

# Varnost informacijskih sistemov



**Matej Kovačič**  
**(CC) 2011 - 2016**

*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-sa/2.5/si/legalcode>>, ali na poštnem naslovu: Inštitut za intelektualno lastnino, Streliška 1, 1000 Ljubljana.*

# Varnost ni izdelek

- Varnost ni izdelek oziroma nekaj, kar lahko kupimo, namestimo in pozabimo, pač pa gre za proces.
- Varnostno kulturo je treba razvijati in gojiti neprestano.
- Informacijska varnost in varnost v prometu: ni dovolj samo dober avto in opravljen izpit, znanje o varnosti je potrebno obnavljati in uporabljati neprestano.

# Kaj je varnost?

- Overjanje, avtentikacija (ang. *authentication*): kdo je pošiljatelj, ko je prejemnik?
- Zaupnost (ang. *confidentiality*): sporočilo ostane znano samo pošiljatelju in prejemniku.
- Nadzor nad dostopom (ang. *access control*): kdo lahko dostopi do sporočila, beleženje dostopov.
- Avtorizacija (ang. *authorization*): kaj nekdo s sporočilom lahko stori?
- Dostopost (ang. *availability*): je sporočilo dostopno?

# Kaj je varnost?

- Celovitost (ang. *integrity*): sporočilo ostane nespremenjeno.
- Preprečevanje tajeja (ang. *nonrepudiation*): pošiljatelj kasneje ne more zatajiti sporočila, prejemnik ne more zatajiti prejema.
- Dopustnost (ang. *admissibility*): varnost terminalne opreme, zagotovilo, da na terminalni opremi na kateri se bo avtenticiral uporabnik in kjer bo uporabnik bral sporočilo ni zlonamernih mehanizmov.

**Napad**

# Napadi na računalniške sisteme

- napadi, ki predpostavljajo **fizični dostop** do računalnika;
- **omrežni napadi** (napadi na komunikacije, napadi na virtualni prostor);
- **zbiranje** različnih **informacij** na internetu;
- posredni, preko napadov na **uporabnika** (socialni inženiring, prevare).

## **Fizični dostop**

# Fizični dostop do računalnika

- Nevarnost zasega podatkov.
- Nevarnost podtikanja prikritega mehanizma (npr. programske aplikacije ali strojnega dodatka), s katerim napadalec pridobi dostop do računalnika ali si ustvari možnosti za krajo gesel.
- Zavržene računalniške komponente, ki vsebujejo trajne pomnilnike (trdi diski, tiskalniki, mobilni telefoni,...).
- Večuporabniška okolja.





SUROVINA



ZA  
PAPIR

# “Bump key”



# Obnavljanje "izbrisanih" podatkov

- Običajno brisanje datotek in celo formatiranje trdih diskov podatkov ne izbriše trajno.
- Poseben problem predstavlja brisanje začasnega pomnilnika (ang. *swap file*) pri zaustavitvi oz. hibernaciji računalnika.
- Vsebinsko že izbrisanih datotek je z različnimi orodji in tehnikami mogoče obnoviti deloma ali v celoti.

|     |  |                           |
|-----|--|---------------------------|
| 16  |  | n.a. d.z. o.r. .n.        |
| 32  |  | a. . i.n. t.e. r.n.       |
| 48  |  | e.t. u... .... V. .       |
| 64  |  | s.k. l.a. d.u. .z.        |
| 80  |  | .d. o.g. o.v. o.r.        |
| 96  |  | o.m. .V. a.m. .s.         |
| 112 |  | p.o. r.o. .a. m. .        |
| 128 |  | a.e. .m. o.j. .n.         |
| 144 |  | a.s. l.o. v.:. .M.        |
| 160 |  | a.t. e.j. .K. o.v.        |
| 176 |  | a... i... ,. . [REDACTED] |
| 192 |  | [REDACTED]                |
| 208 |  | [REDACTED]                |
| 224 |  | [REDACTED]                |
| 240 |  | ,. . n.a. s.l. o.v.       |
| 256 |  | .e. l.e. k.t. r.o.        |
| 272 |  | n.s. k.e. .p. o.a.        |
| 288 |  | t.e. :. . m.a. t.e.       |
| 304 |  | j... k.o. v.a. c.i.       |
| 320 |  | c. [REDACTED]             |
| 336 |  | [REDACTED]                |
| 352 |  | i.n. .G. S.M. .a.         |
| 368 |  | t.e. v.i. l.k. o.:.       |
| 384 |  | [REDACTED]                |
| 400 |  | [REDACTED]                |
| 416 |  | .... L.e. p. . p.o.       |
| 432 |  | z.d. r.a. v.,. ....       |
| 448 |  | M.a. t.e. j. . K.o.       |
| 464 |  | v.a. .i. .... ....        |
| 480 |  | .... .... ....            |
| 496 |  | .... .... ....            |

Forenzična analiza diska z orodjem Autopsy Forensic Browser.

# “Obnavljanje” Windows gesel

The screenshot displays several windows from a Windows XP desktop:

- PPA 1.50 - Brute Force attack - 2.54% (7)**: A window showing a brute force attack progress. It includes a menu (Project, Edit, Recovery, Options, Help) and a list of users with checkboxes. The 'Current User' is identified as Administrator.
- CIA Commander for Windows NT/2000/XP v1.0**: A window showing account details for Administrator, Guest, HelpAssistant, and SUPPORT\_388945a0.
- ERD Commander 2003 Locksmith Wizard**: A window titled 'Select New Password' with a key icon. It prompts the user to select an account and enter a new password. The 'Account' dropdown is set to Administrator, and the 'New Password' field contains 'Killian'.

Additional text visible in the image includes:

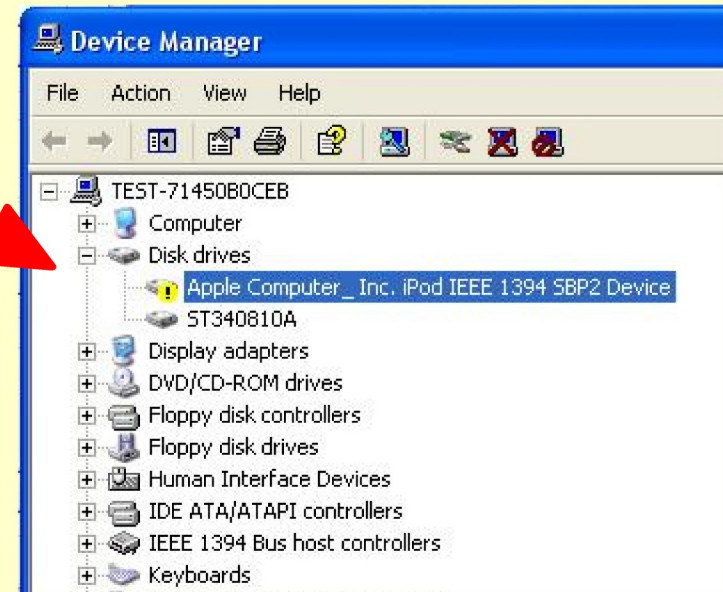
- Machine SID: S-1-5-21-
- Copyright (C)2001, by

Orodja za “obnavljanje” “pozabljenih” gesel za dostop do operacijskega sistema Windows (zahtevajo fizični dostop).

# Zaseg RAM-a preko FireWire vmesnika

```
Root Terminal
[root (knoppix)]# cd /usr/local/pythonraw1394/
[root (pythonraw1394)]# modprobe ohci1394
[root (pythonraw1394)]# modprobe raw1394
[root (pythonraw1394)]# ./romtool -s 0 ipod.csr
Init firwire, port 0
Updated 1024 byte ROM image from ipod.csr
[root (pythonraw1394)]#
```

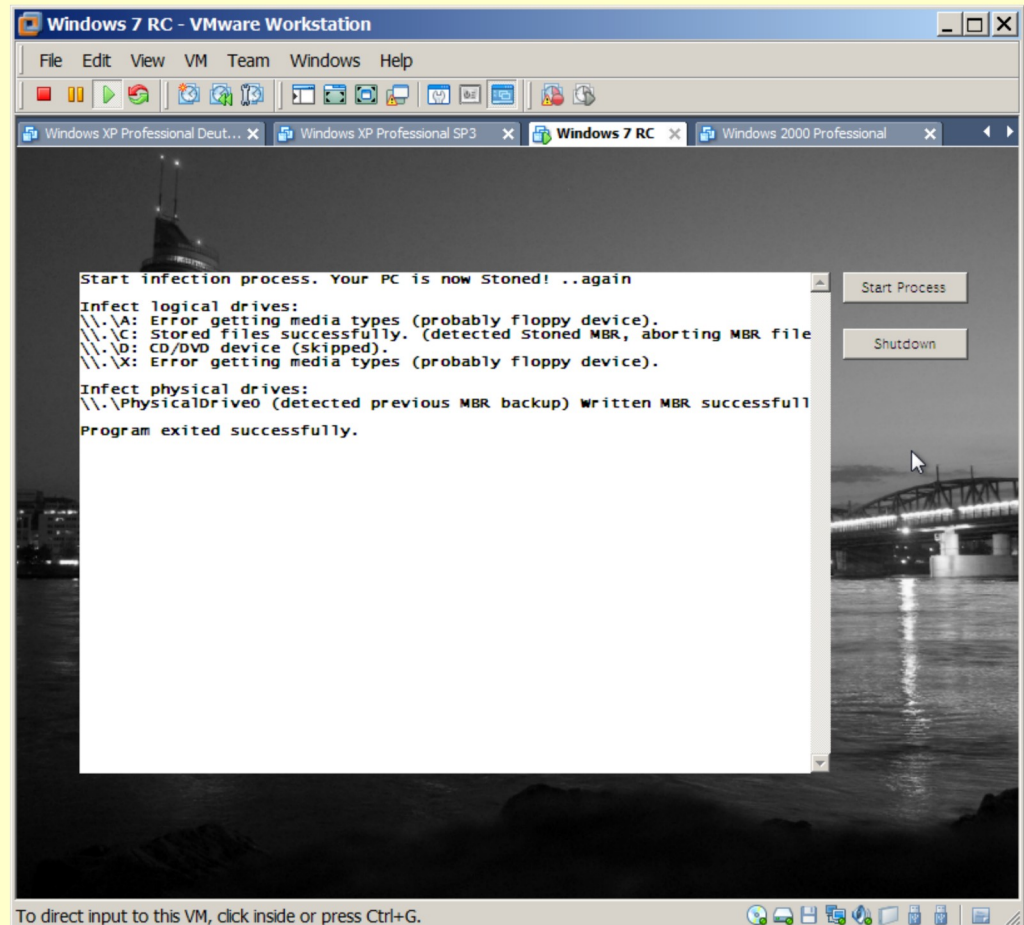
S programom romtool se v računalniku z Linuxom pretvarjamo, da smo iPod...



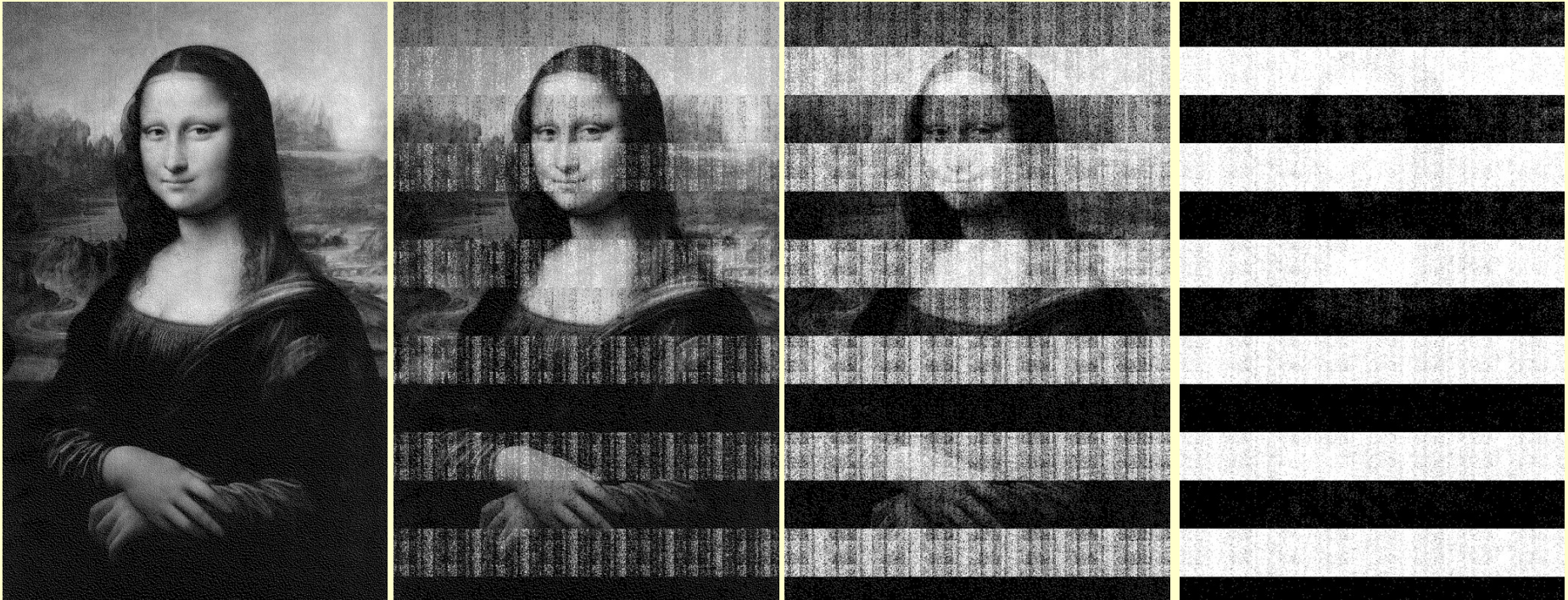
... in Windows Xp med priključenimi napravami prikažejo iPoda!

# Kraja ključev iz RAM-a

- Stoned Bootkit:  
okuži MBR - kraja  
TrueCrypt gesla,  
eskalacija privilegijev za  
CMD v okolju Windows  
po zagonu whoami.exe
- Okužba tudi preko PDF  
datoteke  
<<http://www.stoned-vienna.com/downloads/PDF%20Spread/Stoned%20PDF%20Infector.pdf>>



# Cold boot napad



Zasežena slika po 5 sekundah, 30 sekundah, 60 sekundah in 300 sekundah.

*Vir in avtorstvo: J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum in Edward W. Felten, Princeton University, 2008. <<http://citp.princeton.edu/memory/>>*



# “Evil maid” napad

```
SYSLINUX 3.75 2009-04-16 EBIOS Copyright (C) 1994-2009 H. Peter Anvin et al
Booting the kernel, it will take up to a minute...
hub 1-2:1.0: config failed, can't read hub descriptor (err -22)
Mounting proc filesystem
Mounting sysfs filesystem
Creating /dev
Creating initial device nodes
Loading /lib/kbd/keymaps/1386/qwerty/us.map
Setting up hotplug.
Creating block device nodes.
Creating character device nodes
Making device-mapper control node
Waiting for the USB stick to init...
Waiting for the USB stick to init...
Waiting for the USB stick to init...
Waiting for the USB stick to init...
Waiting for the USB stick to init...
sd 0:0:0: [sdb] Assuming drive cache: write through
sd 0:0:0: [sdb] Assuming drive cache: write through
sd 2:0:0: [sdb] Attached SCSI removable disk
Mount command: mount -r -t vfat /dev/sdb1 /mnt/stick
TARGET = /dev/sda

What do you want to do today: Run [E]vil Maid, [S]hell, [R]eboot
E
remounting /mnt/stick rw...
TrueCrypt EvilMaid patcher v0.1
-----
TrueCrypt Boot Loader detected
PatchTrueCrypt(): Compressed loader size: 11774 bytes
PatchTrueCrypt(): Loader memory size: 0x7000 (28672) bytes
PatchTrueCrypt(): Decompressing the boot loader
PatchTrueCrypt(): Decompression successful
PatchTrueCrypt(): Decompressed loader physical size: 27687 bytes
PatchAskPassword(): Loader is already infected
PatchTrueCrypt(): PatchAskPassword() failed
DisplayTrueCryptPassword(): Password is "_____ "
Saving original sectors in /mnt/stick/sectors-2009-10-15-170716
remounting /mnt/stick in ro...
done; you can reboot safely.

What do you want to do today: Run [E]vil Maid, [S]hell, [R]eboot
```

Evil Maid napad na TrueCrypt in...



...ostanki sirskega jedrskega reaktorja al-Kibar.

# **Internetne prevare**

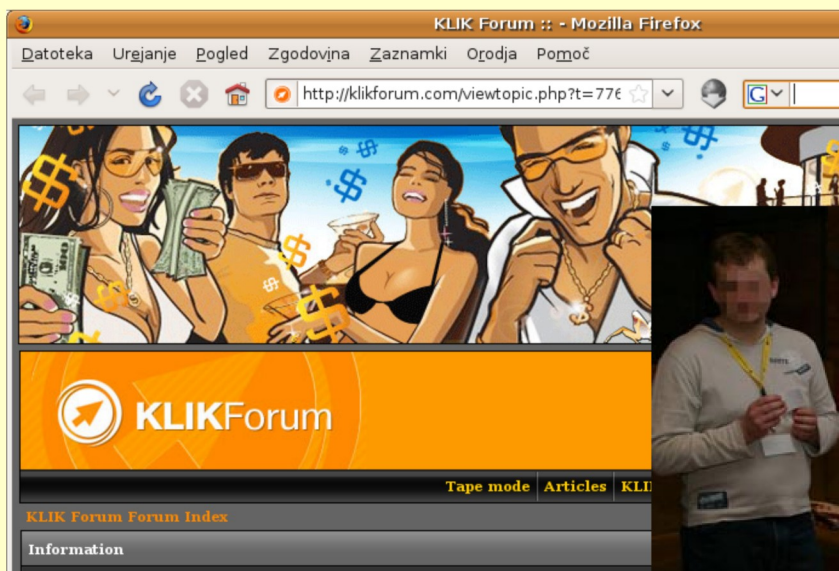
# Kiberkriminal včasih...

- raziskovanje,
- radovednost,
- samodokazovanje,
- zabava,
- vandalizem,...



# ... in kiberkriminal danes

- denar!



Spletna stran "podjetja".

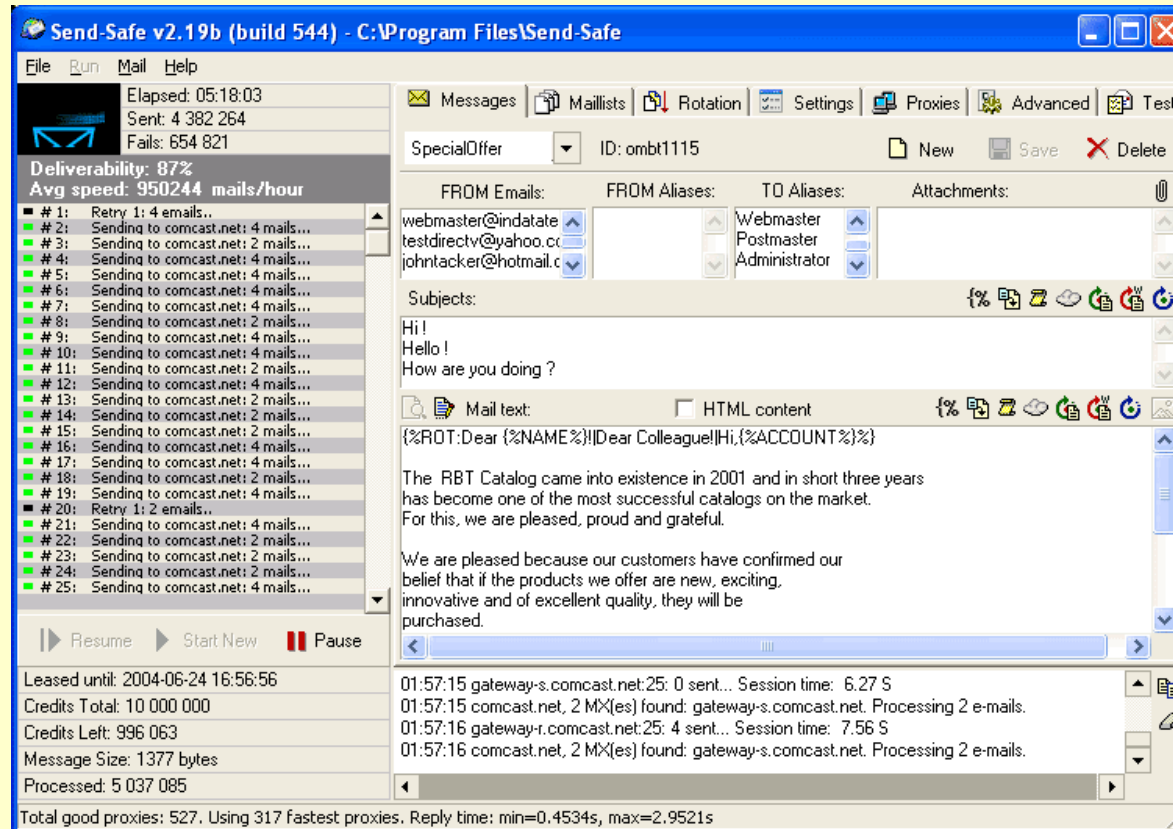


Zabava 95 zaposlenih v ruskem podjetju *Klik team* v Črni gori, februar 2008.



Šifirno-izsiljevalski virus Cryptolocker.

# Spam



Prodaja lažnih in goljufivih izdelkov,  
kraja osebnih podatkov,...

# Verižna pisma

☐ Zadeva: FW: PODPRITE NAS V PROTESTU IN ZAHTEVAH

Od: [REDACTED]

Datum: 14. 04. 2008 13:09

Za: [REDACTED]

Spoštovani,

Če bo koga vznemiril spodnji protest, naj s podpisom prispeva k spremembi.

Pozdrav,

[REDACTED]

-----Original Message-----

From: [REDACTED] [mailto:[REDACTED]]

Sent: Monday, April 14, 2008 12:59 PM

To: [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED];  
[REDACTED] [guest.arnes.si](mailto:guest.arnes.si); [REDACTED]; [REDACTED]; [REDACTED];  
[REDACTED]; [REDACTED]; [REDACTED] [\[REDACTED\].si](mailto:[REDACTED].si);  
[REDACTED] [\[REDACTED\]@national.si](mailto:[REDACTED]@national.si); [REDACTED] [\[REDACTED\]@gmail.com](mailto:[REDACTED]@gmail.com);

[REDACTED]

# Finanční spam

GCME Huge News Release Expected Before Years End!

Ring In The New Year With Cash. GCME is fast becoming a major player in the foreign film market.

With continuing mergers and joint ventures with the industries most influential corporations.

Right now it is at \$0.18. We have seen consistent price jumps following news releases and we have been told to expect big news before the end of the year.





# 419 scam

OFFICIAL LETTER...

FROM:MR.CHOU MUI

Hang Seng Bank Ltd

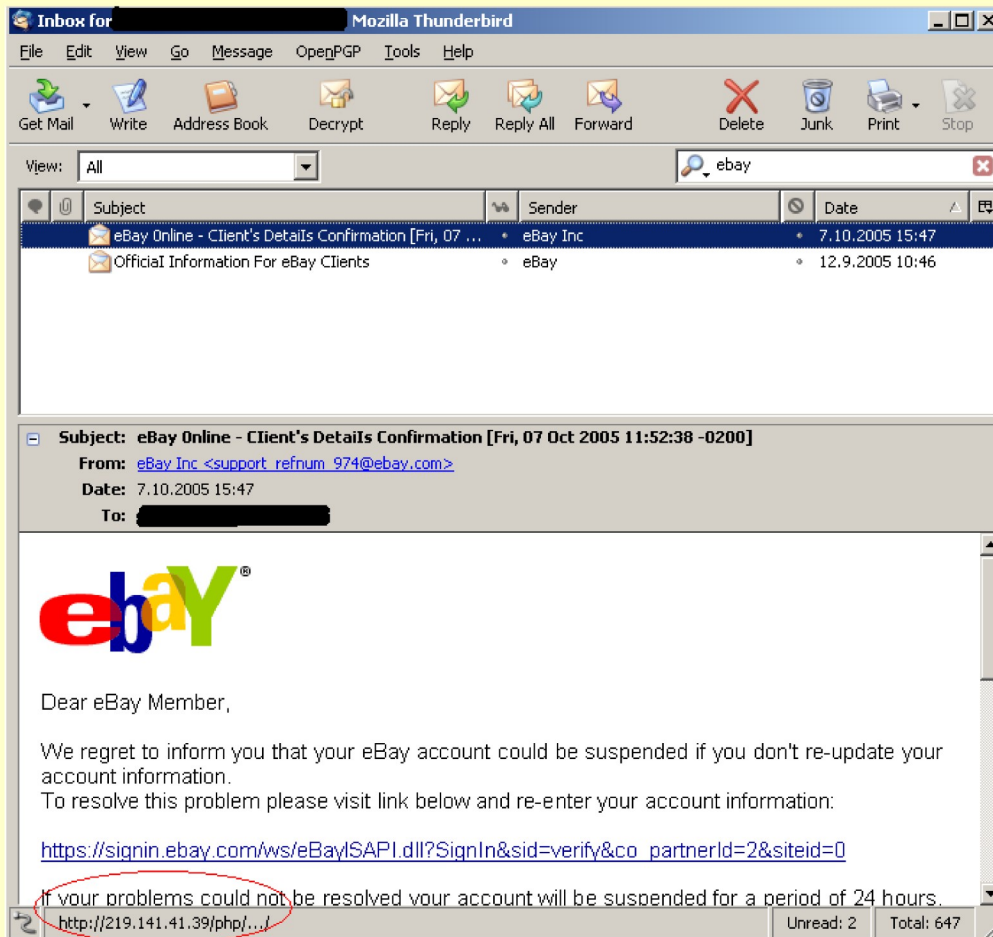
chou\_mui1@uymail.com



Let me start by introducing myself. I am Mr. Chou mui , Assistant Director of Operations of the Hang keng Bank Ltd,Sai Wan Ho Branch,171 Shaukiwan Road Hong Kong.

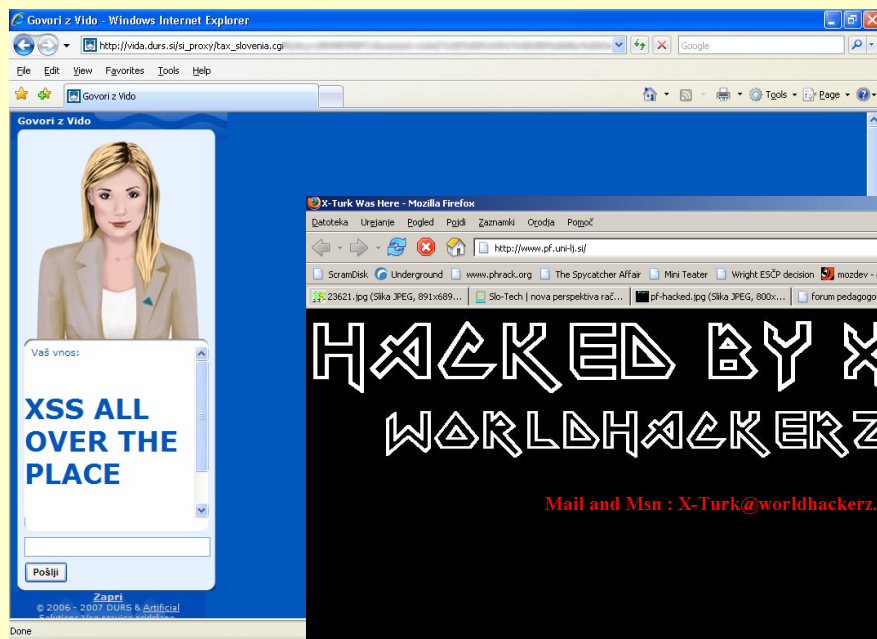
Before the U.S and Iraqi war, our client Hamadi Hashem a business man made a umbered fixed deposit of (346,736,899.68 HKD) for 18 calendar months...

# Ribarjenje

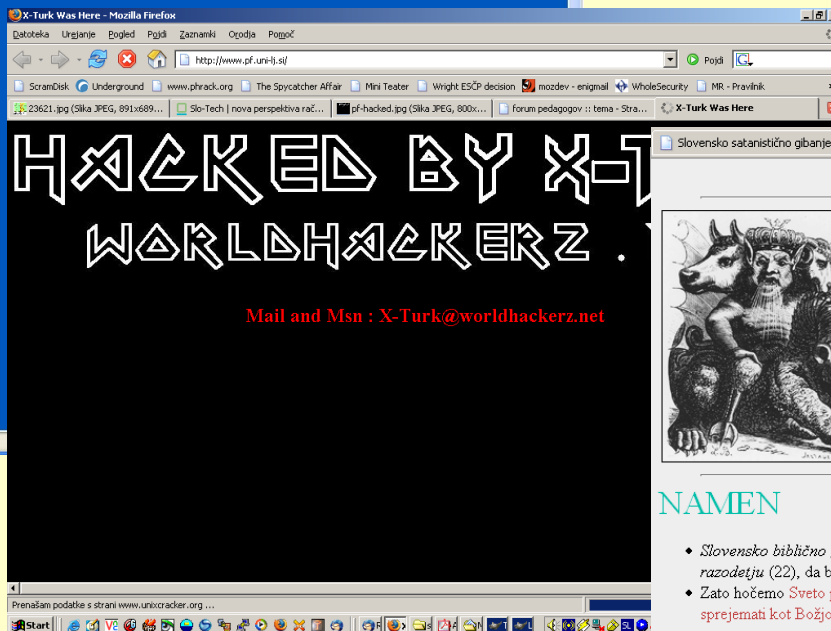


Primer ribarjenja (phisinga) preko neželene e-pošte.

# Razobličjenja spletnih strani



XSS napad na "davčno Vido".

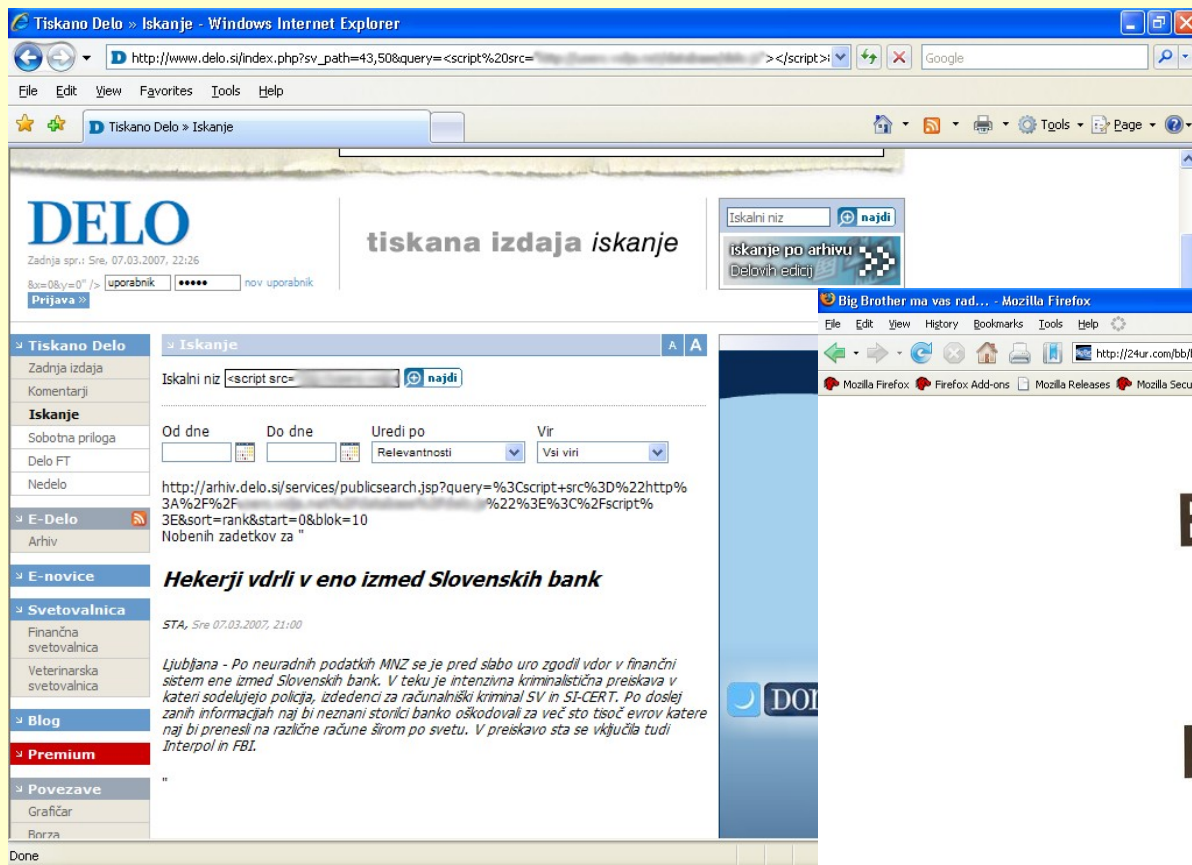


Pravna fakulteta, Univerza v Ljubljani, februar 2007



Razobličjenje spletne strani rimokatoliške cerkve.

# Razobličjenja spletnih strani

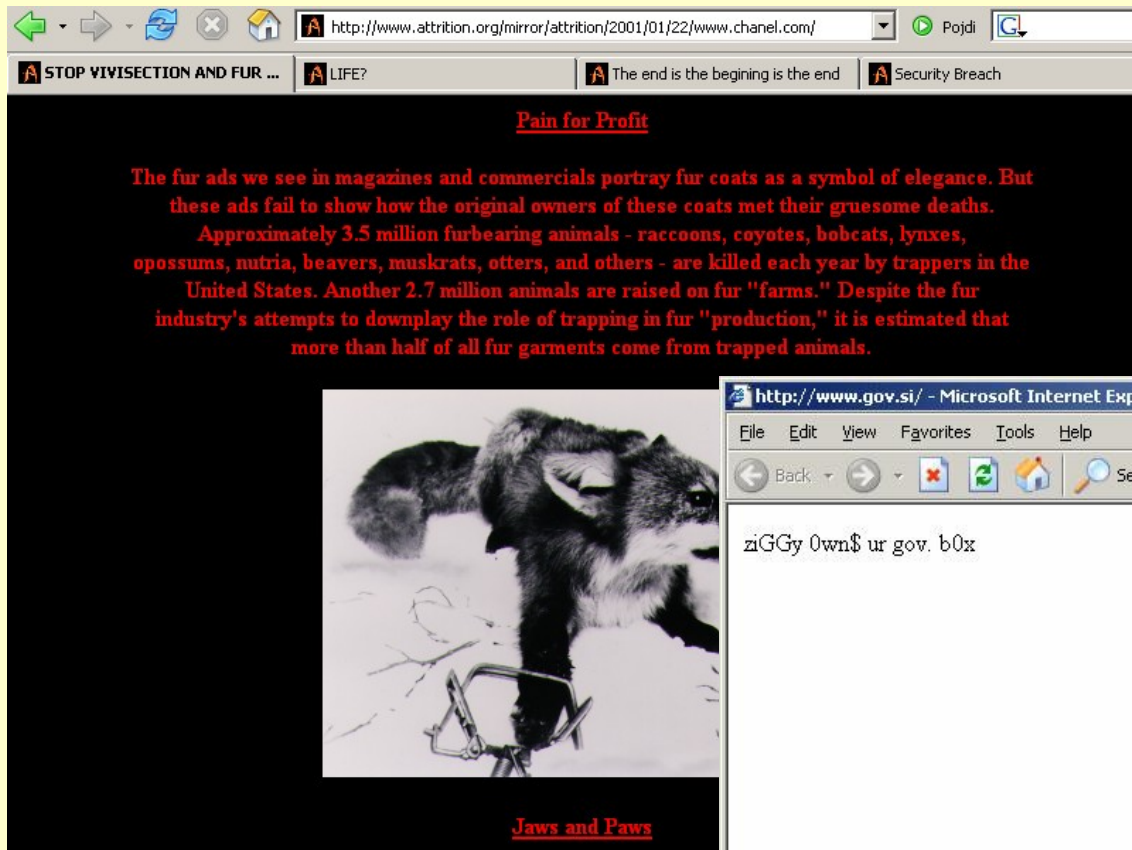


Lažna novica na spletni strani časnika DELO (XSS napad).

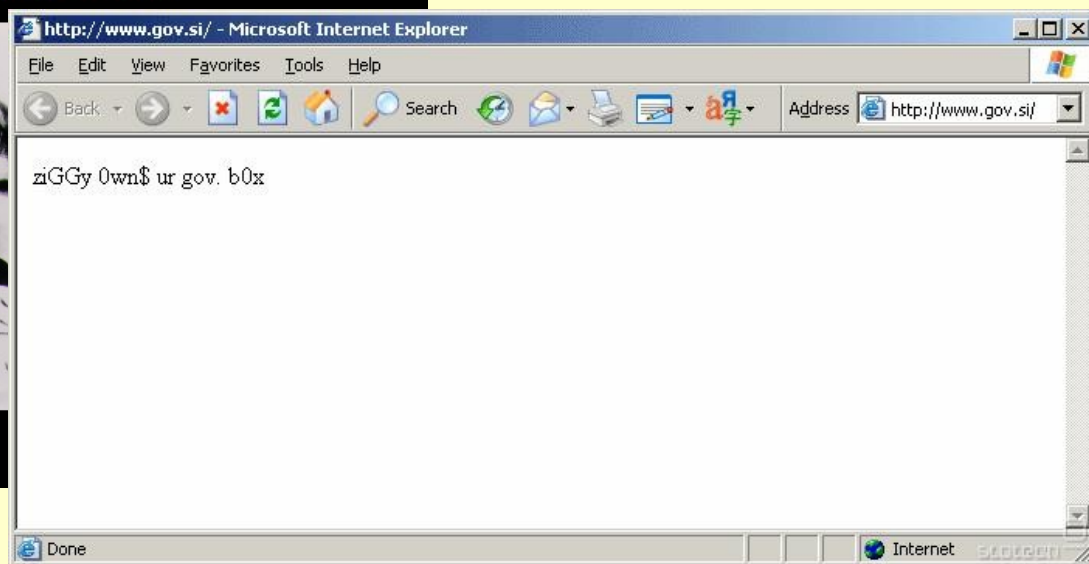


"Big Brother" na 24ur.com (XSS napad).

# Razobličjenja spletnih strani



Razobličjenje spletne strani  
modne hiše Chanell.com



Razobličjenje vladne strani (gov.si).







- zasebni uporabnik
- predplačnik
- poslovni uporabnik

<h3>Dimitrij Rupel postal IŠČI

- TELEFONI IN NAPRAVE
- PAKETI
- STORITVE
- AKCIJE
- TUJINA
- POMOČ IN INFORMACIJE
- VODAFONE LIVE!
- SI.MOST

Iskali ste:

### Dimitrij Rupel postal svetovalec uprave Simobila



Z današnjim dnem dr. Dimitrij Rupel postaja svetovalec Simobila za področje zunanje naročniške politike.

: - )

Število vseh rezultatov: 3  
Prikazani rezultati: 1 - 3  
Stran: 1

### Rezultati iskanja

#### IT specialist v CRM skupini, zadolžen za DMS področje (m/ž)

Želite razvijati svojo profesionalno pot pri enem najuglednejših in najboljših slovenskih zaposlovalcev? Podjetje Si.mobil d.d. je zaupanja vredno podjetje, kjer so ljudje na prvem mestu. Zaposleni v Si.mobilu so visoko usposobljeni profesionalci, ki so zaljubljeni v svoje delo in v komunikacijo. Prek vpetosti v globalne povezave pa zaposleni lahko pridobivajo tudi mednarodno znanje in bogate izkušnje.


#### Novi direktor prodaje

Novi direktor prodaje v družbi Si.mobil je s 3. januarjem 2007 postal Gregor Banič.

#### Nastavitev zunanega odjemalca



# Hackers embed flashing animations on epilepsy support forum

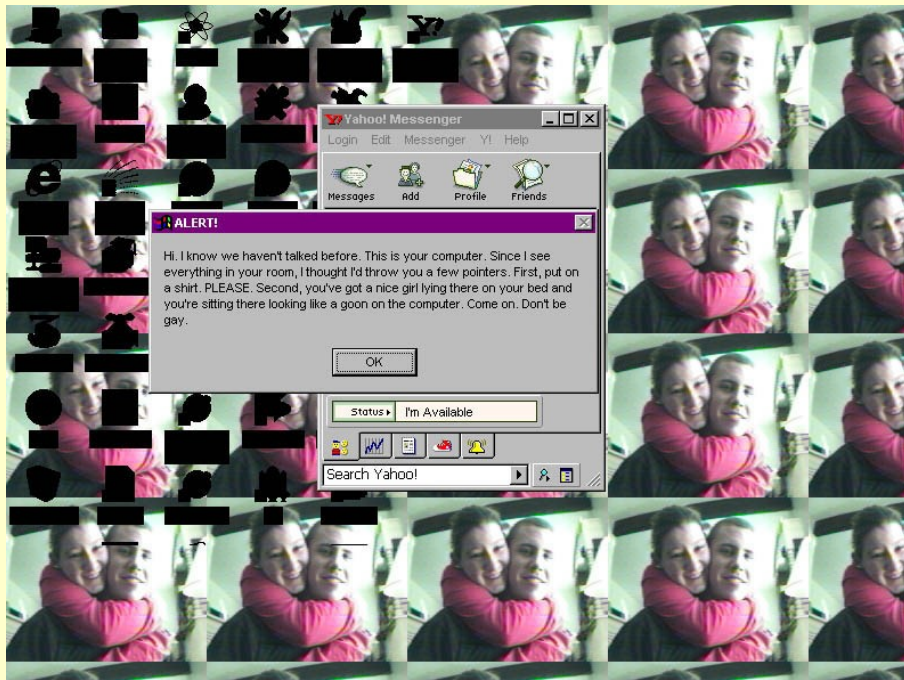
By Darren Murph  posted March 29th 2008 8:50PM

Shortly after hearing a [sad tale](#) of a 7-year old cancer patient having his medication and PSP stolen whilst en route to treatment comes yet another story of the world's meanest [preying](#) on the innocent. This go 'round, a group of griefers (which appear to be members of Anonymous) managed to invade a support forum established by the nonprofit Epilepsy Foundation and use JavaScript code and messages littered with flashing animations to effectively assault dozens of visitors who suffer from the disorder. The Foundation managed to catch wind of the problem within 12 hours of the attack, and while the boards were closed down temporarily to purge it of offending messages, many readers (such as RyAnne Fultz, pictured) experienced headaches and seizures before rescue arrived. Let's just say we sincerely hope the culprits get what's comin' to 'em.

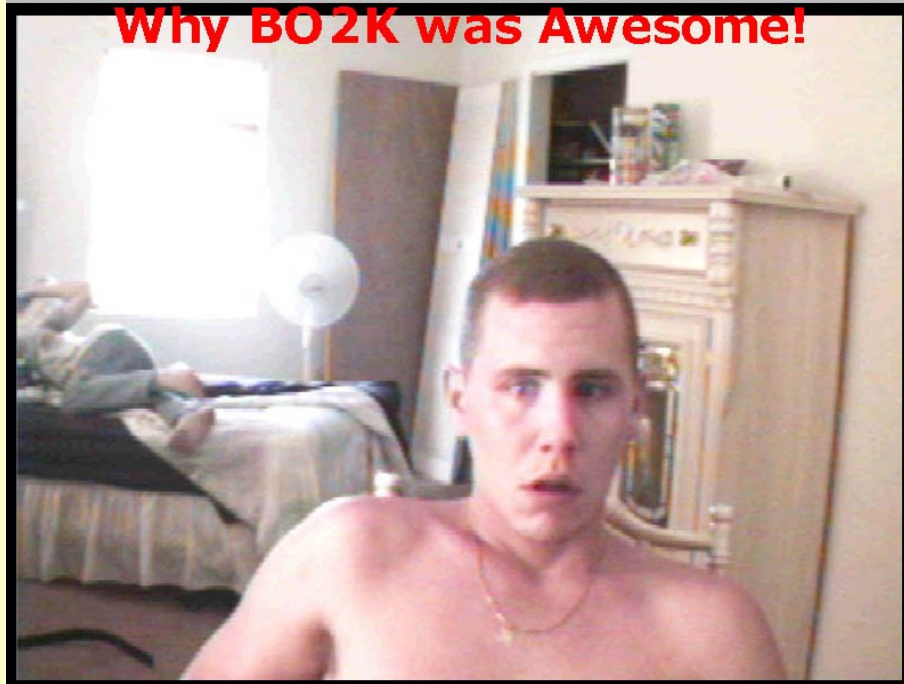


Vir: <http://www.engadget.com/2008/03/29/hackers-embed-flashing-animations-on-epilepsy-support-forum/>

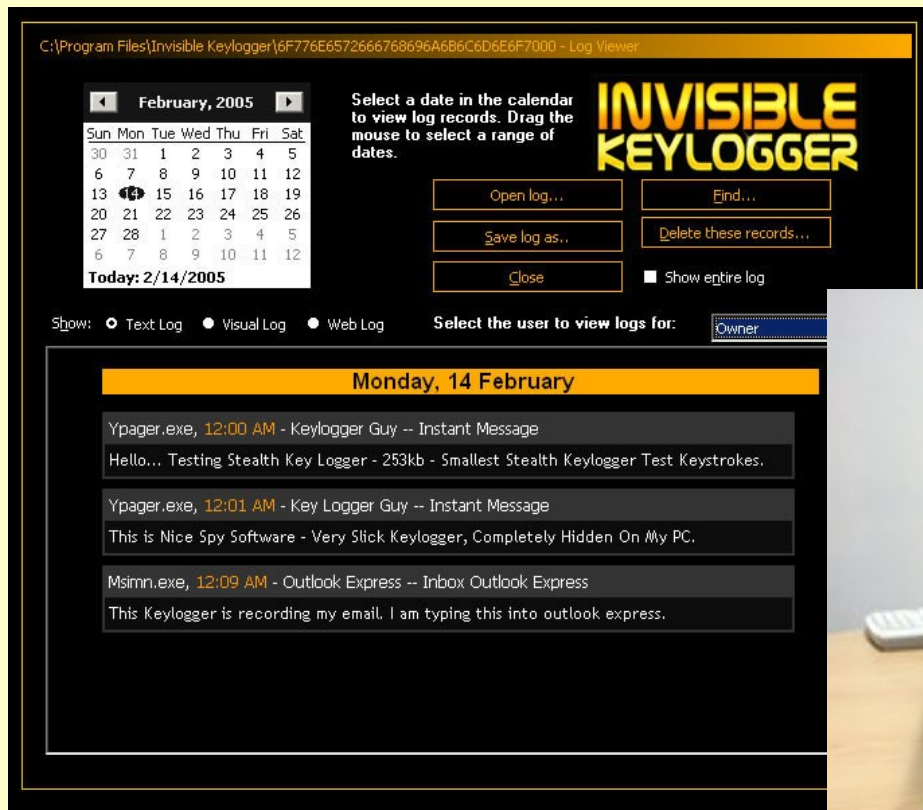
**Vdori in okužbe z zlonamerno programsko opremo**



## Why BO 2K was Awesome!



# Zlonamerno programje... in strojna oprema



Programski...



...in strojni prestrezniki tipkanja (vir  
in avtorstvo: [www.keyghost.com](http://www.keyghost.com))

- » **Novice**
  - » pošlji novice
  - » arhiv
- » **Članki**
- » **Testi**
- » **Forum**
  - » mali oglasi
  - » teme zadnjih 24h
  - » moje teme
  - » sveže teme
  - » zasebna sporočila
  - » iskanje
- » **Pravila**
- » **Povezave**
- » **Ostalo**

» **Anketa**

**Na NESTu me najbolj privlačijo:**



Predlagajte vprašanje za naslednjo anketo



»»» **novice**

Četrtek, 6. 4. 2006

**Hacked by Slokryptor (19:40)**

**Security flaws was found and exploited on this site by Slokryptor**



Slo-tech is vulnerable to multiple XSS holes:

- xss in registration form
- multiple XSS vulnerabilities in forum post - IMG TAG(using some special caracter sets - IE Only)
- many potential vulnerabilities all over the site

Learn secure programming!

I didn't destroy anything, also I didn't place any backdoor!

Check <http://enigmagroup.org> and <http://www.techsploit.com/>

vir: **Hacked** | komentiraj | avtor: Slokryptor

**Apple Boot Camp - ali kako legalno poganjati Windows na Mac-u (13:40)**

Pri Applu so se odločili, da bodo vseeno uradno podprli Windows na svoji strojni opremi. Tako so ustvarili Apple Boot Camp.

» **Nastavitve**  
**darkolor**

Odjavi me

» **Zadnje novice**

- » Hacked by Slokryptor (0)
- » Apple Boot Camp - ali kako legalno poganjati Windows na Mac-u (11)
- » Microsoftu ni všeč, da se predajajo računalniki brez operacijskega sistema (75)
- » Cene prihajajočih procesorjev (57)
- » Novih 2.000 piratskih ovadb (115)

» **Še se kadi**



Intervju s Philipom Zimmermannom



Menjava kondenzatorjev na osnovni plošči

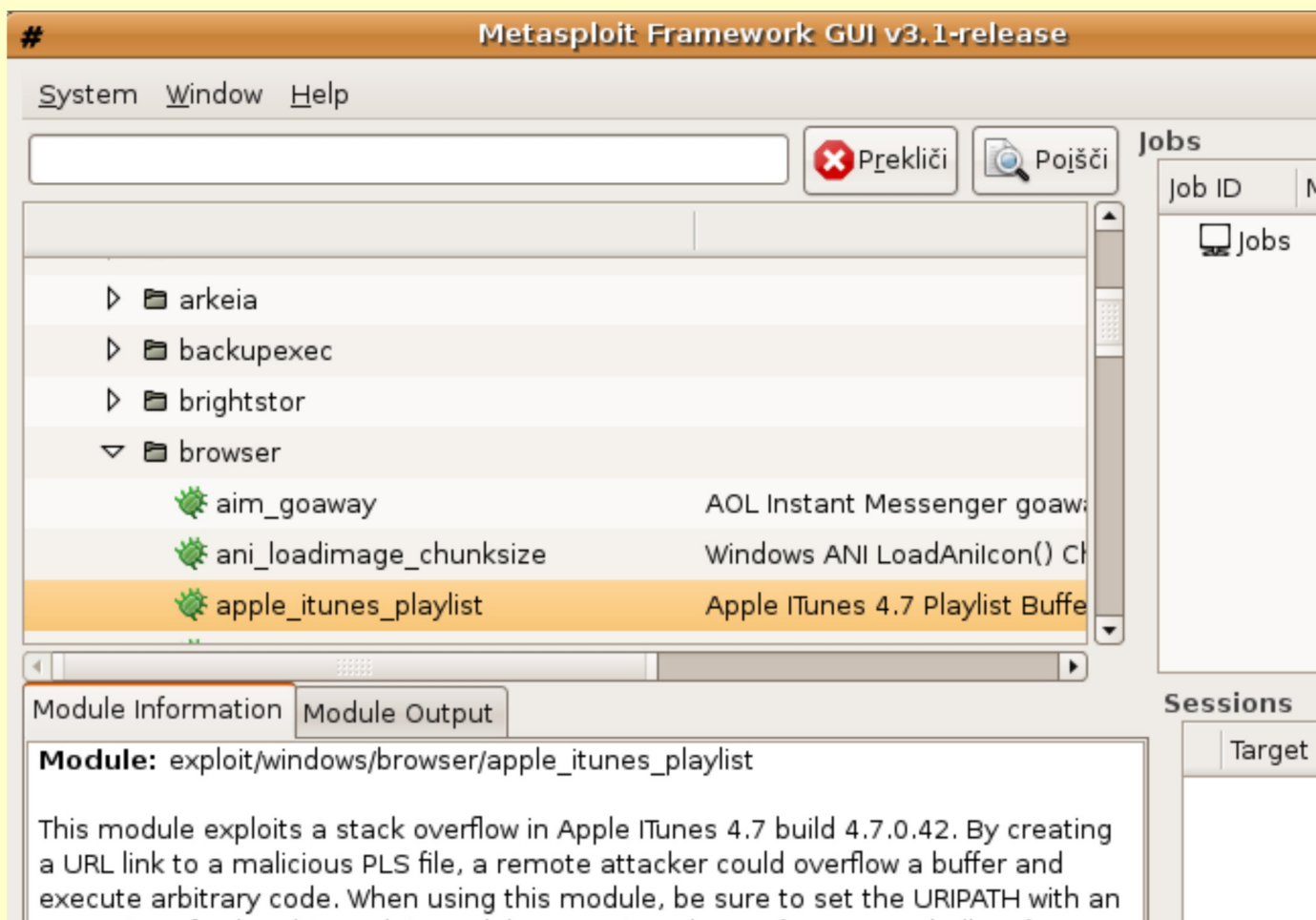


Kršitve avtorskega prava na internetu



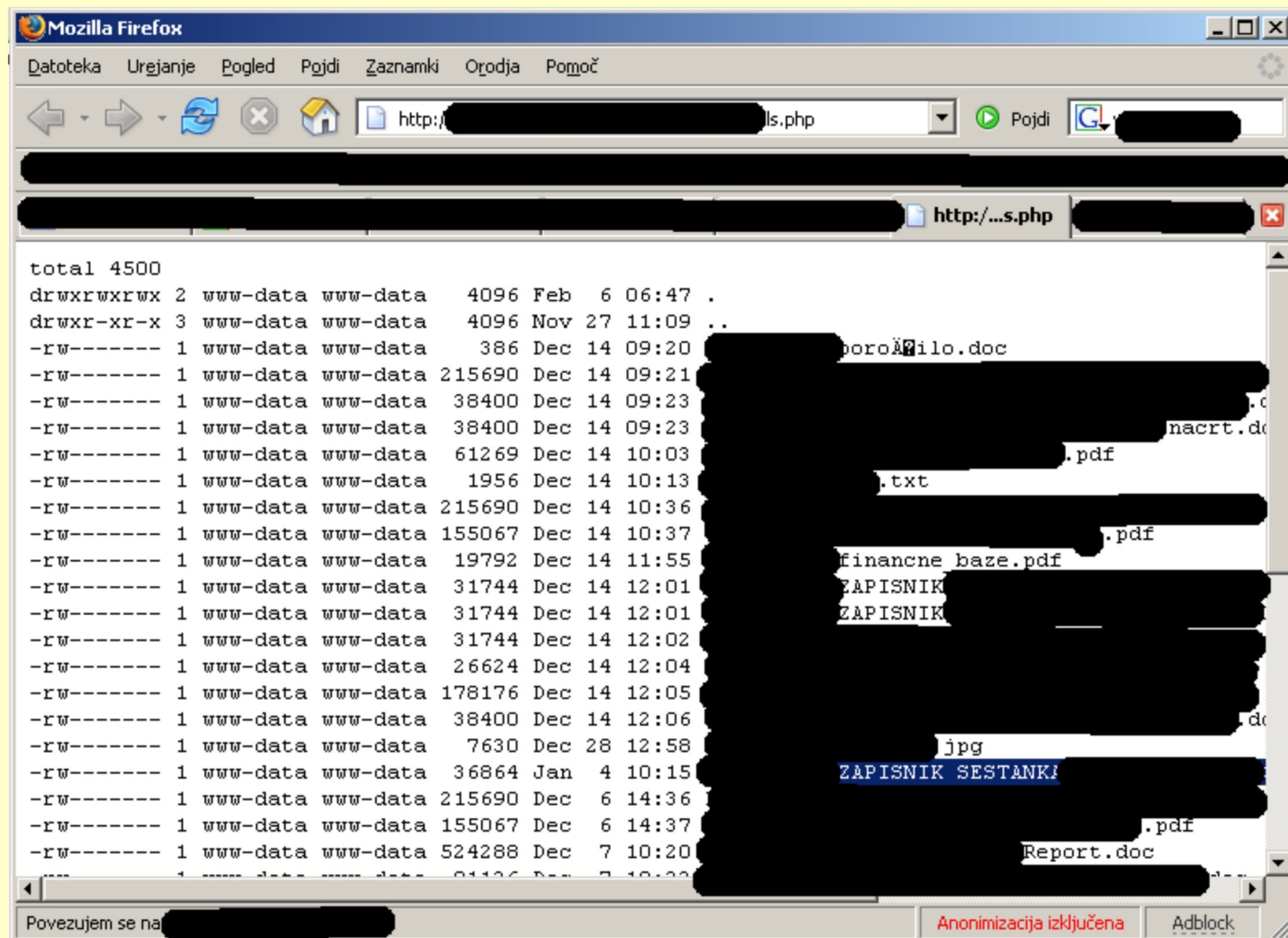
Video nadzor na plačalnikih

# Orodja za vdore



*Metasploit Framework* – zbirka programja za izrabo varnostnih ranljivosti.

# Možnosti poljubnega spreminjanja URL naslovov lahko vodi...



# ...do resnih napadov

The image shows a Mozilla Firefox browser window displaying the Sparkasse website. The address bar shows the URL `https://netstik.sparkasse.si/eb/index.asp`. The page content includes a red hand icon, a user login field, and contact information for Sparkasse (01/583 6666). A pop-up window is overlaid on the page, displaying the details of a MasterCard account. The pop-up window title is "MasterCard kartični račun: [redacted]". The details listed are:

|                                |                                      |
|--------------------------------|--------------------------------------|
| Uporabnik:                     | [redacted]n                          |
| Vrsta kartice:                 | primarna kartica na kartičnem računu |
| Številka kartice:              | 5209 [redacted]                      |
| Veljavnost do:                 | [redacted]-12                        |
| Naziv na kartici:              | [redacted]                           |
| Datum otvoritve kartice:       | [redacted] 2006                      |
| Datum blokacije:               | /                                    |
| Mesečni limit (nakup):         | [redacted] EUR                       |
| Mesečni limit (dvig gotovine): | [redacted] EUR                       |

Below the details, it states: **Za preklic kartice, prosimo, pokličite 01/583 41 83.**

At the bottom of the pop-up window, there is a copyright notice: © 2002-2009, BANKA SPARKASSE d.d. Pravica do napak in sprememb pridržana.



# Napake pri omejitvah dostopa


← → [www.quintessenz.org/d/000100003123](http://www.quintessenz.org/d/000100003123)

**BIG BROTHER AWARDS** quintessenz  
Datenschutz ist Menschenrecht [search](#) / [subscribe](#) / [upload](#) / [kontakt](#)

**CURRENTLY RUNNING**

## Datamining the NSA

An inquiry into the strategies, methods and actors of the "Biometrics Consortium", an NSA led incubator project in the field of biometrics. First results are online, more will be published subsequently.



### Working Drafts, Part1

For more information pls contact **biometrics at quintessenz.org**

### Data sources

- o **Biometrics Consortium List**

**related topics**

- o [Biometrics doqu/base](#)

**related documents**

- o [2004\\_06\\_14, DoD CAC biometric integration.pdf](#)
- o [1999\\_04\\_16, Schellberg Advocate Biometrics Legislation - Privacy Fears in the Age of Privacy Fears](#)
- o [2003\\_06\\_12, Ghanaweb on sagem bribery in nigeria](#)
- o [2004\\_04\\_16, Austrian dataprotection commission on datamining part threee more documents ...](#)

**related campaigns**

- o [Datamining the NSA - Part I](#)

**related links**

<http://www.quintessenz.org/d/000100003134> 24-2004 [ca 60 MB]

prevzem.php5 (Predmet application/pdf) - Mozilla Firefox

Datoteka Urjevanje Pogled Pojdi Zaznamki Orodja Pomoč

http://lgl.esiti.com/si/prevzem.php5?id=24400


Firefox Help Firefox Support Plug-in FAQ

LGL - LUTKOVNO GLEDALIŠČE LJUBLJANA LGL - LUTKOVNO GLEDALIŠČE LJUBLJANA prevzem.php5 (Predmet application...

163% LGL - LUTKOVNO GLEDALIŠČE LJUBLJANA


potrdilo o nakupu / potrdilo o nakupu / potrdilo o nakupu / potrdilo o nakupu / potrdilo o nakupu / potrdilo o nakupu / potrdilo o nakupu / potrdilo o nakupu

Lutkovno gledališče Ljubljana



**VILA MALINA, izven**  
**LGL-Veliki oder, 11. januar 2007 ob 17:00**

| segment       | vrsta | Številka | količina | cena                                    |
|---------------|-------|----------|----------|---|
| Veliki oder   | 6     | 7b       | 1        | 3,24 EUR                                |
| Veliki oder   | 6     | 7a       | 1        | 3,24 EUR                                |
| Veliki oder   | 6     | 6b       | 1        | 3,24 EUR                                |
| Veliki oder   | 6     | 6a       | 1        | 3,24 EUR                                |
| <b>skupaj</b> |       |          |          | <b>12,96 EUR</b><br><b>3.105,73 SIT</b> |



Vaše potrdilo o nakupu zamenjajte za vstopnice na blagajni dvorane.

V primeru, da prireditvev odpade, lahko potrdilo o nakupu zamenjate na blagajni organizatorja za drugo prireditvev ali pa vam organizator vrne denar, ki ga morate prevzeti v enem mesecu na njegovi blagajni. Za vse dodatne informacije nam pišite na elektronski naslov info@lgl.si.

**številka potrdila o nakupu**  
**010-000-107-788-454-883-142760**

Končano Anonimizacija izključena

Start prevze... The GIMP Layers, ... Untitled... LGL - LU... http://l... 10:19

# SQL vrivanje

http://www.kpk-rs.si/sl/iskanje/

Newsletter / Medijsko središče / RSS

REPUBLICA SLOVENIJA

E-OBRAZCI / POGOSTA VPRAŠANJA / ODLOČITVE IN MNENJA / SLOVARČEK / KONTAKT

iskanje

**KOMISIJA ZA PREPREČEVANJE KORUPCIJE**

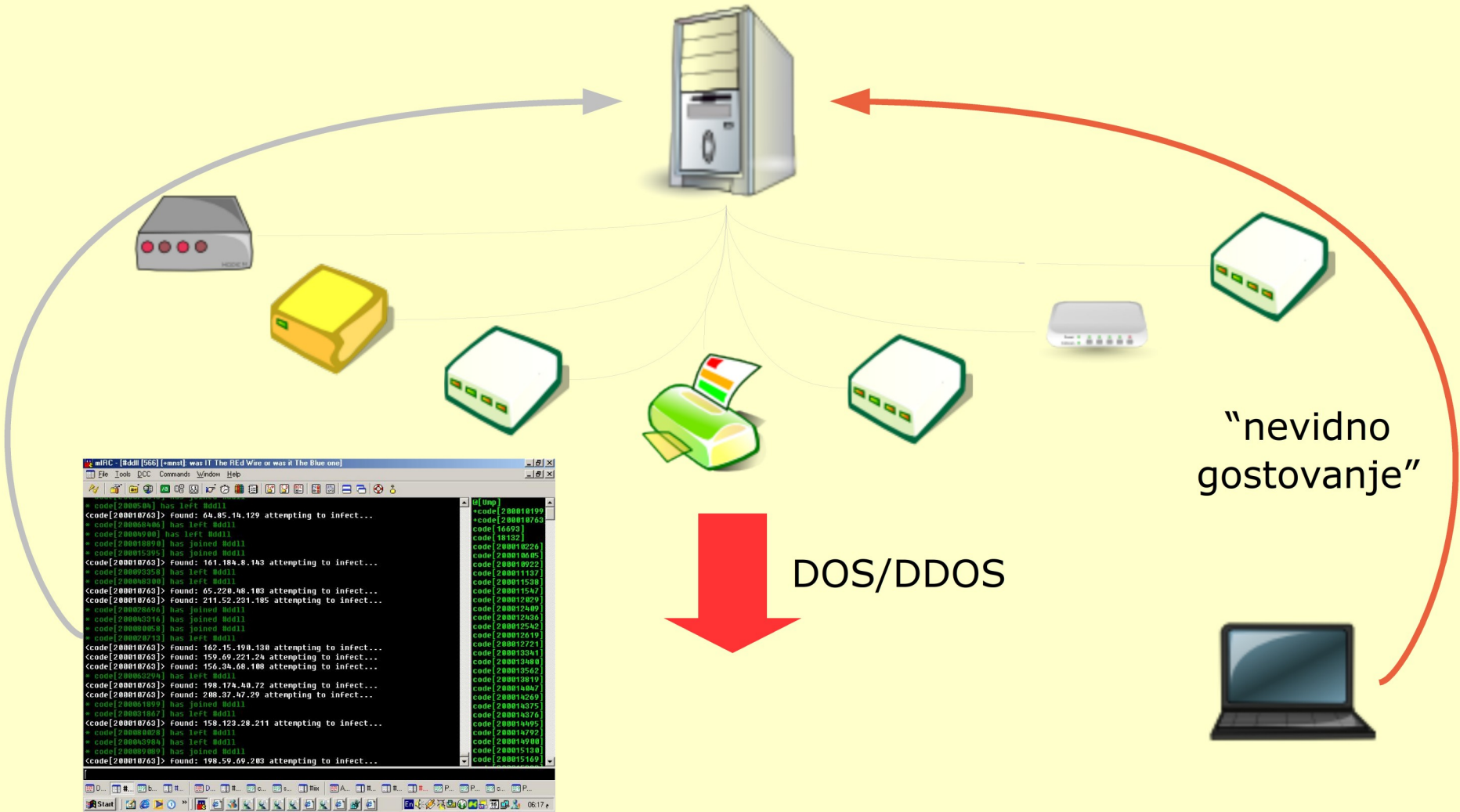
KOMISIJA | KORUPCIJA INTEGRITETA IN ETIKA | ZAVEZANCI IN NJIHOVE DOLŽNOSTI | PREVENTIVA IN NAČRT INTEGRITETE | NADZOR IN PREISKAVE | LOBIRANJE | PROJEKT TRANSPARENTNOST

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '%' OR LOWER(REPLACE(t\_faq.odgovor,'š','š')) LIKE '%\\\\\\\\\\\\\\\\%' at line 1  
SELECT t\_faq.vprasanje AS naslov, t\_faq.odgovor AS vsebina\_1 FROM t\_faq WHERE id\_jezik='sl' AND (LOWER(REPLACE(t\_faq.vprasanje,'š','š')) LIKE '%\\\\\\\\\\\\\\\\%' OR LOWER(REPLACE(t\_faq.odgovor,'š','š')) LIKE '%\\\\\\\\\\\\\\\\%')

## Urejanje zapisov: Novice 2008/2009

| Naslov   | Avtor                     |
|----------|---------------------------|
| ' or 1=1 | Matej Kovačič, 25.11.2008 |

# Prikrita omrežja



"nevidno  
gostovanje"

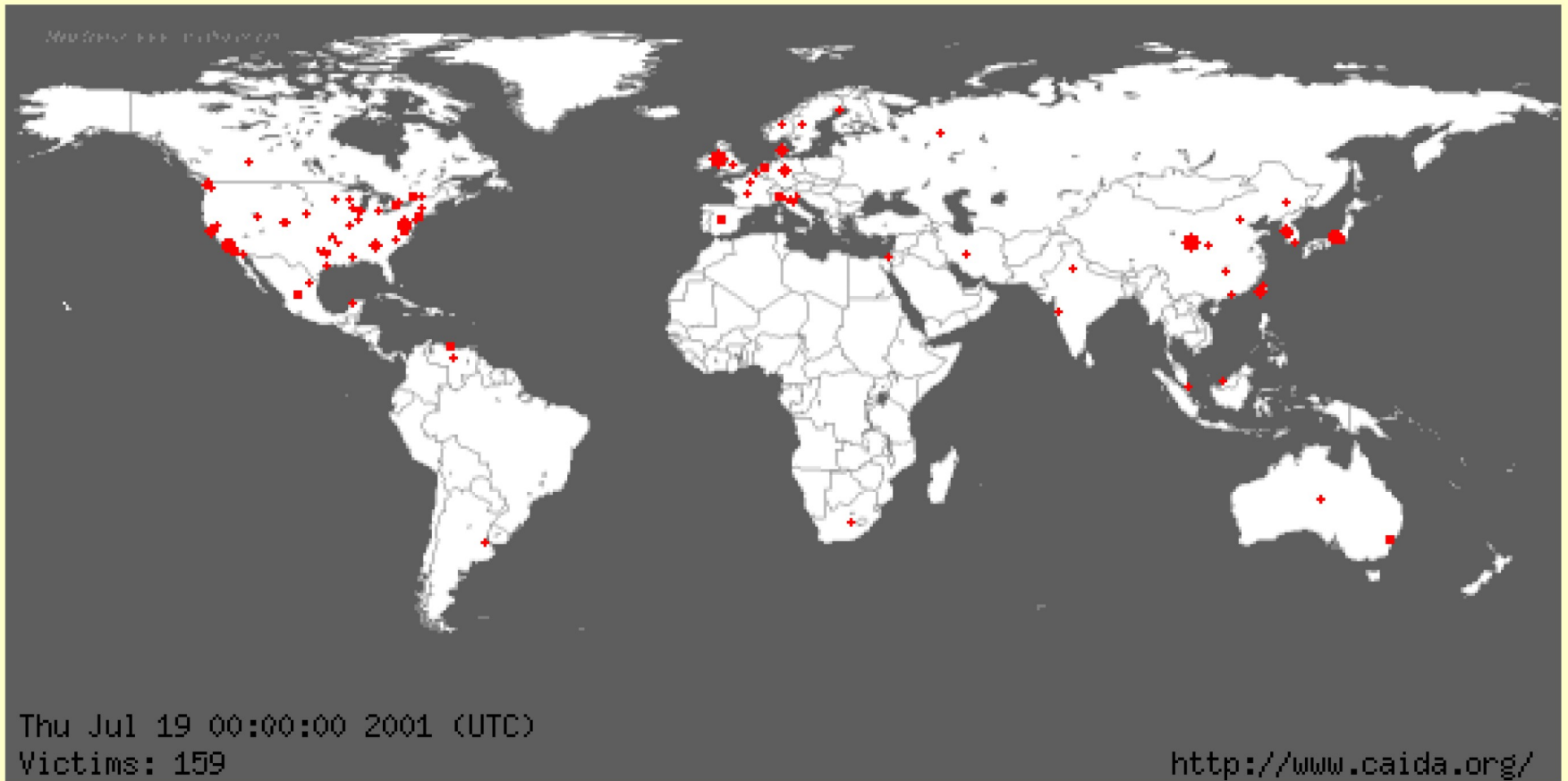
DOS/DDOS

```
mlRC - [Rdill] [666] [msmt] was IT The RED Wine or was it The Blue one
File Tools DCC Commands Window Help
* code[2000505] has left 0dd11
<code[200010763] Found: 64.85.14.129 attempting to infect...
* code[200063405] has left 0dd11
* code[200009090] has left 0dd11
* code[200018098] has joined 0dd11
* code[200015395] has joined 0dd11
<code[200010763] Found: 161.184.8.143 attempting to infect...
* code[200073258] has left 0dd11
* code[200003008] has left 0dd11
<code[200010763] Found: 65.220.48.183 attempting to infect...
<code[200010763] Found: 211.52.231.185 attempting to infect...
* code[200026096] has joined 0dd11
* code[200003216] has joined 0dd11
* code[200004858] has joined 0dd11
* code[200020715] has left 0dd11
<code[200010763] Found: 162.15.108.130 attempting to infect...
<code[200010763] Found: 159.69.224.224 attempting to infect...
<code[200010763] Found: 156.34.68.108 attempting to infect...
* code[200063295] has left 0dd11
<code[200010763] Found: 198.174.40.72 attempting to infect...
<code[200010763] Found: 200.37.47.29 attempting to infect...
* code[200061997] has joined 0dd11
* code[200031867] has left 0dd11
<code[200010763] Found: 158.123.28.211 attempting to infect...
* code[200000000] has left 0dd11
* code[200003984] has left 0dd11
* code[200009809] has joined 0dd11
<code[200010763] Found: 198.59.69.203 attempting to infect...
* code[200010763] Found: 198.59.69.203 attempting to infect...
```

# Prikrita omrežja

```
mIRC - [#ddl [566] [+mnst]: was IT The REd Wire or was it The Blue one]
File Tools DCC Commands Window Help
* code[2000504] has left #ddl1
<code[200010763]> found: 64.85.14.129 attempting to infect...
* code[200068406] has left #ddl1
* code[20004900] has left #ddl1
* code[200018890] has joined #ddl1
* code[200015395] has joined #ddl1
<code[200010763]> found: 161.184.8.143 attempting to infect...
* code[200093358] has left #ddl1
* code[200048300] has left #ddl1
<code[200010763]> found: 65.220.48.103 attempting to infect...
<code[200010763]> found: 211.52.231.185 attempting to infect...
* code[200028696] has joined #ddl1
* code[200043316] has joined #ddl1
* code[200080058] has joined #ddl1
* code[200020713] has left #ddl1
<code[200010763]> found: 162.15.190.130 attempting to infect...
<code[200010763]> found: 159.69.221.24 attempting to infect...
<code[200010763]> found: 156.34.68.108 attempting to infect...
* code[200063294] has left #ddl1
<code[200010763]> found: 198.174.40.72 attempting to infect...
<code[200010763]> found: 208.37.47.29 attempting to infect...
* code[200061899] has joined #ddl1
* code[200031867] has left #ddl1
<code[200010763]> found: 158.123.28.211 attempting to infect...
* code[200080028] has left #ddl1
* code[200043984] has left #ddl1
* code[200089089] has joined #ddl1
<code[200010763]> found: 198.59.69.203 attempting to infect...
@[Ump]
+code[200010199]
+code[200010763]
code[16693]
code[18132]
code[200010226]
code[200010605]
code[200010922]
code[200011137]
code[200011538]
code[200011547]
code[200012029]
code[200012409]
code[200012436]
code[200012542]
code[200012619]
code[200012721]
code[200013341]
code[200013480]
code[200013562]
code[200013819]
code[200014047]
code[200014269]
code[200014375]
code[200014376]
code[200014495]
code[200014792]
code[200014900]
code[200015130]
code[200015169]
```

Pogled na prikrito omrežje iz strani napadalca.



# 'Steganografski' virusi

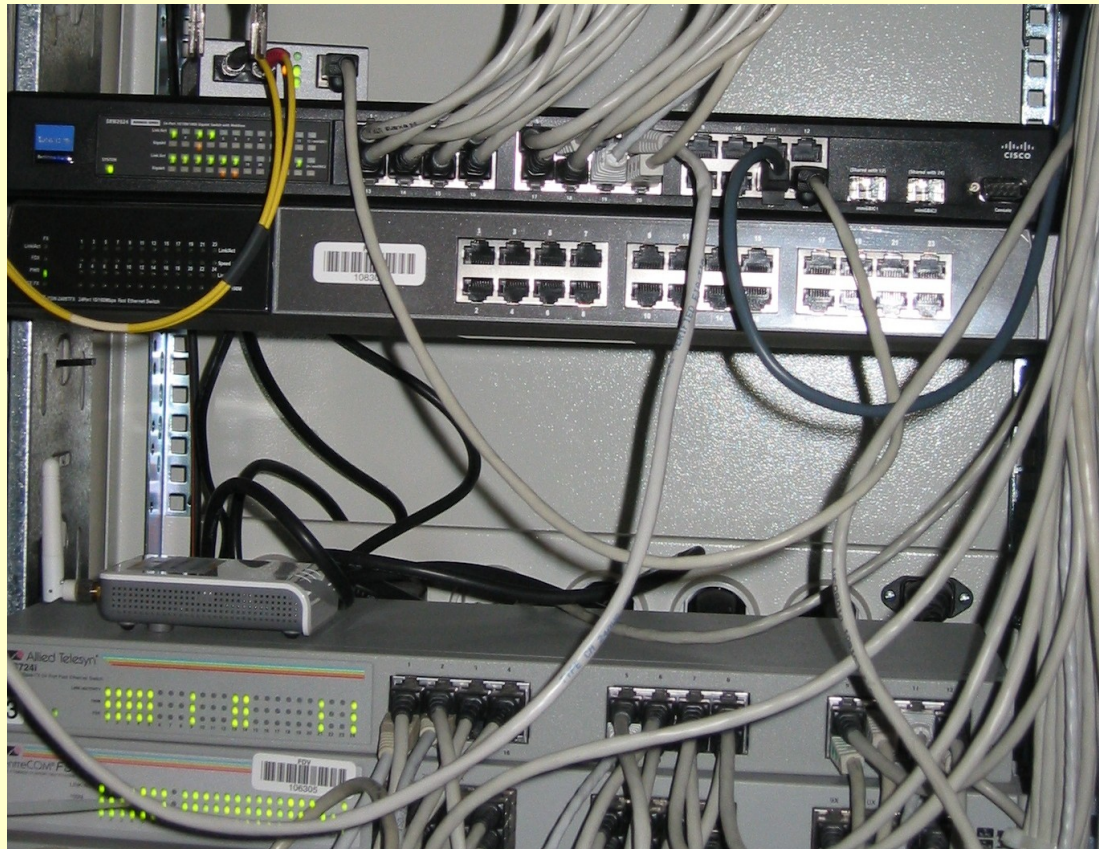
|        | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | A  | B  | C  | D  | E  | F  | 0                | 1     | 2    | 3    | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |  |
|--------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|------------------|-------|------|------|---|---|---|---|---|---|---|---|---|---|---|---|--|
| 0000h: | F4 | 16 | FD | ED | 20 | 01 | 00 | 00 | 00 | 00 | 00 | 00 | 44 | 00 | 00 | 00 | ó.ýí             | ...   | .... | D... |   |   |   |   |   |   |   |   |   |   |   |   |  |
| 0010h: | 62 | A5 | C0 | FB | AE | EB | 31 | CA | 02 | 84 | 11 | DA | 67 | 65 | 19 | C1 | b¥À@e1Ê...       | Úge.Á |      |      |   |   |   |   |   |   |   |   |   |   |   |   |  |
| 0020h: | 12 | 94 | 65 | E0 | BD | DD | 4E | F4 | 01 | 23 | 01 | BD | 6B | FF | 5E | 25 | ."eà%YÑó.#.¥ky^¥ |       |      |      |   |   |   |   |   |   |   |   |   |   |   |   |  |
| 0030h: | 41 | 72 | 68 | 5D | B3 | 1C | ED | 0A | 80 | 92 | 4E | 34 | F0 | 67 | FA | D3 | Arh]'.i.€'N4øgúÓ |       |      |      |   |   |   |   |   |   |   |   |   |   |   |   |  |
| 0040h: | 84 | C1 | 22 | 12 | EC | BB | F2 | 4B | 63 | 92 | E2 | 55 | D1 | 18 | 37 | 88 | „Á".i>òKc'áUÑ.7~ |       |      |      |   |   |   |   |   |   |   |   |   |   |   |   |  |
| 0050h: | 39 | 2D | AC | 25 | F9 | 9E | 4D | 54 |    |    |    |    |    |    |    |    | 9--¥ùžMT         |       |      |      |   |   |   |   |   |   |   |   |   |   |   |   |  |

| Template Results - alureon_head.bt  |           |       |      |                            |
|-------------------------------------|-----------|-------|------|----------------------------|
| Name                                | Value     | Start | Size | Color                      |
| struct ALUREON_CHUNK                |           | 0h    | 58h  | Fg: Bg:                    |
| ... unsigned long crc               | EDFD16F4h | 0h    | 4h   | Fg: Bg: [pink]             |
| ... unsigned long size_decompressed | 120h      | 4h    | 4h   | Fg: Bg: [light blue]       |
| ... unsigned long unknown           | 0h        | 8h    | 4h   | Fg: Bg: [yellow]           |
| ... unsigned long size_data         | 44h       | Ch    | 4h   | Fg: Bg: [blue]             |
| ... unsigned long next_block        | FBC0A562h | 10h   | 4h   | Fg: Bg: [red]              |
| ... unsigned char data[68]          |           | 14h   | 44h  | Fg: [dark blue] Bg: [grey] |

Win32/Alureon.FE – virus, ki dobiva ukaze preko slik objavljenih na spletnih forumih. Slike vsebujejo steganografska sporočila.

Trojan:Win32/Alureon.FE is a trojan that installs other variants of Win32/Alureon, a family of data-stealing trojans. These trojans allow an attacker to intercept incoming and outgoing Internet traffic in order to gather confidential information such as user names, passwords, and credit card data. It may also allow an attacker to transmit malicious data to the infected computer. The trojan may modify DNS settings on the host computer to enable the attacker to perform these tasks. As a result, it may be necessary to reconfigure DNS settings after disinfection. Trojan:Win32/Alureon.FE also modifies the MBR to execute installed Alureon components.

# Vdori



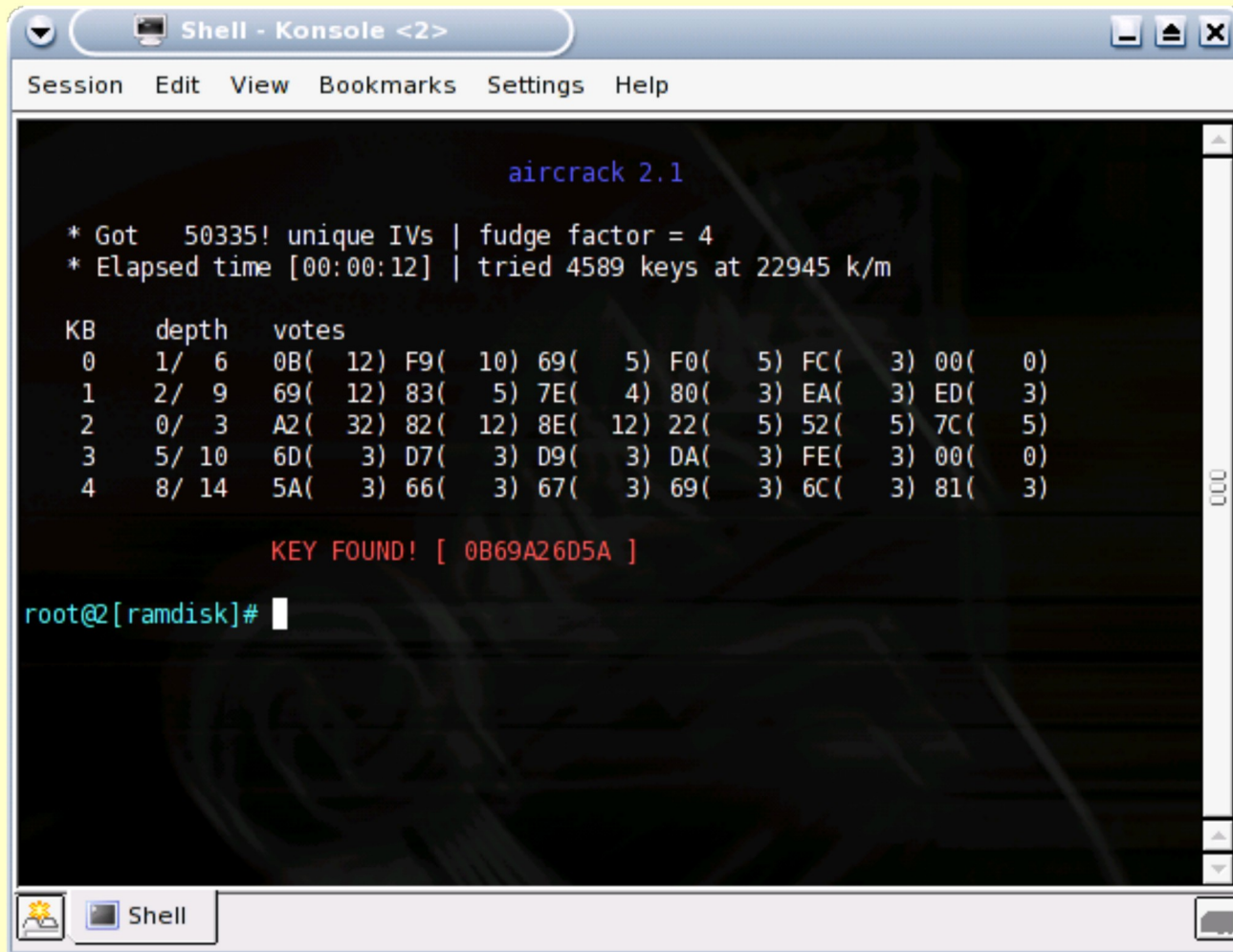
[Primer vdora v poštno banko v Haifi.]





<http://theplugbot.com/>

# Ranljivi niso samo računalniki



```
Shell - Konsole <2>
Session Edit View Bookmarks Settings Help

aircrack 2.1

* Got 50335! unique IVs | fudge factor = 4
* Elapsed time [00:00:12] | tried 4589 keys at 22945 k/m

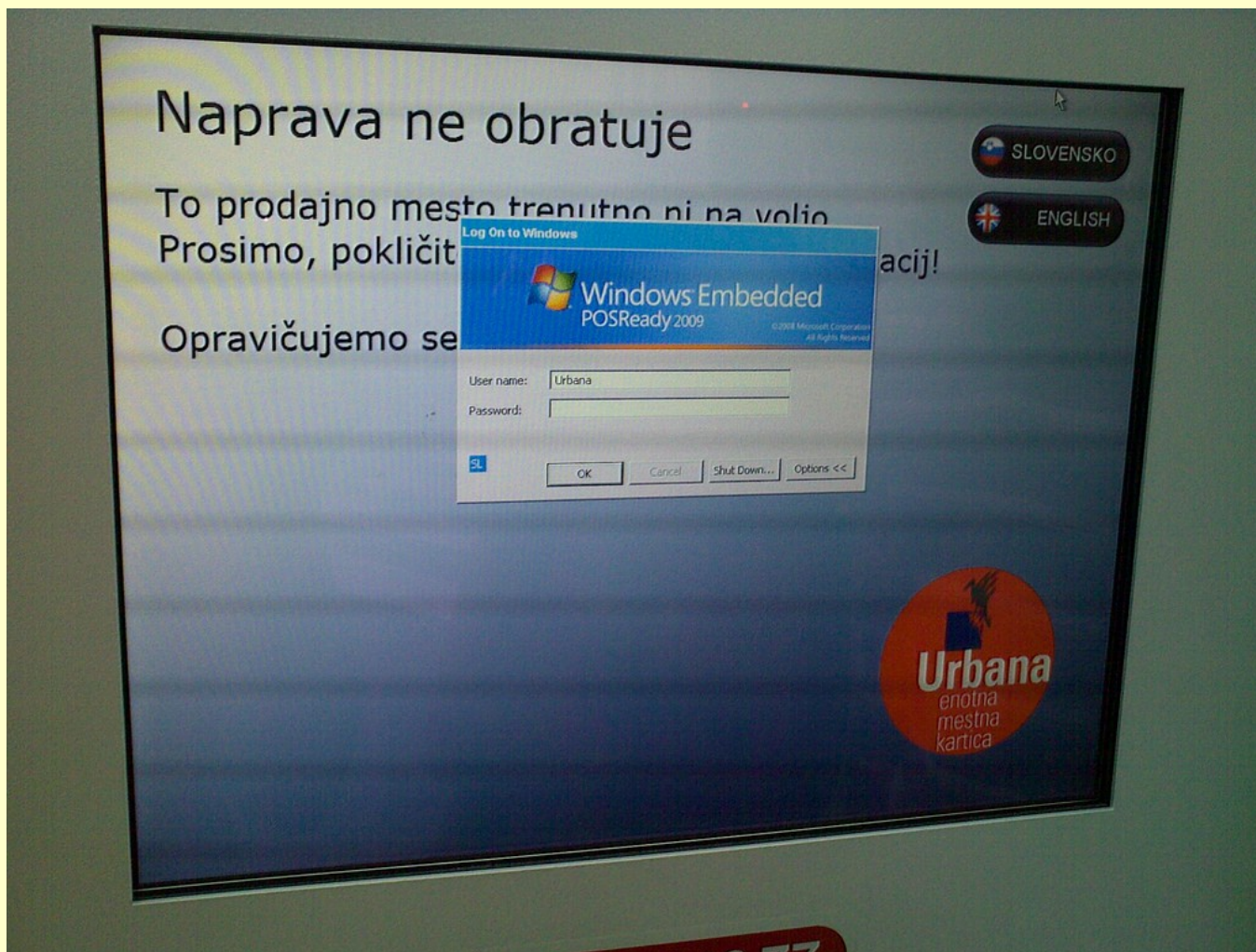
KB   depth  votes
0    1/ 6    0B( 12) F9( 10) 69( 5) F0( 5) FC( 3) 00( 0)
1    2/ 9    69( 12) 83( 5) 7E( 4) 80( 3) EA( 3) ED( 3)
2    0/ 3    A2( 32) 82( 12) 8E( 12) 22( 5) 52( 5) 7C( 5)
3    5/ 10   6D( 3) D7( 3) D9( 3) DA( 3) FE( 3) 00( 0)
4    8/ 14   5A( 3) 66( 3) 67( 3) 69( 3) 6C( 3) 81( 3)

KEY FOUND! [ 0B69A26D5A ]

root@[ramdisk]#
```

Napad na brezžično omrežje.

# Ranljivi niso samo računalniki



# Ranljivi niso samo računalniki



Napad na TV oddajnik.

# Ranljivi niso samo računalniki



Napad na tiskalnik.

# Ranljivi niso samo računalniki

The screenshot shows a web browser window displaying the 'Tenovis WebTerminal' interface. The browser's address bar shows the URL `http://10.254.60.43/index.html`. The page content includes the 'AVAYA' logo, a 'WebTerminal' section with a PIN input field (containing '\*\*\*\*'), a 'Status Connected' indicator, and an 'Abort' button. Below this is a 'goahead WEB SERVER' logo. A system message at the bottom of the browser says 'Applet started.'

Overlaid on the browser is a 'T3IP WebTerminal : mainmenu' window. It displays system information: 'Own call number: 5711', 'MAC address: 00-04-0d-f5-09-6a', 'Application file: T112\_Sp3.bin', and 'Boot- file: T100'. It features buttons for 'Bootline', 'Registration & admission', and 'IP audio settings', each with a corresponding status indicator. At the bottom, there are 'Send data' and 'Cancel' buttons, and a message: 'VoIP Manager active: Configuration access limited!'

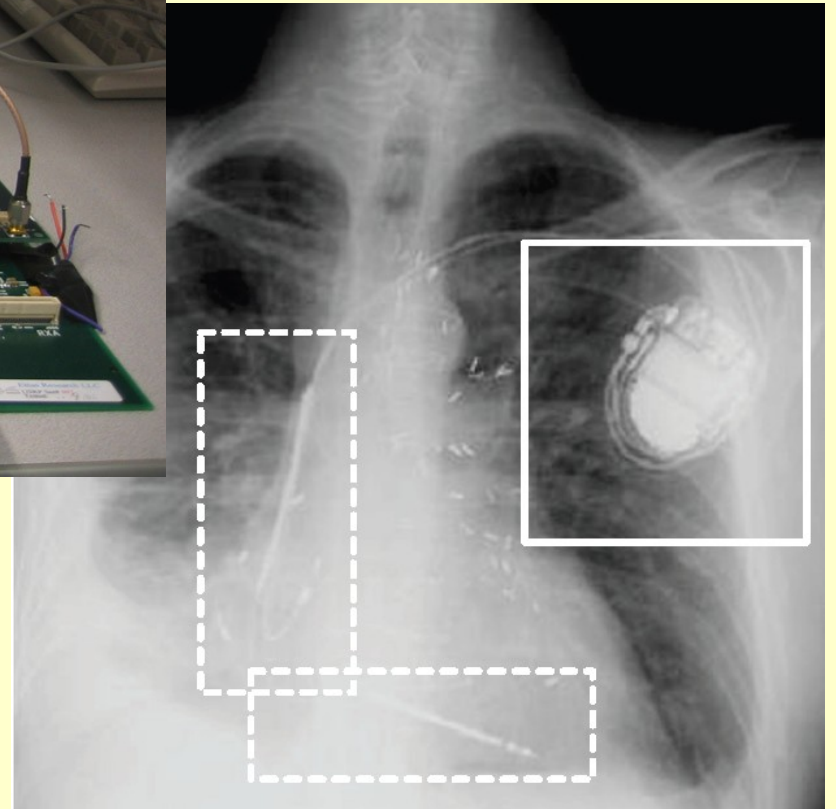
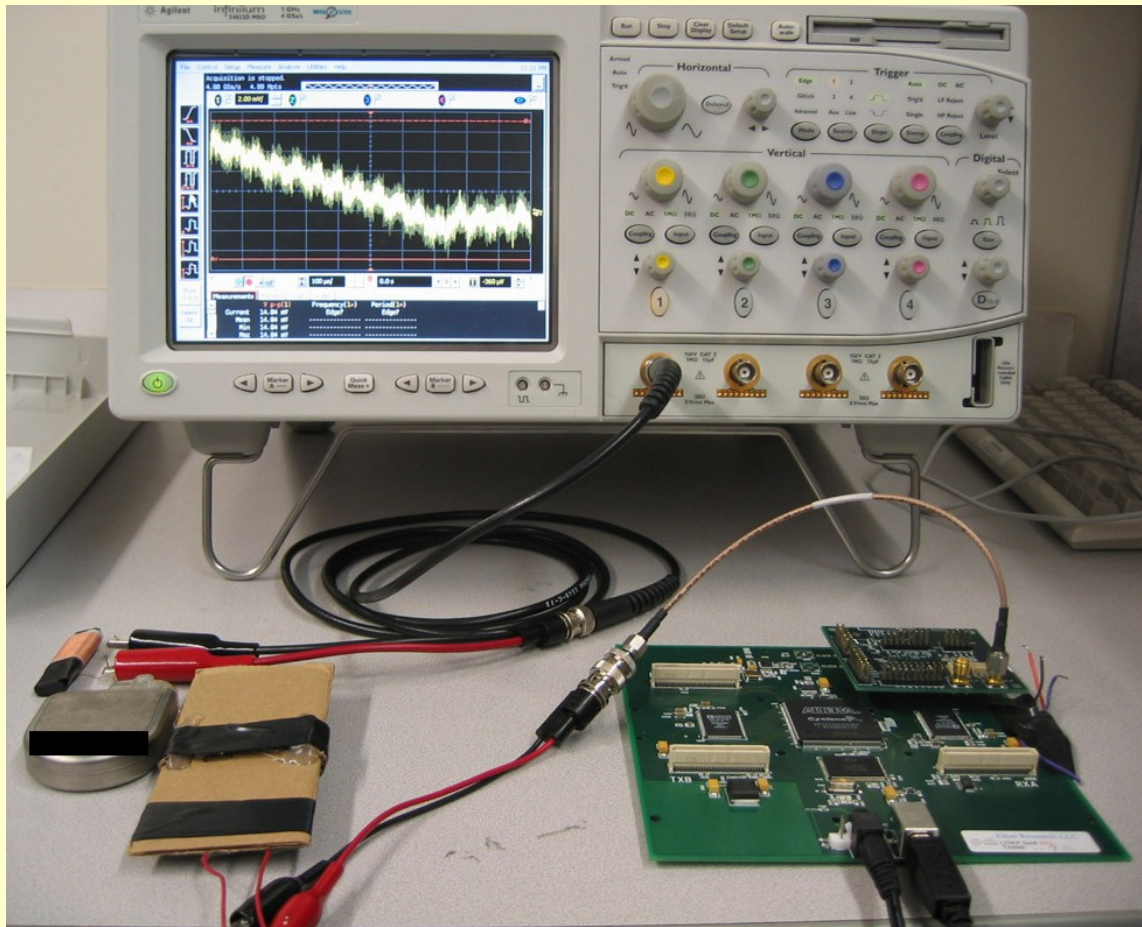
A terminal window titled 'matej@cryptopia: ~' is also overlaid, showing the execution of an nmap scan: `nmap 10.254.60.43`. The output indicates the host is up and port 80/tcp is open with an http service.

The system tray at the bottom shows the user 'matej@cryptopia' and a notification 'Retrieving your IP address.... Anonimizacija izključena'.

Napad na VOIP telefon.

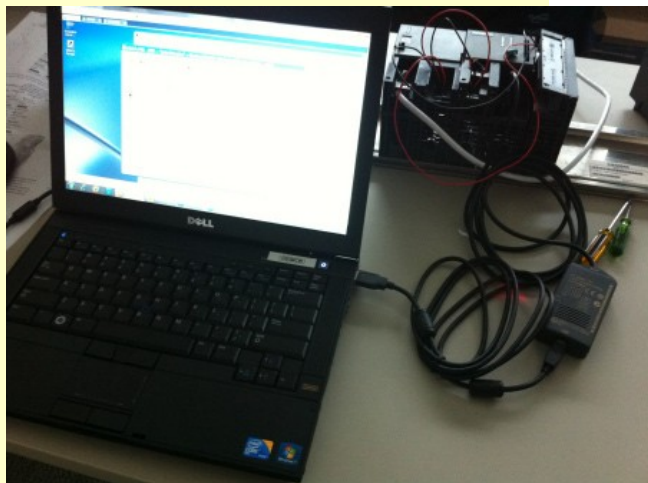
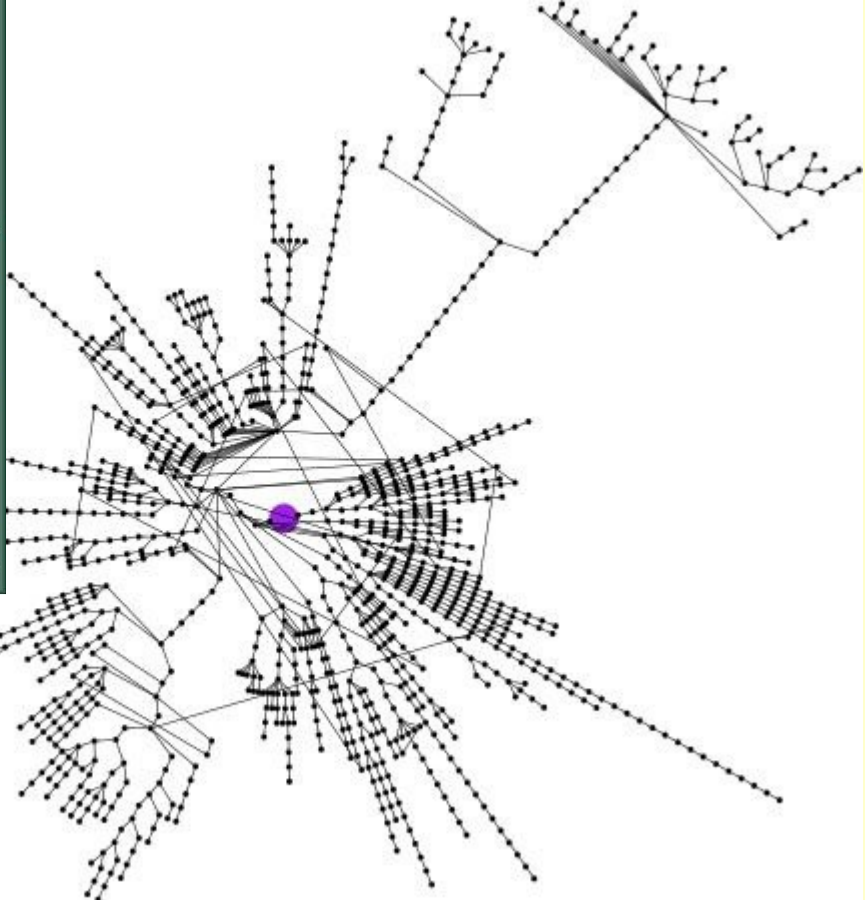
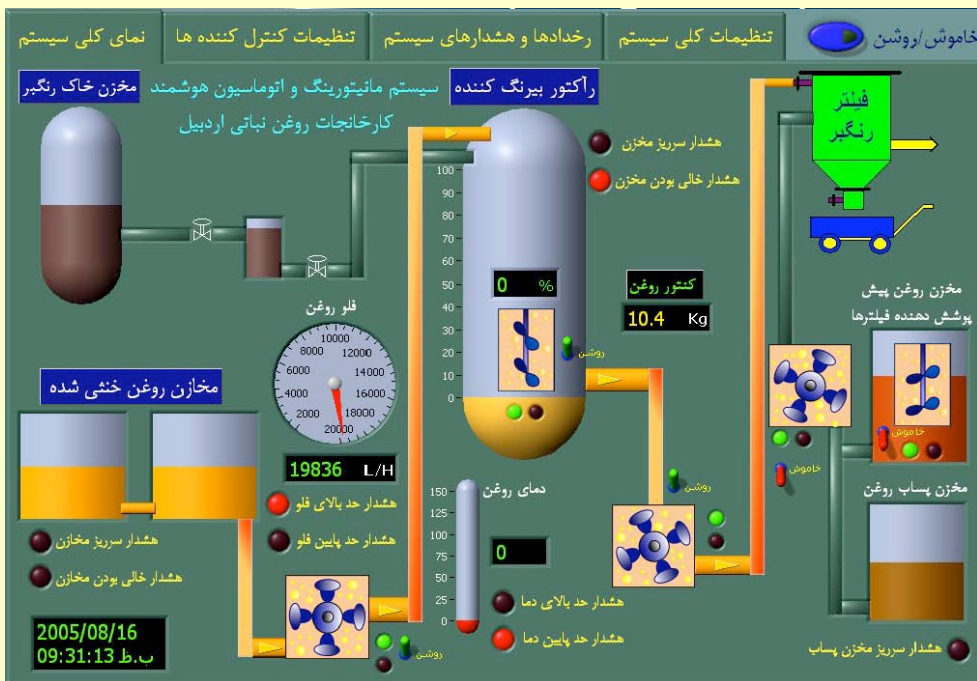


Napad na RFID potne liste.



Napad na srčni spodbujevalnik.

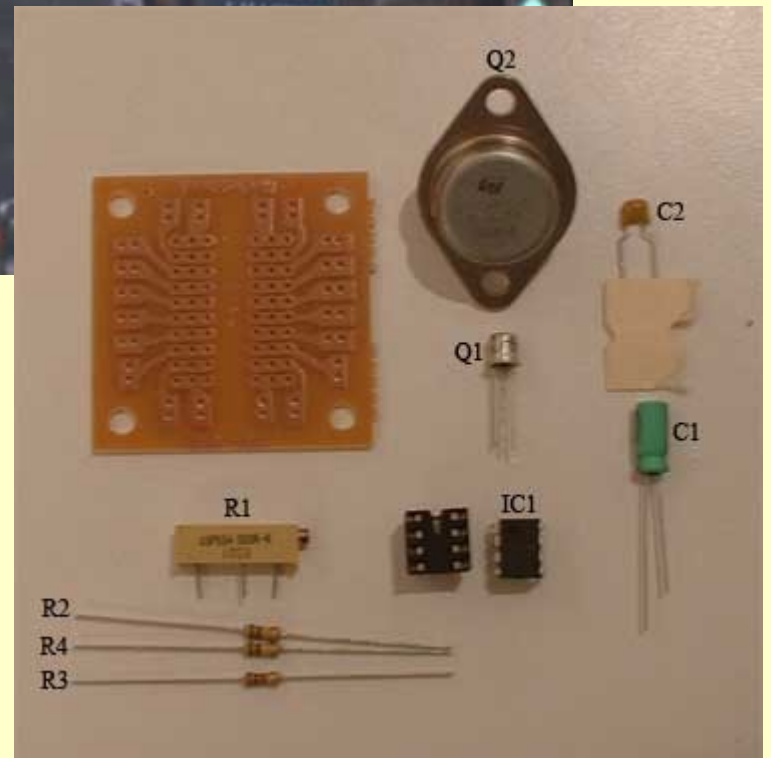




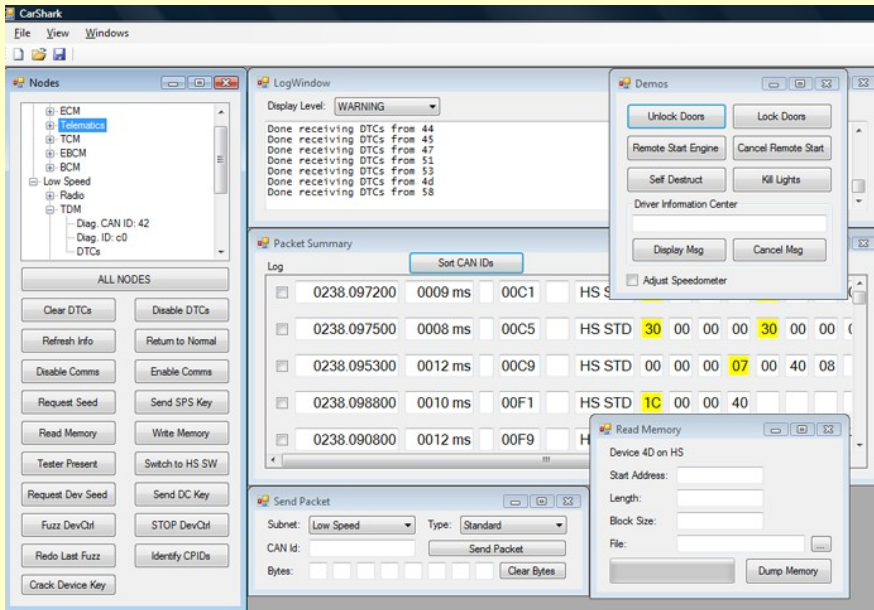
Napadi na SCADA sisteme.

David Maynor in Robert Graham. 2006. SCADA Security and Terrorism: We're not crying wolf.  
 <<https://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf>>

Nicolas Falliere, Liam O Murchu in Eric Chien (Symantec Security). 2011. W32.Stuxnet Dossier.  
 <[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/w32\\_stuxnet\\_dossier.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf)>



Napad na semaforje.  
[Napad na tramvaj.]



Napad na automobile.

<<http://www.autosec.org/pubs/cars-oakland2010.pdf>>

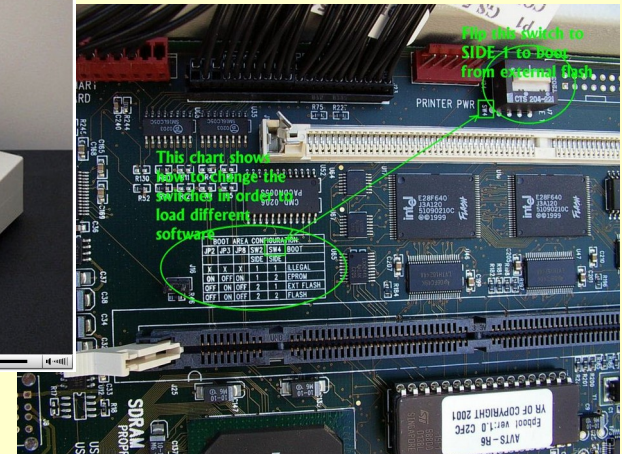
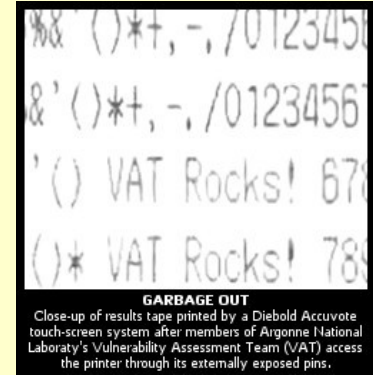


Napad na prometne znake.



Vir in avtorstvo: i.hacked.com,  
<<http://www.i-hacked.com/content/view/274/48/>>

# Napadi na e-volitve



Napad na volilne naprave.

# Napadi na bankomate



Napadi na bankomate.

# Napadi na mobilno telefonijo

The image is a composite of three parts illustrating mobile phone attacks:

- Top Left:** A photograph of a silver Samsung Ektomon mobile phone connected to a computer via a USB cable. A second mobile phone is shown below it.
- Top Right:** A terminal window titled 'matej@cryptopia: ~' showing a list of commands for SIM card manipulation:

```
testcard  Attach built in test SIM
spoofer   Attach spoofing SIM
reader    Attach SIM from reader
remove    Detach SIM card
pin       Enter PIN for SIM card
disable-pin  Disable PIN of SIM card
enable-pin  Enable PIN of SIM card
change-pin Change PIN of SIM card
unlock-pin Change PIN of SIM card
lai       Change LAI of SIM card
```

Below the list, there are several lines of command execution output, including 'OsmocomBB# sin spo', 'OsmocomBB# sin spoofer', and 'OsmocomBB# sin spoofer 1 293...'.  
At the bottom of the terminal, there are two lines of system information:

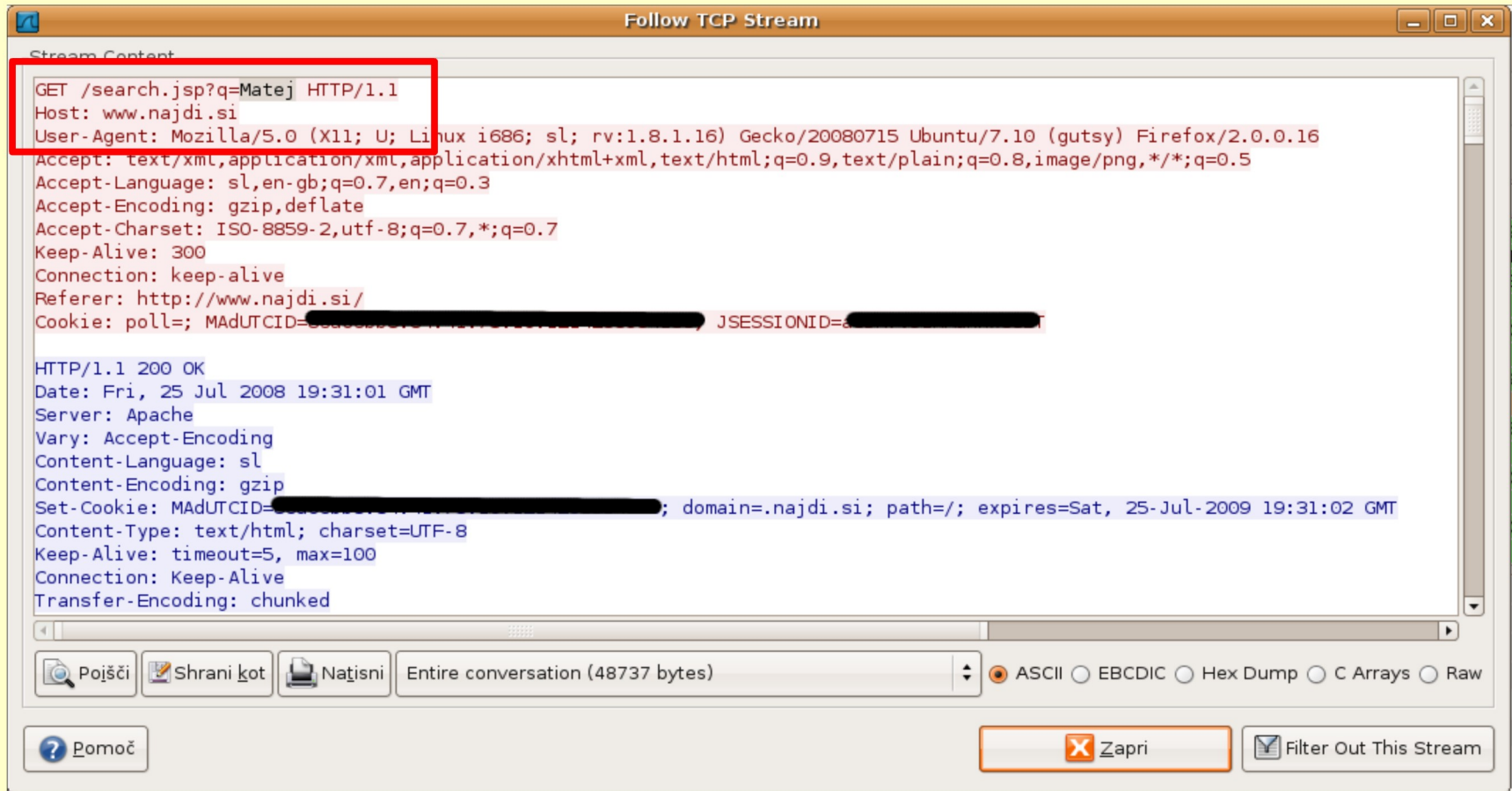
```
81 U, func=UI(DTAP) (RR) System Information type 3
81 U, func=UI(DTAP) (RR) Measurement Report
```
- Bottom:** A network traffic analysis tool (likely Wireshark) showing a packet capture. The selected packet is an SMS (GSM SMS) with the following details:
  - Destination: 170 3.553861000, 127.0.0.1, 127.0.0.1, LAPDm
  - Destination: 171 3.559612000, 127.0.0.1, 127.0.0.1, LAPDm
  - TP-User-Data-Length: (81) depends on Data-Coding-Scheme
  - TP-User-Data: SMS text: Najdi.si SMS (od 046...): test\n(Mobitelova mobilna stran http://m.mobitel.si )The 'TP-User-Data' section is highlighted with a red box. Below the details, there is a hex dump of the packet data.

Napadi na mobilno telefonijo,  
<<https://pravokator.si/index.php/varnost-gsm/>>

# **Prestrezanje komunikacij**



# Zakaj šifriranje?



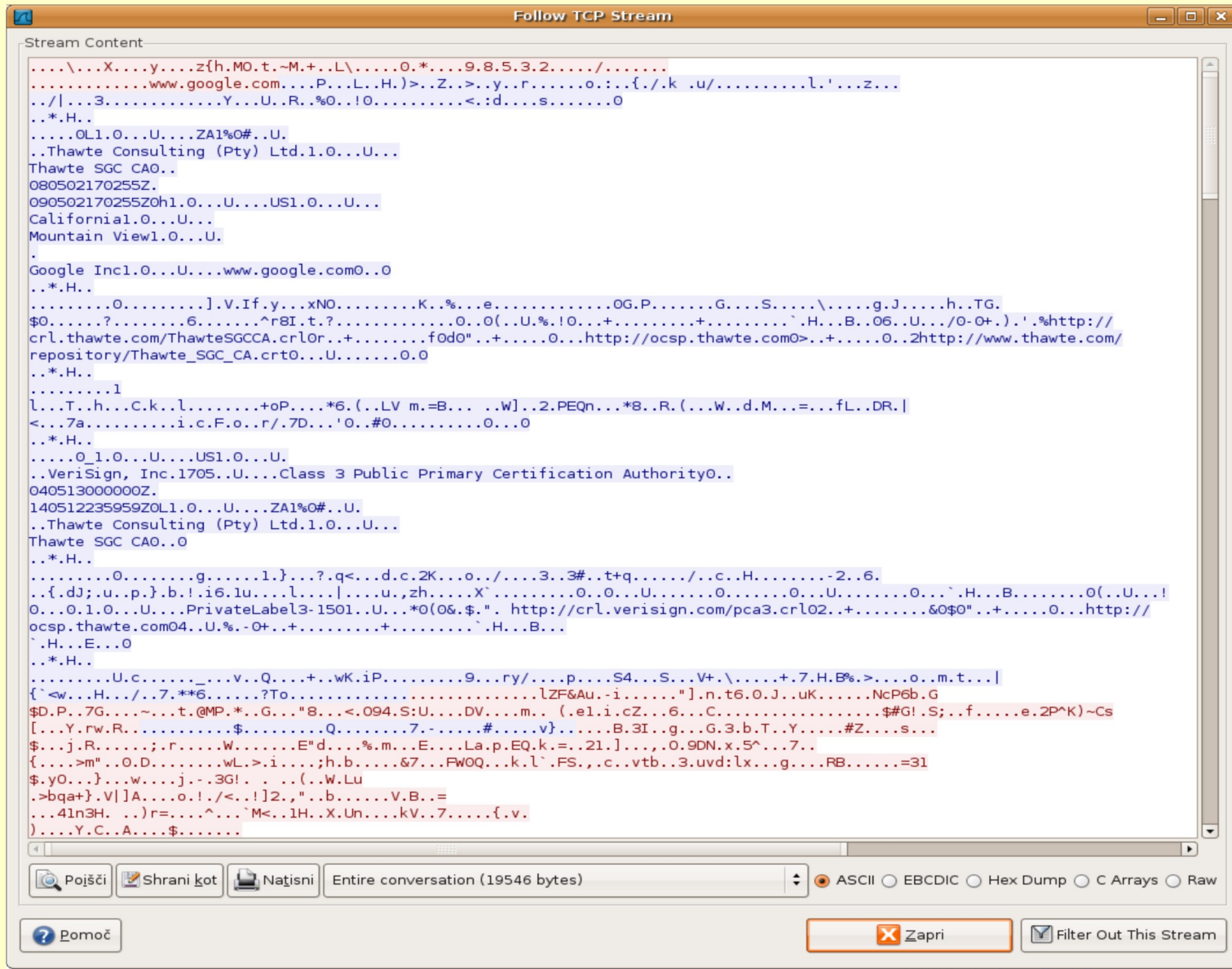
The screenshot shows a window titled "Follow TCP Stream" displaying the raw text of an HTTP transaction. The request is highlighted with a red box and includes the following fields: GET /search.jsp?q=Matej HTTP/1.1, Host: www.najdi.si, and User-Agent: Mozilla/5.0 (X11; U; Linux i686; sl; rv:1.8.1.16) Gecko/20080715 Ubuntu/7.10 (gutsy) Firefox/2.0.0.16. The response includes headers such as Date: Fri, 25 Jul 2008 19:31:01 GMT, Server: Apache, and Content-Type: text/html; charset=UTF-8. The status line is HTTP/1.1 200 OK. The interface also features a search bar, a file save button, and a status bar indicating the entire conversation is 48737 bytes.

```
Stream Content
GET /search.jsp?q=Matej HTTP/1.1
Host: www.najdi.si
User-Agent: Mozilla/5.0 (X11; U; Linux i686; sl; rv:1.8.1.16) Gecko/20080715 Ubuntu/7.10 (gutsy) Firefox/2.0.0.16
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: sl,en-gb;q=0.7,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-2,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.najdi.si/
Cookie: poll=; MADUTCID=; JSESSIONID=

HTTP/1.1 200 OK
Date: Fri, 25 Jul 2008 19:31:01 GMT
Server: Apache
Vary: Accept-Encoding
Content-Language: sl
Content-Encoding: gzip
Set-Cookie: MADUTCID=; domain=.najdi.si; path=/; expires=Sat, 25-Jul-2009 19:31:02 GMT
Content-Type: text/html; charset=UTF-8
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked

Pojšči Shrani kot Našisni Entire conversation (48737 bytes)
Pomoč Zapri Filter Out This Stream
```

Nešifrirana spletna komunikacija.



Šifrirana spletna komunikacija.

# Analiza omrežnega prometa

|     |            |                 |                 |      |   |
|-----|------------|-----------------|-----------------|------|---|
| 921 | 145.190913 | 193. [REDACTED] | 91. [REDACTED]  | TCP  | [REDACTED] smtp [ACK] Seq=79 Ack=219 Win=6432 Len=0   |
| 922 | 145.196186 | 193. [REDACTED] | 91. [REDACTED]  | SMTP | Command: MAIL FROM:<matej.kovacic@[REDACTED]> [ZE=411 |
| 923 | 145.197425 | 91. [REDACTED]  | 193. [REDACTED] | SMTP | Response: 250 OK                                      |
| 924 | 145.197644 | 193. [REDACTED] | 91. [REDACTED]  | SMTP | Command: RCPT TO:<matej.kovacic@[REDACTED]>           |
| 925 | 145.228297 | 91. [REDACTED]  | 193. [REDACTED] | SMTP | Response: 250 OK                                      |
| 926 | 145.228621 | 193. [REDACTED] | 91. [REDACTED]  | SMTP | Command: DATA   |
| 927 | 145.229646 | 91. [REDACTED]  | 193. [REDACTED] | SMTP | Response: 354 Enter message, ending with "." on a li  |
| 928 | 145.236472 | 193. [REDACTED] | 91. [REDACTED]  | SMTP | DATA fragment, 414 bytes                              |
| 929 | 145.243559 | 91. [REDACTED]  | 193. [REDACTED] | SMTP | Response: 250 OK id=1KMGLN-0001x3-7M                  |
| 930 | 145.246496 | 193. [REDACTED] | 91. [REDACTED]  | SMTP | DATA fragment, 6 bytes                                |
| 931 | 145.247380 | 91. [REDACTED]  | 193. [REDACTED] | SMTP | Response: 221 [REDACTED] closing connection           |
| 932 | 145.247621 | 91. [REDACTED]  | 193. [REDACTED] | TCP  | smtp > 43389 [FIN, ACK] Seq=396 Ack=583 Win=6432 Len= |
| 933 | 145.287572 | 193. [REDACTED] | 91. [REDACTED]  | TCP  | 43389 > smtp [ACK] Seq=583 Ack=397 Win=6432 Len=0     |
| 934 | 145.403764 | 193. [REDACTED] | 91. [REDACTED]  | TCP  | 43389 > smtp [FIN, ACK] Seq=583 Ack=397 Win=6432 Len= |
| 935 | 145.404693 | 91. [REDACTED]  | 193. [REDACTED] | TCP  | smtp > 43389 [ACK] Seq=397 Ack=584 Win=6432 Len=0     |

Frame 919 (111 bytes on wire, 111 bytes captured)

Ethernet II, Src: [REDACTED] ([REDACTED]), Dst: [REDACTED] ([REDACTED])

Internet Protocol, Src: 193. [REDACTED] (193. [REDACTED]), Dst: 91. [REDACTED] (91. [REDACTED])

Transmission Control Protocol, Src Port: 43389 (43389), Dst Port: smtp (25), Seq: 21, Ack: 219, Len: 57

SMTP, Mailbox: [REDACTED]

Command: AUTH PLAIN AG1hdGVqLmtvdmFjaWNAKioqKiouc2kAZ2VzbG8hrG==\r\n

Command: AUTH PLAIN AG1hdGVqLmtvdmFjaWNAKioqKiouc2kAZ2VzbG8hrG==

**Uporabniško ime in geslo sta Base64 kodirana...**

Command: AUTH PLAIN matej.kovacic@\*\*\*\*.si|geslo!

# Omrežna analiza VoIP komunikacij

The image displays two windows used for VoIP analysis. The top window is Wireshark, showing a packet capture of SIP messages. The bottom window is RTP Player, showing the audio waveform for a selected packet.

**Wireshark - sip.pcap**

Filter: sip

| No. . | Time      | Source | Destination | Protocol | Info                                      |
|-------|-----------|--------|-------------|----------|---|
| 69    | 14.865457 | 153.5  | 212.1       | SIP/XML  | Request: PUBLISH sip: [redacted]@212.1    |
| 72    | 16.867222 | 153.5  | 212.1       | SIP/XML  | Request: PUBLISH sip: [redacted]@212.1    |
| 82    | 23.453253 | 153.5  | 212.1       | SIP/SDP  | Request: INVITE sip:015805373@212.1, with |
| 83    | 23.461385 | 212.1  | 153.5       | SIP      | Status: 100 Trying                        |
| 84    | 23.466803 | 212.1  | 153.5       | SIP      | Status: 401 Unauthorized                  |
| 85    | 23.475217 | 153.5  | 212.1       | SIP      | Request: ACK sip:015805373@212.1          |
| 86    | 23.530435 | 153.5  | 212.1       | SIP/SDP  | Request: INVITE sip:015805373@212.1 with  |
| 87    | 23.535845 | 212.1  | 153.5       | SIP      | Status: 100 Trying                        |
| 89    | 24.572367 | 212.1  | 153.5       | SIP      | Status: 180 Ringing                       |
| 92    | 25.651003 | 153.5  | 212.1       | SIP      | Request: CANCEL sip:015805373@212.1       |
| 93    | 25.760161 | 212.1  | 153.5       | SIP      | Status: 200 OK                            |
| 94    | 25.769395 | 212.1  | 153.5       | SIP      | Status: 487 Request Cancelled             |
| 97    | 25.985041 | 153.5  | 212.1       | SIP      | Request: ACK sip:015805373@212.1          |

**Packet 82 Details:**

- Frame 82 (1219 bytes on wire, 1219 bytes captured)
- Ethernet II, Src: [redacted]
- Internet Protocol, Src: [redacted]
- User Datagram Protocol, Src Port: sip (5060), Dst: [redacted]
- Session Initiation Protocol

**Packet 82 Payload (Hex):**

```
0000 00 18 73 a3 4e 48 00 15 af e5 25 c8 08 00 45
0010 04 b5 00 00 40 00 40 11 5f 95 99 05 85 5b d4
0020 e4 34 13 c4 13 c4 04 a1 de c4 49 4e 56 49 54
0030
0040
0050
0060 20 32 38 20 4d 61 79 20 32 30 30 39 20 31 32
0070 32 36 3a 35 31 20 47 4d 54 0d 0a 43 53 65 71
0080 20 31 20 49 4e 56 49 54 45 0d 0a 56 69 61 3a
```

File: "/media/MATEJ/sip.pcap" 31 KB 00:00:32

**VoIP - RTP Player (sip\_govor.pcap)**

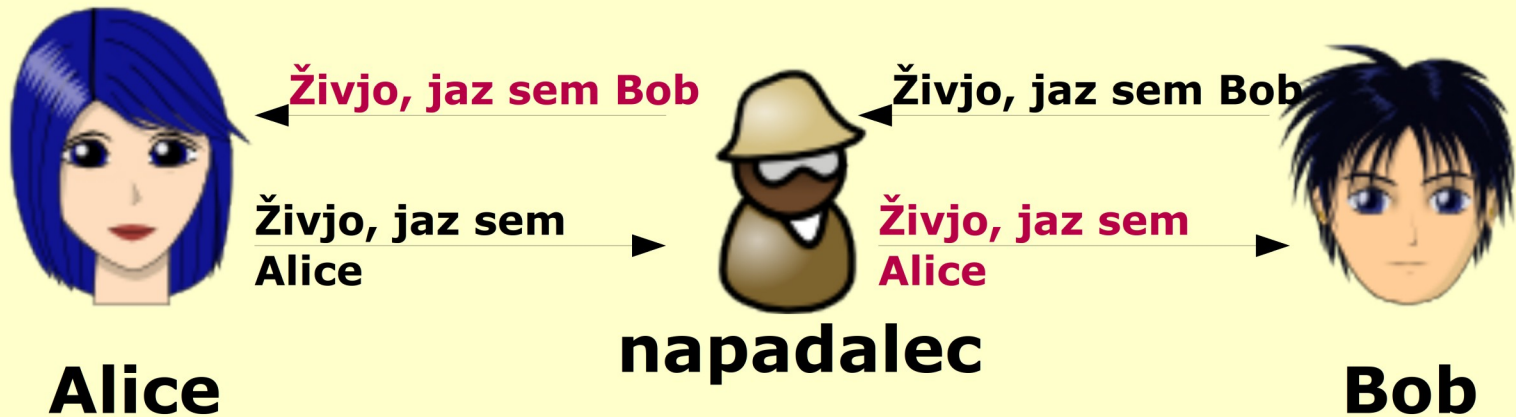
Duration: 11.76 Drop by jitter Buff: 0(0,0%) Out of Seq: 0(0,0%)

Duration: 12.04 Drop by jitter Buff: 0(0,0%) Out of Seq: 1(0,2%)

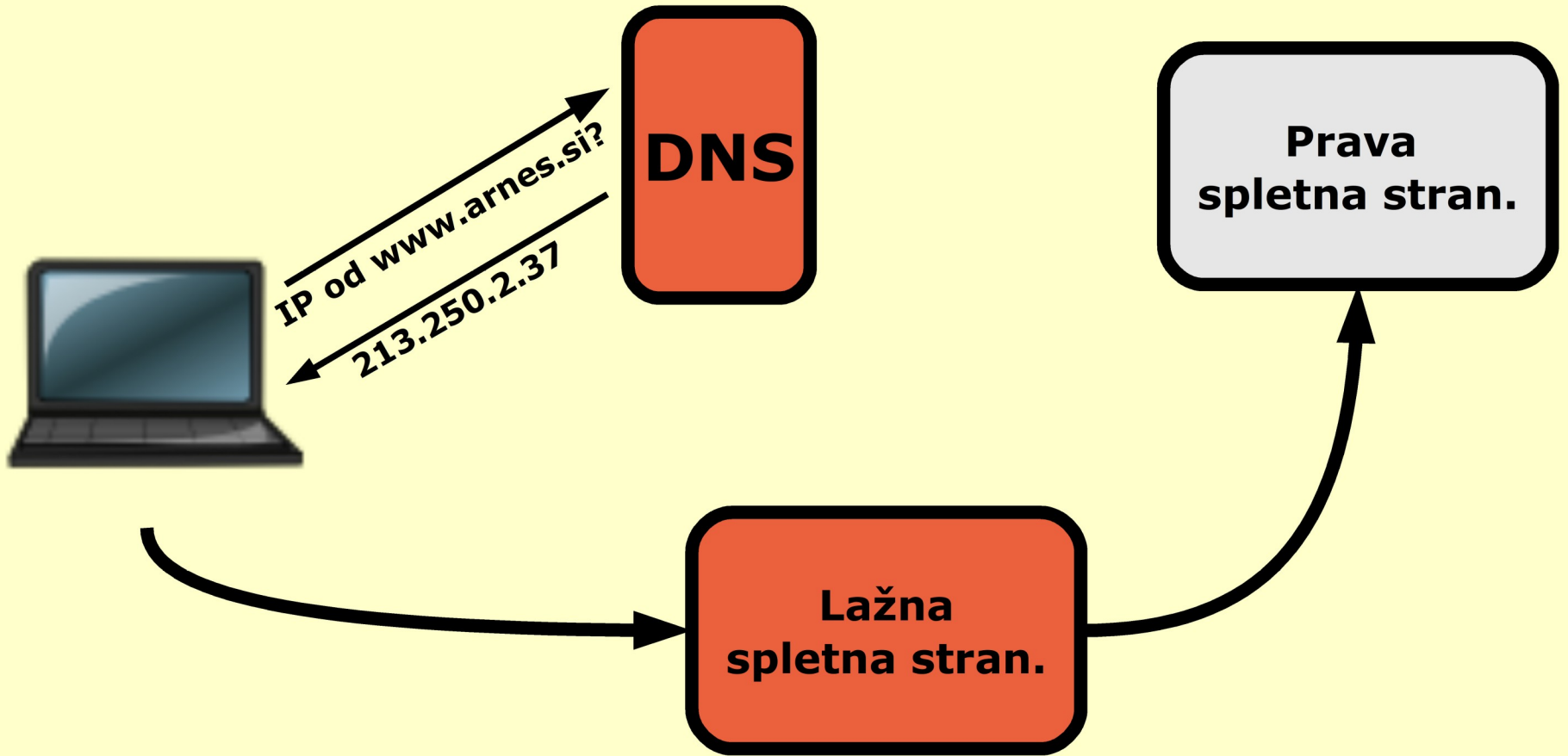
Jitter buffer [ms]: 50

Buttons: Decode, Play, Pause, Stop, Zapri

# Napad s posrednikom (MITM napad)



# DNS preusmerjanje





## Spletno stran je certificirala neznana uradna oseba za certifikate (CA)



Ne morem preveriti identitete strani `posta.owca.info` kot strani, ki ji zaupam.

Možni razlogi za to napako:

- Vaš brskalnik ne prepozna uradne osebe za certifikate (CA), ki je izdala certifikat tej strani
- Certifikat te strani ni popoln zaradi nepravilnih nastavitvev strežnika
- Povezani ste s stranjo, ki se pretvarja, da je `posta.owca.info`, morda zato, da bi si pridobila vaše zaupne podatke.

Prosim, obvestite vzdrževalca strani o tem problemu.

Preden sprejmete ta certifikat, ga morate podrobno pregledati. Ste pripravljeni sprejeti ta certifikat v namene identifikacije spletne strani `posta.owca.info`?

Preveri certifikat ...

- Ta certifikat sprejmi za vedno
- Ta certifikat sprejmi začasno, le za to sejo
- Tega certifikata ne sprejmi in se ne poveži s to spletno stranjo

Prekliči

V redu

# MITM napad na DECT protokol

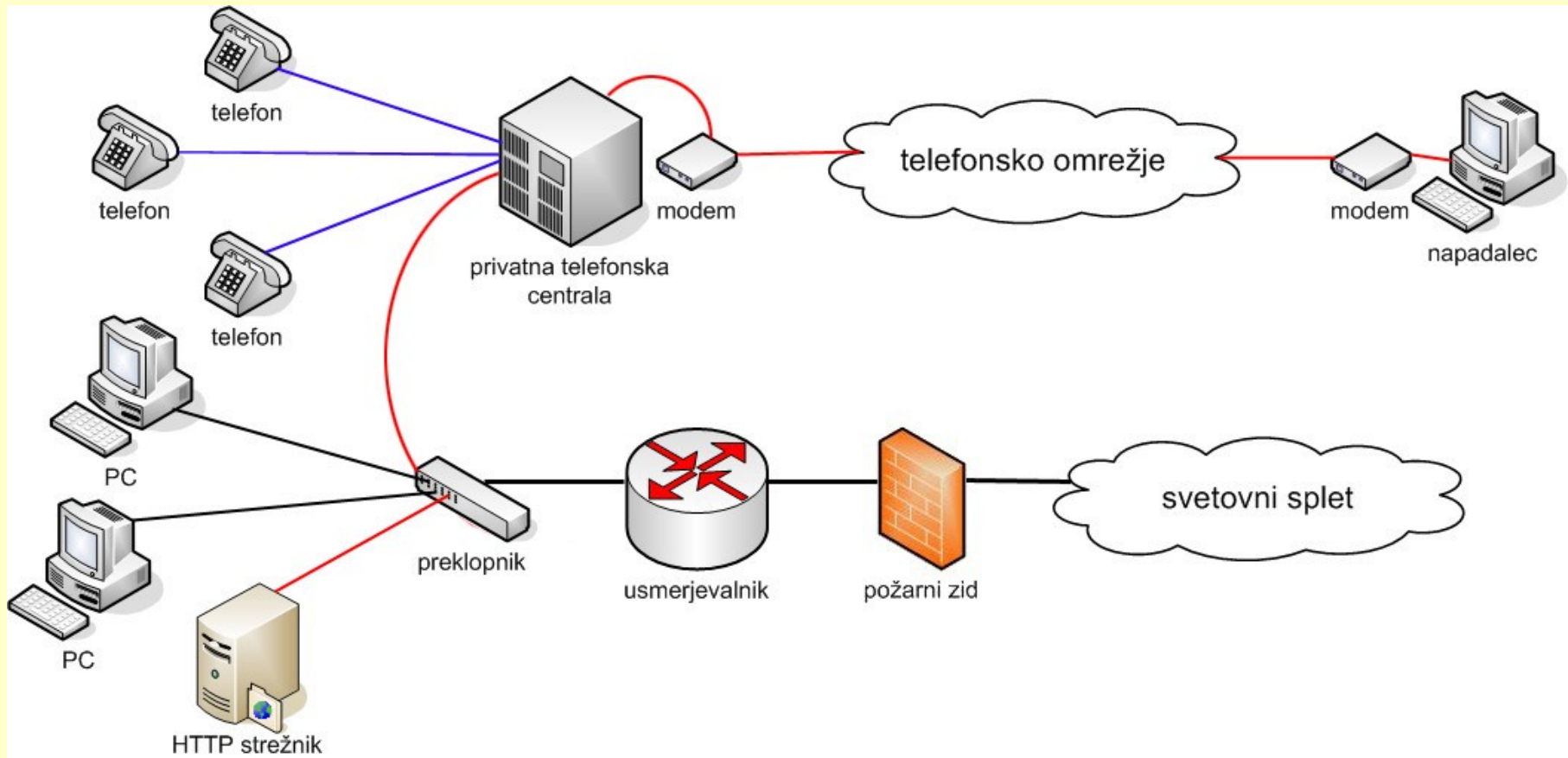
- DECT je protokol, ki se uporablja za zaščito brezžičnih komunikacij pred prisluškovanjem. Uporablja se pri domačih brezžičnih telefonih, pri otroških telefonih (baby phone), sistemih za odpiranje vrat, klicih v sili, brezžičnih čitalcih bančnih kartic, itd..
- Leta 2008 so raziskovalci ugotovili, da je DECT mogoče razbiti s pomočjo navadnega računalnika z operacijskim sistemom Linux ter kartico *ComOnAir*.



Vir in avtorstvo: dedected.org



# Je dostop do lokalnega omrežja res zavarovan?



**Javni ali zasebni prostor?**

# Socialna omrežja: zasebni ali javni prostor?

(8 of 10)



06/11/07

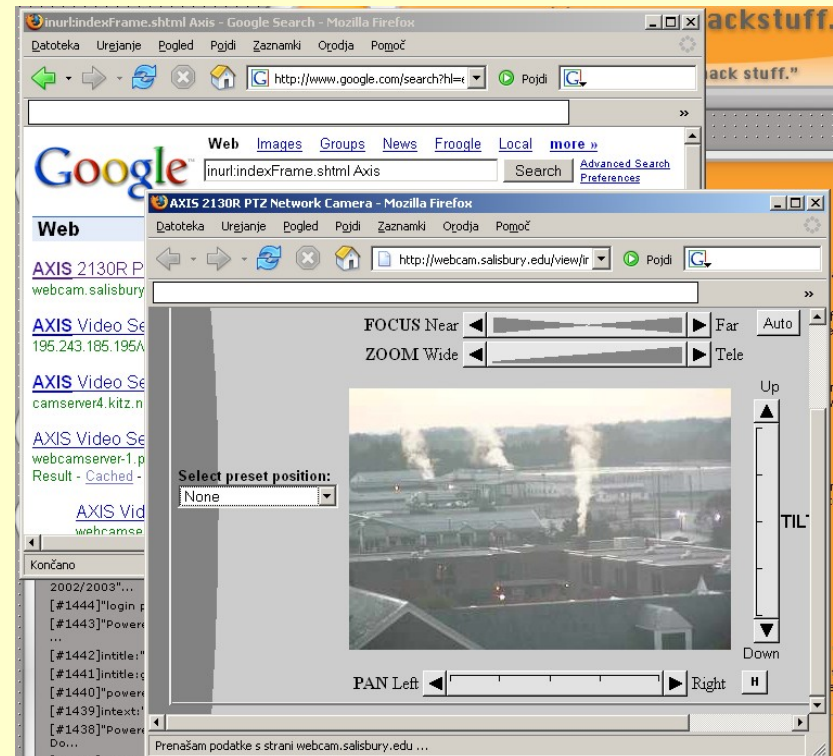


# **Ko zaseben podatek postane *javen***

- McVeigh v. Cohen, 983 F.Supp. 215 (1998).  
Mornariški častnik je v svoj AOL profil vpisal, da je gej, s čimer naj bi kršil politiko "*don't ask, don't tell*".
- "Prikrito" zbiranje osebnih podatkov: Google Toolbar, ki zabeleži vsebino "zasebnih" strani.
- Preprodaja osebnih podatkov in oddaja zunanjim izvajalcem (Toysmart, "outsourcing" vnosa medicinskih kartotek v Indijo).
- Zbiranje javno dostopnih podatkov, Whois baza, "Google hacking")

# “Google hacking”

- Vincent Gaillot, How to use Google to find confidential informations, 2001  
<<http://archive.cert.uni-stuttgart.de/archive/bugtraq/2001/11/msg00135.html>>.
- Johnny Long, Watching the Watchers, Defcon, 2003.
- Leta 2004 izide knjiga Google Hacking for Penetration Testers.
- Google Hacking Database (GHDB).





site:www.fdvinfo.net filetype:xls  Isk

Išči po:  celotnem spletu  straneh v državi Slovenija

Splet

[www.fdvinfo.net/uploads/editor/1169747348razpis%20...](http://www.fdvinfo.net/uploads/editor/1169747348razpis%20...) - 30 sep

[Podobne strani](#)

[www.fdvinfo.net/uploads/editor/timing\\_ure\\_v03.xls](http://www.fdvinfo.net/uploads/editor/timing_ure_v03.xls)

[Podobne strani](#)

[www.fdvinfo.net/uploads/editor/orepma1.xls](http://www.fdvinfo.net/uploads/editor/orepma1.xls)

[Podobne strani](#)

[www.fdvinfo.net/uploads/editor/1213891276imenik\\_re...](http://www.fdvinfo.net/uploads/editor/1213891276imenik_re...)

[Podobne strani](#)

[www.fdvinfo.net/uploads/editor/1167984701seznam-pr...](http://www.fdvinfo.net/uploads/editor/1167984701seznam-pr...) - 30 sep

[Podobne strani](#)

[www.fdvinfo.net/uploads/editor/paket%2012-drugi.xls](http://www.fdvinfo.net/uploads/editor/paket%2012-drugi.xls)

[Podobne strani](#)

[www.fdvinfo.net/uploads/editor/1167984737seznam-pr...](http://www.fdvinfo.net/uploads/editor/1167984737seznam-pr...)

[Podobne strani](#)

[www.fdvinfo.net/uploads/editor/timing\\_v02.xls](http://www.fdvinfo.net/uploads/editor/timing_v02.xls) - 30 sep

[Podobne strani](#)

[www.fdvinfo.net/uploads/editor/1160116879seznam-pr...](http://www.fdvinfo.net/uploads/editor/1160116879seznam-pr...)

[Podobne strani](#)

[www.fdvinfo.net/uploads/editor/1170236210FDV teme ...](http://www.fdvinfo.net/uploads/editor/1170236210FDV teme ...)

[Podobne strani](#)

orepma1 (samo za branje) - OpenOffice.org Calc

Datoteka Uredi Pogled Vstavi Oblika Orodja Podatki Okno Pomoč

|    | A      | B                 | C      | D     | E     | F                                 | G | H |
|----|--------|-------------------|--------|-------|-------|-----------------------------------|---|---|
| 4  |        |                   |        |       |       |                                   |   |   |
| 5  | KDO    | KAJ               | KOLIKO | Z DDV |       | VIR                               |   |   |
| 6  | mvar   | pc z monitorjem19 | 548    | 657,6 |       |                                   |   |   |
| 7  | nusa   | notebook 9105     | 334    | 400,8 |       |                                   |   |   |
| 8  | vasja  | notebook 5000     | 386    | 463,2 | 463   | ird w plus 29807 MID vir (ne MZT) |   |   |
| 9  | gregor | server            | 432    | 518,4 | 172,8 | ird w                             |   |   |
| 10 |        | dodatki za server | 140    | 168   |       |                                   |   |   |
| 11 | vasja  | tiskalnik         | 72     | 86,4  | 85    | ird w                             |   |   |
| 12 | gregor | pc+dodatki        | 140    | 168   |       |                                   |   |   |
| 13 | kejzar | pc                | 117    | 140,4 |       |                                   |   |   |
| 14 | vasja  | pc+dodatki        | 130    | 156   | 156   | ird w                             |   |   |
| 15 | vasja  | monitor19         | 95     | 114   | 114   | ird w                             |   |   |
| 16 | gregor | mor               |        |       |       |                                   |   |   |
| 17 | natasa | mor               |        |       |       |                                   |   |   |
| 18 | katja  | scar              |        |       |       |                                   |   |   |

Delovni list 1 / 3 P

timing\_ure\_v03 (samo za branje) - OpenOffice.org Calc

Datoteka Uredi Pogled Vstavi Oblika Orodja Podatki Okno Pomoč

|   | O   | P    | Q               | R                     | S               | T    | U       | V   |
|---|-----|------|-----------------|-----------------------|-----------------|------|---------|-----|
| 1 |     |      |                 | Finančna konstrukcija |                 |      |         |     |
| 2 |     |      |                 | 2004                  |                 | 2005 |         |     |
| 3 | maj | MSZŠ | Lastna sredstva | MSZŠ                  | Lastna sredstva |      |         | LE  |
| 4 |     |      | 200.000         |                       |                 |      |         | Ma  |
| 5 | 5+1 |      | 100.000         |                       |                 |      | 100.000 | Str |
| 6 |     |      | 5.000           |                       |                 |      |         | Str |
| 7 |     |      | 45.000          |                       | 50.000          |      |         | Str |
| 8 |     |      | 50.000          |                       |                 |      |         | SK  |
| 9 |     |      |                 |                       |                 |      | 10.000  | VR  |

terminski in finančni plan / stroški

Delovni list 1 / 2 PageStyle\_terminski in finančni plan 100% STA

site:www.fdvinfo.net filetype:xls



# Javno ali zasebno?

The screenshot shows a Google search result for a file named "Ocene\_08" (grades) from a website. The search results list several documents, including "Ocene redni", "OCENE", and "Sheet1". The "Ocene\_08" document is highlighted, and its content is displayed in a preview window titled "ocene\_april\_pr (samo za branje) - OpenOffice.org Calc".

The spreadsheet contains the following data:

| TRŽENJE V TRGOVINI NA DROBNO<br>Letni semester 2008<br>Ocene dne 22.4.2008 |          |                            |                            |                        |  |
|--|----------|----------------------------|----------------------------|------------------------|--|
|  | Vpis st  | analiza gosta 1<br>10 točk | analiza gosta 2<br>10 točk | Preizkušnja<br>30 točk |  |
| 1  |          |                            |                            |                        |  |
| 2  | 19326554 |                            |                            | 13,5                   |  |
| 3  | 19398834 | 5                          |                            | 16,5                   |  |
| 4  | 19401312 | 7,5                        | 6                          | 25,5                   |  |
| 5  | 19401331 | 6                          | 7                          | 25,5                   |  |
| 6  | 19401473 | 7,5                        | 10                         | 25,5                   |  |
| 7  | 19401806 |                            |                            |                        |  |
| 8  | 19402546 | 8                          | 9                          | 21                     |  |
| 9  | 19404113 |                            |                            | 21                     |  |
| 10   | 19405597 | 9                          | 8                          | 21                     |  |
| 11   | 19405690 | 5                          |                            | 22,5                   |  |
| 12   | 19405760 | 9                          |                            | 15                     |  |
| 13   |          |                            |                            |                        |  |
| 14   |          |                            |                            |                        |  |

A red arrow points to the cell containing the student ID "19405597" in row 11, column 2.

"Google hacking"

# Javno ali zasebno?

Splet [Slike](#) [Skupine](#) [Spletni dnevniki](#) [Imenik](#) [Gmail](#) [več](#) ▼

Google  Iskanje [Napredno iskanje](#) [Nastavitve](#)

Išči po:  celotnem s

Splet

[\[xls\] Investicije ESRR](#)  
Oblika datoteke: Microsoft Excel - [V obliki HTML](#)  
17, 28/10/2005, 2500000.00, 25000.00, 562500.00,  
TRR, 18, 2, avtorska dela - tehnično strokovno znanje

[Podobne strani](#)

[\[xls\] program MK](#)  
Oblika datoteke: Microsoft Excel - [V obliki HTML](#)  
16, 4a, 29/04/2005, 219780.00, **Nakazilo** na  
**Nakazilo** na TRR, plačilo po predračunu ...

[Podobne strani](#)  
[Več zadetkov na www.ljudmila.org »](#)

[\[xls\] List1](#)  
Oblika datoteke: Microsoft Excel - [V obliki HTML](#)  
17, **Nakazilo** letne premije se nakaže na Planinsko  
s podatki o zavarovancu ob **nakazilu** premije pošlje

[\[xls\] pr.čl.2006](#)  
Oblika datoteke: Microsoft Excel - [V obliki HTML](#)  
3 okt 2005 ... 28, Skupaj za **nakazilo** na PZ  
Obveznost **nakazila** na PZS, ki je sestavljen

[Več zadetkov na www.pzs.si »](#)

[\[xls\] Sheet1](#)  
Oblika datoteke: Microsoft Excel - [V obliki HTML](#)  
11, 09, **Nakazilo** ZBS, Priliv ... 36, 56, Potni stroški  
deviz - **nakazilo** v tujino, Odliv, 1129 ...

[\[xls\] Sheet1](#)  
Oblika datoteke: Microsoft Excel - [V obliki HTML](#)  
11, 09, **Nakazilo** ZBS, Priliv, 12, 21, Vnovče  
**nakazilo** v tujino, Odliv, 1129 ...

[Več zadetkov na www.andersen.si »](#)

(samo za branje) - OpenOffice.org Calc

Datoteka Uredi Pogled Vstavi Oblika Orodja Podatki Okno Pomoč

C34  $f(x)$   $\Sigma$  =

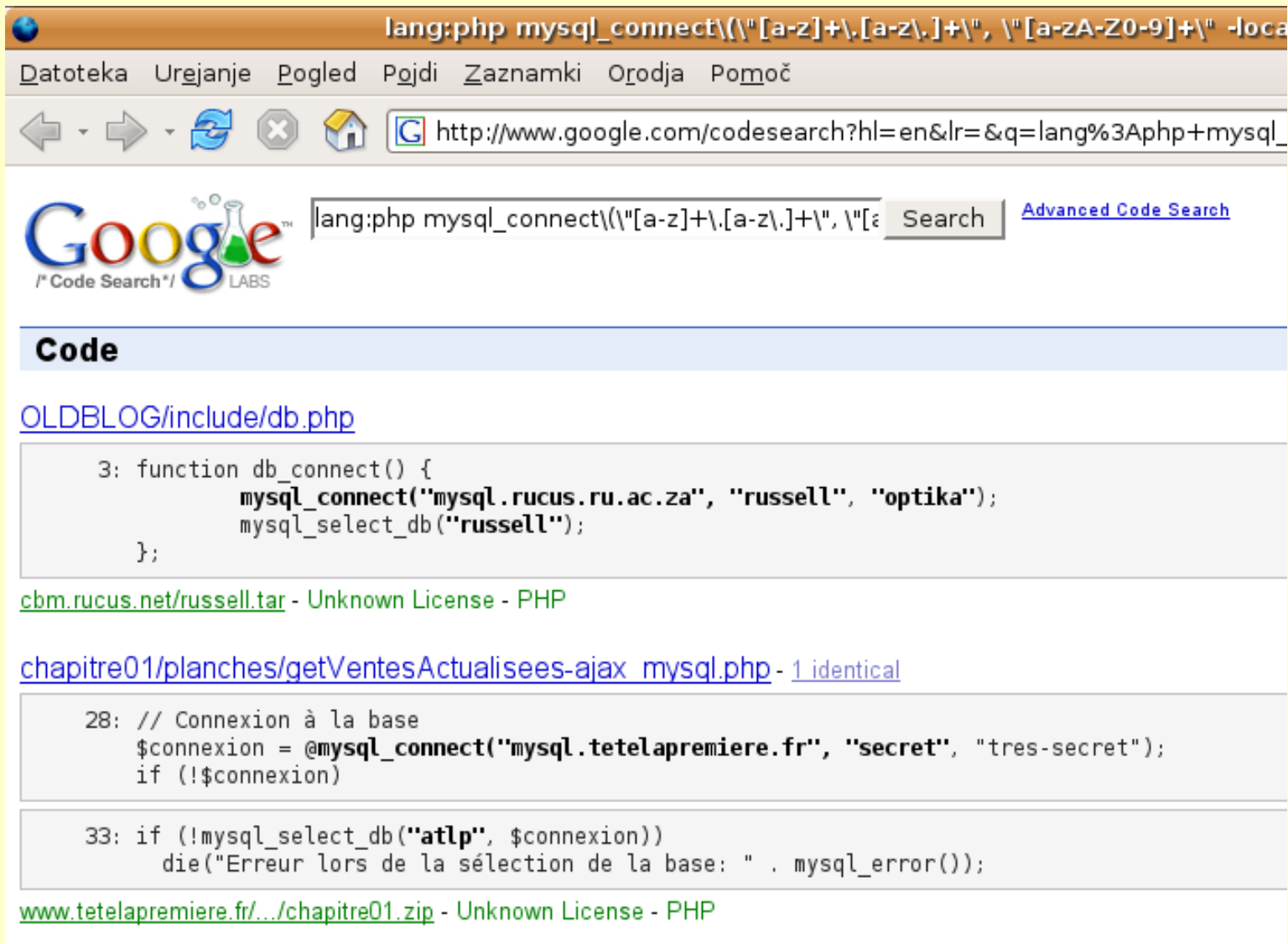
|    | B  | C  | D  | E                  | F                           | G                       |
|----|--|--|--|--------------------|-----------------------------|-------------------------|
| 3  | FINANČNO POROČILO  |  |  | Projekt:           | [redacted]                  |                         |
| 4  | SEZNAM RAČUNOV (v SIT)   |  |  | Izvajalec:         | [redacted]                  |                         |
| 5  |  |  |  | Št. pogodbe:       | Aneks št.1 k pogodbi št. 35 |                         |
| 6  |  |  |  | Št. poročila:      | 1/2005                      |                         |
| 7  |  |  |  | Odbodbe poročanja: | 01. 01. 2005 - 17. 11       |                         |
| 8  | Struktura projekta - glede na odobritev  |  |  |                    |                             |                         |
| 9  | Sklop aktivnosti   | Stroškovna postavka                          | Vrsta spremljajočega dokumenta (vkjučno z referenčno številko IN datumom računa) | Izdajatelj računa  | Datum plačila               | Znesek bre. DDV (v SIT) |
| 10 |  |  |  |                    |                             |                         |
| 11 |  |  |  |                    |                             |                         |
| 12 | 3. Tehnično in strokovno znanje, neposredno vezano na projekt (stroški dela pri postavitvi in administraciji račun |  |  |                    |                             |                         |
| 13 |  |  |  |                    |                             | 6.231.490,              |
| 14 | 1  | avtorska dela - tehnično strokovno znanje za | Avtorska pogodba št.07/2005 z dne 15.01.2005 in Aneks 30.07.2005                 | [redacted]         | 23.03.2005                  | 258.065,00              |
| 15 |  |  |  |                    | 01.04.2005                  | 50.000,00               |
| 16 |  |  |  |                    | 26.10.2005                  | 378.065,00              |
| 17 |  |  |  | skupaj             | 28.10.2005                  | 2.500.000,00            |
| 18 |  |  |  |                    |                             |                         |
| 19 | 2  | avtorska dela - tehnično strokovno znanje za | Avtorska pogodba št.06/2005 z dne 15.01.2005 in Aneks 30.07.2005                 | [redacted]         | 23.03.2005                  | 567.720,00              |
| 20 |  |  |  |                    | 29.04.2005                  | 220.000,00              |

Delovni list 1 / 2 PageStyle\_ [redacted] 100% STA Vsota=0

“Google hacking”



# “Google hacking”



The screenshot shows a web browser window with the address bar containing the search query: `lang:php mysql_connect(\'[a-z]+\.[a-z\.]+\', \'[a-zA-Z0-9]+\') -locat`. The browser's menu bar includes options like "Datoteka", "Urejanje", "Pogled", "Pojdi", "Zaznamki", "Orodja", and "Pomoč". The search results page features the Google Labs logo and a search input field with the same query. Below the search bar, a "Code" section lists search results. The first result is a link to `OLDBLOG/include/db.php` with a code snippet showing a `mysql_connect` function call. The second result is a link to `cbm.rucus.net/russell.tar` with a similar code snippet. The third result is a link to `chapitre01/planches/getVentesActualisees-ajax_mysql.php` with a code snippet showing a `mysql_connect` call and an error handling block.

lang:php mysql\_connect(\'[a-z]+\.[a-z\.]+\', \'[a-zA-Z0-9]+\') -locat

Datoteka Urejanje Pogled Pojdi Zaznamki Orodja Pomoč

http://www.google.com/codesearch?hl=en&lr=&q=lang%3Aphp+mysql\_

Google LABS  
/\* Code Search \*/

lang:php mysql\_connect(\'[a-z]+\.[a-z\.]+\', \'[a-zA-Z0-9]+\') Search [Advanced Code Search](#)

## Code

[OLDBLOG/include/db.php](#)

```
3: function db_connect() {  
    mysql_connect("mysql.rucus.ru.ac.za", "russell", "optika");  
    mysql_select_db("russell");  
};
```

[cbm.rucus.net/russell.tar](#) - Unknown License - PHP

[chapitre01/planches/getVentesActualisees-ajax\\_mysql.php](#) - 1 identical

```
28: // Connexion à la base  
    $connexion = @mysql_connect("mysql.tetelapremiere.fr", "secret", "tres-secret");  
    if (!$connexion)
```

```
33: if (!mysql_select_db("atlp", $connexion))  
    die("Erreur lors de la sélection de la base: " . mysql_error());
```

[www.tetelapremiere.fr/.../chapitre01.zip](#) - Unknown License - PHP

Iskanje gesel za vdor s pomočjo “Google hacking-a”.



**Web** [Images](#) [Video](#) <sup>New!</sup> [News](#) [Maps](#) [more »](#)

intext:mastercard 5424000000000000..5424999999999999

Google Search I'm Feeling Lucky

[Advanced Search](#)  
[Preferences](#)  
[Language Tools](#)

[Advertising Programs](#) - [Business Solutions](#) - [About Google](#) - [Go to Google Slovenia](#)

©2006 Google

# Javno ali zasebno?





# Fakulteta za družbene vede

Univerza v Ljubljani

SPLETNI REFERAT URNIKI PEDAGOGI PREDMETI PROGRAMI KLUB DIPLOMANTOV



## Kontakti

- OSEBNA IZKAZNICA
- POMEMBNI KONTAKTI
- TELEFONSKI IMENIK FDV
- SPLOŠNI E-MAIL NASLOVI

### TELEFONSKI IMENIK

**A B C Č D Đ E F G H I J K L M N O P R S Š T U V Z Ž**

V primeru nejasnosti ali informacije pokličite **5805-100**

|          | Primek in ime        | Interna številka | Številka sobe |
|----------|----------------------|------------------|---------------|
| <b>A</b> |                      |                  |               |
|          | ADAM dr. Frane       | 219              | DS 21         |
|          | AKSENTIJEVIĆ Živojin | 152              | KNJIŽNICA     |
| <b>B</b> |                      |                  |               |
|          | BABIĆ Nela           | 121              | AP 22a        |
|          | BAČLIJA dr. Irena    | 171              | B 103         |
|          | BAHOR mag. Maja      | 256              | DS 12         |
|          | BANJAC Marinko       | 364              | C 231         |
|          | BEBLER dr. Anton     | 327              | AP 27         |
|          | BERCE dr. Jaroslav   | 362              | IDV 610       |

tel\_imenik\_FDV.ods - LibreOffice Calc

Datoteka Uredi Pogled Vstavi Oblika Orodja P

Arial 10

A1 f(=) Σ = Priimek in ime

|     | A                         | B   |
|-----|---------------------------|-----|
| 239 | UHAN dr. Samo             | 296 |
| 240 | VEHOVAR dr. Vasja         | 297 |
| 241 | TOŠ dr. Niko              | 298 |
| 242 | GREGORČIČ dr. Marta       | 299 |
| 243 | VELIKONJA dr. Mitja       | 299 |
| 244 |                           | 300 |
| 245 | BERNIK dr. Ivan           | 301 |
| 246 | JOGAN dr. Maća            | 302 |
| 247 |                           | 303 |
| 248 | KOS dr. Drago             | 304 |
| 249 | DIMC Neli                 | 305 |
| 250 | MALI dr. Franc            | 306 |
| 251 | MENCIN-ČEPLAK dr. Marjeta | 307 |
| 252 | MIHELJAK dr. Vlado        | 308 |
| 253 | RENER dr. Tanja           | 309 |
| 254 | SMRKE dr. Marjan          | 310 |
| 255 | LEBARIČ mag. Vasja        | 311 |
| 256 | TIVADAR dr. Blanka        | 312 |
| 257 | LOZAR MANFREDA dr. Katja  | 313 |

Delovni list 1 / 3 | Privzeto | STA | Vsota=0



Document1 - Microsoft Word

File Edit View Insert Format Tools Table Window Help

Type a question for help

95% Read

UNCLASSIFIED

I. BACKGROUND

A. (U) Administrative Matters

1. (U) Appointing Authority

(U) I was appointed by LTG John R. Vines, Commander, Multi-National Corps-Iraq (MNC-I) on 8 March 2005 to investigate, per U.S. Army Regulation 15-6 (Annex 1B), all the facts and circumstances surrounding the incident at a Traffic Control Point (TCP) in Baghdad, Iraq on 4 March 2005 that resulted in the death of Mr. Nicola Calipari and the wounding of Ms. Giuliana Sgrena and Mr. Andrea Carpani. Lieutenant Colonel Richard Thelin, USMC was appointed as my legal advisor for this investigation. I was directed to thoroughly review (1) the actions of the Soldiers manning the TCP, (2) the training of the Soldiers manning the TCP, (3) TCP procedures, (4) the local security situation, (5) enemy tactics, techniques, and procedures (TTPs), (6) the Rules of Engagement (ROE) employed during the incident, and (7) any coordination effected with the Soldiers at TCP or their higher levels of command on the transport of Ms. Sgrena from Baghdad Baghdad International Airport (BIAP). (Annex 1A).

(U) The appointing letter (Annex 1A) refers to the location of the incident as being a Traffic Control Point (TCP). As will be further explained in this report, the Soldiers involved were actually manning a former Traffic Control Point, but executing a blocking mission. This mission took place at a southbound on-ramp from Route Vernon (also known as Route Force on MNF-I graphics) onto westbound Route Irish, the road to BIAP. The intersection of these two routes has been designated as Checkpoint 541. For purposes of this report, the position will be referred to as Blocking Position 541 (BP 541).

2. (U) Brief Description of the Incident

(U) On the evening of 4 March 2005, personnel of A Company of 1-69 Infantry (attached to 2d Brigade Combat Team, 10th Mountain Division), were patrolling Route

Page 1 Sec 1 1/1 At 15,1 cm Ln 27 Col 60 REC TRK EXT OVR Slovenian

Adobe Acrobat - [sgrena\_report\_bad\_redaction.pdf]

File Edit Document Tools View Window Help

125%

I. BACKGROUND

A. (U) Administrative Matters

1. (U) Appointing Authority

(U) I was appointed by LTG John R. Vines, Commander, Multi-National Corps-Iraq (MNC-I) on 8 March 2005 to investigate, per U.S. Army Regulation 15-6 (Annex 1B), all the facts and circumstances surrounding the incident at a Traffic Control Point (TCP) in Baghdad, Iraq on 4 March 2005 that resulted in the death of Mr. Nicola Calipari and the wounding of Ms. Giuliana Sgrena and Mr. [REDACTED]. Lieutenant Colonel [REDACTED] USMC was appointed as my legal advisor for this investigation. I was directed to thoroughly review (1) the actions of the Soldiers manning the TCP, (2) the training of the Soldiers manning the TCP, (3) TCP procedures, (4) the local security situation, (5) enemy tactics, techniques, and procedures (TTPs), (6) the Rules of Engagement (ROE) employed during the incident, and (7) any coordination effected with the Soldiers at the TCP or their higher levels of command on the transport of Ms. Sgrena from Baghdad to Baghdad International Airport (BIAP). (Annex 1A).

(U) The appointing letter (Annex 1A) refers to the location of the incident as being a Traffic Control Point (TCP). As will be further explained in this report, the Soldiers involved were actually manning a former Traffic Control Point, but executing a blocking mission. This mission took place at a southbound on-ramp from Route Vernon (also known as Route Force on MNF-I graphics) onto westbound Route Irish, the road to BIAP. The intersection of these two routes has been designated as Checkpoint 541. For purposes of this report, the position will be referred to as Blocking Position 541 (BP 541).

2. (U) Brief Description of the Incident

(U) On the evening of 4 March 2005, personnel of [REDACTED] Company of [REDACTED] Infantry (attached to [REDACTED] Brigade Combat Team, [REDACTED] Division), were patrolling Route Irish, the road linking downtown Baghdad with BIAP. Seven of those Soldiers were then

1 of 42 8,5 x 11 in



**Prometni podatki, metapodatki in drugi skriti podatki**

# Prometni podatki

- pri ponudnikih dostopa do interneta, pri ponudnikih vsebin;
- "klepetavost brskalnikov", piškotki, superpiškotki,...



# Analiza prometnih podatkov

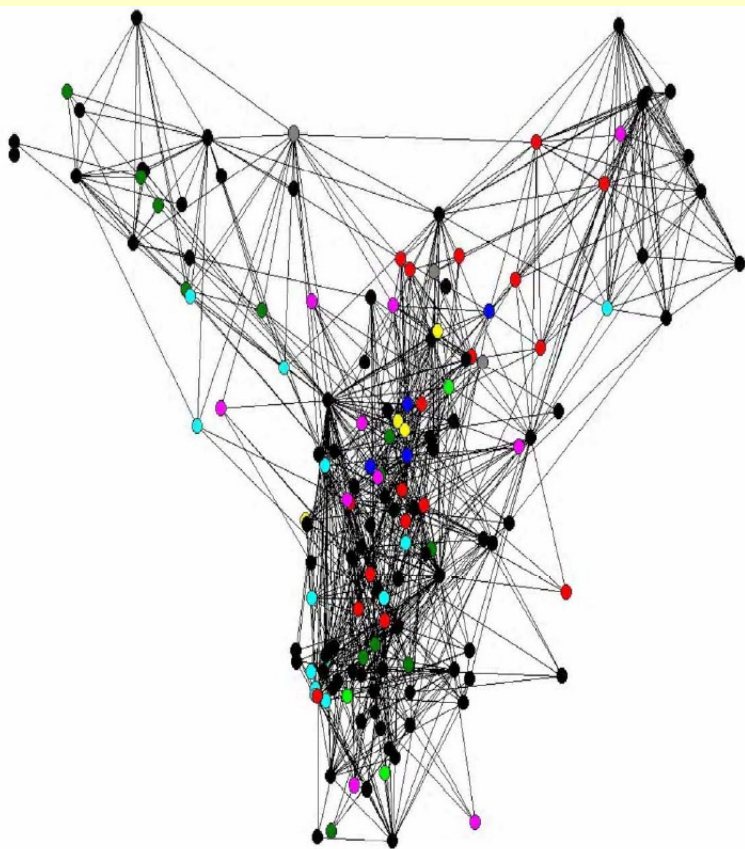


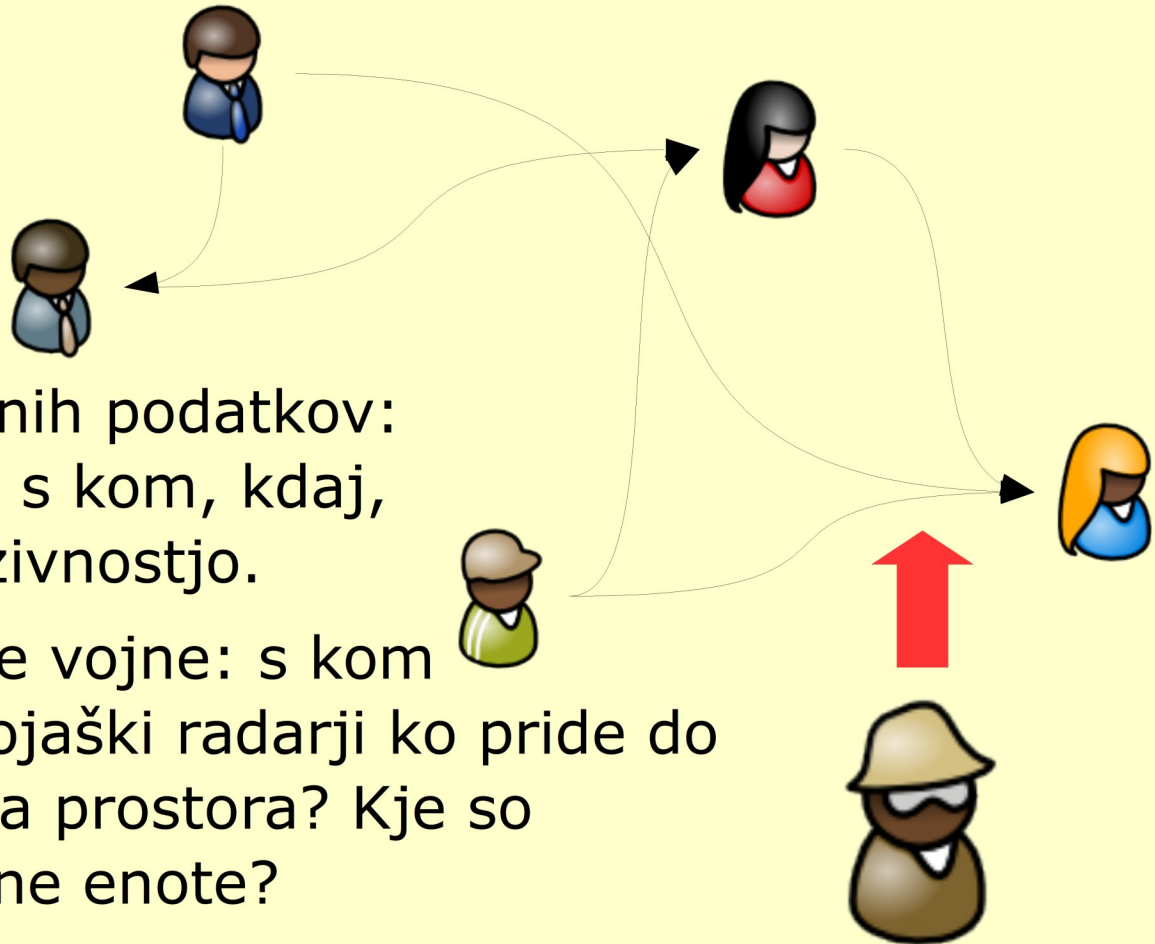
Figure 7: Network showing how the ex employees were connected

Red: Vice President, Blue: President, Black: Employee (non managerial), Grey: In House Lawyer, Pink: Manager, Dark Green: Trader, Light Green: Managing Director, Light Blue: Director, Yellow: CEO

Kdo v Enronu je s kom komuniciral – socialno omrežje zaposlenih.  
Vir in avtorstvo: *Shetty in Adibi, The Enron Email Dataset - Database Schema and Brief Statistical Report, 2004.*



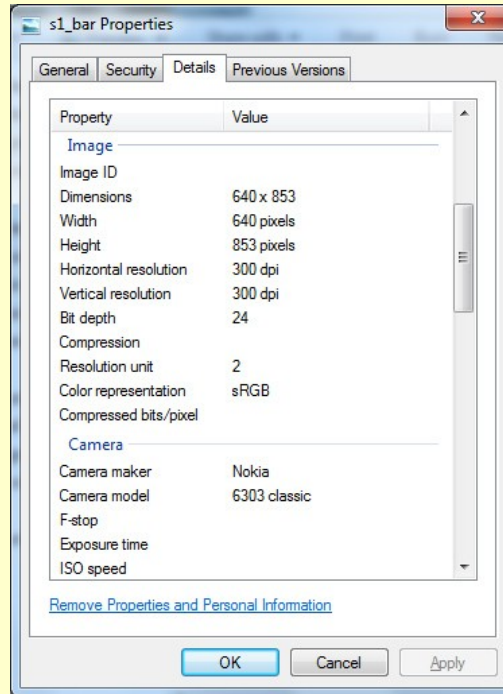
# Analiza prometa



- Analiza prometnih podatkov: kdo komunicira s kom, kdaj, s kakšno intenzivnostjo.
- Primer iz hladne vojne: s kom komunicirajo vojaški radarji ko pride do kršitve zračnega prostora? Kje so locirane sovražne enote?
- Deluje tudi kadar je vsebina komunikacije šifrirana.

**napadalec**

# Skriti metapodatki...



KPK - FOCA Free 3.0

Project Tools Options TaskList About Donate

Directory listing  
DNS Active Cache  
.DS\_Store  
GHDB  
Insecure Methods  
Multiple choices  
SQLi  
Listing  
Leaks  
Proxy  
Users  
ZoneTransfer  
Metadata  
Documents (85/97)  
  .pdf (53)  
  Unknown (32)  
  Metadata Summary  
  Users (15)  
    Folders (0)  
    Printers (0)  
    Software (20)  
    Emails (0)  
    Operating Systems (0)  
    Passwords (0)  
    Servers (0)

**FOCA**

Clean your OpenOffice documents with OOMetaExtractor

| Attribute                                 | Value |
|---|-------|
| <b>All users found (15) - Times found</b> |       |
| Geda                                      | 2     |
| SPECKBACHER                               | 3     |
| RPrah                                     | 3     |
| Pedron_S                                  | 2     |
| Sandra Blagojević                         | 5     |
| Roman Prah                                | 6     |
| Barbara Lavtar                            | 2     |
| Deanna M. Clements                        | 3     |
| User                                      | 12    |
| Readiris                                  | 1     |
| SBlagojevic                               | 2     |
| ktjasa                                    | 5     |
| GHITA Simona                              | 2     |
| King                                      | 1     |
| Neža Pirnat                               | 2     |

| Time     | Source         | Severity | Message  |
|----------|----------------|----------|--|
| 22:34:27 | MetadataSearch | low      | Document metadata extracted: C:\Documents and Settings\kpkMacF\Local Settings\Temp\katalog...  |
| 22:34:28 | MetadataSearch | low      | Document metadata extracted: C:\Documents and Settings\kpkMacF\Local Settings\Temp\Resoluc...  |
| 22:34:28 | MetadataSearch | low      | Document metadata extracted: C:\Documents and Settings\kpkMacF\Local Settings\Temp\seznam...   |
| 22:34:28 | MetadataSearch | low      | Document metadata extracted: C:\Documents and Settings\kpkMacF\Local Settings\Temp\Akcijski... |
| 22:34:28 | MetadataSearch | low      | Document metadata extracted: C:\Documents and Settings\kpkMacF\Local Settings\Temp\inkrimin... |
| 22:34:29 | MetadataSearch | low      | Document metadata extracted: C:\Documents and Settings\kpkMacF\Local Settings\Temp\KATAL...    |
| 22:34:29 | MetadataSearch | low      | Document metadata extracted: C:\Documents and Settings\kpkMacF\Local Settings\Temp\ZIntPK...   |

Conf Deactivate AutoScroll Clear Save log to File


Metadata analyzed !


FOCA, orodje za iskanje in analizo metapodatkov v dokumentih objavljenih na spletnih straneh, <<http://www.informatica64.com/>>

IP-RS - FOCA Free 3.0

Project Tools Options TaskList About Donate

- PC\_Mike Mandel
- PC\_Ministrstvo za pravosodje
- PC\_Mitja Blaganje
- PC\_mlaznik
- PC\_MP
- PC\_mprelesnik
- PC\_Nataša Brenk
- PC\_Nataša Pirc
  - Users
  - Folders
- PC\_Nick
- PC\_npirc
- PC\_P\_Chavdarov
- PC\_Polona Tepina
- PC\_ptepina
- PC\_Publications Office
- PC\_ruseva
- PC\_Rosana Lemut Strl
- PC\_Sandra Vesel
- PC\_Sanja Vraber
- PC\_SBien
- PC\_snovak
- PC\_Sonja Bien
- PC\_sola





**Clean your OpenOffice documents with OOMetaExtractor**

| Attribute  | Value |
|--|-------|
| <b>Users</b>   |       |
| Nataša Pirc  |       |
| <b>Folders</b>   |       |
| C:\Program%20Files\Microsoft%20Office\MEDIA\CAGCAT10\                          |       |
| d:\Dosebno\Moj%20dokumenti\My%20Pictures\Microsoftov%20organizator%20izrezk... |       |
| C:\Documents%20and%20Settings\NPirc\Local%20Settings\Temporary%20Internet...   |       |
| <b>Software</b>  |       |
| Microsoft Office   |       |
| Microsoft Office 2007  |       |

| Time    | Source         | Severity | Message  |
|---------|----------------|----------|--|
| 8:24:13 | MetadataSearch | low      | Document metadata extracted: C:\Documents and Settings\kpkMacF\Local Settings\Temp\Smeric...   |
| 8:24:13 | MetadataSearch | low      | Document metadata extracted: C:\Documents and Settings\kpkMacF\Local Settings\Temp\Smeric...   |
| 8:24:13 | MetadataSearch | low      | Document metadata extracted: C:\Documents and Settings\kpkMacF\Local Settings\Temp\ZAKON...    |
| 8:24:13 | MetadataSearch | low      | Document metadata extracted: C:\Documents and Settings\kpkMacF\Local Settings\Temp\vzorec_...  |
| 8:24:13 | MetadataSearch | low      | Document metadata extracted: C:\Documents and Settings\kpkMacF\Local Settings\Temp\Tersek_...  |
| 8:24:14 | MetadataSearch | low      | Document metadata extracted: C:\Documents and Settings\kpkMacF\Local Settings\Temp\VP_in_...   |
| 8:24:14 | MetadataSearch | low      | Document metadata extracted: C:\Documents and Settings\kpkMacF\Local Settings\Temp\Priloga_... |

Metadata analyzed !

```
sudo nmap -O www.fdv.uni-lj.si
```

```
Starting Nmap 5.21 ( http://nmap.org ) at 2011-11-07 09:21 CET
Nmap scan report for www.fdv.uni-lj.si (193.2.110.7)
Host is up (0.0094s latency).
rDNS record for 193.2.110.7: bumbar.fdv.uni-lj.si
Not shown: 997 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed auth
443/tcp    open  https
Device type: general purpose|WAP
Running (JUST GUESSING) : Microsoft Windows 2008|Vista|7 (90%),
AirSpan embedded (87%), FreeBSD 6.X (87%), Apple embedded (85%)
Aggressive OS guesses: Microsoft Windows Server 2008 Beta 3
(90%), Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or
Windows 7 (90%), AirSpan ProST WiMAX access point (87%),
FreeBSD 6.2-RELEASE (87%), Apple AirPort Extreme WAP v7.3.2
(85%)
No exact OS matches for host (test
OS detection performed. Please report
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up)
```

```
whois slo-tech.com
```

```
Domain name: slo-tech.com
```

```
Administrative Contact:
```

```
Slo-Tech
Primoz Bratanic (primoz@slo-
+386.40*****
Fax:
**** 24
****, SI 1***
SI
```

```
...
Name Servers:
ns.datacenter.si
ns.slo-tech.com
ns1.triera.net
ns2.amis.net
ns2.datacenter.si
ns3.amis.net
sdns.voljatel.si
```

```
Creation date: 21 Apr 2000 09:24:03
Expiration date: 21 Apr 2017 09:24:00
```

```
dig kpk-rs.si MX
```

```
; <<> DiG 9.7.1-P2 <<> kpk-rs.si MX
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id:
59356
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY:
2, ADDITIONAL: 0
;; QUESTION SECTION:
;kpk-rs.si.                                IN
MX
;; ANSWER SECTION:
kpk-rs.si.                                35707      IN
MX      10 mail2.gov.si.
kpk-rs.si.                                35707      IN
MX      10 mail1.gov.si.
;; AUTHORITY SECTION:
kpk-rs.si.                                82536      IN
NS      kanin.arnes.si.
kpk-rs.si.                                82536      IN
NS      nanos.arnes.si.
;; Query time: 9 msec
;; SERVER: 193.2.1.66#53(193.2.1.66)
;; WHEN: Mon Nov 7 09:18:50 2011
;; MSG SIZE rcvd: 121
```

Identifikacija  
strežnikov  
organizacije s  
standardnimi  
omrežnimi orodji...

**Gesla**

# Uporaba privzetih gesel

10.254.60.9: tiptel innovaphone 21-Mozilla Firefox

Datoteka Urejanje Pogled Zgodovina Zaznamki Orodja Pomoč

http://10.254.60.9/

unauthentic

RtpDumpScript - The Wir... UCSniff IP Video Sniffer oxid.it - Cain & Abel 10.254.60.9: tiptel innova...

**tiptel innovaphone 21 Gateway**

- Diagnostics
  - Info
  - Log
  - Trace
  - Config show
  - IP Interfaces
  - IP Routing
  - Ping
- Gateway
  - Config
  - Voice Interfaces
  - Calls
  - Call Counter
- Administration
  - Licenses
  - Config save (all)
  - Config save (config)
  - Config save (LDAP)

**Info**

Version V5.01 sp3 IP21[06-5977], Bootcode[322], HW[109] 2048/8192

Serialno 00-90-33-04-1e-d9

Coder 2 channels

HDLC 0 channels

Sync source -

SNTP Server 0.0.0.0

LDAP Replication off

Localtime \*\*: \*\*: \*\*: \*\*: \*

Uptime 43d 2h 43m 8s

Relay Licenses

PBX Licenses

http://10.254.60.9/

RtpDumpScript - The Wir... UCSniff IP Video Sniffer oxid.it - Cain & Abel Nalaganje...

**tiptel innovaphone 21 Gateway**

**Info**

Version V5.01 sp3 IP21[06-5977], Bootcode[322], HW[109] 2048/8192

Localtime \*\*: \*\*: \*\*: \*\*: \*

Uptime 43d 2h 43m 8s

**Avtentikacija**

http://10.254.60.9 zahteva uporabniško ime in geslo. Stran sporoča: "IP21-04-1e-d9"

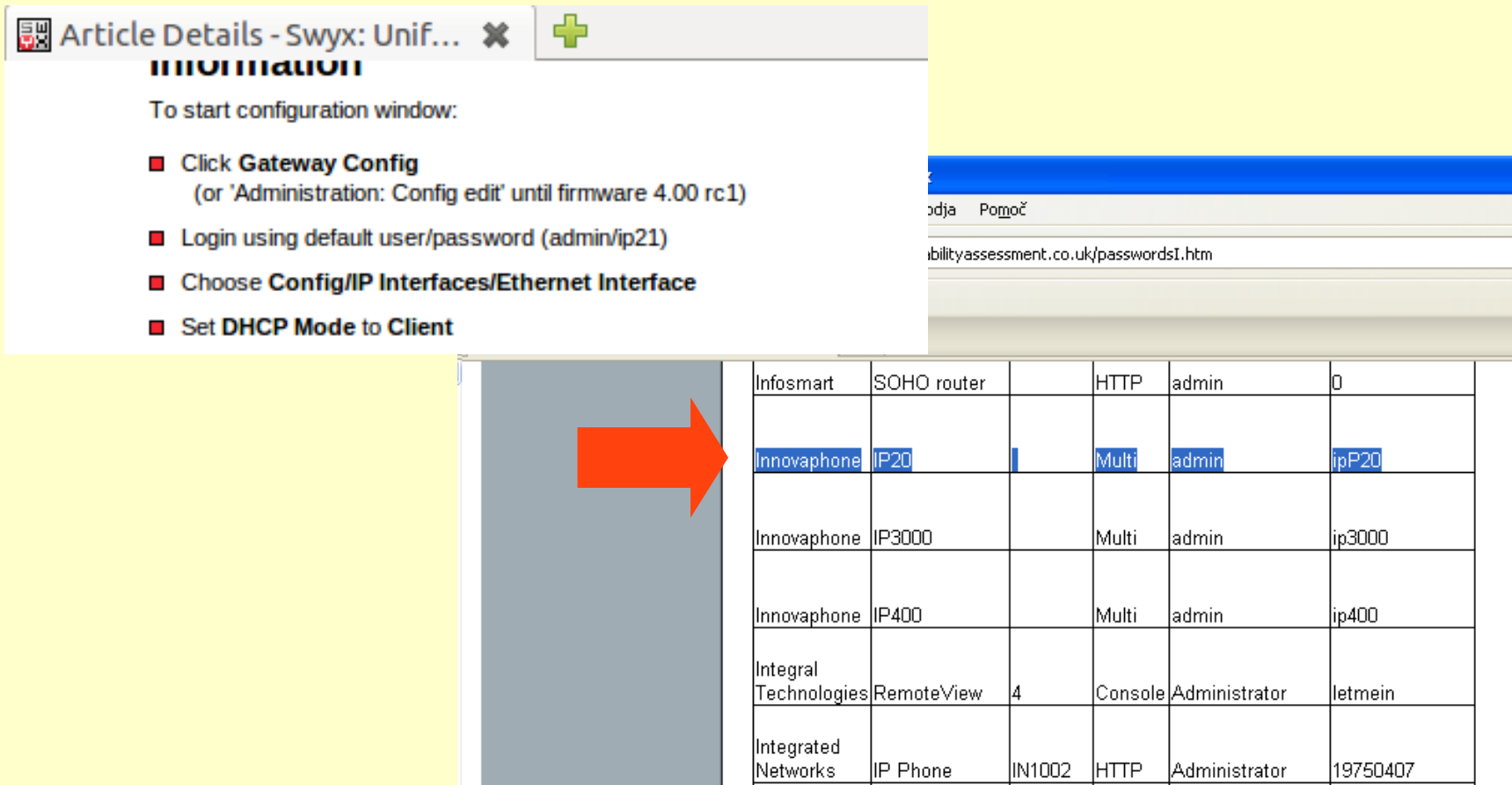
Uporabniško ime:

Geslo:

Prekliči V redu

# Uporaba privzetih gesel

Google: "Tiptel Innovaphone 21"



The image shows a browser window with a search result for 'Tiptel Innovaphone 21'. The search result includes a list of steps to start configuration and a table of default credentials for various routers. A red arrow points to the 'Innovaphone IP20' entry in the table.

**Information**

To start configuration window:

- Click **Gateway Config**  
(or 'Administration: Config edit' until firmware 4.00 rc1)
- Login using default user/password (admin/ip21)
- Choose **Config/IP Interfaces/Ethernet Interface**
- Set **DHCP Mode to Client**

|                       |             |        |         |               |          |
|-----------------------|-------------|--------|---------|---------------|----------|
| Infosmart             | SOHO router |        | HTTP    | admin         | 0        |
| Innovaphone           | IP20        |        | Multi   | admin         | ipP20    |
| Innovaphone           | IP3000      |        | Multi   | admin         | ip3000   |
| Innovaphone           | IP400       |        | Multi   | admin         | ip400    |
| Integral Technologies | RemoteView  | 4      | Console | Administrator | letmein  |
| Integrated Networks   | IP Phone    | IN1002 | HTTP    | Administrator | 19750407 |



# Uporaba privzetih gesel

The image shows two overlapping screenshots of a web browser window displaying the configuration page for a 'tiptel innovaphone 21 Gateway'. The browser's address bar shows 'http://10.254.60.9/'.

The top screenshot shows the 'Diagnostics' menu on the left, with 'Trace' selected. The main content area displays the following text:

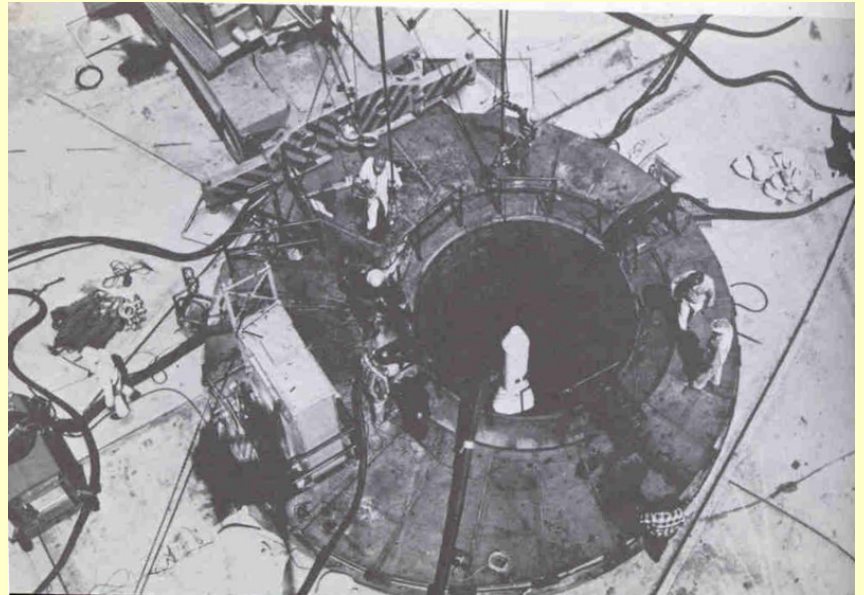
```
V5.01 sp3 IP21[06-5977], Bootcode[322], HW[109] 2048/8192  
IP21-04-1e-d9  
end of  
reset-  
ok
```

The bottom screenshot shows the 'IP Routing table' section, which contains the following table:

| net addr        | net mask        | gateway         | interface | state |
|-----------------|-----------------|-----------------|-----------|-------|
| 255.255.255.255 | 255.255.255.255 | 255.255.255.255 | local     | Up    |
| 10.254.60.9     | 255.255.255.255 | 0.0.0.0         | local     | Up    |
| 10.254.60.63    | 255.255.255.255 | 255.255.255.255 | ETH0      | Up    |
| 10.254.60.0     | 255.255.255.192 | 0.0.0.0         | ETH0      | Up    |
| 127.0.0.0       | 255.0.0.0       | 127.0.0.1       | local     | Up    |
| 224.0.0.0       | 224.0.0.0       | 224.0.0.0       | ETH0      | Up    |
| default         | out             | 10.254.60.1     | ETH0      | Up    |



В МУЗЕЕ ЯДЕРНОГО ОРУЖИЯ АРЗАМАСА-16



During the early to mid-1970s, during my stint as a Minuteman launch officer, they still had not been changed. Our launch checklist in fact instructed us, the firing crew, to double-check the locking panel in our underground launch bunker to ensure that no digits other than zero had been inadvertently dialed into the panel. SAC remained far less concerned about unauthorized launches than about the potential of these safeguards to interfere with the implementation of wartime launch orders. **And so the “secret unlock code” during the height of the nuclear crises of the Cold War remained constant at 00000000.**

# Ustrezna uporaba gesel?

We hacked Dan's assets first through finding bugs and writing 0day, and then through abusing him giving away passwords and his silly password scheme. Check out just some of his passes:

```
fuck.hackers, 0hn0z (root account on his mail box), fuck.omg, fuck.vps,  
ohhai
```

Five character root password? Niiiiiiice.

From .mysql\_history:

```
SET PASSWORD FOR 'root'@'localhost' = PASSWORD('fuck.mysql');
```

See the pattern?

Adding fuel to the fire (and hopefully flames to his talks!), Dan has a messy personal life involving him, his girlfriend, and other girls who he would love to get with. For once, we are mostly sparing the girlfriend. Who says chivalry is dead? But we'll still point out the dating torrents that Kaminsky downloads.

From: Greg Hoglund <greg@hbgary.com> ISun, Feb 6, 2011 at 1:59 PM  
To: jussi <jussij@gmail.com>

im in europe and need to ssh into the server. can you drop open up firewall and allow ssh through port 59022 or something vague?  
and is our root password still 88j4bb3rw0cky88 or did we change to 88Scr3am3r88 ?  
thanks

From: jussi jaakonaho <jussij@gmail.com> ISun, Feb 6, 2011 at 2:06 PM  
To: Greg Hoglund <greg@hbgary.com>

hi, do you have public ip? or should i just drop fw?  
and it is w0cky - tho no remote root access allowed

From: Greg Hoglund <greg@hbgary.com> ISun, Feb 6, 2011 at 2:08 PM  
To: jussi jaakonaho <jussij@gmail.com>

no i dont have the public ip with me at the moment because im ready for a small meeting and im in a rush. if anything just reset my password to changeme123 and give me public ip and ill ssh in and reset my pw.

From: jussi jaakonaho <jussij@gmail.com> ISun, Feb 6, 2011 at 2:10 PM  
To: Greg Hoglund <greg@hbgary.com>

ok,  
takes couple mins, i will mail you when ready. ssh runs on 47152

Napad na informacijsko-varnostno podjetje HBGary (podjetje je za ameriško vlado izvajalo "napade" proti skupini Anonymous).

...a little later:

```
bash-3.2# ssh hoglund@65.74.181.141 -p 47152
[unauthorized access prohibited]
hoglund@65.74.181.141's password:
[hoglund@www hoglund]$ unset
[hoglund@www hoglund]$ unset HIST
[hoglund@www hoglund]$ unset HISTFLE
[hoglund@www hoglund]$ unset HISTFILE
[hoglund@www hoglund]$ uname -a;hostname
Linux www.rootkit.com 2.4.21-40.ELsmp #1 SMP Wed
Mar 15 14:21:45 EST 2006 i686 i686 i386
GNU/Linux
www.rootkit.com
[hoglund@www hoglund]$ su -
Password:
[root@www root]# unset HIST
[root@www root]# unset HISTFILE
[root@www root]# uname -a;hostname;id
Linux www.rootkit.com 2.4.21-40.ELsmp #1 SMP Wed
Mar 15 14:21:45 EST 2006 i686 i686 i386
GNU/Linux
www.rootkit.com
uid=0(root) gid=0(root)
groups=0(root),1200(varmistus)
```

# Avtentikacija uporabnika po imenu?

Zadeva: Remote Download server ;)

Od: [redacted]

Datum: 09. 07. 2007 01:52

Za: [matej.kovacic@gmail.com](mailto:matej.kovacic@gmail.com)

Zivjo!

Takole, v Win 2000 si najprej naloži Remote Desktop Client.

Dobiš ga na:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=80111f21>

Nato se z njim povežeš na [redacted]

user: [redacted]

LP, Darko

**PERSPEKTIVA**  
PERSPEKTIVA  
BOZZHO PERSPEKTIVA  
D.O.O.BA, s.r.l.  
WTC, Dunajska cesta 156  
1000 Ljubljana, Slovenija  
E: +386 (0)1 / 56 88 225  
F: +386 (0)1 / 56 88 141

Stran: 1 / 1

**PETROL D.D.**  
DUNAJSKA CESTA 50  
1000 LJUBLJANA

ID št. za DDV kupca: [redacted]

**RAČUN:** [redacted]

V Ljubljani, [redacted] 2007  
Datum odpošiljanja blaga [redacted] 2007  
oz. opravljanja storitev: [redacted] 2007  
Datum zapadlosti: [redacted] 2007

Predmet: Pogodba o svetovanju pri izvedbi in izvedbi prevzema javne družbe, z dne [redacted] 2007

| Opis   | Faktura (V št.) | Osna brez DDV | Dreška (v št.)      |
|--|-----------------|---------------|---------------------|
| Na podlagi 8. člena pogodbe o svetovanju pri izvedbi in izvedbi prevzema javne družbe, z dne 19.09.2007, vam zaračunavamo:   |                 |               |                     |
| - fiksni del provizije za izvedbo prevzemnih opravil in za svetovanje  | 1               | 60.000,00     | 60.000,00           |
| - variabilni del provizije za svetovanje v višini 0,40 % od transakcijske vred. delnic, ki predstavljajo prvih 29,99% delnic, za katere so akcep. sprejeli prev. pon.      | 1               | 683.760,00    | 683.760,00          |
| - variabilni del provizije za svetovanje v višini 0,85 % od transakcijske vrednosti delnic, ki presegajo 30,00 % delnic za katere so akceptanti sprejeli prevzemno ponudbo | 1               | 115.225,66    | 115.225,66          |
| Vrednost brez DDV  |                 | 858.985,66    | 858.985,66          |
| 1 - DDV - Osnovna stopnja 20,0 %   |                 |               | 171.797,13          |
| Osnova:  |                 | 858.985,66    | 171.797,13          |
| <b>SKUPAJ €</b>  |                 |               | <b>1.030.782,79</b> |
| Znes v SIT   |                 |               | 247.016.787,79      |

Prosimo vas, da fakturni znesek nakažete na TRR : SI56 0600 0011 8721 024 pri Banki Celje, d.d.  
PRI PLAČILU SE SKLJUČUJE NA [redacted]

Prilpavila: [redacted]

**PERSPEKTIVA**  
BOZZHO PERSPEKTIVA D.O.O.BA, s.r.l.

Član uprave:  
Mladen Kalliterna

Identifikacijsko število za DDV: SI53104172  
Matinska številka: 57541564  
Osnovni kapital: 150.916.000,00 SIT  
Številka registrskega vločka: 1/03344/031  
Drešče je spletno pri: [redacted]

Primer sporočil prispelih na moj Gmail račun...

In West Memphis District Court yesterday, Tristian Wilson was set to appear on the docket for a bond hearing on the charges. When he did not appear, Judge William "Pal" Rainey inquired about his release and found that a jail staff member released Wilson by the authority of a fax sent to the jail late Saturday night.

According to Assistant Chief Mike Allen, **a fax was sent to the jail** which stated "*Upon decision between Judge Rainey and the West Memphis Police Department CID Division Tristian Wilson is to be released immediately on this date of October 30, 2004 with a waiver of all fines, bonds and settlements per Judge Rainey and Detective McDugle.*"

# Neustrezna avtentikacija

Mozilla Firefox browser window showing the URL `https://erisk.sigov.si/erisk/index.faces`. The browser's address bar and tabs show the site. A red box highlights the text **e-RISK DUNZ** in the top navigation bar. To the right, the user is identified as **Matej Kovačič / KOMISIJA ZA PREPREČEVANJE KORUPCIJE**. The date is **Cetrtek, 10. marec, 2011**. There are links for **O aplikaciji**, **Omožiti**, and **Odiava**.

'Podatki o strani' window for `https://erisk.sigov.si/erisk/index.faces`. It shows security-related icons: Splošno, Večpredstavnost, Dovoljenja, and Varnost.

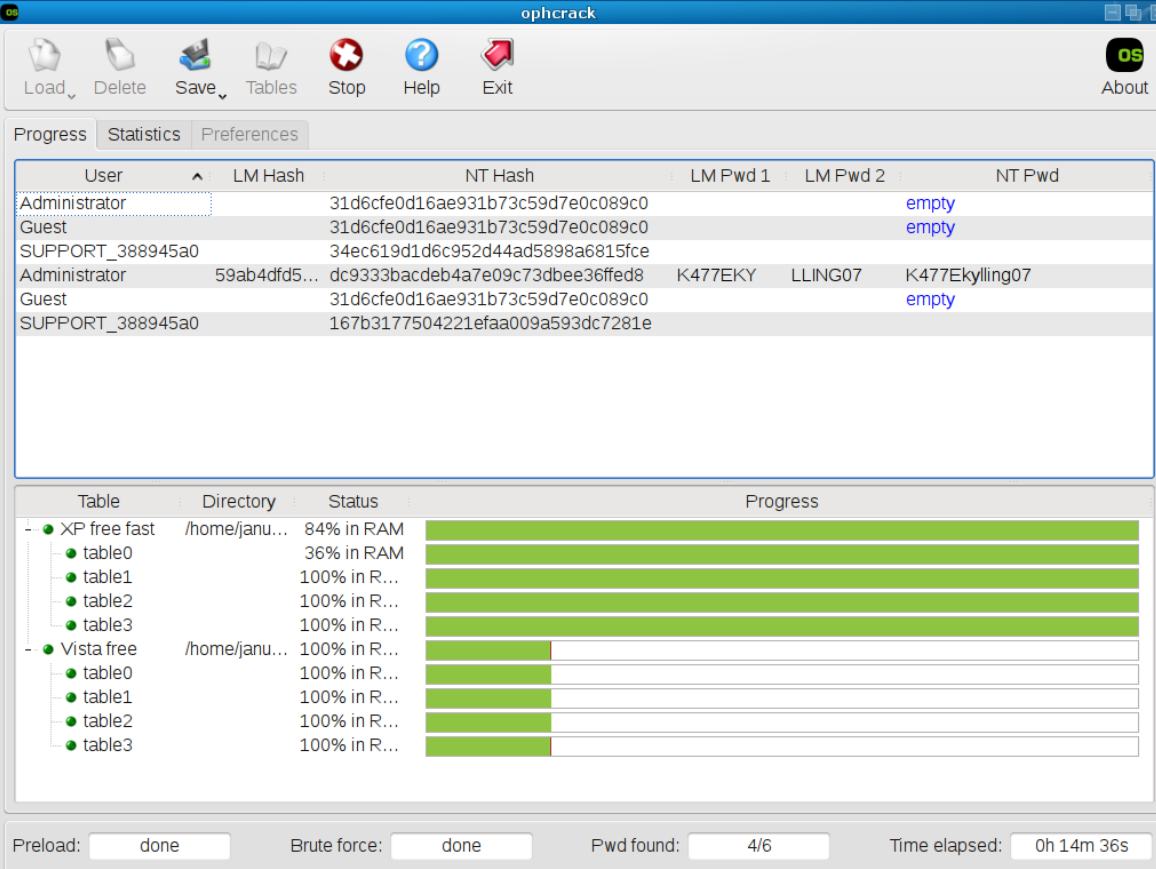
'Piškoti' window for `sigov.si`. It lists cookies for `erisk.sigov.si` with names `JSESSIONID`, `LtpaToken`, and `LtpaToken2`. A red arrow points to the `JSESSIONID` cookie details, which include the value `0000IXLMzTJWUZUQTVL_er6b:C075CB88E4DE844900001B00`.

Mozilla Firefox browser window showing the URL `https://erisk.sigov.si/erisk/logoff` highlighted in a red box. The browser's address bar and tabs show the site.

'Piškoti' window for `sigov.si`. It lists cookies for `erisk.sigov.si` with names `JSESSIONID`, `LtpaToken`, and `LtpaToken2`. A red arrow points to the `JSESSIONID` cookie details, which include the value `0000IXLMzTJWUZUQTVL_er6b:C075CB88E4DE844900001B00`.

'Podatki o strani' window for `https://erisk.sigov.si/erisk/logoff`. It shows security-related icons: Splošno, Dovoljenja, and Varnost. The 'Preveril:' section contains the warning: **Ta spletna stran ne vsebuje podatkov o lastništvu. state-institutions**. There are buttons for **Preglej digitalno potrdilo**, **Preglej piškote**, and **Preglej shranjena gesla**.

# Razbijanje gesel



The screenshot shows the ophcrack application window. The title bar reads "ophcrack". The menu bar includes "Load", "Delete", "Save", "Tables", "Stop", "Help", "Exit", and "About". The main window is divided into two sections. The top section is a table with columns: "User", "LM Hash", "NT Hash", "LM Pwd 1", "LM Pwd 2", and "NT Pwd". The bottom section is a progress bar with columns: "Table", "Directory", "Status", and "Progress".

| User             | LM Hash      | NT Hash                          | LM Pwd 1 | LM Pwd 2 | NT Pwd         |
|------------------|--------------|----------------------------------|----------|----------|----------------|
| Administrator    |              | 31d6cfe0d16ae931b73c59d7e0c089c0 |          |          | empty          |
| Guest            |              | 31d6cfe0d16ae931b73c59d7e0c089c0 |          |          | empty          |
| SUPPORT_388945a0 |              | 34ec619d1d6c952d44ad5898a6815fce |          |          |                |
| Administrator    | 59ab4dfd5... | dc9333bacdeb4a7e09c73dbee36ffed8 | K477EKY  | LLING07  | K477Ekylling07 |
| Guest            |              | 31d6cfe0d16ae931b73c59d7e0c089c0 |          |          | empty          |
| SUPPORT_388945a0 |              | 167b3177504221efaa009a593dc7281e |          |          |                |

| Table        | Directory     | Status       | Progress                         |
|--------------|---------------|--------------|----------------------------------|
| XP free fast | /home/janu... | 84% in RAM   | <div style="width: 84%;"></div>  |
| ● table0     |               | 36% in RAM   | <div style="width: 36%;"></div>  |
| ● table1     |               | 100% in R... | <div style="width: 100%;"></div> |
| ● table2     |               | 100% in R... | <div style="width: 100%;"></div> |
| ● table3     |               | 100% in R... | <div style="width: 100%;"></div> |
| Vista free   | /home/janu... | 100% in R... | <div style="width: 100%;"></div> |
| ● table0     |               | 100% in R... | <div style="width: 100%;"></div> |
| ● table1     |               | 100% in R... | <div style="width: 100%;"></div> |
| ● table2     |               | 100% in R... | <div style="width: 100%;"></div> |
| ● table3     |               | 100% in R... | <div style="width: 100%;"></div> |

Preload:  Brute force:  Pwd found:  Time elapsed:

- Napad s slovarjem: seznami besed ("wordliste").
- Mavrične tabele (MD5, LM, NTLM...).



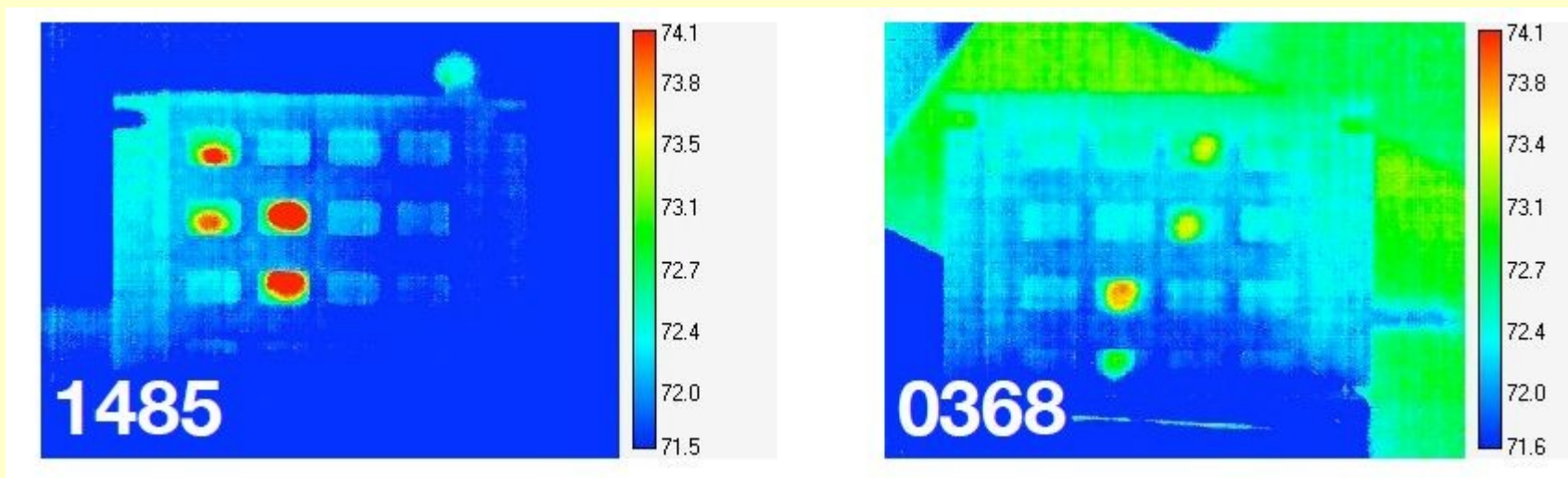


Napad z grobo silo je mogoč tudi v fizičnem svetu...  
Vir in avtorstvo: <<http://www.kvogt.com/autodialer/>>



Vir: Schneier.com, <[http://www.schneier.com/blog/archives/2009/07/information\\_lea\\_1.html](http://www.schneier.com/blog/archives/2009/07/information_lea_1.html)>.

Pri 4-mestnem geslu je vseh možnih kombinacij 10.000. V zgornjem primeru je možnih kombinacij samo še 24. Levo geslo je najbolj verjetno 1986 ali 1968, desno pa 1234.



Keaton Mowery, Sarah Meiklejohn, Stefan Savage. 2011. Heat of the Moment: Characterizing the Efficacy of Thermal Camera-Based Attacks. <[https://db.usenix.org/events/woot11/tech/final\\_files/Mowery.pdf](https://db.usenix.org/events/woot11/tech/final_files/Mowery.pdf)>.

Raziskovalci so ugotovili, da je mogoče z infrardečo kamero beležiti temperaturo posameznih tipk. Pritisnjene tipke ob vnosu PIN-a so toplejše od neuporabljenih, tako da lahko na ta način 'preberemo' kodo tudi, če uporabnik številčnico zakrije z roko. Če posnetek preberejo takoj po vnosu številke, lahko z 80-odstotno natančnostjo povedo, katere tipke so bile pritisnjene, nato pa odstotek pada. Po minuti pade na polovico, po poldrugi minuti pa na 20 odstotkov, ker tipke oddajo toploto. Pri tem je podatke lažje prebrati s plastičnih, saj toploto odvajajo počasneje od kovinskih.

# **Napadi na strojno opremo**

# Napad na krmilnik trdega diska, mrežne kartice,...

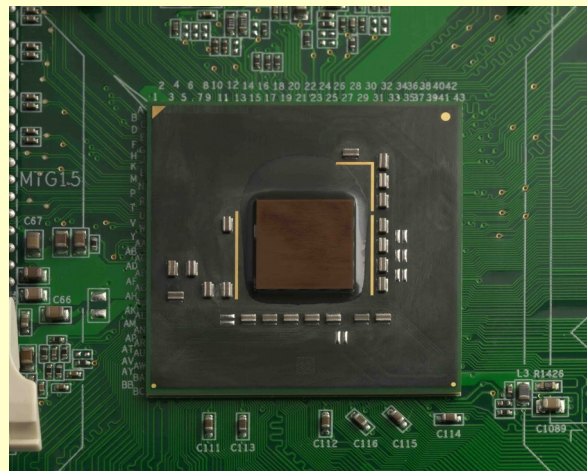
```
archimede:~/nicssh$ nicssh -c 10.4.4.233
Connecting to 10.4.4.233
ICMP Echo Reply from OS - no nicfw
Goodbye!
archimede:~/nicssh$ nicssh -c8 10.4.4.234
Connecting to 10.4.4.234
ICMP Echo Reply from nicfw (Windows system)
Requesting tcp/80 with cloaking (-8)
nicssh> ?
help memory* sniff* send* reboot cleanup quit
nicssh> cleanup
Clean up requested - wiping GPU...
Received packet from NIC: nicssh wiped
Remote hardware is 00:12:79:94:a3:52
Remote loading standard firmware via UDP.....done
Connection with remote lost, nicfw wiped
Goodbye!
archimede:~/nicssh$ nicssh -ig 10.4.4.234
Connecting to 10.4.4.234
ICMP Echo Reply from OS - no nicfw
Installation requested: nicfw (-i), nicssh (-g)
Remote hardware on LAN is 00:12:79:94:a3:52
Remote loading nicfw via UDP.....done
Connection lost (expected) - please wait...
ICMP Echo Reply from nicfw (Windows system)
Requesting GPU from nicfw...nVidia
Remote loading nicssh via UDP.....done
Connecting to nicssh
nicssh> ?
help memory* sniff* send* reboot cleanup quit
nicssh> quit
Disconnecting from nicssh
Goodbye!
archimede:~/nicssh$ cd
archimede:~$
```



```
jeroen@spritesws:~$ telnet localhost 4444
Trying ::1...
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Open On-Chip Debugger
> halt
target state: halted
target halted in Thumb state due to debug-request, current mode
: Supervisor
cpsr: 0x000000f3 pc: 0x0000a3c6
MMU: disabled, D-Cache: disabled, I-Cache: disabled
> load_image hack/jump.bin 0x78 bin
4 bytes written at address 0x00000078
downloaded 4 bytes in 0.006731s (0.580 KiB/s)
> load_image hack/hack.bin 0xffe30000 bin
144 bytes written at address 0xffe30000
downloaded 144 bytes in 0.029191s (4.817 KiB/s)
> resume
>
```

# SMM korenski kompleti (Ring -2)

- Ring -2: System Management Mode (SMM) je najbolj privilegiran način delovanja procesorja na x86/x86\_64 arhitekturah.
- Ring -3: napad na vPro/AMT čipe.

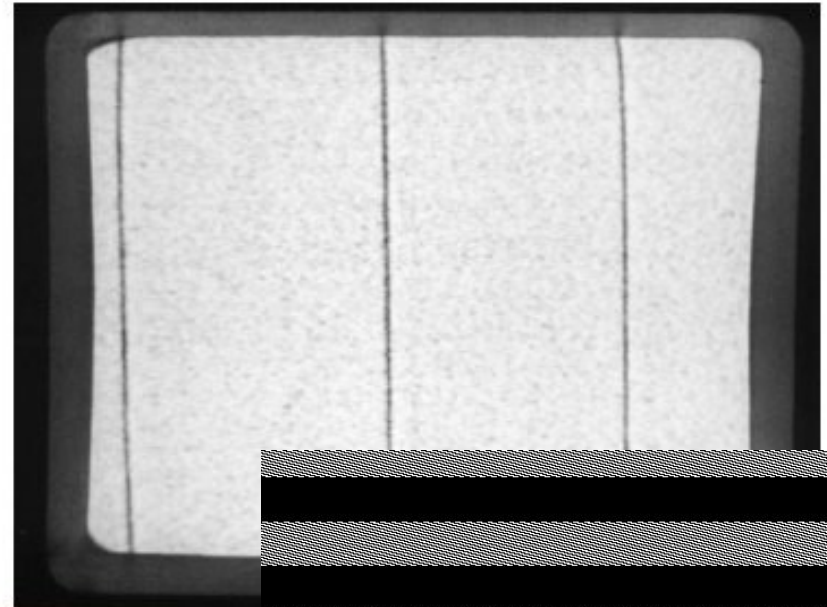


Slika Q35 čipa (MCH) v katerega so namestili korenski komplet. Več informacij: <<https://slo-tech.com/novice/t369218>>

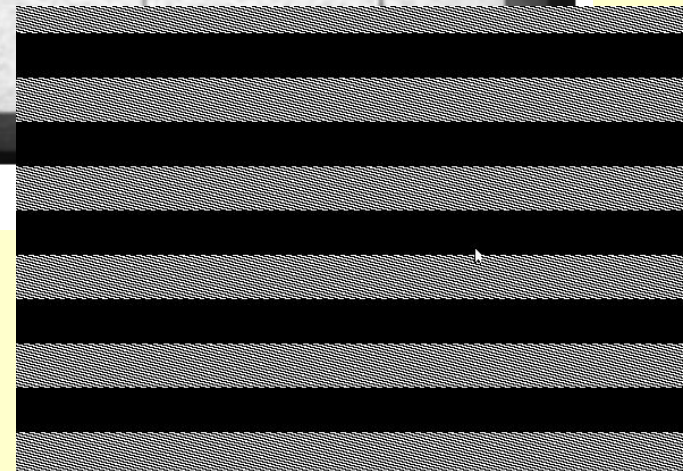
Vir in avtorstvo: Joanna Rutkowska, <<http://theinvisiblethings.blogspot.com/2009/08/vegas-toys-part-i-ring-3-tools.html>>.

- **Attacks on and Countermeasures for USB Hardware Token Devices,** <[http://www.grandideastudio.com/files/security/tokens/usb\\_hardware\\_token.pdf](http://www.grandideastudio.com/files/security/tokens/usb_hardware_token.pdf)>, 2000.
- **Hit by a Bus: Physical Access Attacks with Firewire,** <[http://www.security-assessment.com/files/presentations/ab\\_firewire\\_rux2k6-final.pdf](http://www.security-assessment.com/files/presentations/ab_firewire_rux2k6-final.pdf)>, 2006.
- **Implementing and Detecting a PCI Rootkit,** <[http://www.ngssoftware.com/research/papers/Implementing\\_And\\_Detecting\\_A\\_PCI\\_Rootkit.pdf](http://www.ngssoftware.com/research/papers/Implementing_And_Detecting_A_PCI_Rootkit.pdf)>, 2006.

# Tempest napad



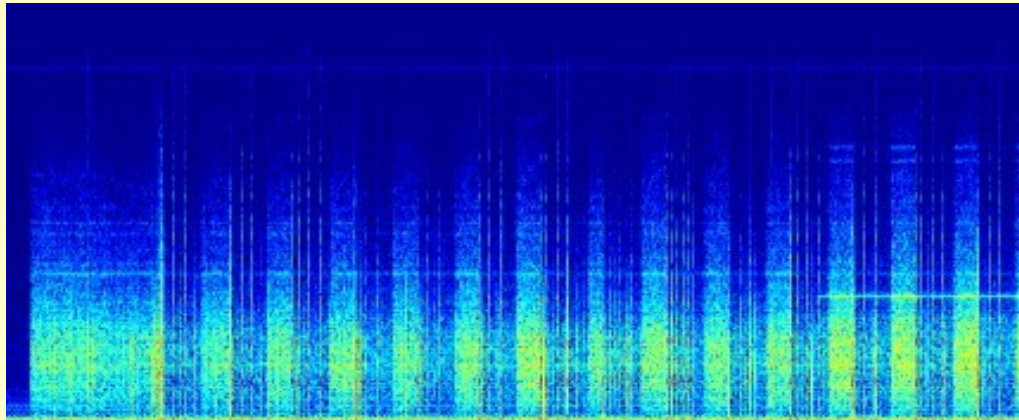
Vir: prosojnice Markusa G. Kuhna in Rossa J. Andersona "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations"





# Tempest napad

- Prestrezanje elektromagnetnih signalov kontrolerja trdega diska (tempest napad), za kar ni potreben fizičen ali mrežni stik z računalnikom.



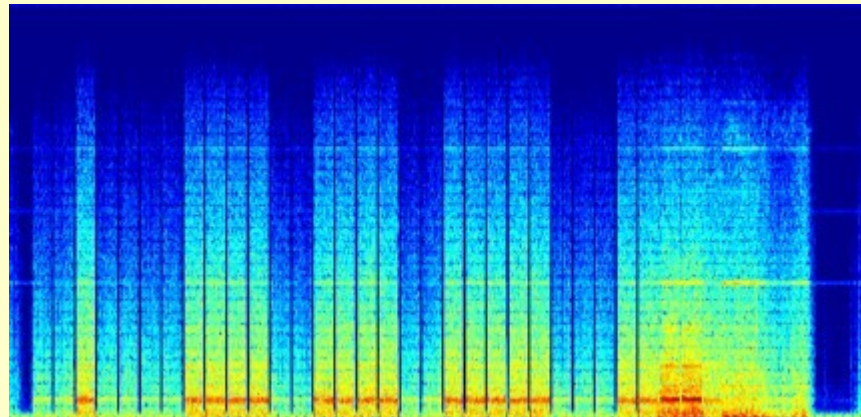
- Sonogram elektromagnetnih signalov ob pisanju na trdi disk. Avtor je na podlagi spremljanja elektromagnetnih signalov lahko rekonstruiral kdaj se zapisujejo enke in kdaj ničle. Vir in avtorstvo: Oğuz Berke Durak, Hidden Data Transmission by Controlling Electromagnetic Emanations of Computers, <<http://abaababa.ouvaton.org/tempest/>>.

# Tempest napad

Tempest napad na RAM

Poslano:

- 0010 0001 1110 0111 1001 1111 0001 1001



Sprejeto:

- 0010 0001 1110 0111 1001 1111 0001 1110

Vir in avtorstvo: Oğuz Berke Durak.

# Tempest napad

- Tempest napad na volilne naprave na Nizozemskem, 2006



Vir in avtorstvo: Wels, Wessling, Gonggrijp in Németh, organizacija "*We don't trust voting computers*", <<http://www.wijvertrouwenstemcomputersniet.nl/English>>  
Video na YouTube: <<http://www.youtube.com/watch?v=B05wPomCjEY>>.

# General guidelines for security\*

1. Do not assume anything. / Ne predpostavljaj ničesar.
2. Trust no-one, nothing. / Nikomur, ničemur ne zaupaj.
3. Nothing is secure. / Nič ni varno.
4. Security is a trade-off with usability. / Večja varnost pomeni manjšo udobnost.
5. Paranoia is your friend. / Paranoja je tvoja prijateljica.

\* **Splošne varnostne smernice**, iz priročnika orodja *Advanced Intrusion Detection Environment*, "The Aide manual" <<http://www.cs.tut.fi/%7Erammer/aide/manual.html>>.

**Zaščita**

# Osnovna zaščita

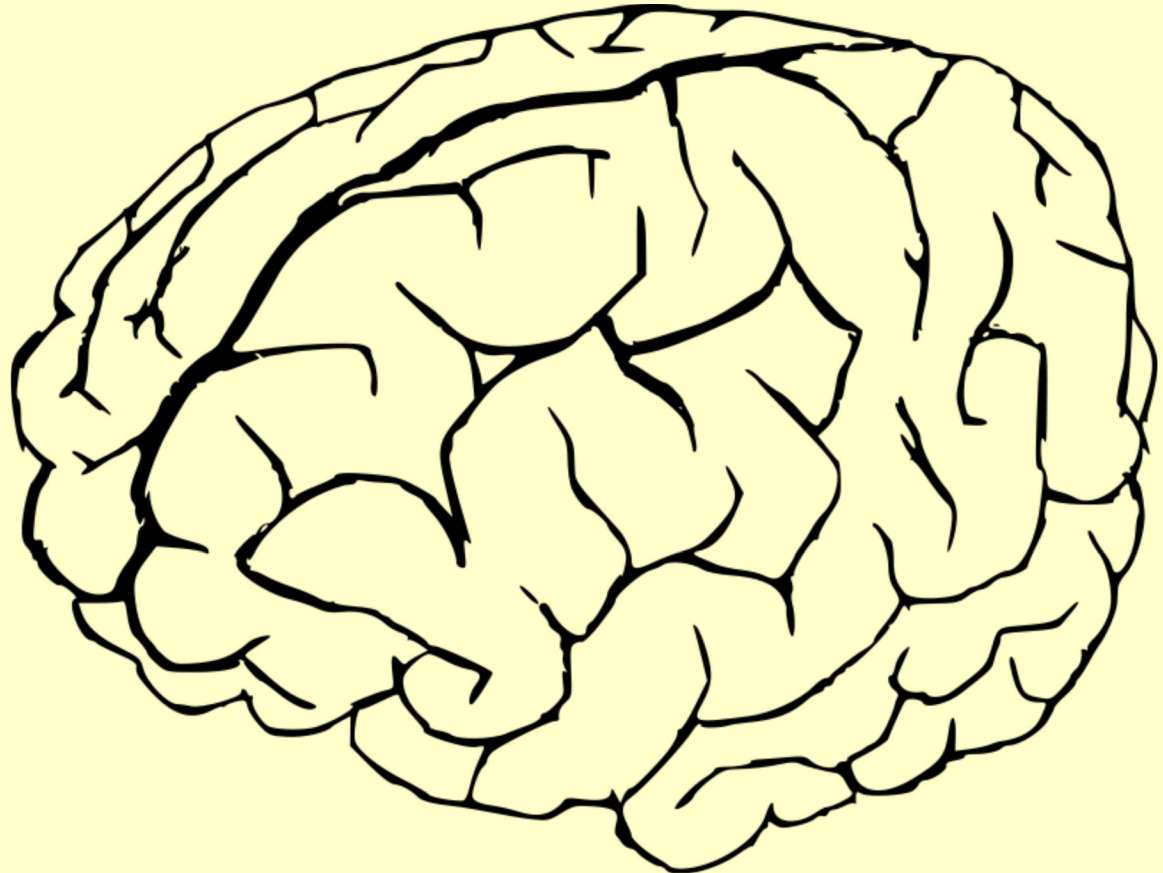
- **Nekatere tehnike osnovne zaščite računalniških sistemov:**
  - uporaba ustreznih gesel;
  - pazljivost pri večuporabniških sistemih;
  - redno posodobljen sistem;
  - požarni zid;
  - uporaba protivirusnih in protismetnih (antispymware) programov;
  - ustrezna varnostna kultura;
  - fizična varnost;
  - ...

# Naprednejša zaščita

- **Nekatere tehnike naprednejše zaščite:**
  - varno brisanje podatkov;
  - šifriranje:
    - šifriranje razdelkov trdih diskov kjer so shranjeni občutljivi podatki (tudi začasnega "swap" pomnilnika);
    - šifriranje elektronske pošte;
  - anonimizacija uporabe interneta (preprečimo analizo prometnih podatkov):
    - "remailerji";
    - anonimizacijska omrežja.

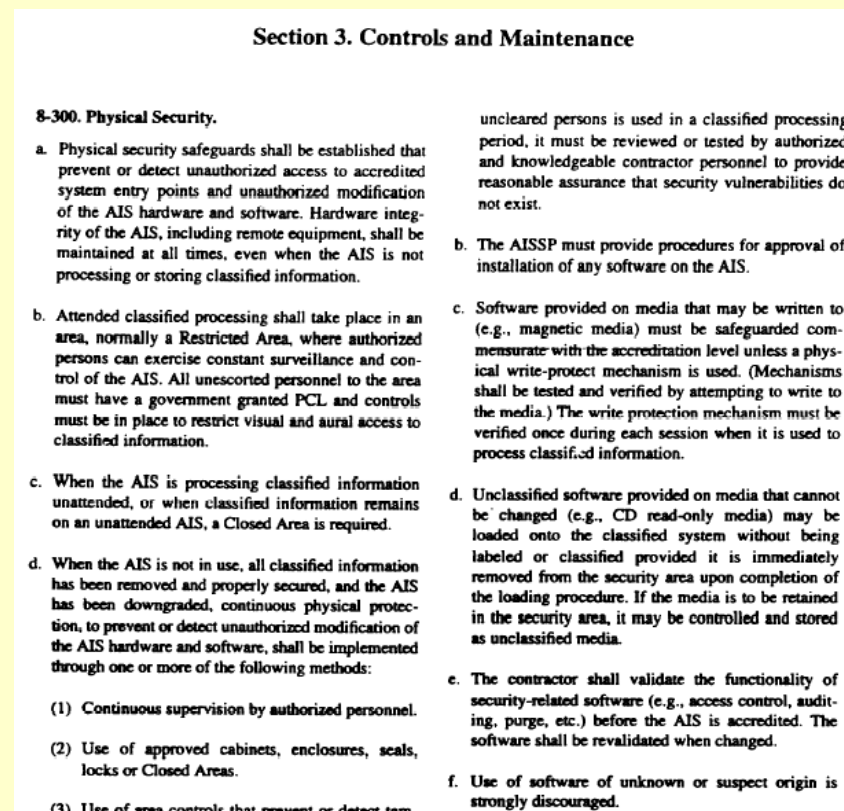
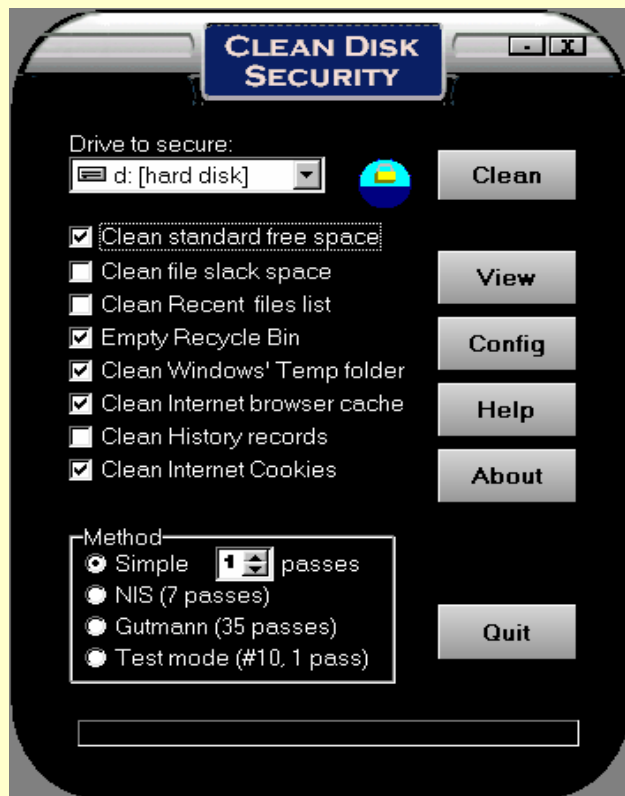
# Še bolj napredna zaščita

- Nekaj znanja, **doslednosti** in zdrava pamet. ;-)





# Trajno brisanje podatkov



Varno brisanje s Clean Disk Security (pri dnevniških datotečnih sistemih je neučinkovito!) ter ameriški vojaški priročnik *National Industrial Security Program Operating Manual* (NISPOM 1995), poglavje 8, sekcija 3 (Controls and Maintenance), ki predpisuje varno brisanje podatkov.

# Trajno brisanje podatkov

```
Darik's Boot and Nuke 1.0.7
----- Options -----
Entropy: Linux Kernel (urandom)
PRNG:    Merseenne Twister (mt19937ar-cok)
Method:  DoD Short
Verify:  Last Pass
Rounds:  1
----- Statistics -----
Runtime:
Remaining:
Load Averages:
Throughput:
Errors:

----- Wipe Method -----

Quick Erase                syslinux.cfg: nuke="dwipe --method dodshort"
RCMP TSSIT OPS-II         Security Level: Medium (3 passes)
▶ DoD Short
DoD 5220.22-M
Gutmann Wipe
PRNG Stream

The American Department of Defense 5220.22-M short wipe.
This method is composed of passes 1,2,7 from the standard wipe.

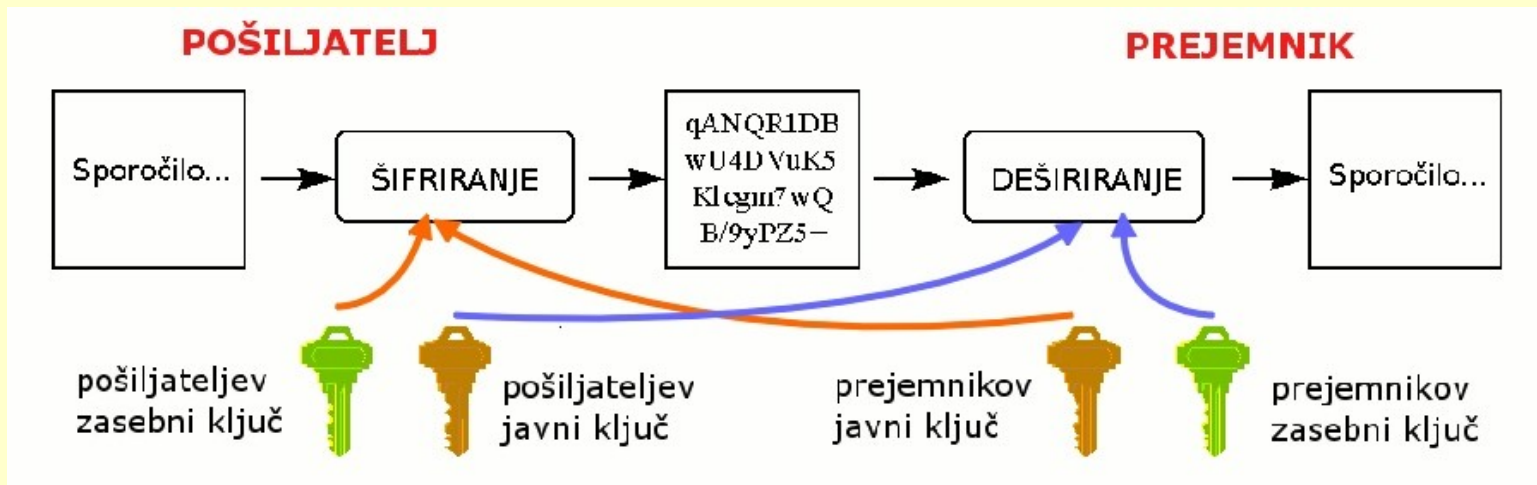
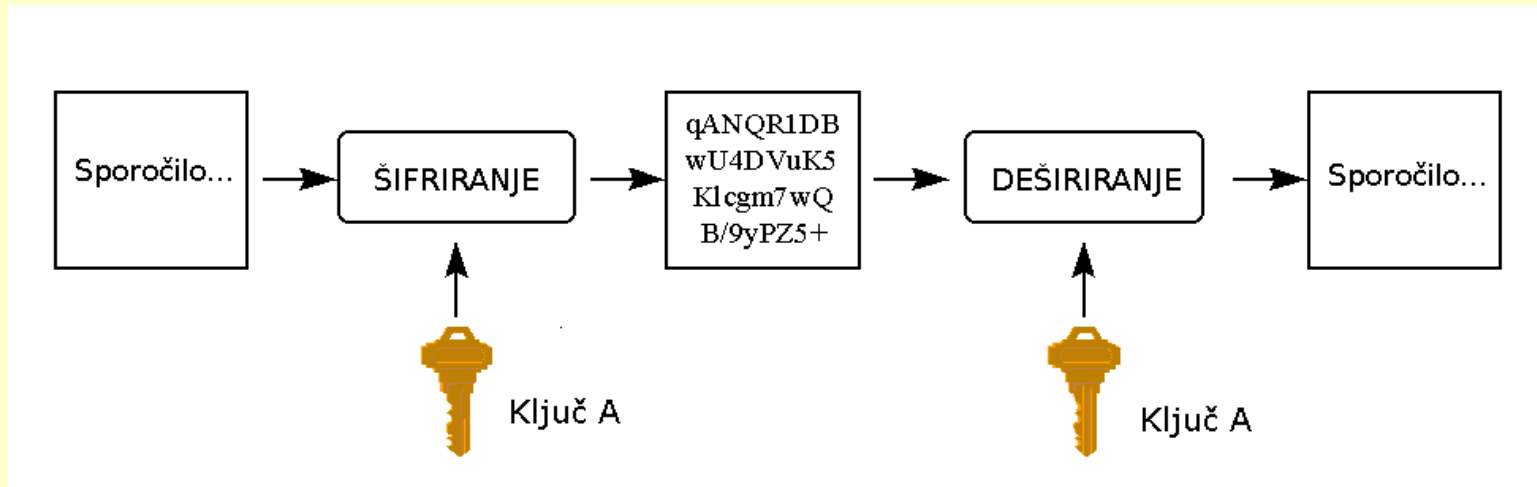
J=Up K=Down Space=Select
```

**DBAN - Darik's Boot and Nuke**, orodje namenjeno uničevanju vsebine trdih diskov. Zažene se iz zagonske diskete. < <http://dban.sourceforge.net/>>. Vir in avtorstvo: dokumentacija programa.

# Kriptografija

- Pri varovanju podatkov uporabljamo simetrične, asimetrične in zgostitvene algoritme.
- **Simetričnimi algoritmi** ali algoritmi z zasebnim ključem: imamo samo en ključ, s katerim zašifriramo in dešifriramo sporočilo. Običajno so ti algoritmi hitri, težko pa je varno izmenjati ključ. Problem predstavlja tudi *število ključev* - vsak uporabnik mora imeti za vsakega dopisovalca svoj ključ.
- **Asimetrični algoritmi** ali algoritmi z javnim ključem: uporabnik ima dva ključa, enega objavi, drugi ostane tajen. Vsi, ki mu hočejo poslati sporočilo, bodo uporabili njegov javni ključ za šifriranje sporočila. Dešifriral pa ga bo lahko le on sam s svojim tajnim ključem in javnim ključem pošiljatelja. Te metode so računsko bolj zahtevne in zato počasnejše kot simetrične.
- **Zgostitveni algoritmi** poljubno dolg tekst preslikajo v število fiksne dolžine, kar je uporabno za digitalni podpis. Najbolj znana algoritma sta MD5 in SHA.

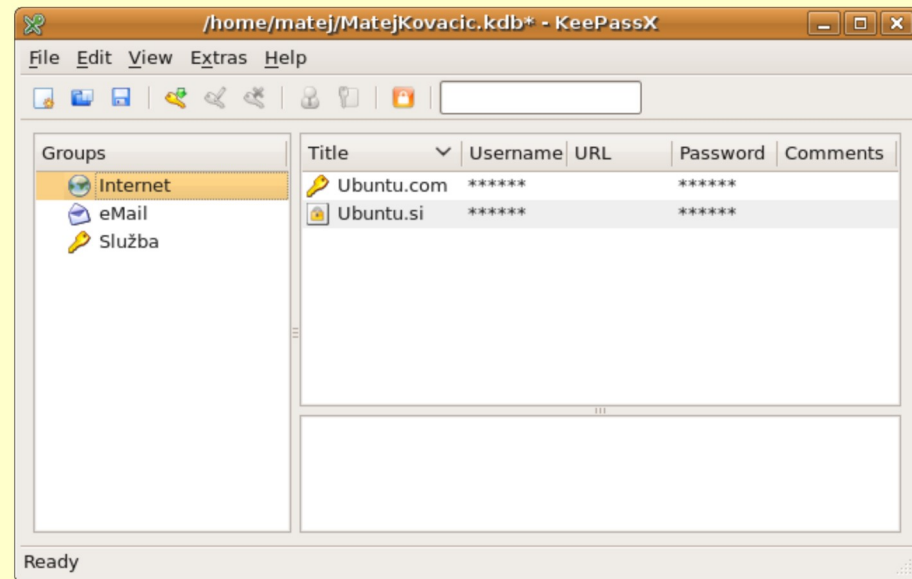
# Kriptografija



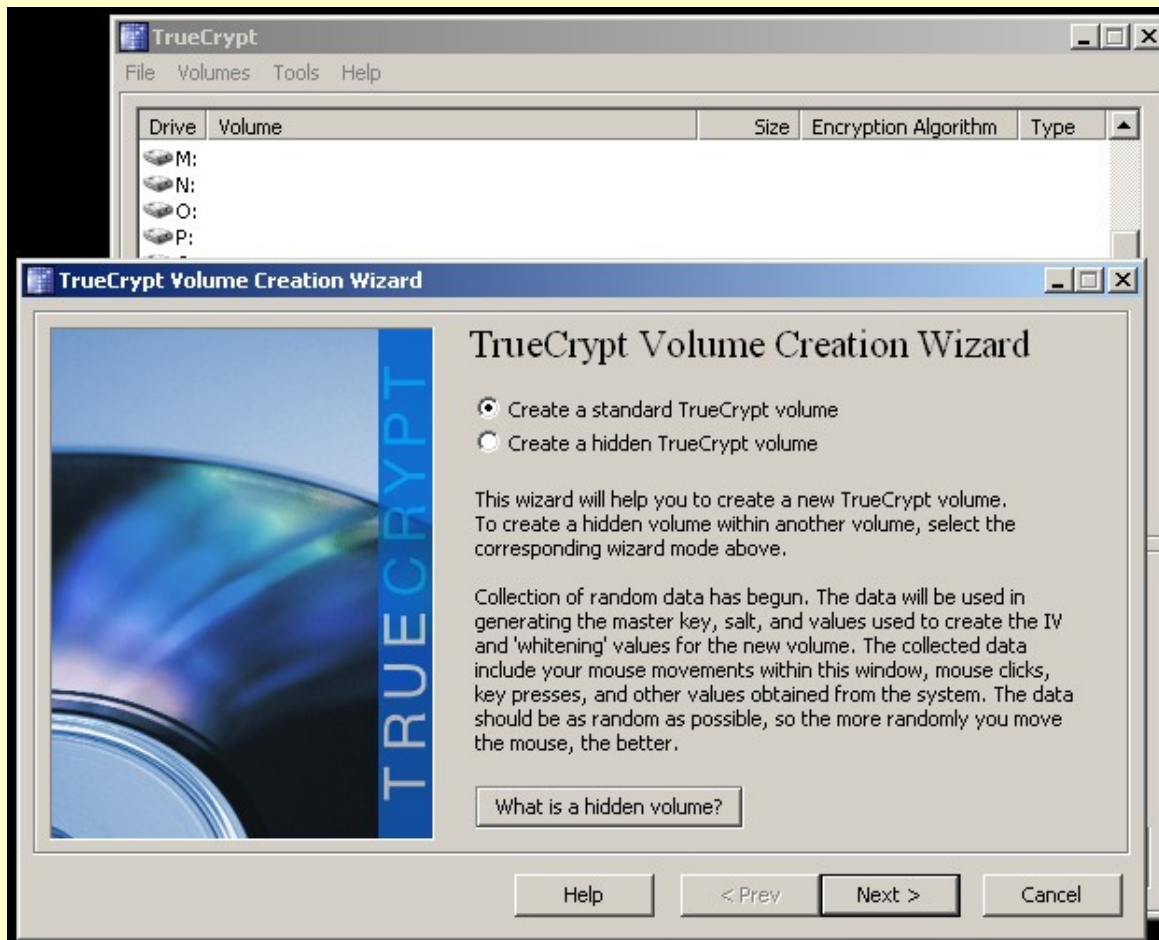
Shematski prikaz simetrične kriptografije in kriptografije z javnimi ključi.

# Shrambe gesel/ključev

- Šifrirni ključi so lahko shranjeni:
  - kot kontrolna vsota (npr. SAM/SYSKEY, možno razbijanje!),
  - v posebnem programu (npr. *KeePassX*, vgrajena programska varnostna naprava v *Firefoxu*, itd.),
  - v kontejnerju,
  - v strojnih žetonih.



# Šifriranje nosilcev podatkov



Šifriranje (navideznih) diskovnih particij s programom *TrueCrypt*. Program omogoča tudi skrite šifrirane particije.

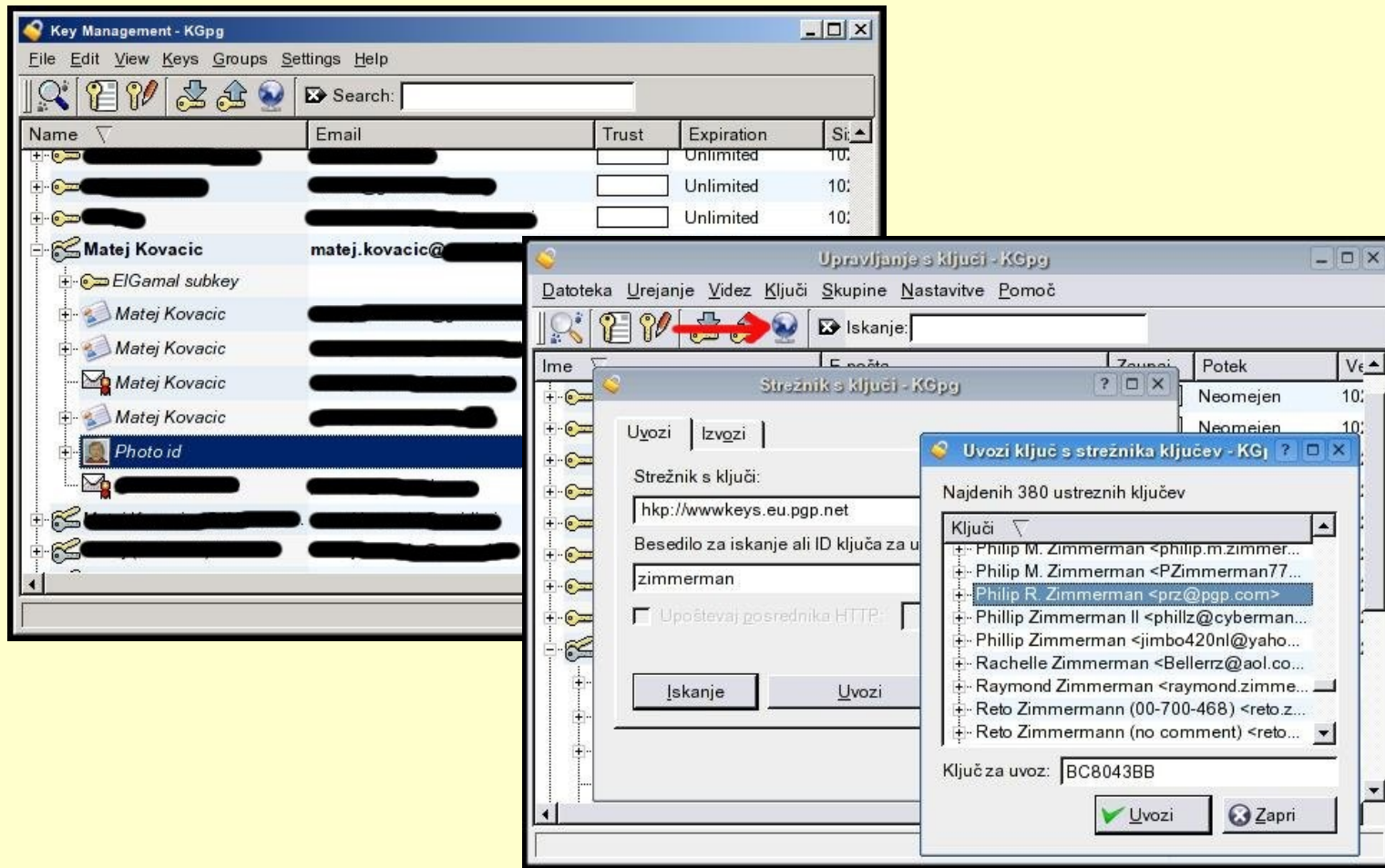
# Šifrirni kontejner v LUKS formatu



Omogoča tudi menjavo gesel:

- dodamo novo geslo
- odstranimo starega.

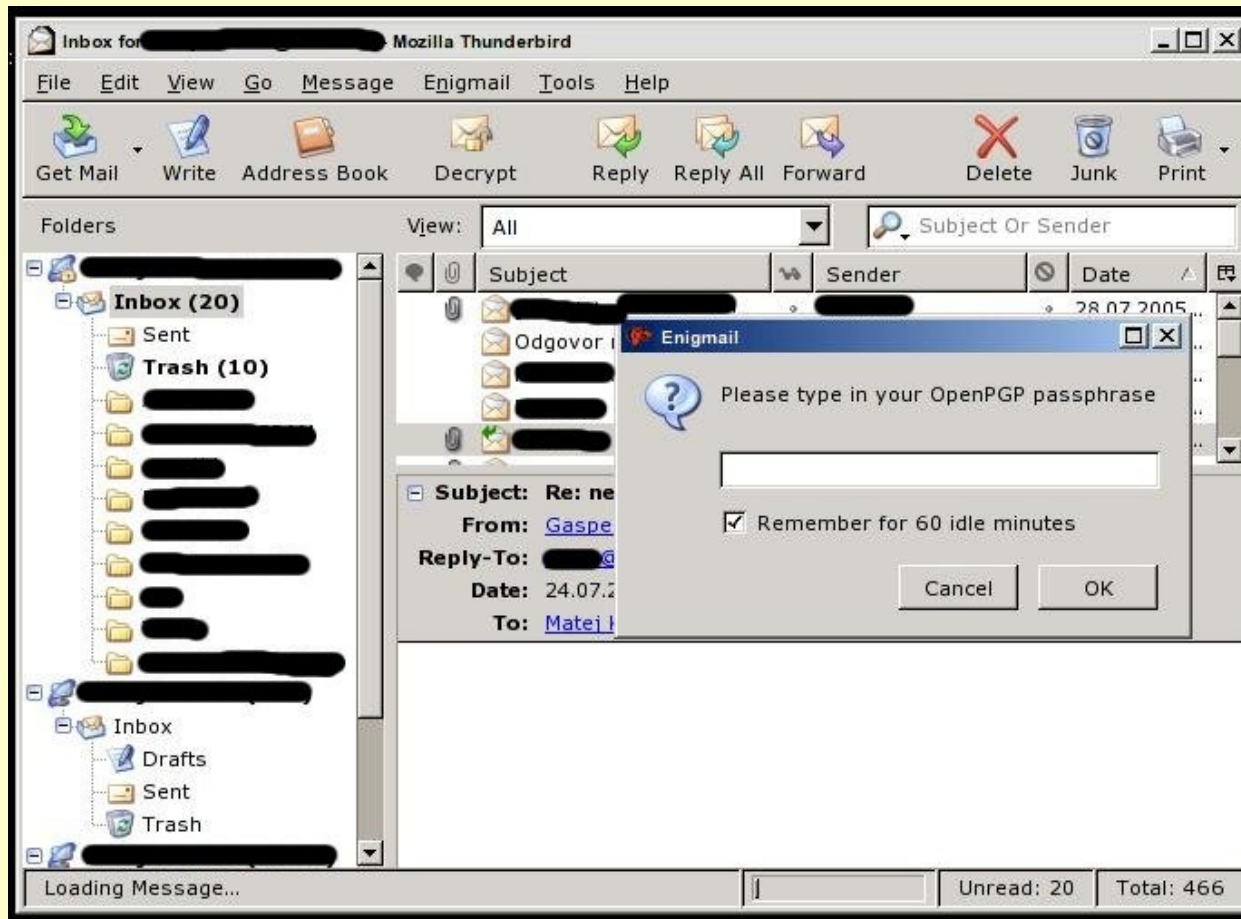
# Šifriranje e-pošte



Šifrirni program *GPG* (*GNU Privacy Guard*) - upravljanje s šifrirnimi ključi v okolju Linux.

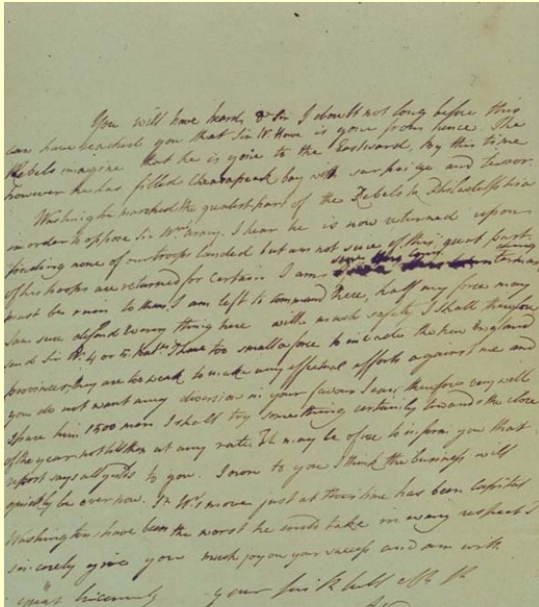


# Šifriranje e-pošte



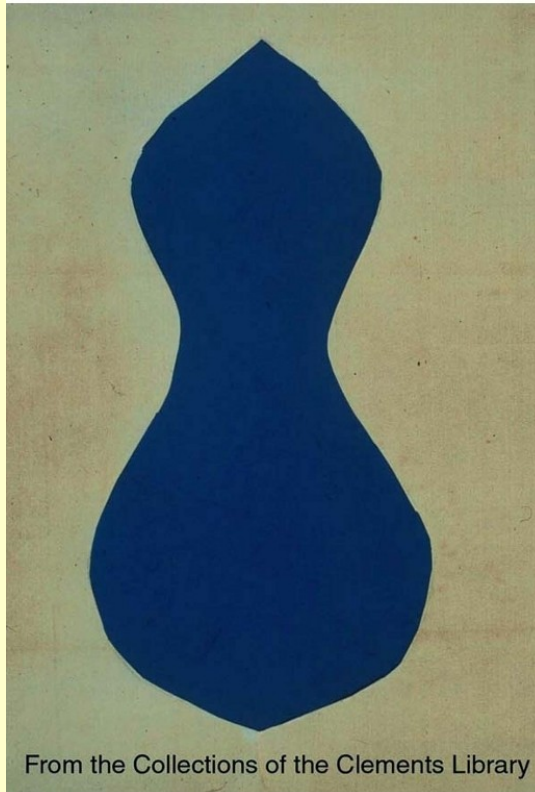
Šifriranje elektronske pošte v odprtokodnem odjemalcu elektronske pošte *Mozilla Thunderbird* z dodatkom *Enigmail*.

# Skrivanje podatkov

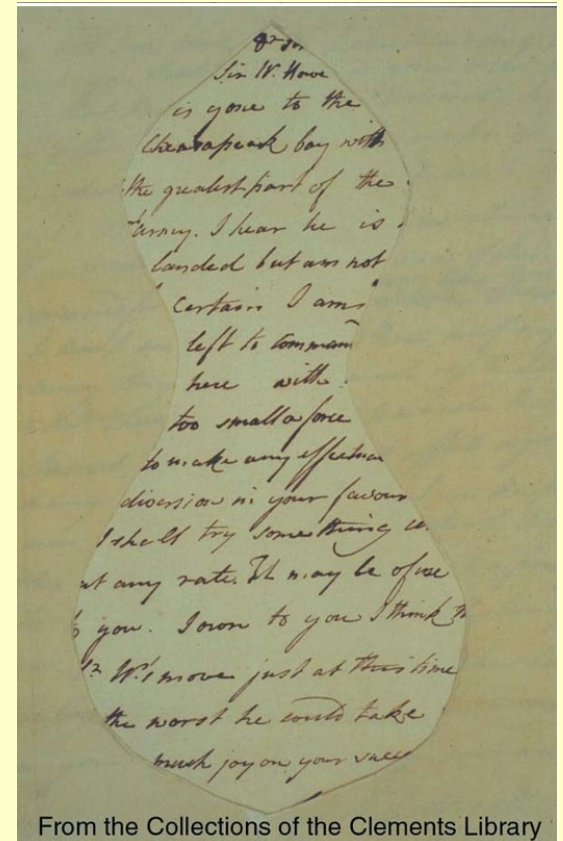


You will have heard, & so I should not long before this  
can have heard that Sir W. Howe is your prisoner. The  
Rebels imagine that he is gone to the Westward, by this time  
however he has filled Chesapeake Bay with his boats and troops.  
Washington attacked the greatest part of the Rebels in Delwarell's Bay  
in order to oppose to W. Howe, I hear he is now returned upon  
pending none of our troops landed, but we are not sure of this, great parts  
of his boats are returned for certain. I am ~~not~~ <sup>not</sup> ~~at all~~ <sup>at all</sup> ~~at all~~ <sup>at all</sup>  
must be even so that I am left to command here, half my force may  
be some distant Army being here with such rapid I shall therefore  
and be the 4 or 5000, these too small a force to undertake to have England  
and however they are too weak to make any effectual effort against me and  
you do not want any diversion in your favour, I am therefore very well  
I have been 1500 men I should try something certainly toward the close  
of the year, whether at any rate, it may be of use to inform you that  
I must say adieu to you. I own to you I think the business will  
quickly be over now. Sir W. Howe just at this time has been captured  
Washington have been the worst he could take in every respect I  
I'm really yours your true friend and am with  
great sincerity your friend  
J. Burgoyne

From the Collections of the Clements Library



From the Collections of the Clements Library



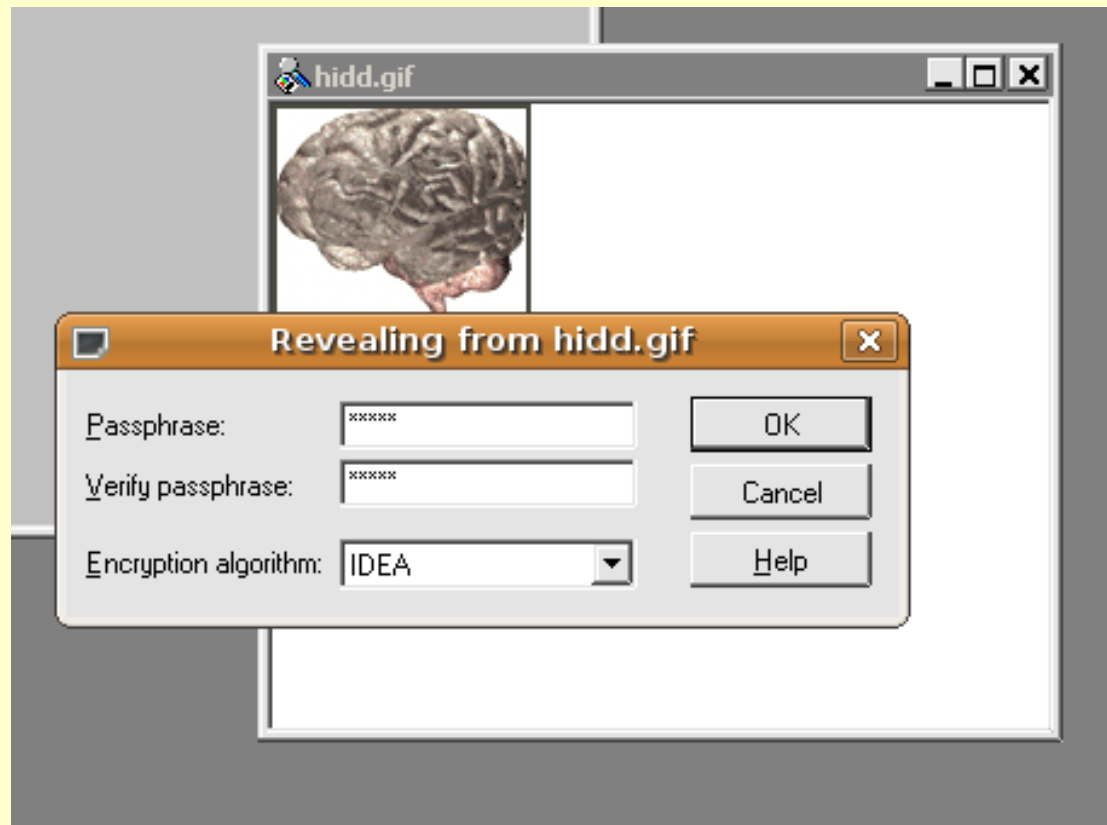
Sir W. Howe  
is gone to the  
Chesapeake Bay with  
the greatest part of the  
Army. I hear he is  
landed but we are not  
certain I am  
left to command  
here with  
too small a force  
to make any effectual  
diversion in your favour  
I should try something  
at any rate. It may be of use  
to you. I own to you I think  
that W. Howe just at this time  
the worst he could take  
with great joy on your side

From the Collections of the Clements Library

Maskirano pismo: 10. avgust 1777, Henry Clinton -> John Burgoyne.

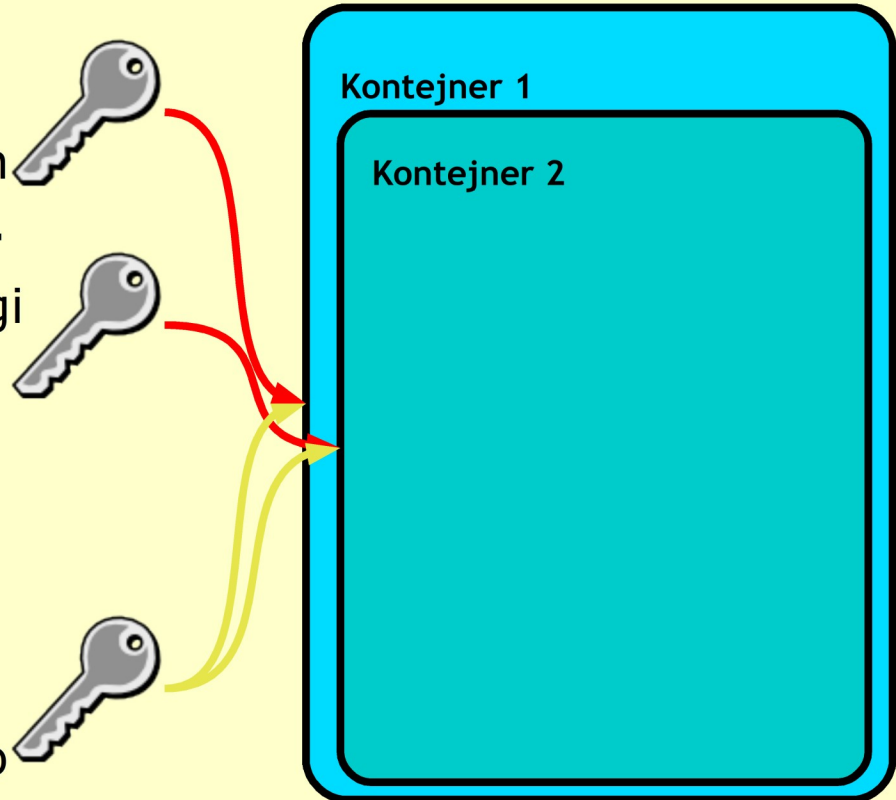
<http://www.si.umich.edu/spies/letter-1777august10-1.html>

# S-Tools



# Skrivanje podatkov v gnezdene šifrirne kontejnerje (verodostojno zanikanje)

- **Prvi ključ** odklene prvi kontejner. Podatki se lahko zapisujejo v celoten kontejner, tudi v skritega.
- **Drugi ključ** odklene drugi kontejner, ki ne dovoli pisanja podatkov v nadrejeni, prvi kontejner.
- **Tretji ključ** odklene prvi in drugi kontejner: v prvi kontejner lahko zapisujemo, vendar ne po območju kjer se nahaja skriti drugi kontejner.



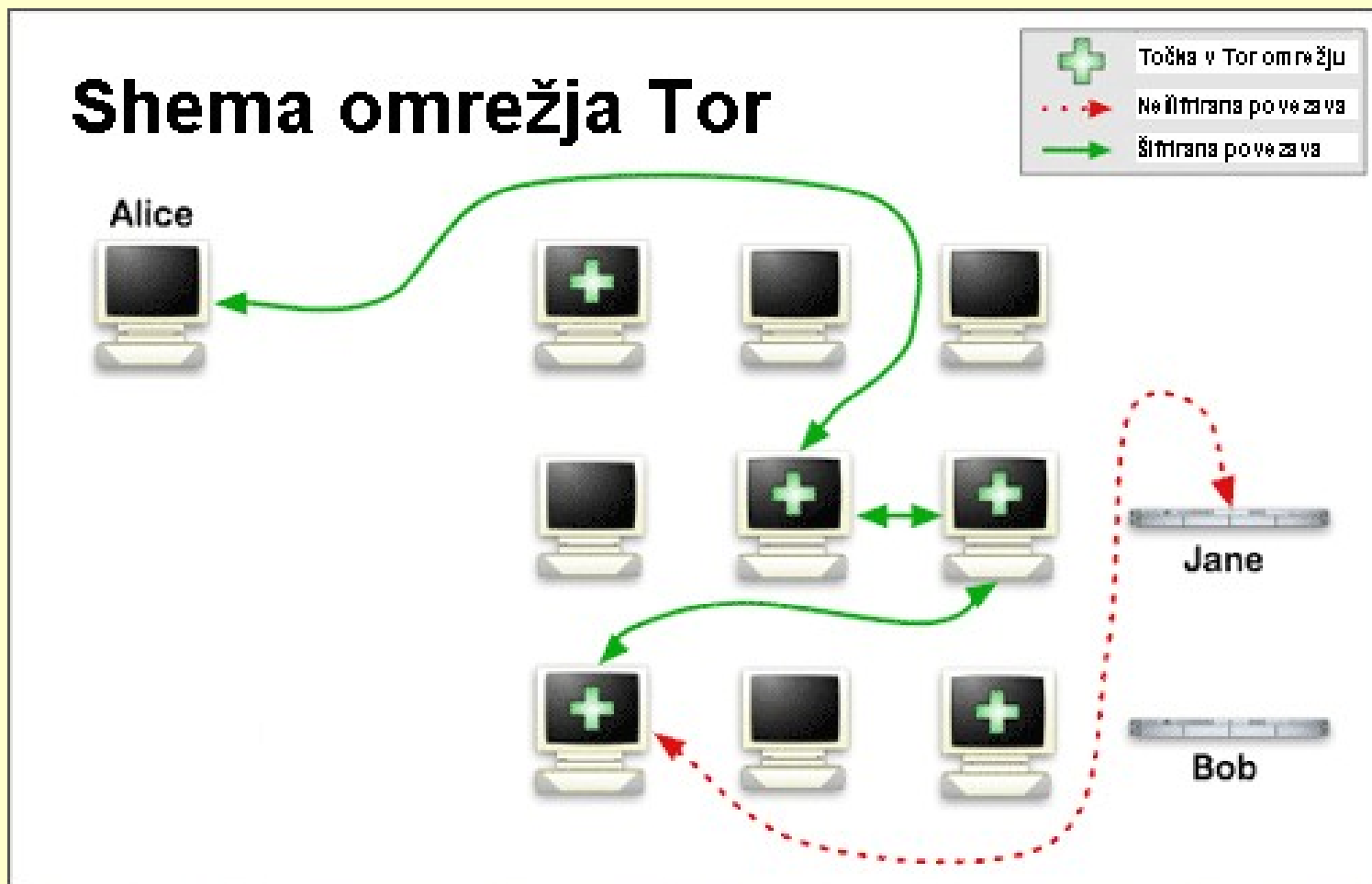
# Anonimno pošiljanje e-pošte

The screenshot shows the 'Mixminion Message Sender 1.2.1-Beta' application window. The interface includes a menu bar with 'File', 'Mixminion', 'Options', and 'Help'. The main area contains several input fields and buttons: 'From' (set to 'Anon User'), 'To', 'NewsGroup' (set to 'alt.privacy.anon-server'), 'Subject', and 'References'. There are also checkboxes for 'Debug', 'Use .sig', 'SURB Reply', and 'Include SURB'. A 'Number of Hops' dropdown is set to '6', and a 'Mail2News Gateway' dropdown is set to '@m2n.mixmin.net'. At the bottom, there are buttons for 'Reset form', 'Clear Message', 'Queue Msg Only', 'Clear Form when Sending', and 'Send Message'. The window title bar shows standard Windows window controls.

Pošiljanje elektronske pošte preko s pomočjo "remailer-ja" *Mixminion*. Uporaba programa omogoča tudi anonimno odgovarjanje na anonimna sporočila. Sporočila potujejo čez več anonimizacijskih strežnikov (tim. *mixi*) v šifrirani obliki.

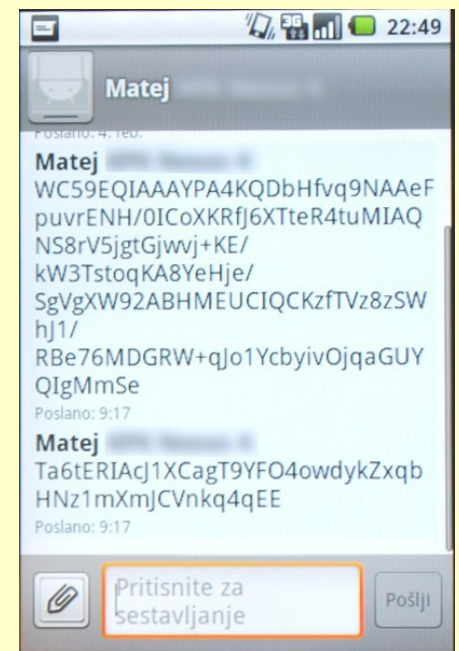
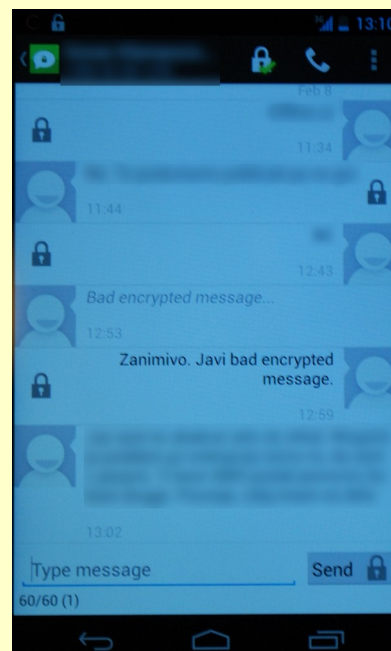
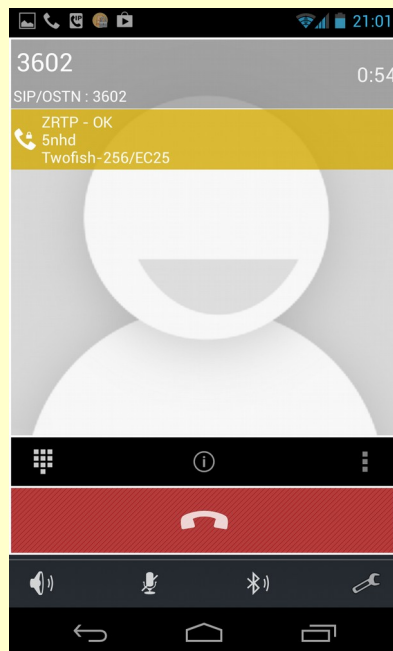
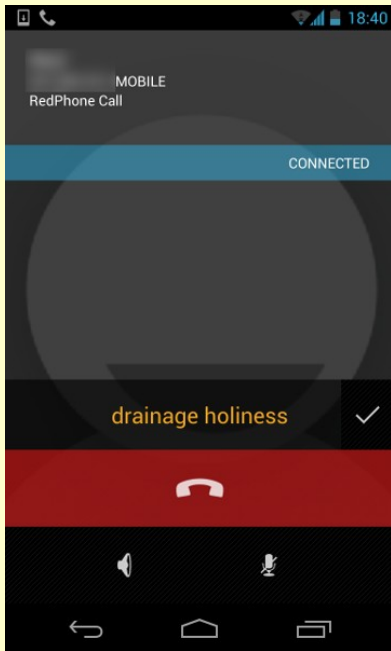
# Anonimizacijsko omrežje Tor

## Shema omrežja Tor



Prikaz delovanja anonimizacijskega omrežja *Tor*.

# Varnost mobilne telefonije





**Vprašanja?**