Mobile Security

Matej Kovačič
https://pravokator.si

Authentication problem

Mobile telephony does not have built-in proper authentication.

Caller or. SMS sender is "authenticated" only by his mobile number.

Result: Caller ID spoofing is possible!

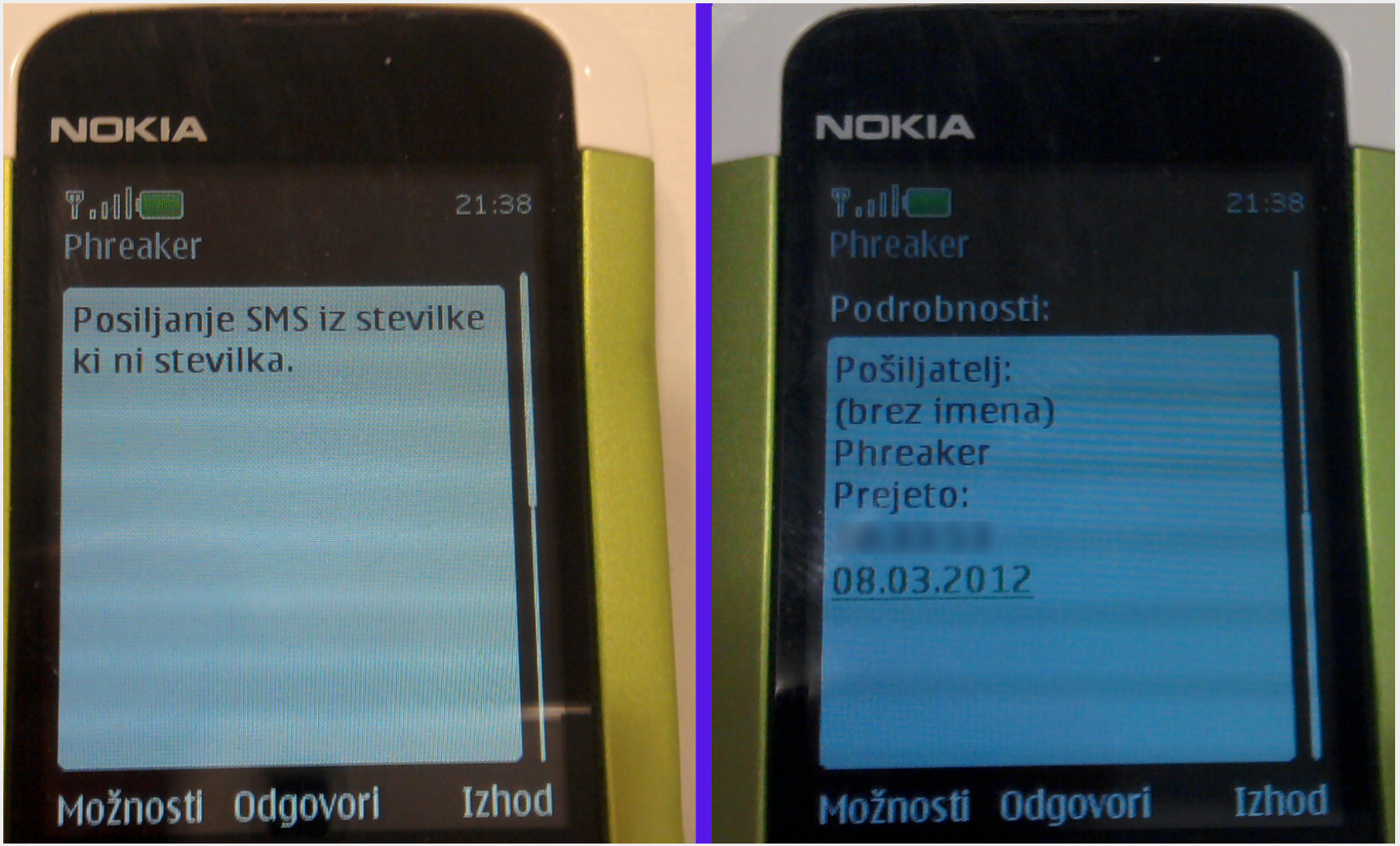
There is also lack of authentication among telecom providers.

Result: several possible attacks on SS7 infrastructure!

Mobile network is not authenticated to the mobile phone.

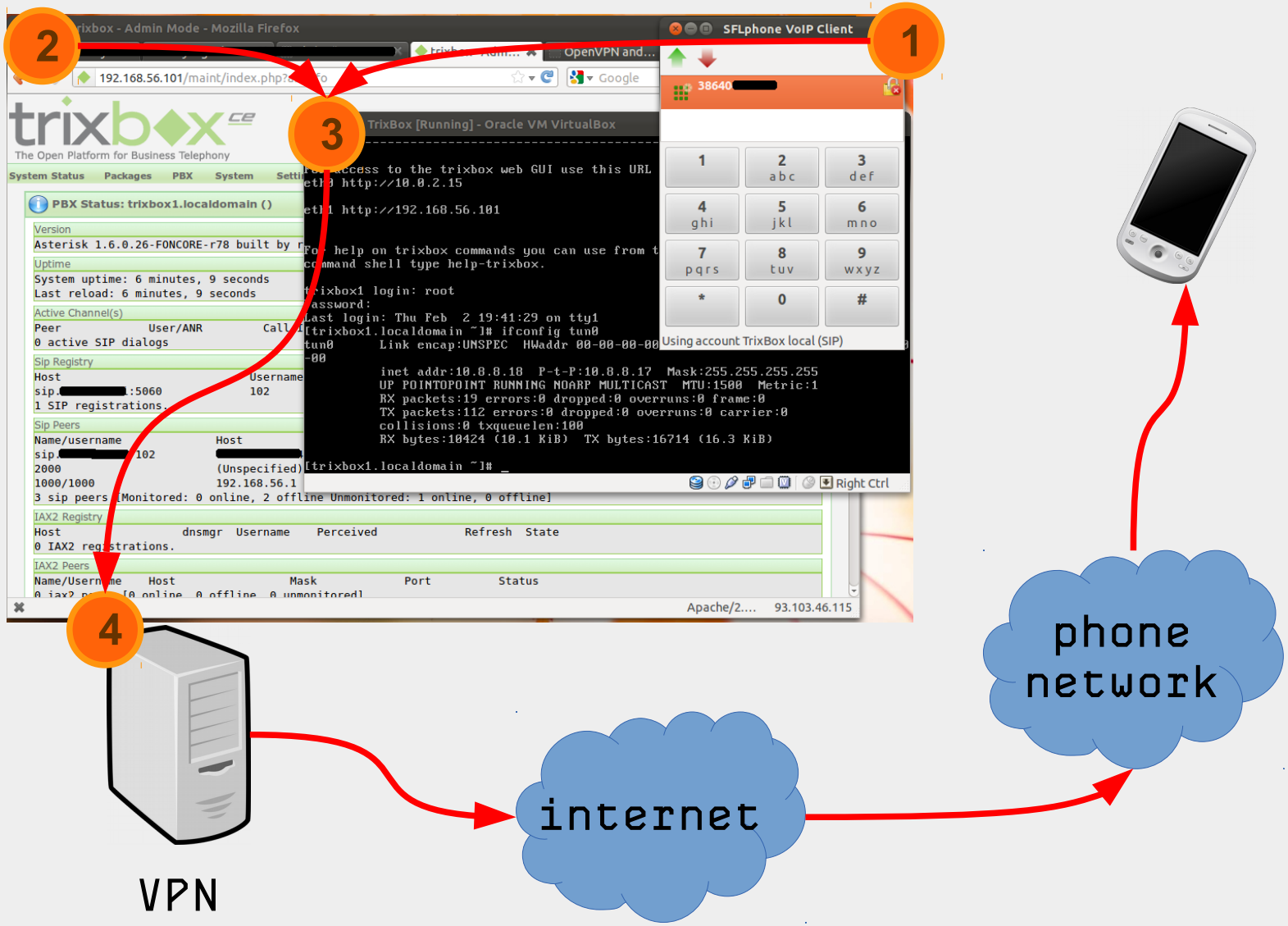
Result: fake base stations (i. e. IMSI catchers) could be used!

SMS spoofing

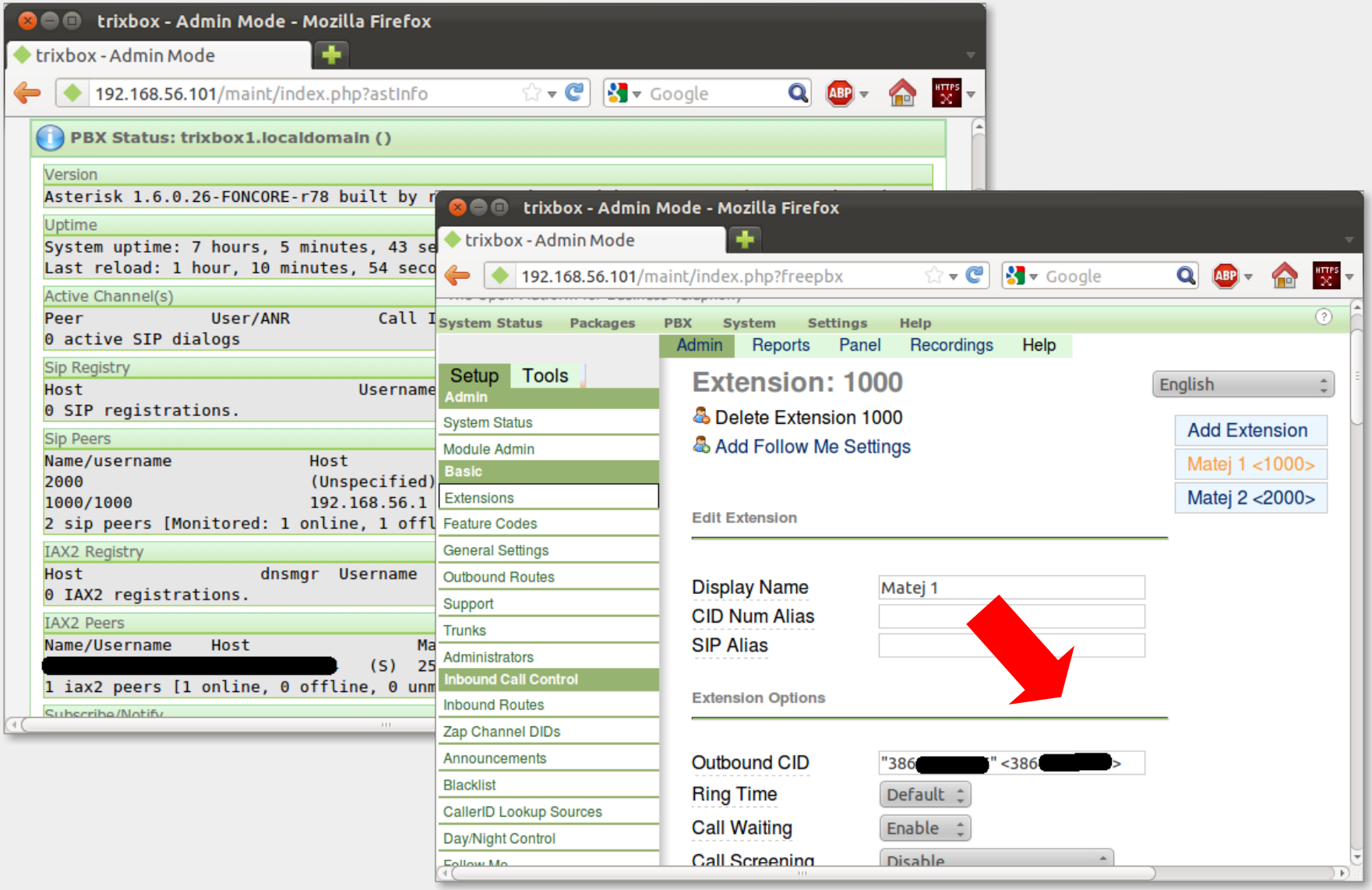


<http://provider.com/sms/json?username=xxxxxxxx&password=xxxxxxxxx&from=Phreaker&to=38631123456&text=Sending%20of%20SMS%20from%20number%20which%20is%20not%20a%20number.>

CallerID spoofing

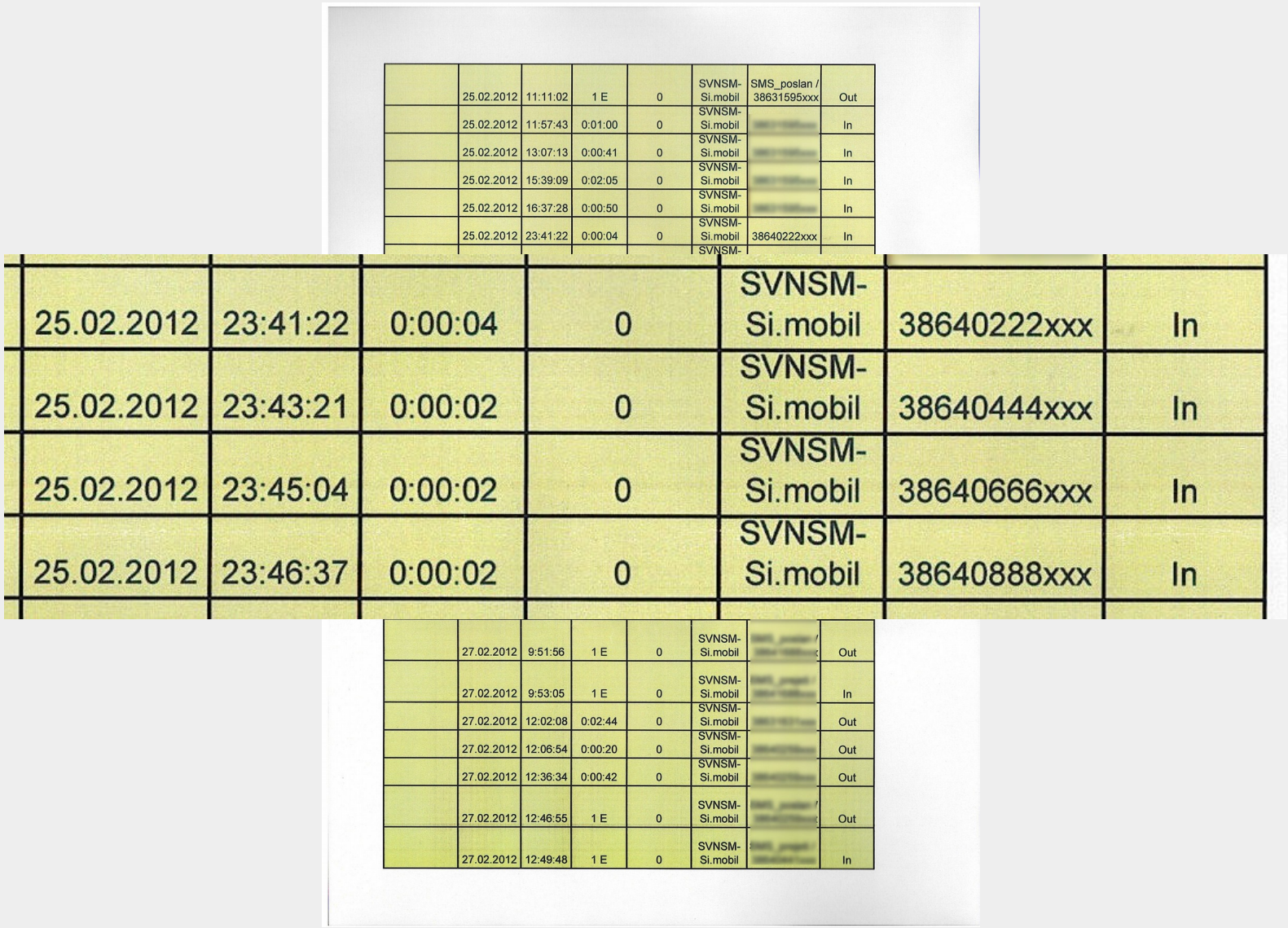


CallerID spoofing



CallerID spoofing

CallerID spoofing



	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 of spoofing :-)

GSM module to open garage or front door

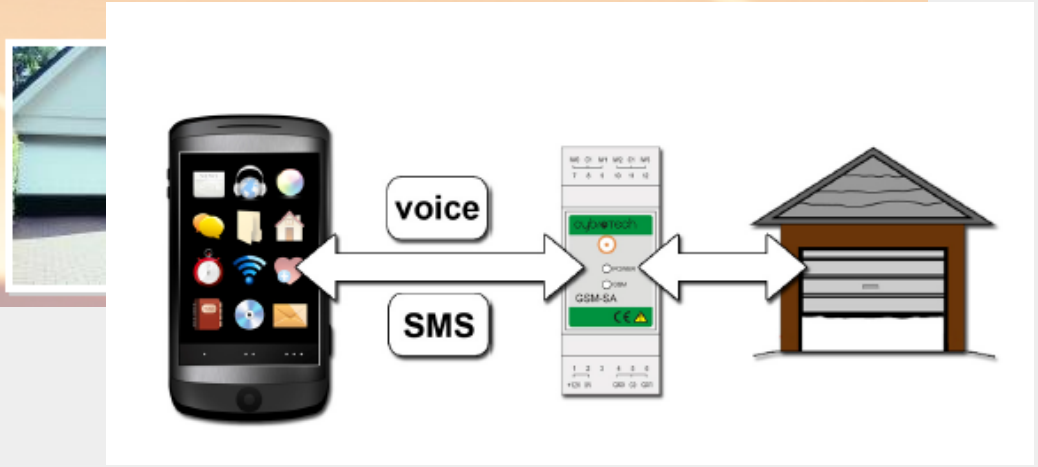
We offer a useful device with a simple phone call opens or closes the automated garage or front door.

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.

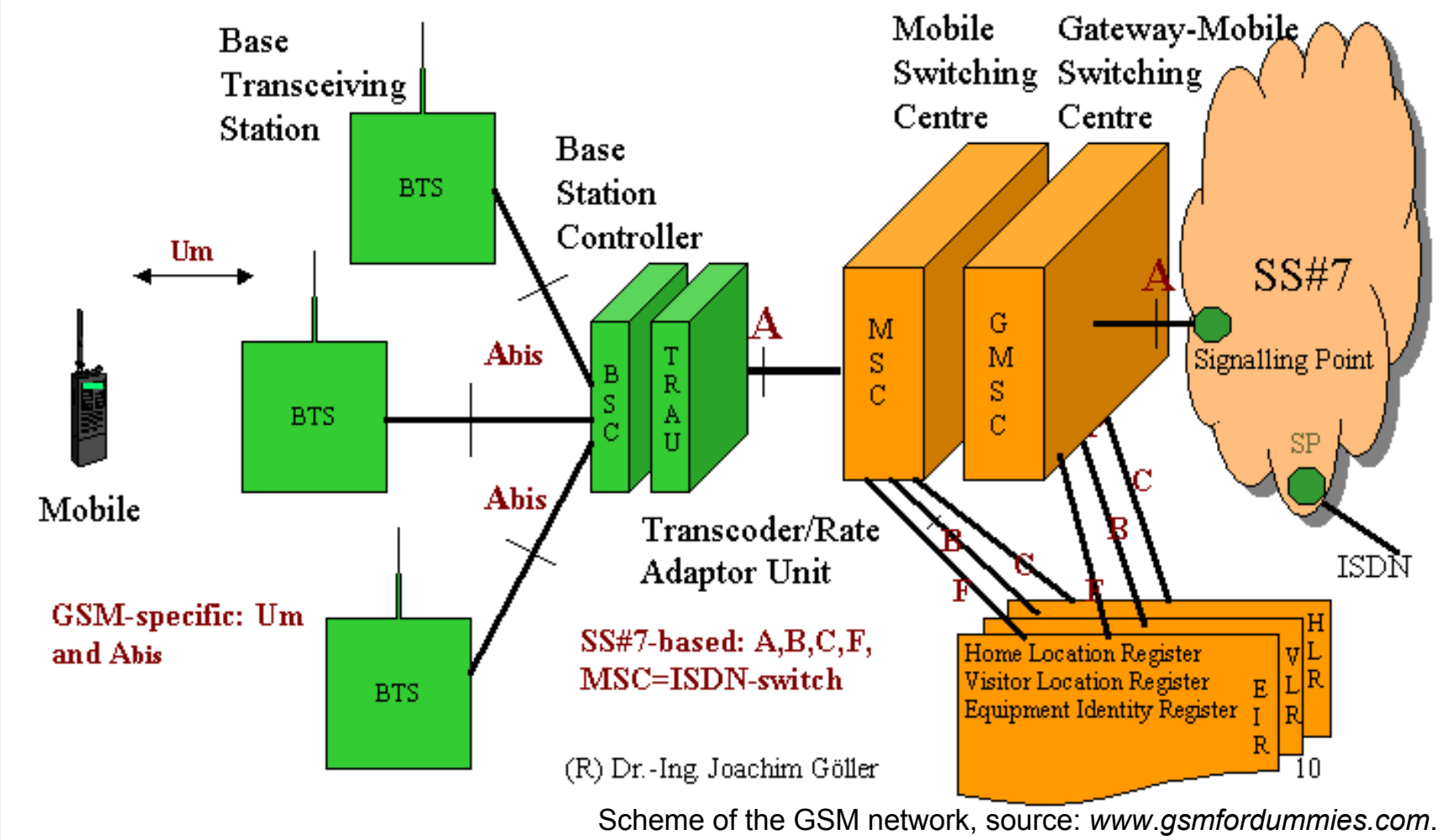
Iku d.o.o. offers you:

- 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 additional equipment and appliances, because we assume that the mobile phone is already



Some GSM basics



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

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

Capturing the signal in the past...

1 Use of phones with Calypso chipset...

```
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!
```

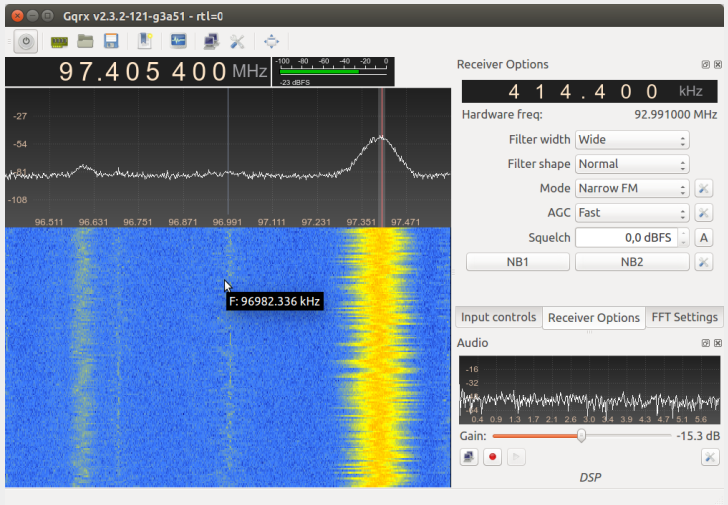
2 Connecting the phone to a computer with a special cable and loading modified ROM...

```
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)
Terminal 0  Terminal 1  Terminal 2  Terminal 3  Terminal 4
```

3 Running the applications for capture and analysis.

Capturing the signal today...

DVB-T device (with Elonics 4000 čhipset; ~20 EUR).

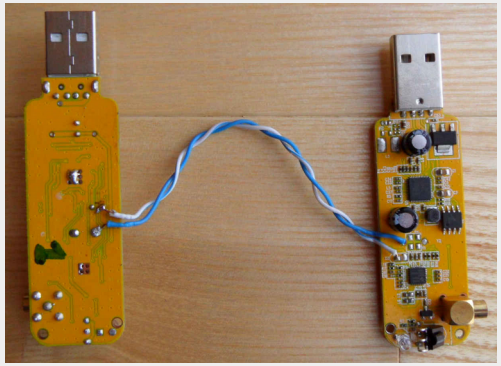


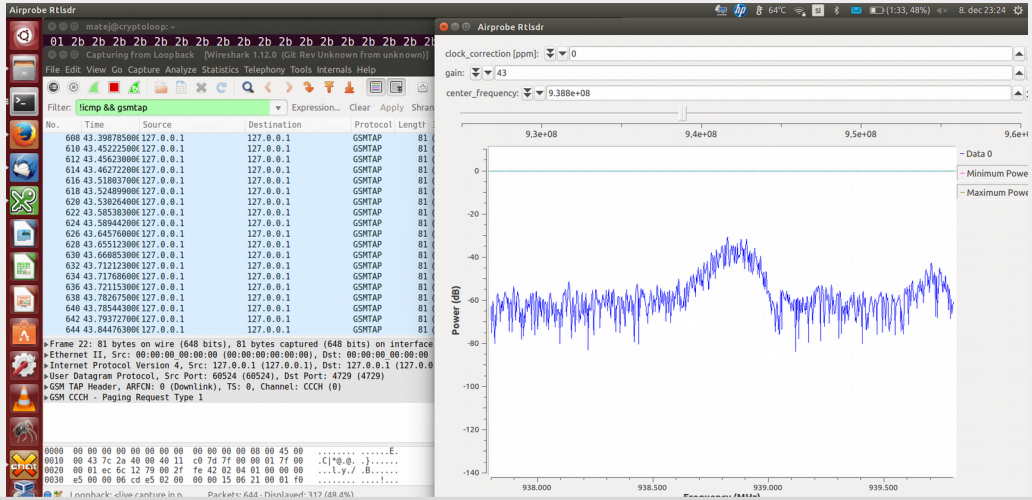
gr-gsm

Toolset for capture and analysis of GSM signals.

```
grgsm_livemon -p 35 -f 938.8M
```

```
wireshark -k -Y '!icmp && gsmtap' -i lo
```

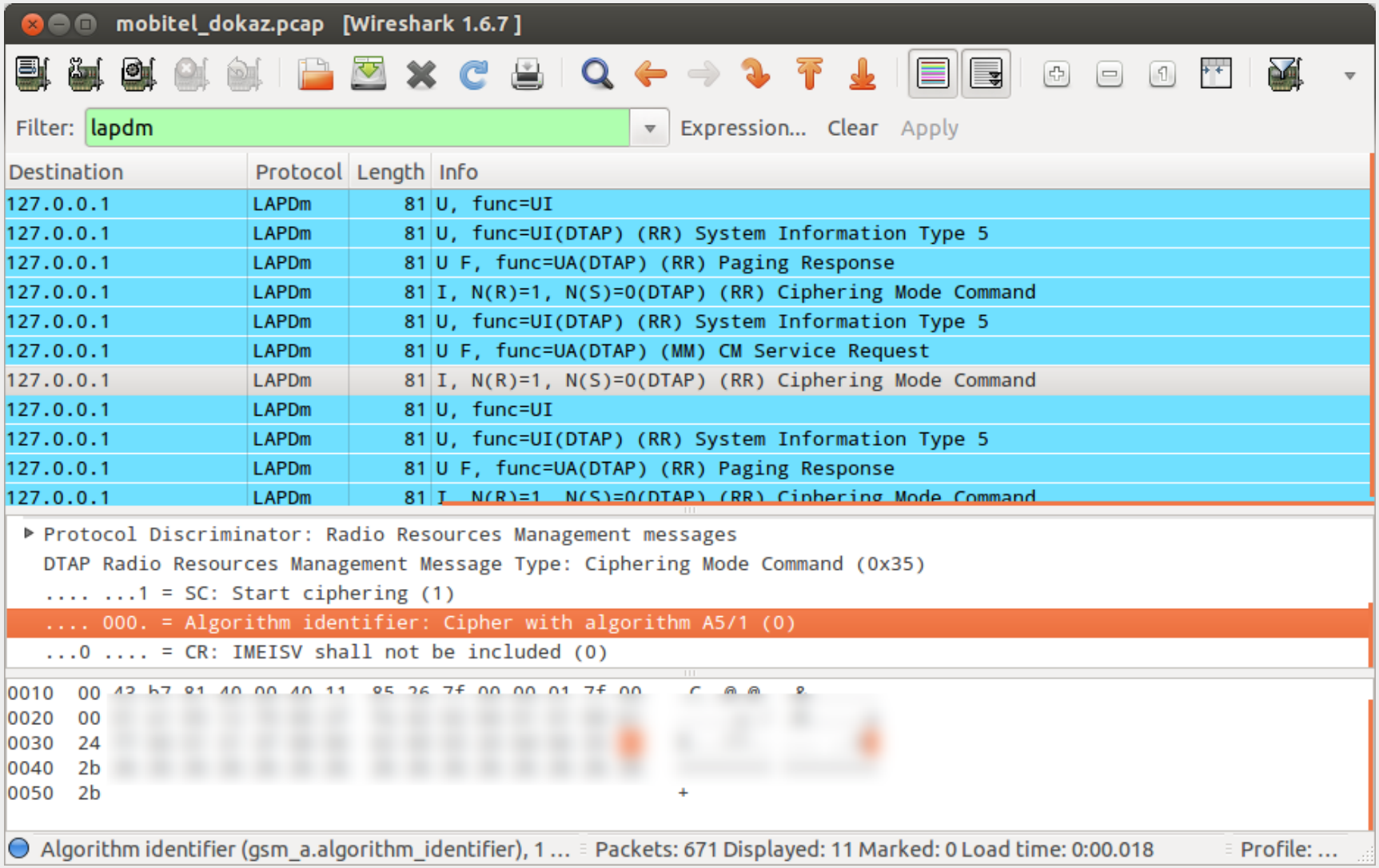





```
grgsm_scanner -p 35
```

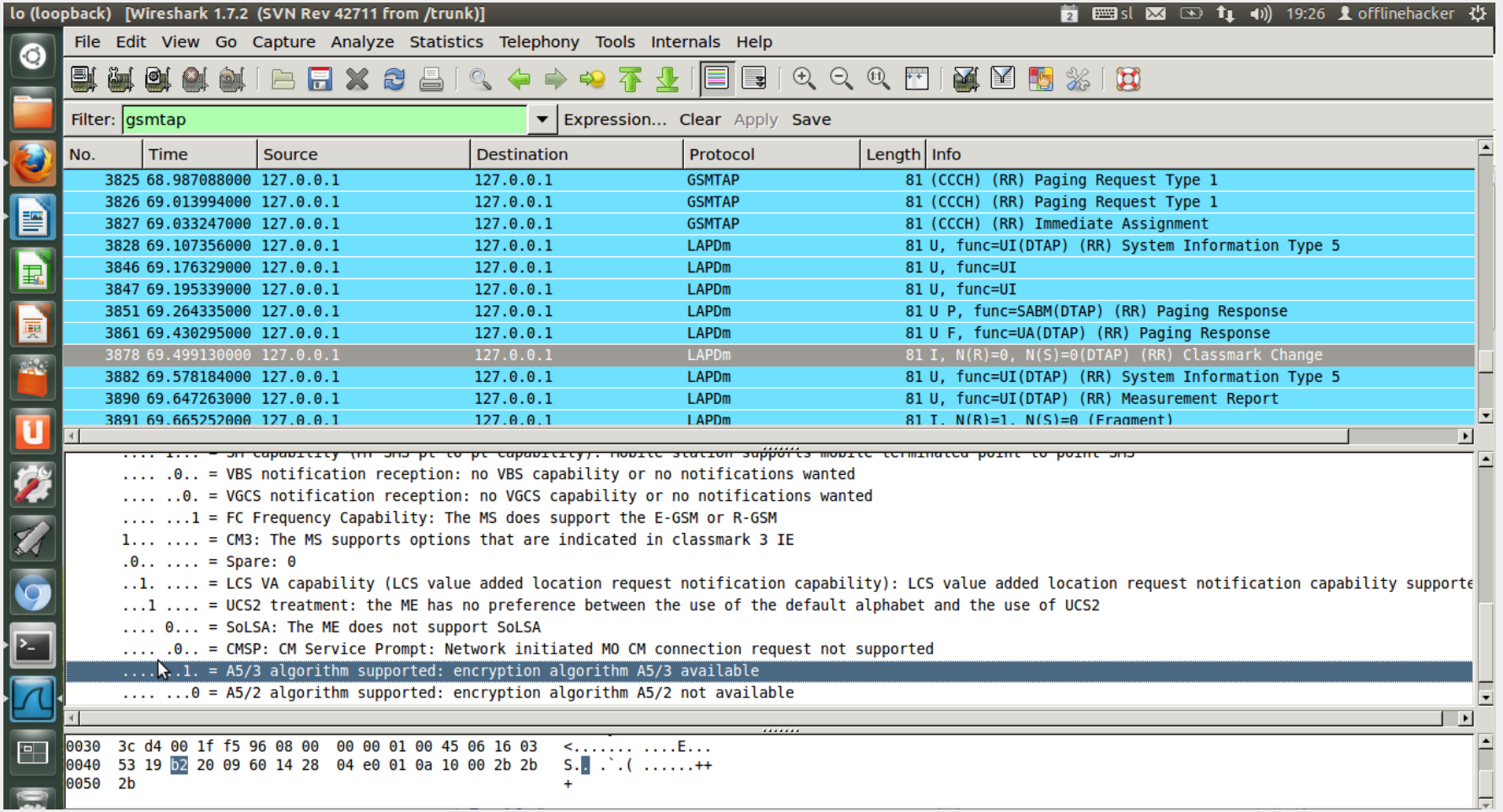
```
linux; GNU C++ version 4.9.1; Boost_105500; UHD_003.007.003-0-unknown


ARFCN:   18, Freq:  938.6M, CID:     0, LAC:   100, MCC: 293, MNC:  40, Pwr: -35
ARFCN:   24, Freq:  939.8M, CID:  1313, LAC:   100, MCC: 293, MNC:  40, Pwr: -33
ARFCN:   26, Freq:  940.2M, CID:   501, LAC:   100, MCC: 293, MNC:  40, Pwr: -27
ARFCN:  124, Freq:  959.8M, CID:     0, LAC:     0, MCC:   0, MNC:   0, Pwr: -29
```

GSM security analysis in 2012



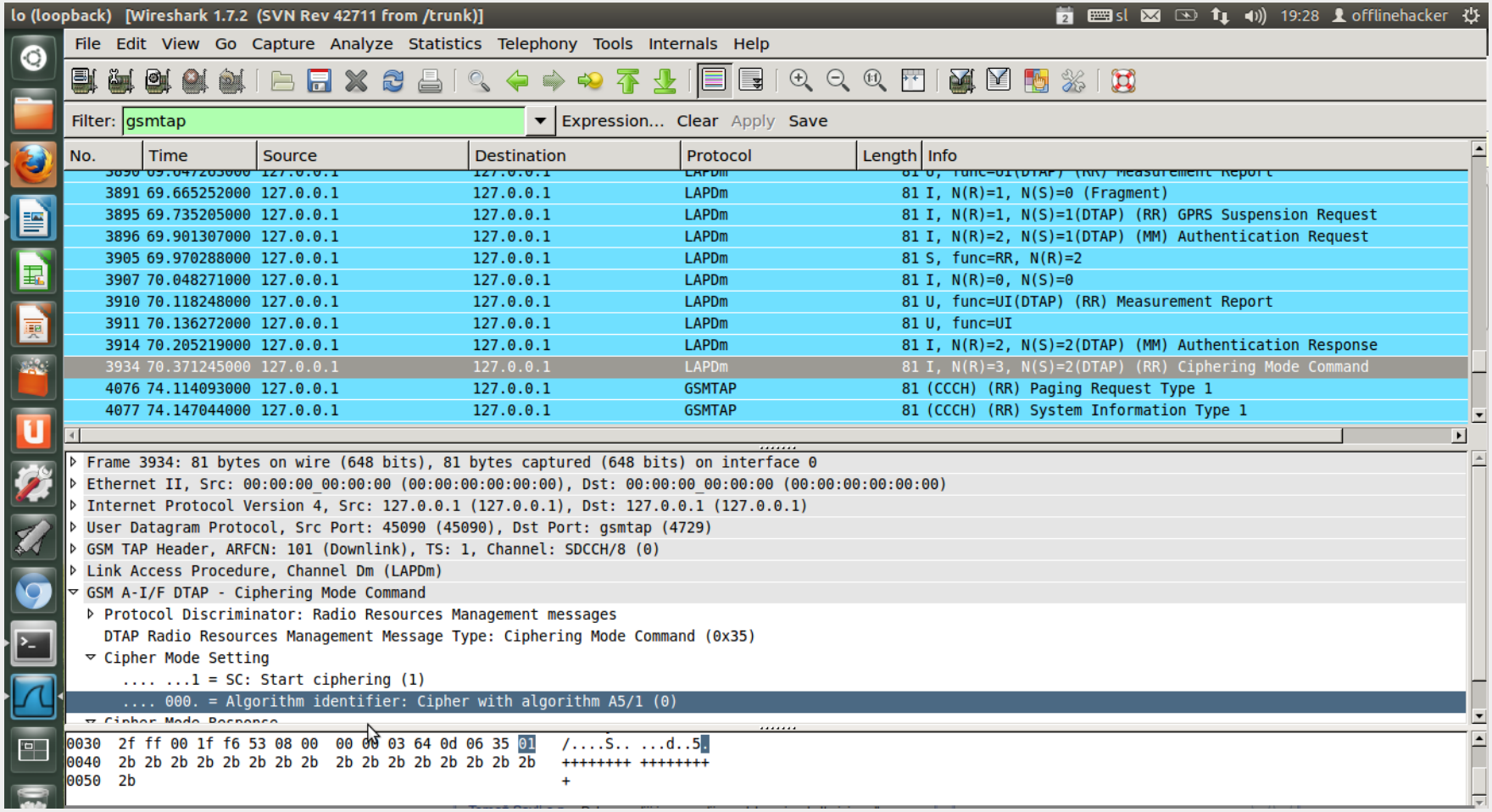
Some mobile operators were using A5/1 ciphering...

GSM security analysis in 2012



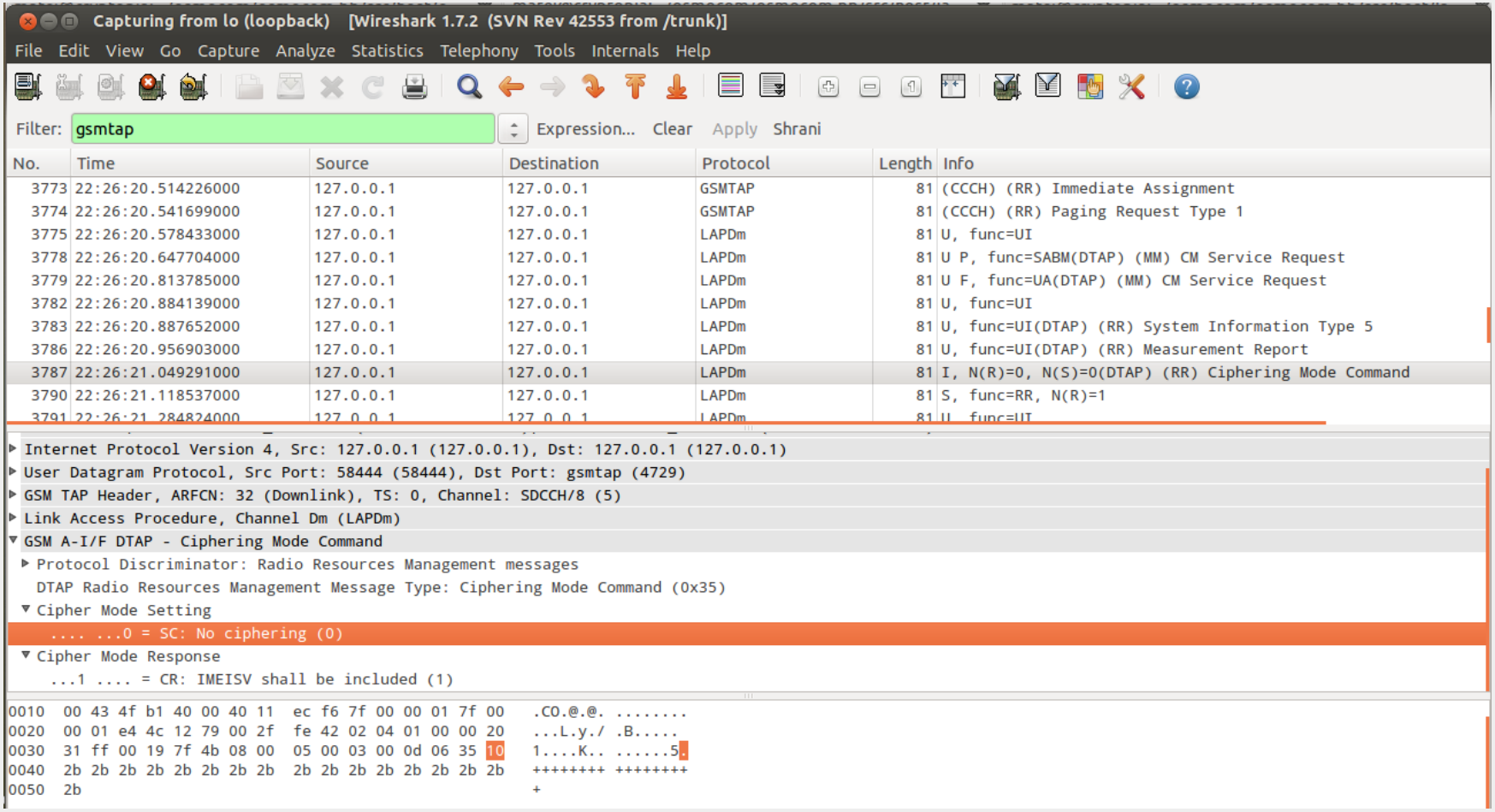
If mobile phone said it supports A5/3...

GSM security analysis in 2012



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

GSM security analysis in 2012

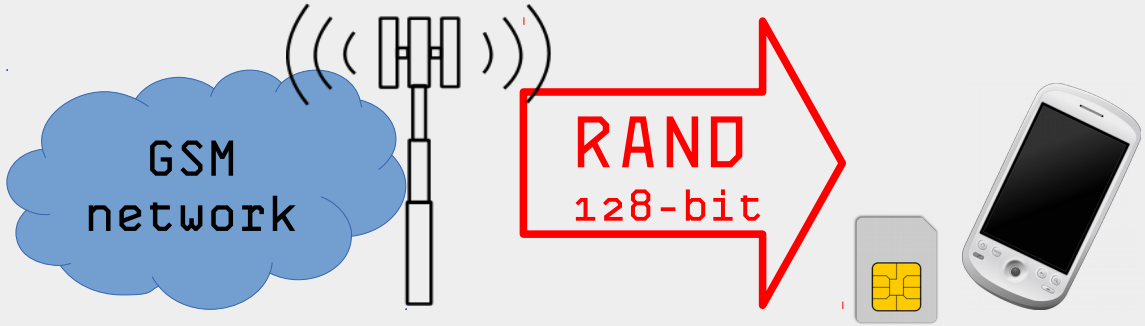


In one network it was possible to switch off the encryption completely...

GSM encryption

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.

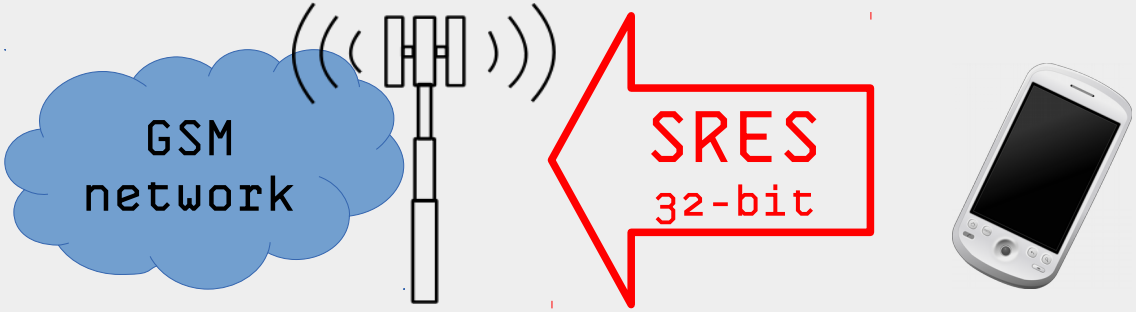
1.



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

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

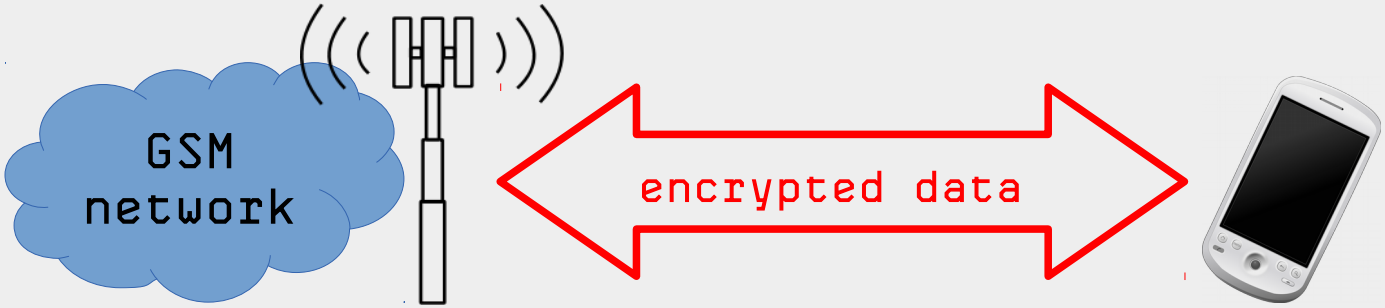
2.



GSM encryption

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.

GSM cryptanalysis

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

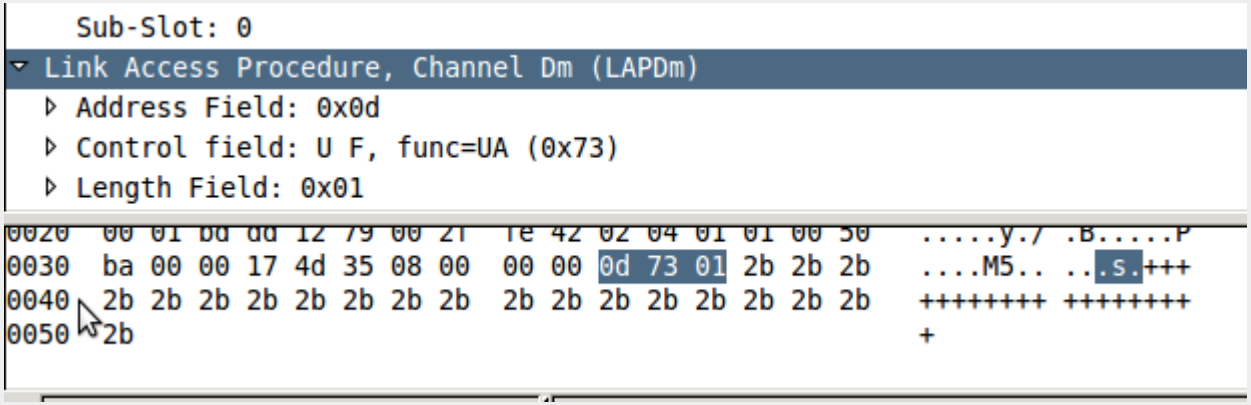
Kraken

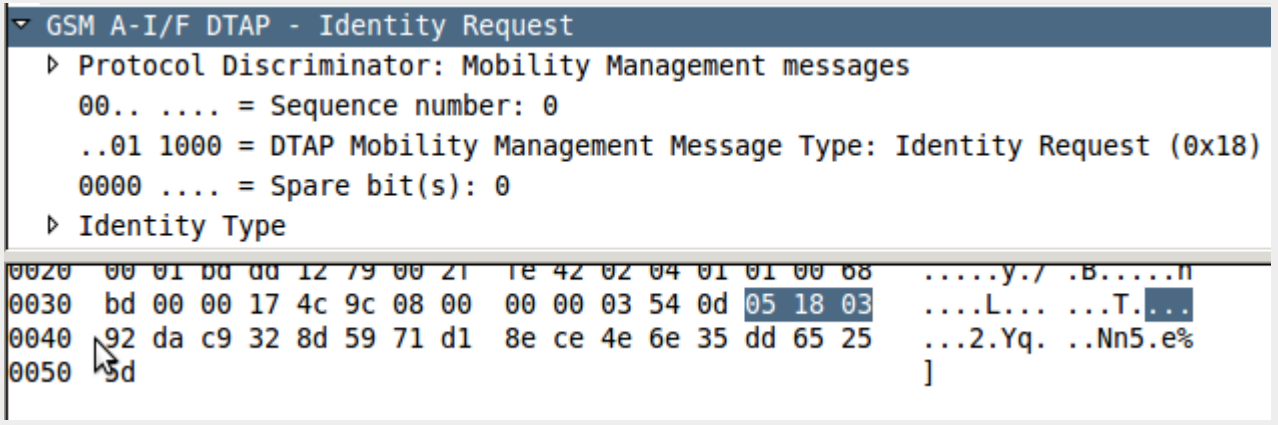
ENCRYPTED MESSAGE (XOR)

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

Kc

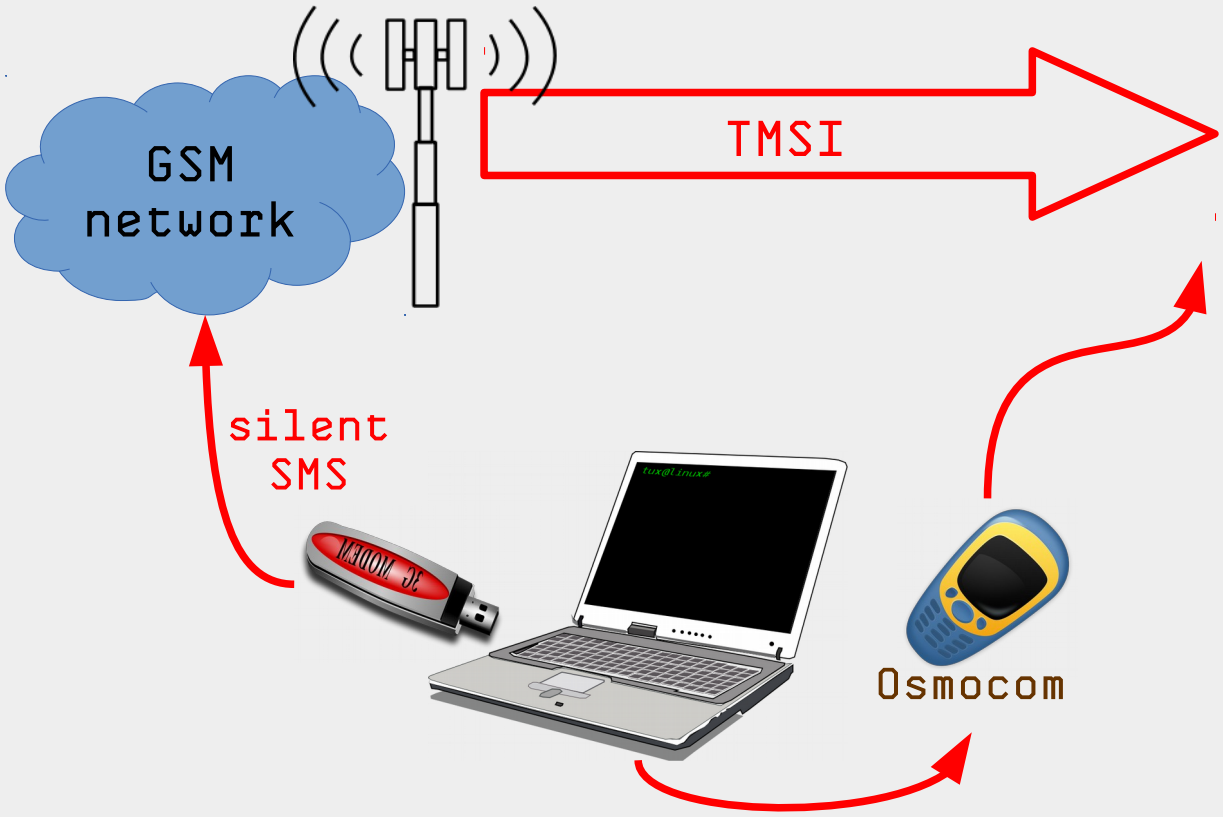
Random padding vs. non-random padding





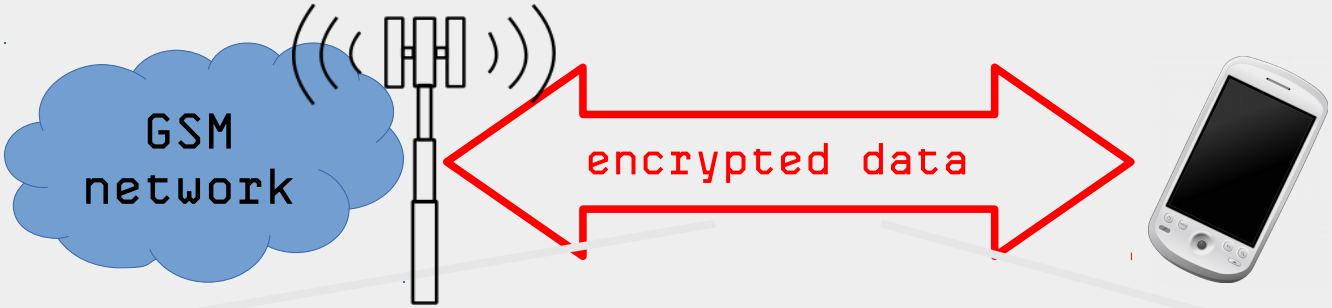
Locating the user in mobile network

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



Mobile phone user does not detect reception of silent SMS.

Cryptanalysis in practice



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

CONTENT OF DATA BURST IN GSM

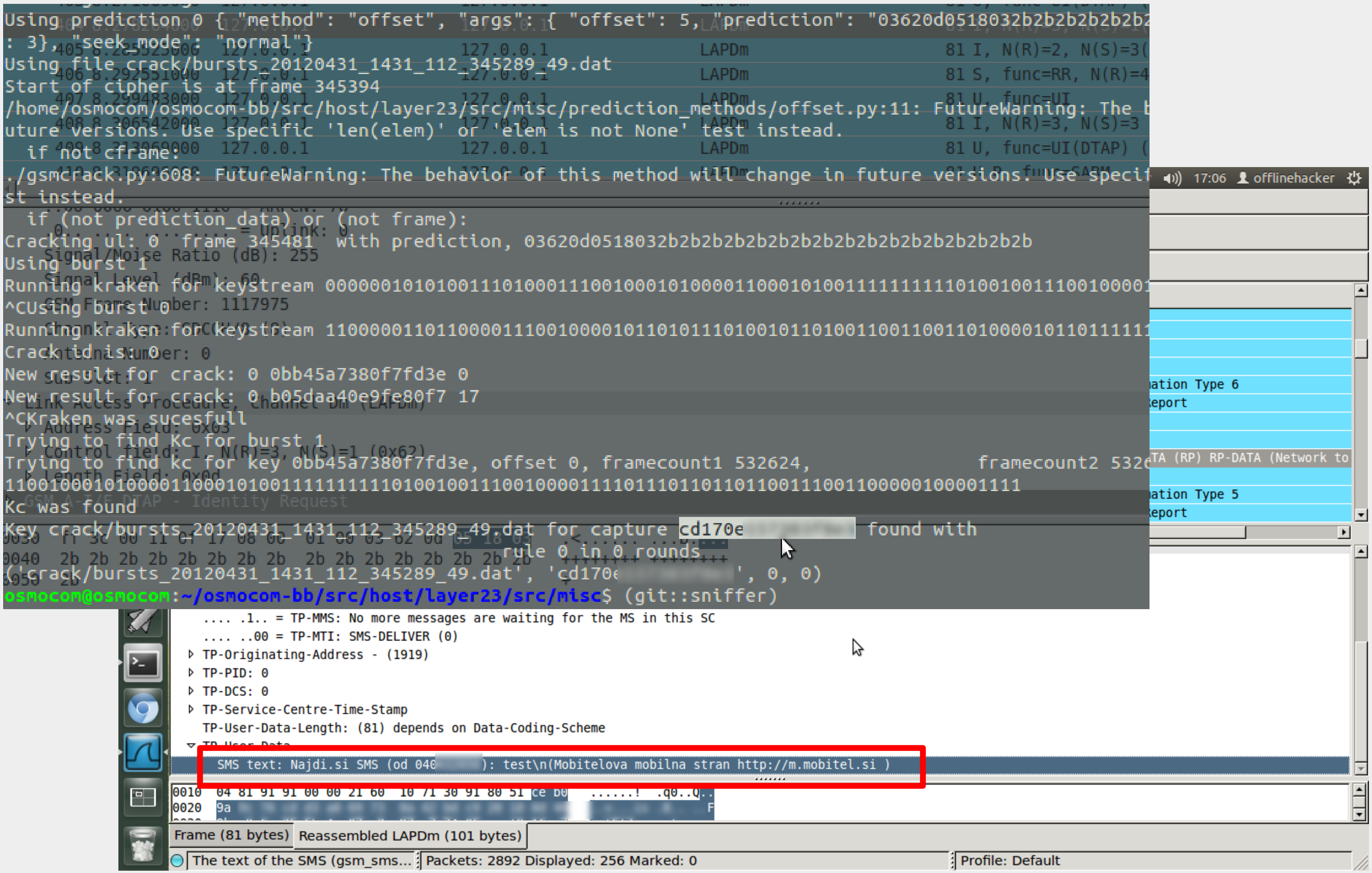
72	FE	BC	10	74	70	C4	2B	2B	2B	2B	2B	2B

Kraken

- 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!

Kc

Cryptanalysis in practice

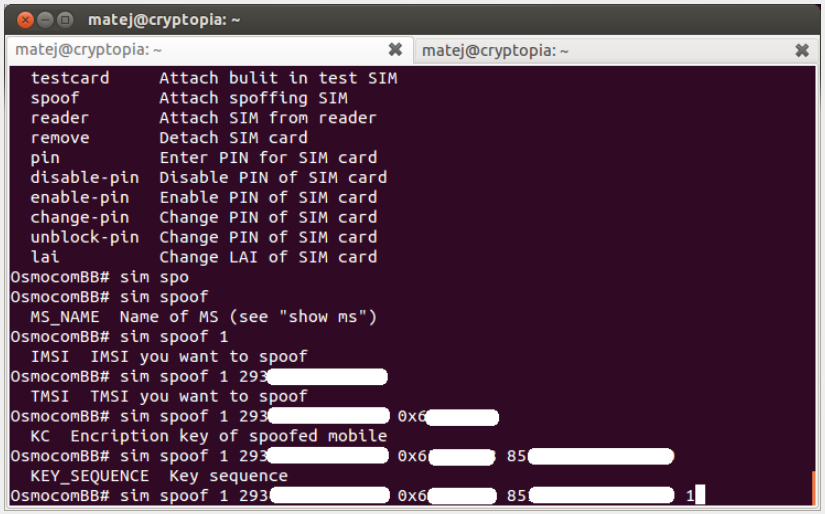


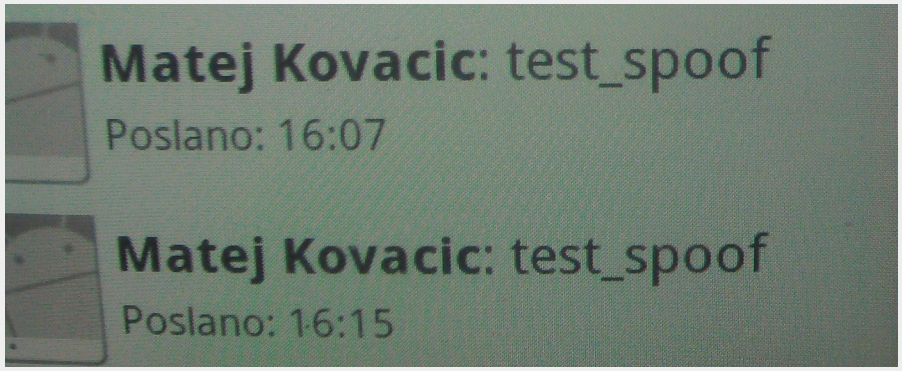
Mobile *identity* spoofing

For mobile **identity** spoofing we need:

- IMSI number (can get it via SS7 lookup),
- TMSI number (capture it from the network),
- session key (we crack it),
- key sequence number (capture it from the network).

In networks with A5/0 we need only TMSI and key sequence number – no cryptanalysis needed!

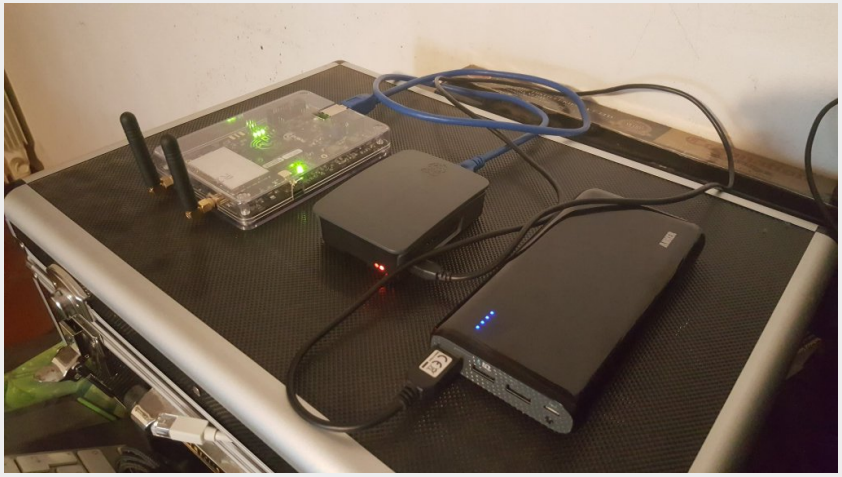


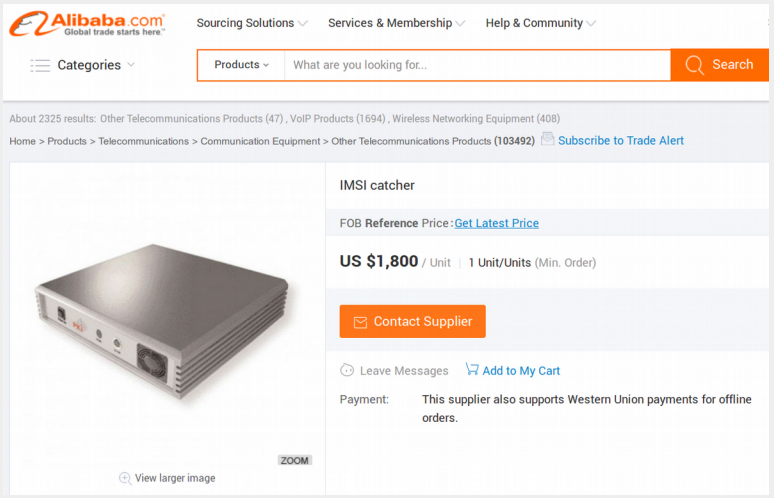


Two SMS messages sent by spoofed mobile identity.

IMSI Catchers

Basically, they are fake base stations





IMSI Catchers – how do they work?

First, they false introduce themselves as legitimate base station.

Then they report false Location Area code to the nearby mobile phones.

Now mobile phones are contact IMSI Catcher (Location Update), but with their TMSI number.

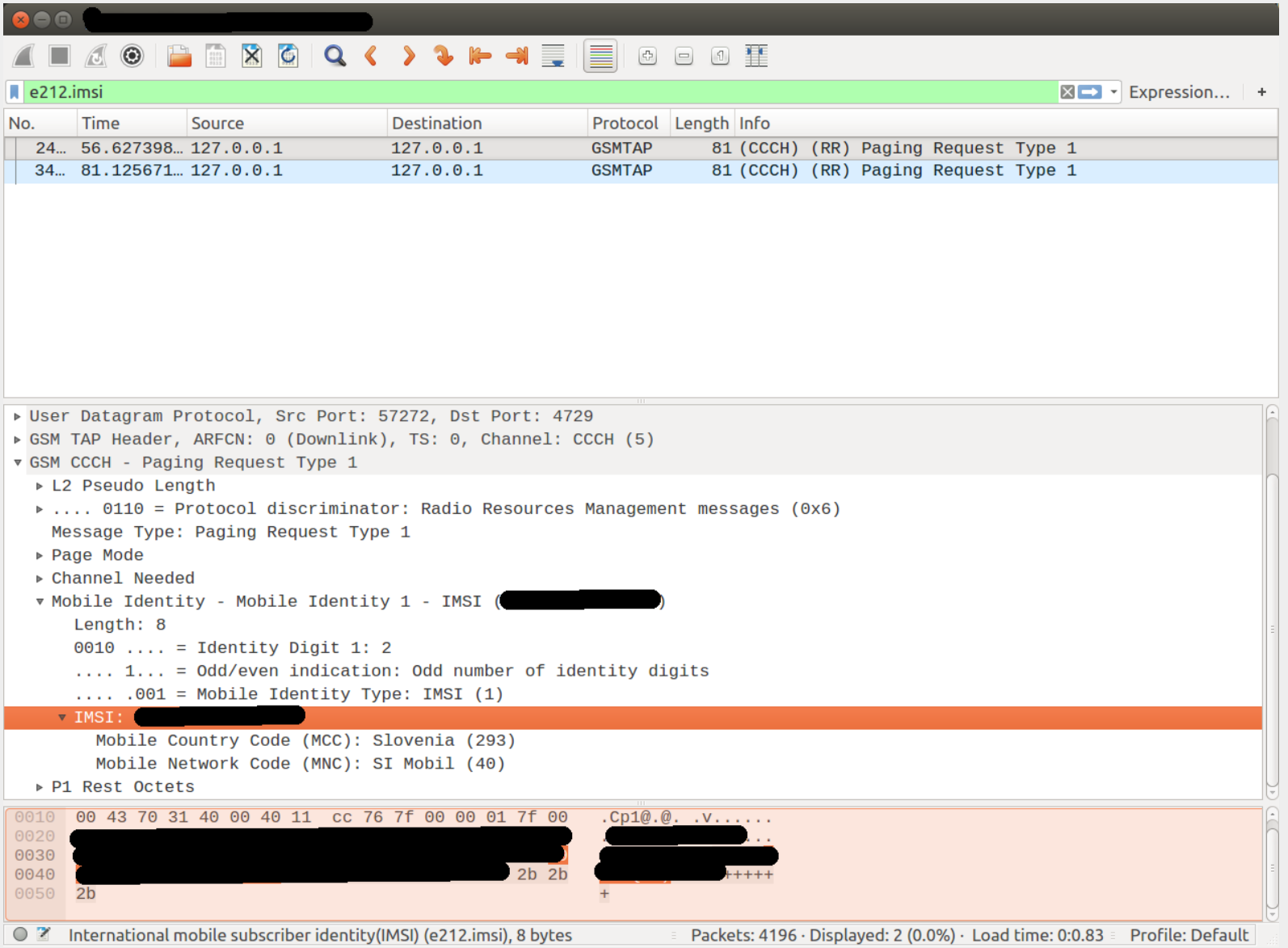
IMSI Catcher now false claims that mobile phone's TMSI has expired and requestts re-authentication.

Mobile phone now reports IMSI and IMEI number to IMSI Catcher.

IMSI Catcher now says it cannot accept a mobile phone (Location Update Reject), and redirects mobile phone back to the original operator.

Or not...

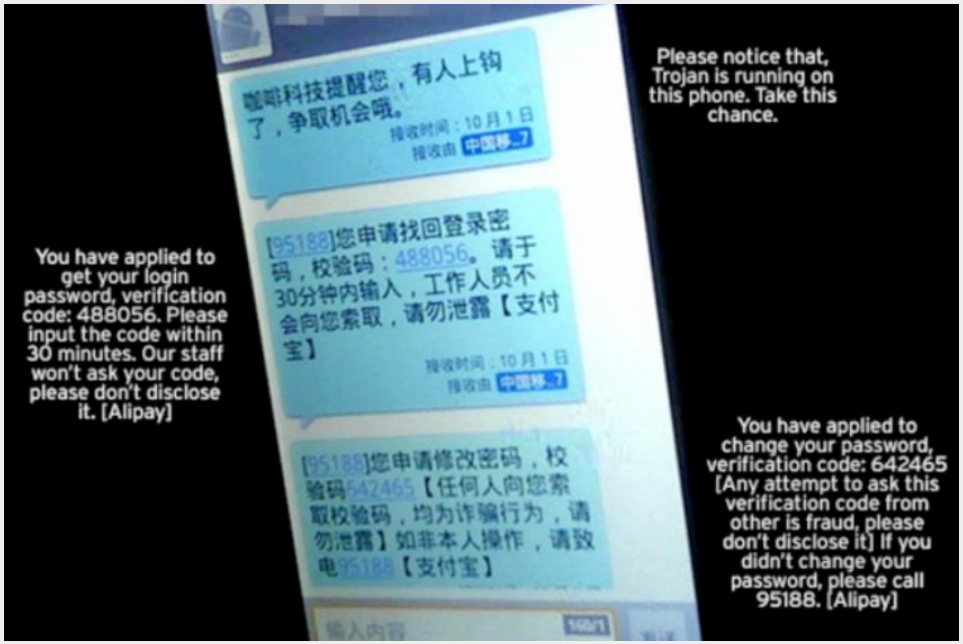
IMSI Catchers - can we detect them?



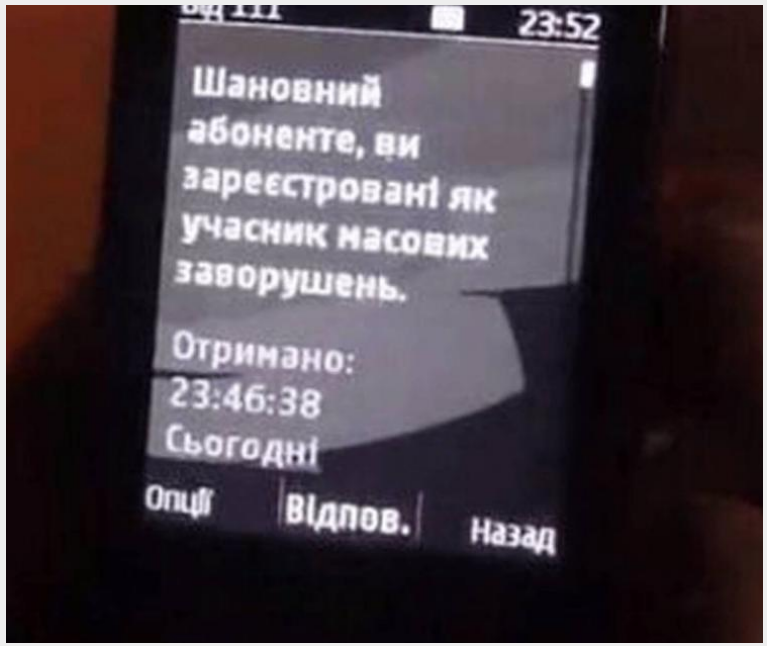
IMSI Catchers – what can they do?

IMSI Catcher can:

- **reveal the exact location** of a mobile phone,
- offer mobile phone a network connectivity and perform **MITM attack**,
- start calls and send SMS messages **past the network**.



Chinese SMS SPAM messages.

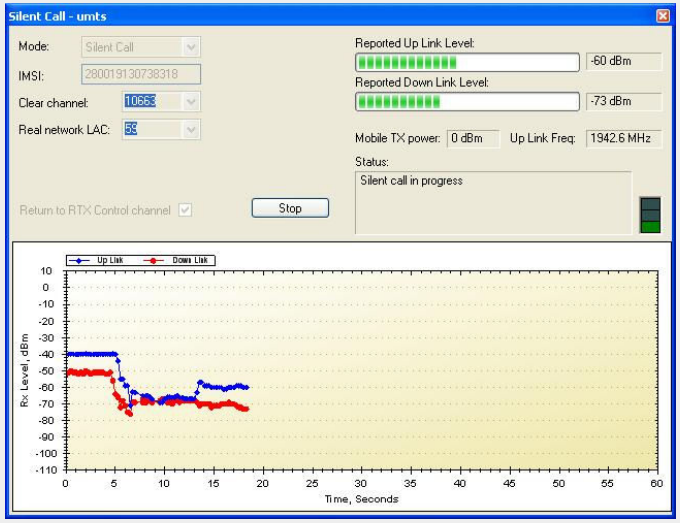


Ukraine – message to protestors.

IMSI Catchers – what can they do?

IMSI Catcher can also:

- **isolate** mobile phone from his network,
- **disable** the phone so it needs to be rebooted or **empty** his battery,
- performs a **silent call**, which opens the microphone and changes mobile phone to an eavesropping device,
- **installs malware** via baseband attack.



UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- X

IN THE MATTER OF AN APPLICATION OF :
THE UNITED STATES OF AMERICA FOR
AUTHORIZATION TO CONTINUE TO :
INTERCEPT ORAL COMMUNICATIONS
OCCURRING AT (i) THE SEATING AREA :
INSIDE BRUNELLO TRATTORIA, 227 EAST
MAIN STREET, NEW ROCHELLE, NEW YORK :
10801; (ii) THE SEATING AREA INSIDE
MARIO'S RESTAURANT, 2342 ARTHUR :
AVENUE, BRONX, NEW YORK 10458;
(iii) THE SEATING AREA INSIDE :
AGOSTINO'S RESTAURANT, 969 BOSTON
POST ROAD, NEW ROCHELLE, NEW YORK :
10801; AND (iv) THE SEATING AREA
INSIDE THE MARINA RESTAURANT, WRIGHT :
ISLAND MARINA, 290 DRAKE AVENUE, NEW

APPLICATION FOR AN
ORDER AUTHORIZING THE
INTERCEPTION OF ORAL
COMMUNICATIONS

Some SS7 attacks

Signalling System #7 is a protocol for exchanging data among telephone operators.

SS7 enables access to Home Location Register, Visitor Location Register and Mobile Switching Center...

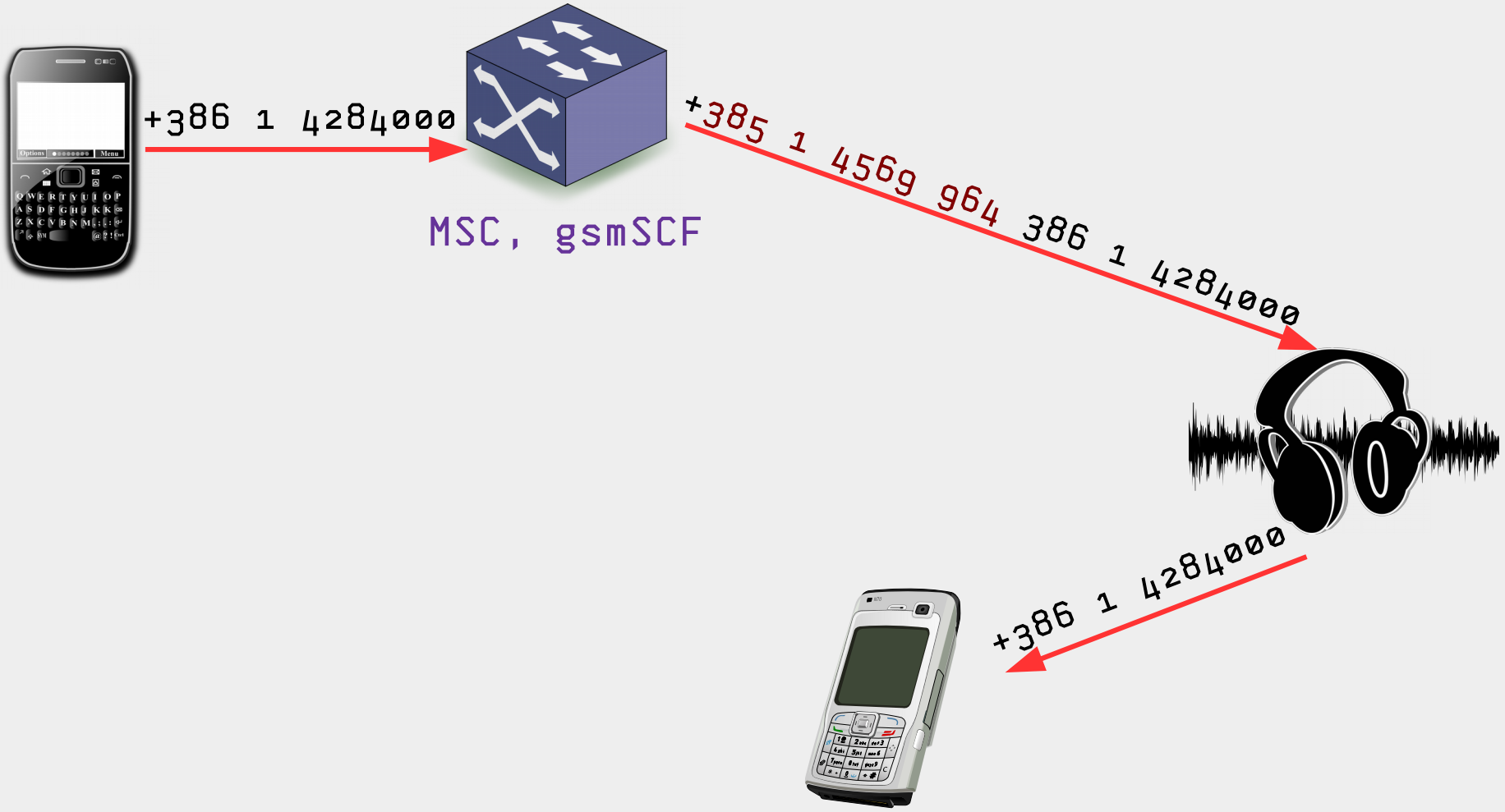
Since the authentication in SS7 is flawed, SS7 could bring us some fun...

Example: CAMEL (Customised Applications for Mobile networks Enhanced Logic) protocol abuse.

- User is roaming in some foreign network.
- User's local HLR tells roaming network's VLR that every time user wants to make a call, MSC should contact gsmSCF (GSM Service Control Function) in home network and ask what to do with a call.
- If user is calling "local number", gsmSCF rewrites number to international format (+386...) and tells MSC to continue with the new number.

Example: intercepting outgoing calls

...



Example: intercepting incoming calls

An attacker pretends that a subscriber is in his "network" by sending the *updateLocation* with his *Global Title* to the subscriber's HLR.

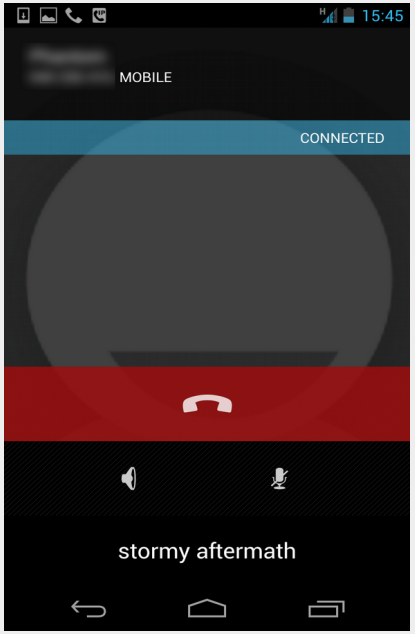
All calls and SMS messages for that subscriber are now routed to the attacker.

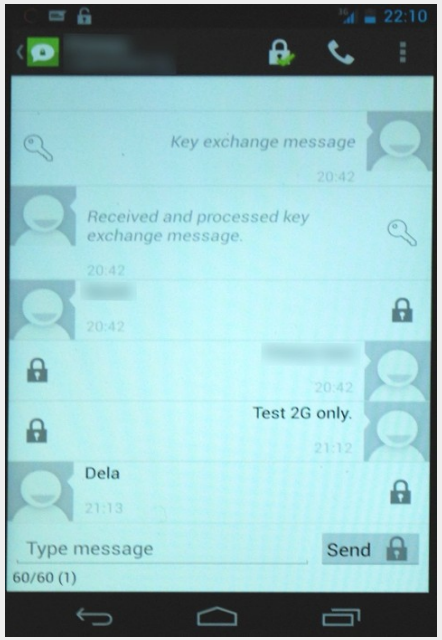
Now a victim logs into her/his bank account, and since s/he is using two-factor authentication, her/his bank sends SMS to her/his number with mTAN access code...

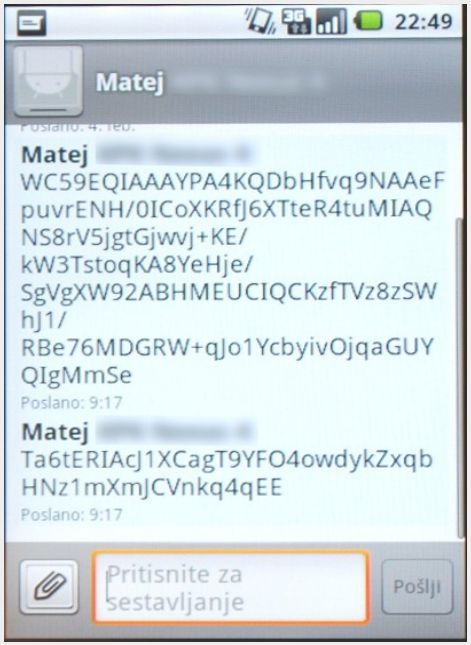

BUSTED!

Protection

Encryption of mobile communications

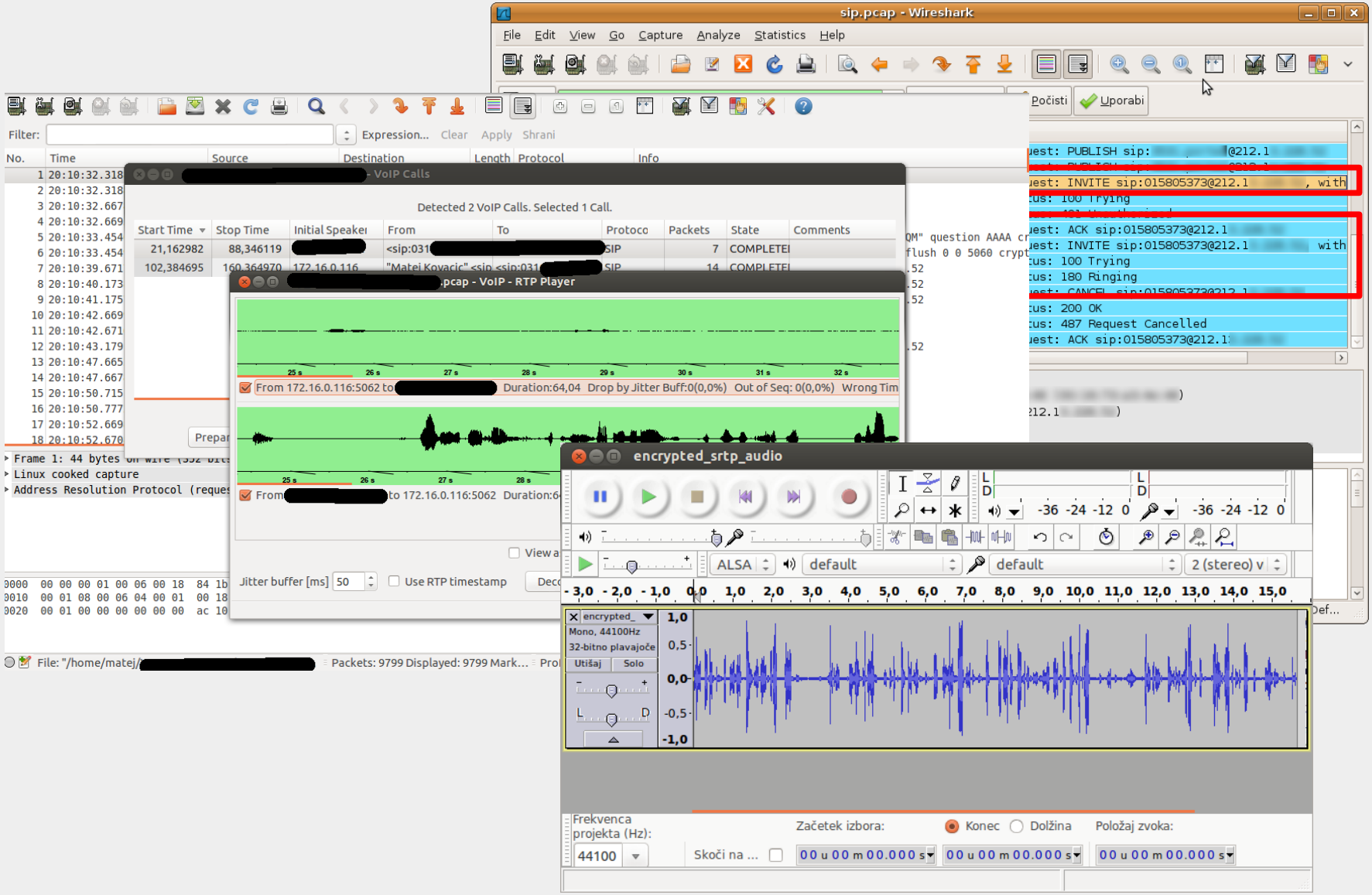






The main approach is to use data transfer and encryption on an application level.

Unencrypted vs. encrypted phone call



Signal application

There are several applications for encrypted mobile communications.

However, Signal app by Whisper Systems seems to be the best. On a technical level it has:

- strong encryption algorithms,
- perferct forward secrecy and future secrecy,
- detection of MITM attacks,
- »end-to-end« encryption,
- asynchronous communication,
- encrypted storage of messages.

Technical solution prevents eavesdropping on a communication link and by the operator.

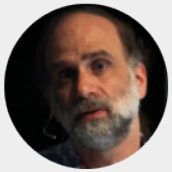
Signal application

User level:

- easy to use,
- free of charge,

> After reading the code, I literally discovered a line of drool running down my face. It's really nice.
>
> — **Matt Green**, Cryptographer, Johns Hopkins University

- source code is completely open,
- application has been security reviewed.



> I am regularly impressed with the thought and care put into both the security and the usability of this app. It's my first choice for an encrypted conversation.
>
> — **Bruce Schneier**, internationally renowned security technologist

> Signal is the most scalable encryption tool we have. It is free and peer reviewed. I encourage people to use it everyday.
>
> — **Laura Poitras**, Oscar winning filmmaker and journalist

Signal application

There are minimal traffic data logged.

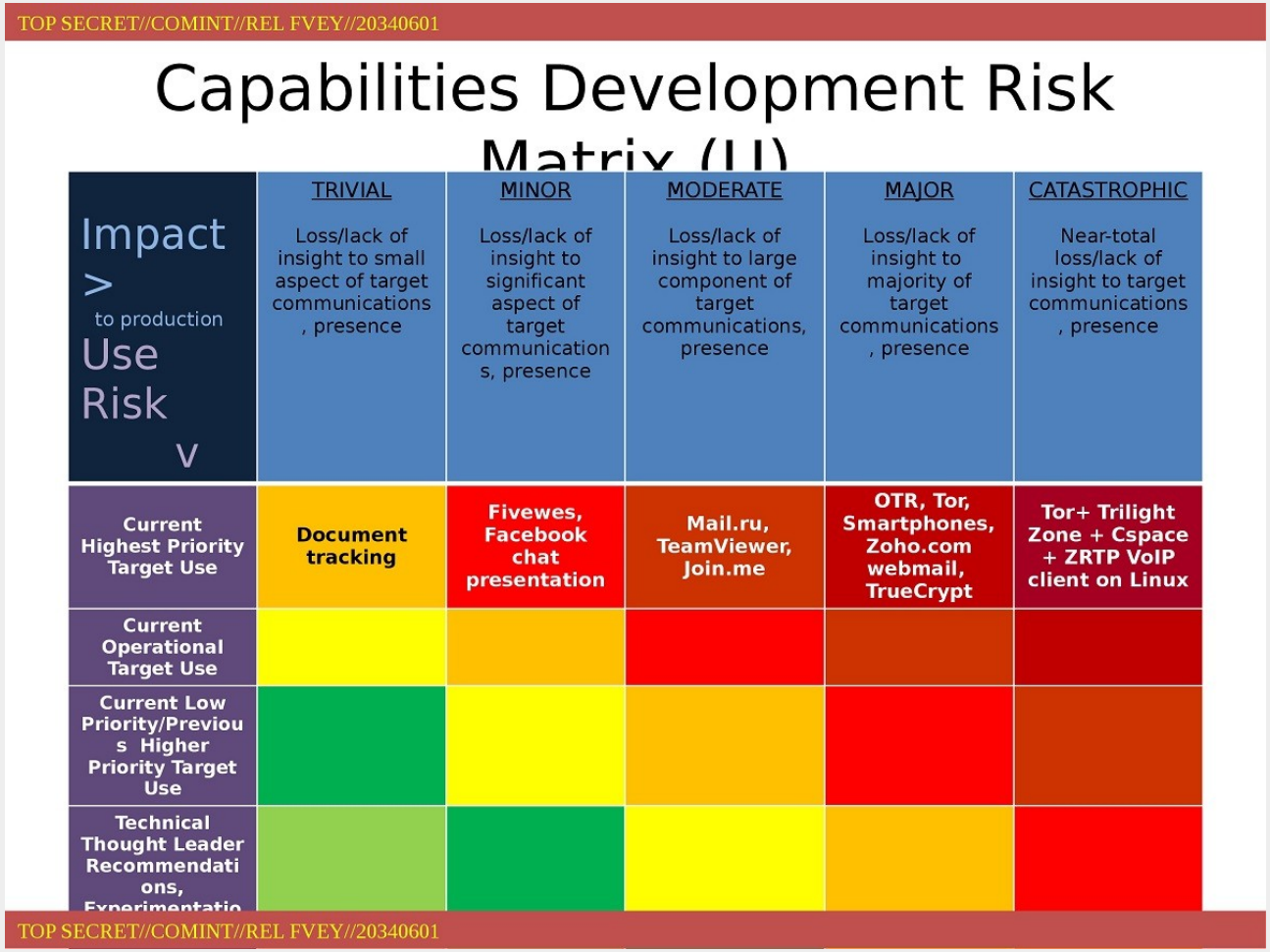
Attachment A

Account	Information
[redacted]	N/A
[redacted]	Last connection date: [redacted] Unix millis Account created: [redacted] Unix millis

Signal could be further anonymized:

- by registering "unrelated phone number",
- by using over Tor network,
- developers are building censorship circumvention into it.

Even NSA is »recommending« it! :-)



TOP SECRET//COMINT//REL FVEY//20340601

Capabilities Development Risk Matrix (U)

Impact > to production Use Risk v	TRIVIAL Loss/lack of insight to small aspect of target communications, presence	MINOR Loss/lack of insight to significant aspect of target communications, presence	MODERATE Loss/lack of insight to large component of target communications, presence	MAJOR Loss/lack of insight to majority of target communications, presence	CATASTROPHIC Near-total loss/lack of insight to target communications, presence
Current Highest Priority Target Use	Document tracking	Fivewes, Facebook chat presentation	Mail.ru, TeamViewer, Join.me	OTR, Tor, Smartphones, Zoho.com webmail, TrueCrypt	Tor+ Trilight Zone + Cspace + ZRTP VoIP client on Linux
Current Operational Target Use					
Current Low Priority/Previous Higher Priority Target Use					
Technical Thought Leader Recommendations, Experimentatio					

TOP SECRET//COMINT//REL FVEY//20340601

Things become "catastrophic" for the NSA at level five - when, for example, a subject uses a combination of Tor, another anonymization service, the instant messaging system CSpace and a system for Internet telephony (voice over IP) called ZRTP. This type of combination results in a "near-total loss/lack of insight to target communications, presence," the NSA document states. (Der Spiegel)

Signal protocol

Open Whisper Systems developed cryptographic protocol Signal in 2013.

Currently the protocol is being implemented in:

- Facebook Messenger (July 2015) – monthly about a billion of users,
- WhatsApp (April 2016) – more than a billion of registered users,
- Google Alo (September 2016) – since October 2016 Google Alo is default messenger on Pixel mobile phones,
- Viber (May 2015) – partly implemented – it has more than 100 million of monthly active users.

Towards anonymity

Using of anonymisation network increases latency. So no real time communication is possible!

However, Signal supports voice messages, which can be sent over Tor network.

In group chat they can be used as fully anonymous push-to-talk system.

There are also being developed solutions which enable strong anoymity and solutions which does not need central infrastructure. Examples:

- **Ring** is VoIP client which supports decentralized communication, anoymous identities and peer-to-peer discovery and connection.
- **Briar** is peer-to-peer encrypted messaging and forums application, does not require internet access and does not use cloud.

Conclusion

Information security and encryption of communications is becoming widely adopted in last years.

Use of strong encryption is becoming simplified.

Average user does not need to be proactive to get security (and security updates) – security is becoming a norm.

Companies are paying attention to implementing security features, security testing, etc.

Legislation requires implementation of security practices.

Yes, there are still some problems, especially on a hardware level. But problems are being discussed and solutions sought.

Eavesdropping is becoming harder and more expensive.

Anoymity: how to reveal your real target???

Questions?

https://pravokator.si