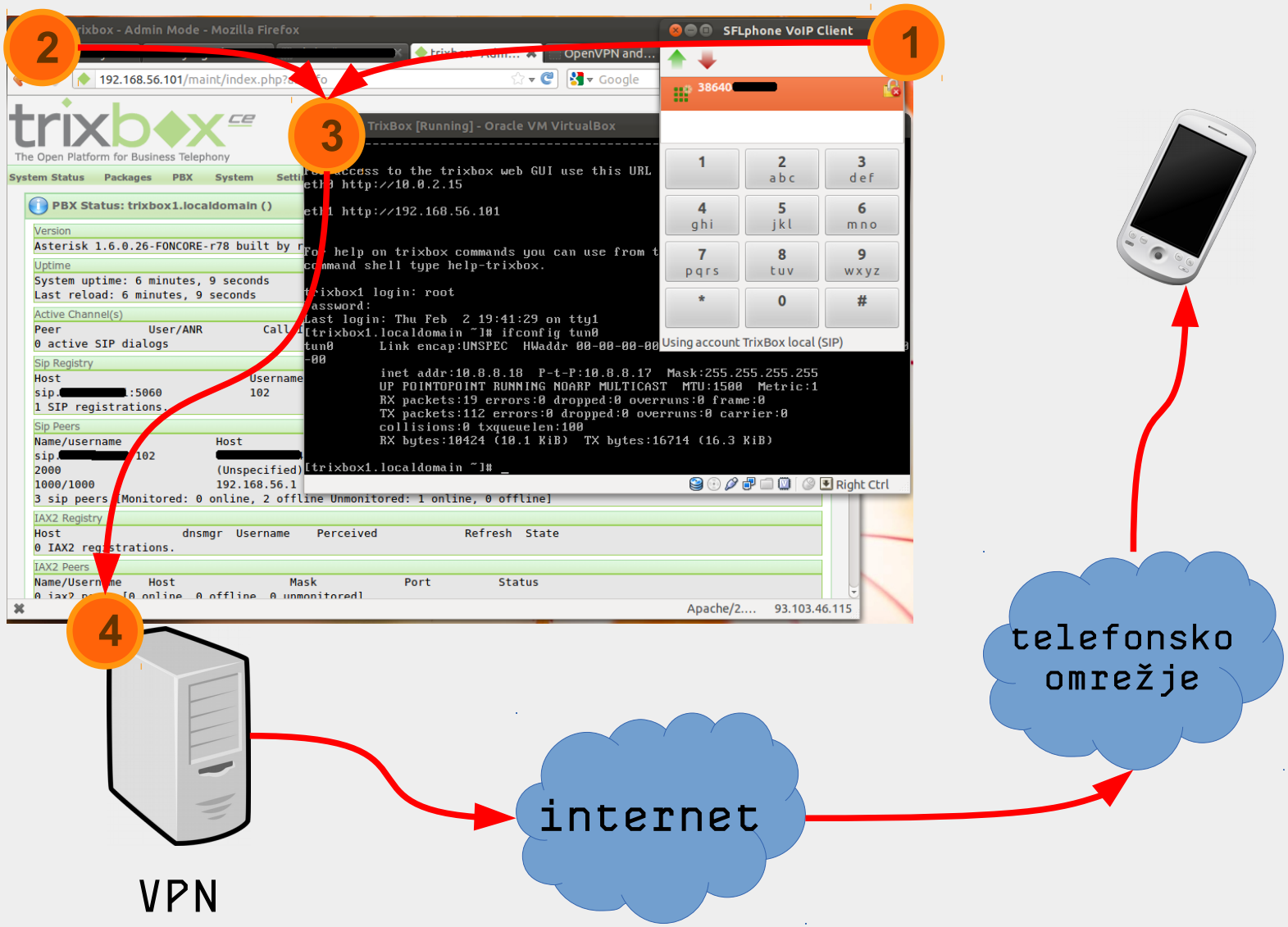
Kako zasebno komunicirati s pametnimi telefoni?

Matej Kovačič
https://pravokator.si

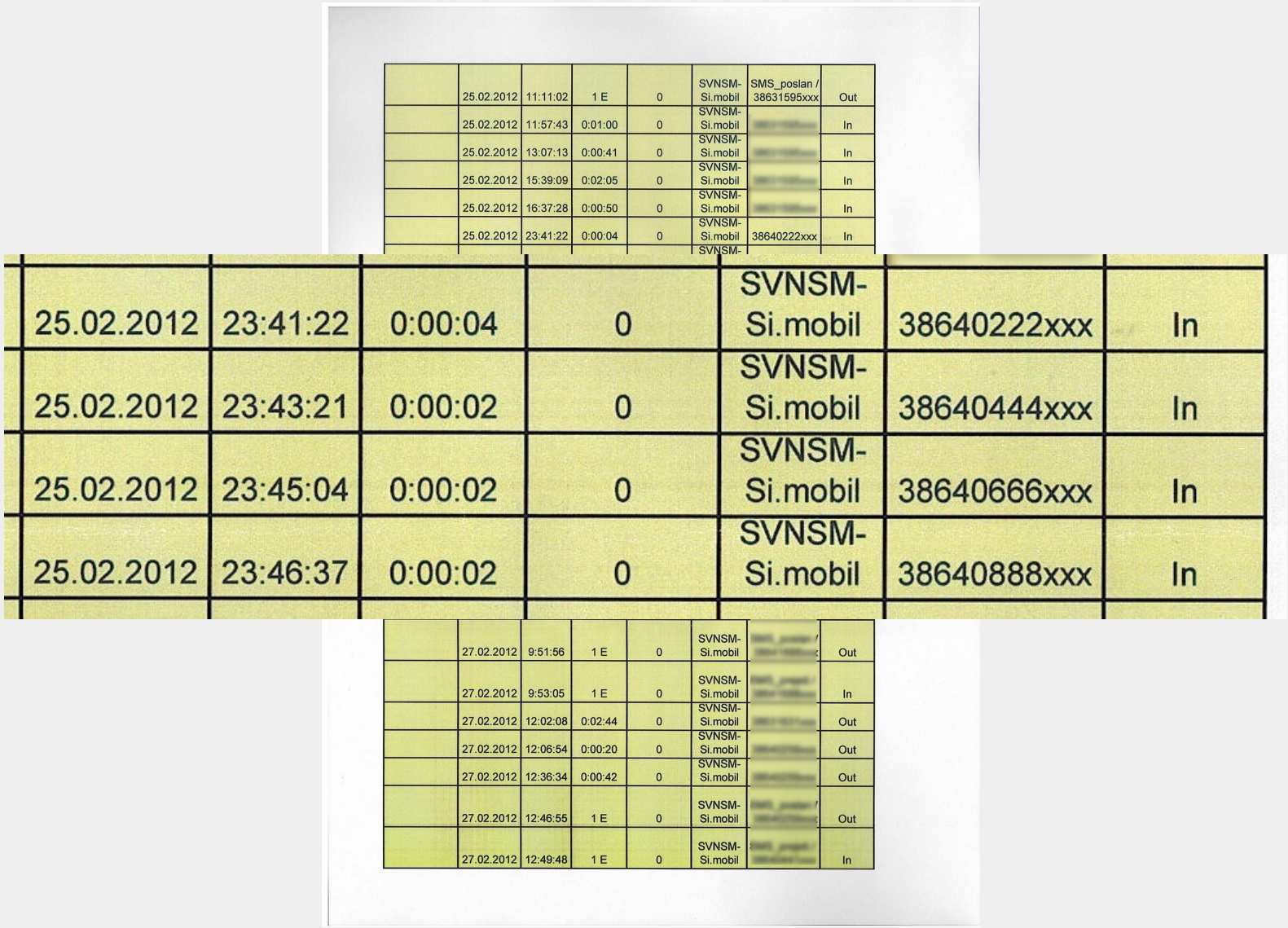
Nekaj težav
z obstoječo
tehnologijo...

Problem avtentikacije



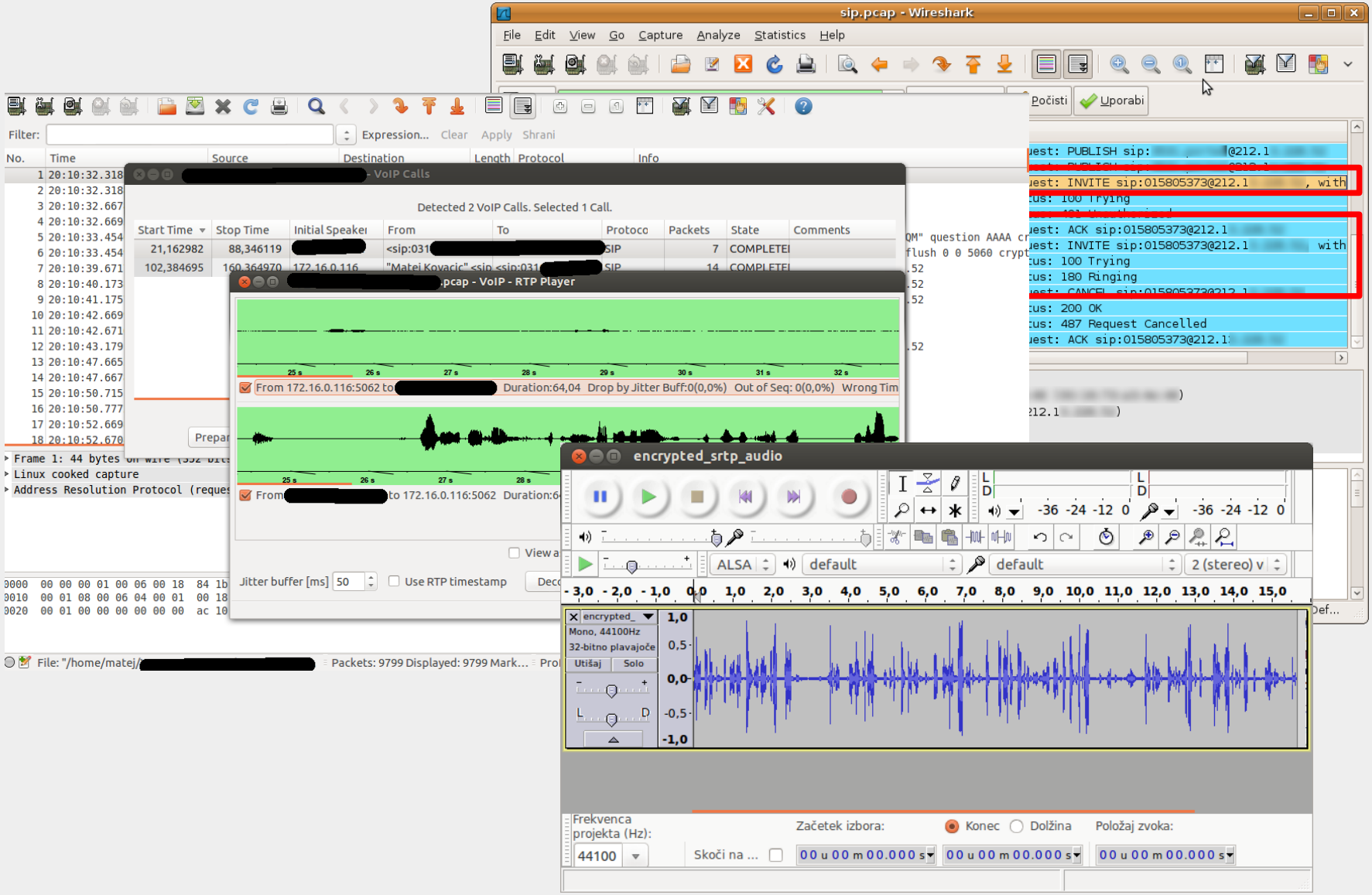
Problem avtentikacije

Problem avtentikacije



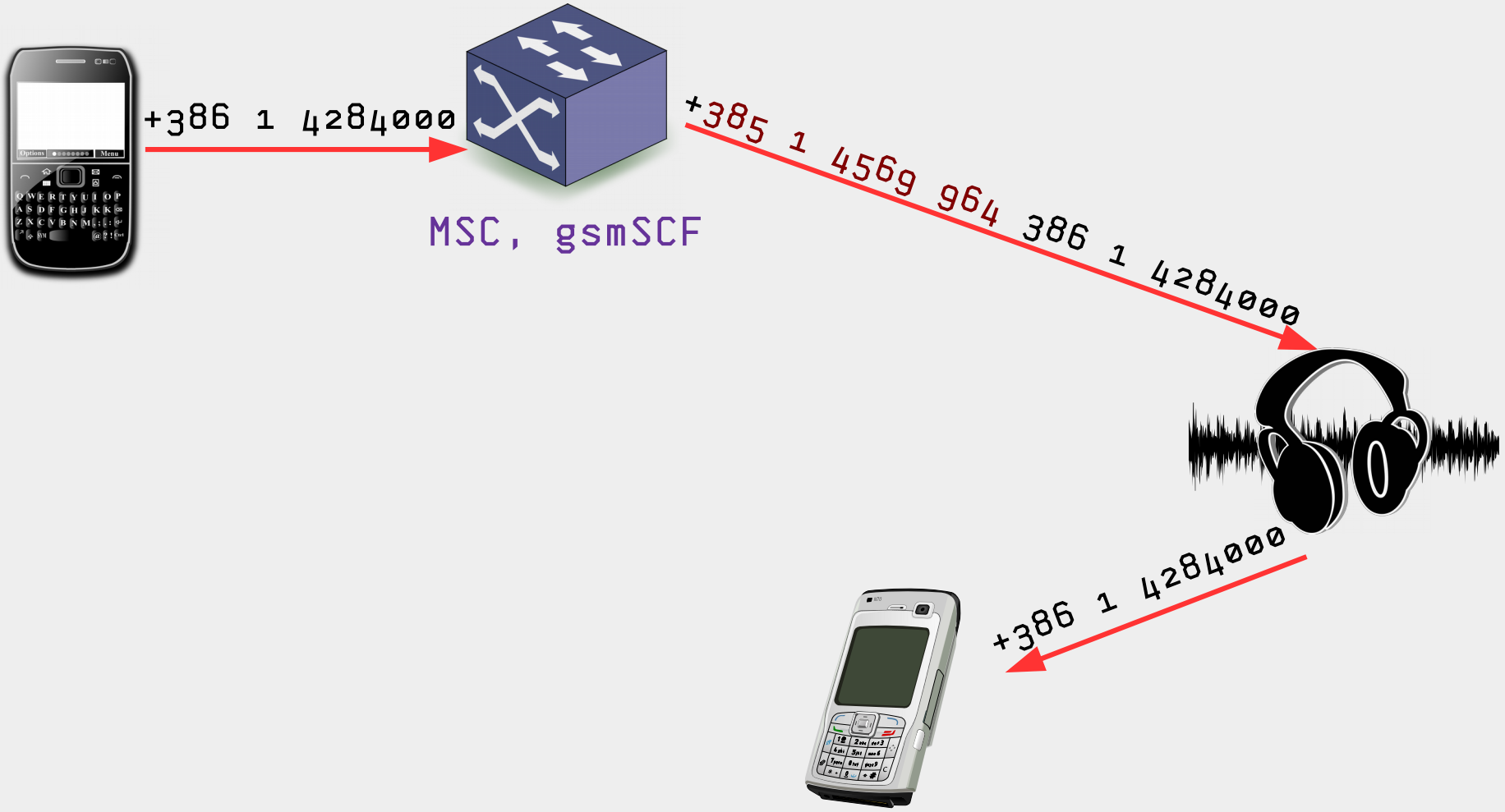
	25.02.2012	11:11:02	1 E	0	SVNSM-Si.mobil	SMS_poslan / 38631595xxx	Out
	25.02.2012	11:57:43	0:01:00	0	SVNSM-Si.mobil		In
	25.02.2012	13:07:13	0:00:41	0	SVNSM-Si.mobil		In
	25.02.2012	15:39:09	0:02:05	0	SVNSM-Si.mobil		In
	25.02.2012	16:37:28	0:00:50	0	SVNSM-Si.mobil		In
	25.02.2012	23:41:22	0:00:04	0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

Problem prestrezanja



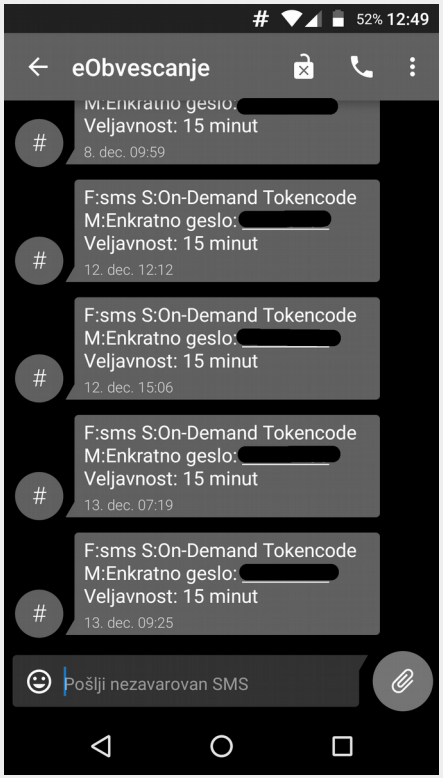
Problem preusmerjanja

...



Problem preusmerjanja

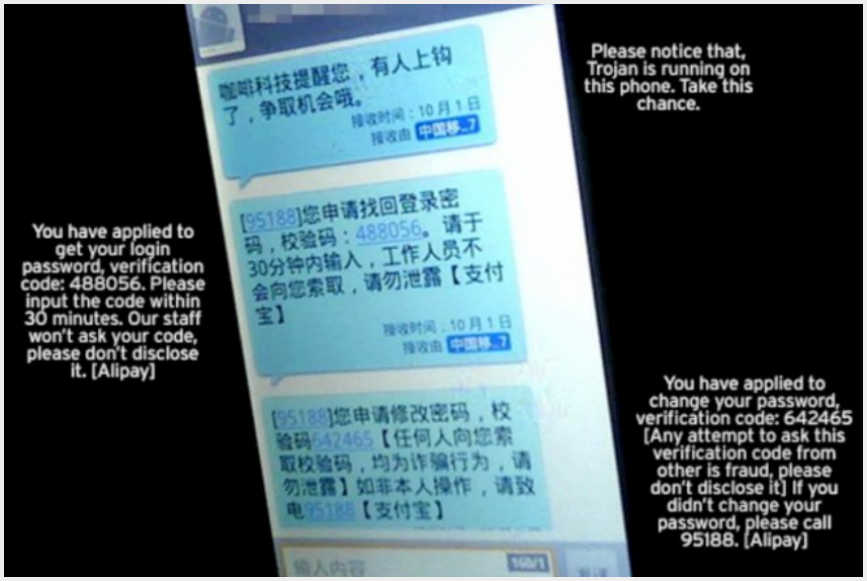
Napadalec se pretvarja, da uporabnik gostuje v njegovem omrežju. S tem doseže, da so dohodni klici in SMS sporočila preusmerjeni k napadalcu.

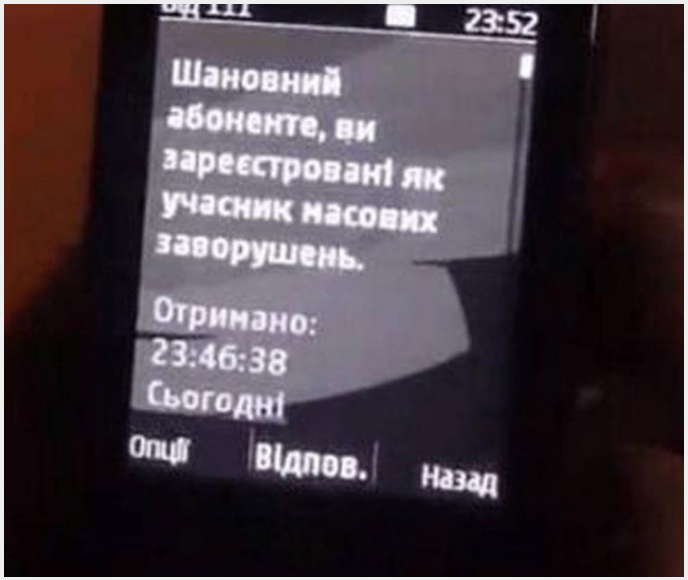


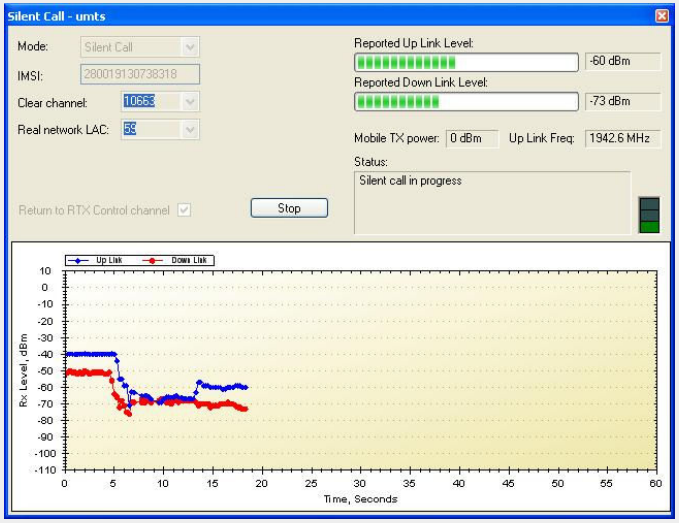
Zdaj se napadalec prijavi v žrtvino spletno banko in ker žrtev uporablja 2FA, banka po SMS-u pošlje mTAN dostopno kodo...

Ali pa se napadalec skuša prijaviti v službeno omrežje... :-)

Lovilci IMSI številk







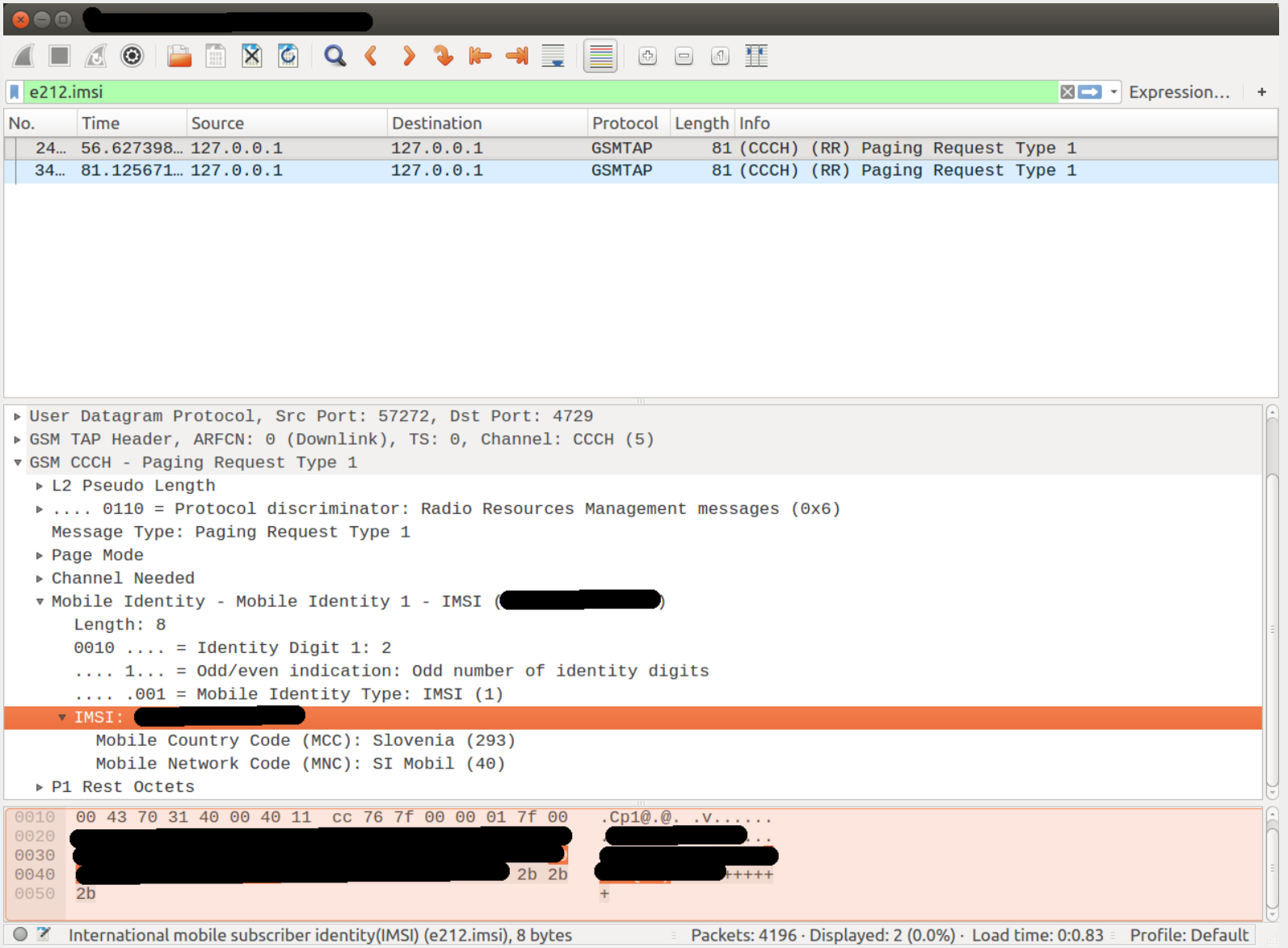
UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- 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, 280 DRAKE AVENUE, NEW

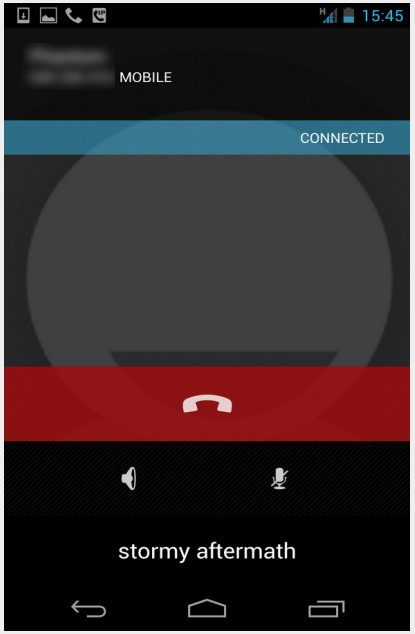
APPLICATION FOR AN ORDER AUTHORIZING THE INTERCEPTION OF ORAL COMMUNICATIONS

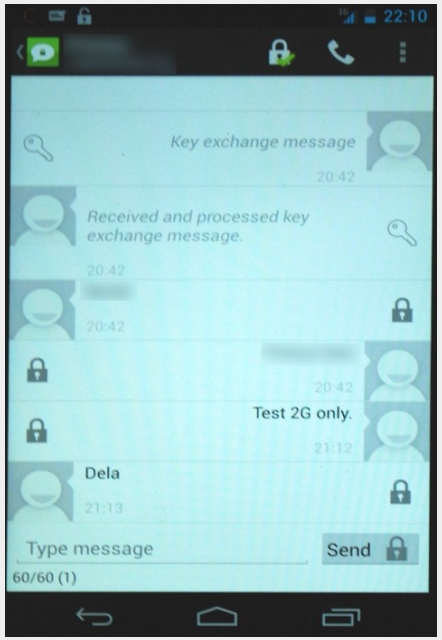
Lovilci IMSI številk

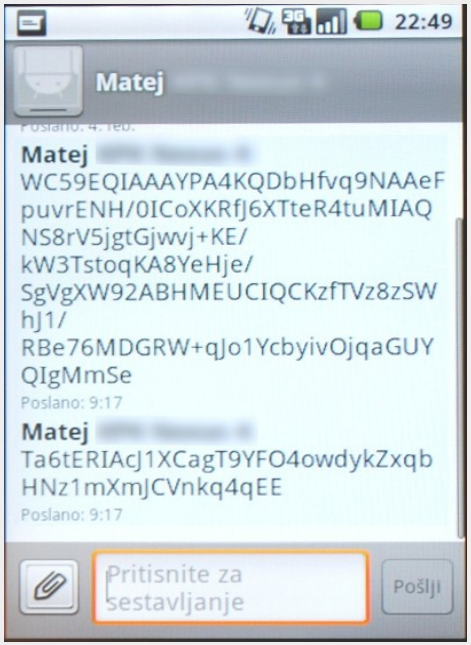


In nekaj rešitev.

Šifriranje, šifriranje, šifriranje







Prenos podatkov ter šifriranje na aplikacijskem nivoju!

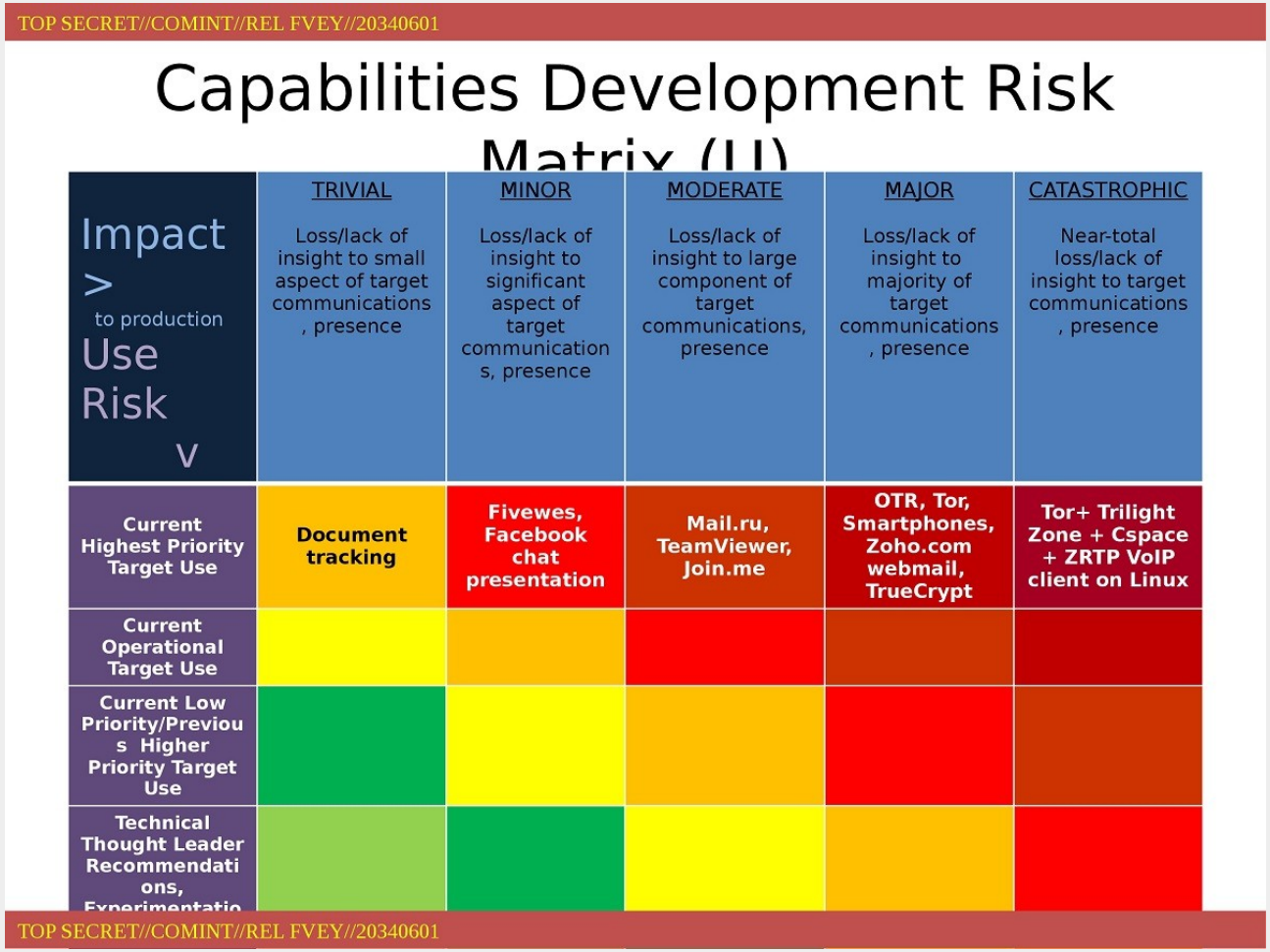
Prometni podatki, anonimizacija

Attachment A

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

Zaobid cenzure, anonimizacija?

Šifriranje "priporoča" tudi NSA



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)

Vprašanja?