

# Slepo zaupanje digitalnim dokazom?

## Primer mobilne telefonije

**Matej Kovačič**

**(CC) 2012**

Delo je izdano pod Creative Commons licenco: "Priznanje avtorstva-Nekomercialno-Deljenje pod enakimi pogoji 2.5 Slovenija". Celotno pravno besedilo licence je dostopno na spletni strani: <http://creativecommons.org/licenses/by-nc-ša/2.5/si/legalcode>, ali na poštnem naslovu: Inštitut za intelektualno lastnino, Čufarjeva ulica 17, 1000 Ljubljana.

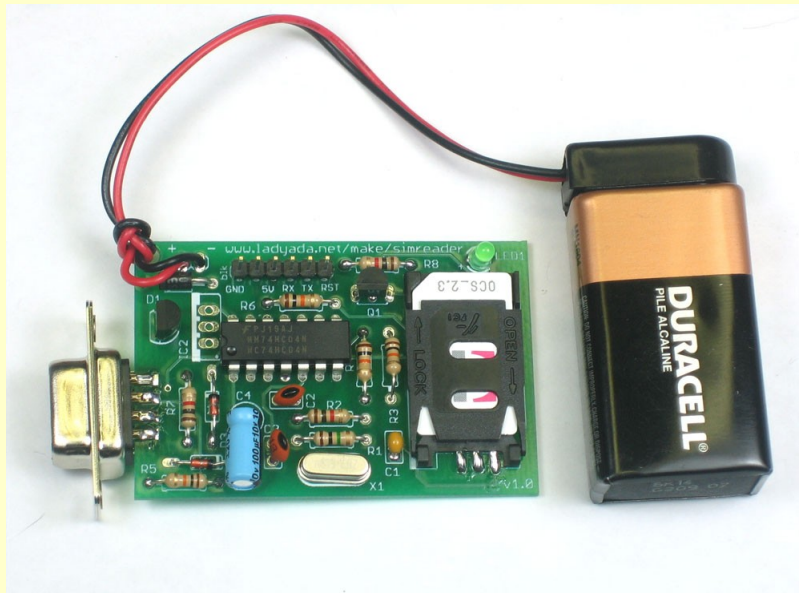
Slike: (CC) OpenClipArt.org, Matej Kovačič (osebni arhiv) in navedeni avtorji (C).

# Zaupanje v računalniško generirane dokaze?

- Sergey Bratus, Ashlyn Lembree in Anna Shubina. 2010. Software on the Witness Stand: What Should It Take for Us to Trust It?
- Na sodiščih se danes že rutinsko uporabljajo prometni podatki, ki jih beležijo ponudniki dostopa do interneta ter različni strežniki in druge omrežne naprave, podatki iz mobilnih telefonov, podatki iz digitalnih nadzornih videokamer, itd. Tudi pri digitalni forenziki digitalne dokaze išče in analizira različna programska oprema, saj je podatkov pogosto preveč, da bi jih lahko ročno, brez pomoči programov pregledal posamezni preiskovalec.
- Težava: sodišča digitalne dokaze, zlasti računalniško generirane digitalne dokaze praviloma dojemajo kot zaupanja vredne same po sebi (avtorji uporabljajo izraz *inherently trustworthy evidence*).
- Na sodišču ima obramba pravico so soočanja s tožniki in (navzkrižnega) zaslišanja prič. A kaj storiti, če je »priča« računalnik oz. programska oprema?

# Primer 1: podatki iz SIM kartice

## 1: čitalec SIM kartic



# Primer 1: podatki iz SIM kartice

## 2: spreminjanje vsebine in metapodatkov SMS sporočil na SIM kartici

SMS edit

Message Text (44 / 160)

Septembra 2001 bo teroristicni napad na W TC.

Date: Fri Jan 12 1  
From: 640 [REDACTED]  
Status: Deleted

Save Prekliči

(2/35) sms messages

Status	Date	From	Message
Read	Wed Oct 15 16:04:57 2014	123456	Sporocilo iz prihodnosti...
Read	Fri Jan 12 18:54:37 2001	+38640 [REDACTED]	Septembra 2001 bo teroristicni napad na WTC.

SMS\_export.txt (~/.Namizje/SIMreader) - gedit

```
# Date, From, ServiceCenter, Message
Wed Oct 15 16:04:57 2014,123456,+38641001333,Sporocilo iz prihodnosti...
Fri Jan 12 18:54:37 2001,+38640 [REDACTED],+38641001333,Septembra 2001 bo teroristicni napad na WTC.
```

Običajno besedilo | Širina tabulatorja: 8 | Vr. 2, St. 70 | VST

SIM Information

Location: 293F40  
MSISDN: 000000486  
Serial number: 89386400707  
IMSI number: 2934001135  
SIM phase: Phase 2+

	Activated	Tries left
PIN1	Yes	3
PIN2	Yes	3

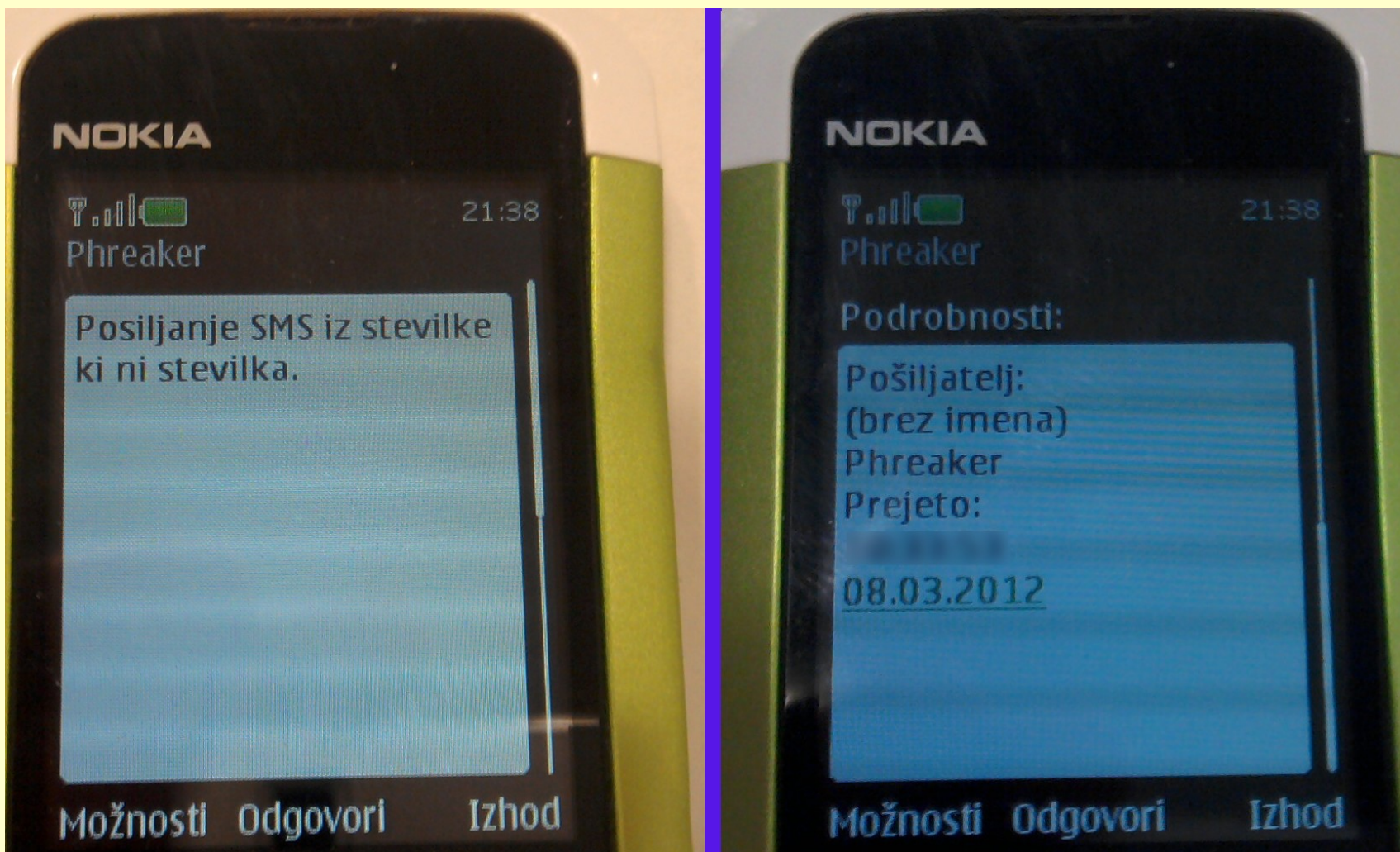


# Primer 1: podatki iz SIM kartice

3: rezultat



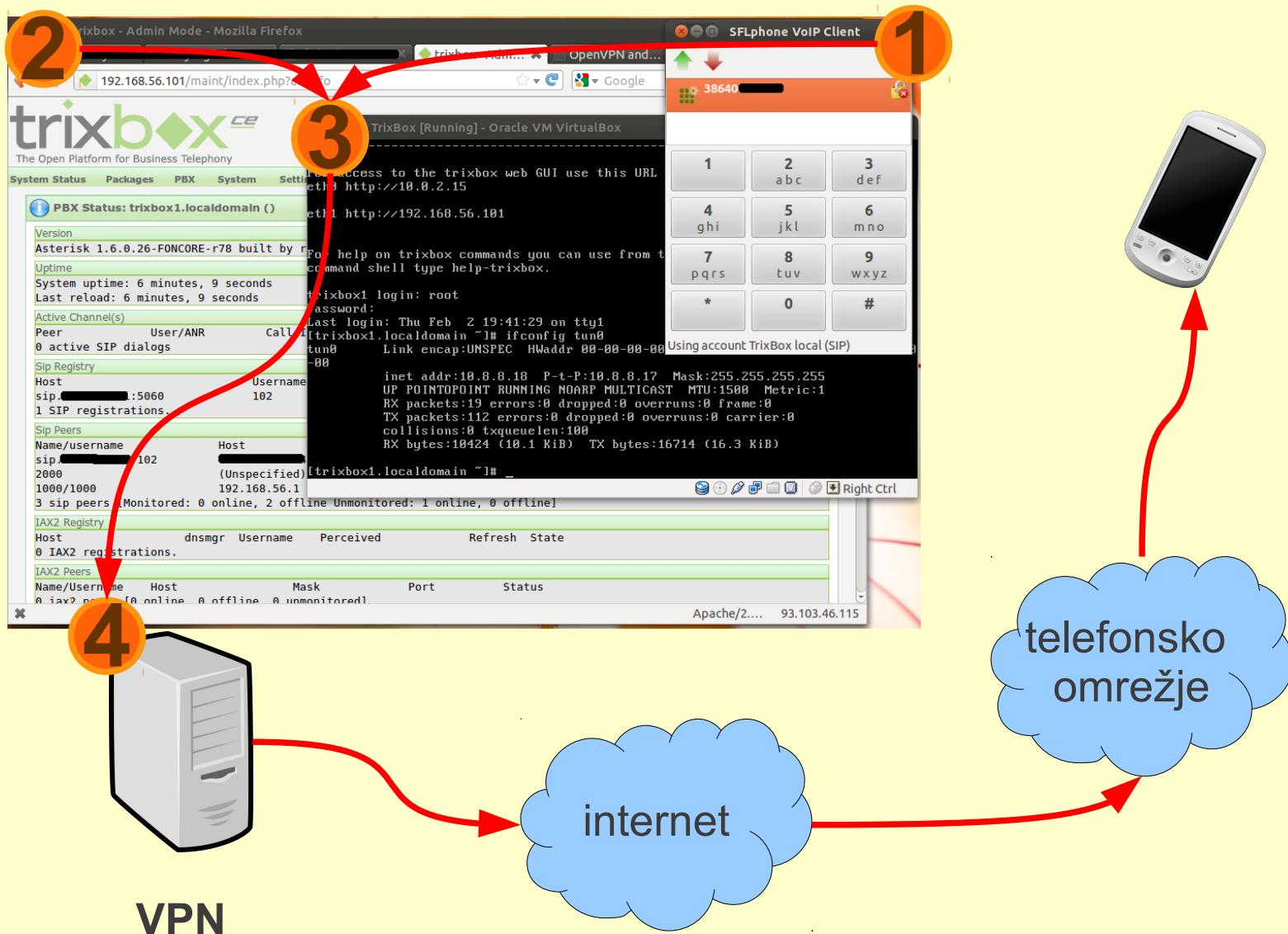
## Primer 2: pošiljanje SMS sporočil "iz" poljubne številke





# Primer 3: klicanje s poljubno klicno identifikacijo

## 1: vzpostavitev infrastrukture



# Primer 3: klicanje s poljubno klicno identifikacijo

## 2: pogled v virtualno telefonsko centralo

The image shows two overlapping browser windows displaying the Trixbox Admin Mode interface. The left window shows the 'PBX Status' page, and the right window shows the 'Extension: 1000' configuration page.

**trixbox - Admin Mode - Mozilla Firefox**  
trixbox - Admin Mode  
192.168.56.101/maint/index.php?astInfo

**PBX Status: trixbox1.localdomain ()**

Version  
Asterisk 1.6.0.26-FONCORE-r78 built by root @ revision

Uptime  
System uptime: 7 hours, 5 minutes, 43 seconds  
Last reload: 1 hour, 10 minutes, 54 seconds

Active Channel(s)  
Peer User/ANR Call ID F  
0 active SIP dialogs

Sip Registry  
Host Username Refres  
0 SIP registrations.

Sip Peers  
Name/username Host Dyn Nat A  
2000 (Unspecified) D N  
1000/1000 192.168.56.1 D N  
2 sip peers [Monitored: 1 online, 1 offline Unmonitored]

IAX2 Registry  
Host dnsmgr Username Perceived  
0 IAX2 registrations.

IAX2 Peers  
Name/Username Host Mask  
(S) 255.255.255.255  
1 iax2 peers [1 online, 0 offline, 0 unmonitored]

trixbox - Admin Mode - Mozilla Firefox  
trixbox - Admin Mode  
192.168.56.101/maint/index.php?freepbx

System Status Packages PBX System Settings Help  
Admin Reports Panel Recordings Help

Setup Tools  
Admin  
System Status  
Module Admin  
Basic  
Extensions  
Feature Codes  
General Settings  
Outbound Routes  
Support  
Trunks  
Administrators  
Inbound Call Control  
Inbound Routes  
Zap Channel DIDs  
Announcements  
Blacklist  
CallerID Lookup Sources  
Day/Night Control  
Follow Me

Extension: 1000  
Delete Extension 1000  
Add Follow Me Settings  
Add Extension  
Matej 1 <1000>  
Matej 2 <2000>

Edit Extension

Display Name Matej 1  
CID Num Alias  
SIP Alias

Extension Options

Outbound CID "386 [redacted]" <386 [redacted]>  
Ring Time Default  
Call Waiting Enable  
Call Screening Disable



# Primer 3: klicanje s poljubno klicno identifikacijo

## 3: rezultat na telefonu





# Primer 3: klicanje s poljubno klicno identifikacijo

## 4: prometni podatki pri operaterju

	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	23:41:22	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



**vprašanja?**



---

<http://www.Pravokator.si>

**Slepo zaupanje digitalnim dokazom – primer SIM kartic <<http://t.co/Fkmxvghk>>**

**Ko pokličejo hekerji – spreminjanje klicne identifikacije telefonskih klicev  
<<http://t.co/bBx2NIGQ>>**