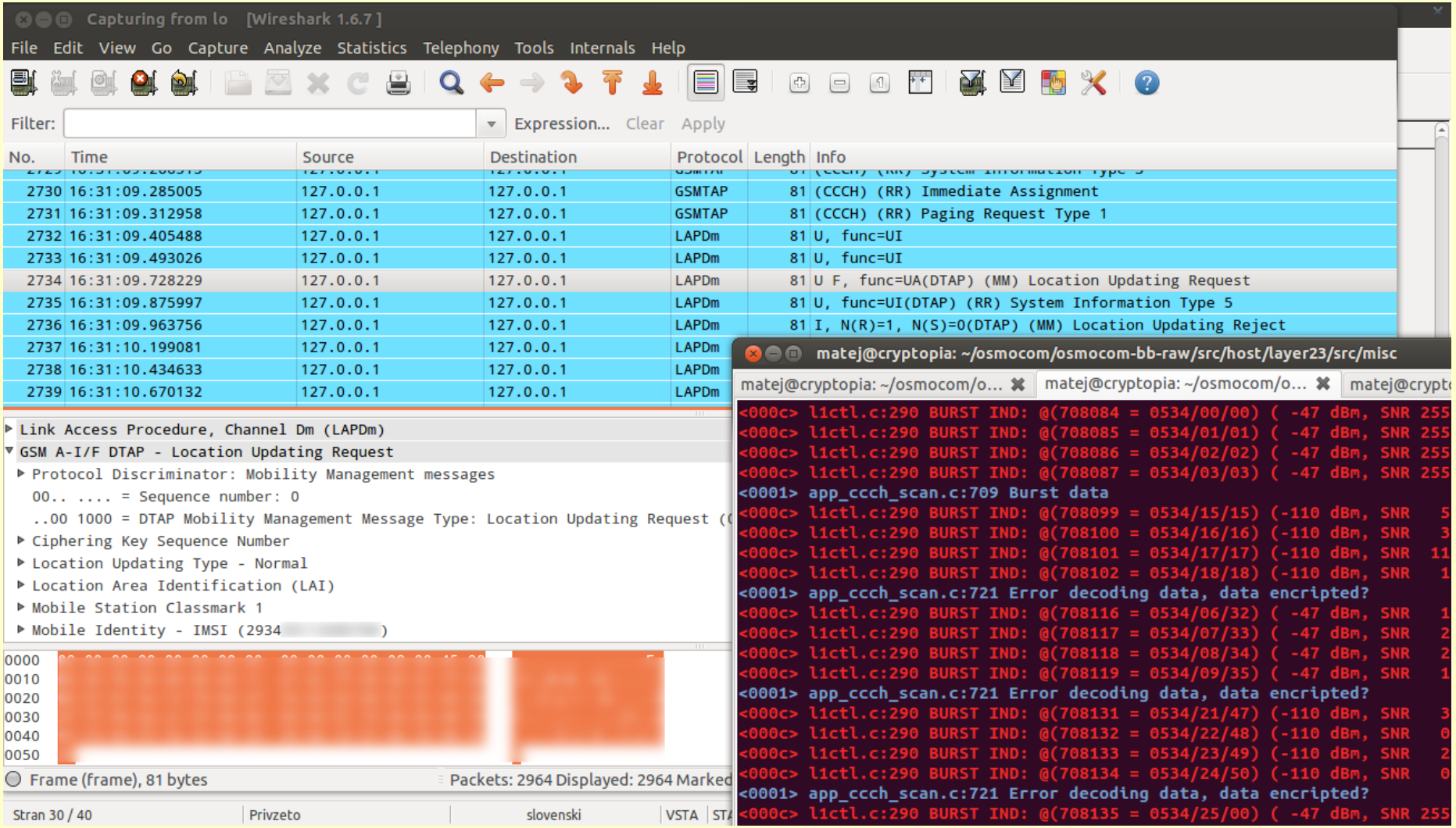
```
Die ID code: 7e540b2fc90393bb
======================================================================
REG_DPLL=0x2413
CNTL_ARM_CLK=0xf0a1
CNTL_CLK=0xff91
CNTL_RST=0xfff3
CNTL_ARM_DIV=0xfff9
======================================================================
Power up simcard:


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*.

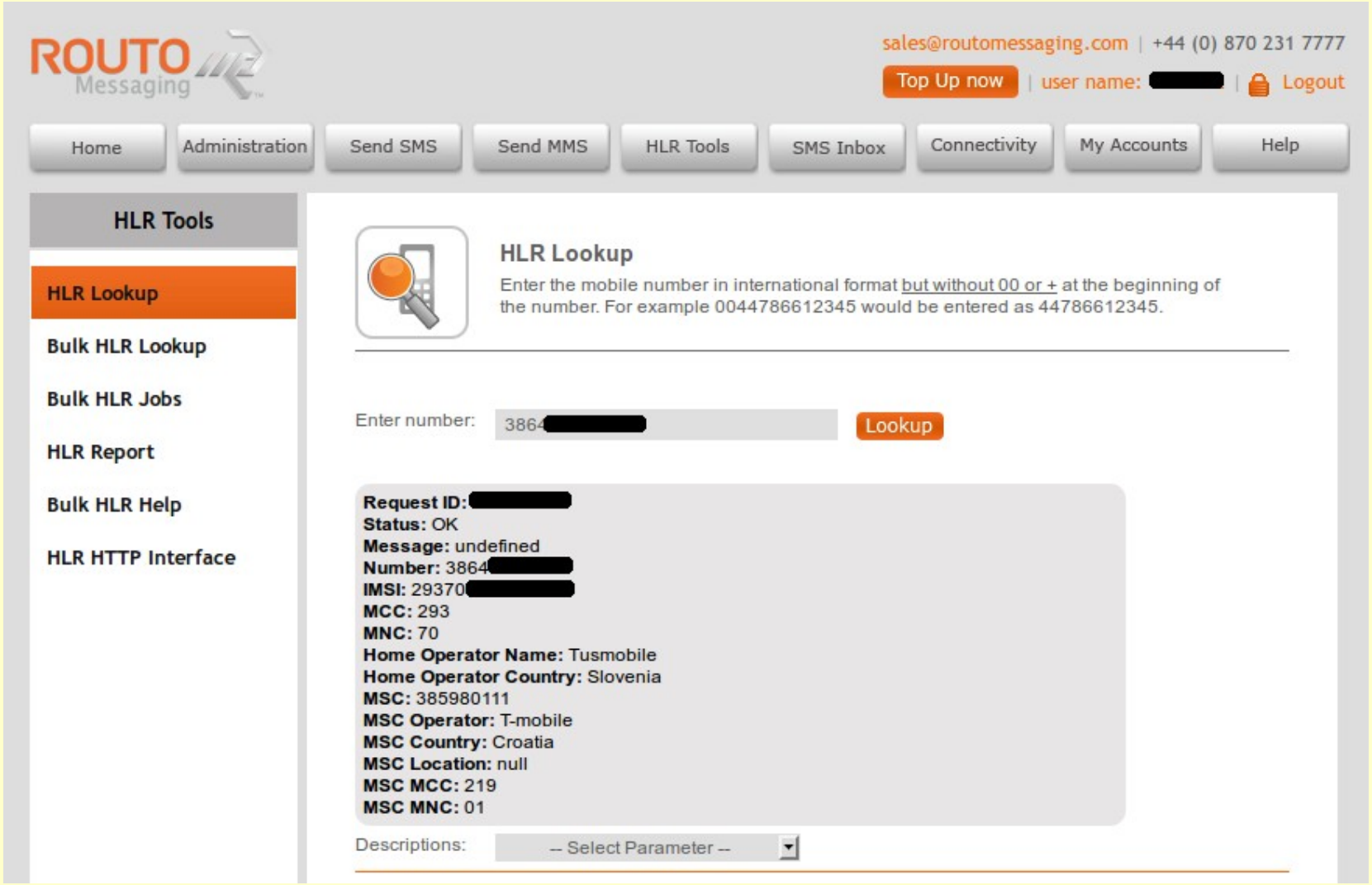
Analiza GSM prometa...



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

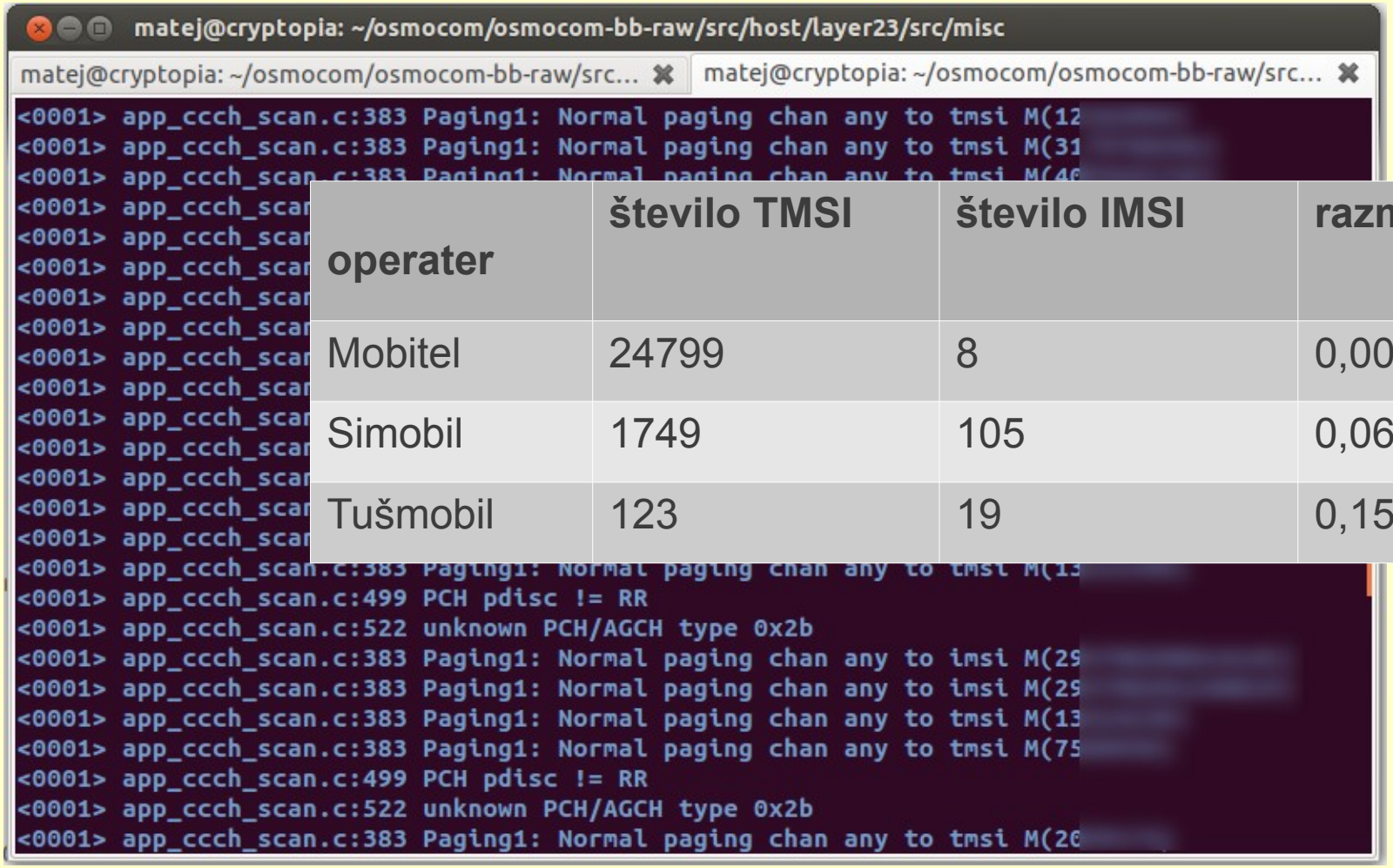
Varnostni pregled slovenskih GSM omrežij

HLR vpogled



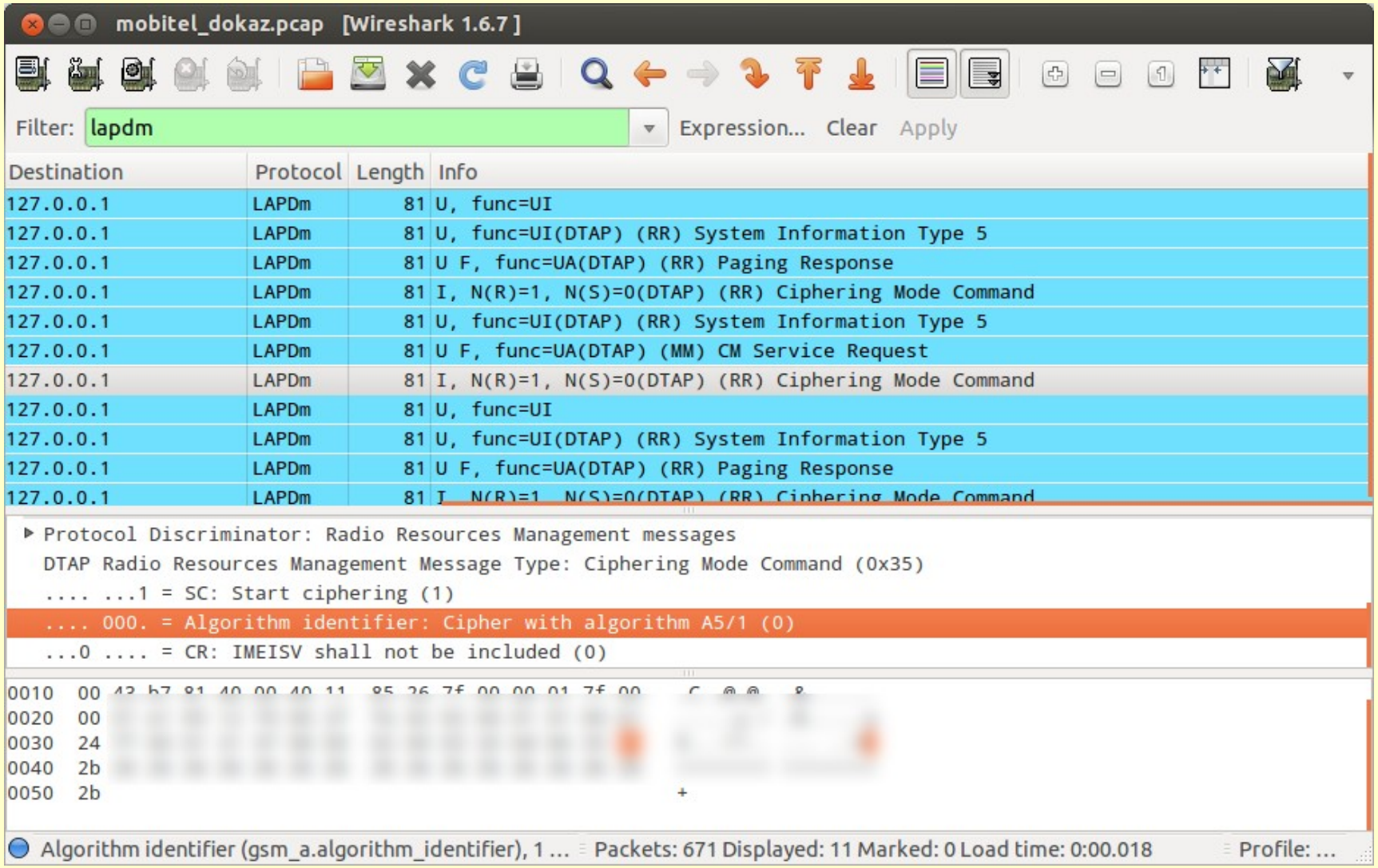
HLR vpogled preko SS7 razkrije IMSI številko in operaterja uporabnika, v nekaterih primerih pa tudi grobo lokacijo.

Uporaba TMSI številk



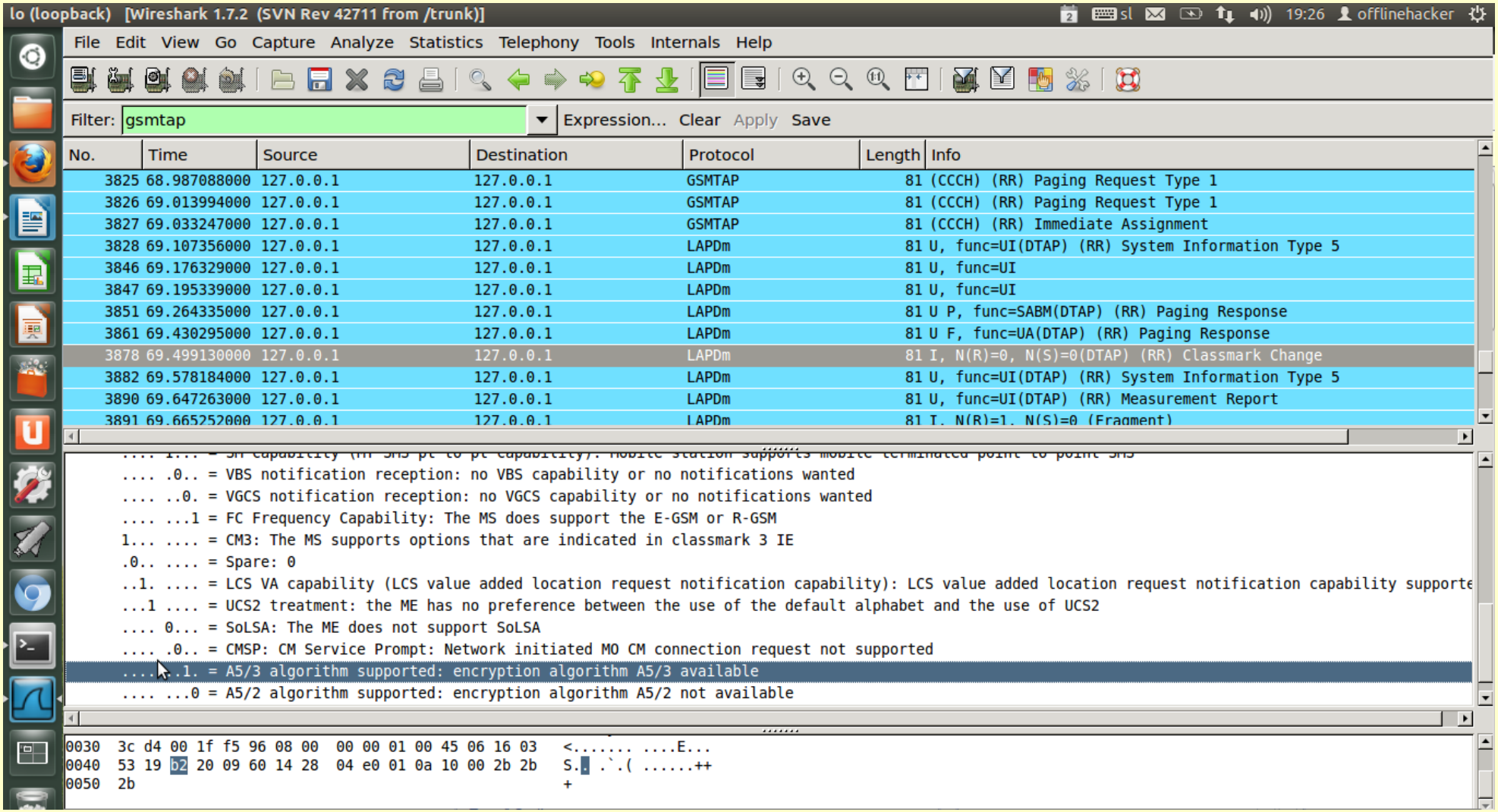
operater	število TMSI	število IMSI	razmerje
Mobitel	24799	8	0,000322594
Simobil	1749	105	0,060034305
Tušmobil	123	19	0,154471545

Uporaba šifriranja - Mobitel



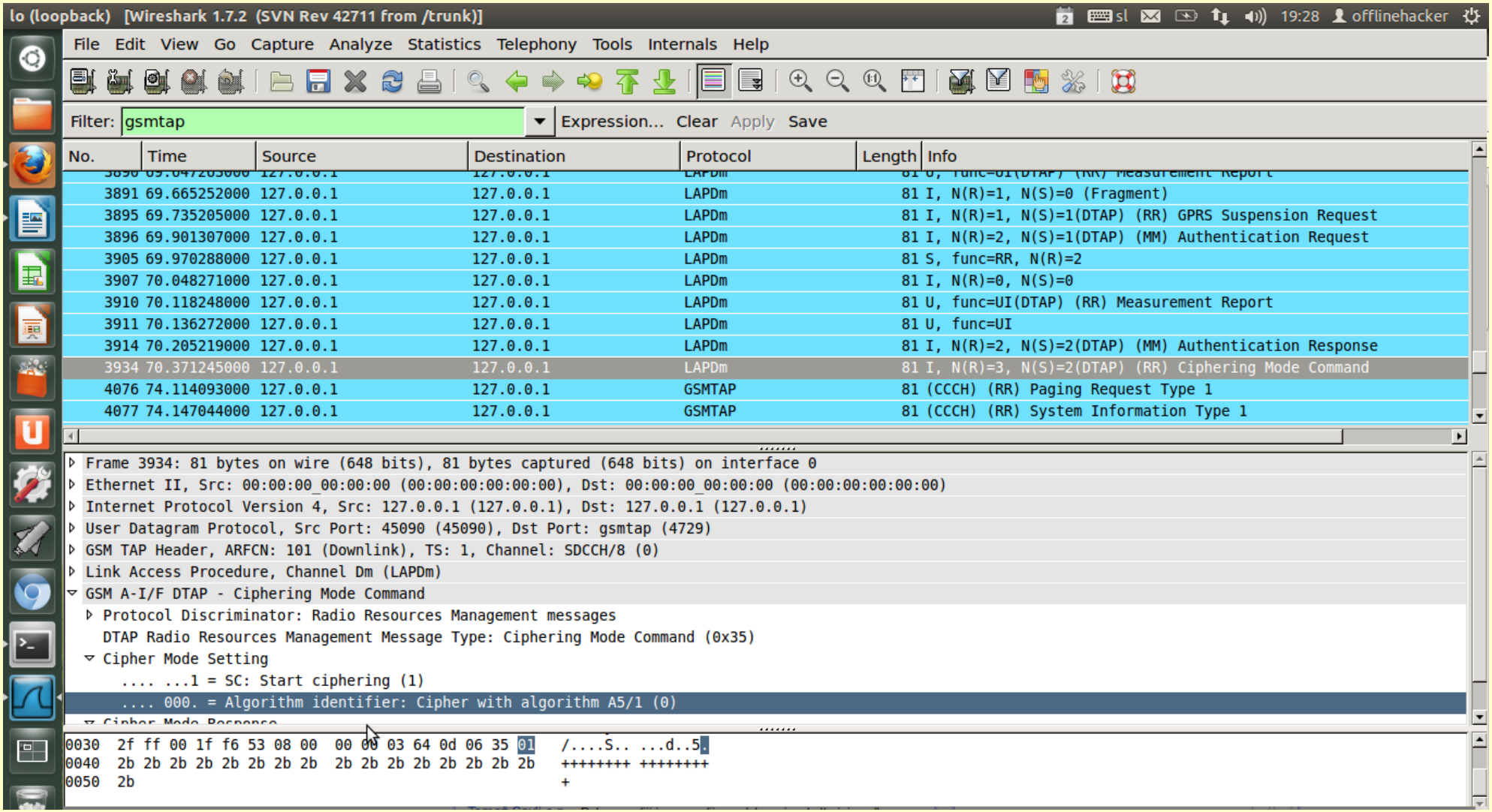
Mobitel uporablja šifriranje A5/1

Uporaba šifriranja - Mobitel



Če mobilni telefon sporoči, da podpira A5/3...

Uporaba šifriranja - Mobitel

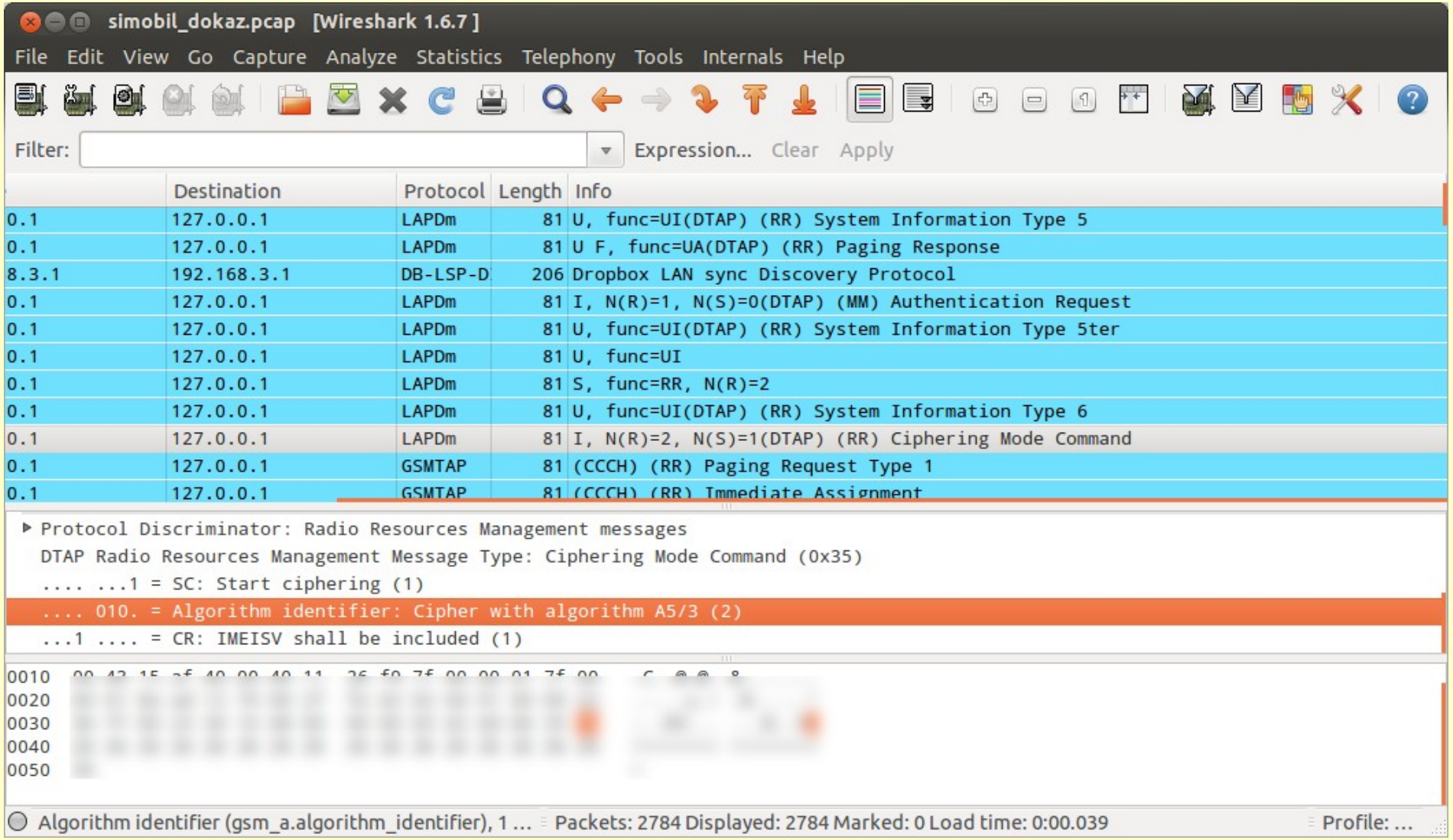


...omrežje odgovori,da je na voljo samo A5/1.

“V omrežja, predvsem pa v terminale, se postopoma uvaja že nekaj let tako pri nas kot po svetu, vendar imajo nekateri stari terminali težave z A5/3, zato še ni v celoti nadomestil A5/1. Nove bazne postaje pa že podpirajo protokol A5/3 pri govornih storitvah v omrežju GSM.”

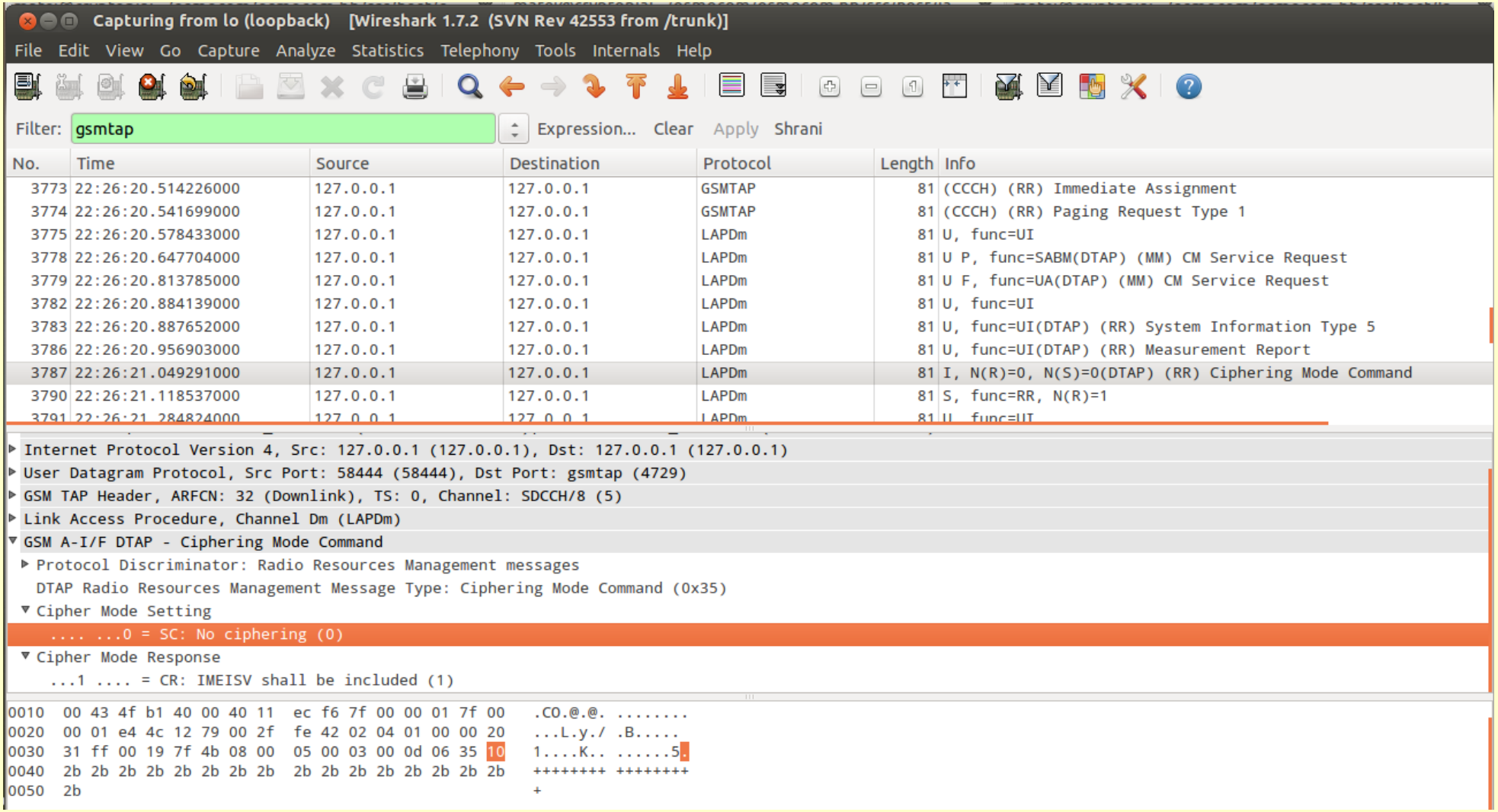
Telekom Slovenije, Služba za korporativno komuniciranje, junij 2012

Uporaba šifriranja - Simobil



Simobil uporablja A5/3...

Uporaba šifriranja - Simobil



...vendar pa (je) omogoča(l) tudi uporabo A5/0.

“A5/0 pri nas ni uporabljan, absolutno ne.”

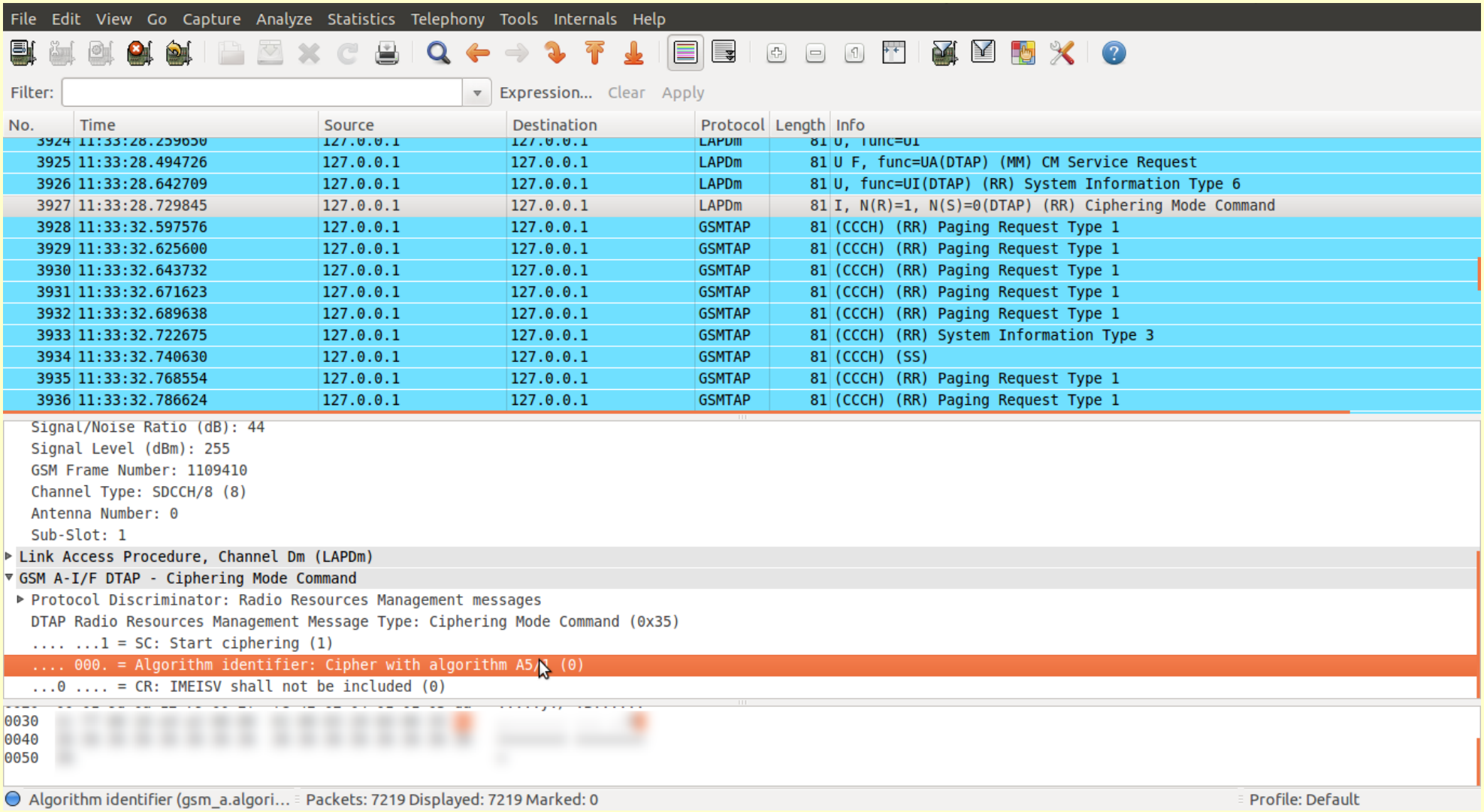
Andraž Zmajšek, vodja informacijske varnosti, in Luka Šušteršič, vodja službe za storitve jedrnega omrežja pri Simobilu za revijo Monitor, novembra 2011

“V juniju 2012 pa smo izklopili možnost uporabe nešifriranega algoritma A5/0.”

Andraž Zmajšek, vodja informacijske varnosti na Si.mobilu, junija 2012

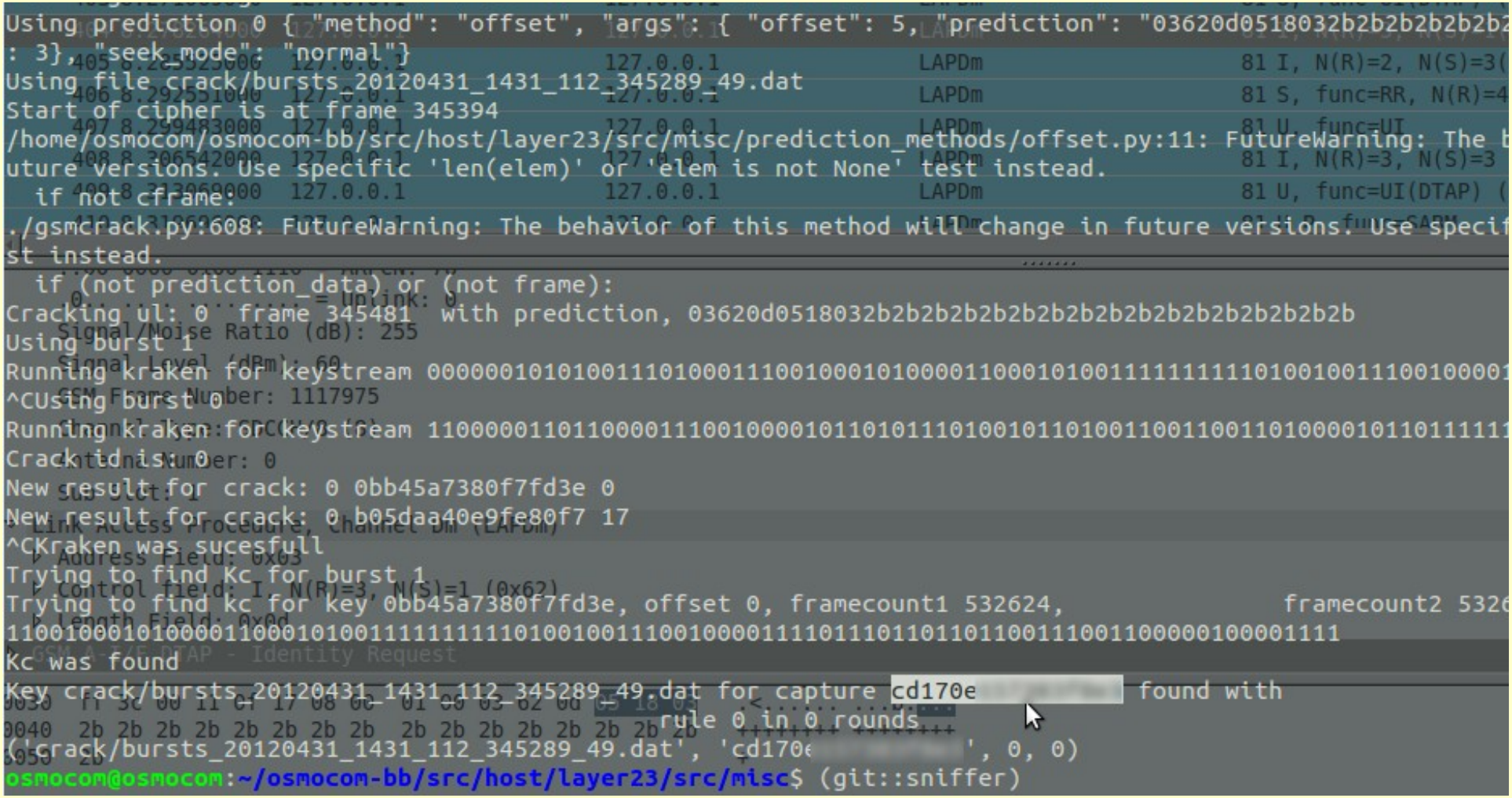
Simobil je uporabo A5/0
onemogočil dan po objavi članka
na Slo-Tech.com (13. junija 2012)

Uporaba šifriranja - Tušmobil



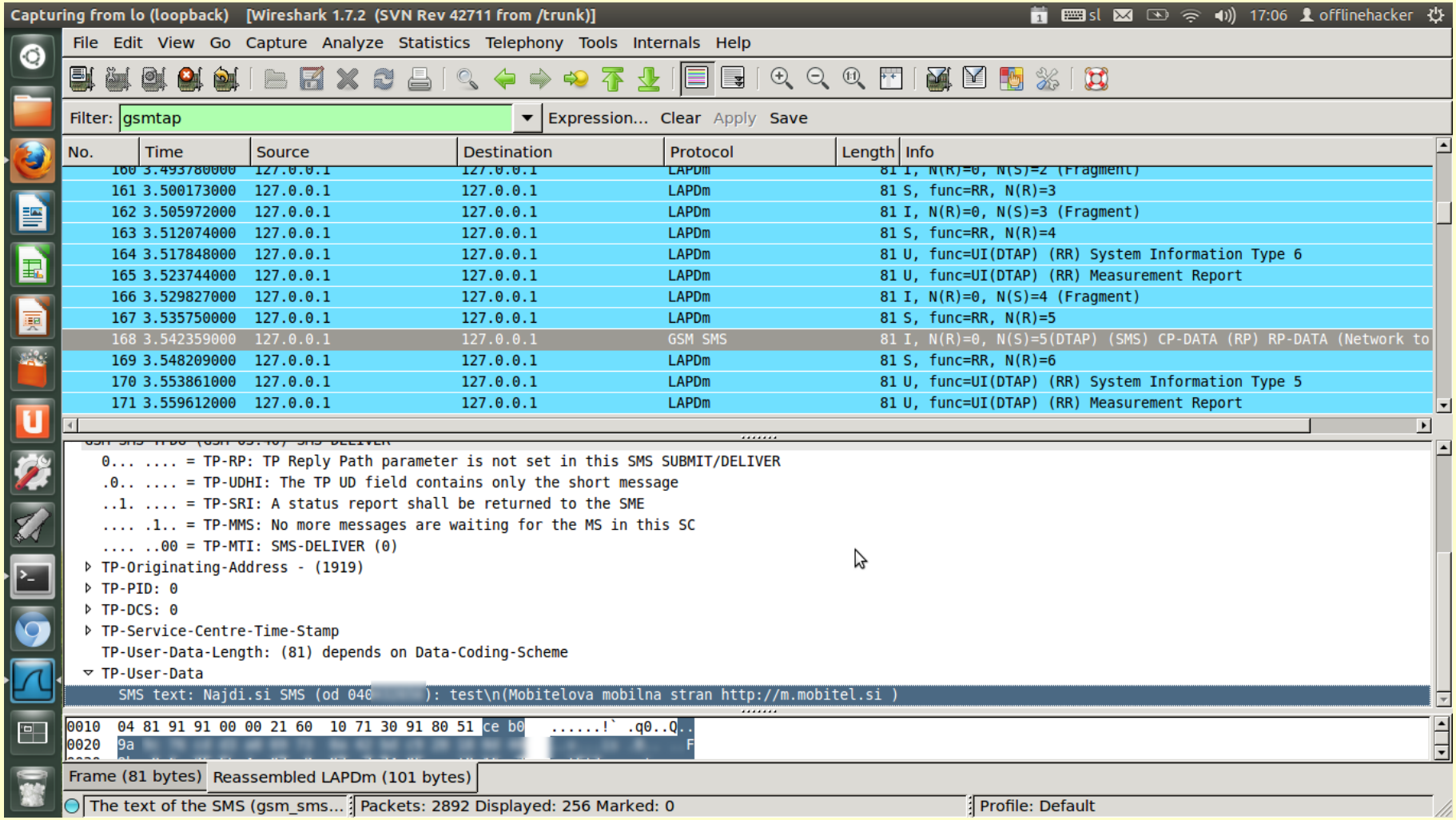
Tušmobil uporablja A5/1.

Razbijanje A5/1 sejnega šifrirnega ključa Kc



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

Razbijanje A5/1 sejnega šifrirnega ključa Kc

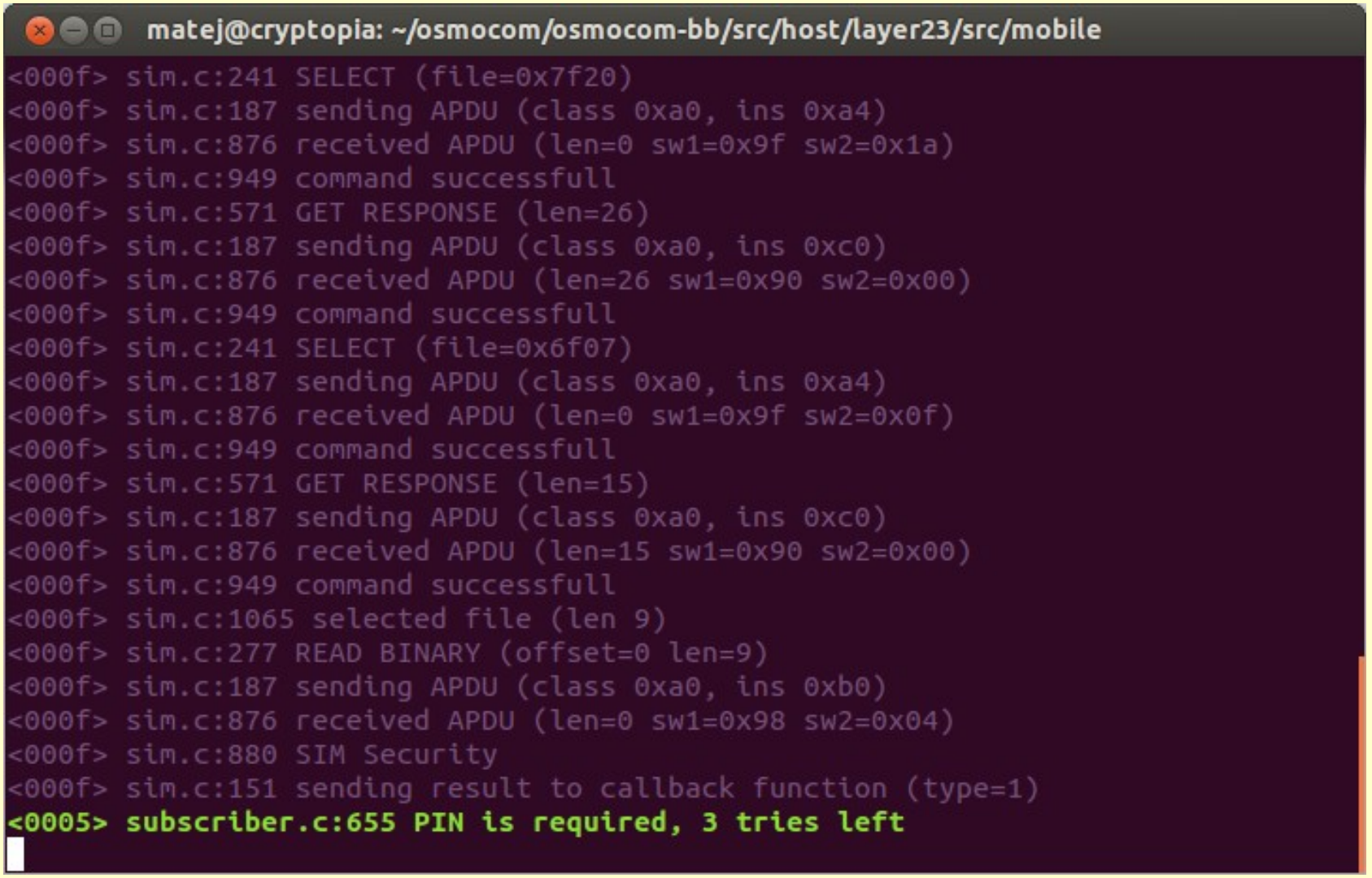


… in dešifrirano SMS sporočilo (prejeto preko 2G).

Ponarejanje mobilne identitete v GSM omrežju

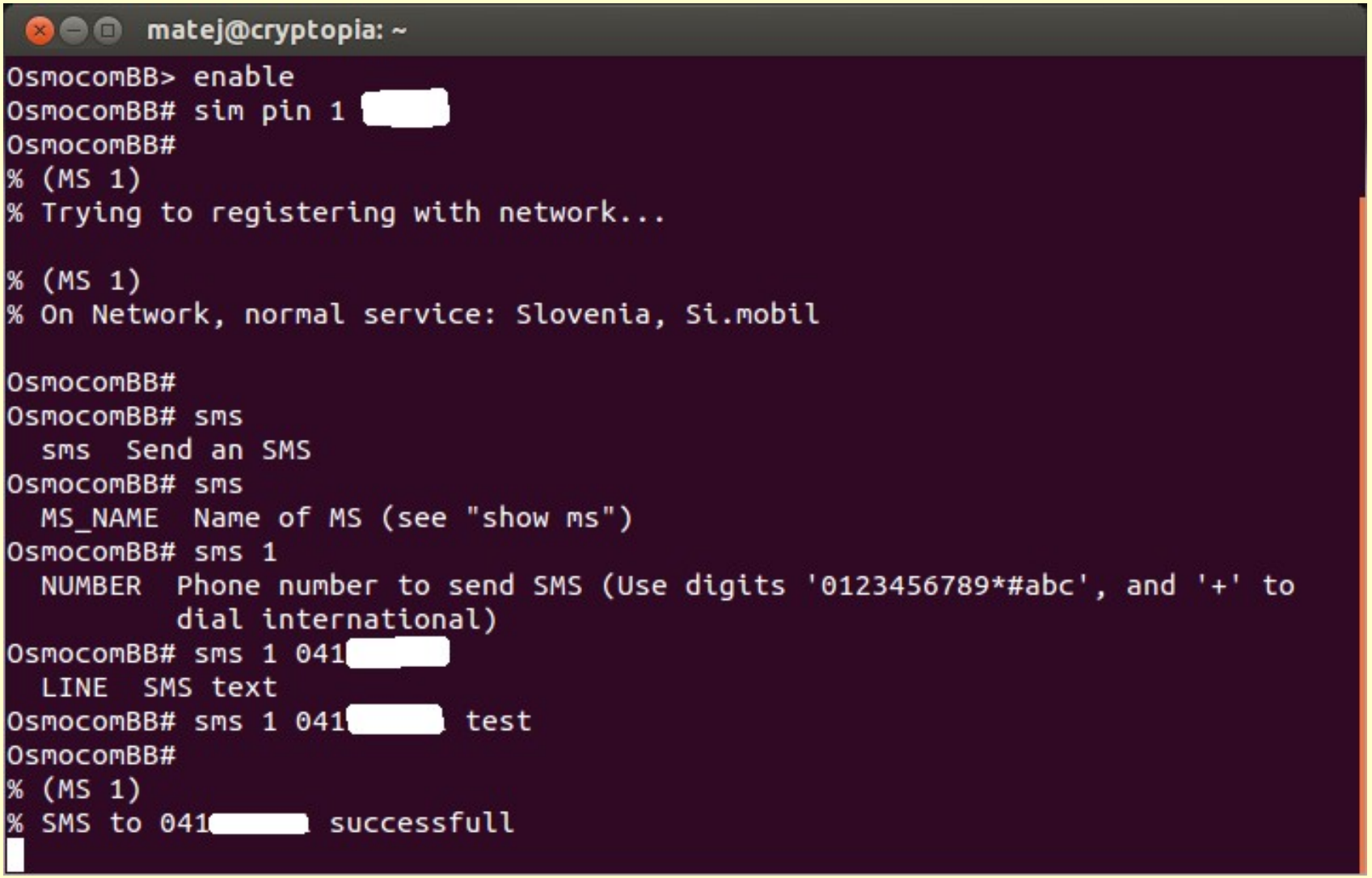
(brez posedovanja mobilnega telefona in/ali SIM kartice tarče)

Aplikacija *mobile*



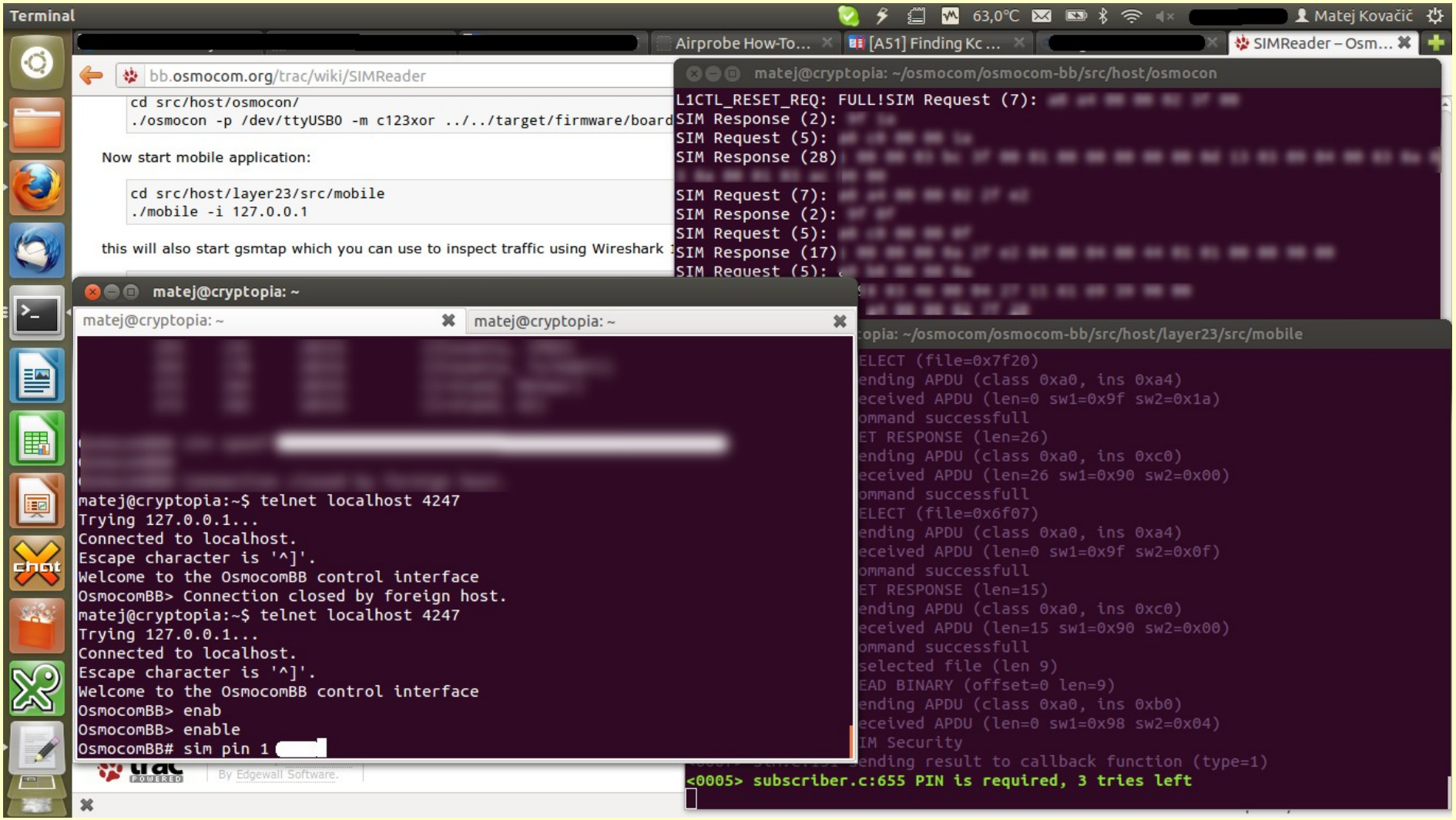
Aplikacija *mobile* omogoča klicanje ter pošiljanje in sprejemanje SMS sporočil na OsmocomBB mobilnih telefonih.

Aplikacija *mobile*



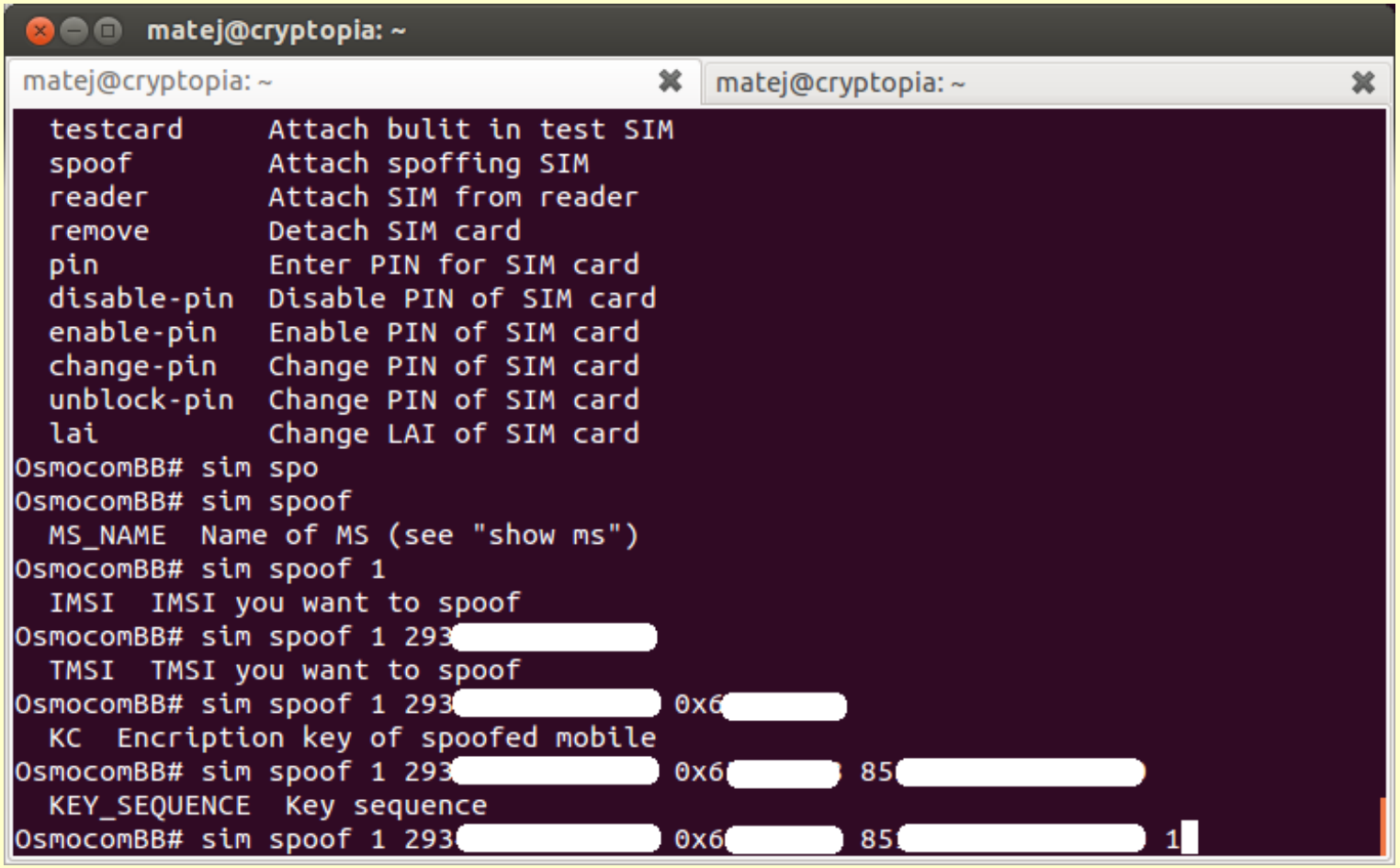
Pošiljanje SMS sporočila iz aplikacije *mobile*.

Aplikacija *mobile*



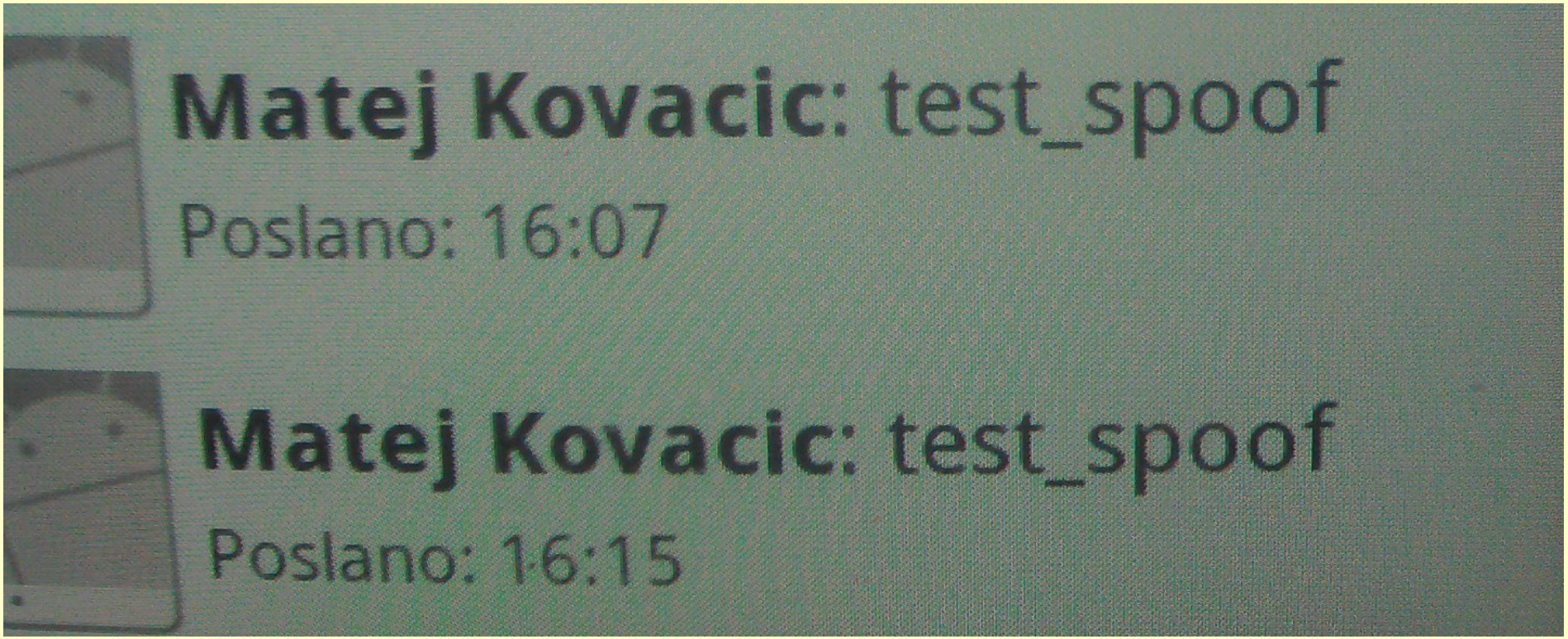
Uporaba aplikacije *mobile*. V ozadju Osmocom ROM nalagalnik, aplikacija *mobile* in (v ospredju) konzola aplikacije *mobile*.

“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.
[video]

“Glede možnosti zlorabe identitete uporabnika mobilnega omrežja medtem v Telekomu pravijo, da so te v njihovem omrežju preprečene z vrsto standardnih in nadstandardnih varnostnih mehanizmov.”

Odgovor Telekoma (objavljen na STA) na članke
o varnostnih ranljivostih v slovenskih GSM

Tabela varnosti

	Mobitel	Simobil	Tušmobil
uporaba TMSI številk	praviloma da (razmerje: 0,0003)	pogosto (razmerje: 0,06)	manj pogosto (razmerje: 0,154)
uporaba šifrirnih algoritmov	A5/1	A5/3	A5/1
HLR vpogled	ne razkrije lokacije in operaterja pri katerem je uporabnik trenutno registriran, prav tako MSC ne razkrije roaming operaterja	še nismo preverjali	razkrije lokacijo preko razkritja MSC številke, MSC operaterja in države
dodeljevanje iste TMSI številke ob ponovnem prižiganju telefona na območju iste bazne postaje	da	da	nismo preverjali
ali omrežje dovoli A5/0	ne	od 13. junija 2012 ne več	ne
ali je mogoče ponarediti mobilno identiteto če imamo šifrirni ključ	da	da	nismo preverjali (najverjetneje da)
ali je mogoče ponarediti mobilno identiteto če nimamo šifrirnega ključa	ne	od 13, junija 2012 ne več	ne
Po kolikšnem času omrežje zamenja šifrirni ključ, če je priključen na isto bazno postajo in je telefon vključen.	>10 ur	še nismo preverjali, več kot 1 uro	nismo preverjali
Možnost sprejema tihih sporočil.	da	da	da

Predlogi glede izboljšanja varnosti slovenskih GSM omrežij

- Uvedba uporabe A5/3.
- Prepoved uporabe A5/0.
- Pogostejša in dosledna menjava TMSI številk.
- Bazna postaja (BTS) bi v podatkovnih okvirjih okvirjih morala uporabljati naključno bitno zapolnjevanje (ang. *randomized padding*) - specifikacije TS 44.006, različice od 6.7.0 dalje (od oktobra 2008 dalje).
- Osvežitev sejnega šifrirnega ključa pred vsakim klicem ali pošiljanjem SMS sporočila.

Predlogi glede izboljšanja varnosti slovenskih GSM omrežij

- Poskrbeti za naključnost tim. sistemskih obvestil omrežja telefonu (ang. *system information messages*).
- Implementacija standarda 3GPP TR 23.840 (tim. SMS "home routing" standard).
- Uvedba medsebojne avtentikacije (ang. *mutal authentication*) SIM kartice z omrežjem, npr. EAP-SIM; nadgradnjo je mogoče opraviti na daljavo preko tim. OTA (Over the Air).
- Redno preverjanje varnosti s strani neodvisnih zunanjih strokovnjakov.

“Denial is a common tactic that substitutes deliberate ignorance for thoughtful planning.”

-- Charles Tremper

Vprašanje revije Monitor: “Če smo konkretni, če kak GSM operater trdi, da se njim ne da prisluškovati, je to bolj, hm, bikov kakec?”

“Če govorimo o nekih laboratorijskih okoliščinah ali zelo kontroliranih okoliščinah, je to možno. Toda zelo veliko stvari se mora pokriti, da pridemo do tega.”

Andraž Zmajšek, vodja informacijske varnosti, in Luka Šušteršič, vodja službe za storitve jedrnega omrežja pri Simobilu za Monitor, novembra 2011

“V mobilnem operaterju Tušmobil so za STA na kratko dejali le to, da je njihovo omrežje 'varno in zavarovano v skladu z vsemi sodobnimi varnostnimi standardi, primerljivimi z ostalimi slovenskimi in evropskimi operaterji'.”

Vir: STA.si, junij 2012

“Mobitelovo omrežje je izjemno kakovostno, zanesljivo in varno. Zadostuje najstrožjim kriterijem in kljub številnim tovrstnim navedbam o vdorih in zlorabah mobilni komunikacij v Mobitelovem omrežju nismo zabeležili nobenega primera zlorabe identitete uporabnika.”

Telekom Slovenije, Služba za korporativno komuniciranje, junij 2012

BUSTED!

Vprašanja?