The Phonebusters

Matej Kovačič

Kidz, don't try this at home!

For the described procedures certified equipment has been used.

We also performed an analysis of our own communications, We did not caused any interference in the Slovenian GSM networks.

No SIM card has been cloned. No mobile phone has been harmed or tortured.

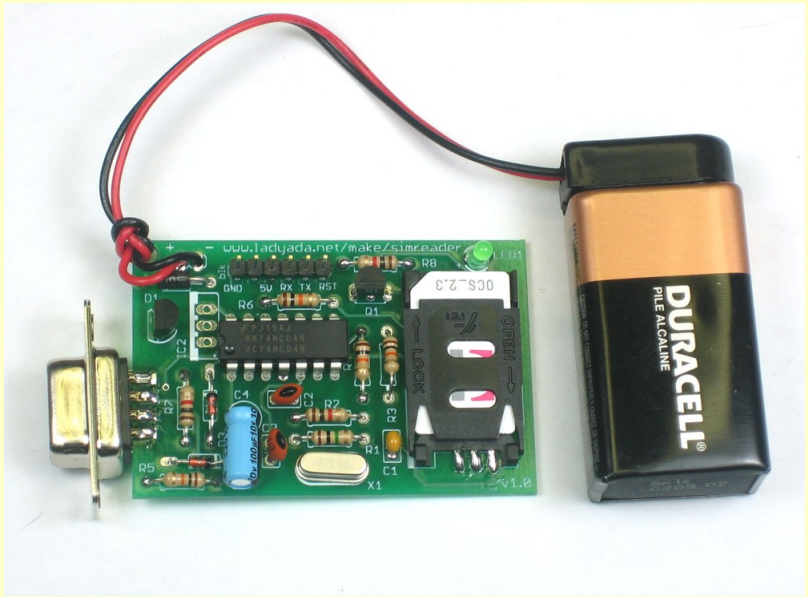
The purpose of our study was to draw attention to the security vulnerabilities in the Slovenian GSM networks. Our aim is to improve GSM security and consequently to increase the level of privacy of mobile users. We would like that Slovenian mobile operators begin to invest more in network security and protection of its users.

Our study also showed the weaknesses in the retention of traffic data (so-called data retention) – we believe that reliability of traffic data in criminal proceedings is questionable.

Data on a SIM card

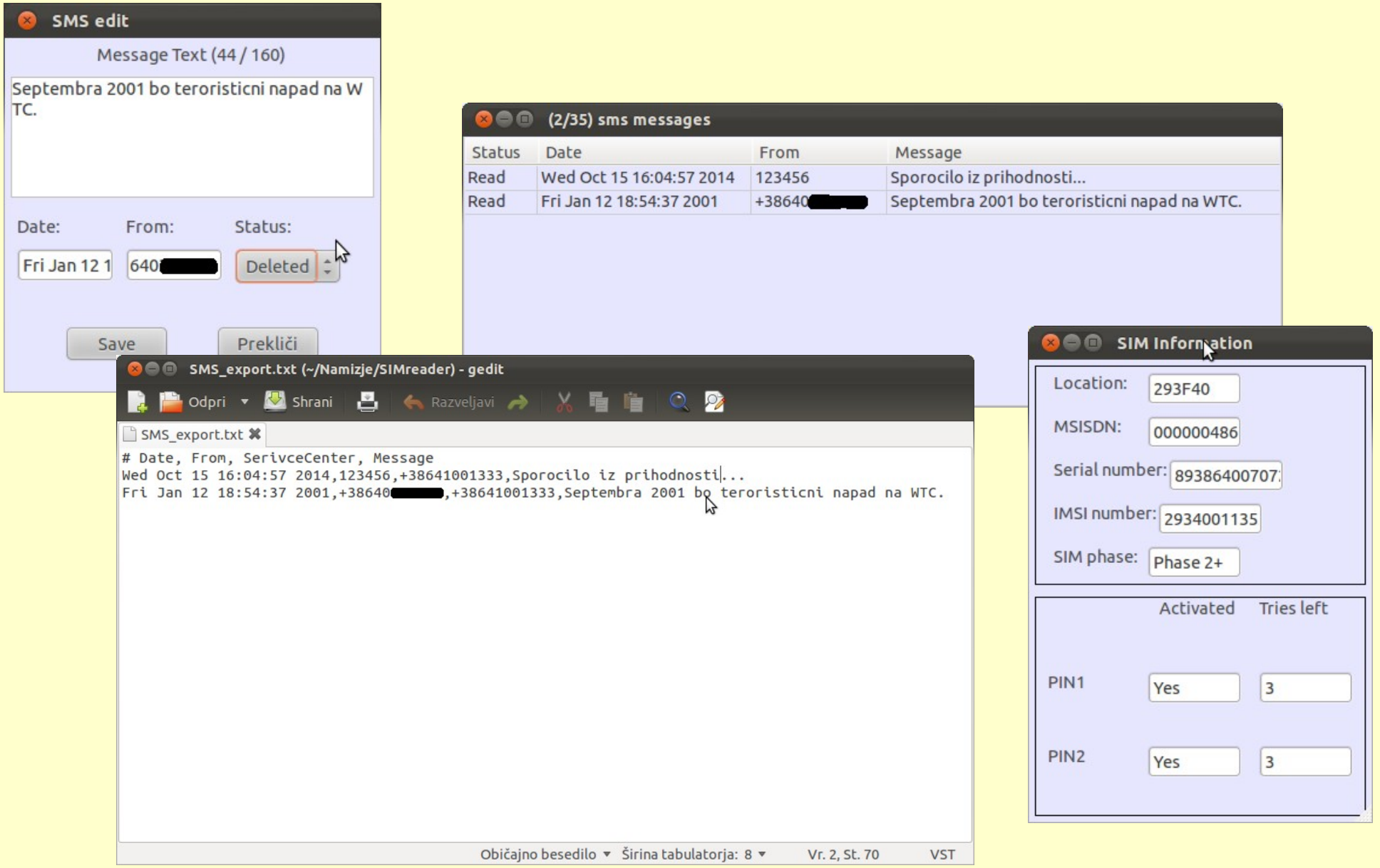
Data on a SIM card

1: SIM card reader



Data on a SIM card

2: changing contens of data on a SIM card, including SMS content and metadata



Data on a SIM card

3: result

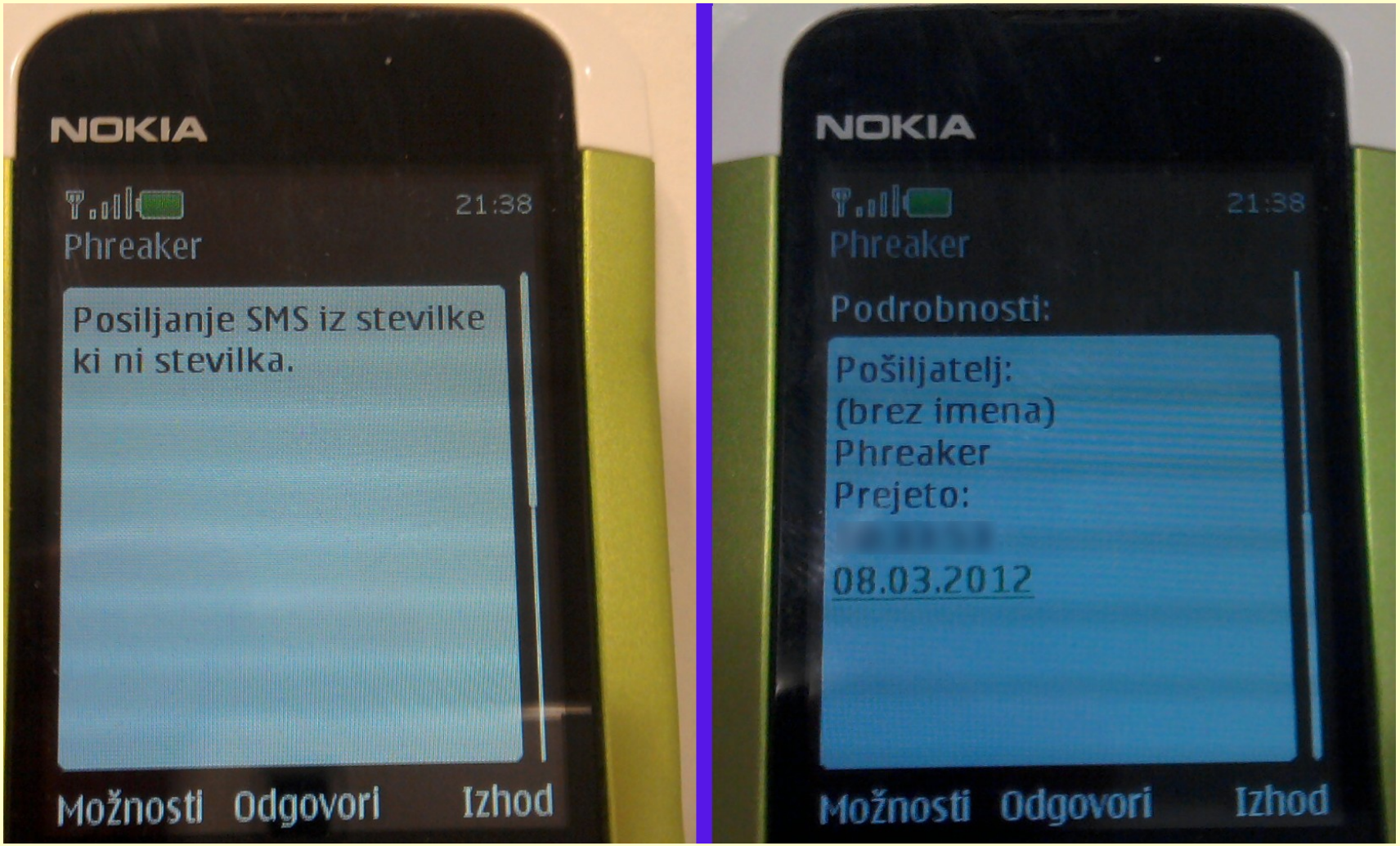

BUSTED!

Spoofing the identity of SMS sender

Sending of SMS “from” arbitrary number

<http://provider.com/sms/json?username=xxxxxxxx&password=xxxxxxxxx&from=Phreaker&to=38631123456&text=Sending%20of%20SMS%20from%20number%20which%20is%20not%20a%20number.>

Sending of SMS “from” arbitrary number



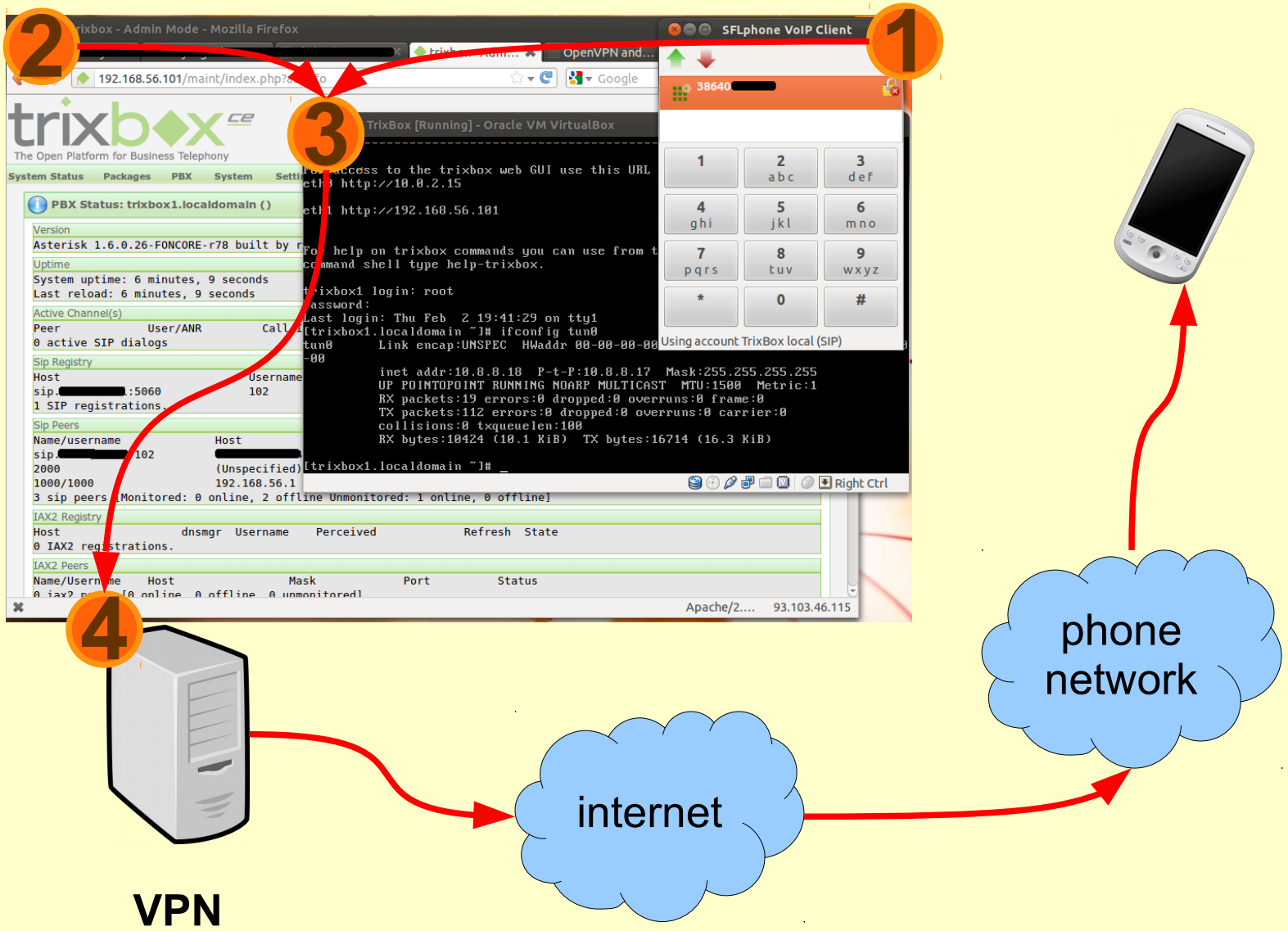

BUSTED!

Spoofing the identity of a caller

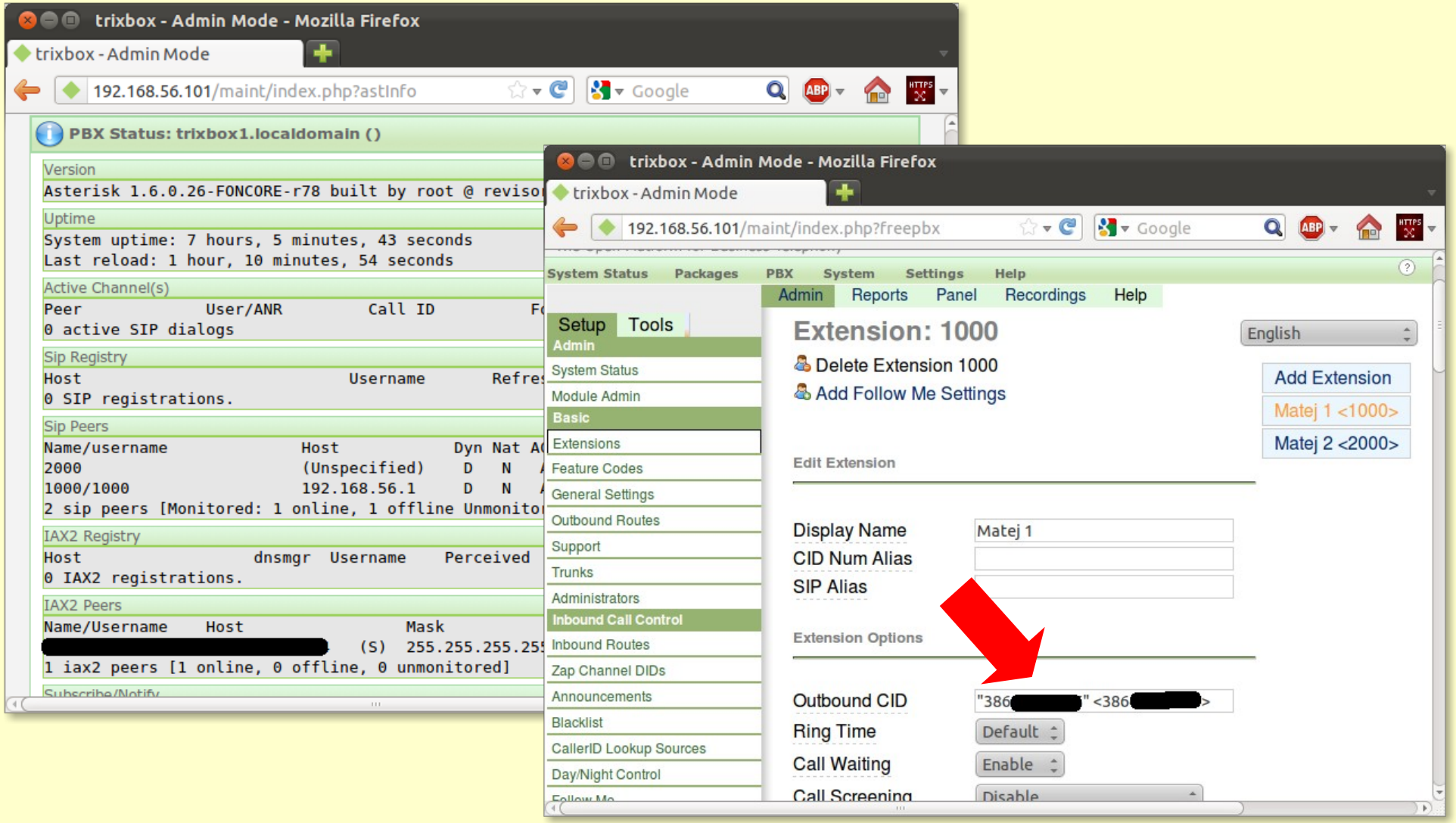
(some operators implemented security patches, but in certain circumstances, procedure still works)

Calling with arbitrary caller ID

1: setting-up the infrastructure



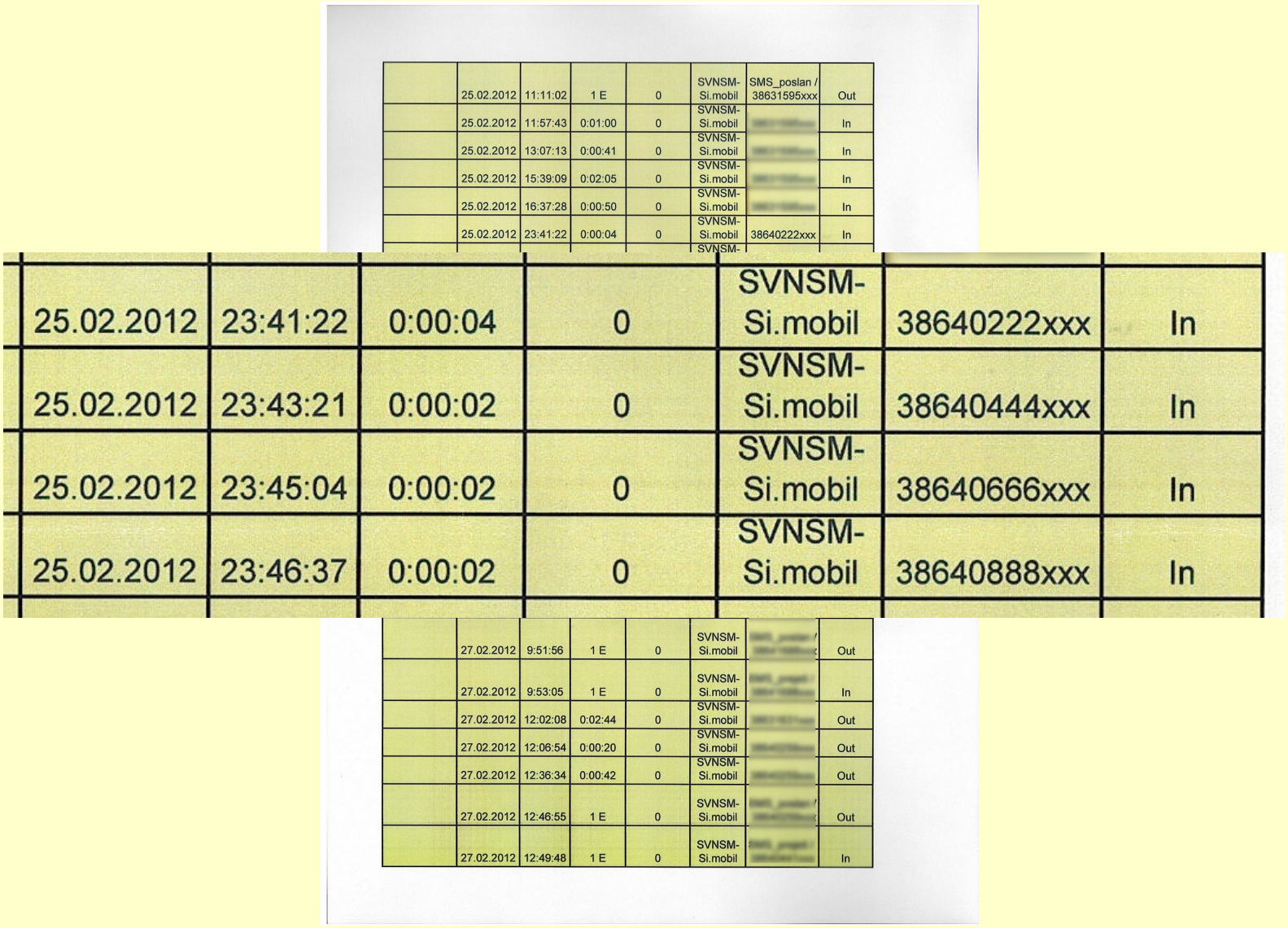
Calling with arbitrary caller ID
2: look into the virtual PBX



Calling with arbitrary caller ID

3: result on a phone

Calling with arbitrary caller ID
4: traffic data recorded by the mobile provider



	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

Practical use :-)

GSM module for unlocking the door

GSM module to open garage or front door

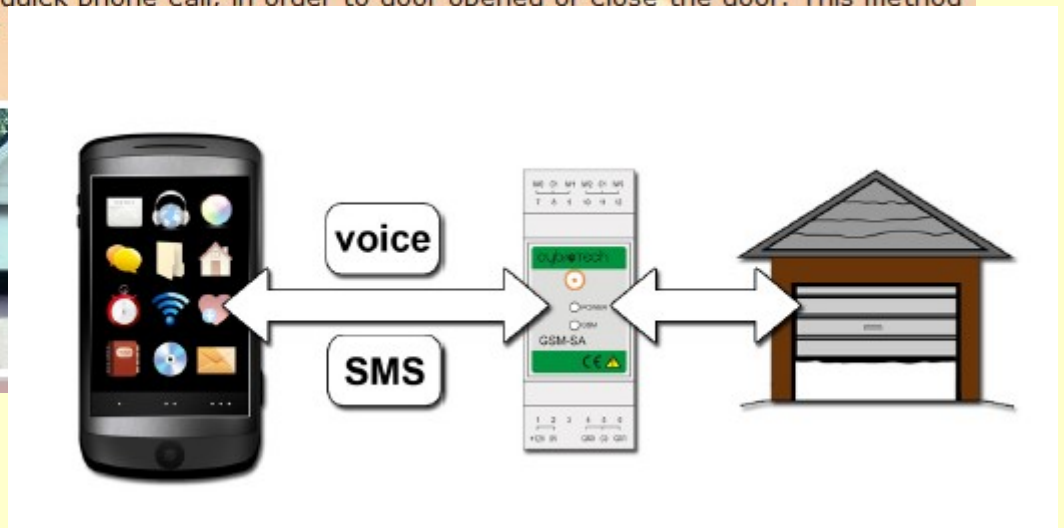
We offer a useful device with a simple phone call opens or closes the automated garage or front door.

GSM module is a device which allows an authorized user to open or close the door. Device recognizes up to five specific phone numbers from which they can call on a GSM module which opens or closes the door.

Iku d.o.o. offers you:

- delivery of a package with instructions for use,
- mounting points agreed upon (please call us and we will send you the offer).

Using the GSM module to open the door:
on automated garage, front door or other GSM module is installed, in which the records are up to five phone (mobile) numbers, which is possible with a quick phone call, in order to door opened or close the door. This method accounts for the use of remote controls or
mobile phone is already




BUSTED!

GSM traffic security

GSM security – the beginning of the story

John Nevil Maskelyne
(1839 – 1917)

Kiberpipa
(2012)

Wiki
The Hacker's Choice

Search Titles Text
Login

Redirected from page "*A5CrackingProject*"

Clear message

Immutable Page *Info* *Attachments* More Actions: *FindPage* *RecentChanges*

cracking a5

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.

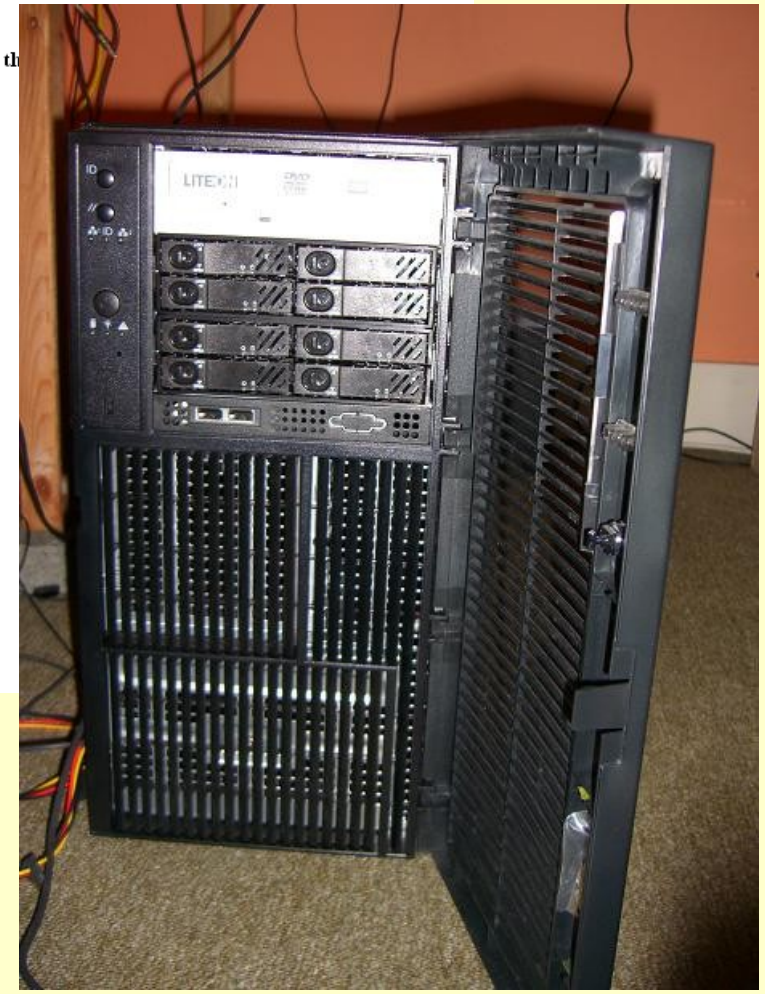
NEWS: We have created a PRIVATE A5 mailinglist. If you feel you have something to contribute to th
The reason for this has been explained on the public mailinglist a5 [at] lists.segfault.net.

Powered by *EFF*.

Contents

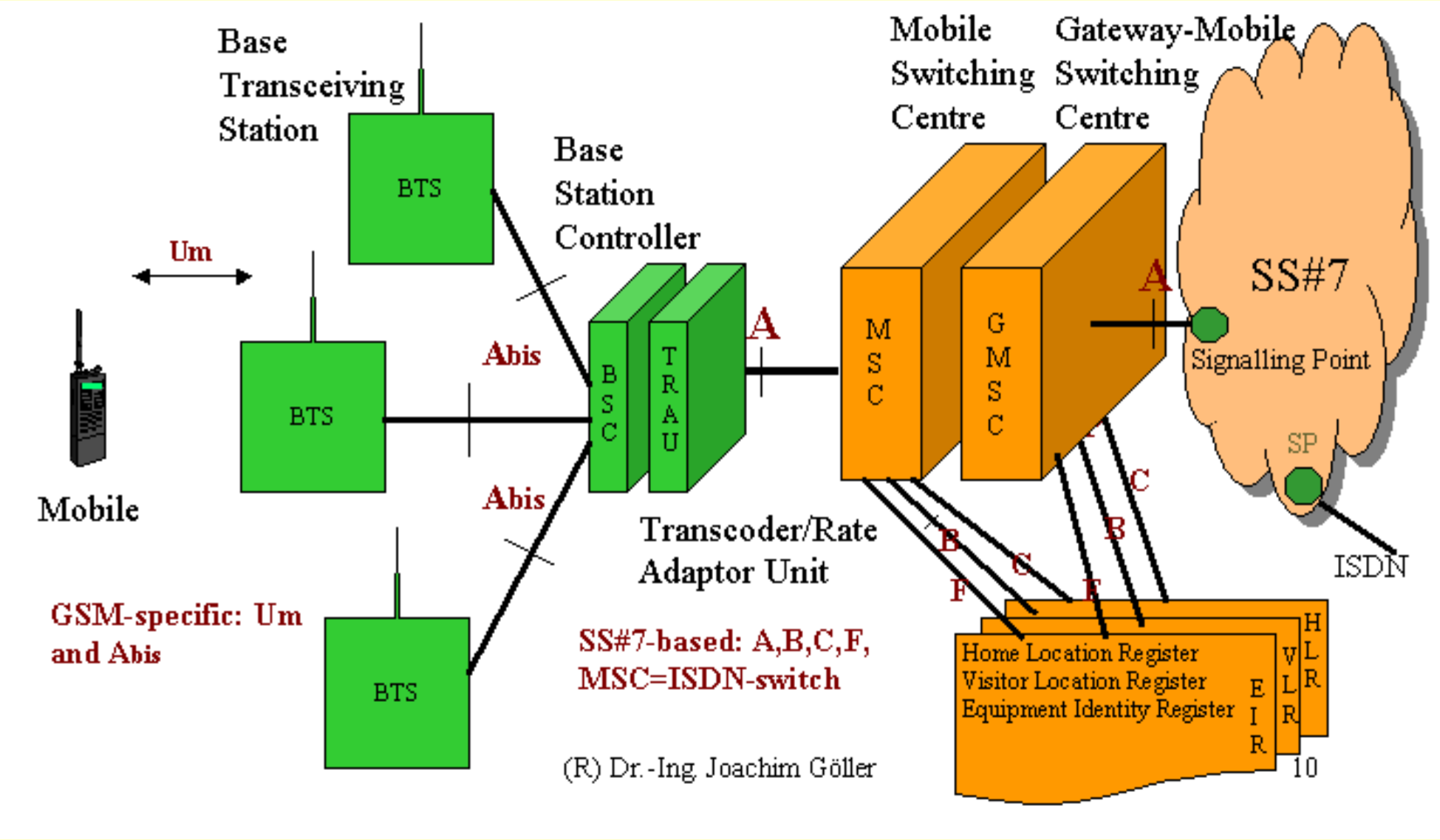
GSM cracking project

Nokia 3310



A5 Buster

Some GSM basics



SIM card and mobile equipent, IMSI, TMSI, A5/x, "broadcast channels" and data channels...

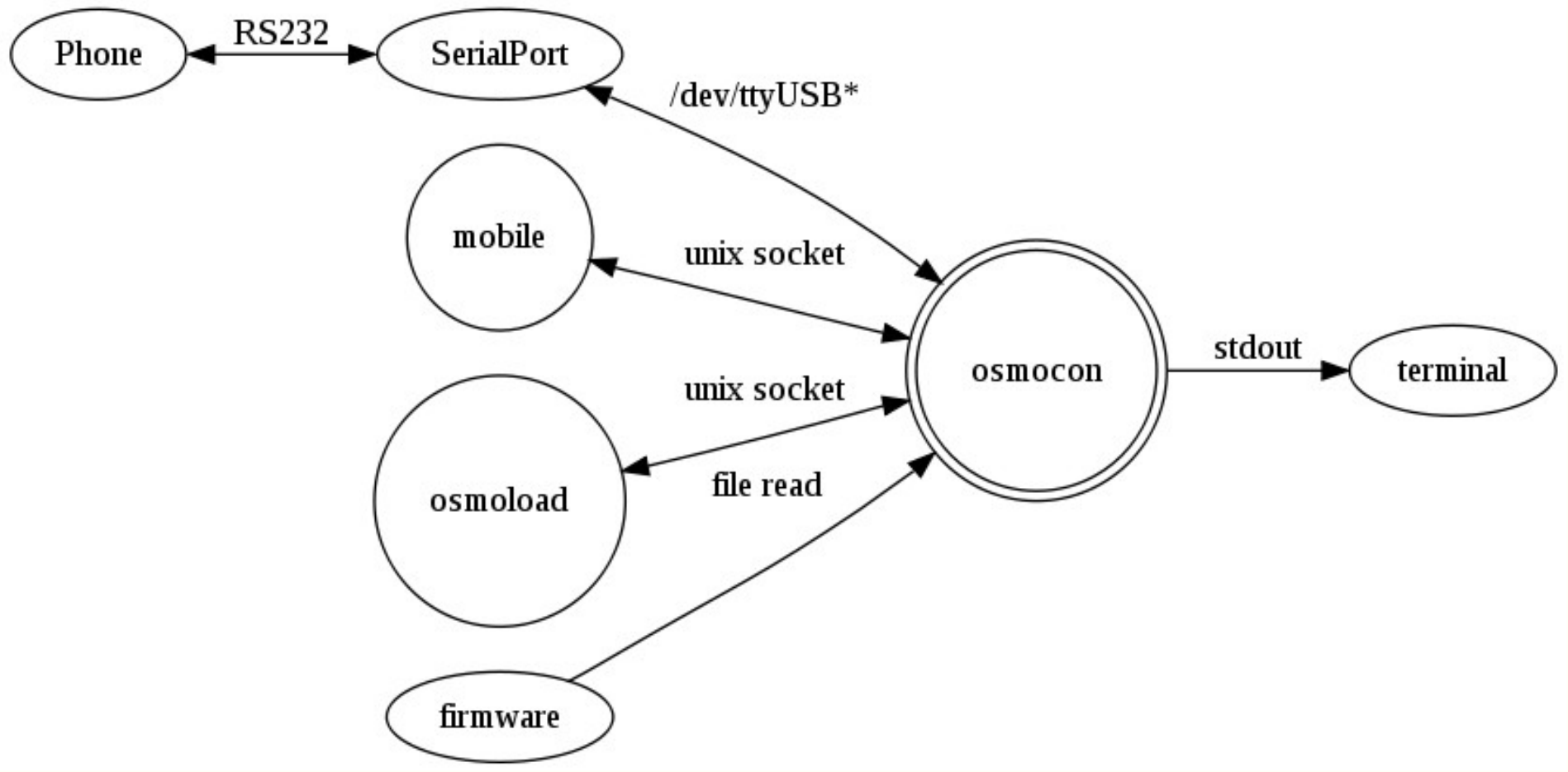
Scheme of the GSM network, source: *www.gsmfordummies.com*.

OsmocomBB

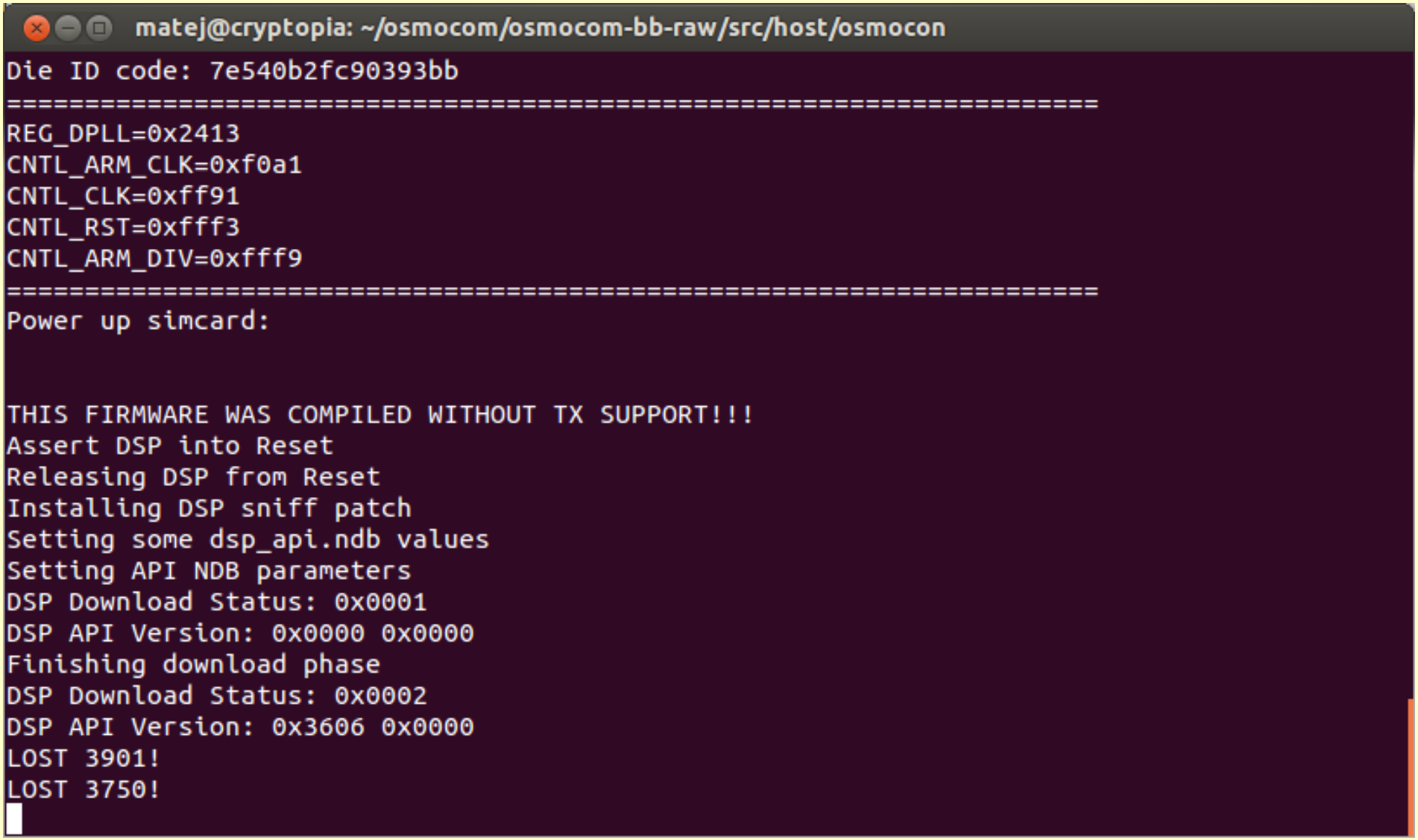
Mobile phone with Calypso chipset...

Hardware part can consist of other devices too, see RTL-SDR project!

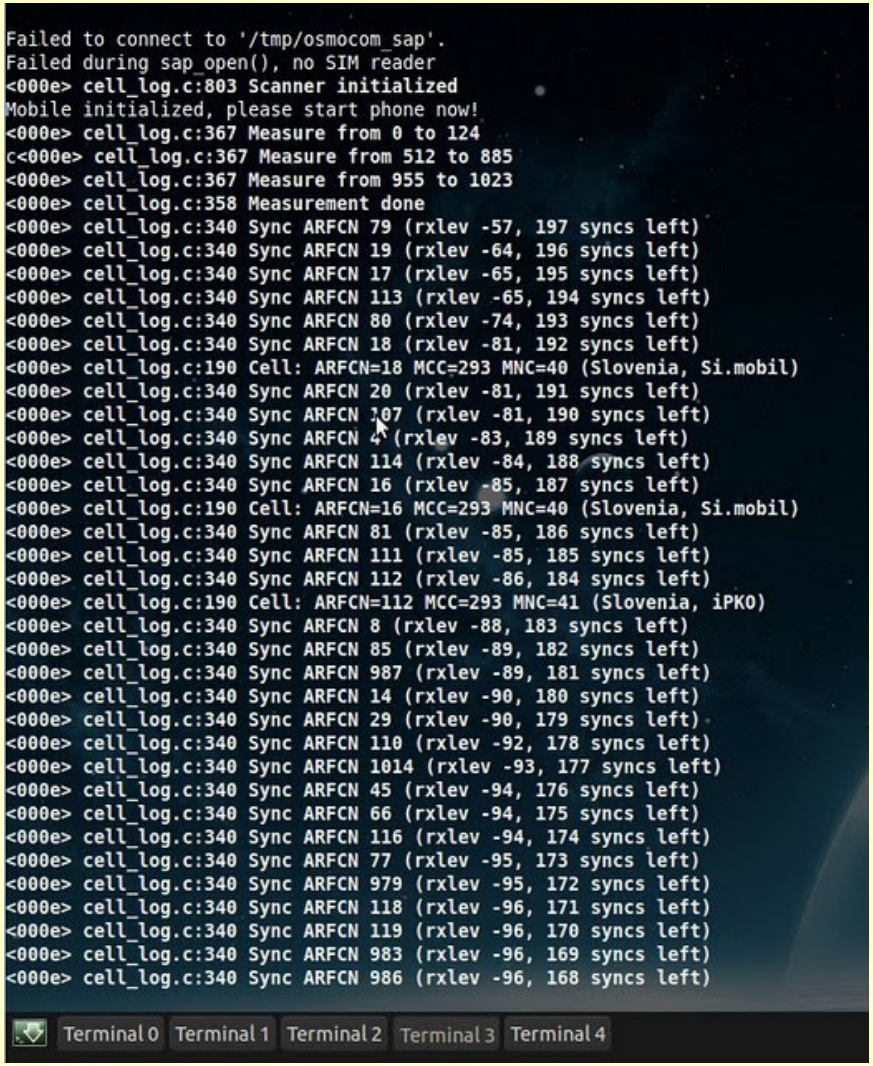
...and OsmocomBB firmware



Loading romloader

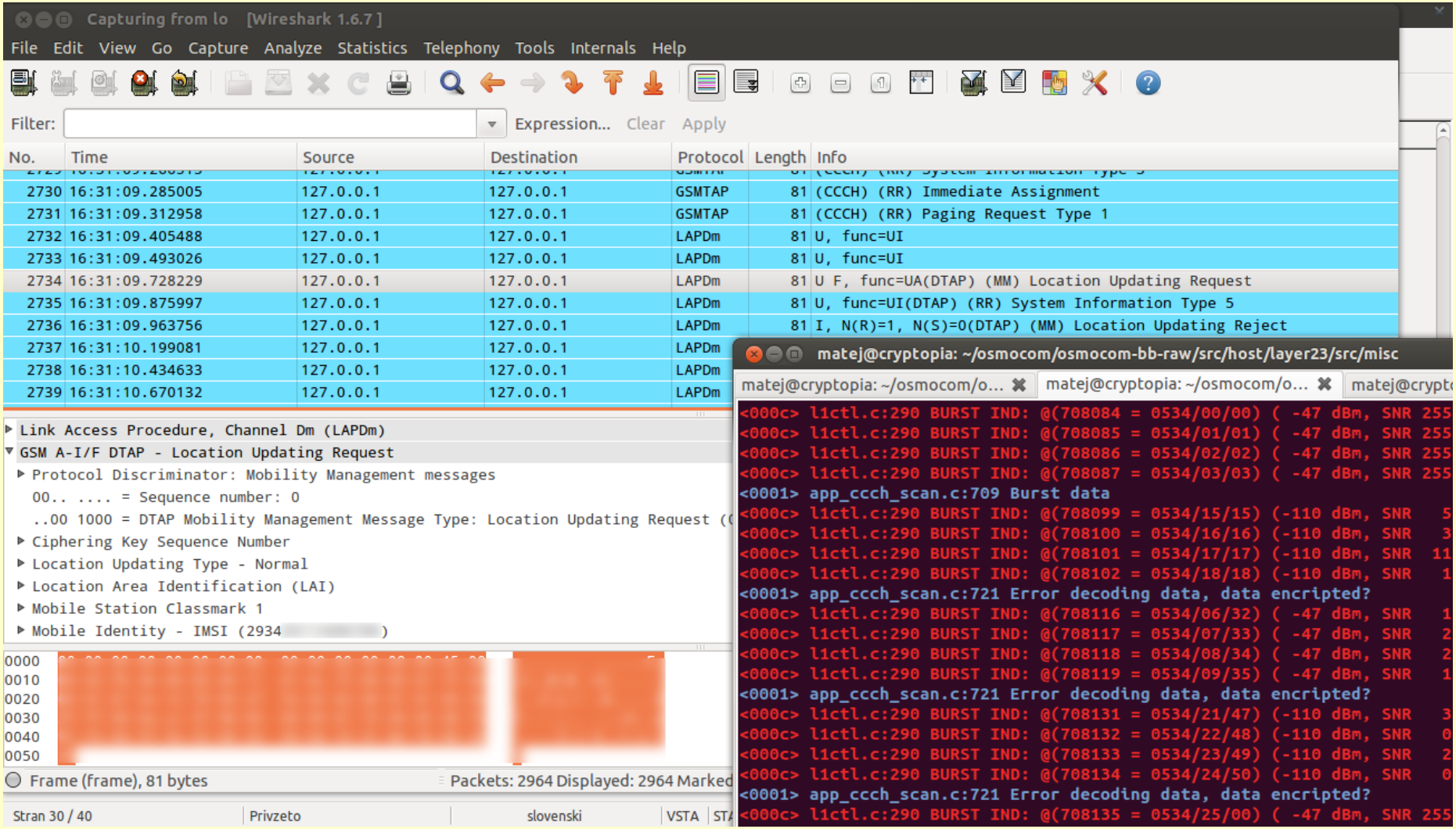


Base station scan...



ARFCN scan with *cell_log* application.

GSM traffic analysis...



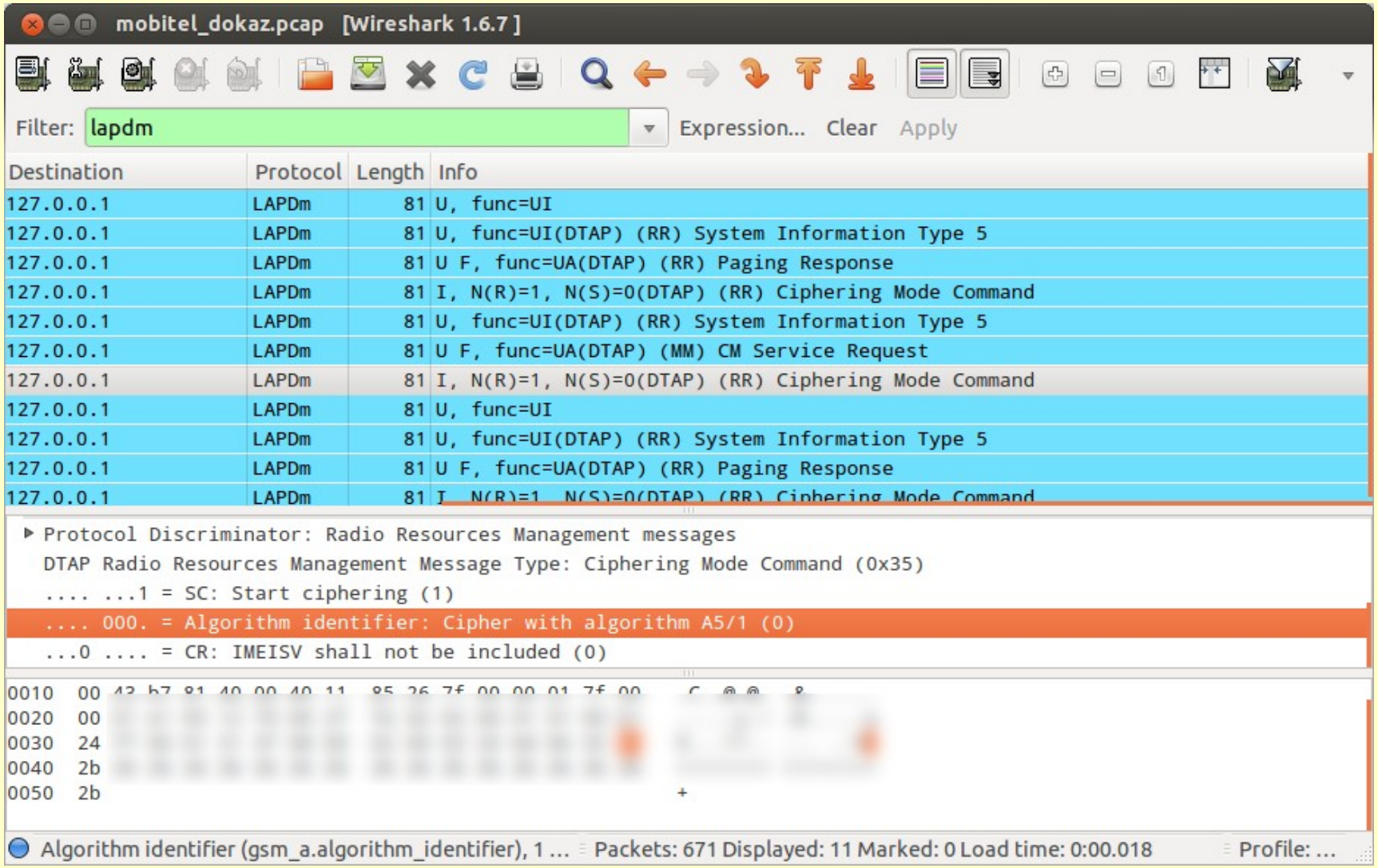
GSM traffic analysis. Traffic is captured with *ccch_scan* application and shown in Wireshark.

Security analysis of slovenian GSM networks

Authors: Jaka Hudoklin, Matej Kovačič, Primož Bratanič

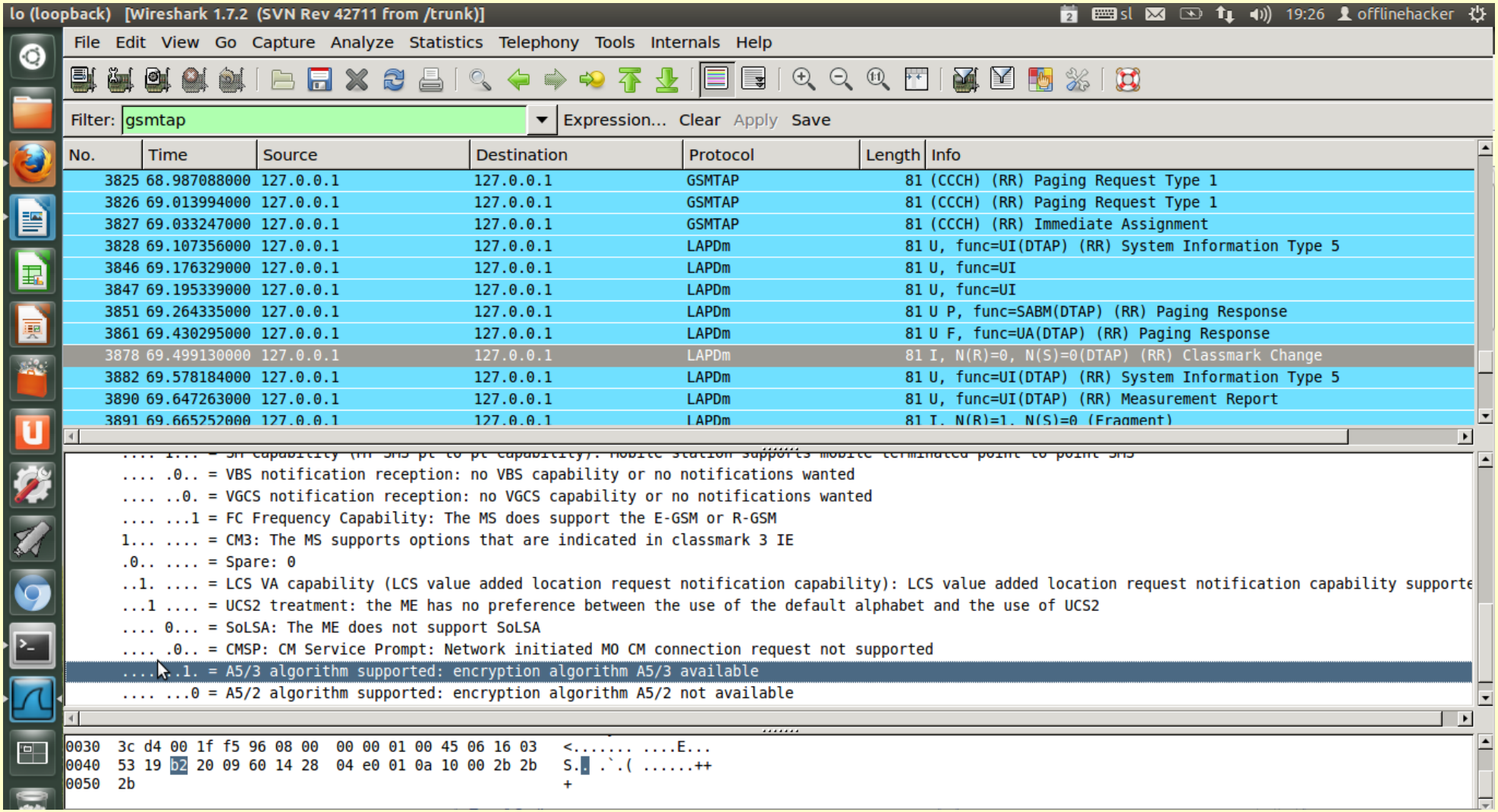
[some vulnerabilities described are already fixed]

Use of encryption - Mobitel



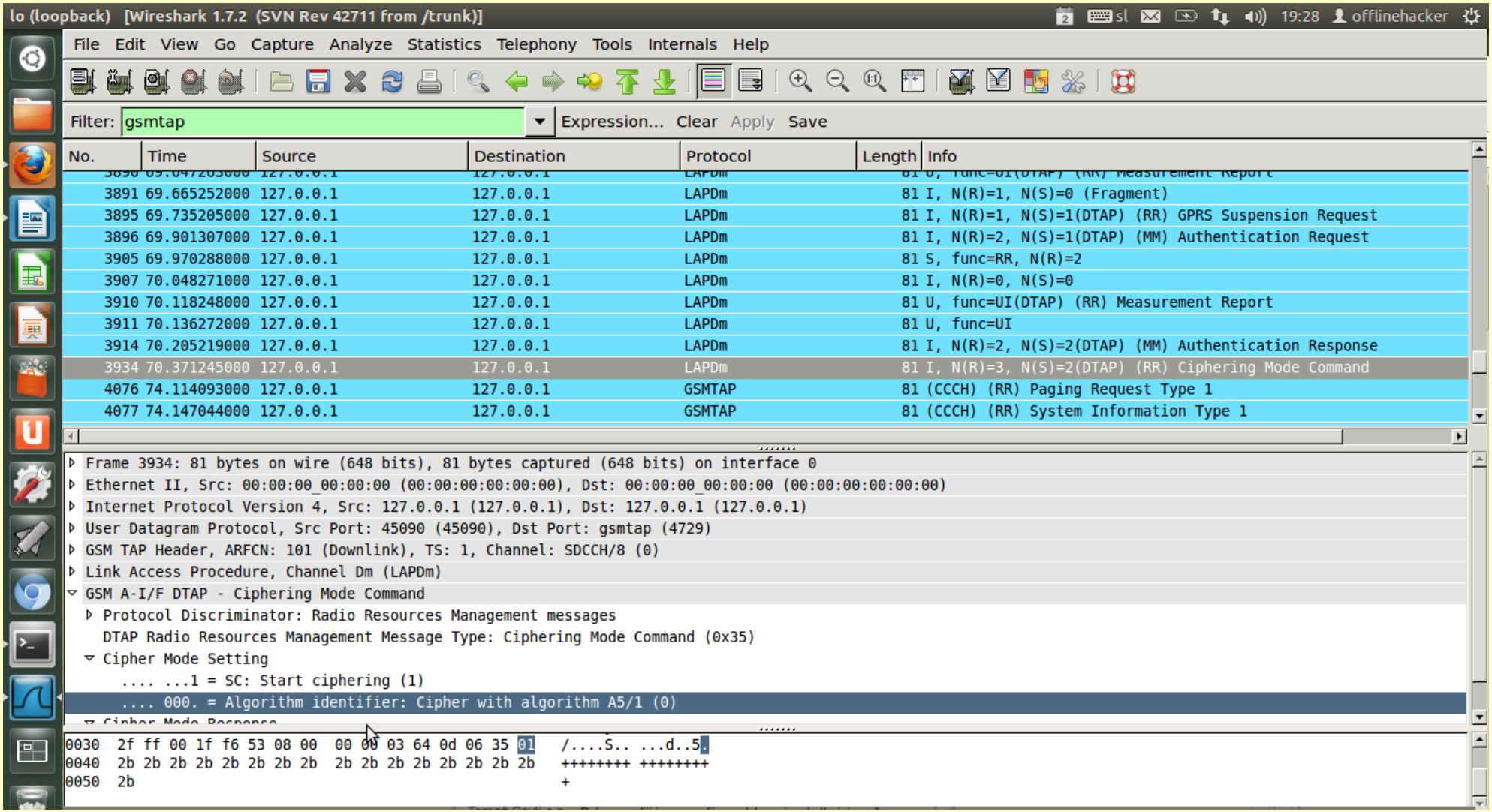
Mobitel was using A5/1 encryption.

Use of encryption - Mobitel



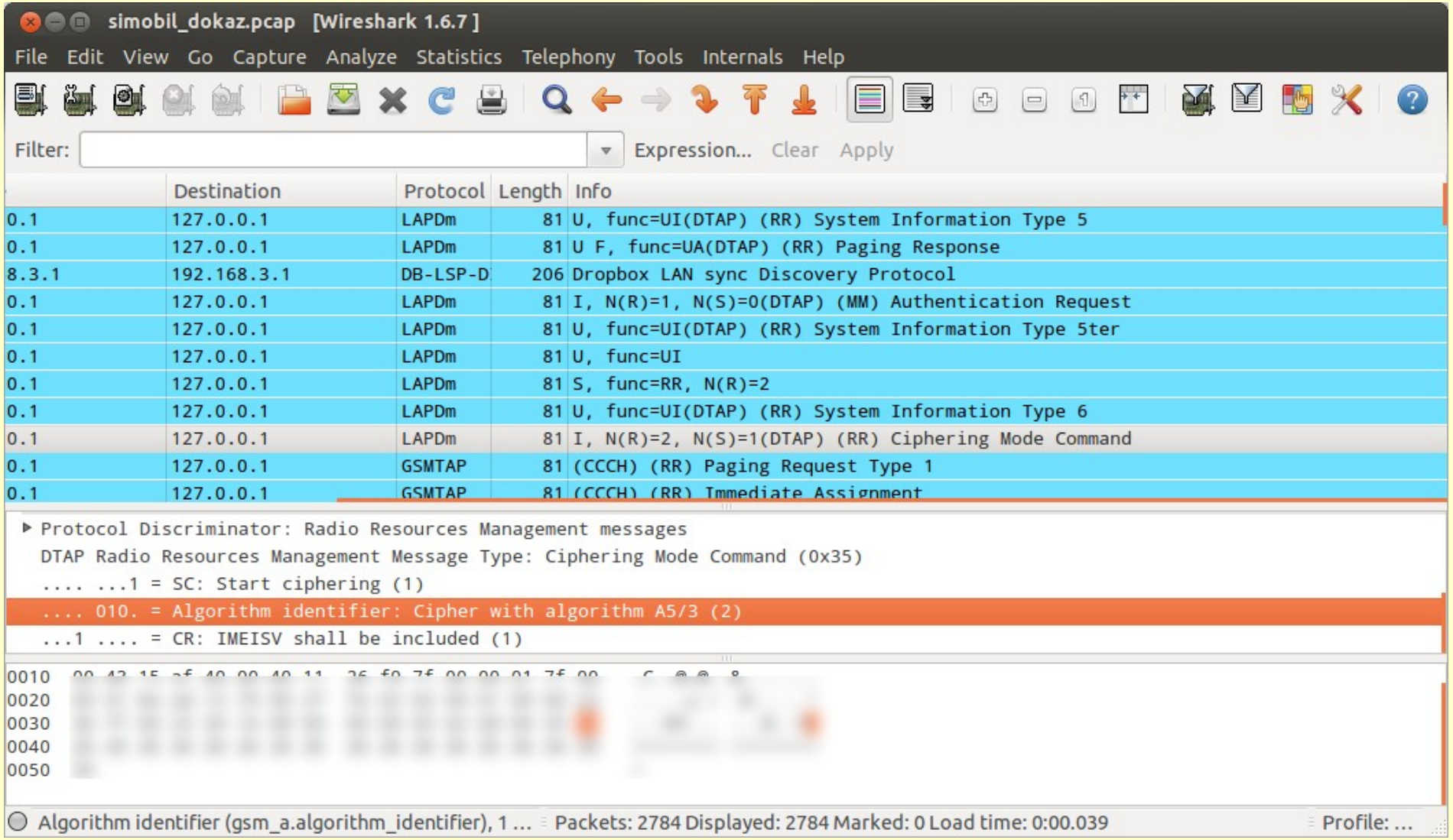
If mobile phone said it is supporting A5/3...

Use of encryption - Mobitel



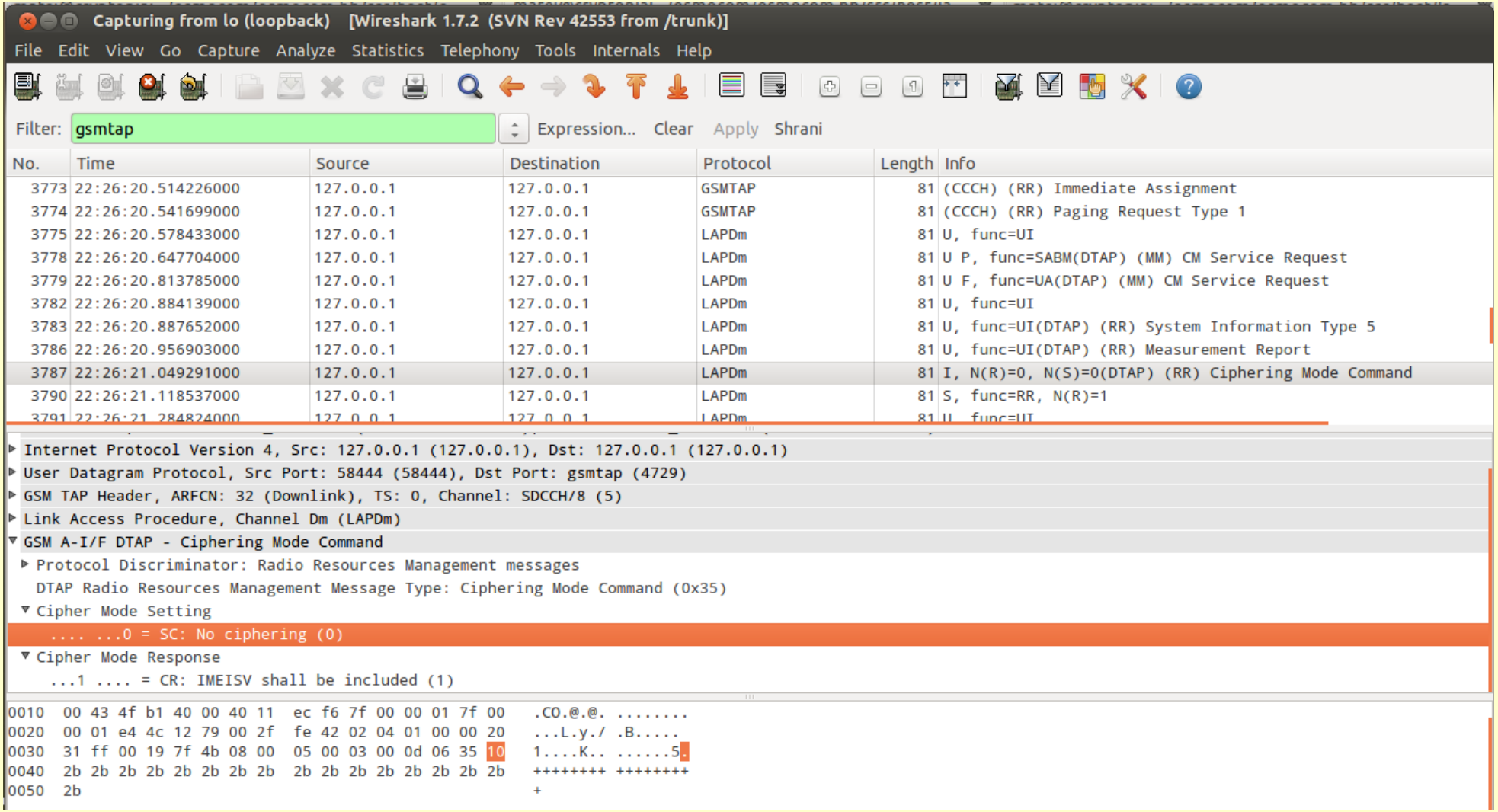
...network replied that only A5/1 is available.

Use of encryption - Simobil



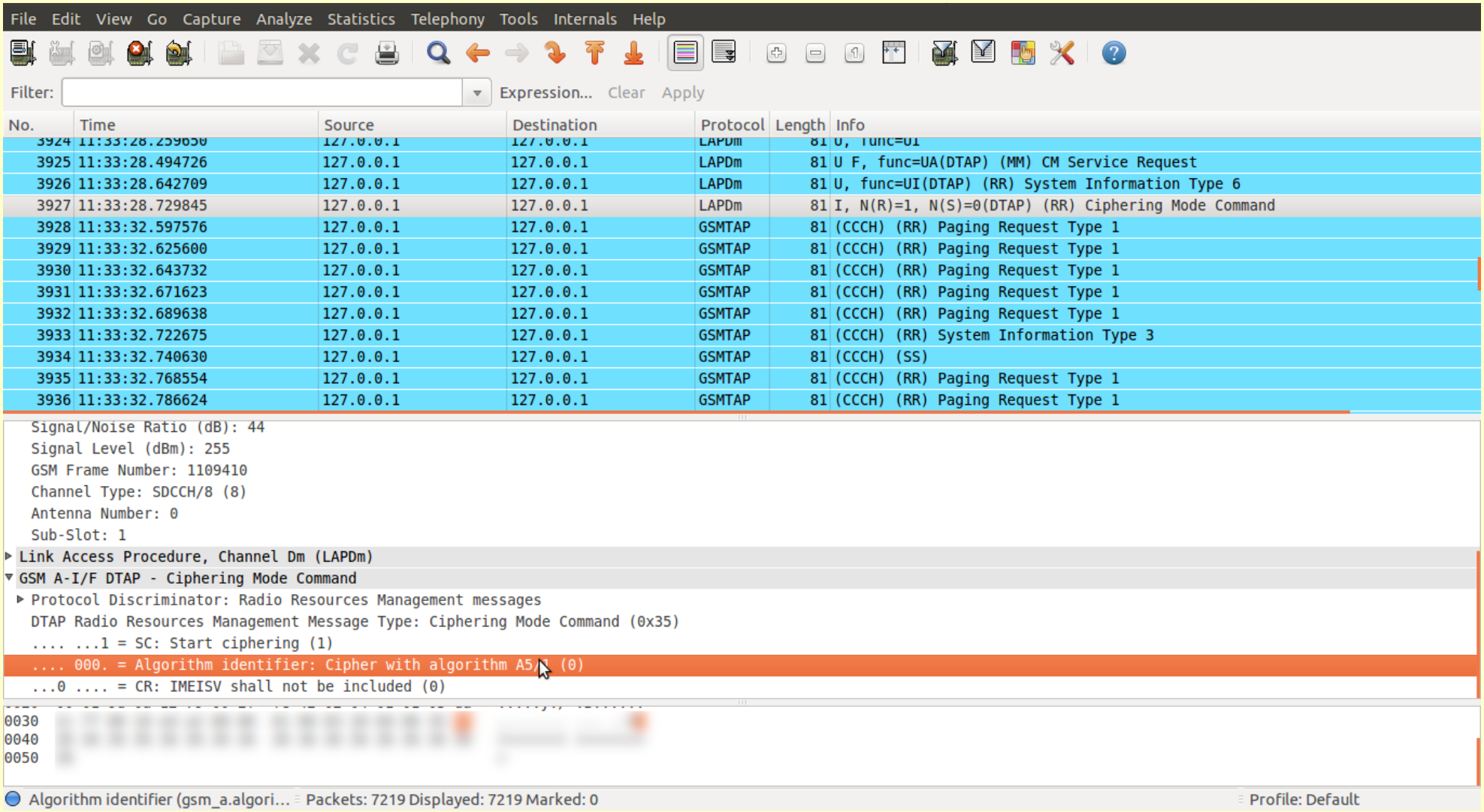
Simobil was using A5/3 also, however...

Use of encryption - Simobil



...it was possible to switch the encryption completely off (use of A5/0).

Use of encryption - Tušmobil



Tušmobil was using encryption algorithm A5/1.

Cryptanalysis if session key Kc

(without possession of mobile phone and/or SIM card)

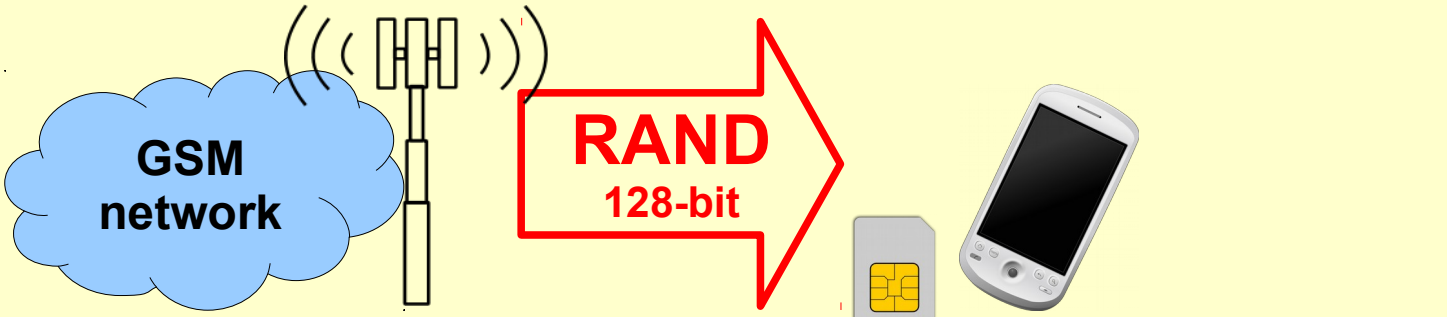
[on this specific attack are vulnerable only networks with A5/1 and without random padding]

[slightly modified attack can be successfully used against networks with random padding]

Creating of session key Kc

Encryption key **Ki** is stored on a SIM card **and in** HLR registry. Session key **Kc** derives from **Ki**, and is used to encryption of SMS and voice conversation.

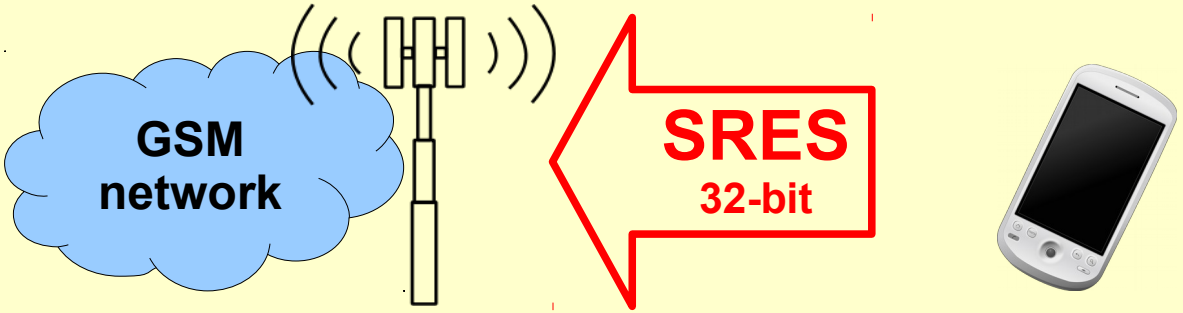
1.



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

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

2.



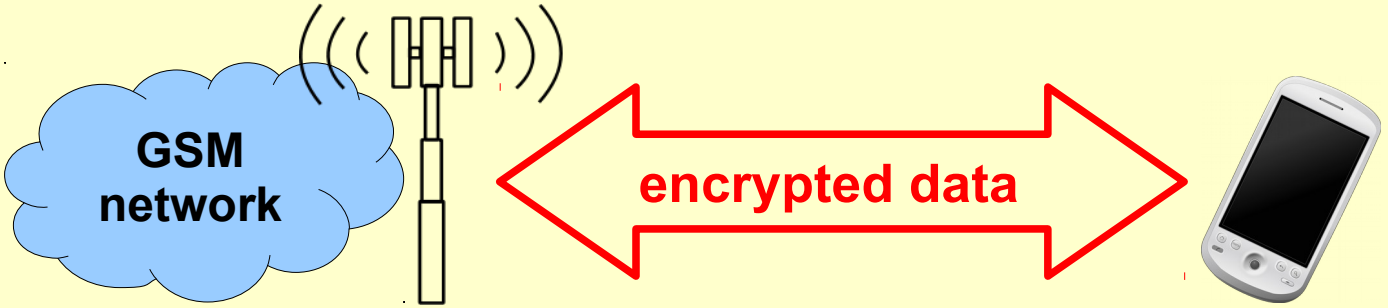
Network verifies **SRES** from mobile phone.

Creating of session key Kc

3. On both sides Kc is created (with use of A8 algorithm):

Ki + RAND @ A8 = **Kc**

4.



If SRES is the same on both sides, network and mobile phone have both the same Kc. That means session key is "exchanged" without being transfered through the network. Encryption is now being done with Kc + A5/x. "Over the air" are transferred only encrypted data.

Cryptanalysis of A5/1

a theory

CONTENT OF DATA BURST IN GSM

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

f(Kc)

"ONE-TIME" KEY FOR ENCRYPTION OD DATA STREAM

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

Kraken

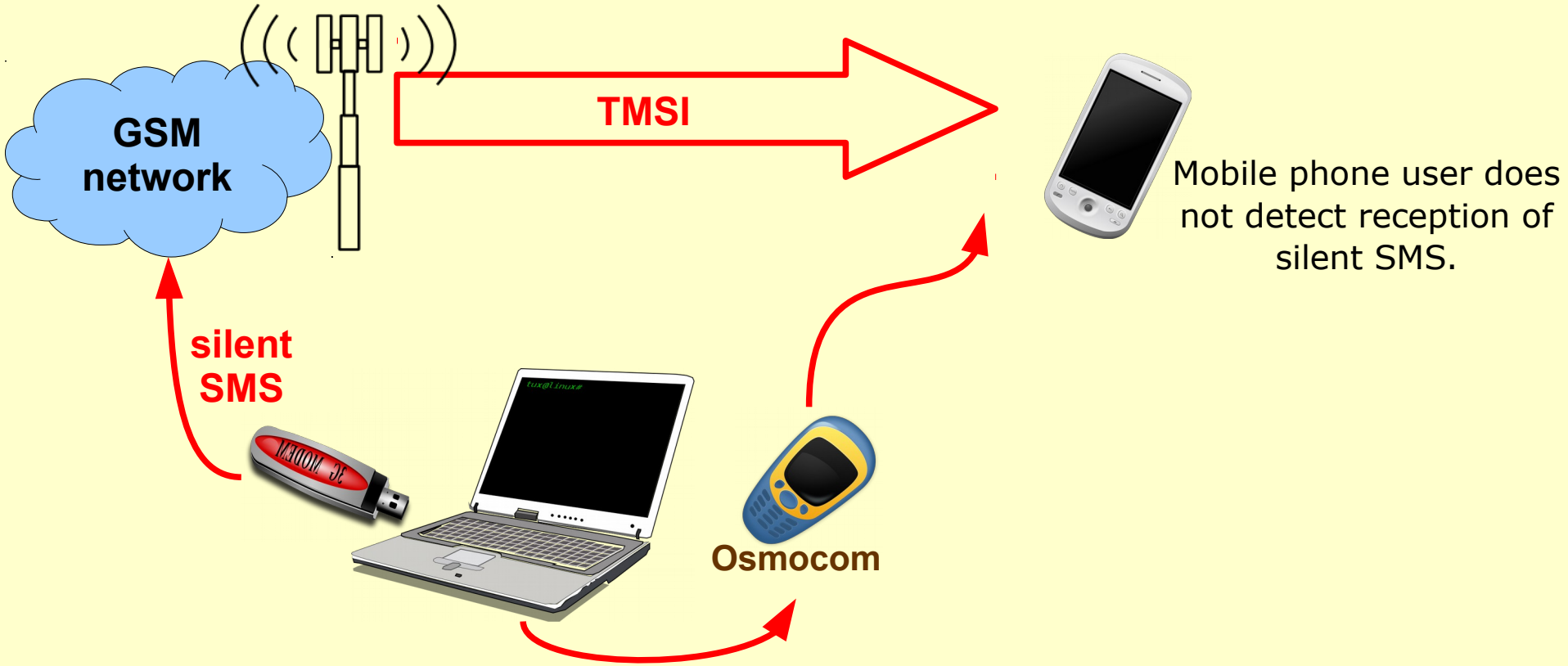
ENCRYPTED MESSAGE (XOR)

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

Kc

Locating of user in mobile network

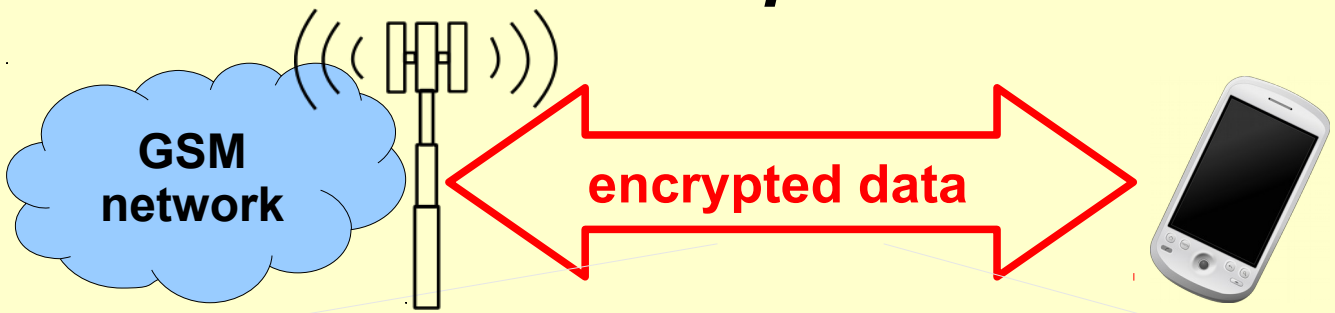
We start sending silent SMS'es to a mobile number. During this we observe which TMSI number is receiving (encrypted) data.



Capture and cryptanalysis of A5/1

a practice

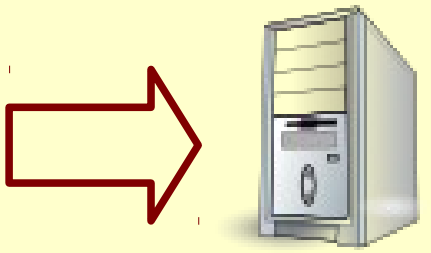
5.



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

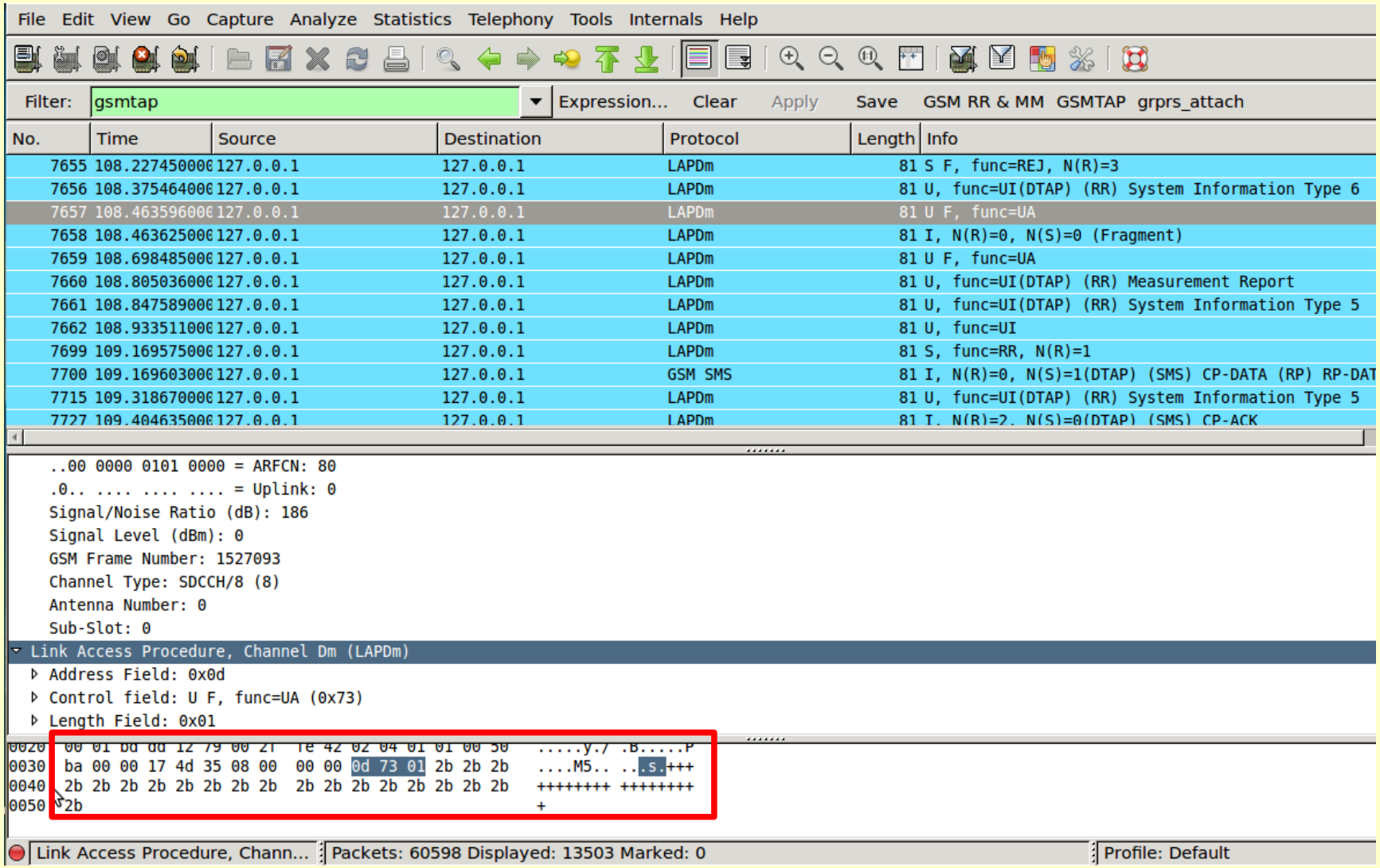
CONTENT OF DATA BURST IN GSM

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

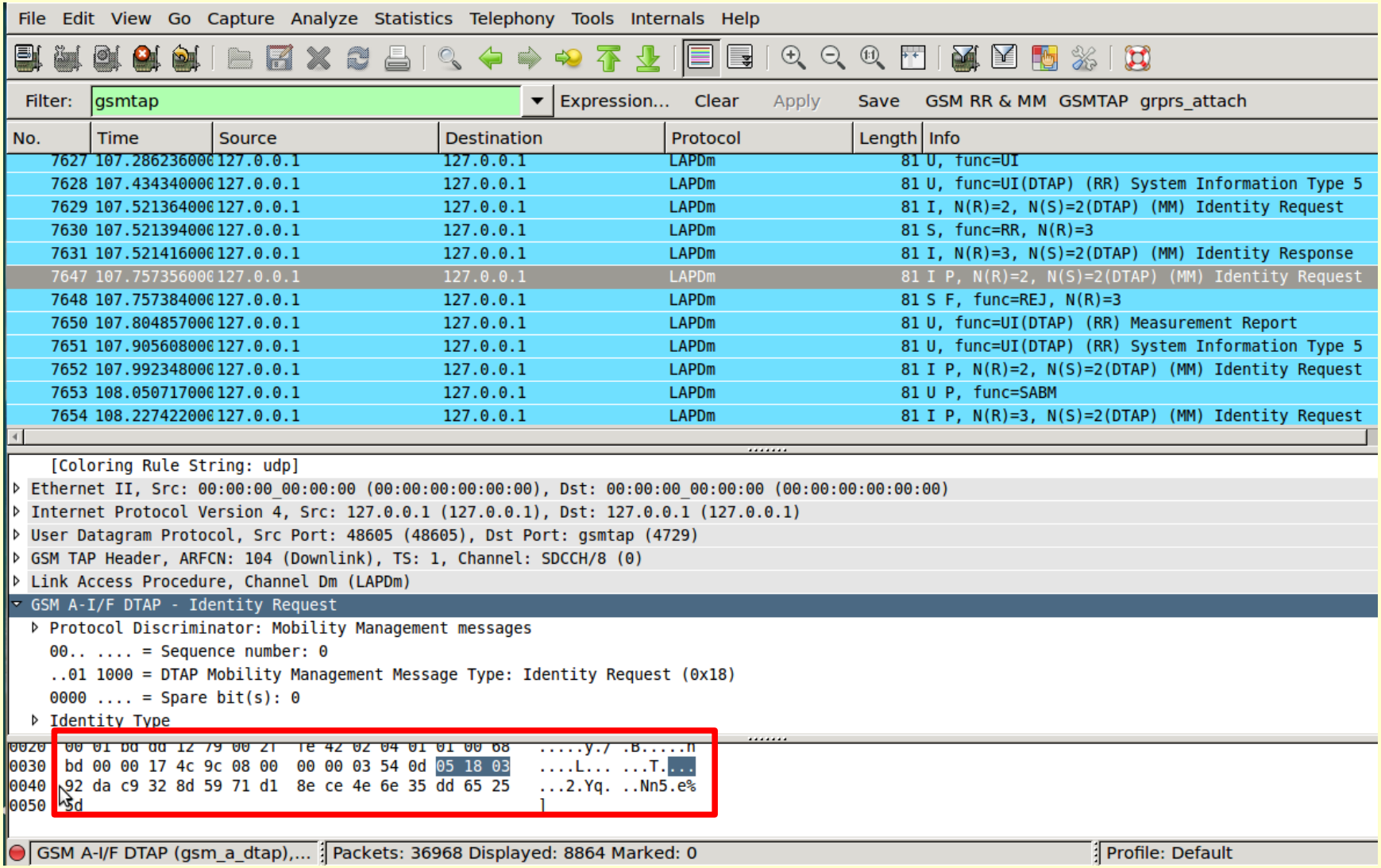


- From the “air” we passively capture encrypted data packets.
- With the help of guessing the contents of the GSM burst (guessing the padding bits) we calculate “one-time” encryption key.
- We use cryptanalysis to reconstruct session key Kc.
- In the process we need no access to the SIM card, mobile phone or mobile network!

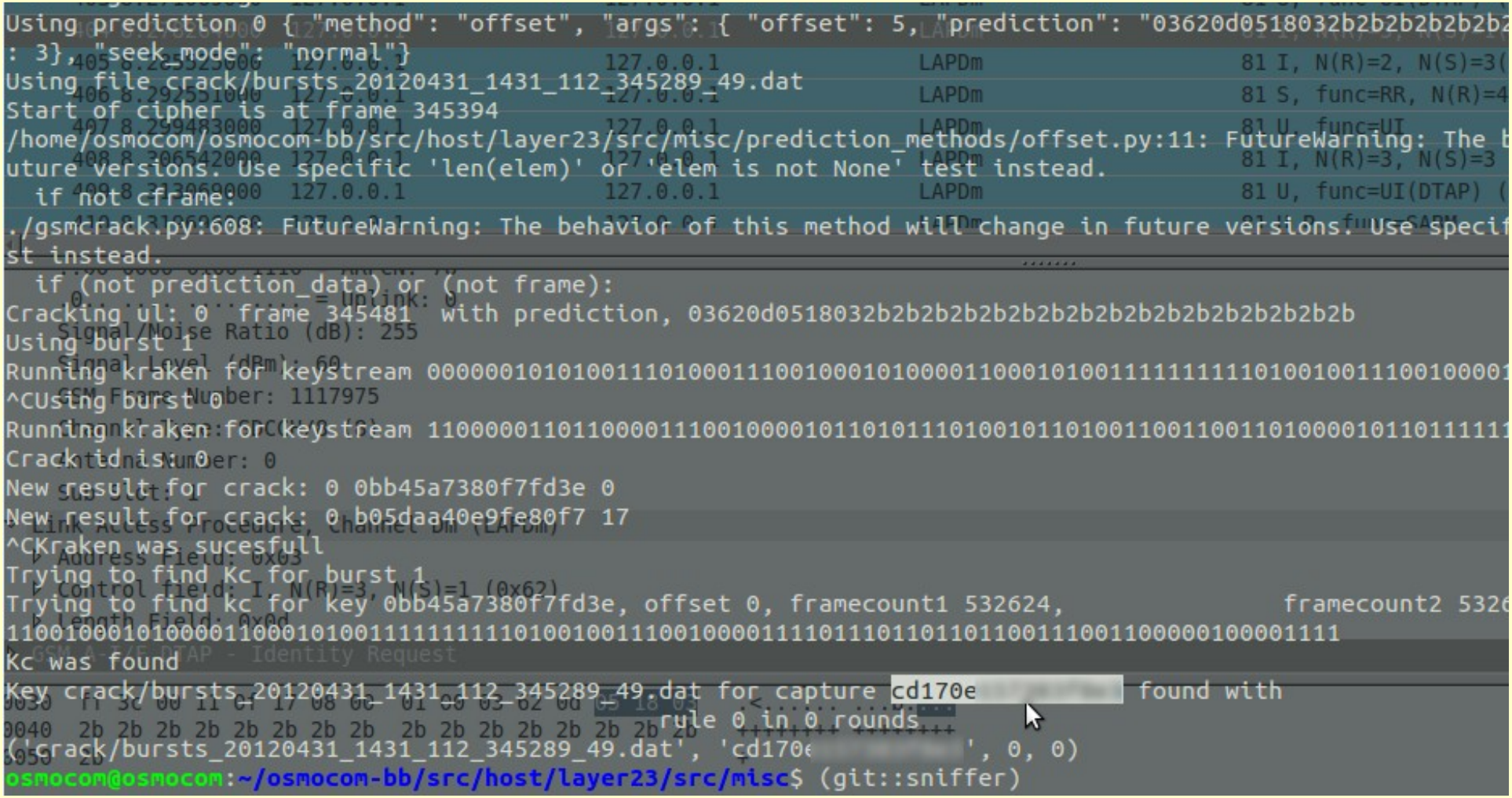
Non-random padding



Random padding

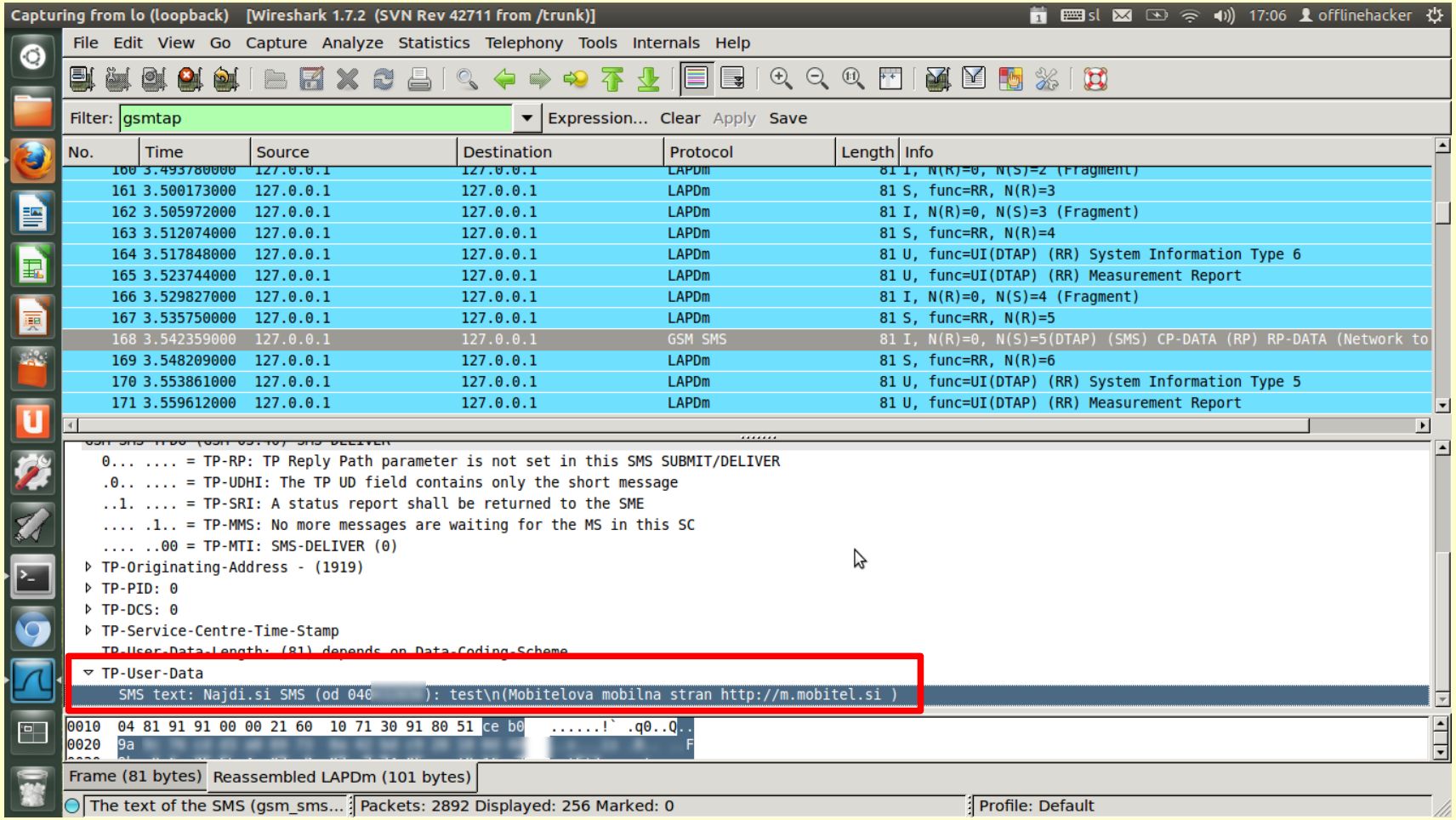


Cracking A5/1 session key Kc in a practice



Cracking (cryptanalysis) with Kraken and predictions we are using in our *gsmcrack.py*...

Cracking A5/1 session key Kc in a practice



… and decrypted SMS message (received through 2G network).
Application gsmcrack.py automatically identifies the TMSI number from the phone number (by sending silent SMS's). When we have TMSI of the “target”, our application is able to automatically follow the phone to an assigned dedicated channel and record encrypted message.


BUSTED!

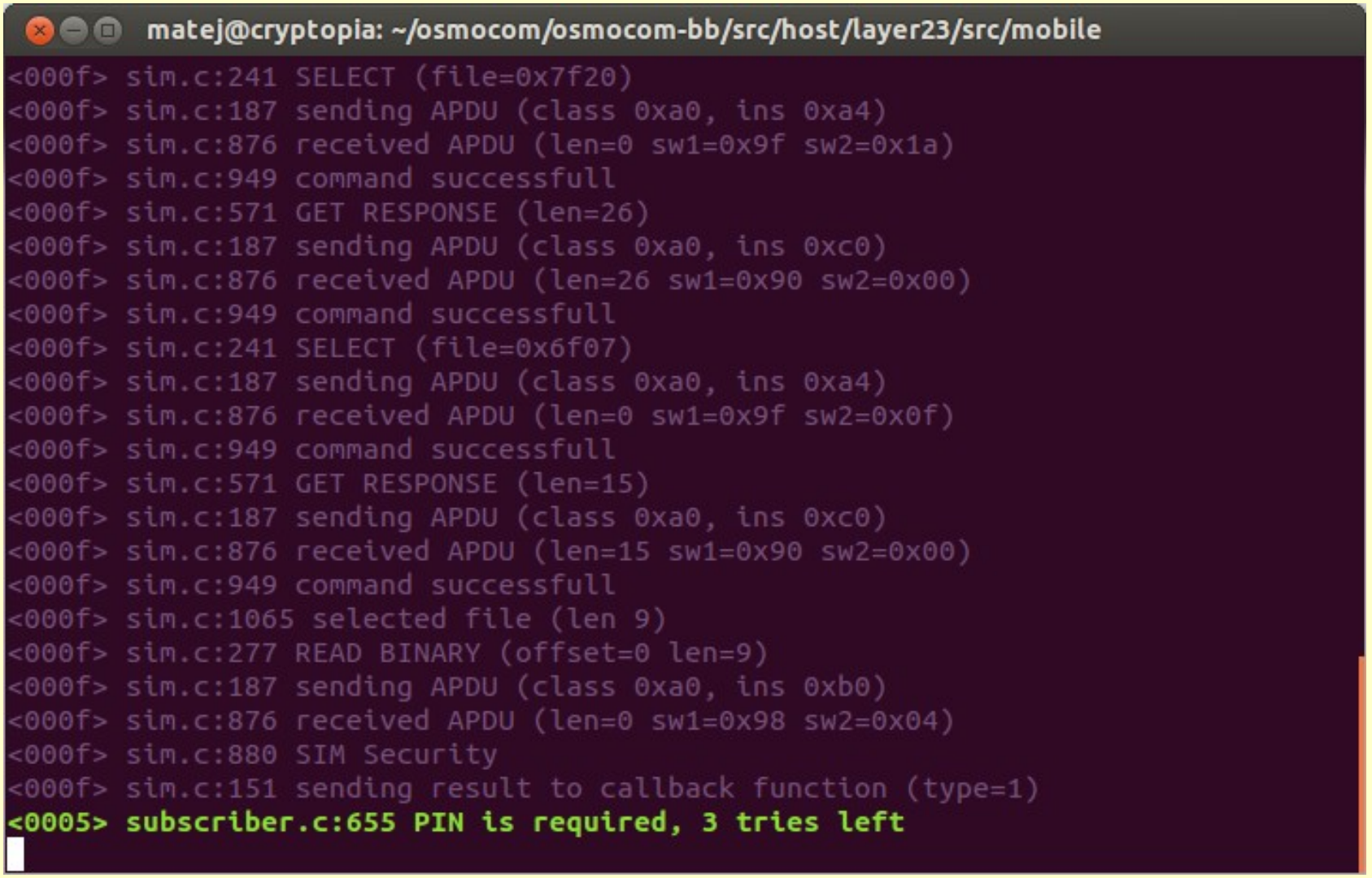
Mobile identity

Mobile identity spoofing in GSM network

(without possession of mobile phone and/or SIM card)

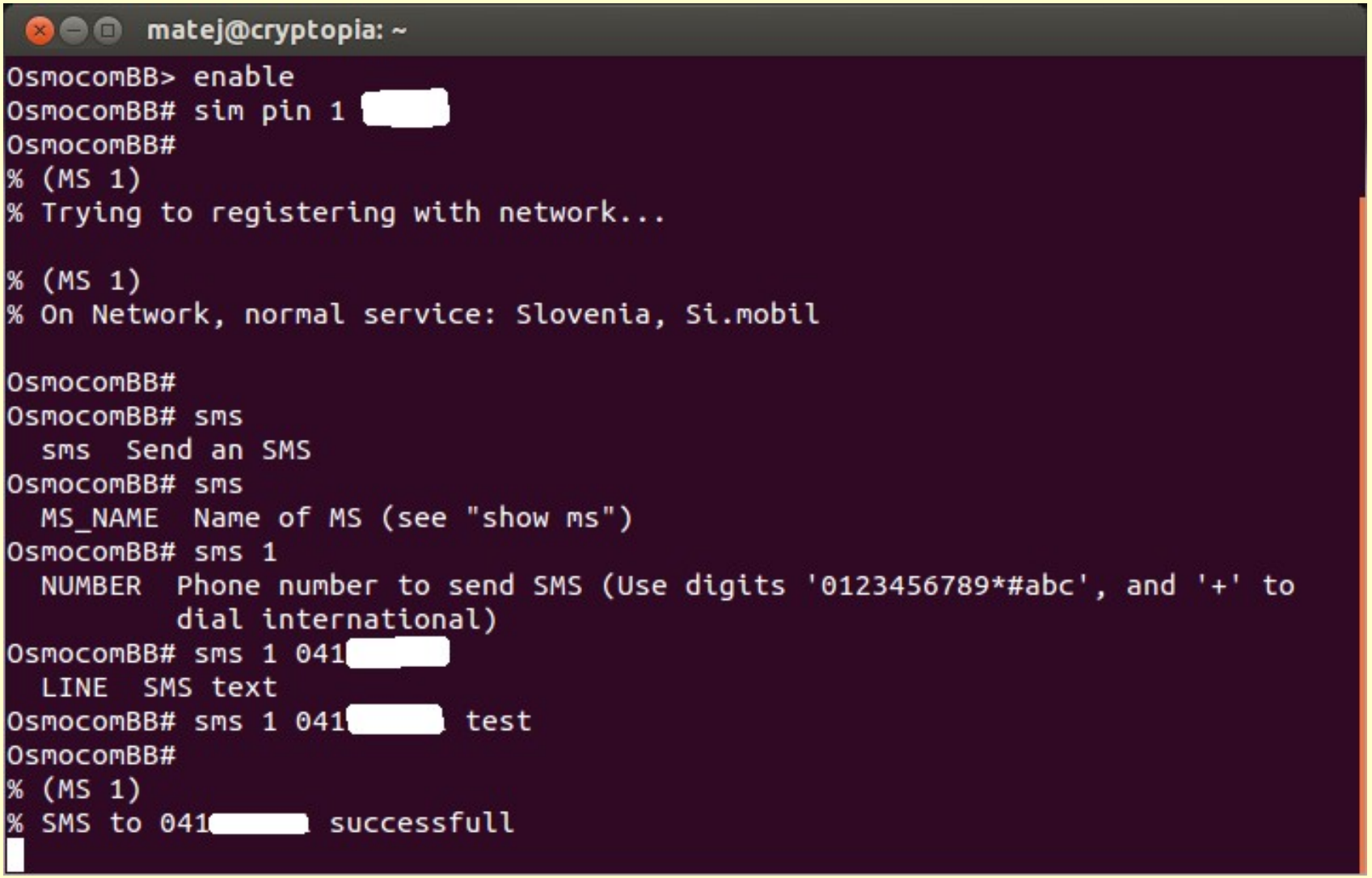
[vulrenability were fixed in most of slovenian GSM networks, procedure described is not working anymore]

Application *mobile*



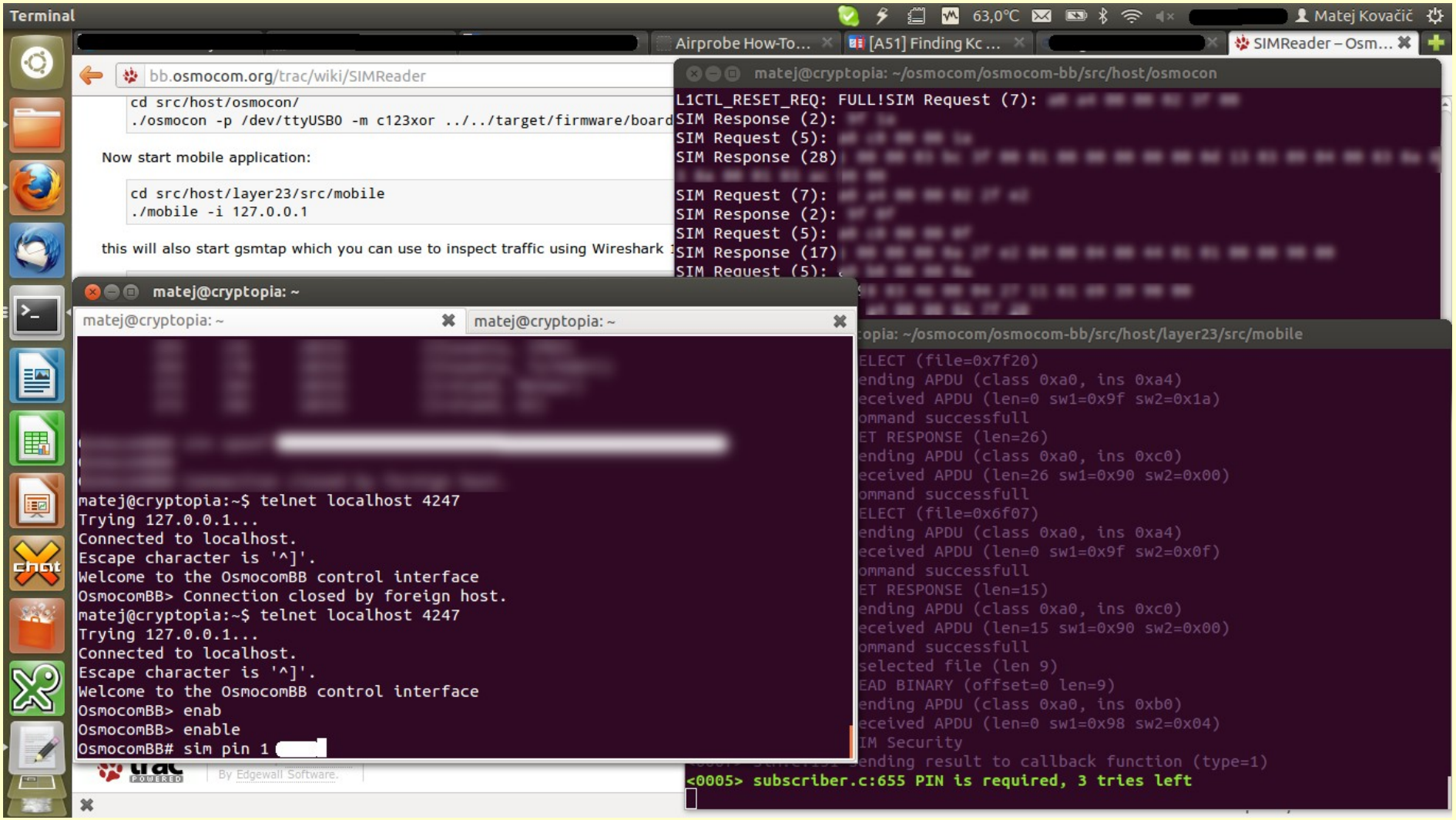
Application *mobile* is used fro calling and sending and receiving SMS messages on a OsmocomBB mobile phones.

Application *mobile*



Sending of SMS message from application *mobile*.

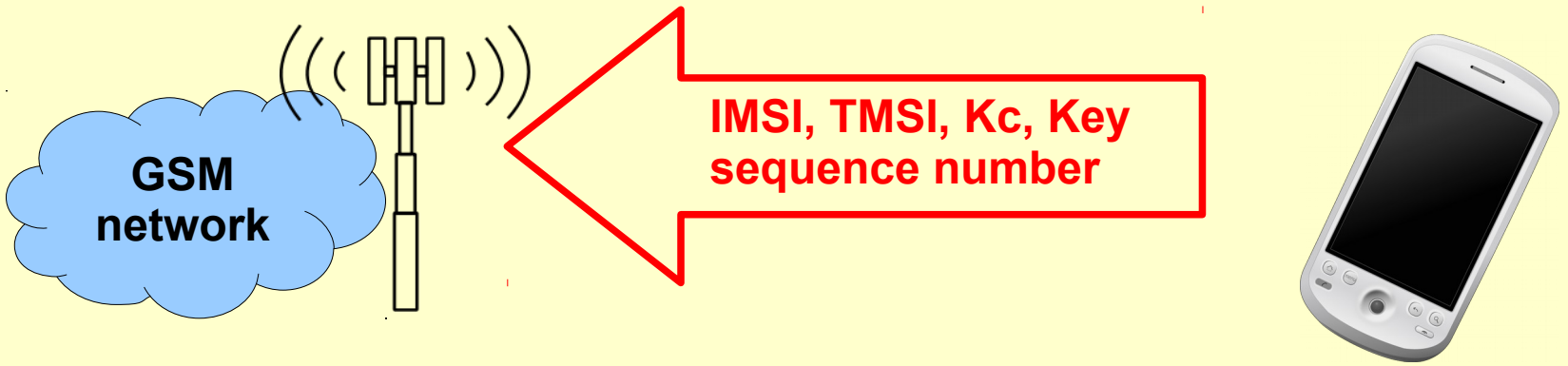
Application *mobile*



Use of application *mobile*. In the background Osmocom ROM loader, aplication *mobile* and (in front) console of application *mobile*.

Mobile identity in mobile network

Users in the mobile network does not identify themselves by the phone number, but with the IMSI and TMSI number. Important parameters are also the encryption key Kc and the Key sequence number.

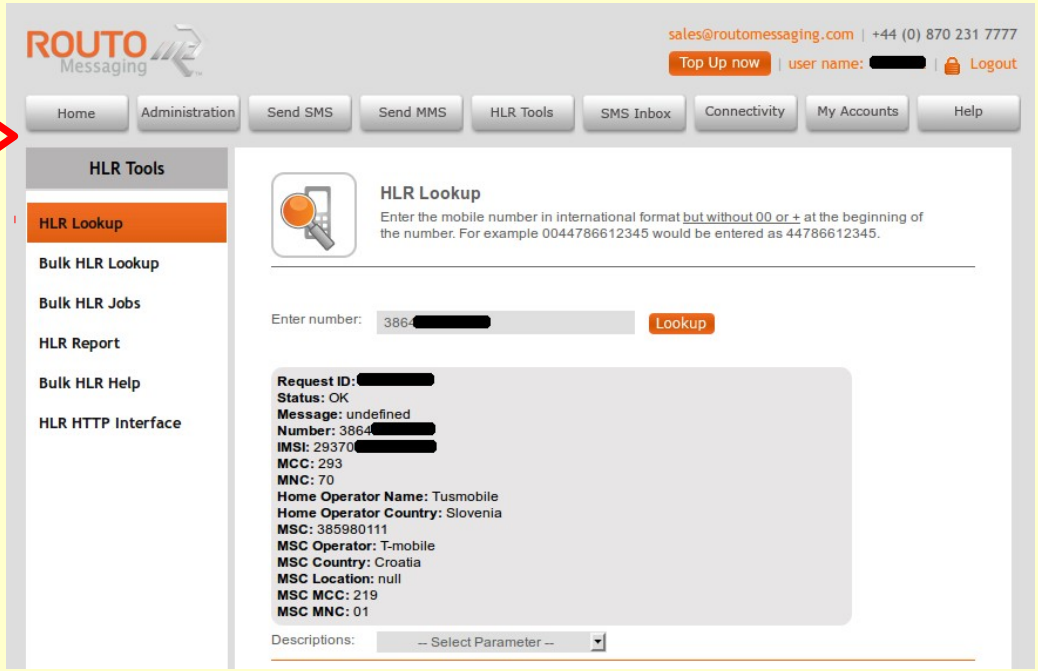


Mobile identity spoofing

If Kc does not change by every transaction, mobile identity can be easily spoofed. First, we have to identify IMSI number of our target...

1.

HLR lookup

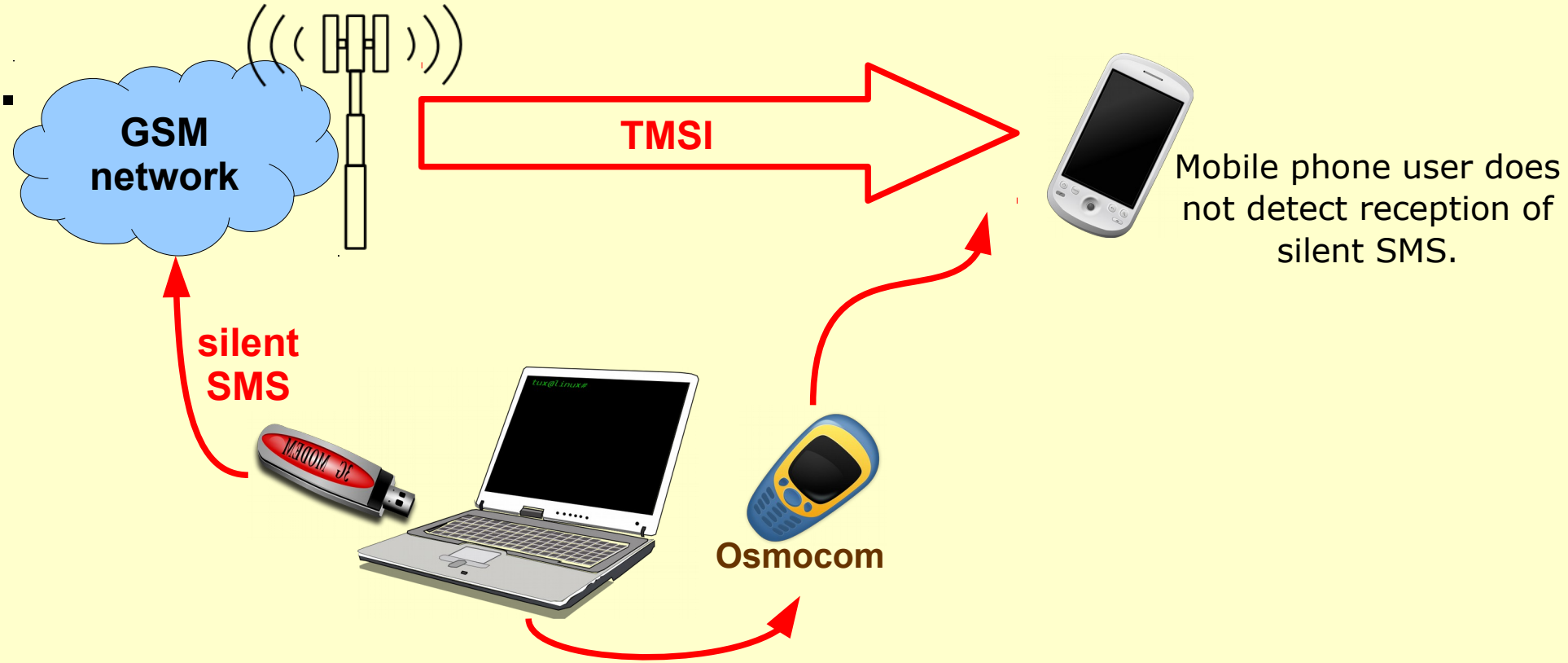


HLR lookup is done through web service – we get IMSI number.

Detection of TMSI number

TMSI number is discovered by sending silent SMS messages. Meanwhile we intercept some GSM bursts (for cryptanalysis) and key sequence number.

2.



Reconstruction of Kc

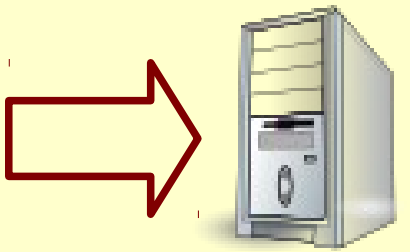
Session encryption key Kc in recovered through cryptanalysis. Now we have all information needed...

3.

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

CONTENT OF DATA BURST IN GSM

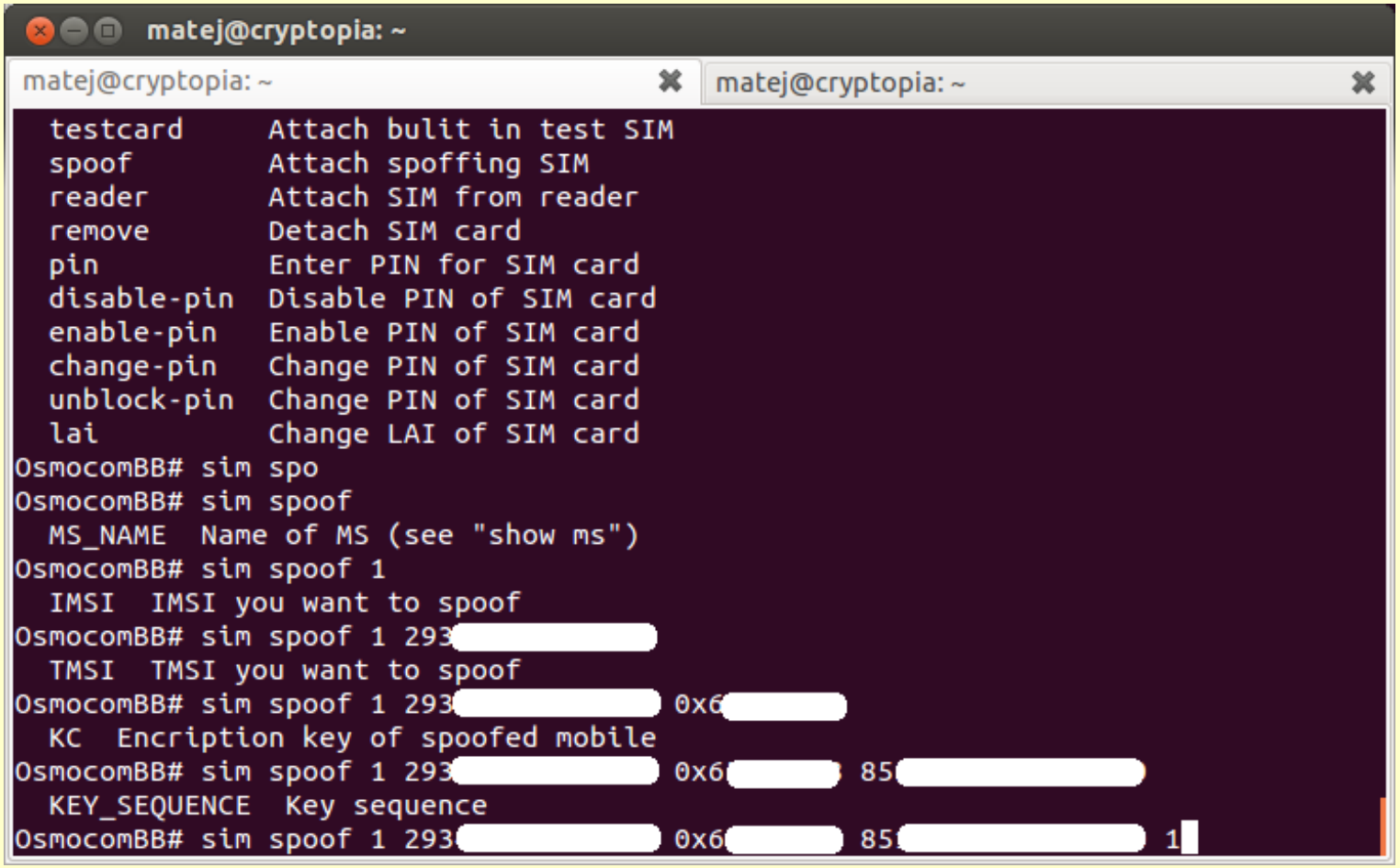
72	FE	BC	10	74	70	C4	2B	2B	2B	2B	2B	2B



Kraken

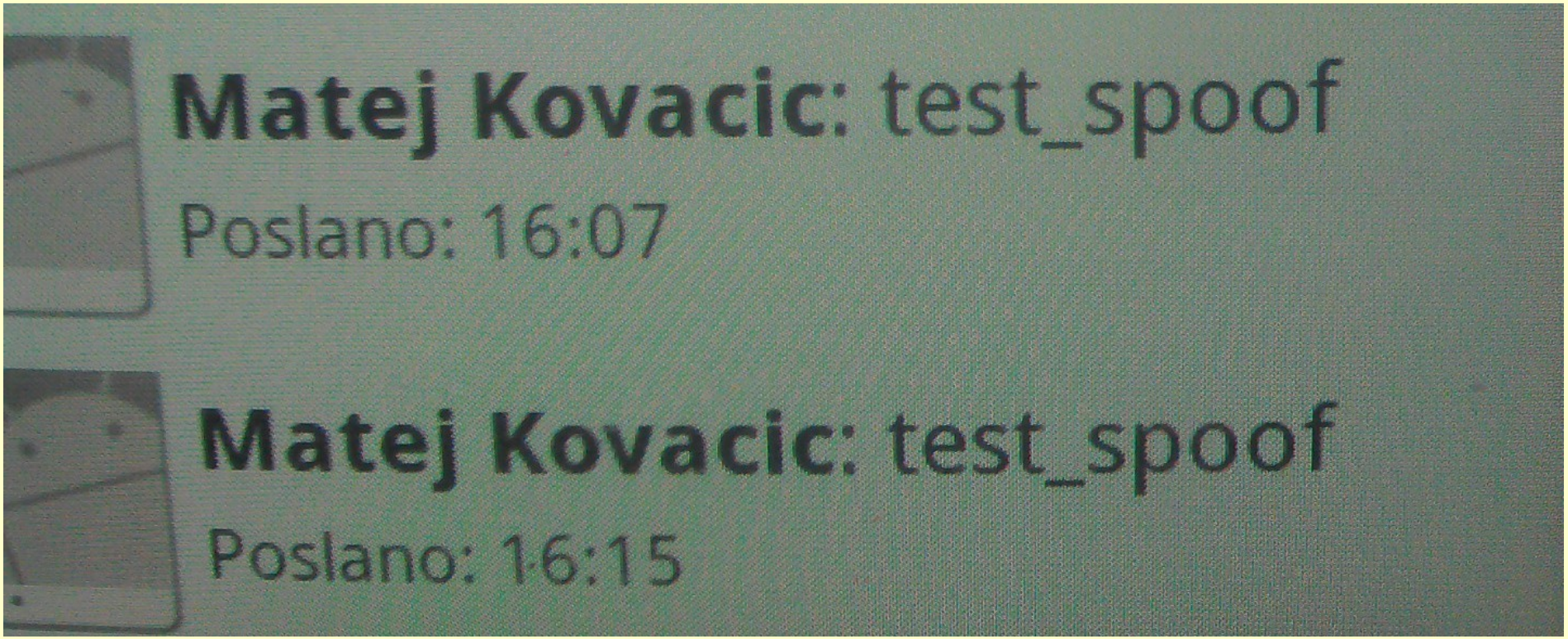
Kc

“SIM spoof”



Mobile identitity spoofing with “sim spoof” command. For spoofing we need IMSI number (SS7 lookup), TMSI number (from the network), session key (we chack it) and key sequence number (from the network).
In networks with A5/0 we need only TMSI and key sequence number – no cryptanalysis needed!

Mobile identity spoofing



Two SMS messages sent by spoofed mobile identity.
Similarly it is possible to spoof voice calls too.
[video]


BUSTED!

"We strongly emphasize that the abuse of identity in the network of Telekom Slovenia is not possible."

...

Abuse of the mobile identity in the Mobitel's network is prevented by the high standard mechanisms. ***No network in the world has better protection than we have in our GSM network****. Therefore, once again we remind that claims of abuse of user identity in the Telekom network are not real, however misuse of an identity outside of our network is not in our hands."*

Reply from Telekom Slovenije for DELO newspaper, July, 30th 2012, <http://www.delo.si/druzba/infoteh/mobitelovo-omrezje-kljub-zagotovilom-telekoma-se-slabo-zasciteno.html>

Traffic data in data retention database

What does it means for the data retention measures and eavesdropping?

“Courts tend to regard computer-generated materials as inherently trustworthy evidence.”

“This has consequences for court procedure. In a court witnesses are sworn in and cross-examined to expose biases and conflicts. But what about software as a witness?”

Sergey Bratus, Ashlyn Lembree in Anna Shubina. 2010.

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

“Miran Kimovec from Mobitel company, who was the next witness, was also unable to explain how it was possible to record the eavesdropped conversation while Reich's mobile phone has hot been registered to any of the Slovenian mobile operators. "Theoretically it would be possible that an Austrian citizen in Kranj caught a signal from Austrian operator, but practically it is almost impossible," he said. The trial will continue.”

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


BUSTED!

Mobile network security

Some other attacks on mobile networks

- **Disconnect mobile network from the network**: attacker who knows IMSI and TMSI number of the target, can disconnect target's mobile phone with [redacted] commands.

- **Shut down of a part of a mobile network**: if attackers sends more than [redacted] than base station has [redacted] in less than [redacted] seconds – mobile network shuts down. It is [redacted] [redacted] attack which consequence is denial of the service.


BUSTED!

Mobile network authentication

Problem: mobile network does not authenticate to mobile phone

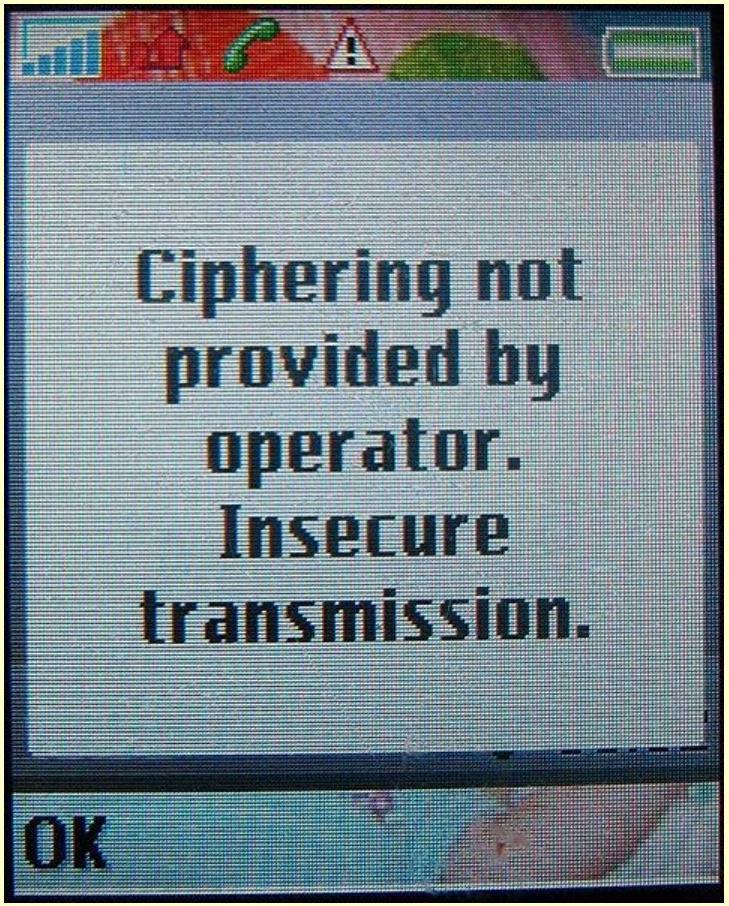
- The design of GSM network requires authentication of a mobile phone to to mobile network. But on the other side, mobile network **does not** authenticate to mobile phone
- Translation: mobile phone does not know to which network is really connected.

- Consequence: it is possible to perform attack with "IMSI-catcher", special device, which pretends to be a legitimate base station. Since mobile phone does not know that this base station is fake, it connects to it.


Guardian
SESSIONS
NETWORK
SYSTEM STATUS
IMSI
IMEI
425010778089821
352924024951985
2013-06-02 14:47:05
moria
352926023551237
2013-06-02 14:47:05
425010779019913
353818056222712
2013-06-02 14:43:01
Septier
Communication Ltd.

Problem: mobile network <u>does not</u> authenticate to mobile phone

- When a mobile phone is connected to a fake base station, it »orders« him to stop encryption.
- GSM standard recommends ("*should*") informing the user when communication is not encrypted (3GPP Rel.9 TS 33.102-920 "3G Security Architecture" 5.5.1 Visibility, ciphering indicator feature - 3GPP TS 22.101")



Problem: mobile network <u>does not</u> authenticate to mobile phone

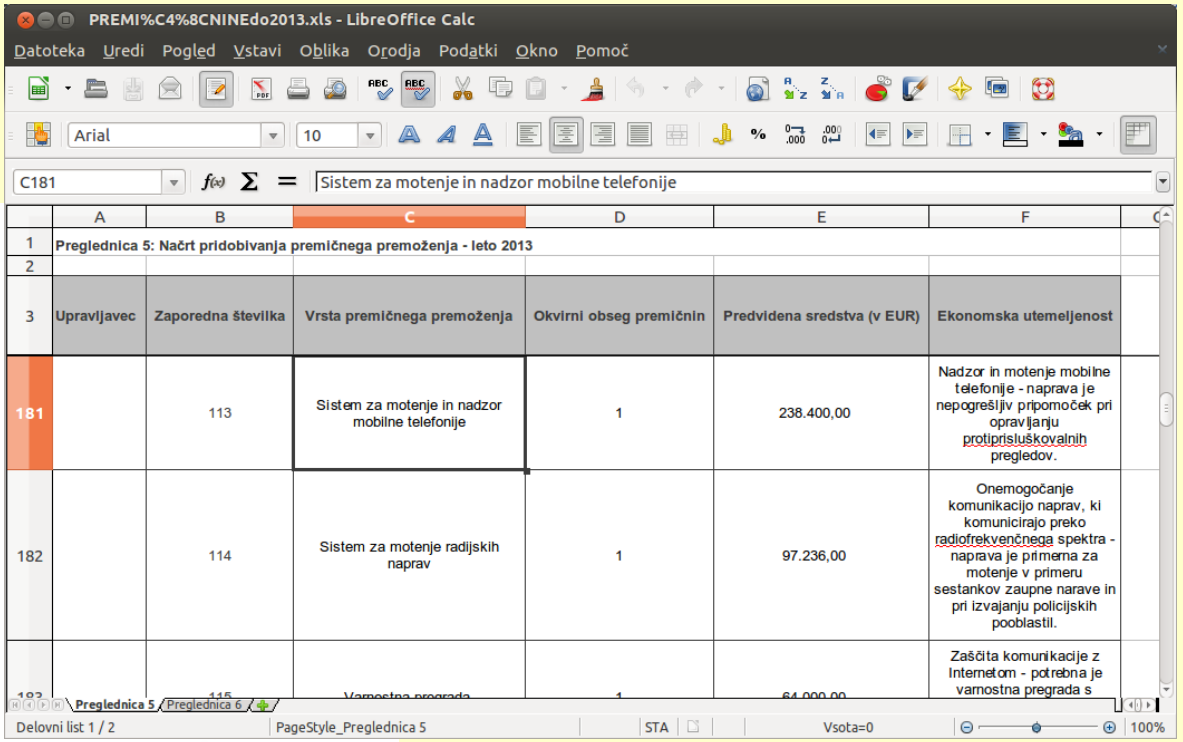
- But this notice is not shown if there is a special setting on a SIM card.

> 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: mobile network <u>does not</u> authenticate to mobile phone

Ciphering indicator is not very clear on some mobile phones, and even not shown at all on some others.

IMSI Catcher could be bought...



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:

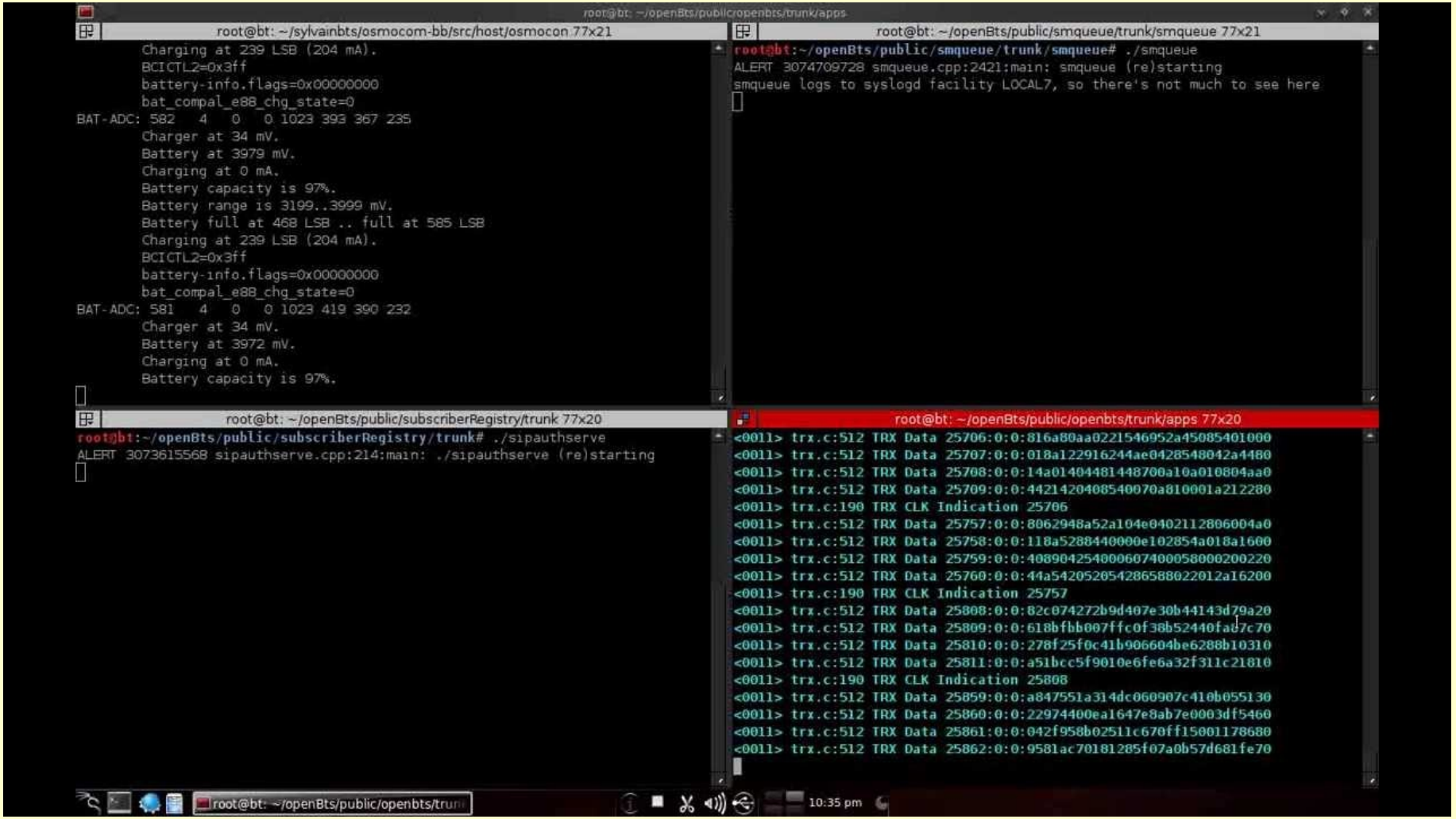
1. *Naziv ter naslov naročnika, ki bo izvedel naročilo po Uredbi o obrambnih in zaupnih naročilih:*

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

2. *Predmet naročila:*

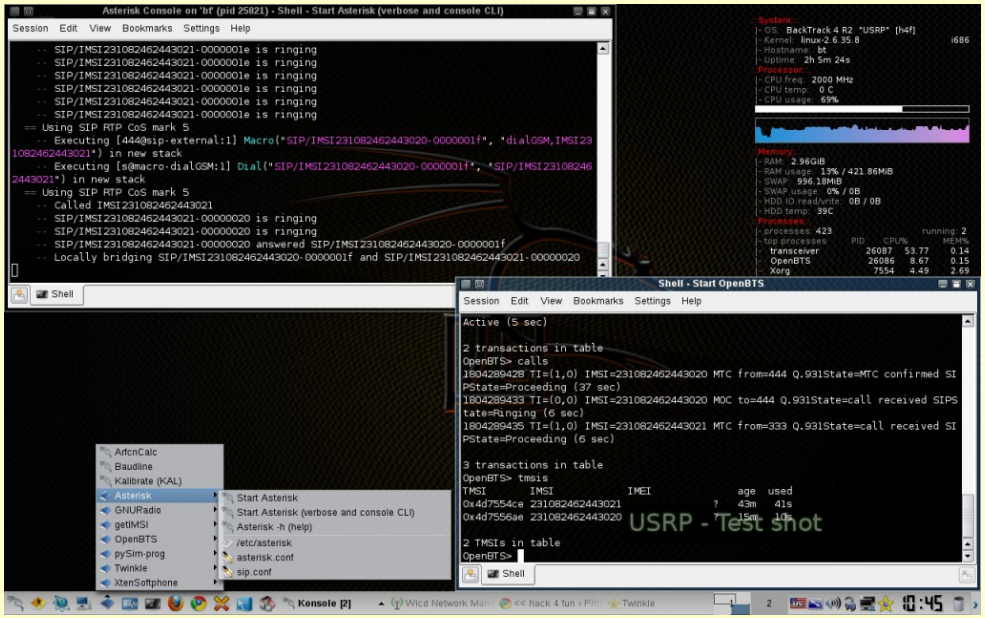
Nadgradnja sistema za [redacted]

...or we can build our own



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>.

...or we can build our own (2)



Source and copyright: prof. dr. ing. Andreas Steil, <http://www.fh-kl.de/~andreas.steil/Projekte/OpenBTS/>

and

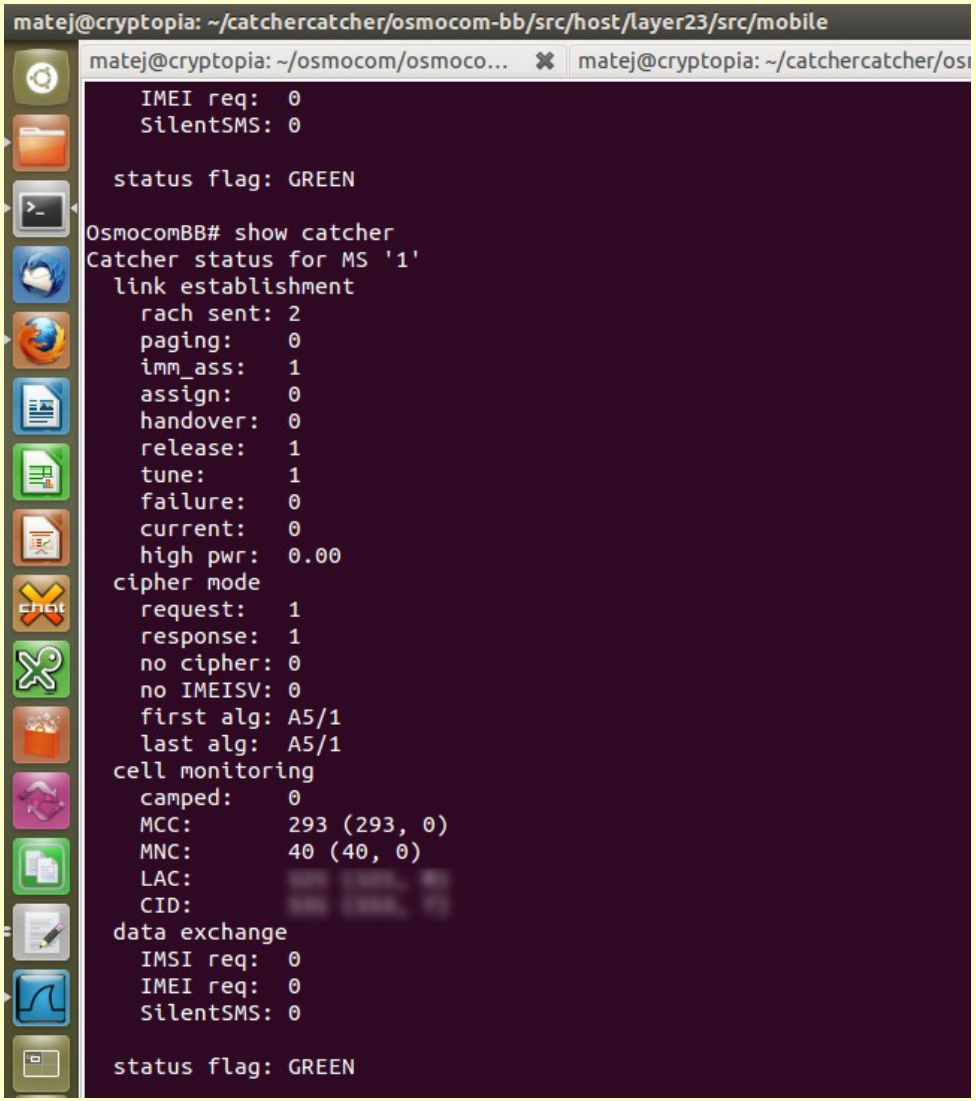
BackTrack R2 USRP Test Shot, <http://www.serverfault.sk/2011/03/backtrack-r2-usrp-test-shot-rfx900/>.

...or we can build our own (3)

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 detection

(Catcher Catcher)



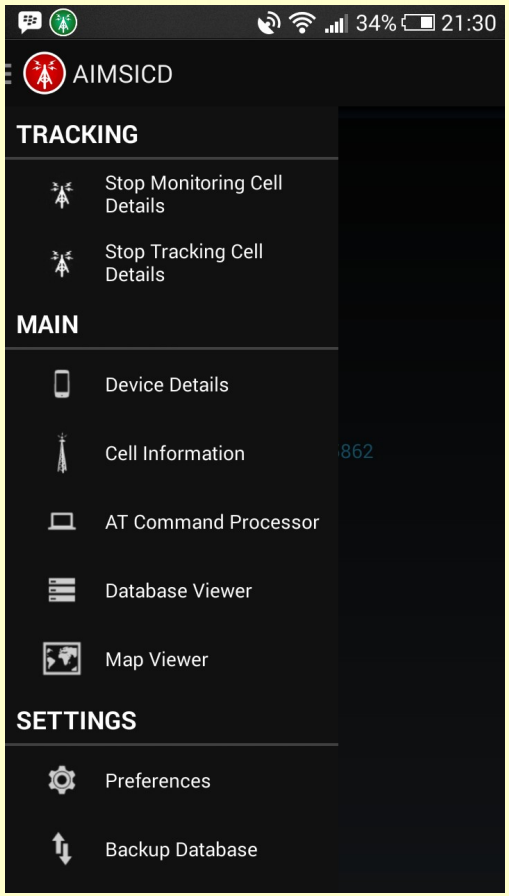

```
Catcher status for MS '1'
  link establishment
    rach sent: 78
    paging:    1
    imm_ass:   0
    assign:    0
    handover:  0
    release:   0
    tune:      0
    failure:   0
    current:   1
    high pwr:  -
  cipher mode
    request:   0
    response:  0
    no cipher: 0
    no IMEISV: 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
```

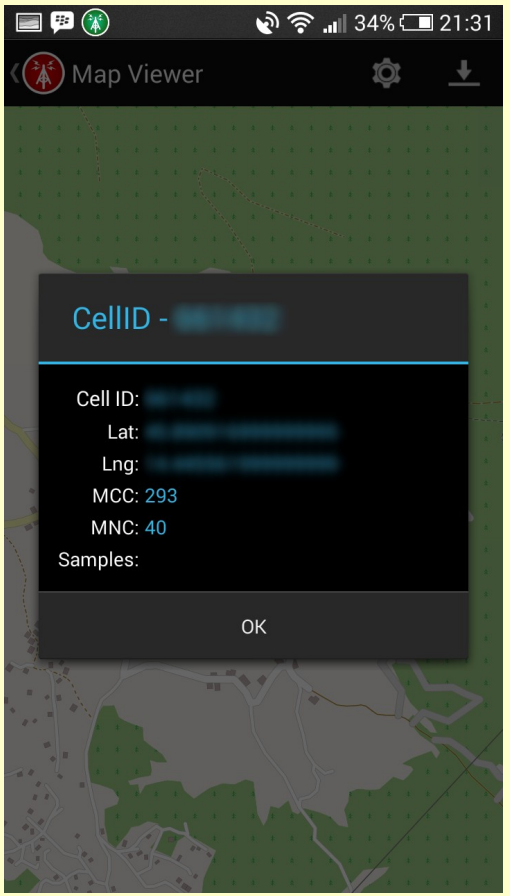
...is available only for Osmocom platform

(FemtoCatcher is available only for Verizone network).

IMSI catcher detection

(AIMSICD)





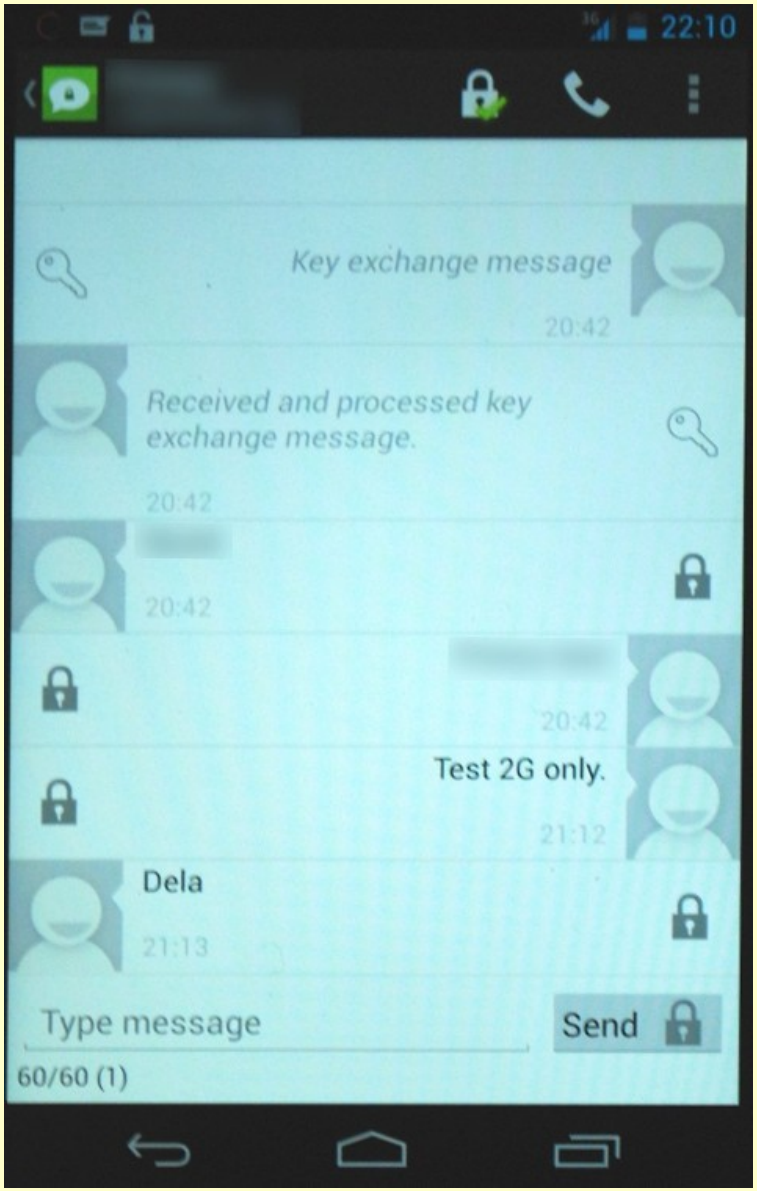

BUSTED!

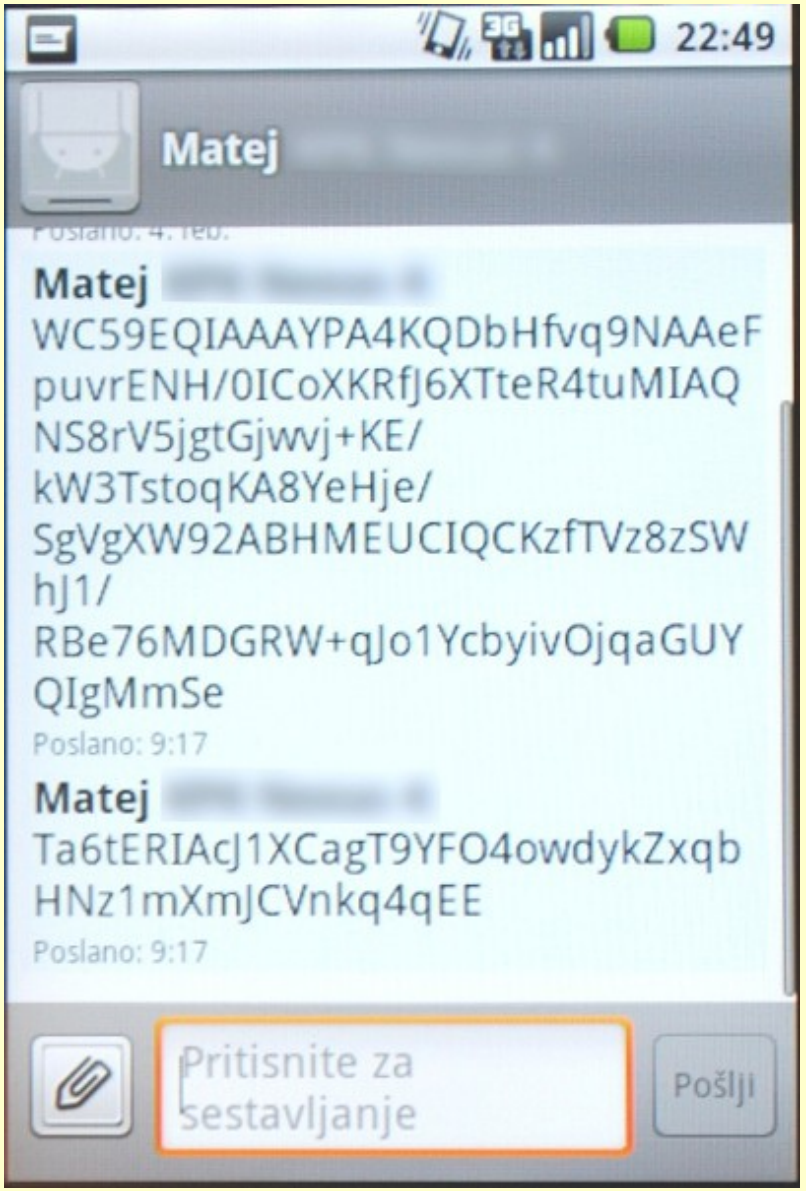
Smartphones security

Main approaches to smartphone security

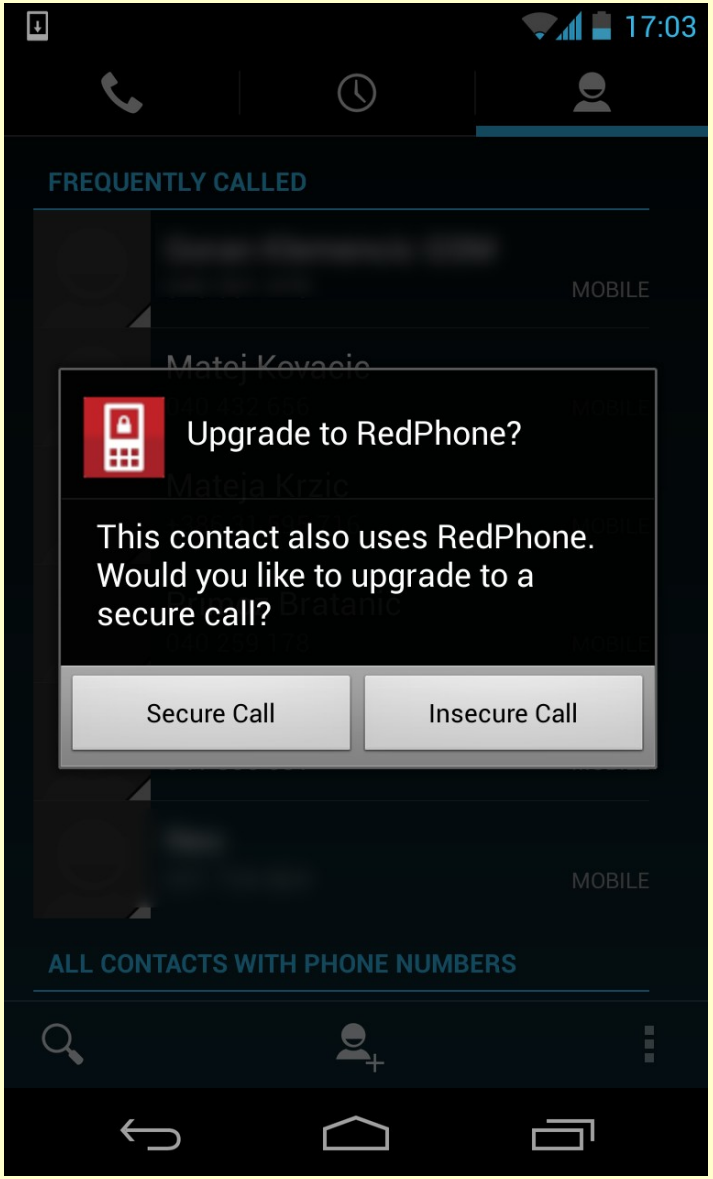
- “Security enhanced” OS (usually some fork of Android, for instance Replicant, PrivatOS (Blackphone), Guardian ROM, CyanogenMod, etc.).
- Antivirus/malware detection.
- User/process separation.
- Screen lock with password (with brute force protection).
- Internal memory encryption.
- Encryption of digital communications (ZRTP VoIP calls, VPN,...).
- Anonimisation/hiding of traffic data.

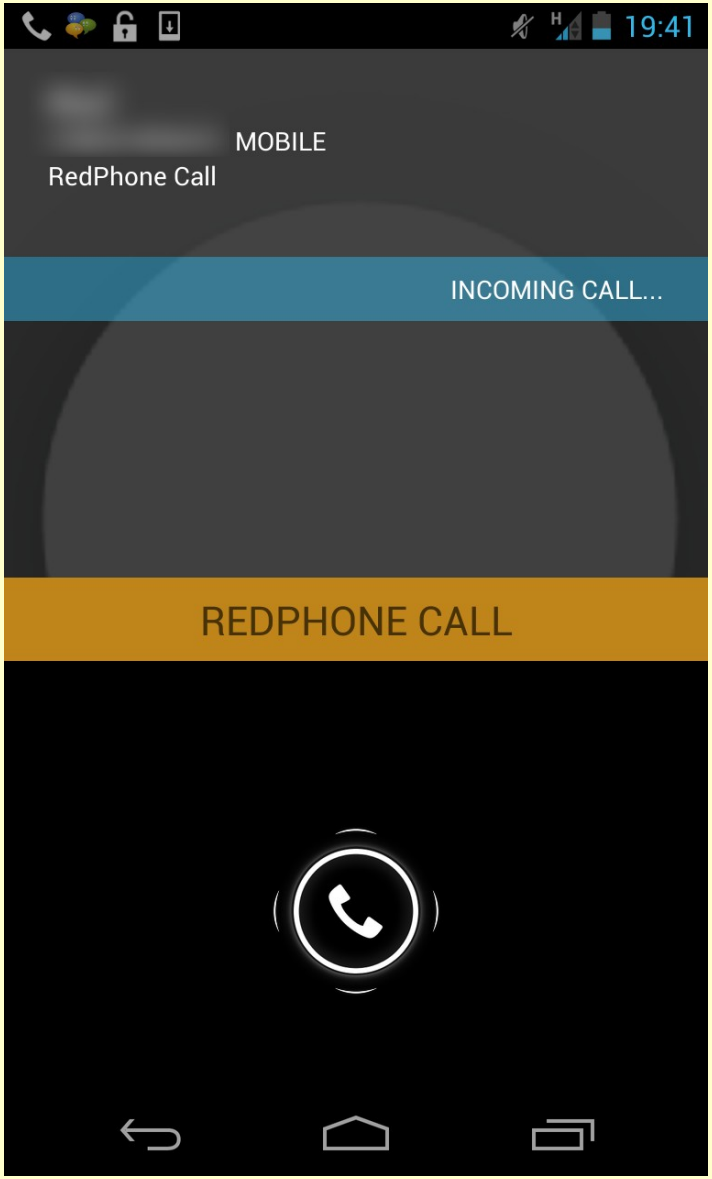
Encrypted SMS messages: TextSecure



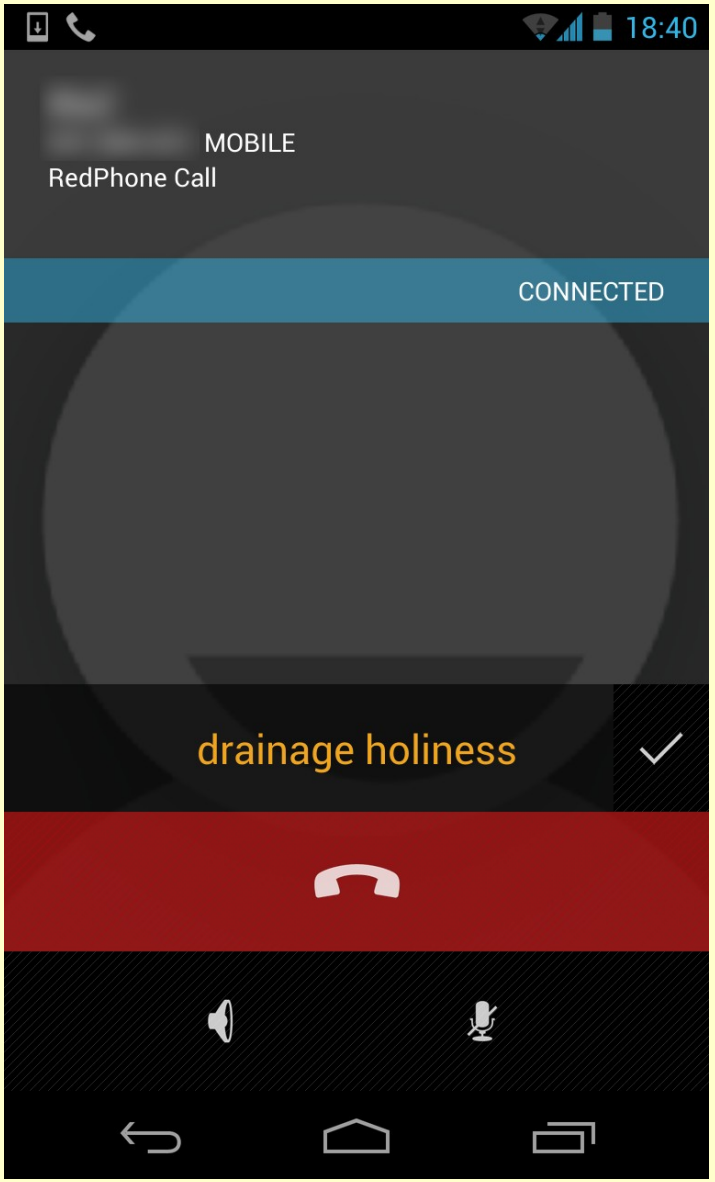


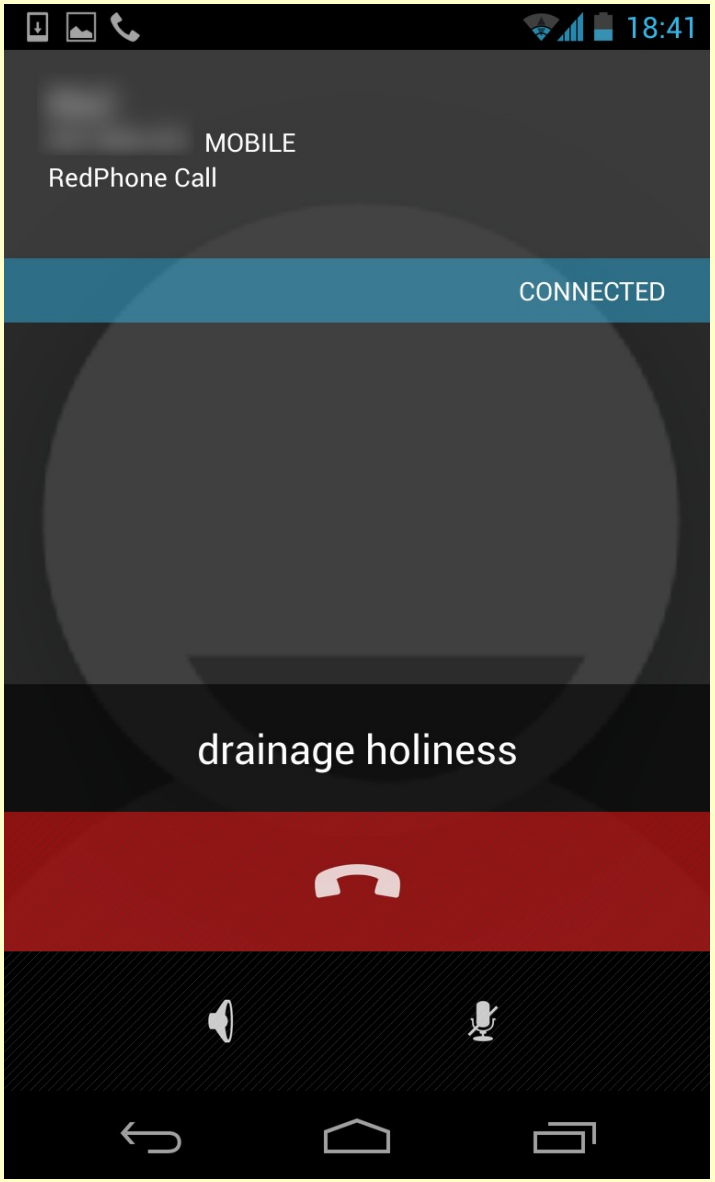
Encrypted phone calls: RedPhone



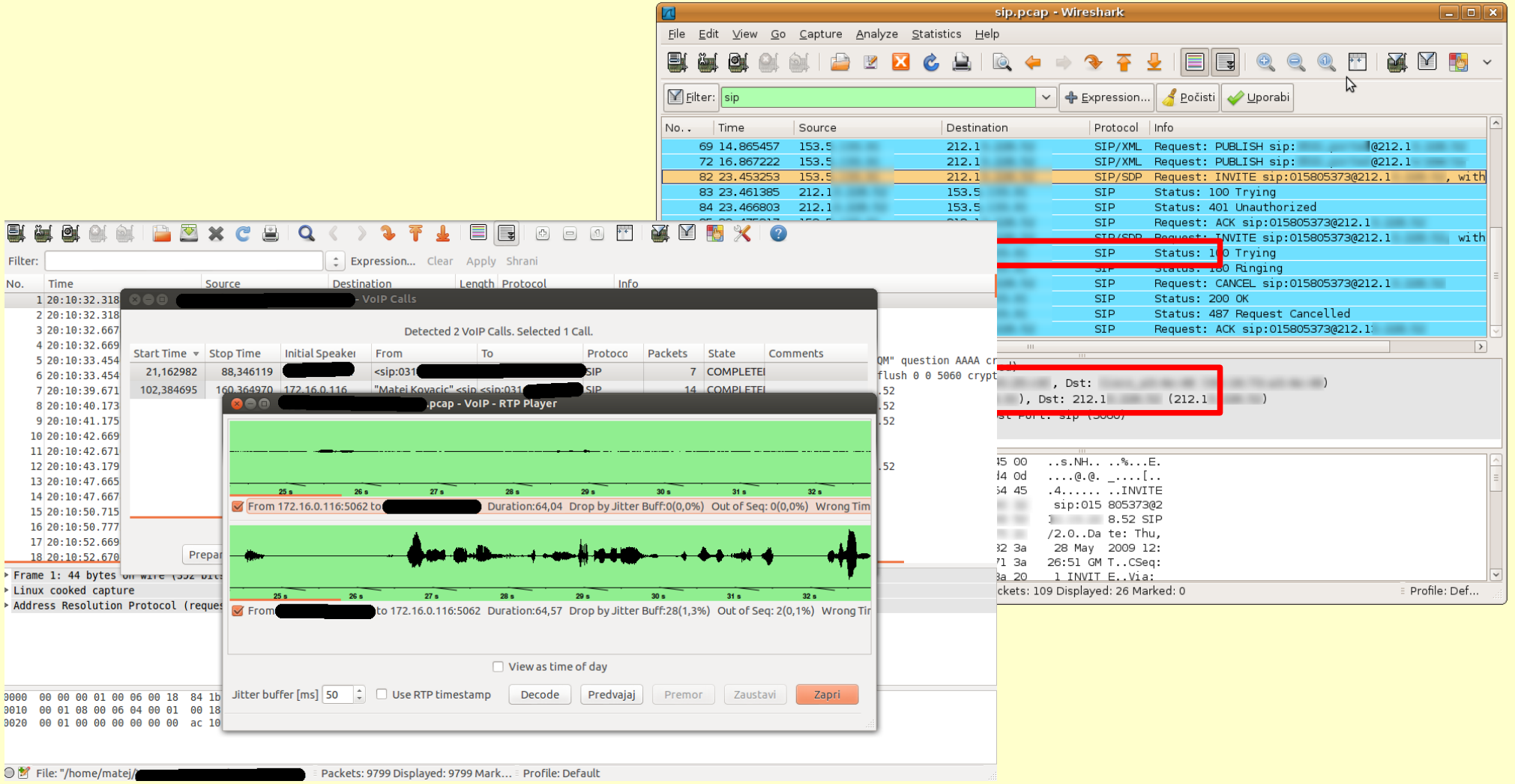


Encrypted phone calls: RedPhone



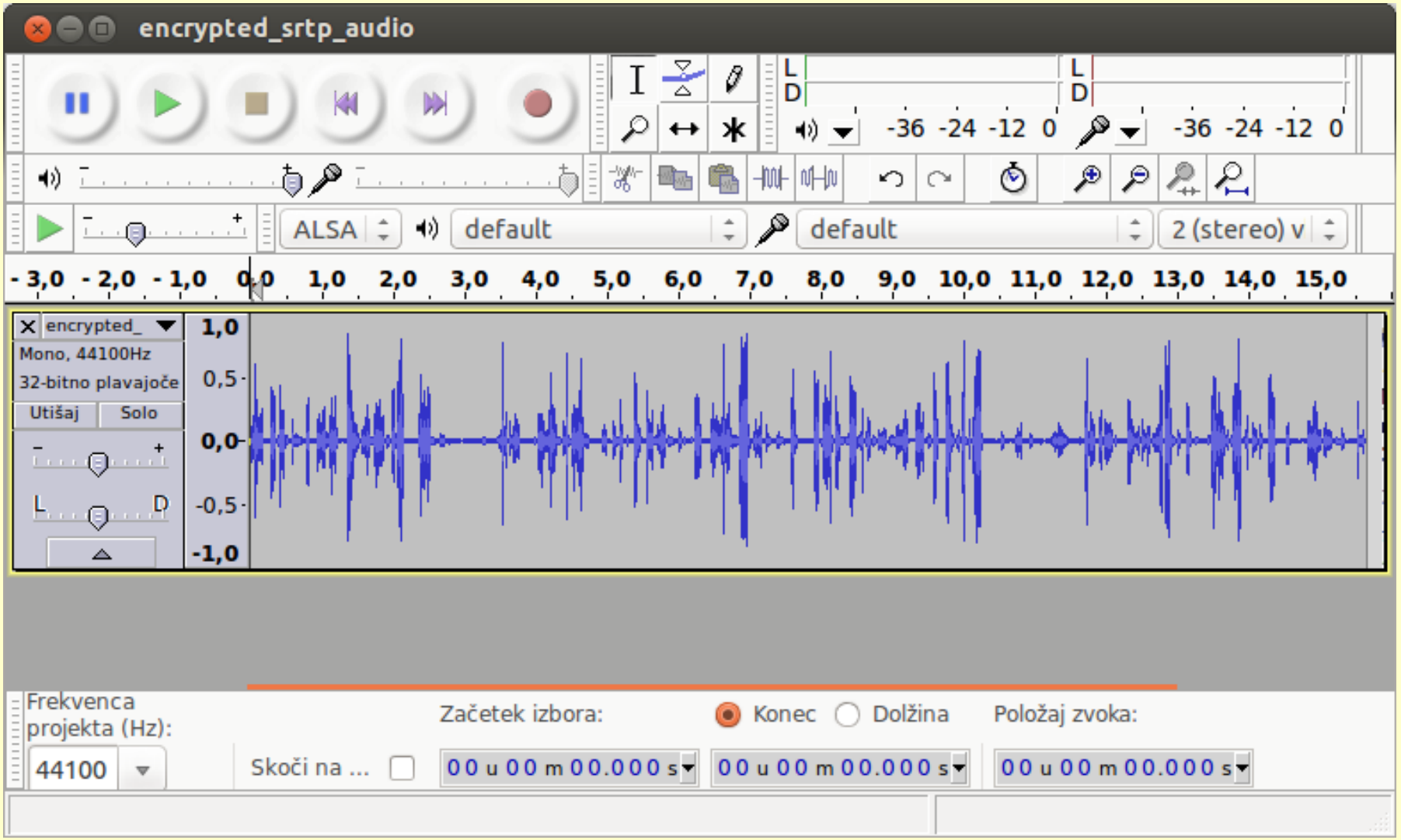


Unencrypted phone call (IP telefonija)



[Demo]

Encrypted phone call

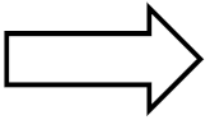


[Demo]

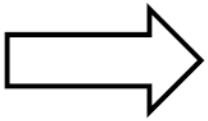
Traffic data of RedPhone calls

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



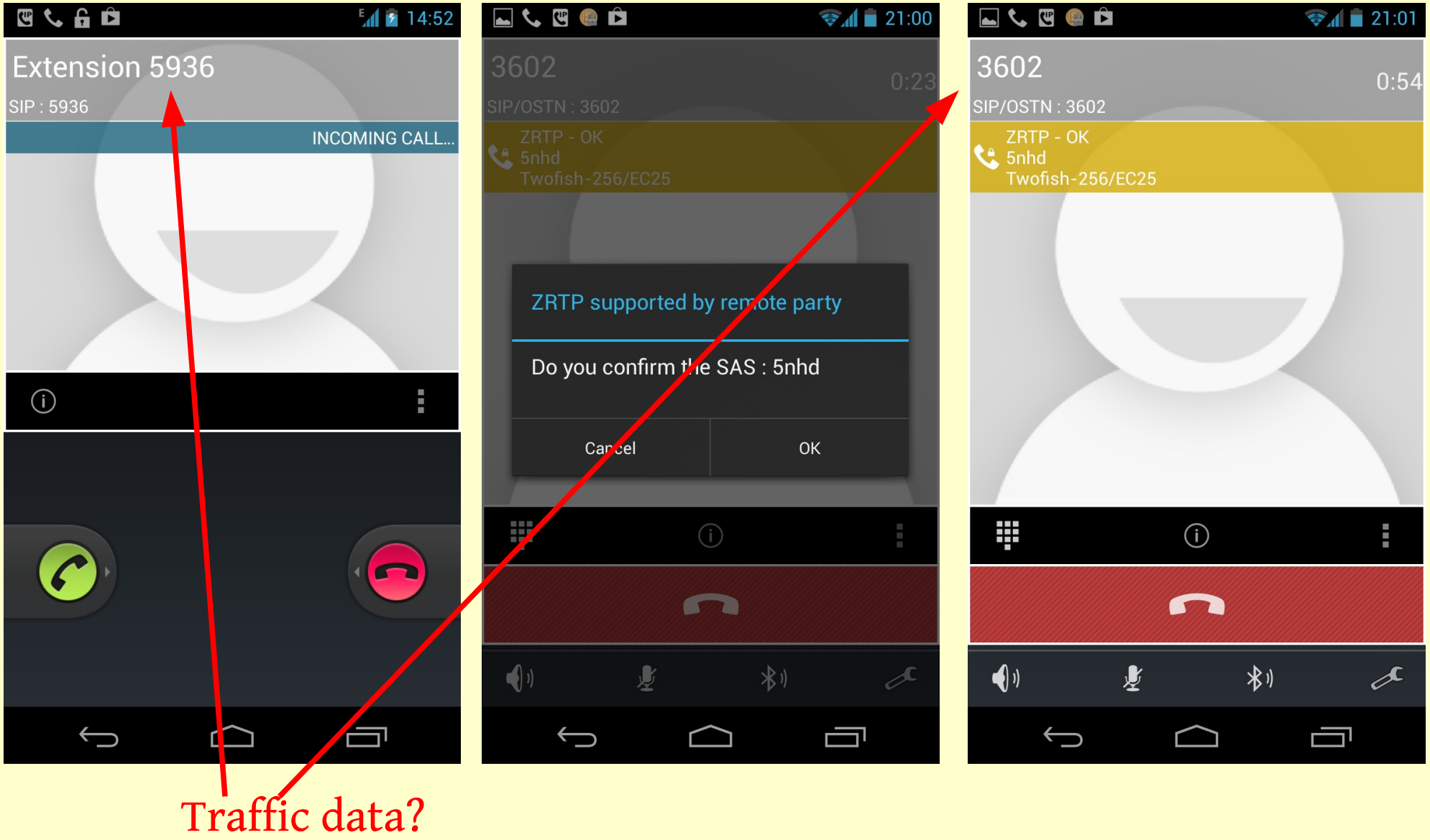
tip klica	klicana oseba	datum in čas	trajanje
RP klic	Nemčija	Jun 1, 2013 12:52:36 PM	37
RP klic	Nemčija	Jun 1, 2013 12:53:28 PM	23
RP klic	Nemčija	Jun 1, 2013 12:54:40 PM	22
RP klic	Nemčija	Jun 1, 2013 12:59:26 PM	17



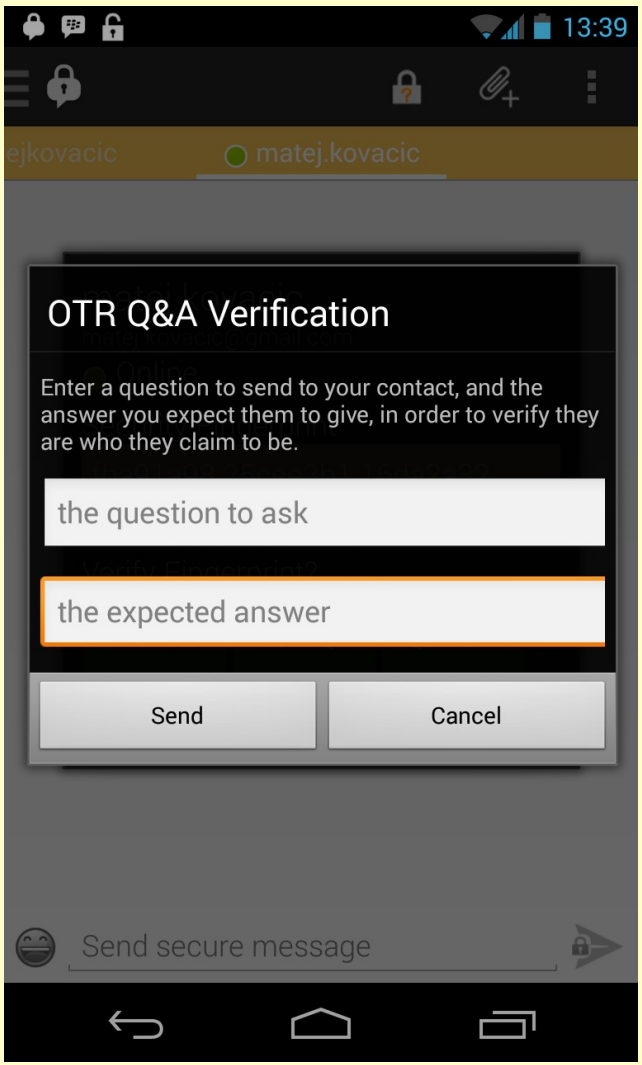
tip klica	klicana oseba	datum in čas	trajanje
RP klic	Nemčija	Jun 1, 2013 5:59:51 PM	10
RP klic	Nemčija	Jun 1, 2013 6:21:14 PM	70

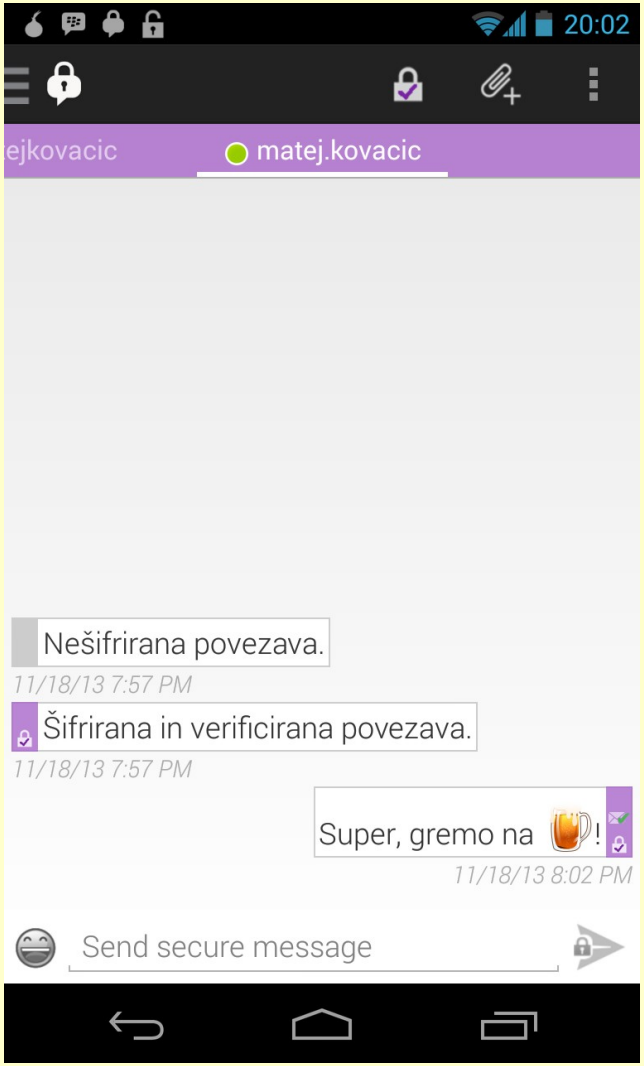
tip klica	klicana oseba	datum in čas	trajanje
RP klic	Slovenija3	Jun 2, 2013 10:47:14 AM	11
RP klic	Slovenija3	Jun 2, 2013 10:47:52 AM	64
RP klic	Slovenija3	Jun 2, 2013 10:49:03 AM	102
RP klic	Slovenija3	Jun 2, 2013 10:50:52 AM	70
RP klic	Slovenija4	Jun 2, 2013 11:59:36 AM	2
RP SMS	Slovenija4	Jun 2,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

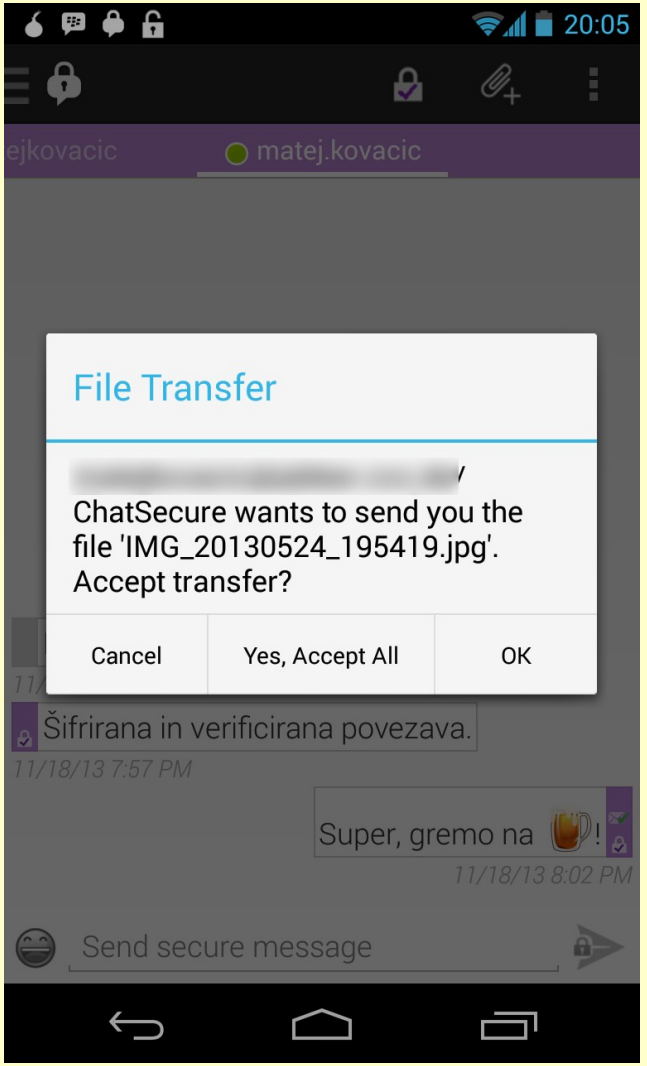
Encrypted calls: CsipSimple and OSTN



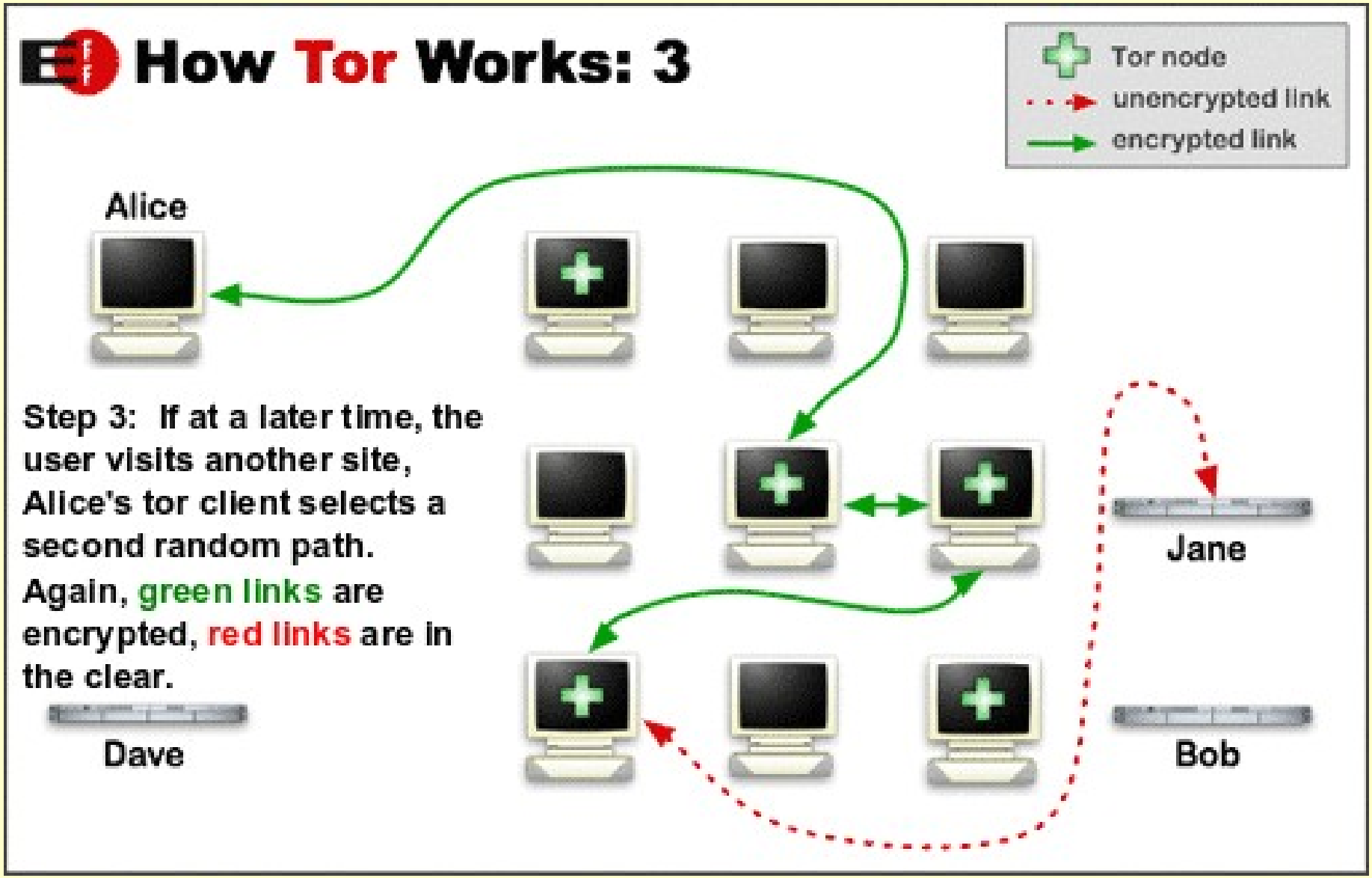
Encrypted instant messages: ChatSecure



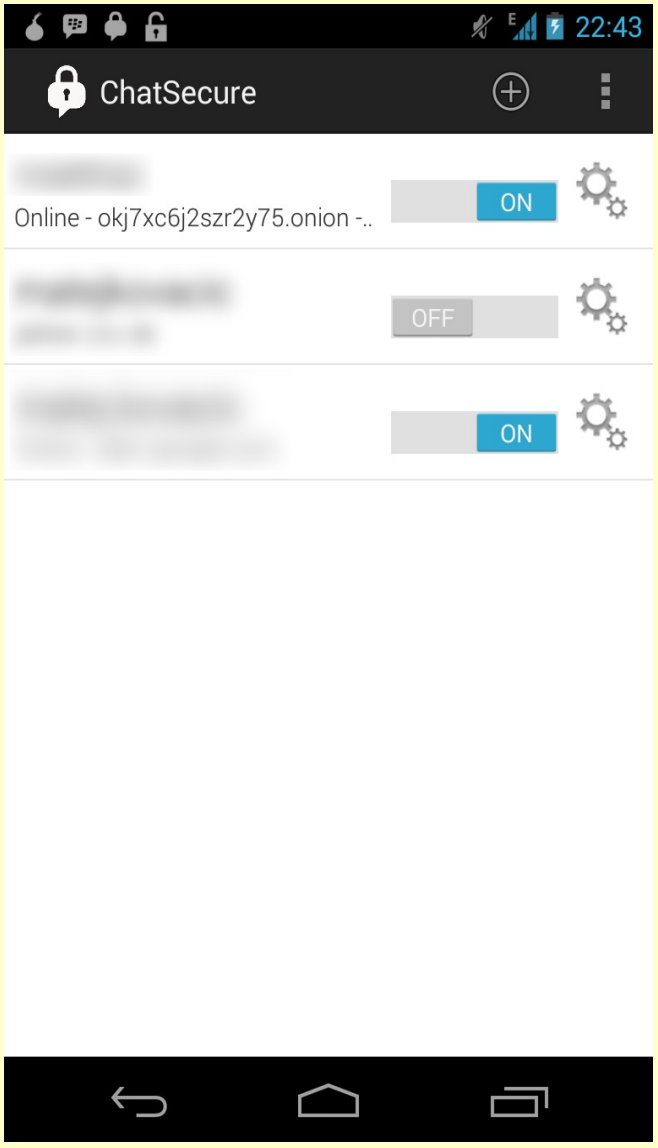




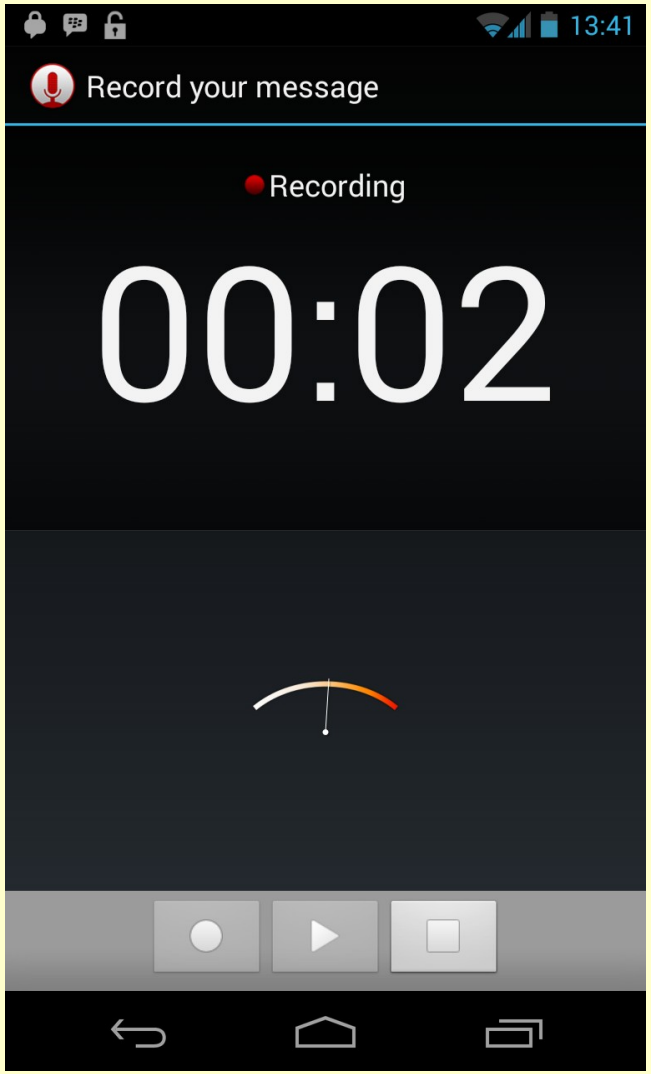
Anonymisation...

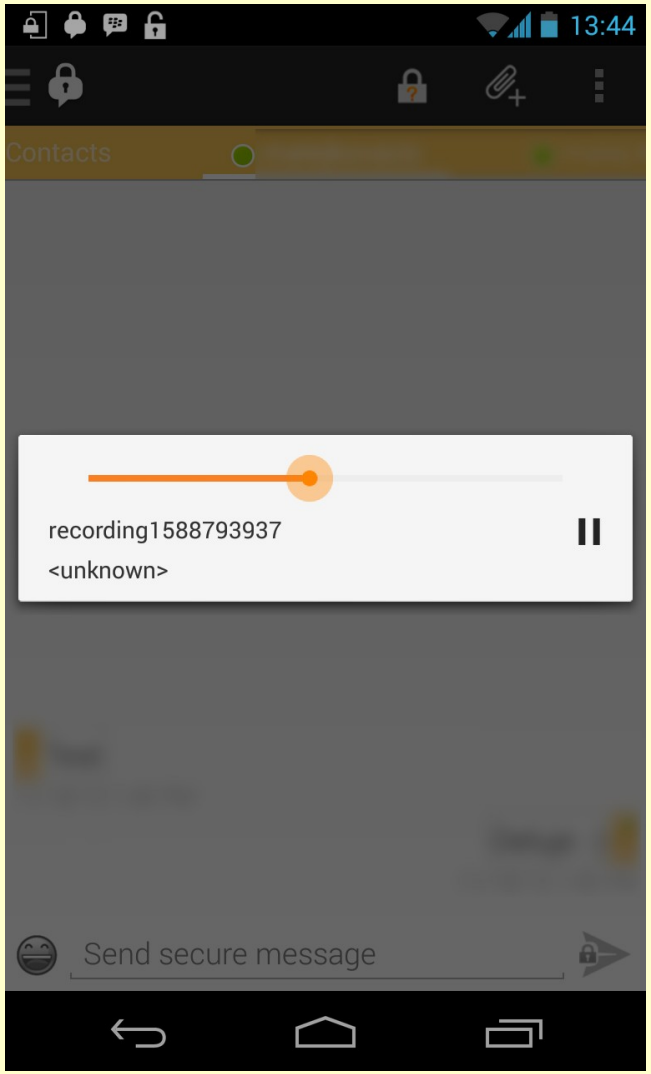


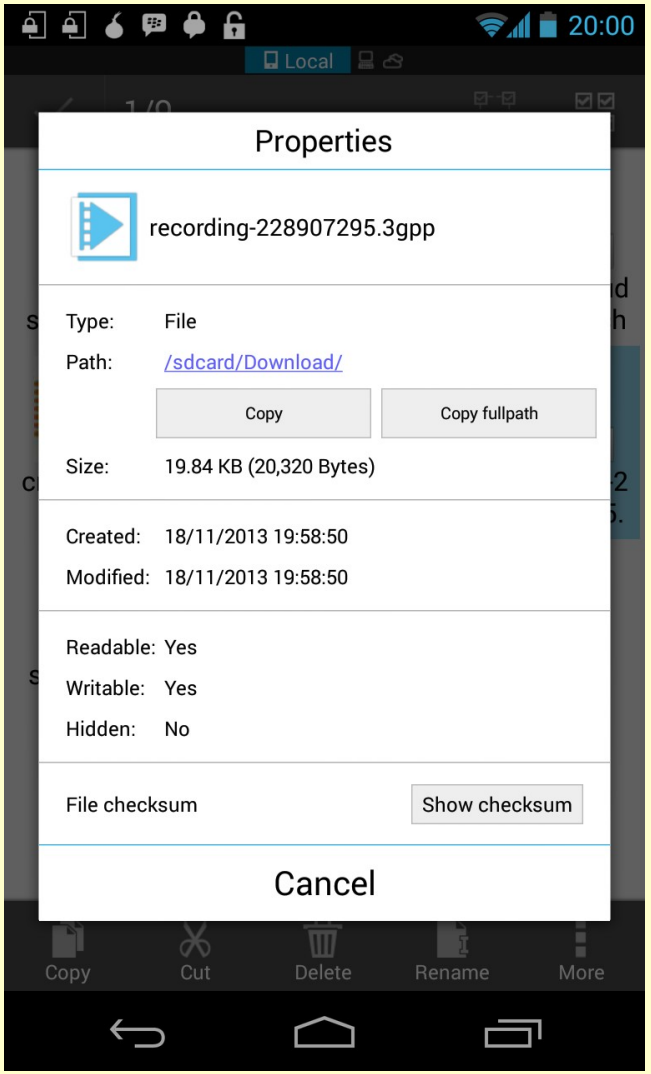
...of voice communication on a mobile phone



Voice communication on a mobile phone through Tor network







	Encrypted in transit?	Encrypted so the provider can't read it?	Can you verify contacts' identities?	Are past comms secure if your keys are stolen?	Is the code open to independent review?	Is security design properly documented?	Has there been any recent code audit?
Secret							
Signal / RedPhone							
Silent Phone							
Silent Text							
Skype							

https://www.eff.org/secure-messaging-scorecard

Location tracking

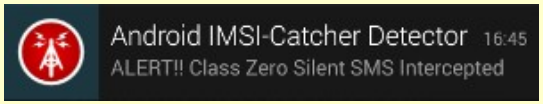
Location privacy

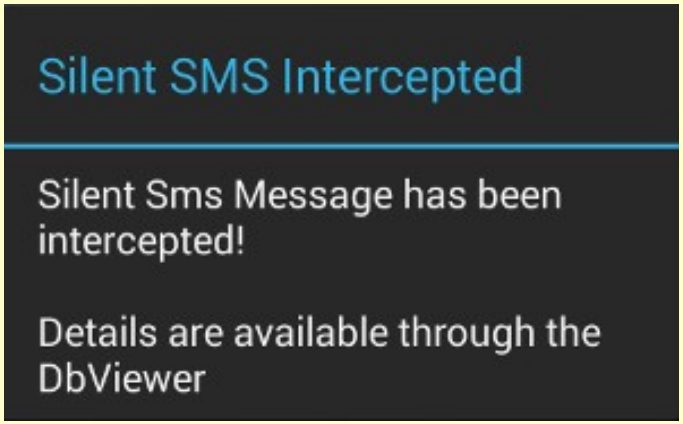
- *"Cell phones are 'Stalin's dream.'*
  Cell phones are tools of Big Brother. I'm not going to carry a tracking device that records where I go all the time, and I'm not going to carry a surveillance device that can be turned on to eavesdrop."

--Richard Stallman, March 2011

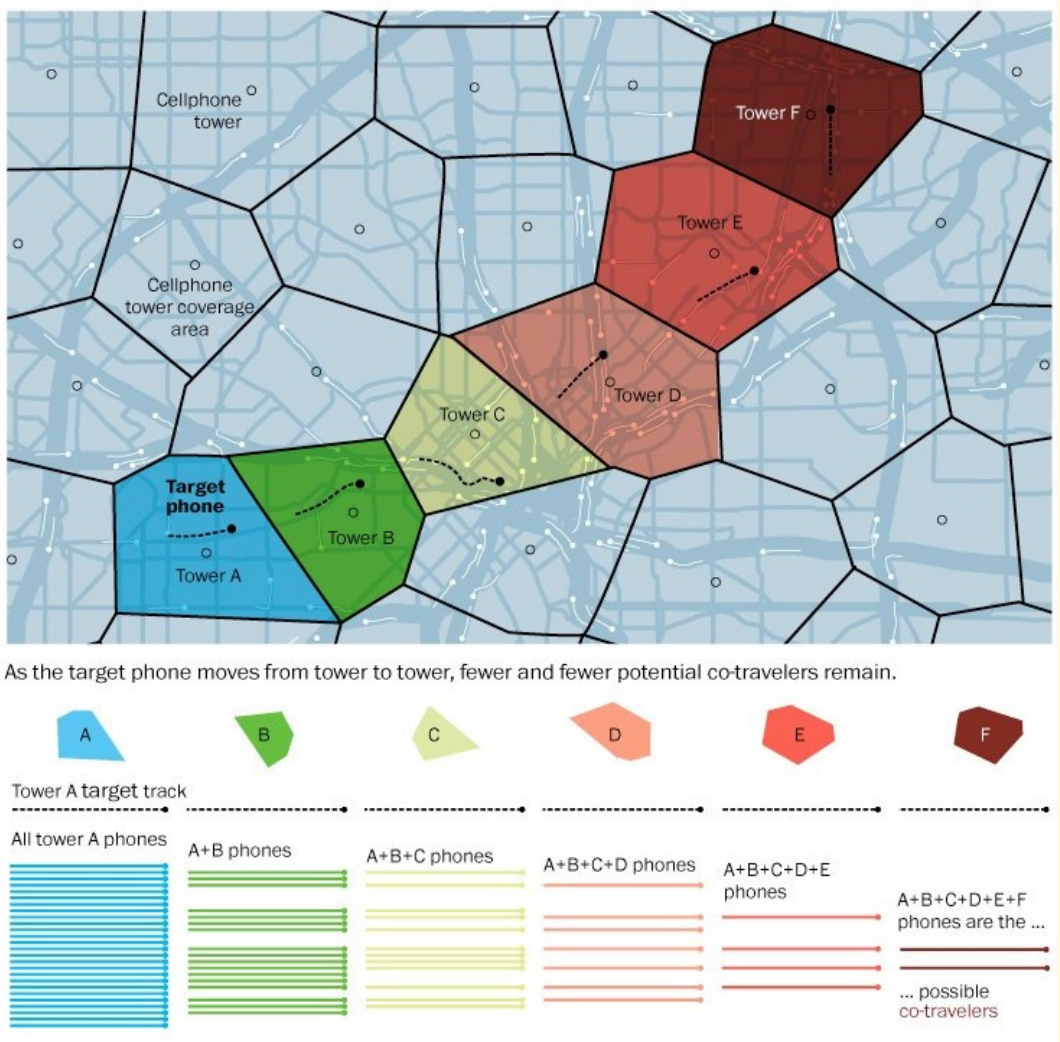
Silent SMS

- Silent SMS (Type-0 ping”) is a special SMS message, which is not shown on a mobile phone. However, read receipt is generated and traffic data are also recorded (it is different from Class-0 SMS, so called flash SMS).
- Silent SMS'es are usually used for locating users.
  - German police sent about half million of silent SMS'es in 2010.





Location privacy



Source and copyright: 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/>.

Location privacy

- It is known that location tracking is being used for target assassinations with drones.
- Spoofing/blocking of network or radio identifiers:
  - IMEI: mostly illegal, there is an application *IMEI modifier*, which is not easy to use;
  - Bluetooth: switch it off;
  - NFC: switch it off;
  - MAC address: MAC changer/spoofer is not working on all devices, device needs to be *rooted*;
  - IMSI: only with changing of a SIM card.

Location privacy

- The only solution is to completely log out from the network... but then we are not talking about **mobile** phone anymore.
- SIM card removal is not enough – in that case mobile phone searches for base stations and still broadcasts IMEI number.

- The problem of location tracking cannot really be solved.

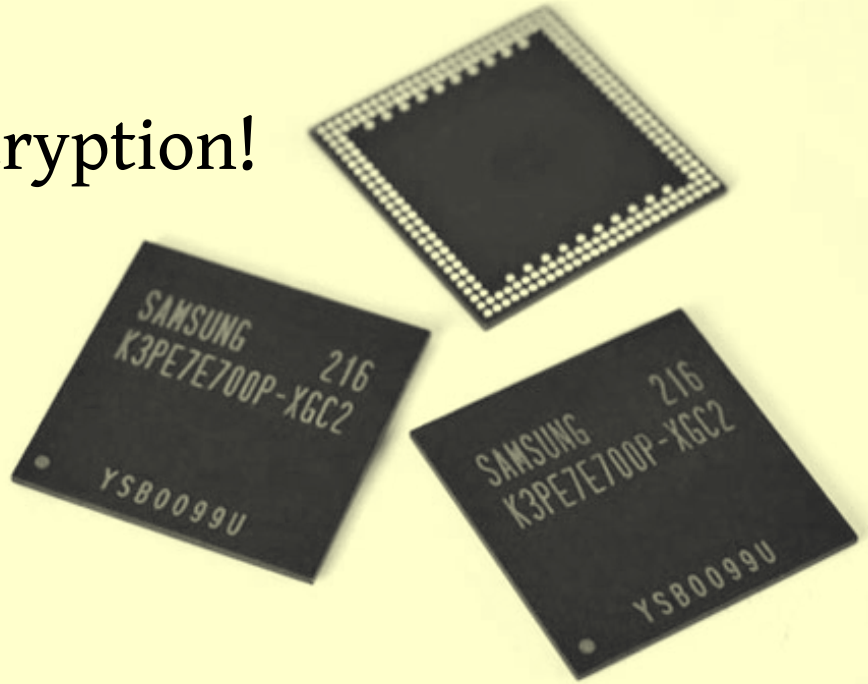

BUSTED!

Attacks to internal memory

Attacks to internal memory

- Problematic especially because of:
  - access to data on a mobile phone,
  - injecting malware.

- Solution: internal memory encryption! However...



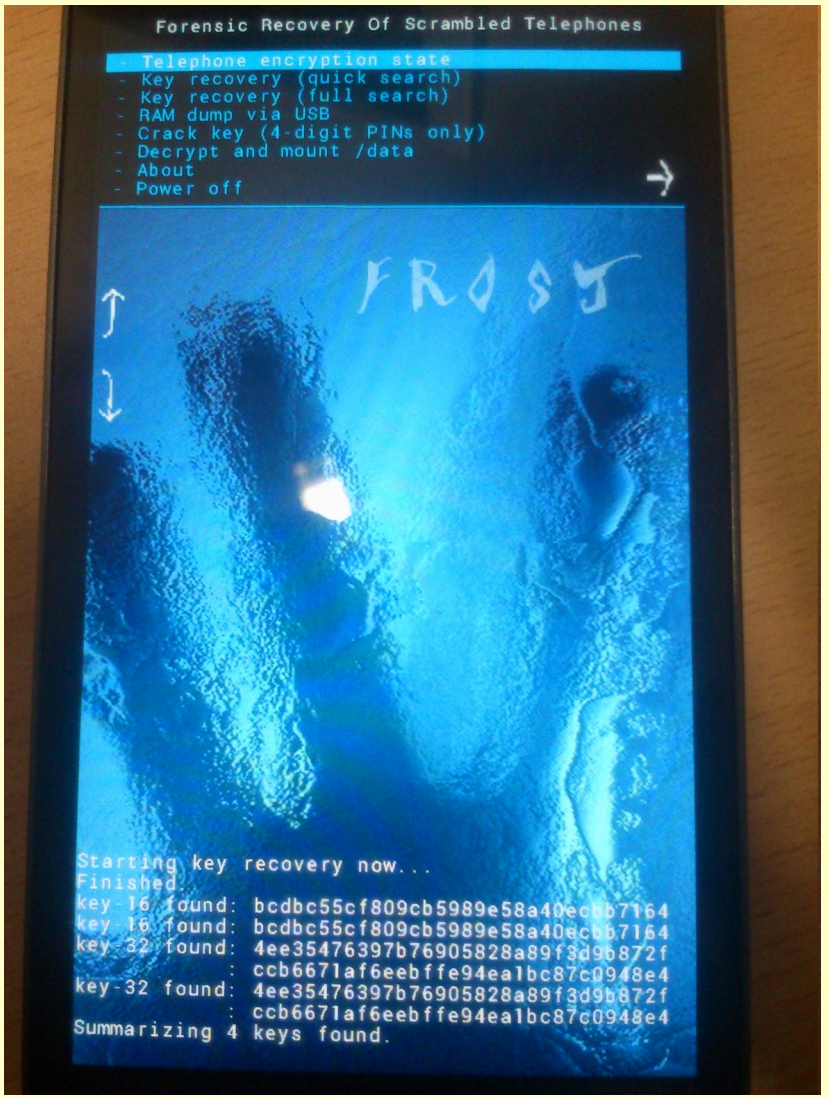
Tradeoff between security and usability

- Typical problem of tradeoff between security and usability is implementation of encryption of internal memory in Android.
- Currently, there is only one password for both the encryption and the screen lock. This password could be maximum 16 characters long. This is adequate protection for screen unlocking, but not for offline attacks.
- Using the same password:
  - (+) decreased probability that user would forget the password;
  - (-) it is not likely that user would use long password at frequent use (screen unlocking is frequent use!);
  - (-) short password (up to 16 characters) does not offer enough protection against *offline* attacks.

Cold Boot attack on mobile phones

- Cold Boot attack could be used to gain encryption keys from the encrypted mobile phone.

- Proof of concept: Tilo Müller, Michael Spreitzenbarth and Felix Freiling have developed tool called FROST (*Forensic Recovery Of Scrambled Telephones*).



Cold Boot attack on mobile phones

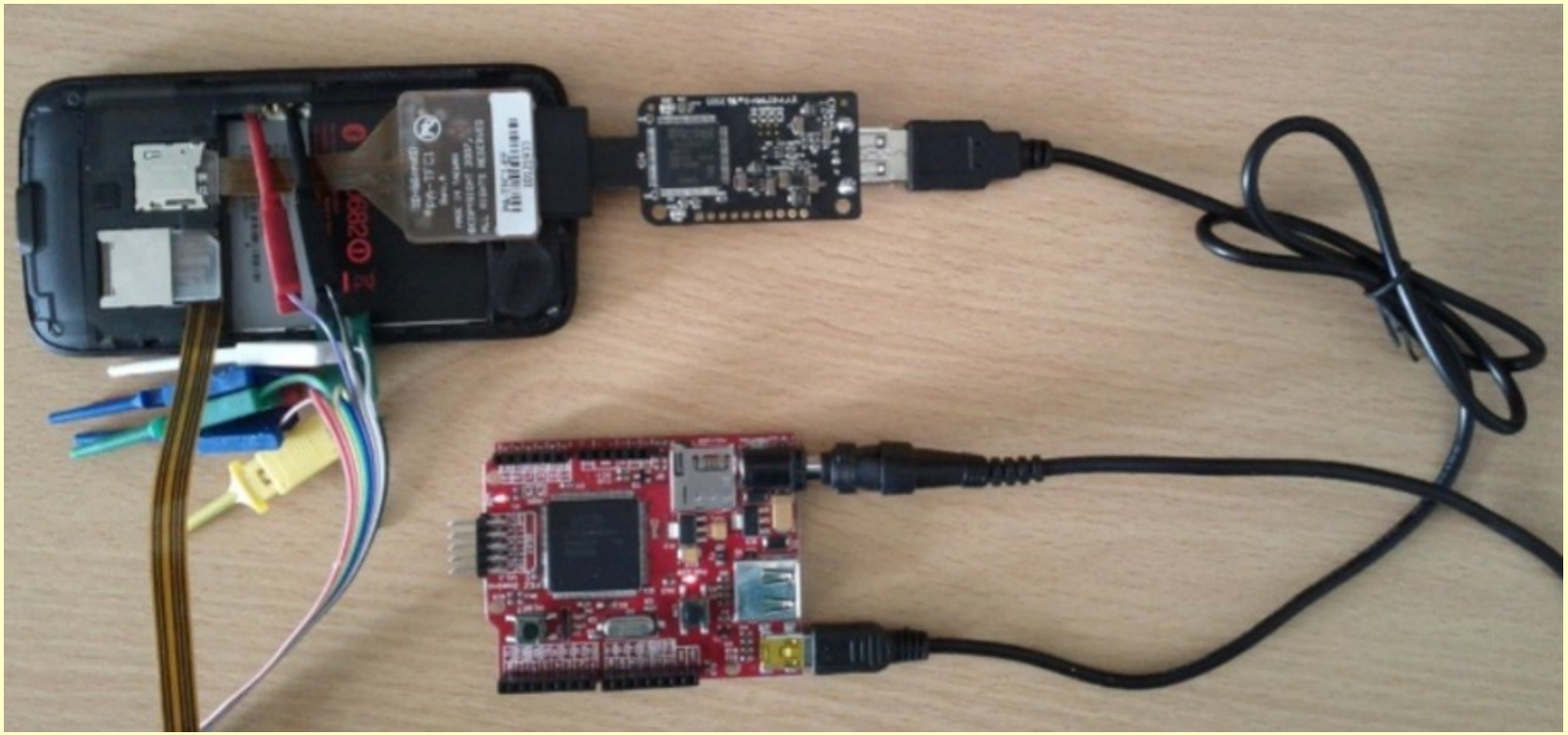
- On a personal computers there is some kind of protection against Cold Boot attack:
  - TRESOR: encryption keys could be stored in CPU cache instead of RAM-u (on processor with AES-NI instruction set);
  - PrivateCore vCage: RAM encryption (with TPM module and Intel Trusted Execution Technology - vCage Host loads a secure hypervisor into CPU cache and is acting as a gateway to encrypt memory paging in and out between the CPU cache and RAM).

- Mobile phones **does not have** such a technology (yet?).

Evil Maid attack on mobile phones

- Evil Maid attack (against computers protected with TrueCrypt) was introduced in 2009 by Joanna Rutkowska.
- Physical access is needed.
- Similar attack against mobile phones was introduced in 2012 by Thomas Cannon from Viaforensics.
- He has shown how to inject malware on a mobile phone through malformed USB charger.
- Malware can intercept passwords or enable remote access to mobile phone.

Evil Maid attack on mobile phones



Thomas Cannon, Into The Droid - Gaining Access to Android User Data,
<https://www.defcon.org/images/defcon-20/dc-20-presentations/Cannon/DEFCON-20-Cannon-Into-The-Droid.pdf>

Evil Maid attack on mobile phones

- Possible solution is *dm-verity* (since Android 4.4):
  - provides integrity checking of file system and is detecting rootkits with root privileges (checks if booting a device is in the same state as when it was last used);
  - however, it does not check if bootloader has been properly authenticated;
  - can not detect a trojan placed in the ARM Trustzone (the *Security Extensions of ARM processors*) or on a SIM card.


BUSTED!

Baseband attacks

How much processors does your mobile phone have?

- Application processor (Tegra, Exynos, Snapdragon,...).
- Processor on a SIM card.
- Radio processor (*baseband processor, modem, radio*):
  - running *real time OS*;
  - is primary processor;
  - usually has full control over all the other hardware (including camera, microphone, screen, etc.);
  - some smartphones even use a shared memory architecture to transfer data from the baseband processor and application processor.

Attacks over the radio processor

- There are known cases, where law enforcement agencies used a covert listening device (a so called "*roving bug*") in their investigations. One of the first known cases is from 2006 - in that case FBI remotely activated the cell phone microphone and listened to conversations in the vicinity of the phone, during its criminal investigation.

- Moreover, as Ralf-Philipp Weinman from the University of Luxembourg has shown that radio processors contain several security vulnerabilities. It is even possible to access a mobile phone from the network (through radio processor).

Attacks over the radio processor

- The group of developers who are working on Replicant, recently found that Android running on a Samsung Galaxy mobile phones contains backdoor.
  - A specific software code allows direct communication with the radio processor in a way that radio processor has direct access to the Android file system (reading, writing and erasing files). That software is able to access the user data, even if they are encrypted.

- Karsten Nohl has shown in 2013 that SIM cards are also vulnerable.


BUSTED!

What about using external encryption device?

Using external, separated encryption device

- To prevent bypassing encryption software running on a mobile phone with malware, it is possible to use **external encryption device** (for instance JackPair).
  - Device is connected between mobile phone and earphones.
  - However, activation of external microphone does not physically turn the built-in microphone off!
    Attacker can turn the internal microphone on with malware and thus effectively bypasses the encryption.


BUSTED!

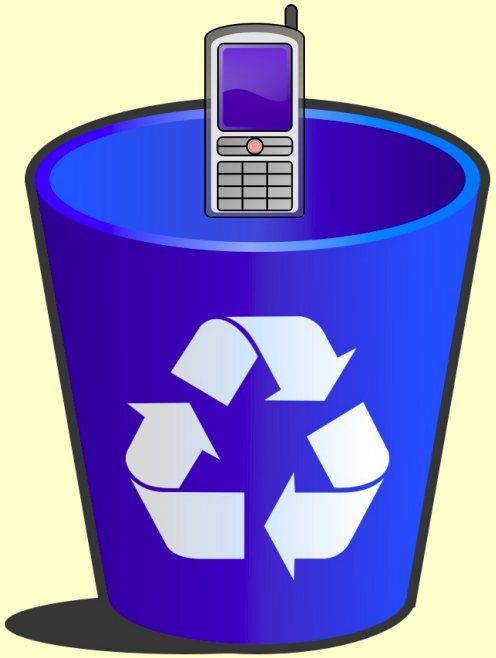
Conclusion

- Data on a SIM card?
- Spoofing the identity of SMS sender?
- Spoofing the identity of a caller?
- GSM traffic security?
- Mobile identity?
- Traffic data in data retention database?
- Mobile network security?
- Mobile network authentication?
- Smartphones security:
  - Location tracking?
  - Attacks to internal memory?
  - Baseband attacks?
  - Using external encryption device?

Conclusion

- Mobile phone security is not easy!
- Just buying some security software or “installing an antivirus” is not the final solution.

- Anyway, the question is how deep we need to go, what is our threat model?
  - sometimes sceen lock is enough...
  - ...sometimes using applications for encrypting communication is necessary..
  - ...sometimes we must consider using the trash. :-)



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

--Bruce Schneier

BUSTED!

Questions?

http://pravokator.si