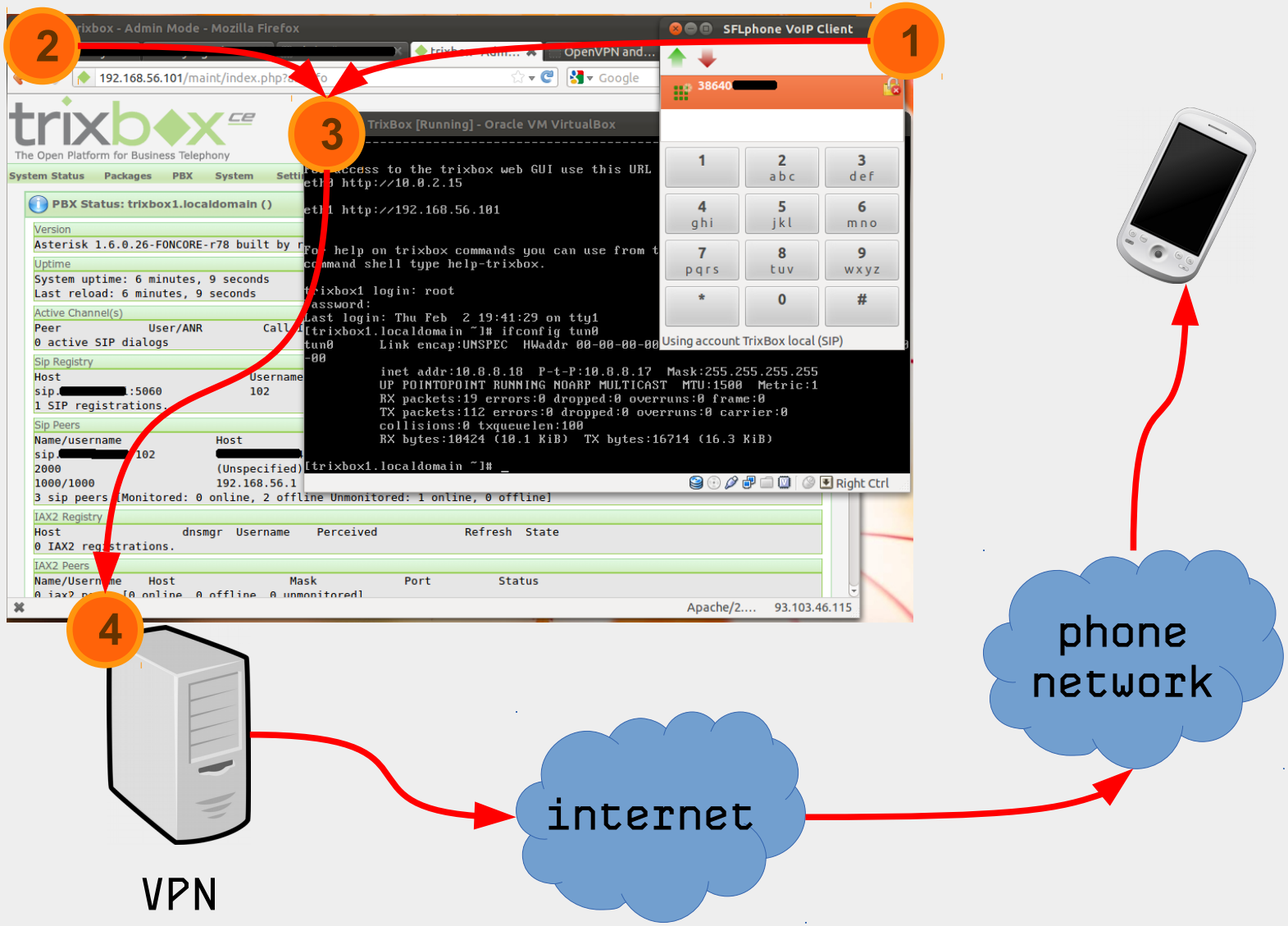
Mobile communications security

Matej Kovačič, (CC) 2017

Jozef Stefan Institute

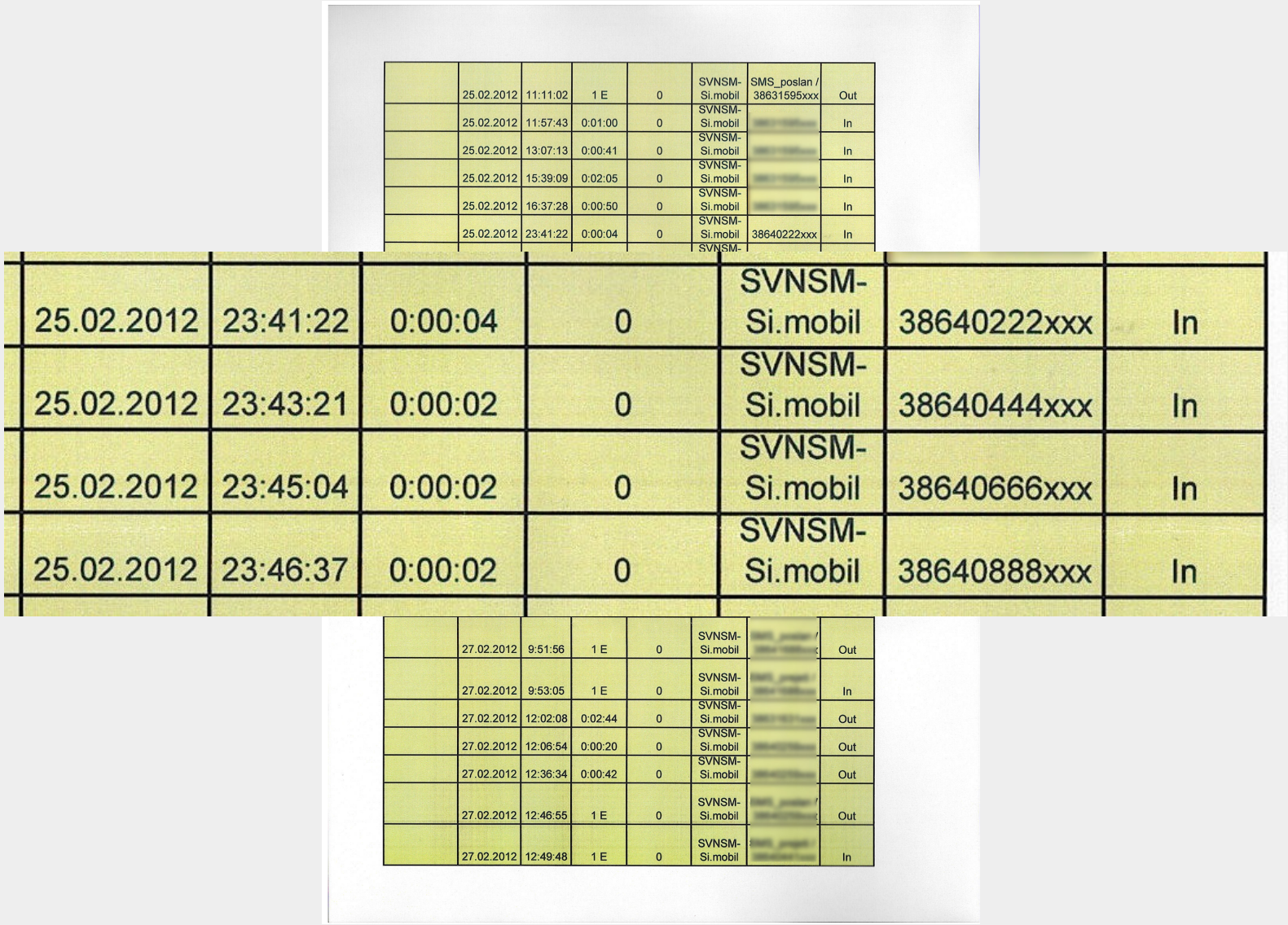
Part I:
Identity spoofing

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

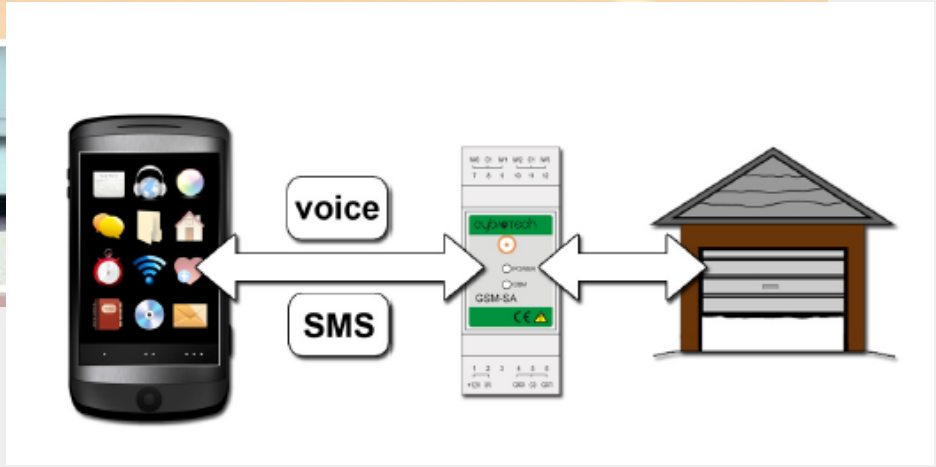
We offer a useful device with a simple phone call opens or closes the automated garage or front door.

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:

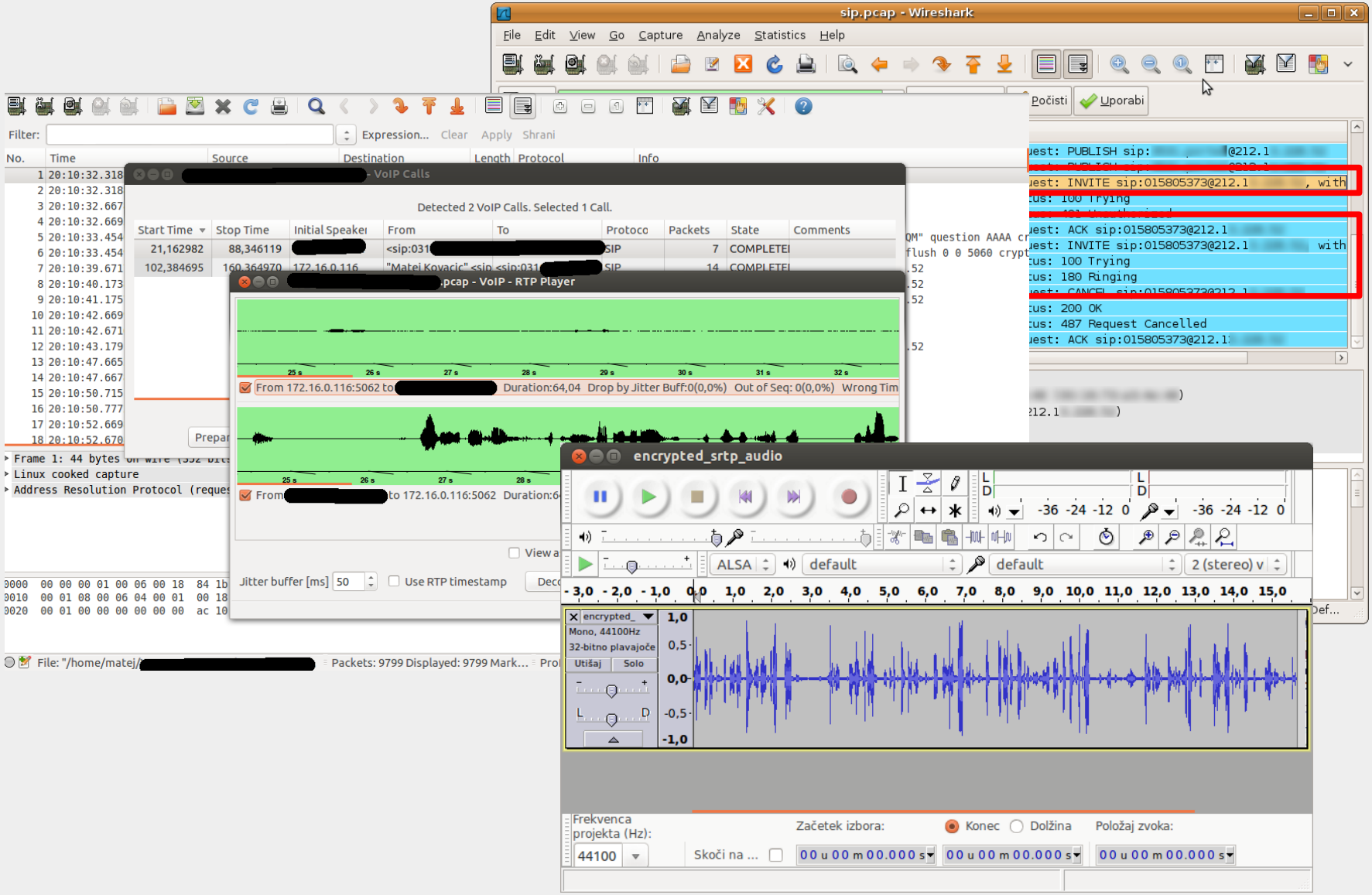
- delivery of a package with instructions for use,
- mounting points agreed upon (please call us and we will send you the offer).

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



Part II: Intercepting (VoIP) communications

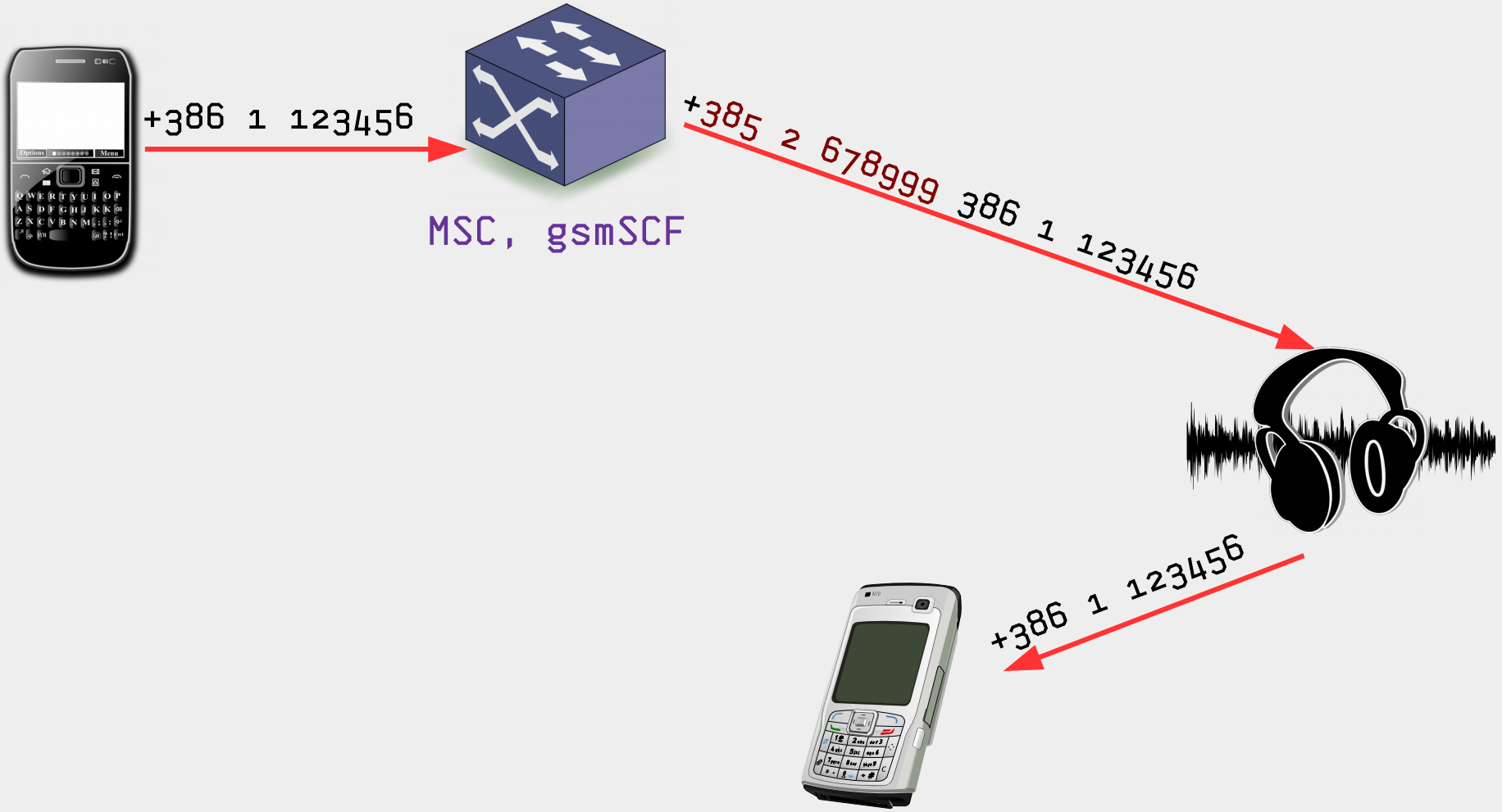
Unencrypted vs. encrypted phone call



Part III:
Rerouting outgoing calls

Example: intercepting outgoing calls

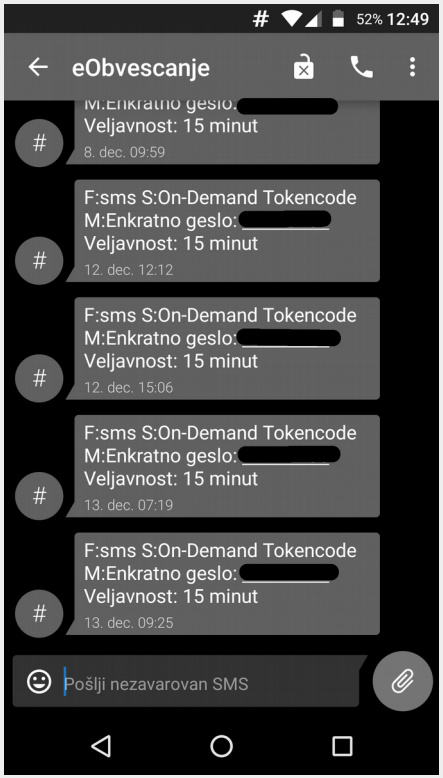
SS7 attacks.



Part IV: Rerouting incoming calls/SMS messages

Example: intercepting incoming calls

An attacker pretends that a subscriber is roaming in his network... From this point on, all calls and SMS messages for that subscriber are routed to the attacker.



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

How to obtain SS7 access?

Posing as a potential customer, this reporter registered an email domain—“smsrouter.co”— and, acting as a new text-message routing service, approached a division of a large-scale, legitimate telecommunications provider in Western Europe.

After exchanging emails over a weeklong period (and specifying the fake company would need coverage in Europe), the telco provided a quote: a one-time setup fee of around $2,650, with 50 percent paid upfront and the rest with the first invoice after testing, and then a $6,600 monthly rental fee for a so-called global title (GT)—a designated address for routing messages. The telco also offered to connect The Daily Beast’s imaginary company over a SIGTRAN link.

-- https://www.thedailybeast.com/you-can-spy-like-the-nsa-for-a-few-thousand-bucks

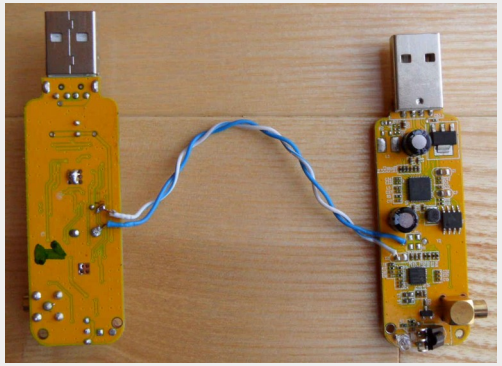
Part V:
GSM Interception

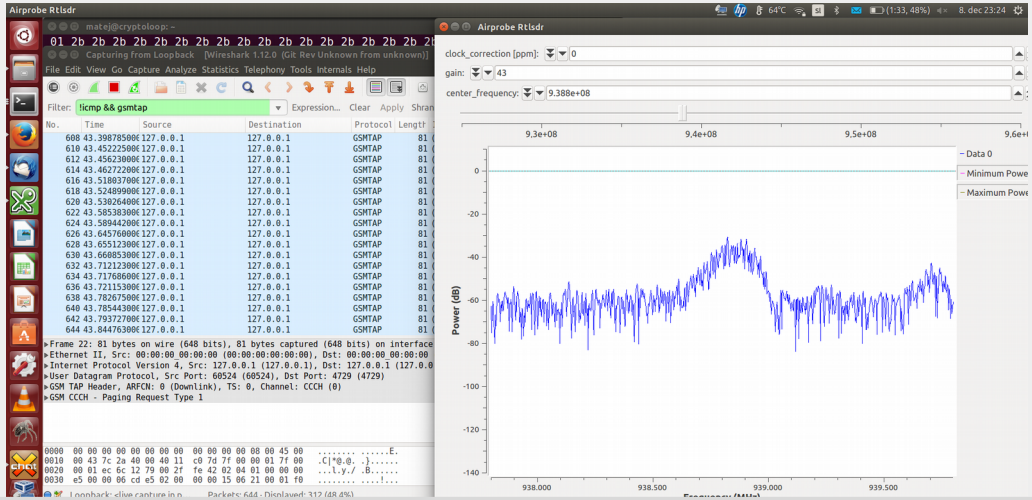
gr-gsm

Toolset for capture and analysis of GSM signals.

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

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





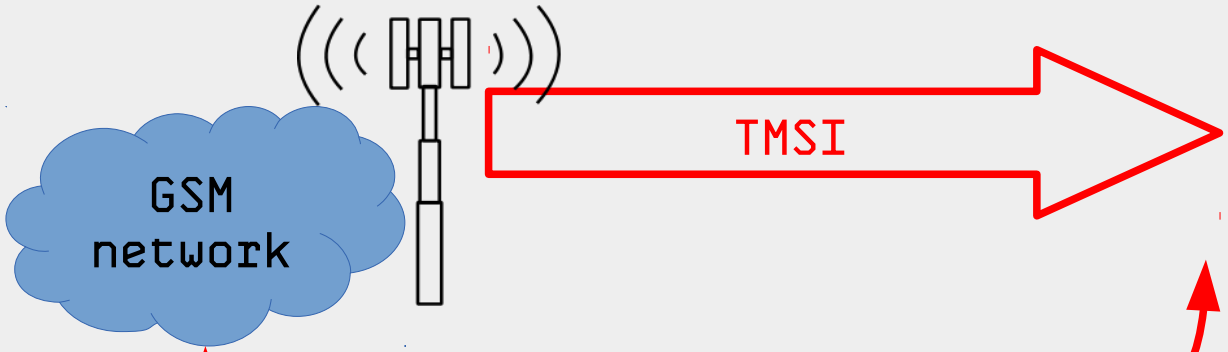

```
grgsm_scanner -p 35
```

```
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
```

Osmocom/gr-gsm

Typical (passive) attack setup...

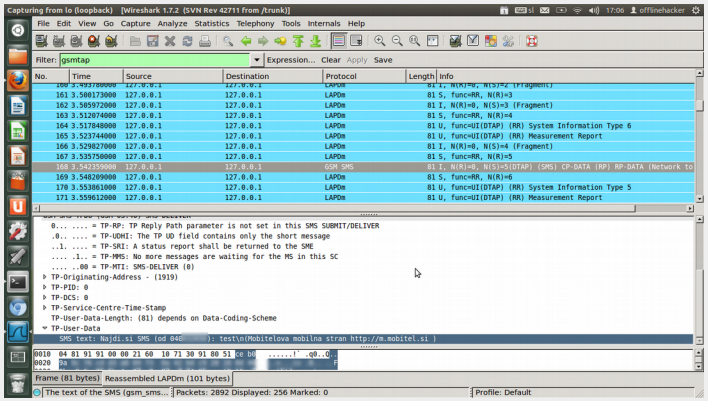


Mobile phone user does not detect reception of silent SMS.

silent
SMS

Osmocom

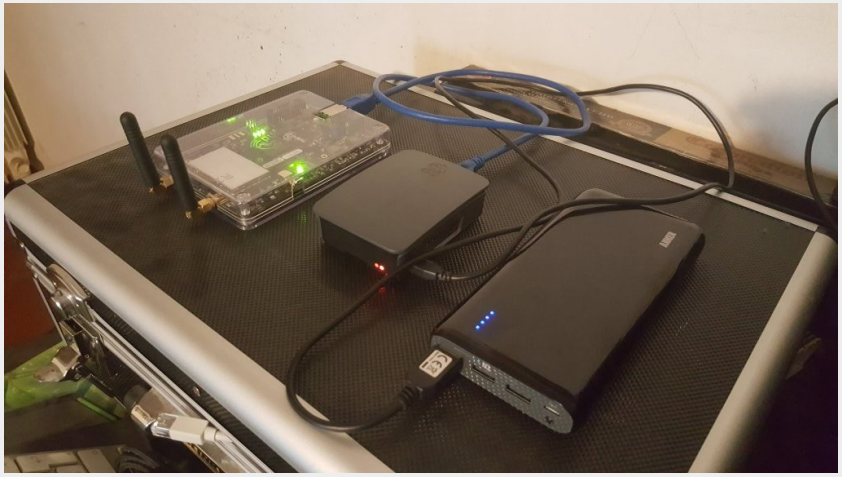
Attacker is intercepting wireless communications and performs cryptanalysis...

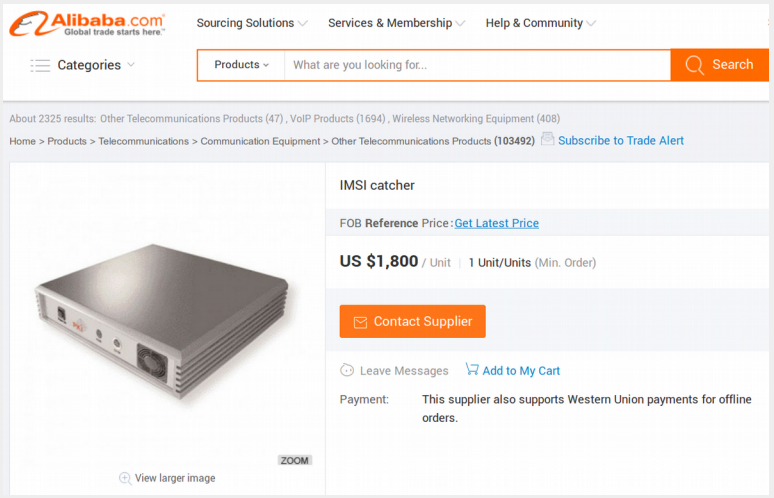


Part VI:
IMSI Catchers

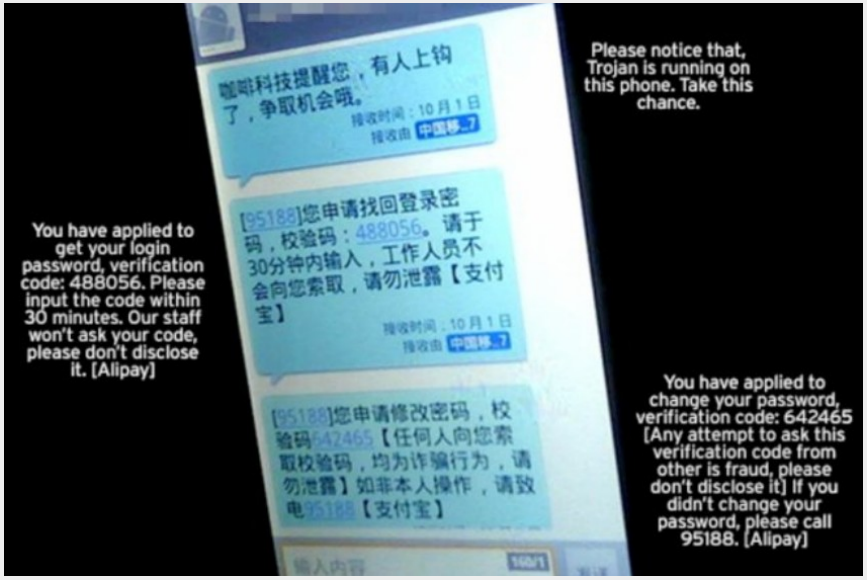
IMSI Catchers

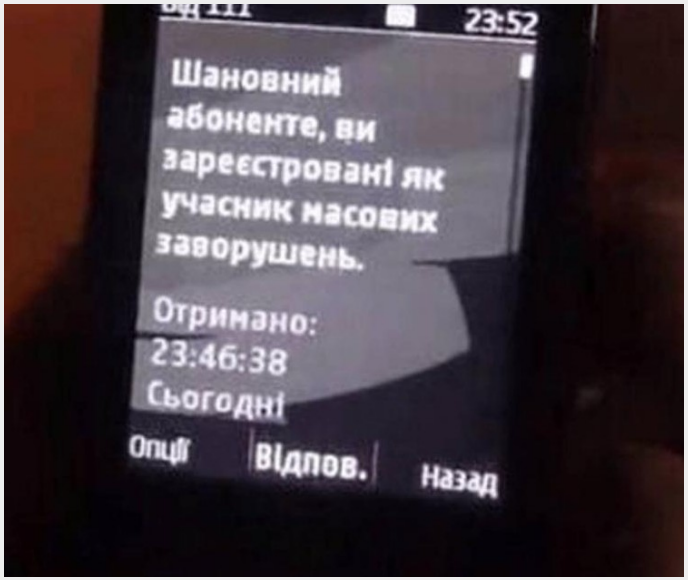
Basically, they are fake base stations…

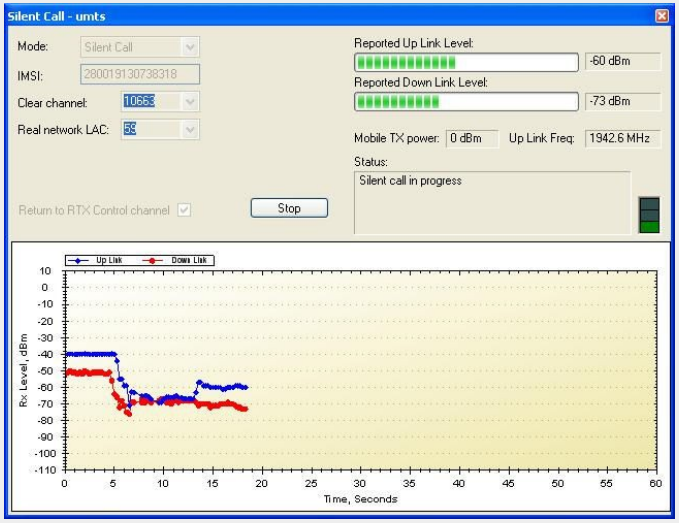




IMSI Catchers







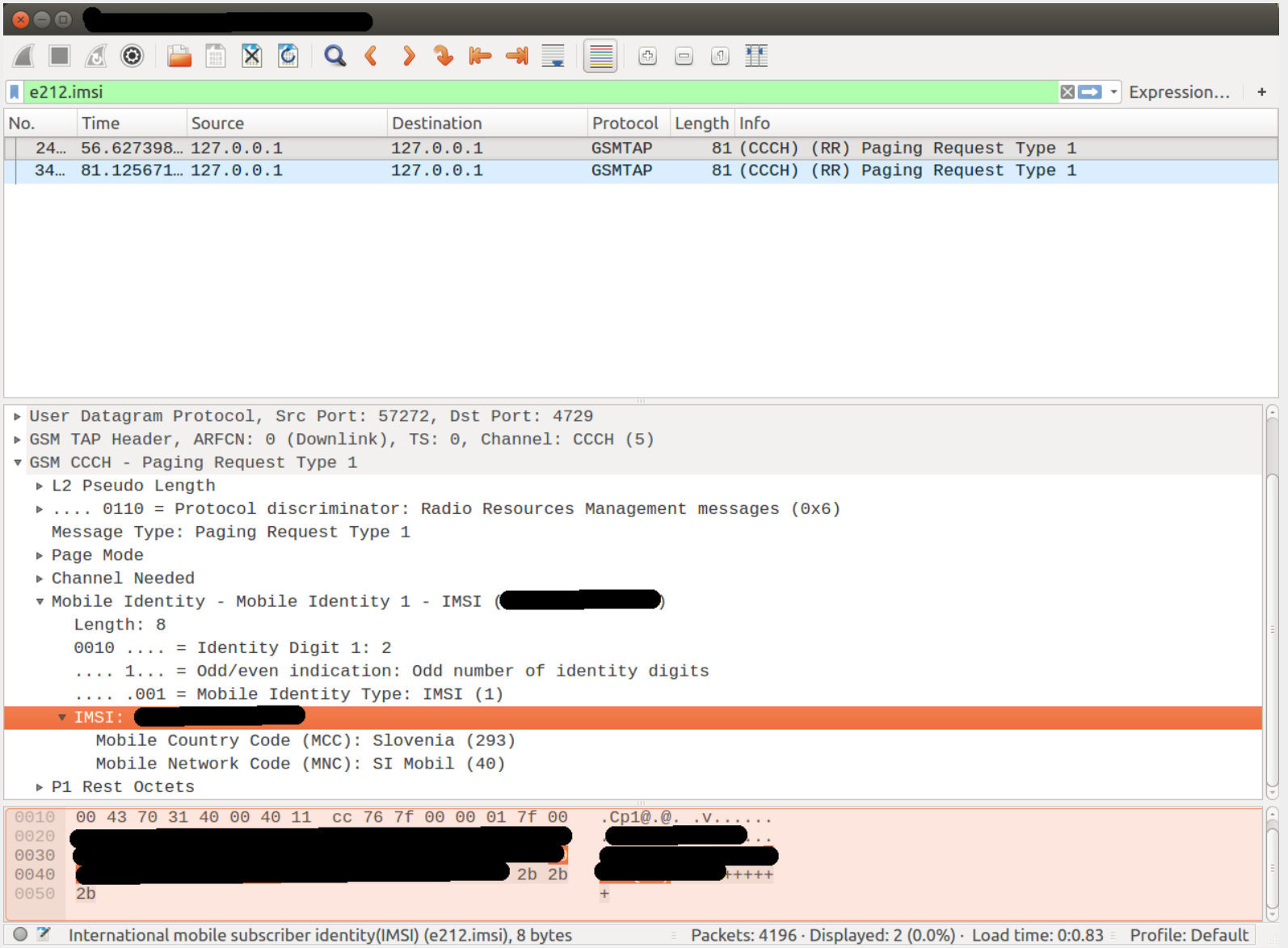
UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- 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

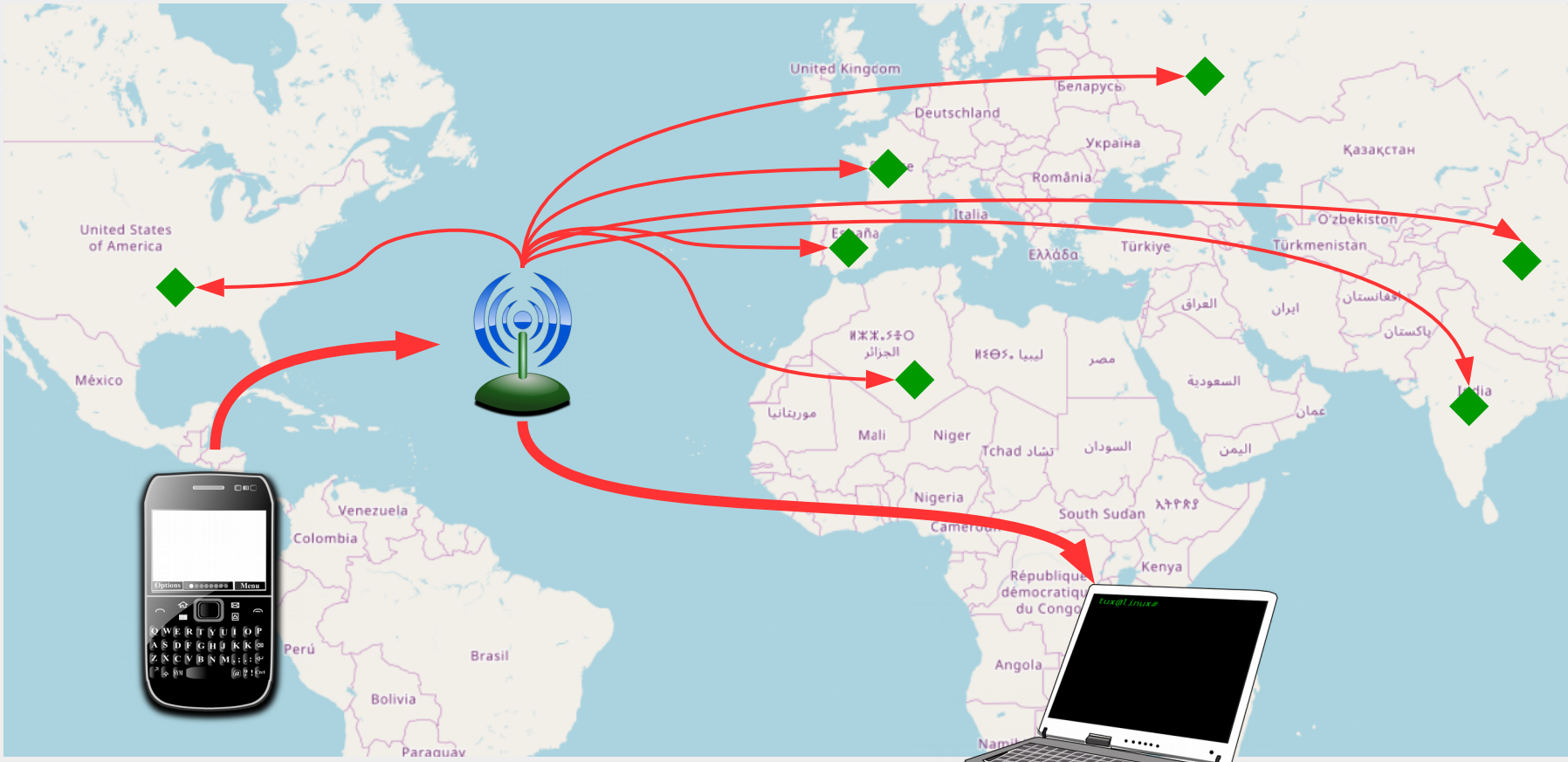
IMSI Catcher (*when it is caught :-)*)



Part VII:
Mobile Phone Infection
(via “classical” malware or via baseband attack)

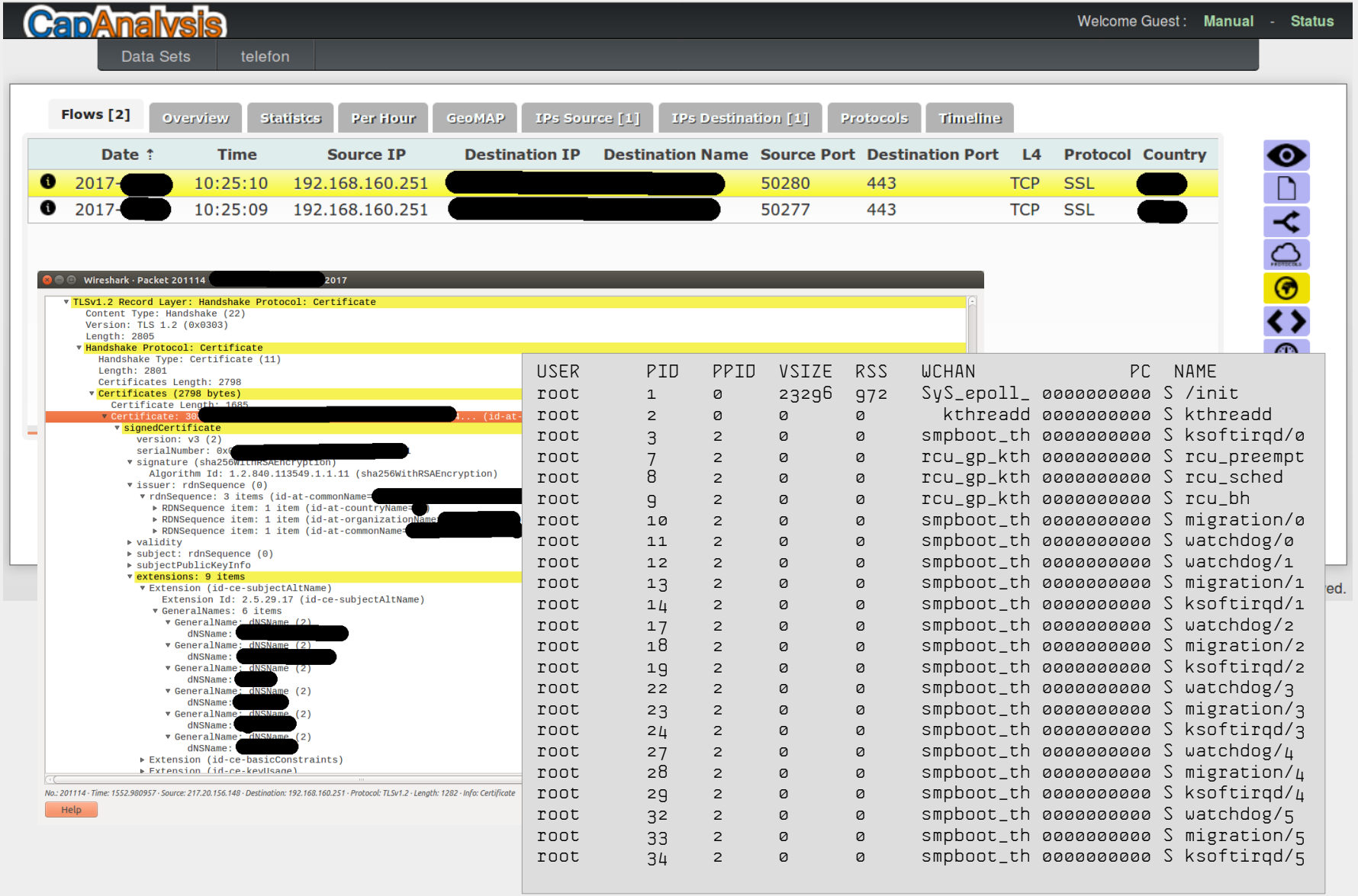
Real Case (Netflow Analysis)

First we intercept mobile phone network connections and collect IP network traffic.



Then we analyse netflow data.

Real Case (Netflow Analysis)



Questions?

Matej Kovačič
matej.kovacic@ijs.si

https://telefoncek.si