Varnost informacijskih sistemov

Matej Kovačič

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 tajenja (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

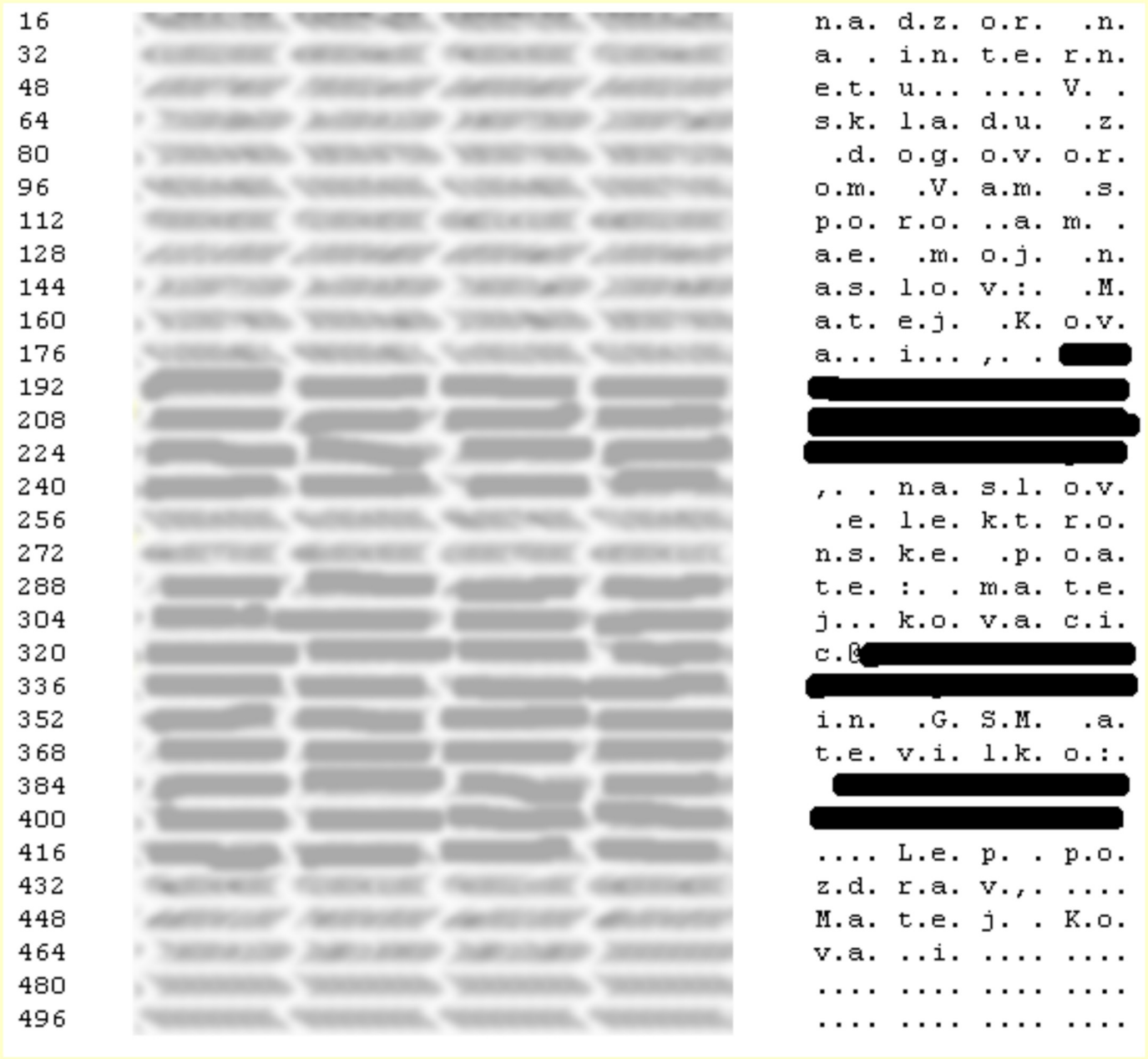
- Nevarnost zasega podatkov.
- Nevarnost podtikanja prikritega mehanizma (npr. programske aplikacije ali strojnega dodatka), s katerim napadalec pridobi dostop do računalnika ali si ustvari možnosti za krajo gesel.
- Zavržene računalniške komponente, ki vsebujejo trajne pomnilnike (trdi diski, tiskalniki,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


SUROVINA
ZA
PAPIR

“Bump key”

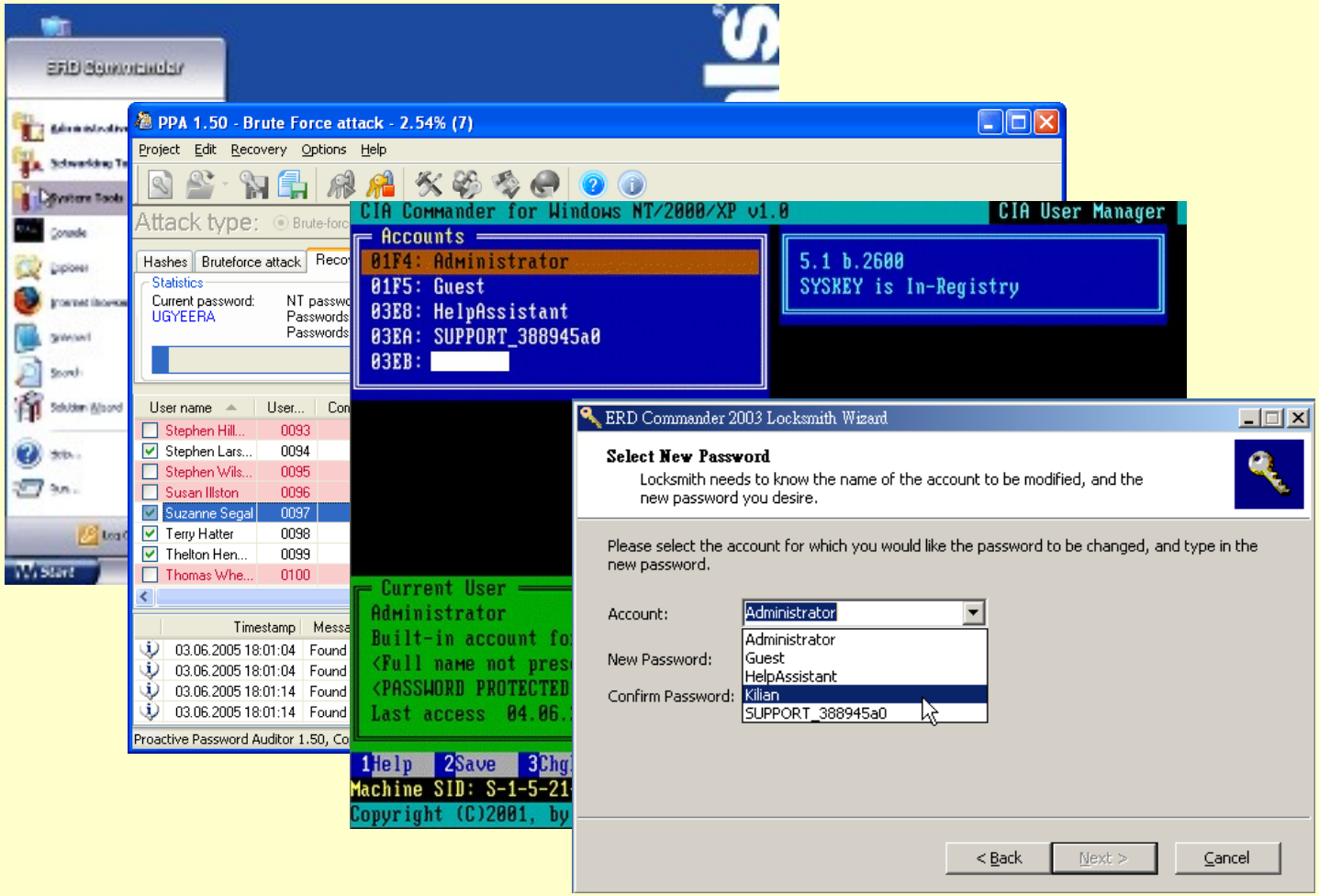
Obnavljanje “izbrisanih” podatkov

- 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.
- Vsebino že izbrisanih datotek je z različnimi orodji in tehnikami mogoče obnoviti deloma ali v celoti.



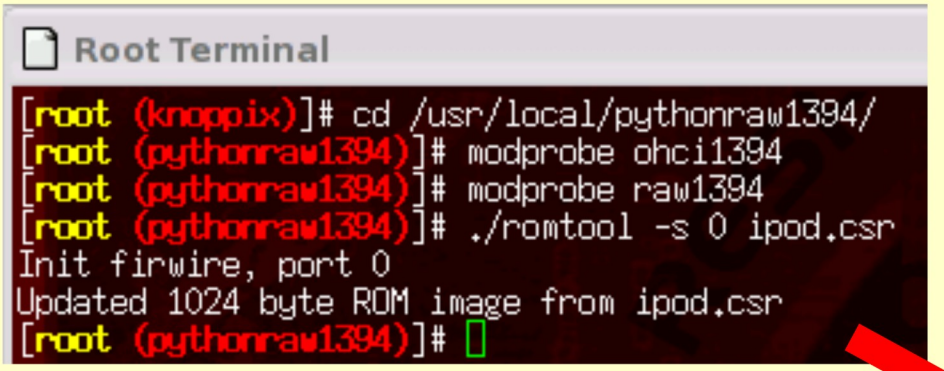
Forenzična analiza diska z orodjem Autopsy Forensic Browser.

“Obnavljanje” Windows gesel

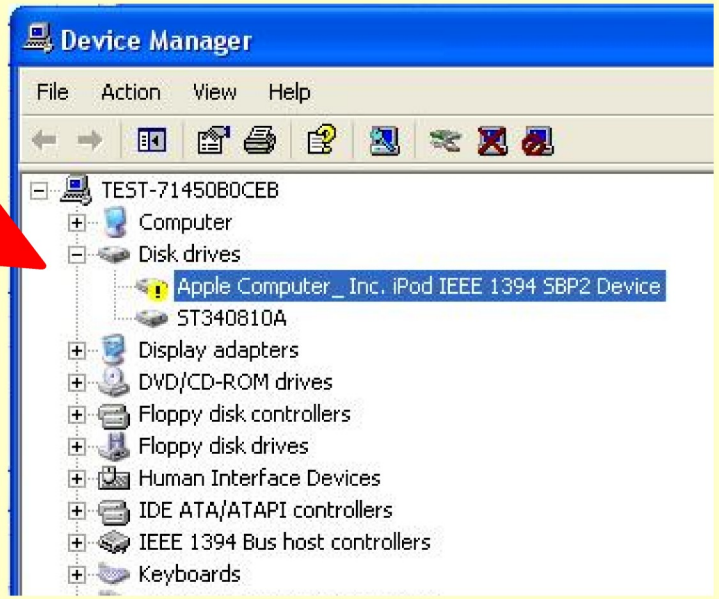


Orodja za “obnavljanje” “pozabljenih” gesel za dostop do operacijskega sistema Windows (zahtevajo fizični dostop).

Zaseg RAM-a preko FireWire vmesnika



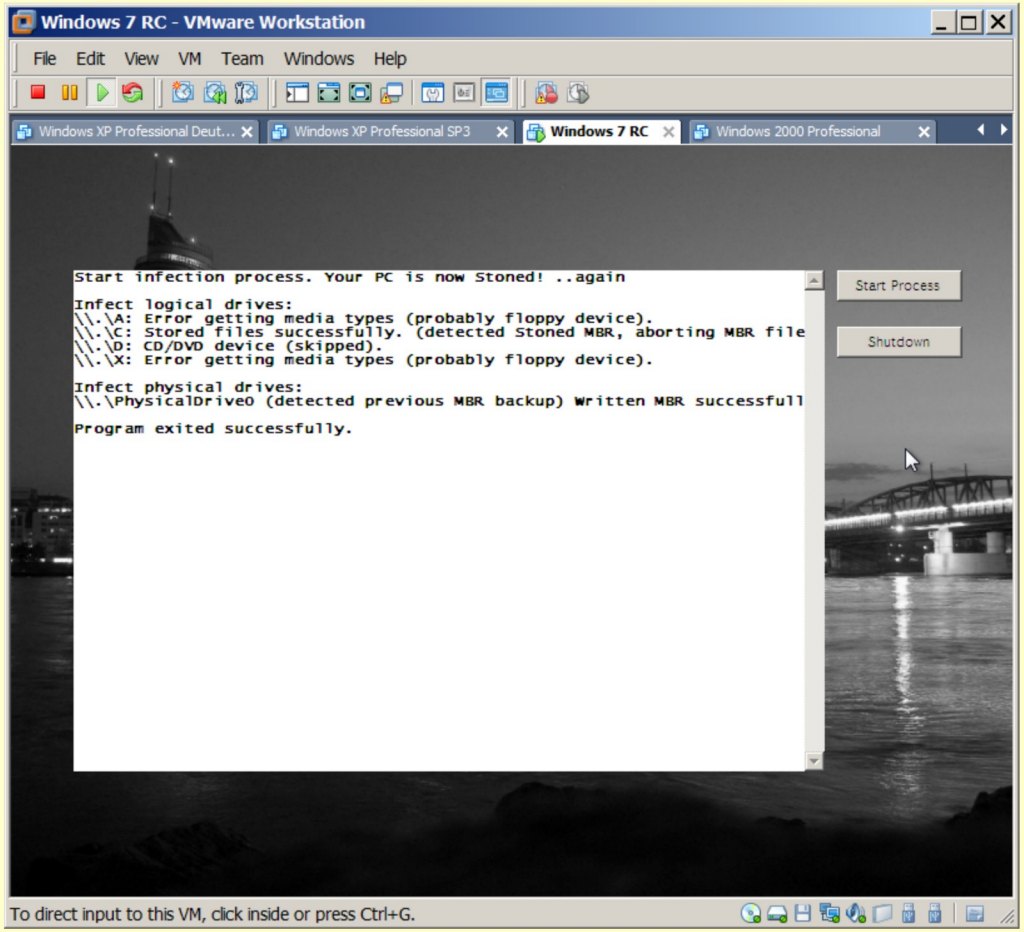
S programom romtool se v računalniku z Linuxom pretvarjamo, da smo iPod...



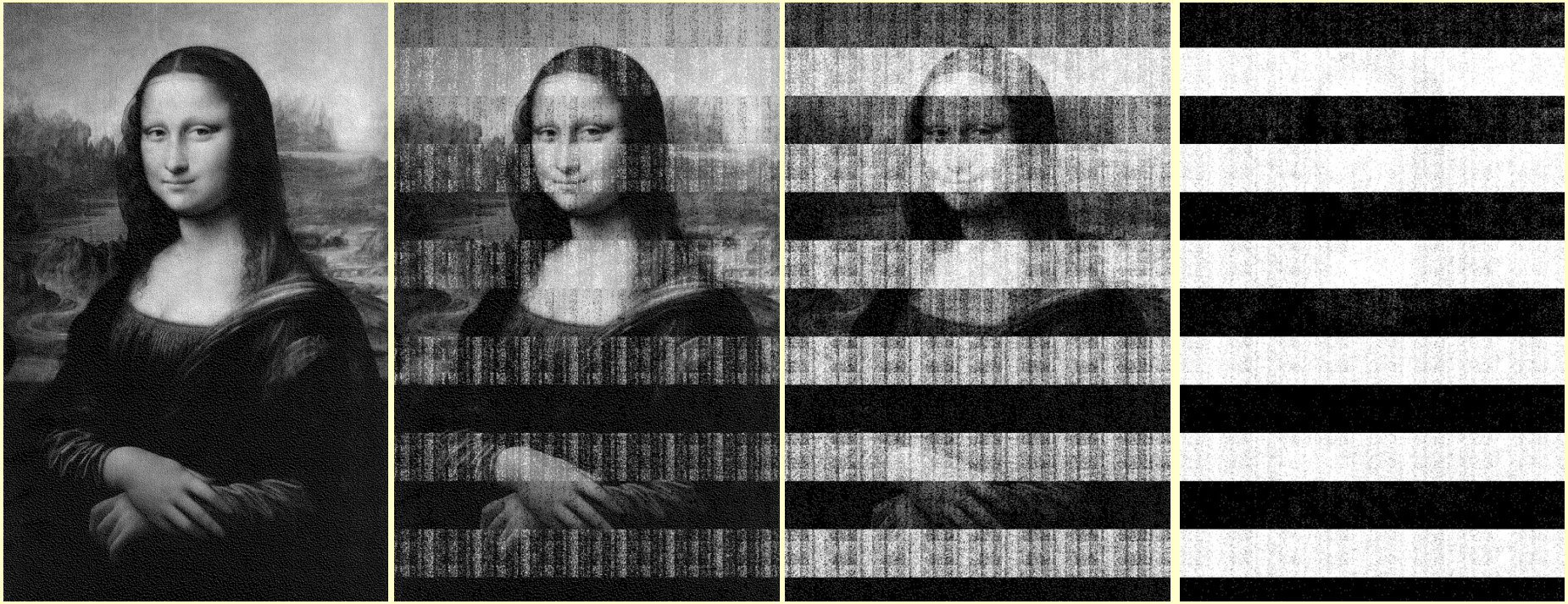
... in Windows Xp med priključenimi napravami prikažejo iPoda!

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, Prineton 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/i386/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 2:0:0:0: [sdb] Assuming drive cache: write through
sd 2:0:0:0: [sdb] Assuming drive cache: write through
sd 2:0:0:0: [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 "[redacted]"
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...

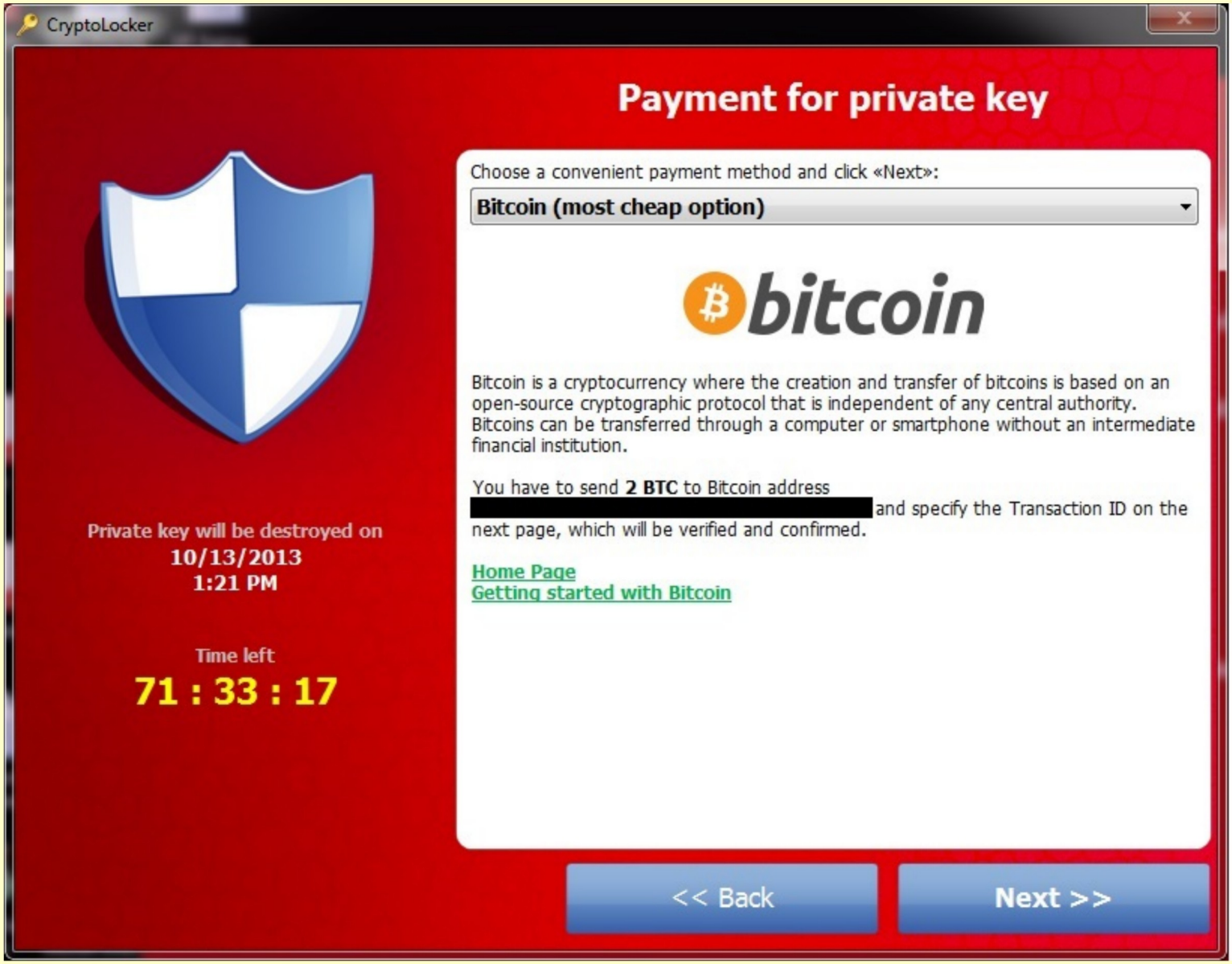
- raziskovanje,
- radovednost,
- samodokazovanje,
- zabava,
- vandalizem,...

… in kiberkriminal danes

- denar!

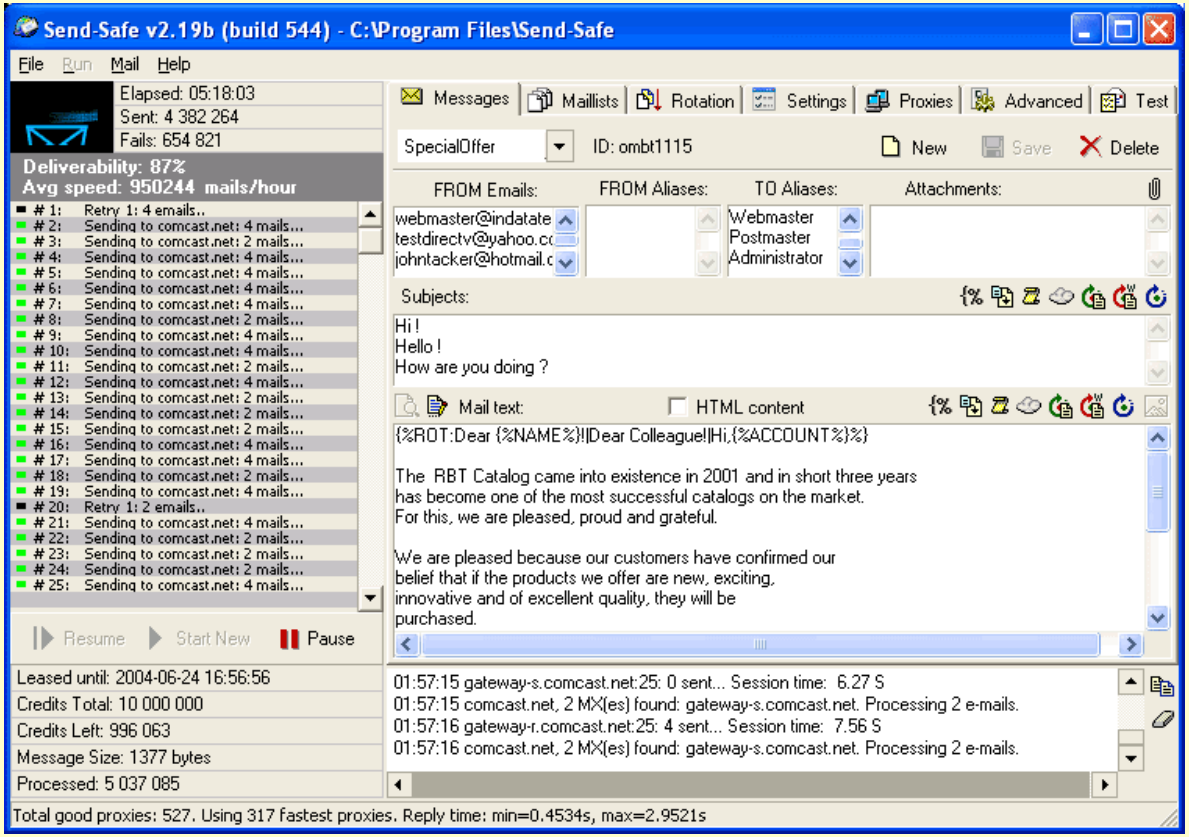
Spletna stran "podjetja".

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



Šifrirno-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]guest.arnes.si; [redacted]; [redacted]; [redacted]
[redacted]; [redacted]si;
[redacted]tional.si; [redacted]agmail.com;
[redacted]

Finančni 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

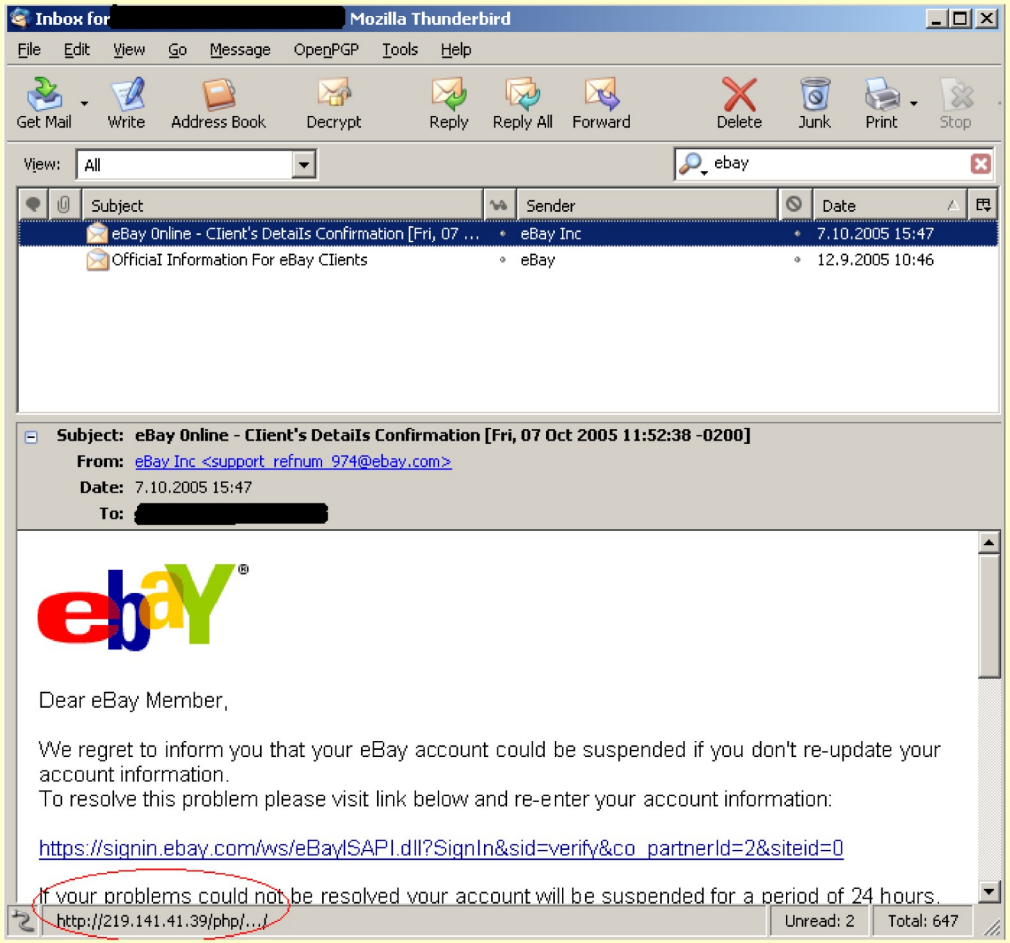
Hang Seng Bank Ltd

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.

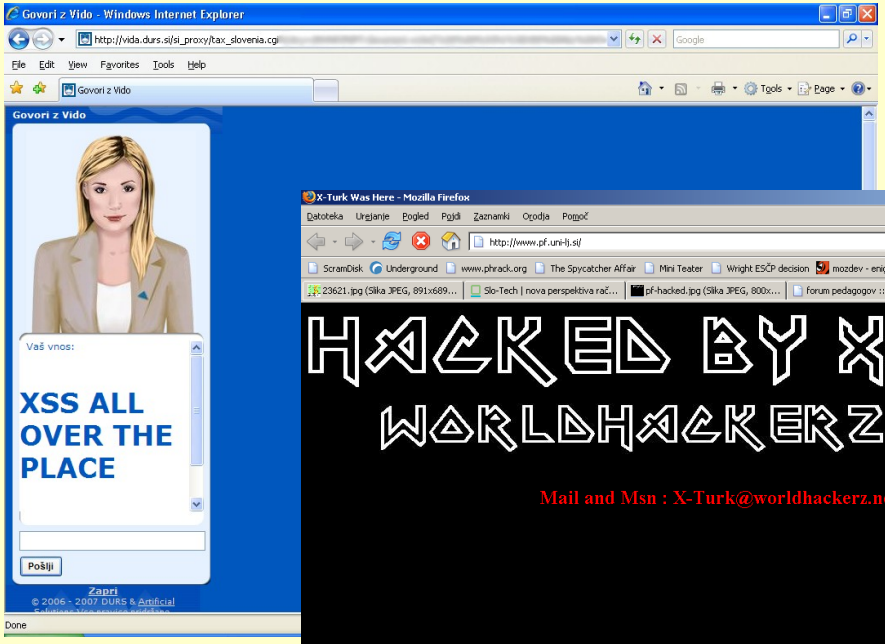
Before the U.S and Iraqi war, our client Hamadi Hashem a business man made a umbered fixed deposit of (346,736,899.68 HKD) for 18 calendar months...

Ribarjenje

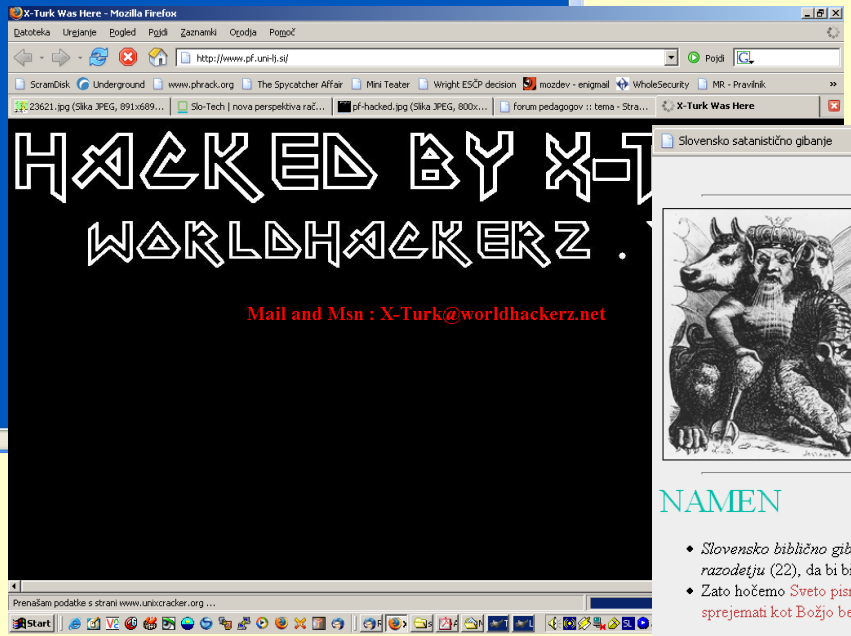


Primer ribarjenja (phisinga) preko neželene e-pošte.

Razobličenja spletnih strani



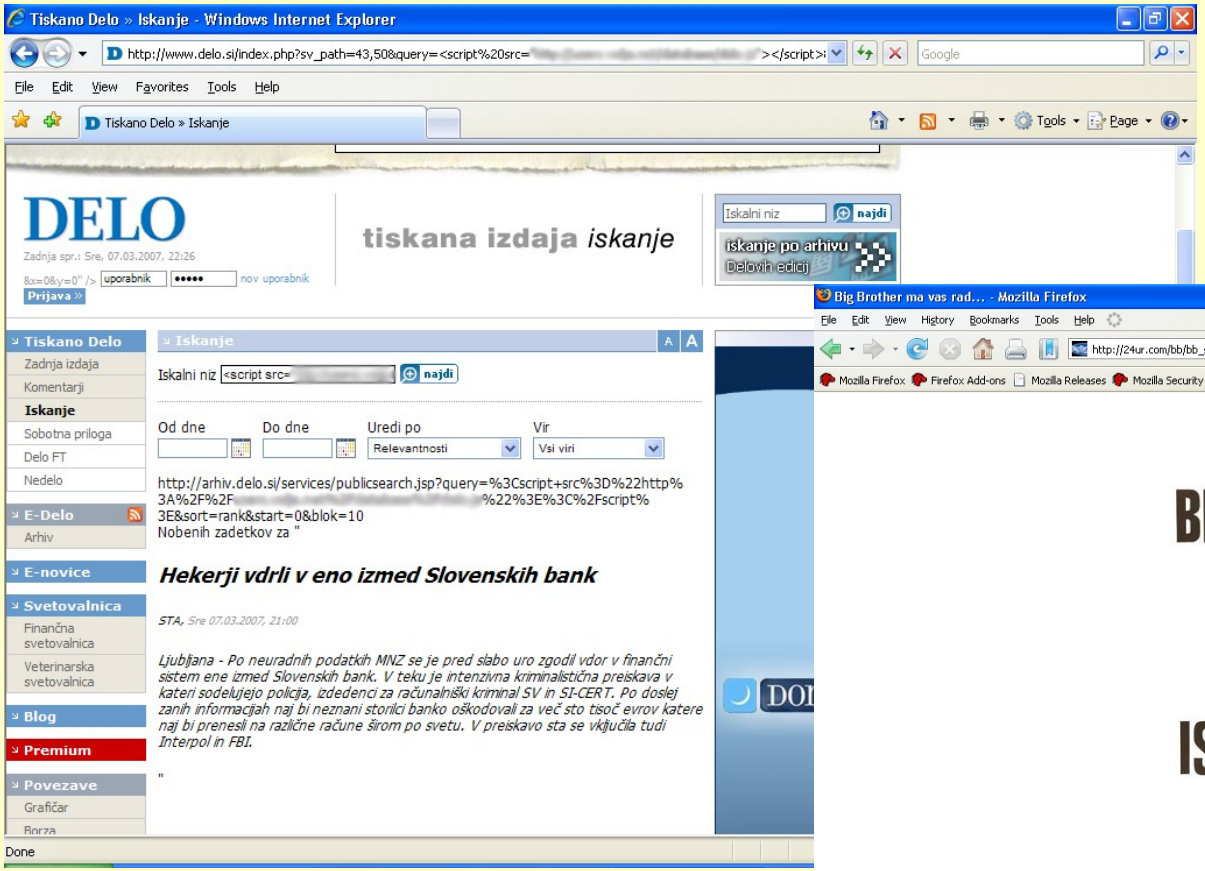
XSS napad na "davčno Vido".



Pravna fakulteta, Univerza v Ljubljani, februar 2007

Razobličenje spletne strani rimokatoliške cerkve.

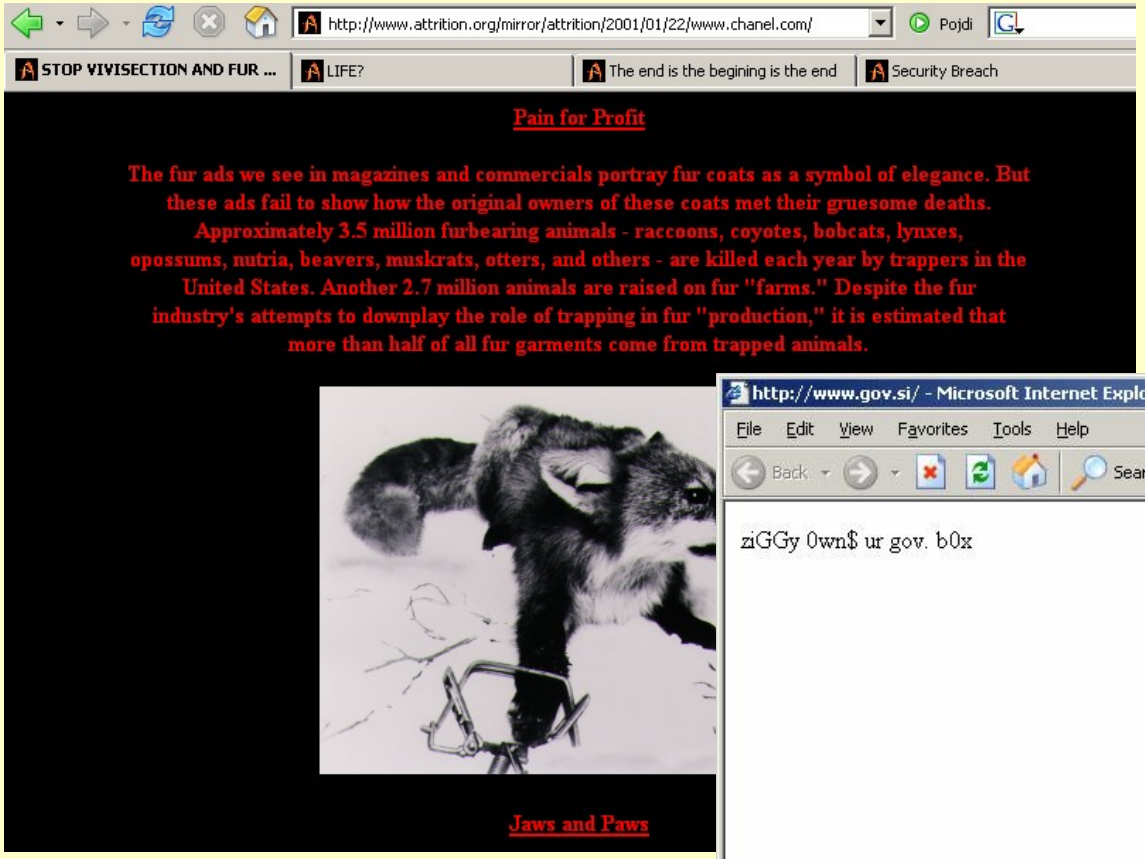
Razobličenja spletnih strani



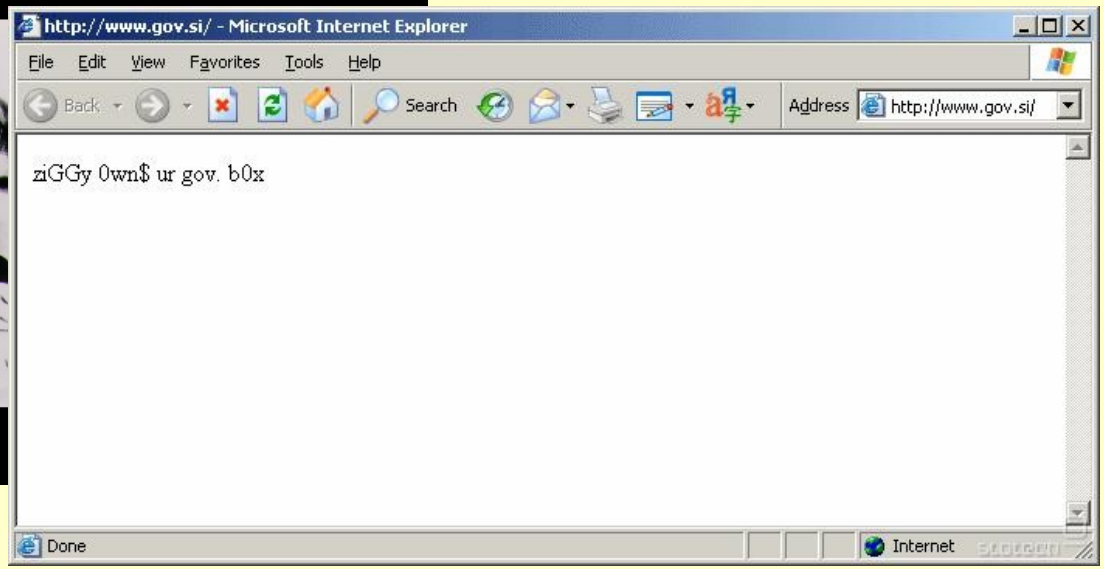
Lažna novica na spletni strani časnika DELO (XSS napad).

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

Razobličenja spletnih strani

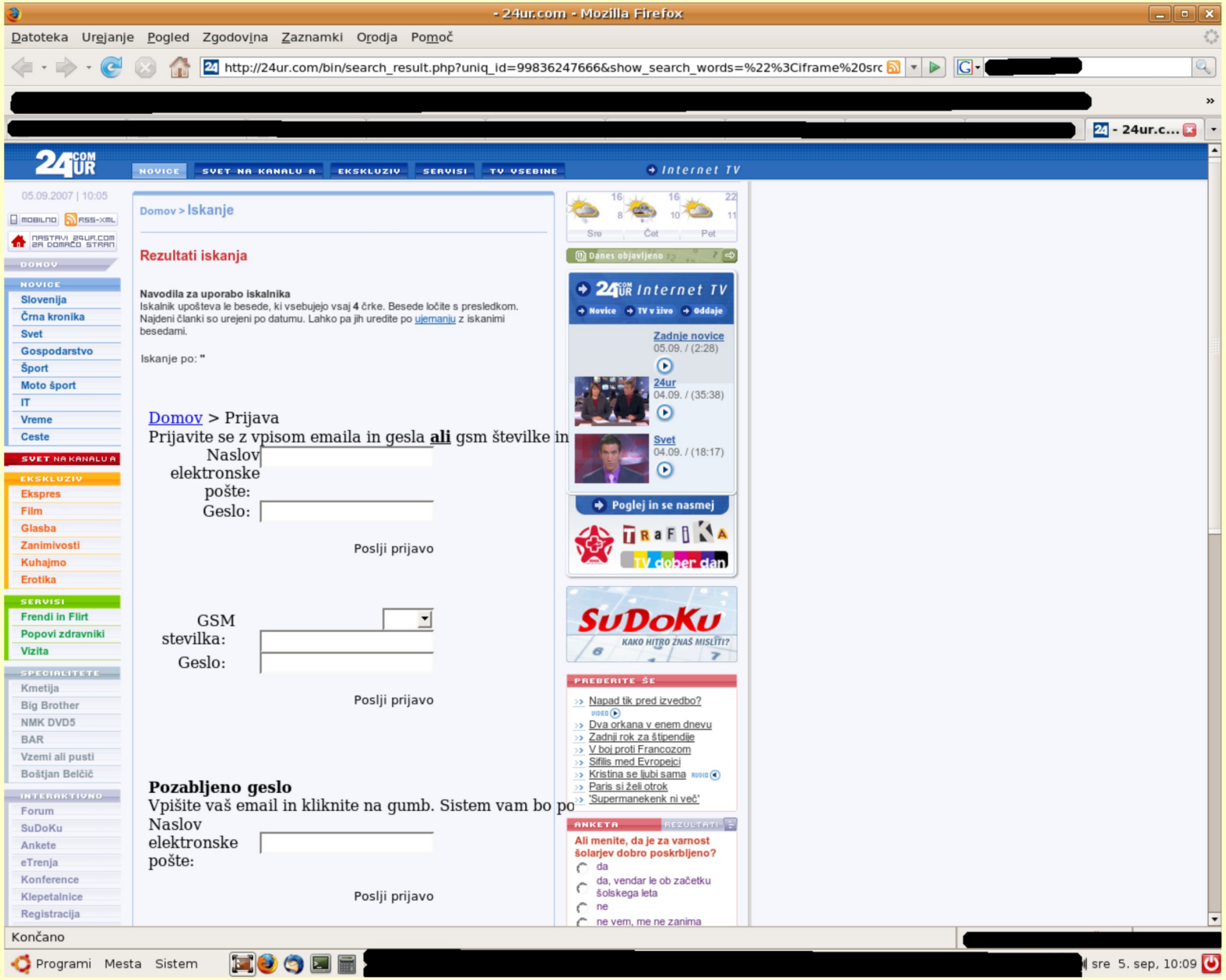


Razobličenje spletne strani modne hiše Chanell.com



Razobličenje vladne strani (gov.si).


24ur.com - - Mozilla Firefox
Datoteka Urejanje Pogled Zgodovina Zaznamki Orodja Pomoč
http://24ur.com/bin/expert_search_result.php?query=%22%3Ciframe%20src=http://www
Rodila na vislicah
Kriv je napad na hrvaško
VIDEO: Grobost do Britney
Internet TV
24UR POPOLDNE
PET DO PETIH
VSAK DELAVNIK
pop
24ur.com - poptv.si
29.02.2008 | 13:28
MOBILNO
RSS-XML
PODCAST NASTAVITVE
NASTAVI 24UR.COM ZA DOMAČO STRAN
POP TV IN KANAL A NA SATELITU
NOVICE
Slovenija
Črna kronika
Svet
Gospodarstvo
Šport
Moto šport
IT
Vreme
Ceste
SVET NA KANALU A
EKSKLUZIV
Ekspres
Film
Glasba
Zanimivosti
Kuhajmo
Erotika
SERVISI
Frendi in Flirt
Popovi zdravniki
Vizita
SPECIALITETE
24ur.com kartica
Big Brother
Grda Račka
Notpadu
Kmetija
NMK DVD6
Vzemi ali pusti
Boštjan Belčič
Preberite še
Dan redkih bolezni
29.02. | 13:03
Maskota dr. Janeza Drnovška po njegovi smrti še bolj priljubljena!
Naš novinar je preveril, zakaj je priljubljenost maskote pokojnega dr. Janeza Drnovška iz dneva v dan bolj priljubljena.
poptv.si
PREDVAJAJ
Blokiraj
BigBrother
PRISKRBI SI
KARTICO
24UR COM
ŽE SEDAJ
NOVICE
29.02. | 13:08
'Mi odpiramo meje'
VIDEO
Casino Mulino je bil najboljši ponudnik za nakup zemljišč, pravi Čerar in dodaja: "Joras dela zdrahe."
29.02. | 13:08
'Saga s smetmi končana'
Regijskega centra za ravnanje z odpadki v Tenetišah ne bo, bo pa deponija kratek čas še služila svojemu namenu.
29.02. | 13:20
Črna princesa umorjena?
Je Črna princesa umrla nasilne smrti? Borila se je za ukinitev obrezovanja afriških deklic.
29.02. | 11:44
Duduja ne boli več
Minil ni niti teden dni po grozljivi
EKSKLUZIV
29.02. | 13:25
Prvo tetoviranje očesa
V javnosti so se pojavile fotografije prvega tetoviranja, narejenega na človeškem očesu.
29.02. | 11:45
Nadiya razgaljena v spodnjicah!
Vrhunska plesalka Nadiya Bychkova, sicer tudi televizijska voditeljica, se je
29.02. | 11:31
'Moje prsi so OK'
Spoznajte Leno Alexandro, novo norveško pevsko zvezdo, ki je zelo seksi in prsata
Pet
Sob
Ned
Danes objavljeno
FRENDI FLIRT
OBJAVI SVOJ VIDEO
Najnovejši video
najlači radnik n...
mawro
Najnovejša fotka
Osebna slika
lea
Najnovejši blog
kako je pa svet m...
Črkica
24UR Internet TV
Novice
TV v živo
Oddaje
Zadnje novice
Končano
Anonimizacija izključena
Programi Mesta Sistem
24ur.com - - Mozilla Fi...
SVN
pet 29. feb, 13:30



Prikaz možnosti XSS ribarjenja na spletni strani 24ur.com.

Si.mobil d.d. - Mozilla Firefox

Datoteka Urejanje Pogled Zgodovina Zaznamki Orodja Pomoč

http://www.simobil.si/sl/search.cp2?q=<h3>Dimitrij+Rupel+postal+svetovalec+

unauthenticated

Si.mobil Vodafone live! Orto | Prodajna mesta | Vprašajte nas | Registrirajte se | English

si.mobil

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.

Nastavitve zunanjega odjemalca

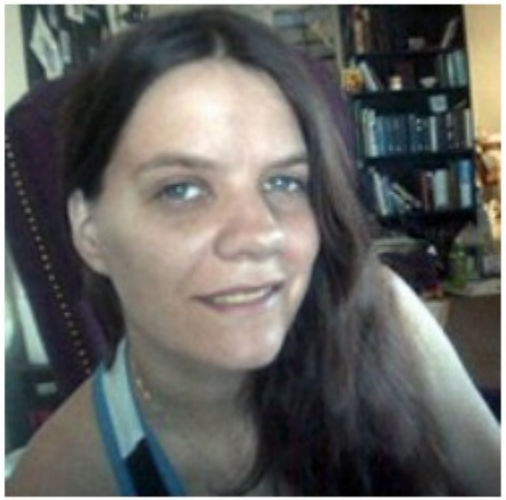
Končano

Apache 1337 [redacted] Anonimizacija izključena

Programi Mesta Sistem [XC... [Pr... Si.... [Se... TO... *go... SVN pet 16. jan, 10:28

Hackers embed flashing animations on epilepsy support forum

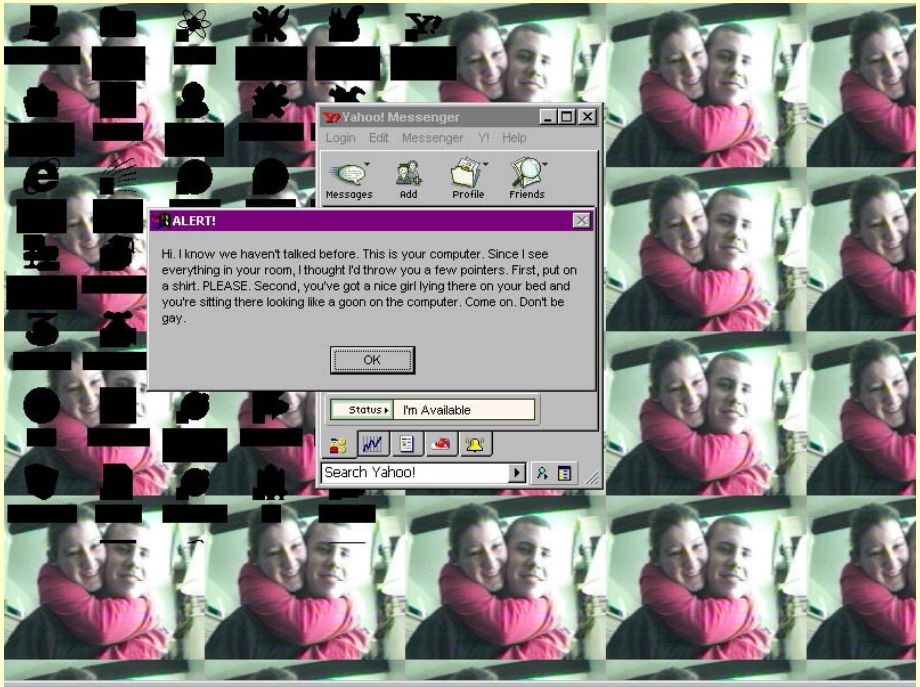
By Darren Murph posted March 29th 2008 8:50PM

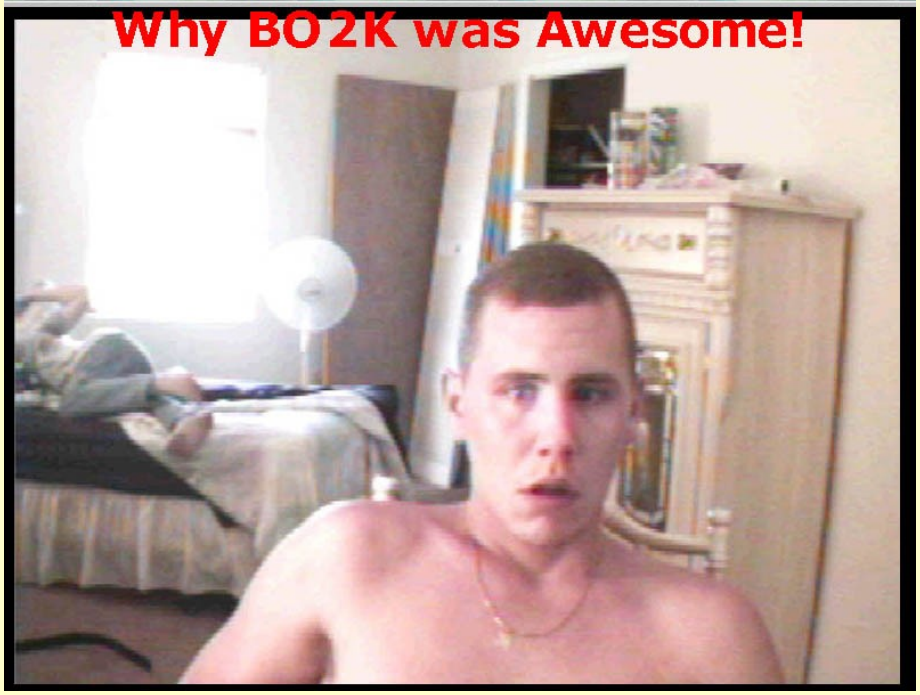


Shortly after hearing a sad tale of a 7-year old cancer patient having his medication and PSP stolen whilst en route to treatment comes yet another story of the world's meanest preying on the innocent. This go 'round, a group of griefers (which appear to be members of Anonymous) managed to invade a support 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.

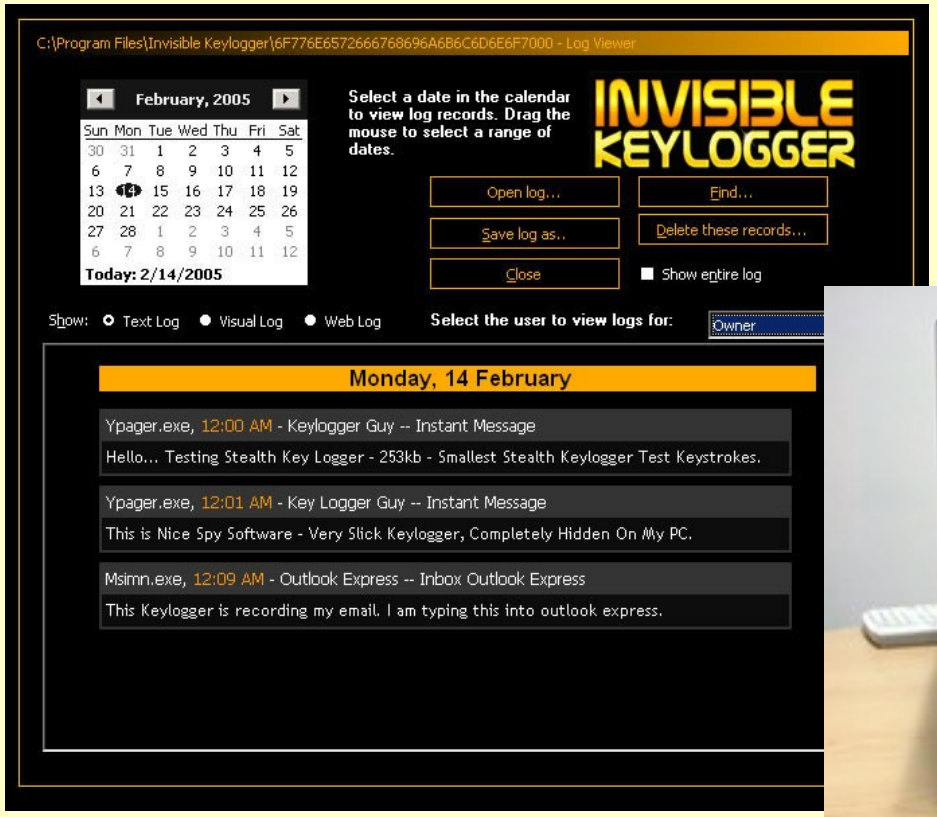
Vir: http://www.engadget.com/2008/03/29/hackers-embed-flashing-animations-on-epilepsy-support-forum/

Vdori in okužbe z zlonamerno programsko opremo


Yahoo! Messenger
Login Edit Messenger Y! Help
Messages Add Profile Friends
ALERT!
Hi. I know we haven't talked before. This is your computer. Since I see everything in your room, I thought I'd throw you a few pointers. First, put on a shirt. PLEASE. Second, you've got a nice girl lying there on your bed and you're sitting there looking like a goon on the computer. Come on. Don't be gay.
OK
Status I'm Available
Search Yahoo!


Why BO2K was Awesome!

Zlonamerno programje... in strojna oprema



Programski...

...in strojni prestrezniki tipkanja (vir in avtorstvo: www.keyghost.com)

Slo-Tech | nova perspektiva računalništva - Opera

File Edit View Bookmarks Tools Help

New tab | Slo-Tech | nova perspekt...

http://www.slo-tech.com/

Google

Na NESTu me najbolj privlačijo:

rožice	47%	(131)
druženje	21%	(59)
predavanja	12%	(34)
tekmovanja	10%	(27)
lahkotno igranje	9%	(25)

Skupaj glasov: **276**

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 holles:
- xss in registration form
- multiple XSS vulnerabilities in forum post - IMG TAG(using some special caracter sets - IE Only)
- many potencial 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.

Interviju s Philipom Zimmermannom

Menjava kondenzatorjev na osnovni plošči

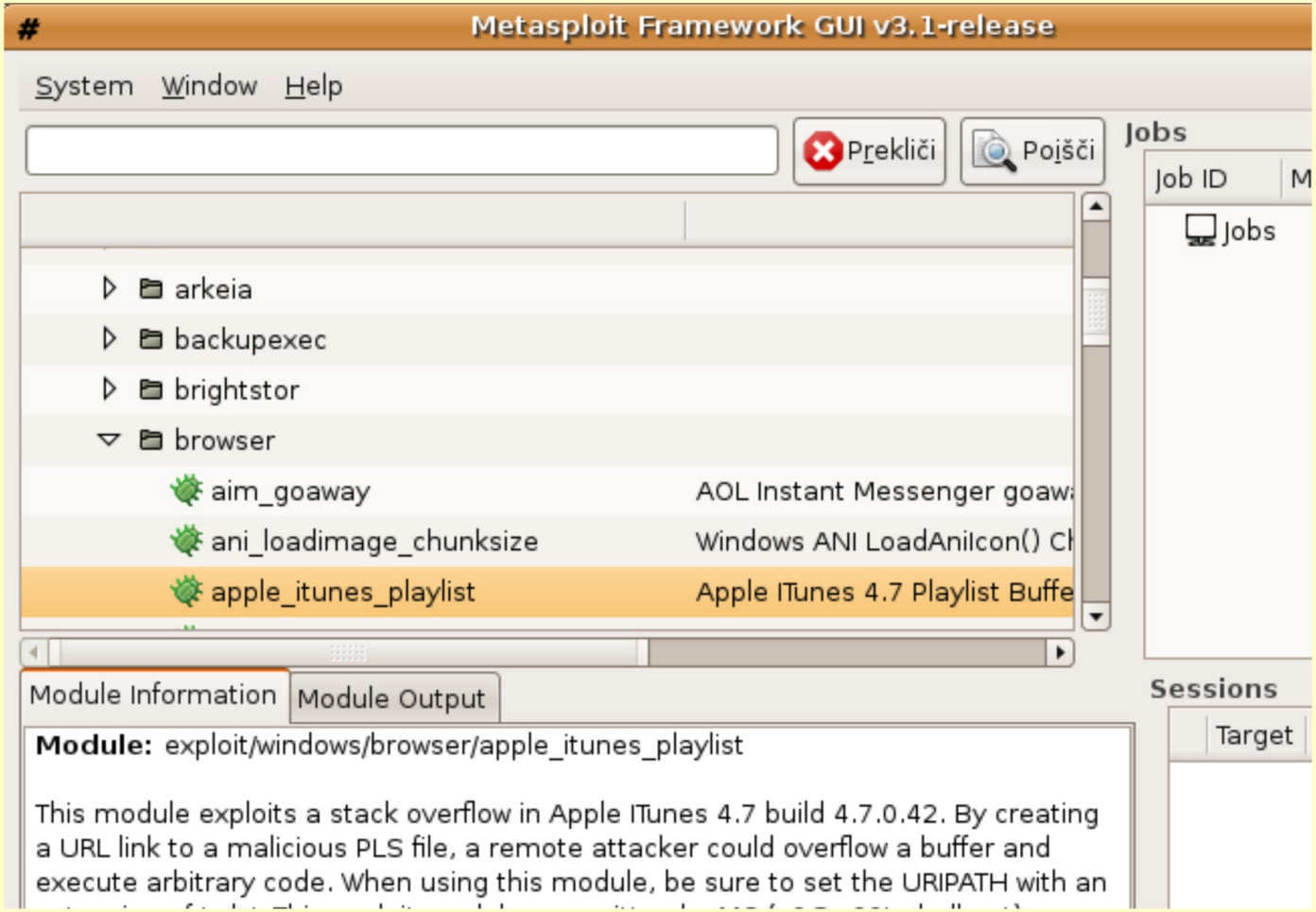
Kršitve avtorskega prava na internetu

Video nadzor na

Start

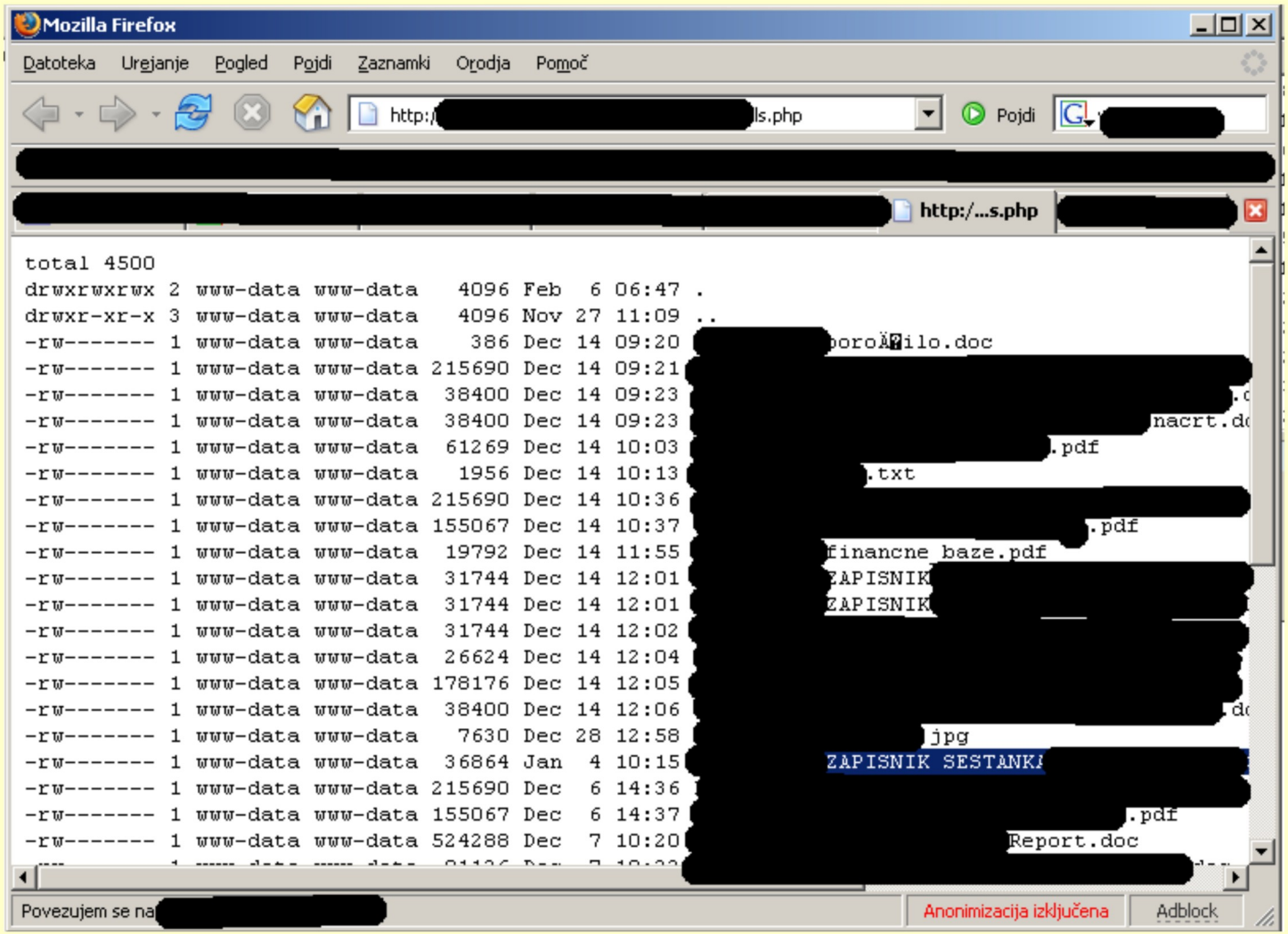
19:50 Četrtek

Orodja za vdore

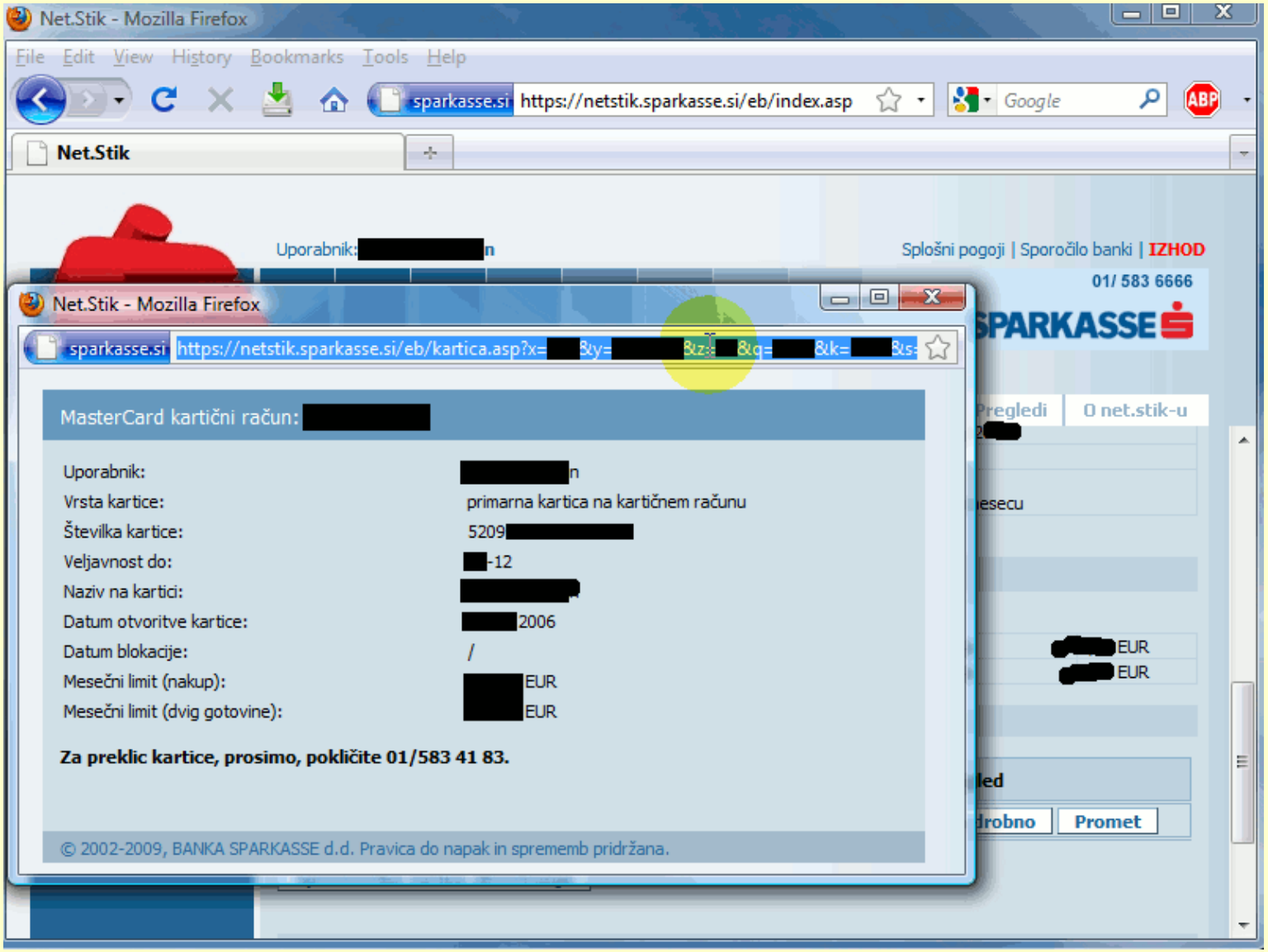


Metasploit Framework – zbirka programja za izrabo varnostnih ranljivosti.

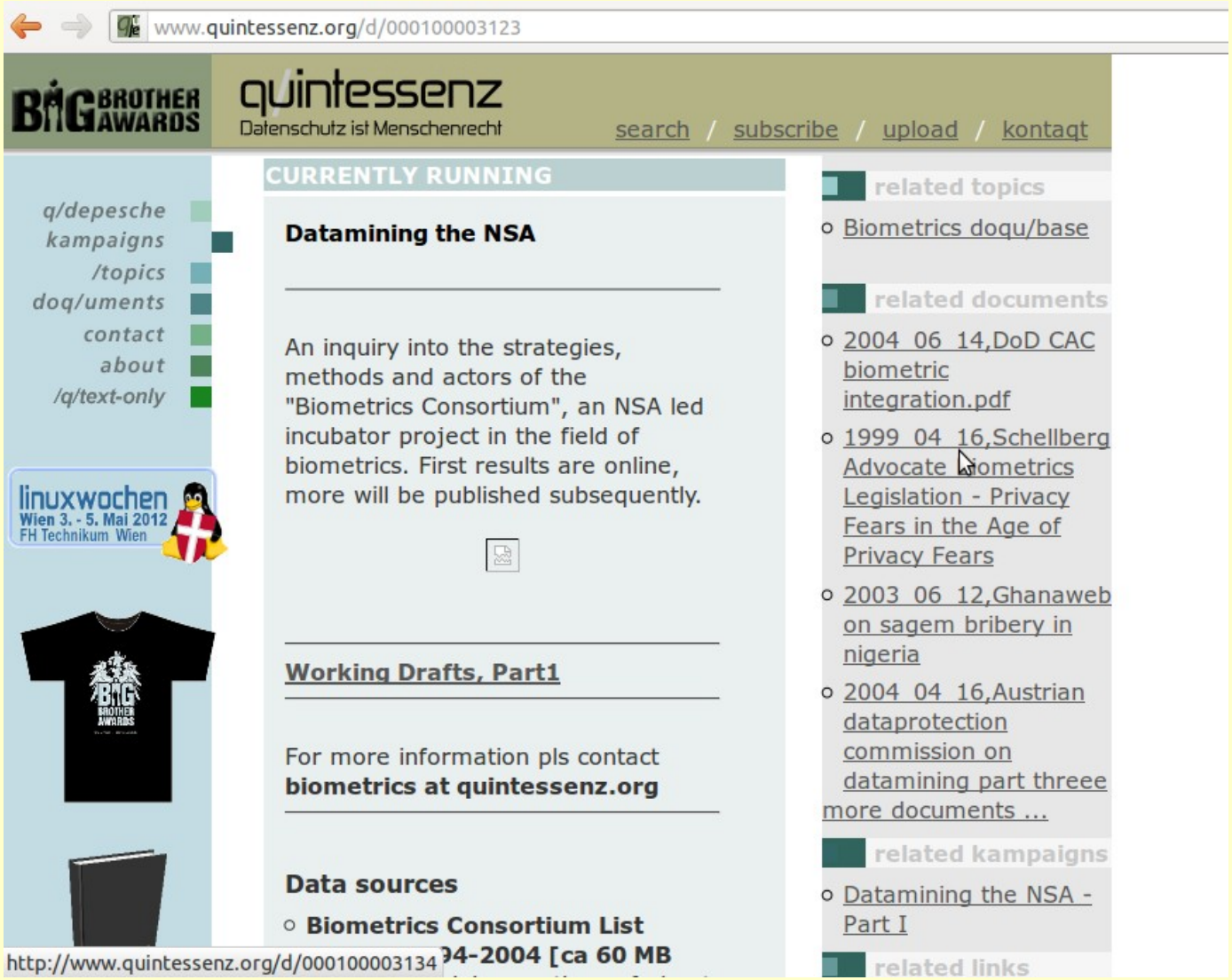
Možnosti poljubnega spreminjanja URL naslovov lahko vodi...



...do resnih napadov



Napake pri omejitvah dostopa



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

Datoteka Urejanje Pogled Pojdi Zaznamki Orodja Pomoč

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

Pojdi lgl

Firefox Help Firefox Support Plug-in FAQ

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

163%

LGL - LUTKOVNO GLEDALIŠČE LJUBLJANA

Bookmarks Thumbnails Comments Signatures

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 gledališèe Ljubljana

[redacted]

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
skupaj				**12,96 EUR** **3.105,73 SIT**

številka potrdila o nakupu

010-000-107-788-454-883-142760

Vaše potrdilo o nakupu zamenjajte za vstopnice na blagajni dvorane.

V primeru, da prireditev odpade, lahko potrdilo o nakupu zamenjate na blagajni organizatorja za drugo prireditev 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.

1 of 1 8,26 x 11,69 in

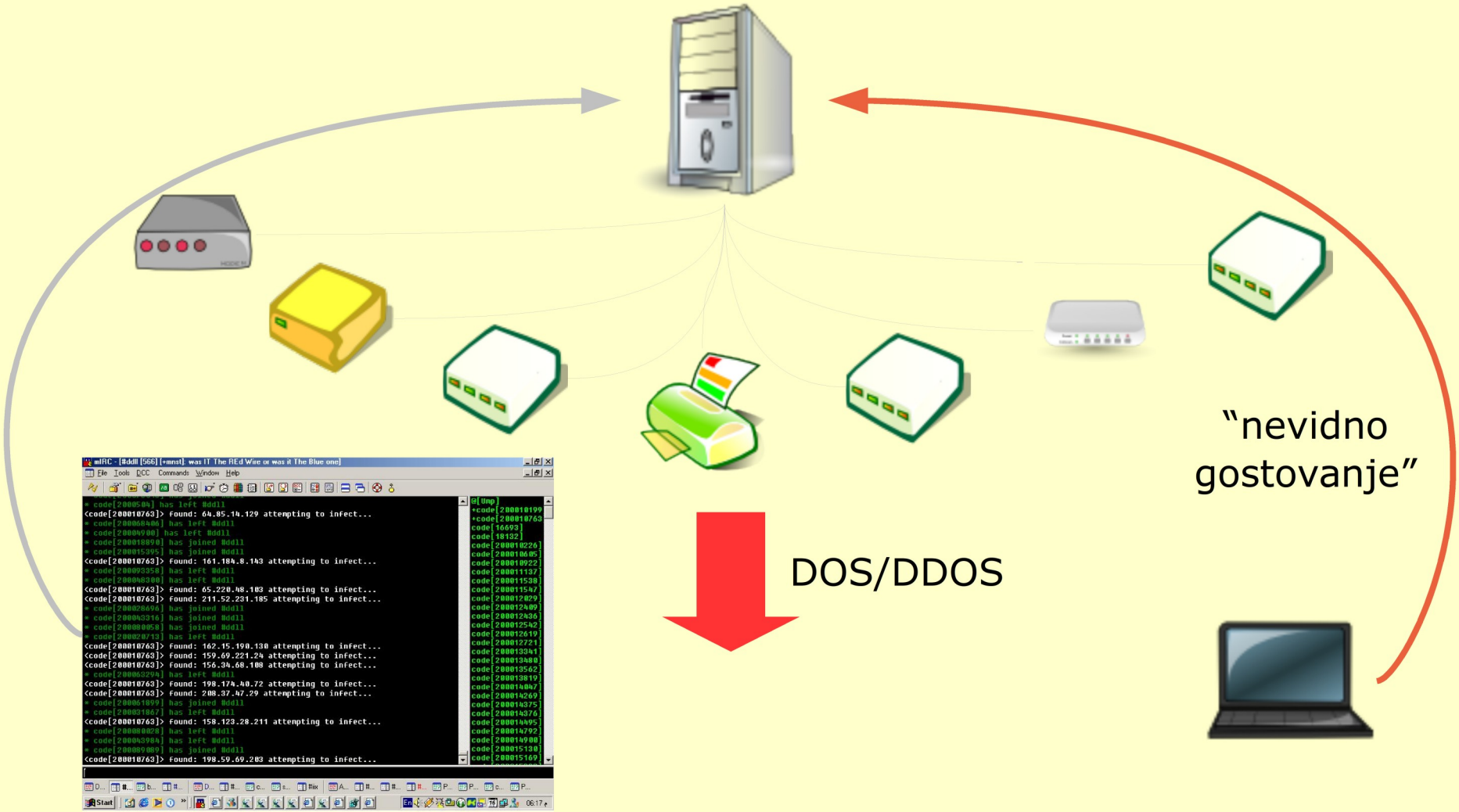
Končano

Anonimizacija izključena

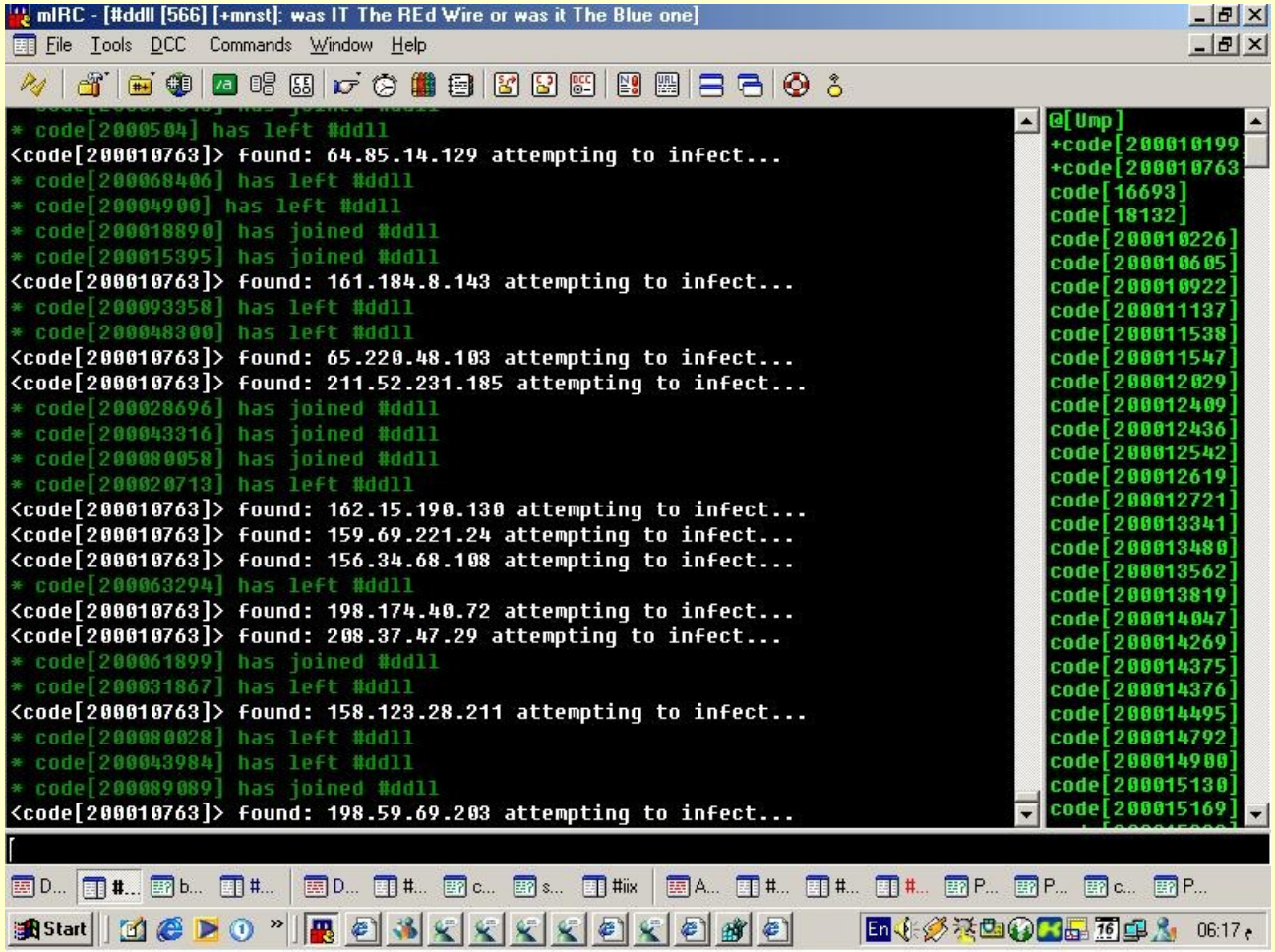
Start prevze... The GIMP Layers, ... Untitled... LGL - LU... http://l... 10:19

SQL vrivanje

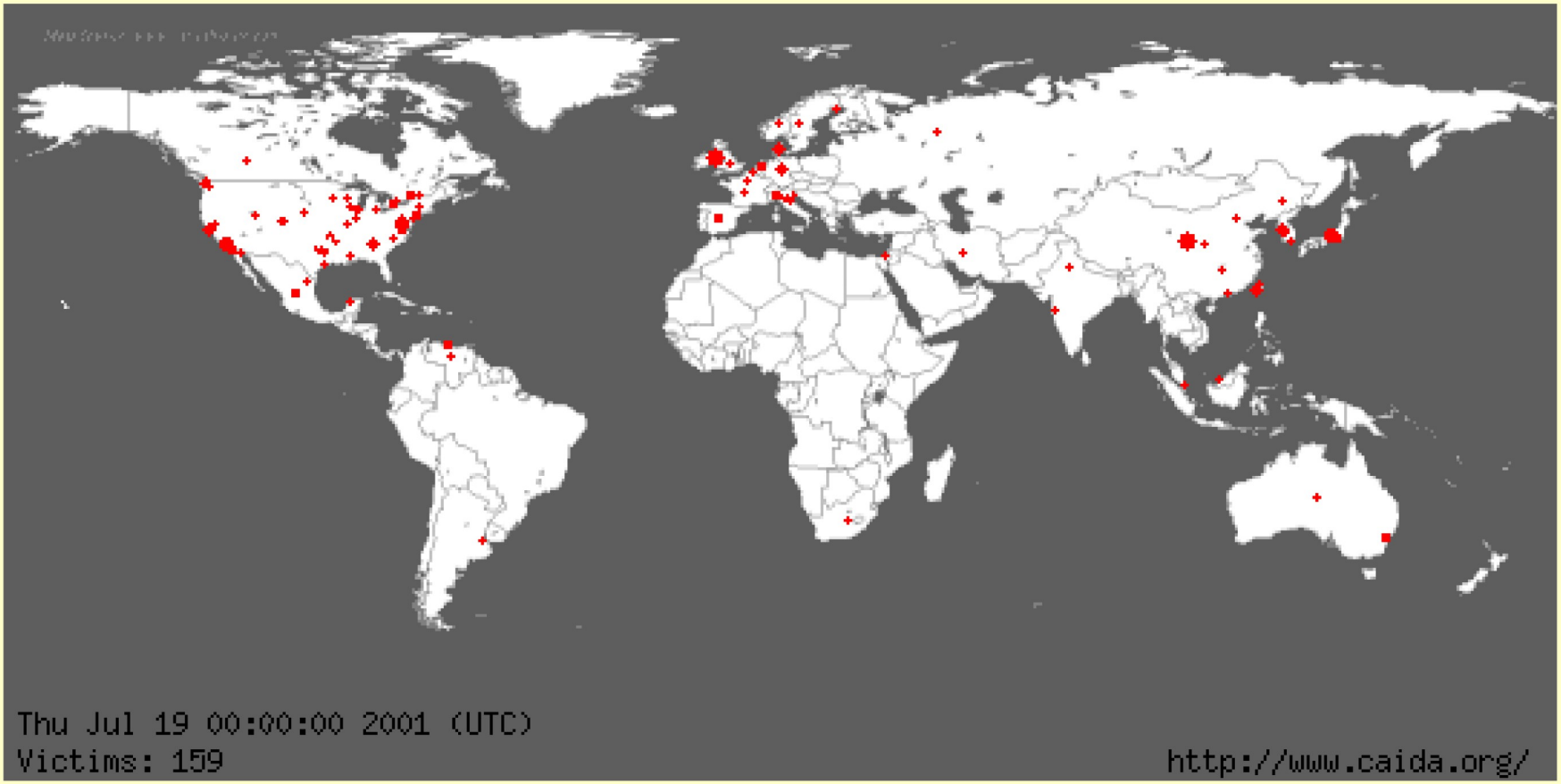
Prikrita omrežja



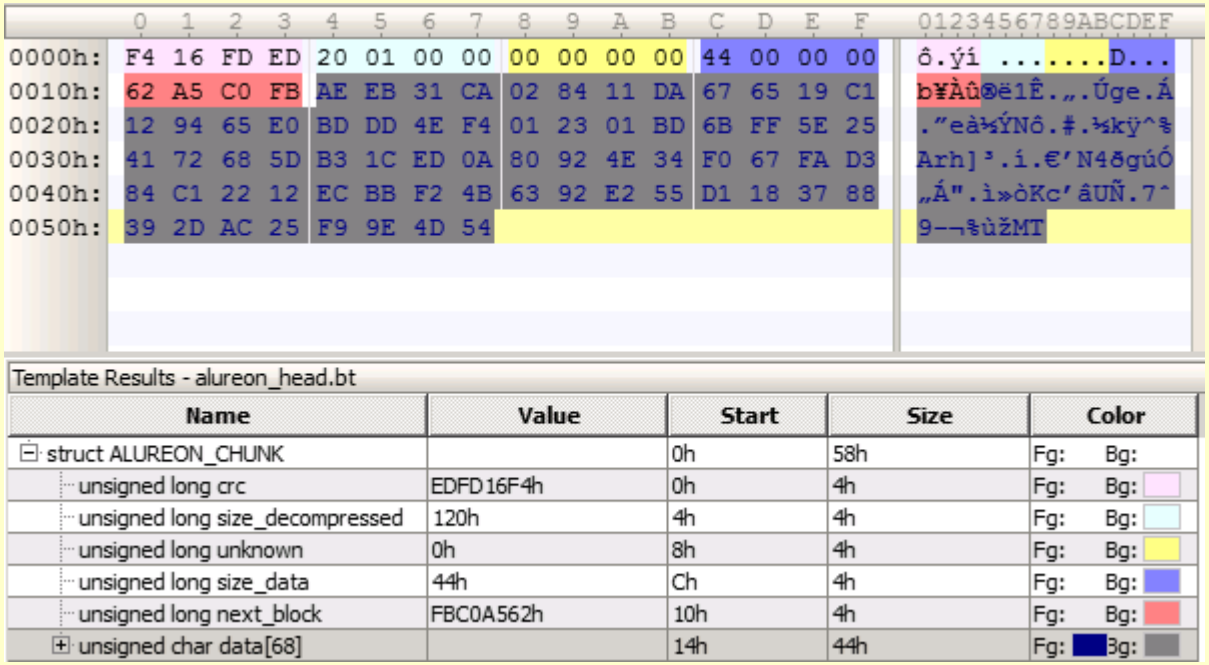
Prikrita omrežja



Pogled na prikrito omrežje iz strani napadalca.


Thu Jul 19 00:00:00 2001 (UTC)
Victims: 159
http://www.caida.org/

'Steganografski' virusi



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	F4	16	FD	ED	20	01	00	00	00	00	00	00	44	00	00	00	ô.ýí ....D...
0010h:	62	A5	C0	FB	AE	EB	31	CA	02	84	11	DA	67	65	19	C1	b¥ÀûëlÊ.„.Úge.Á
0020h:	12	94	65	E0	BD	DD	4E	F4	01	23	01	BD	6B	FF	5E	25	.”eà½ÝNô.#.½kÿ^%
0030h:	41	72	68	5D	B3	1C	ED	0A	80	92	4E	34	F0	67	FA	D3	Arh]³.í.€’N4ðgúÓ
0040h:	84	C1	22	12	EC	BB	F2	4B	63	92	E2	55	D1	18	37	88	„Á".ì»òKc’âUÑ.7^
0050h:	39	2D	AC	25	F9	9E	4D	54									9-¬%ùžMT

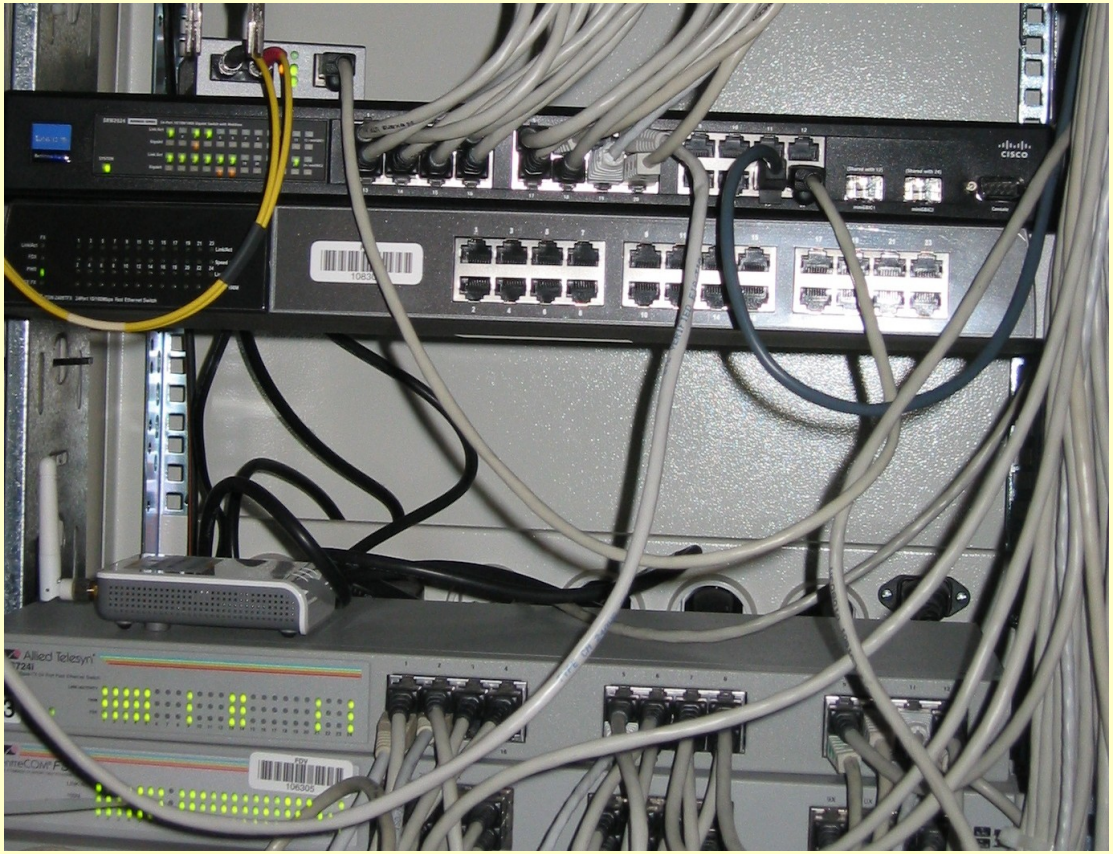
Template Results - alureon_head.bt

Name	Value	Start	Size	Color
struct ALUREON_CHUNK		0h	58h	Fg: Bg:
unsigned long crc	EDFD16F4h	0h	4h	Fg: Bg:
unsigned long size_decompressed	120h	4h	4h	Fg: Bg:
unsigned long unknown	0h	8h	4h	Fg: Bg:
unsigned long size_data	44h	Ch	4h	Fg: Bg:
unsigned long next_block	FBC0A562h	10h	4h	Fg: Bg:
unsigned char data[68]		14h	44h	Fg: Bg:

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.

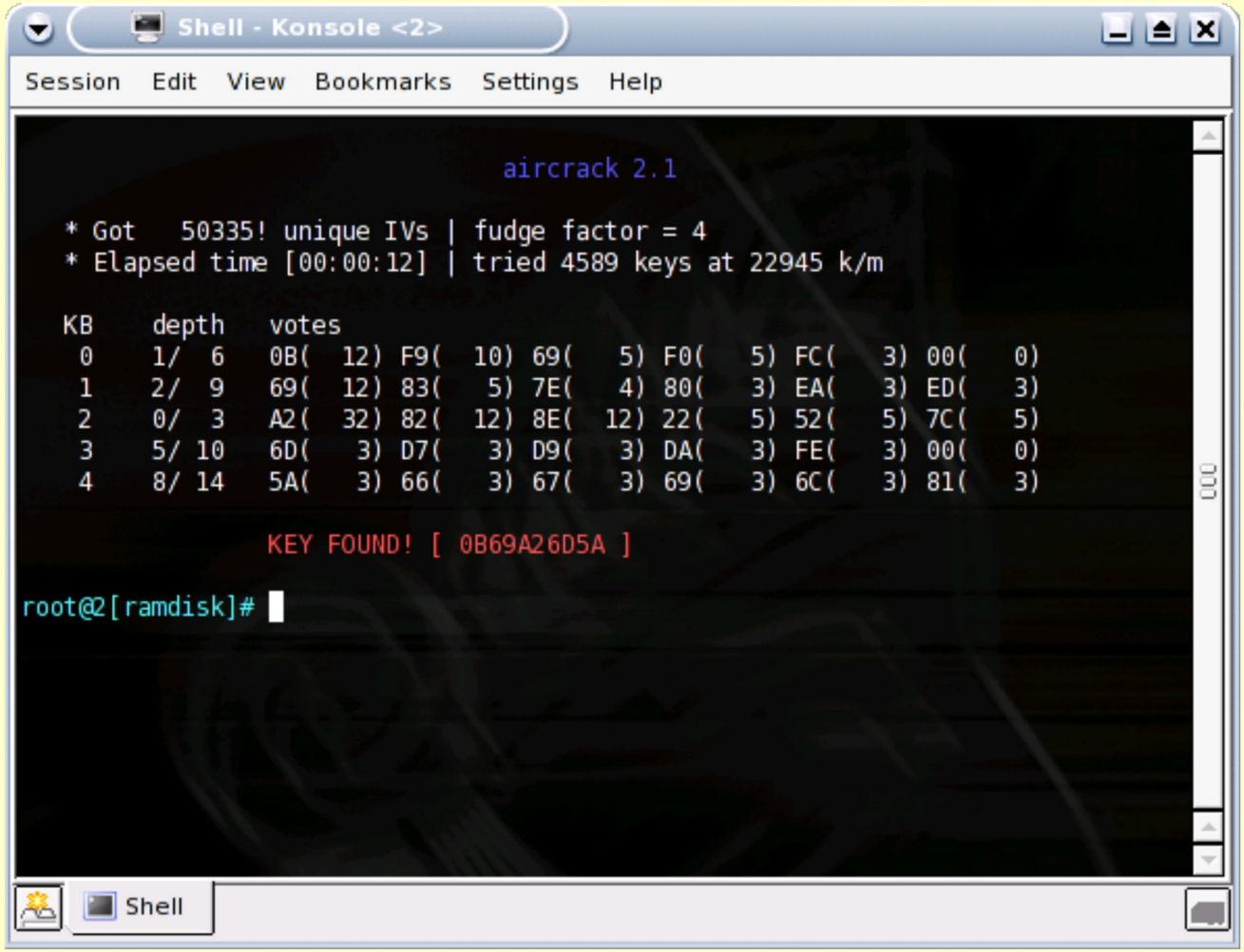
Vdori



[Primer vdora v poštno banko v Haifi.]

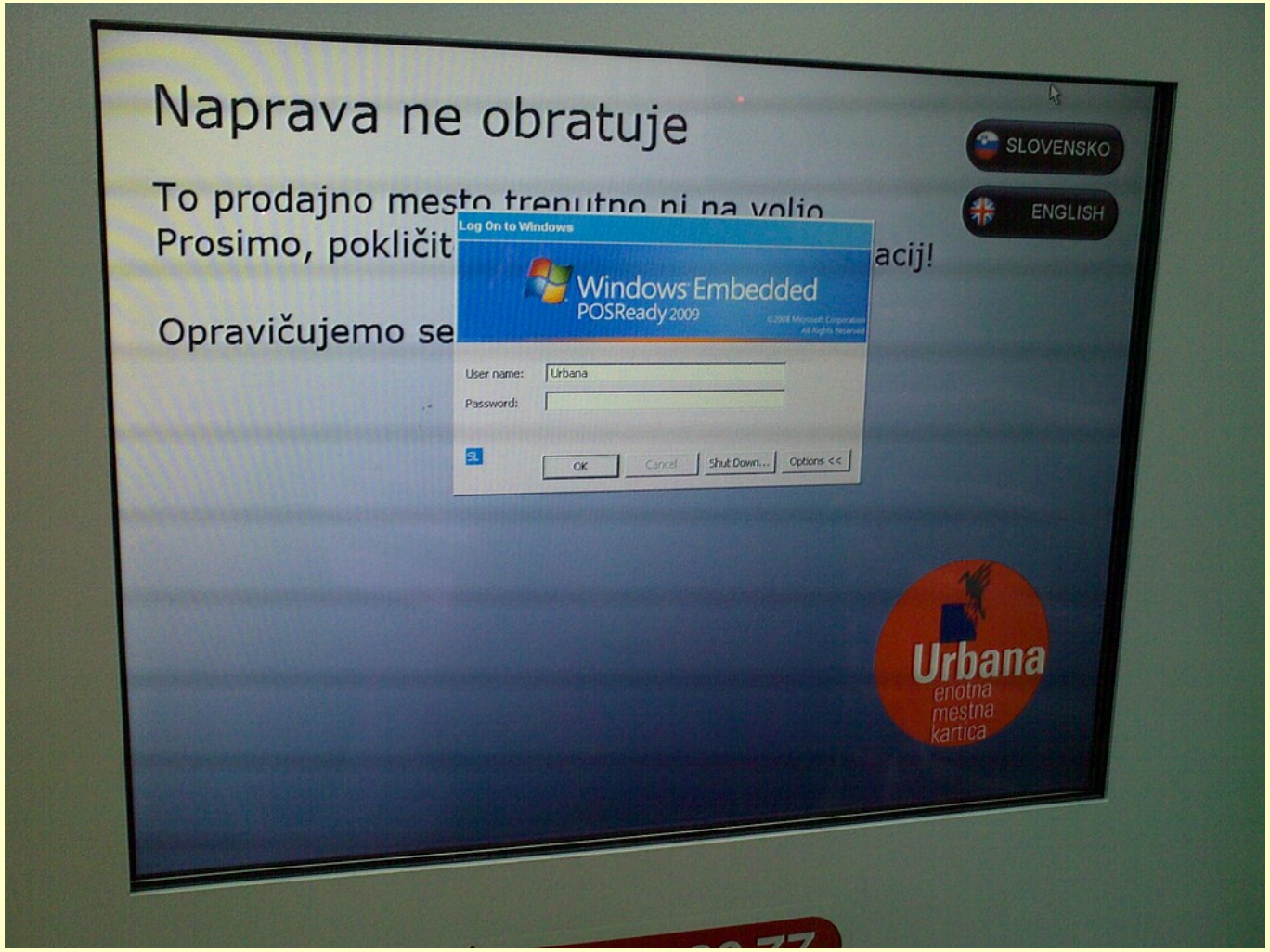
http://theplugbot.com/

Ranljivi niso samo računalniki



Napad na brezžično omrežje.

Ranljivi niso samo računalniki



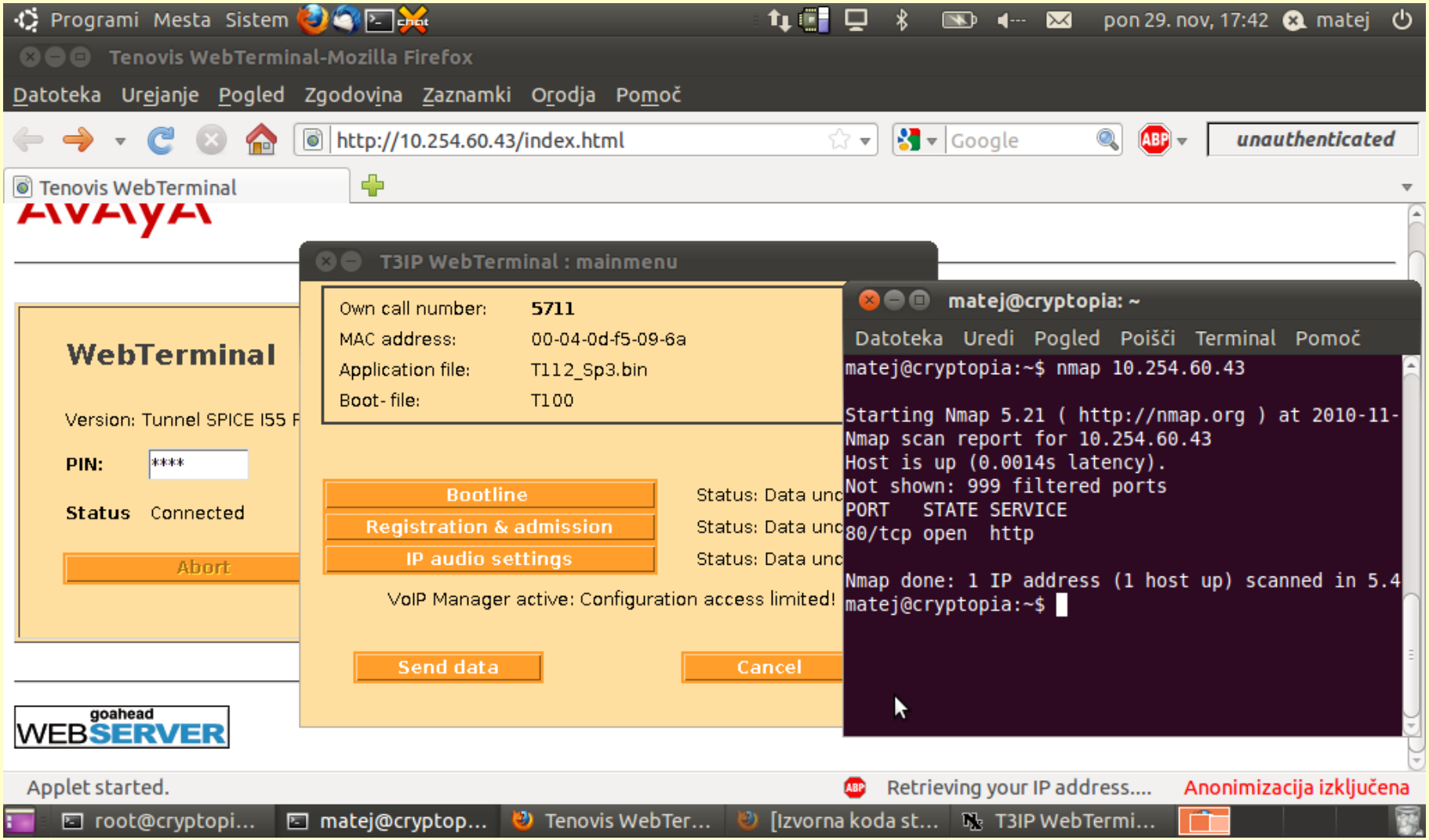
Ranljivi niso samo računalniki

Napad na TV oddajnik.

Ranljivi niso samo računalniki

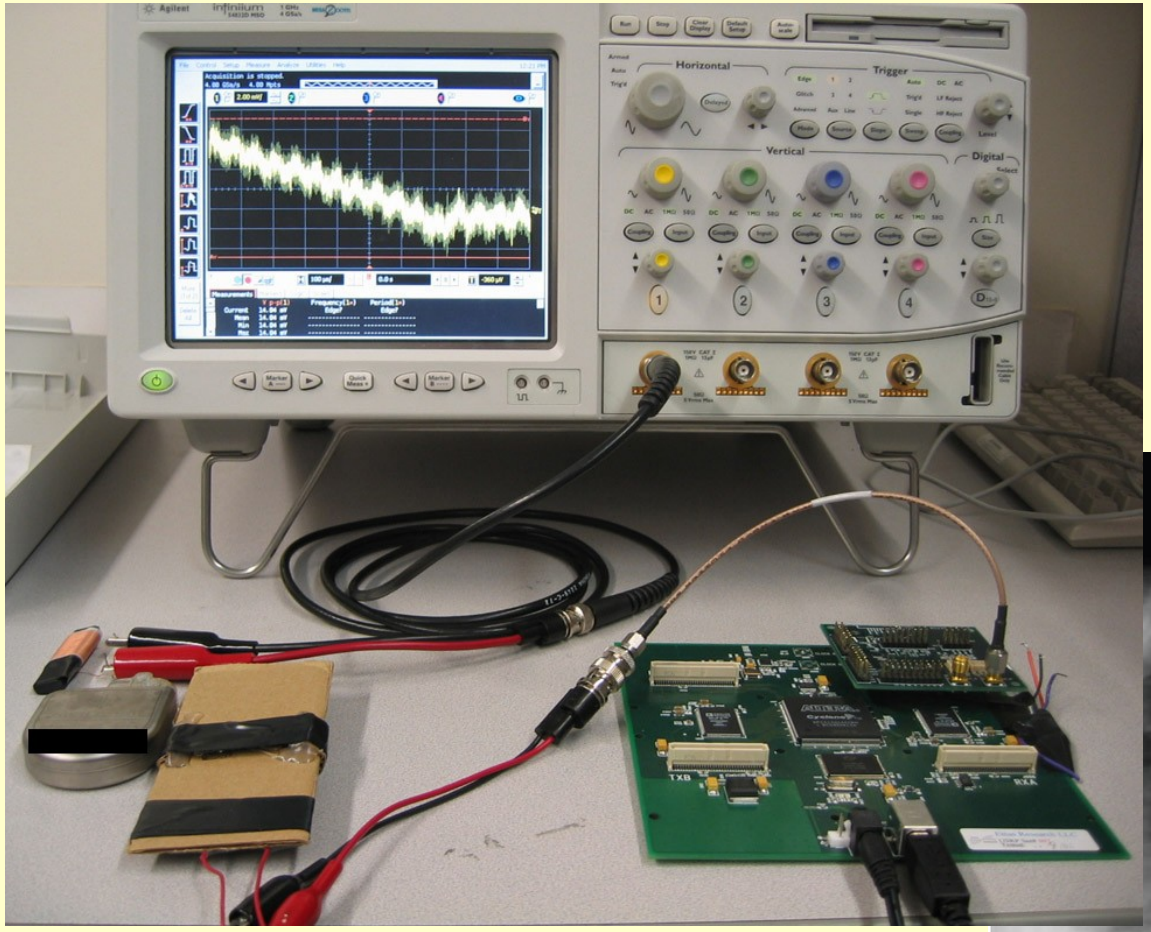
Napad na tiskalnik.

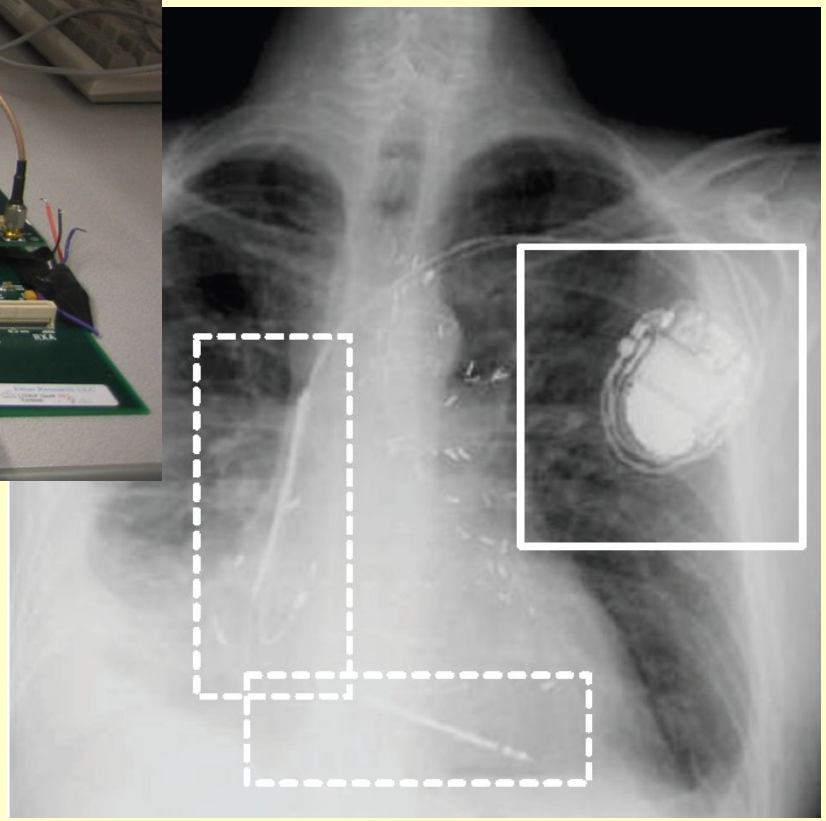
Ranljivi niso samo računalniki



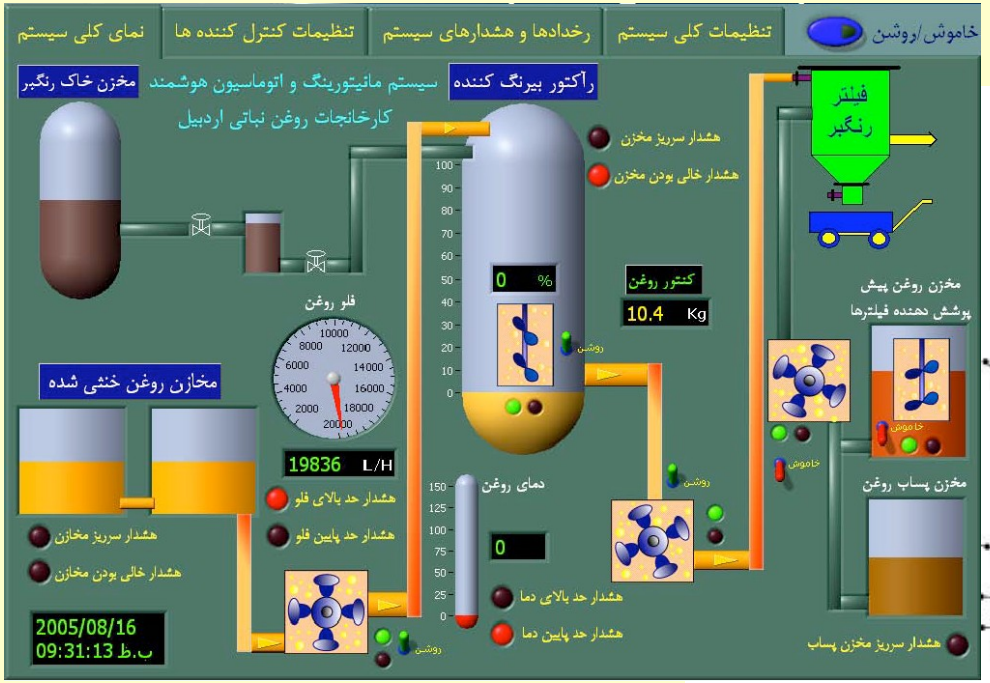
Napad na VOIP telefon.

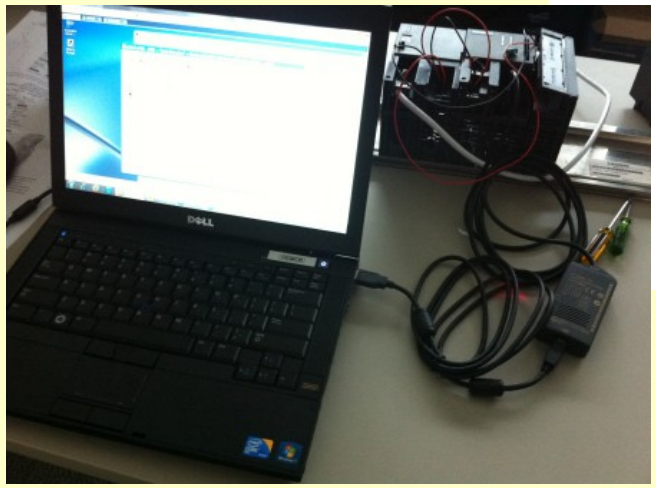
Napad na RFID potne liste.

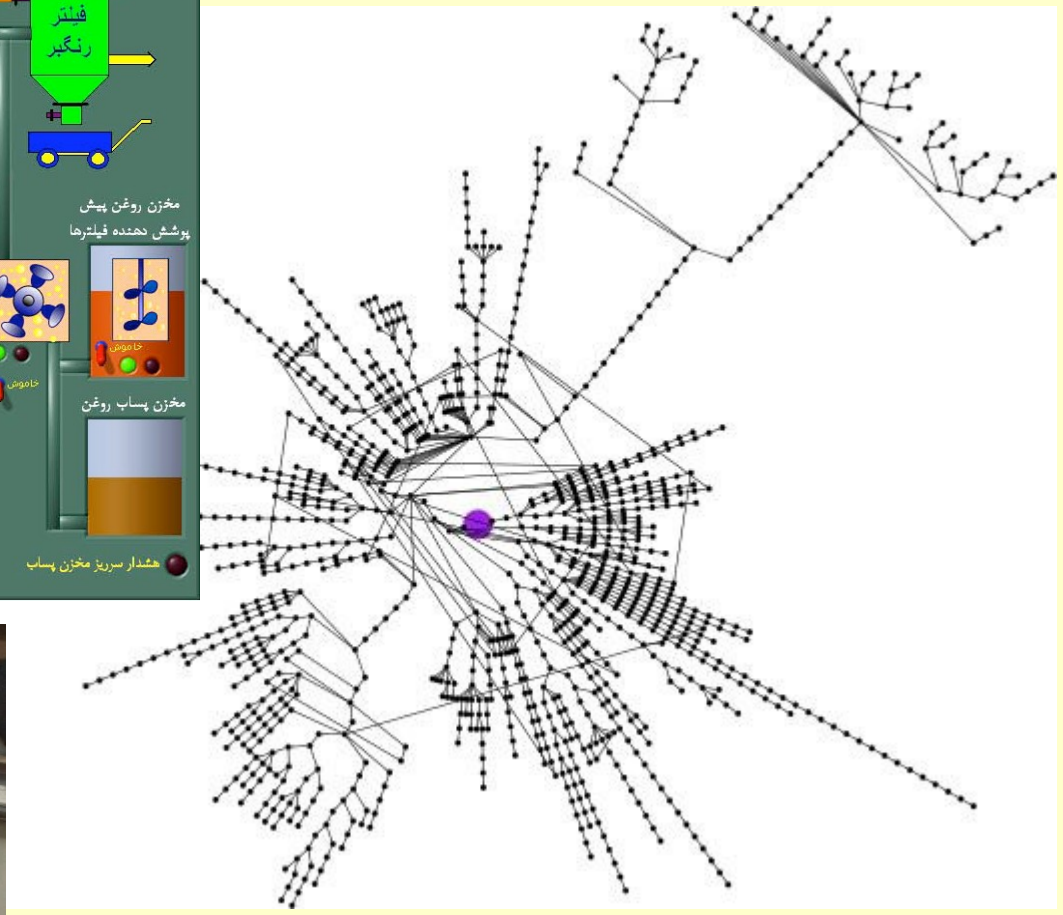




Napad na srčni spodbujevalnik.



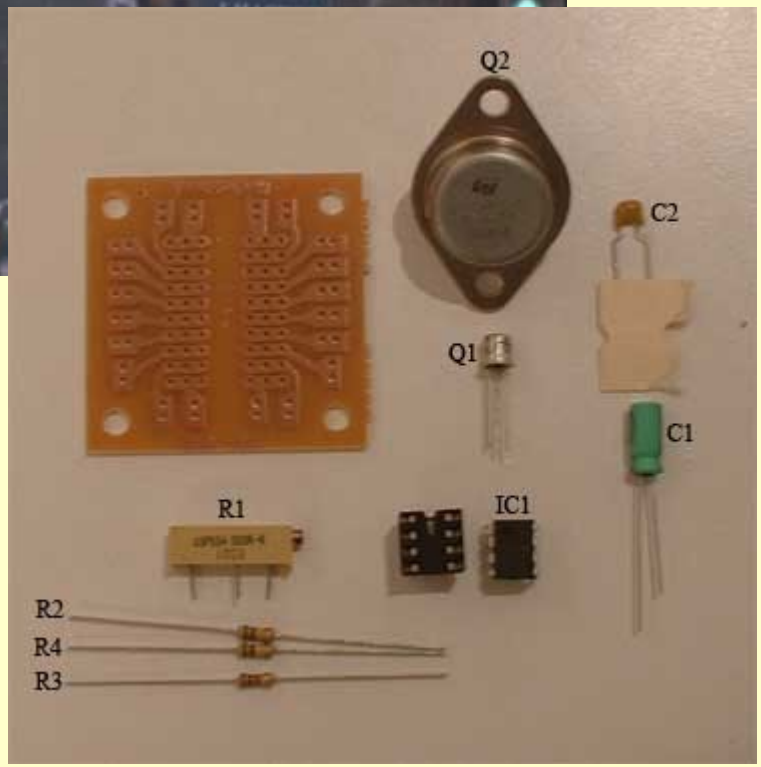




Napadi na SCADA sisteme.

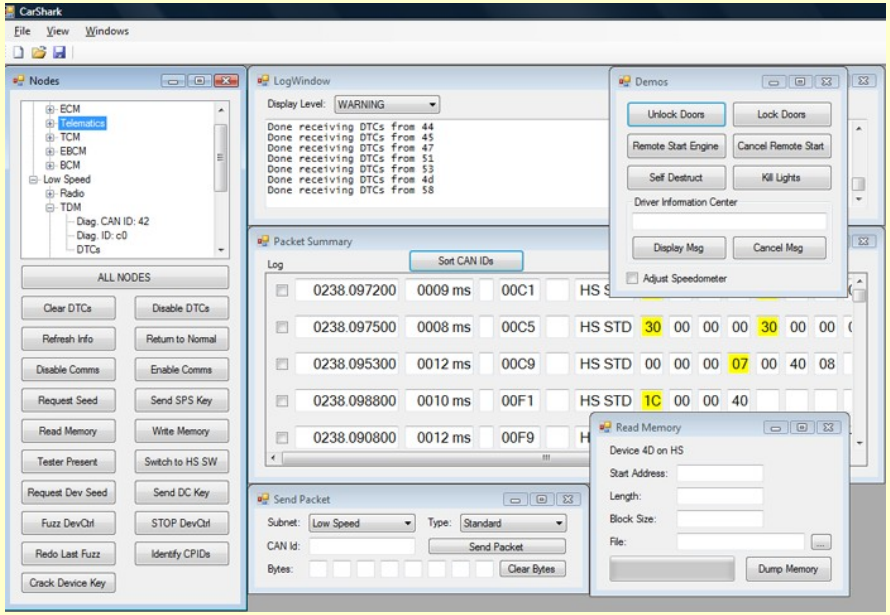
David Maynor in Robert Graham. 2006. SCADA Security and Terrorism: We're not crying wolf. <https://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf>

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>



Napad na semaforje.

[Napad na tramvaj.]



Napad na avtomobile.

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

Napad na prometne znake.

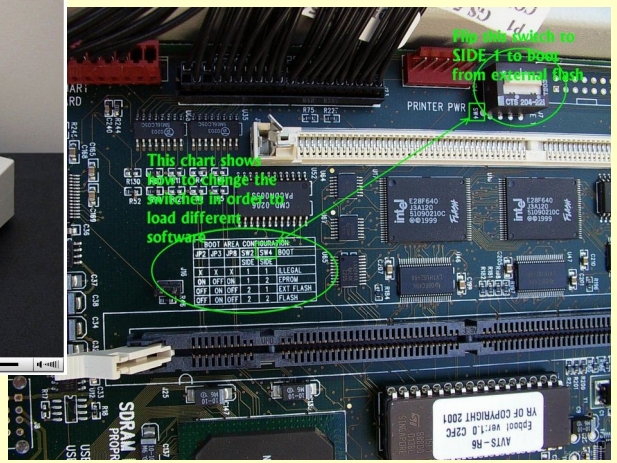
Vir in avtorstvo: i.hacked.com,
<http://www.i-hacked.com/content/view/274/48/>

Napadi na e-volitve

NO MILLION DOLLAR DONATION NEEDED
As seen in Argonne's demonstration of the Diebold attack, the parts needed cost no more than $26.

NO 'TOUCH' NEEDED
Argonne National Laboratory's Vulnerability Assessment Team 'secretly' takes over a Diebold Accuvote touch-screen voting system with a $16 remote control.

GARBAGE OUT
Close-up of results tape printed by a Diebold Accuvote touch-screen system after members of Argonne National Laboraty's Vulnerability Assessment Team (VAT) access the printer through its externally exposed pins.

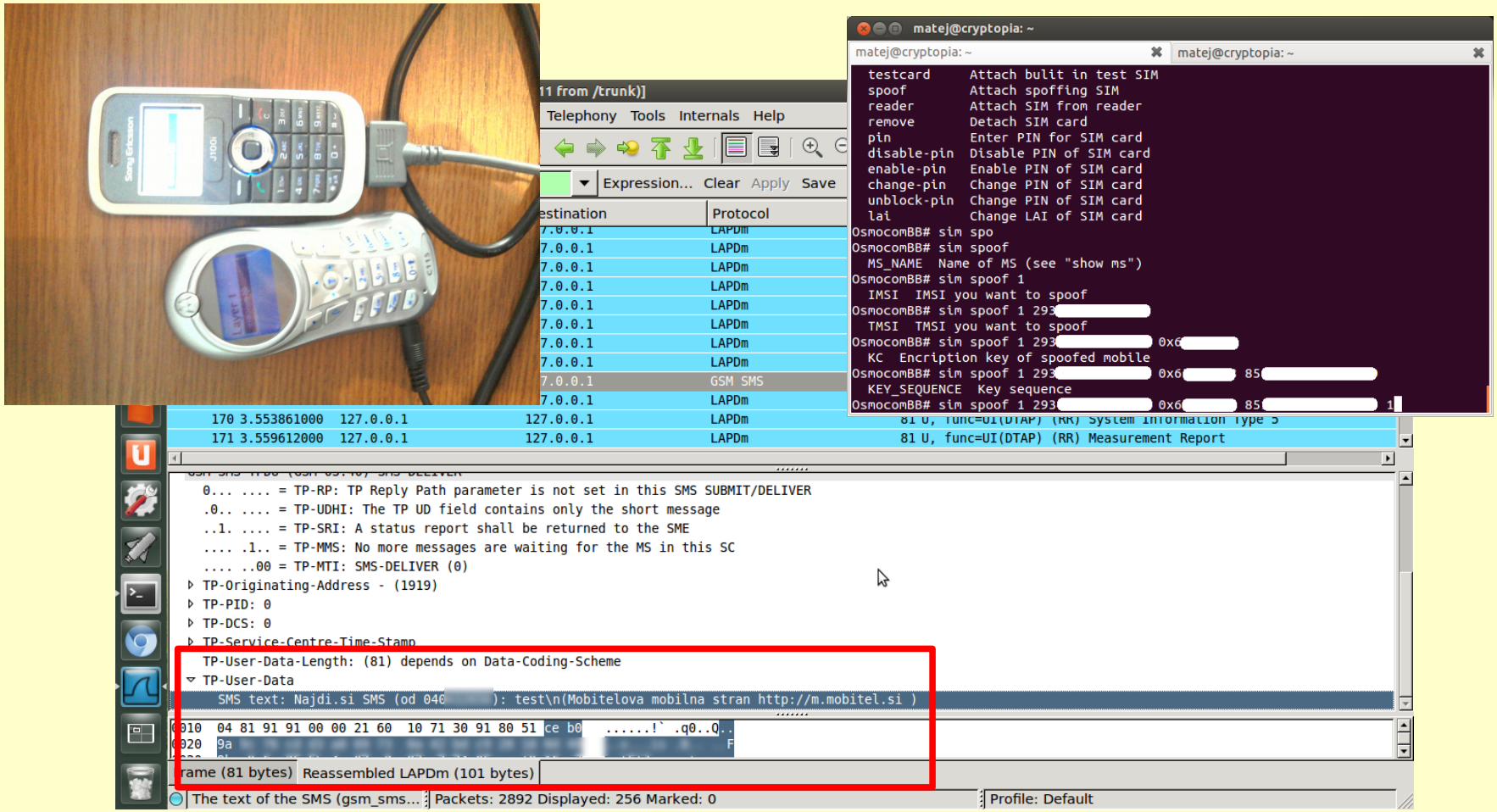


Napad na volilne naprave.

Napadi na bankomate

Napadi na bankomate.

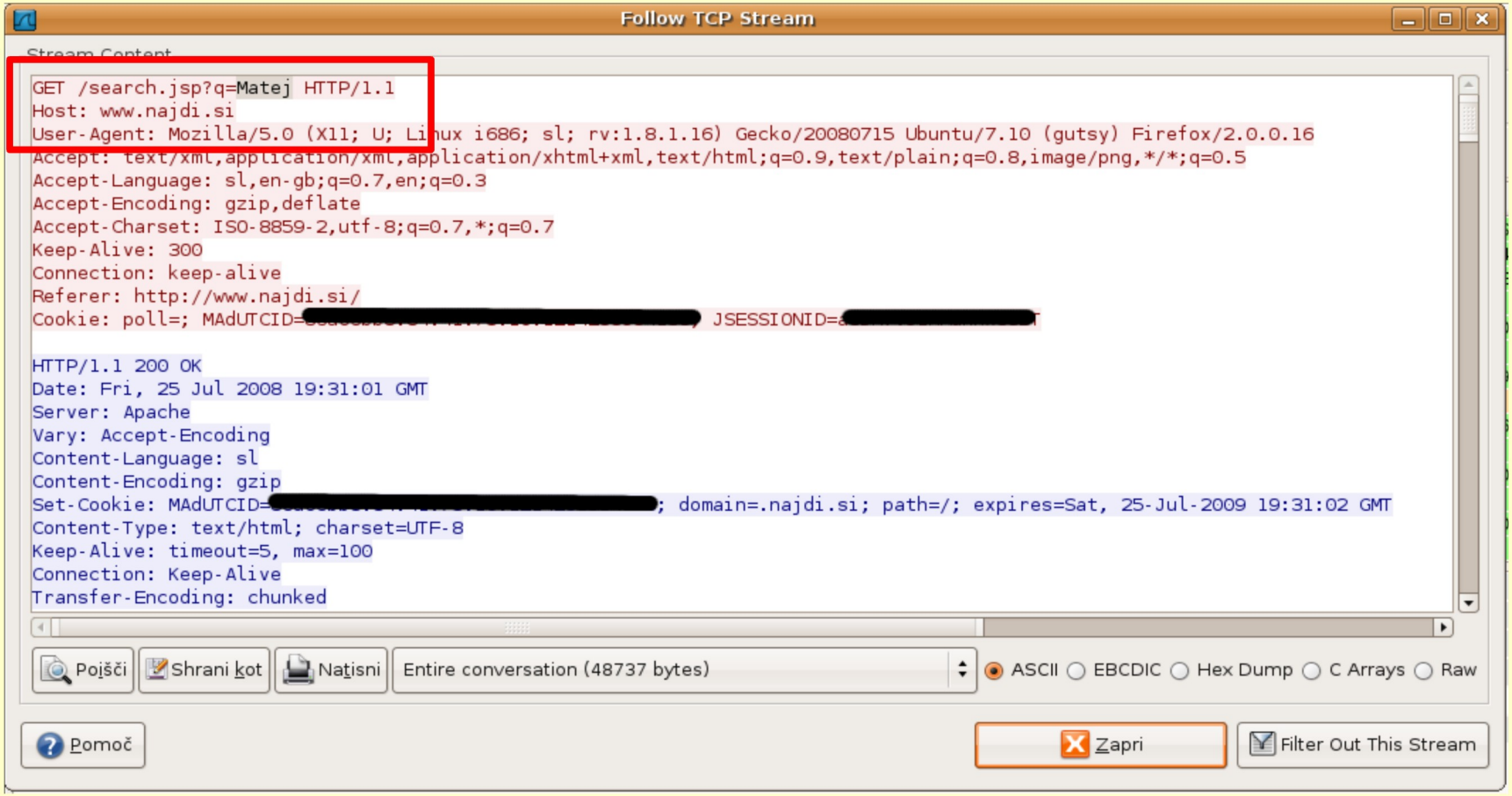
Napadi na mobilno telefonijo



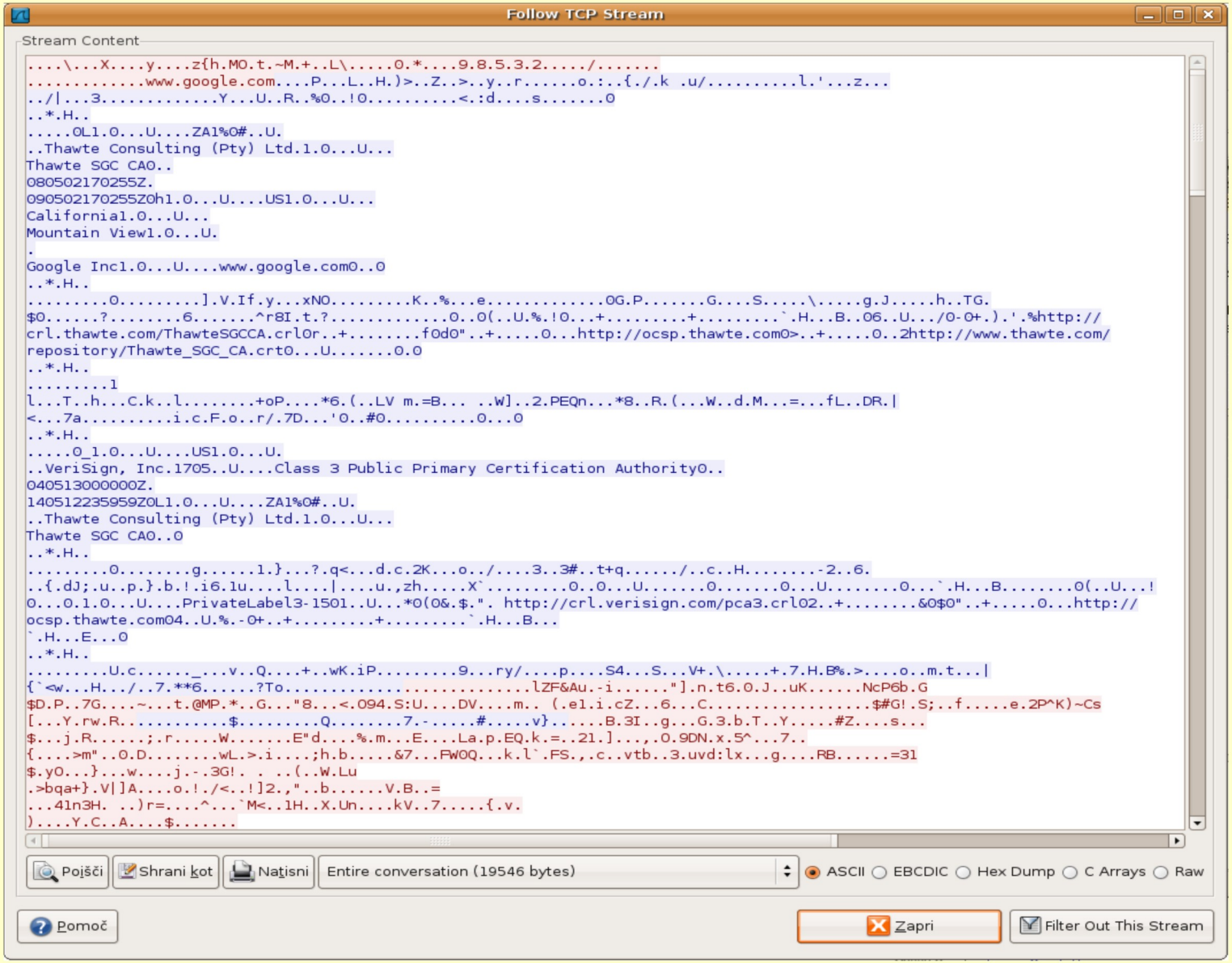
Napadi na mobilno telefonijo,
<https://pravokator.si/index.php/varnost-gsm/>

Prestrezanje komunikacij

Zakaj šifriranje?

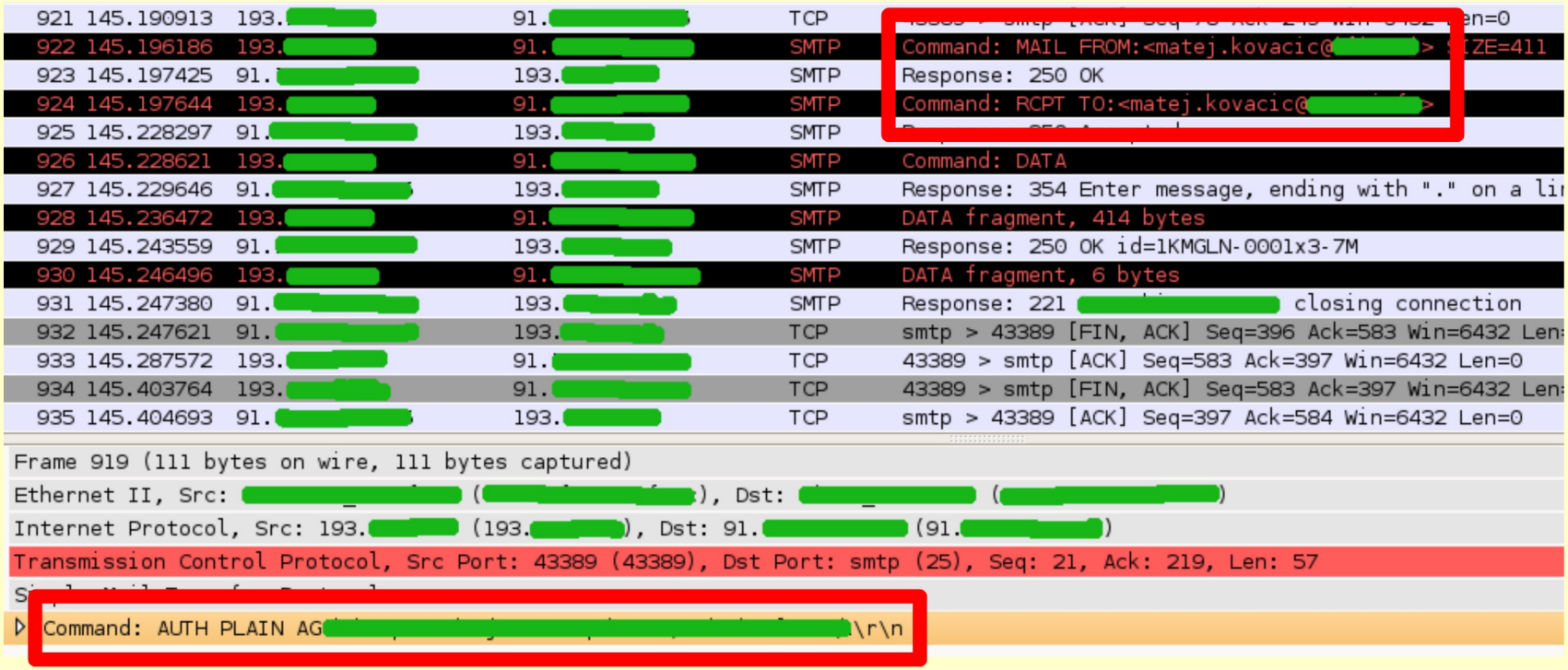


Nešifrirana spletna komunikacija.



Šifrirana spletna komunikacija.

Analiza omrežnega prometa

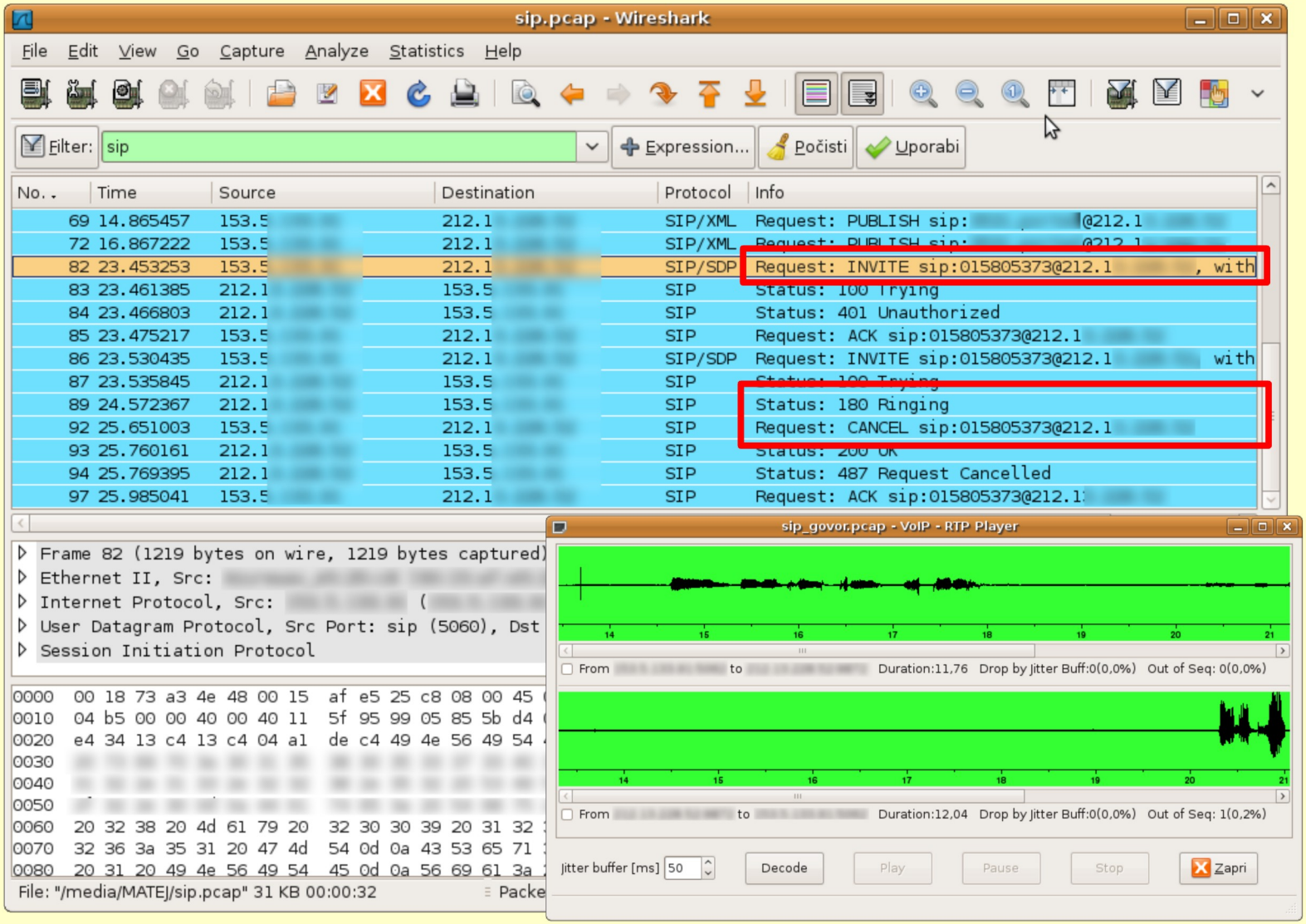


Command: AUTH PLAIN AG1hdGVqLmtvdmFjaWNAKioqKiouc2kAZ2VzbG8hrg==

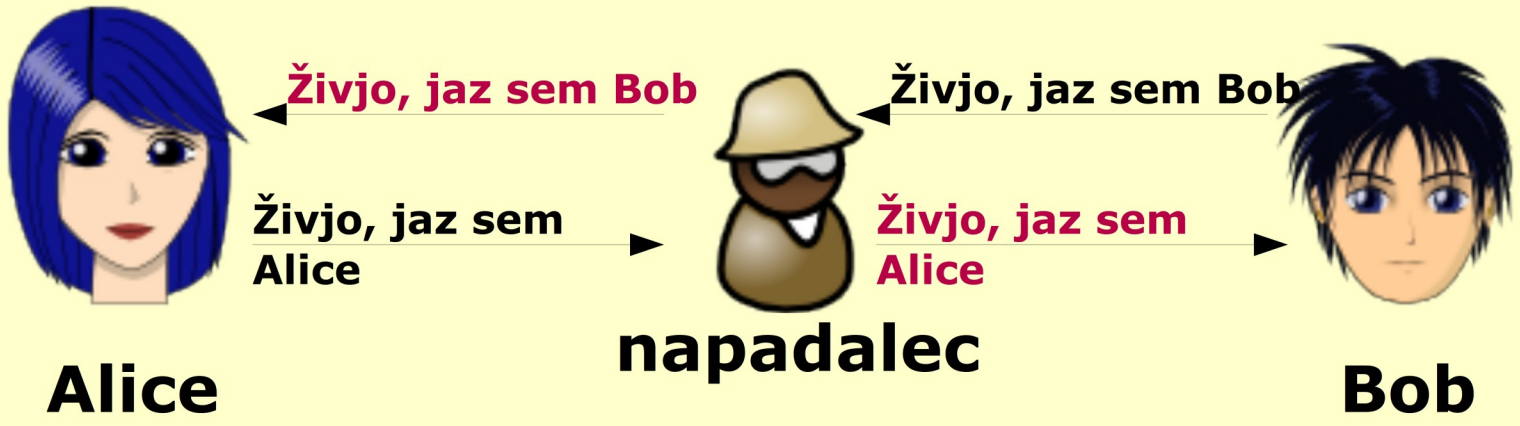
Uporabniško ime in geslo sta Base64 kodirana...

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

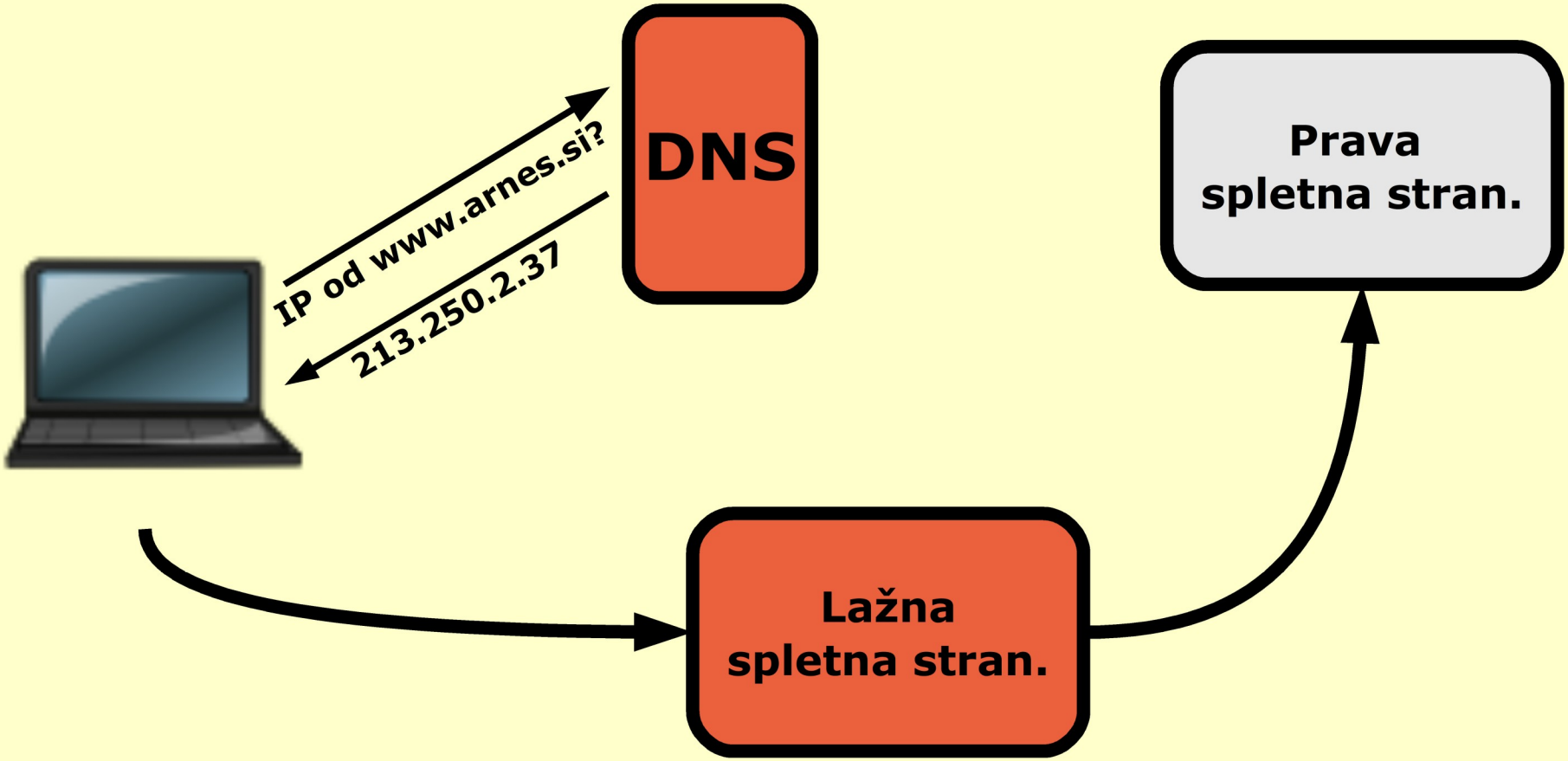
Omrežna analiza VoIP komunikacij

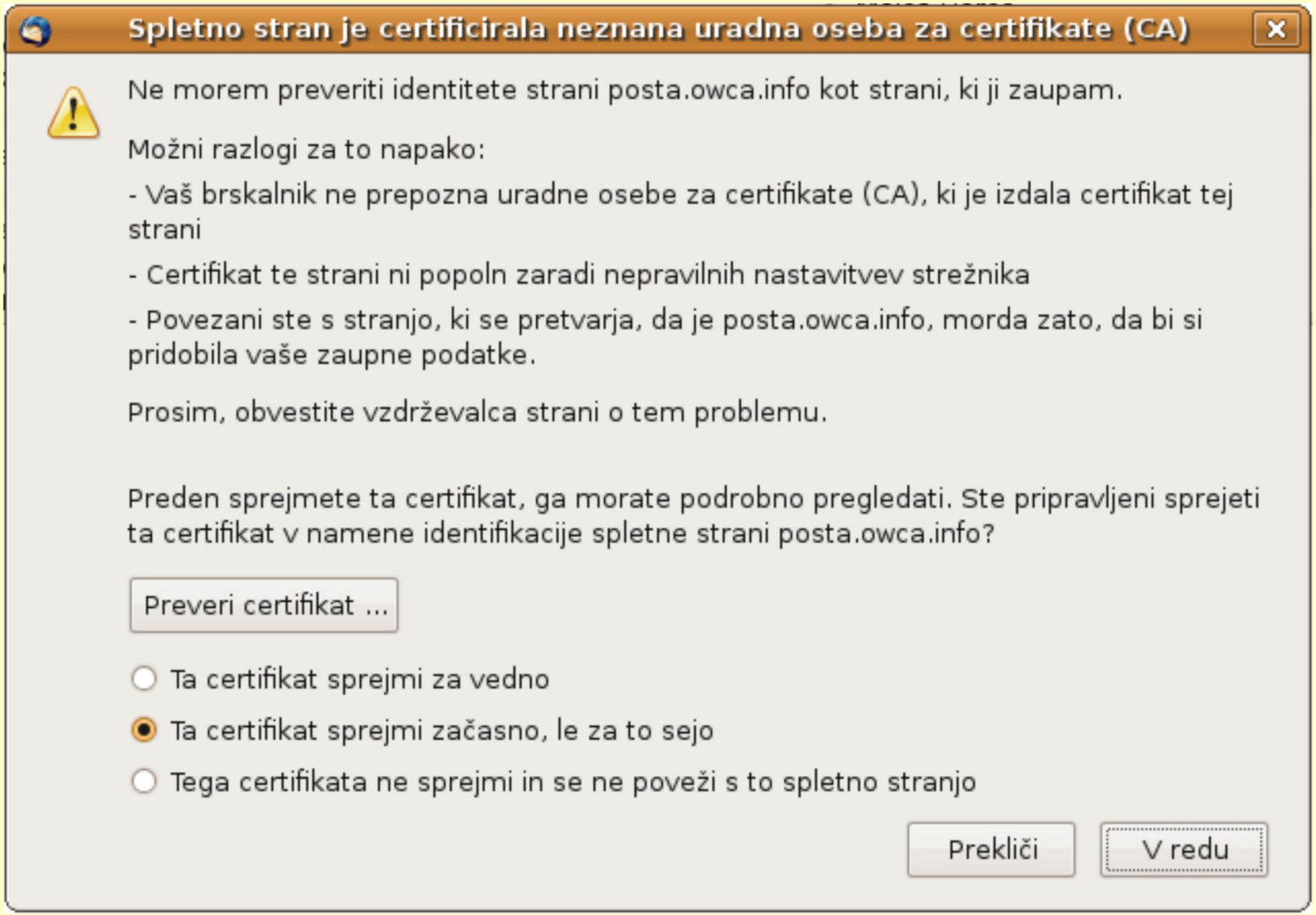


Napad s posrednikom (MITM napad)



DNS preusmerjanje



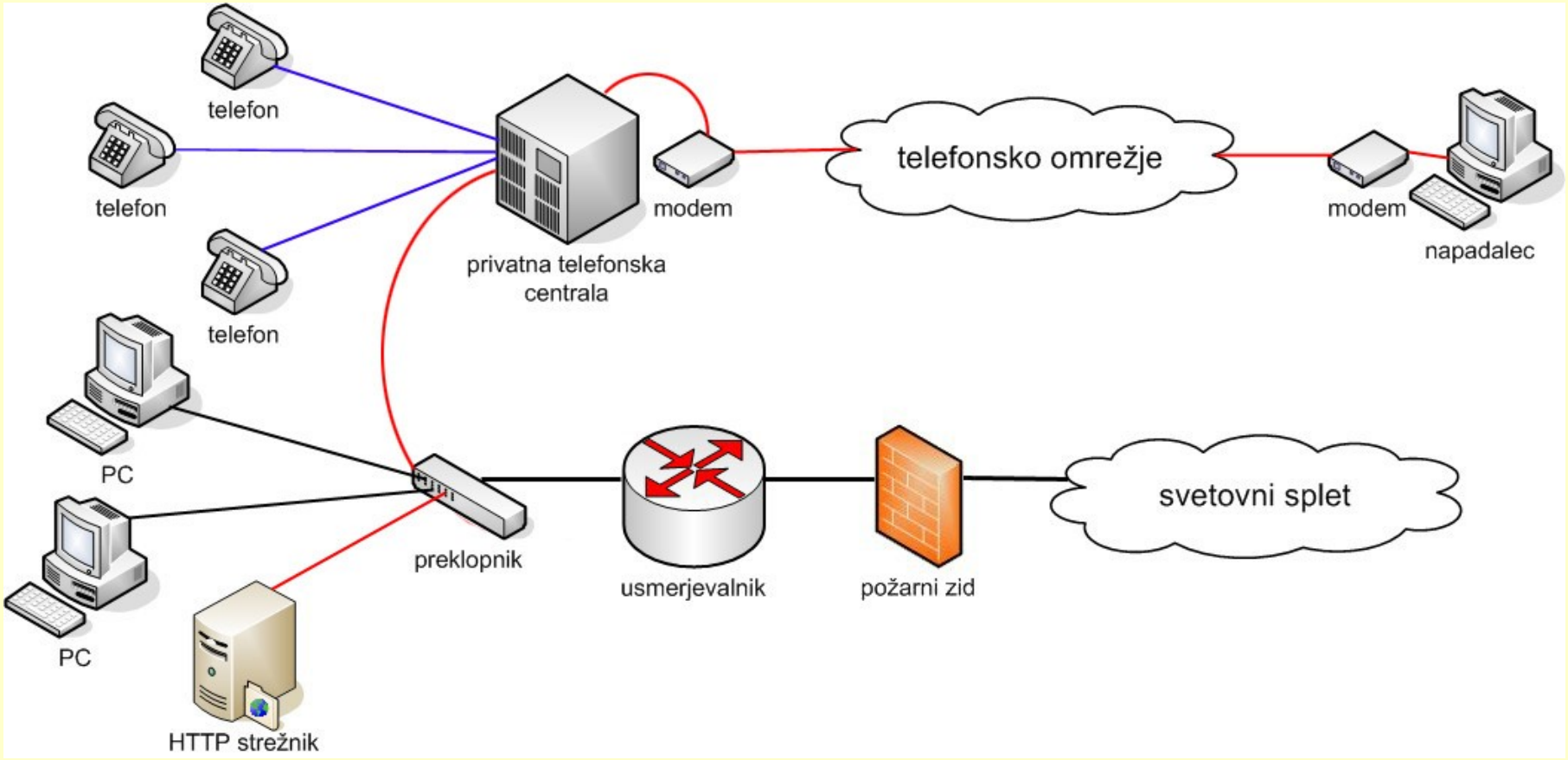

Spletno stran je certificirala neznana uradna oseba za certifikate (CA)
Ne morem preveriti identitete strani posta.owca.info kot strani, ki ji zaupam.
Možni razlogi za to napako:
- Vaš brskalnik ne prepozna uradne osebe za certifikate (CA), ki je izdala certifikat tej strani
- Certifikat te strani ni 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*.

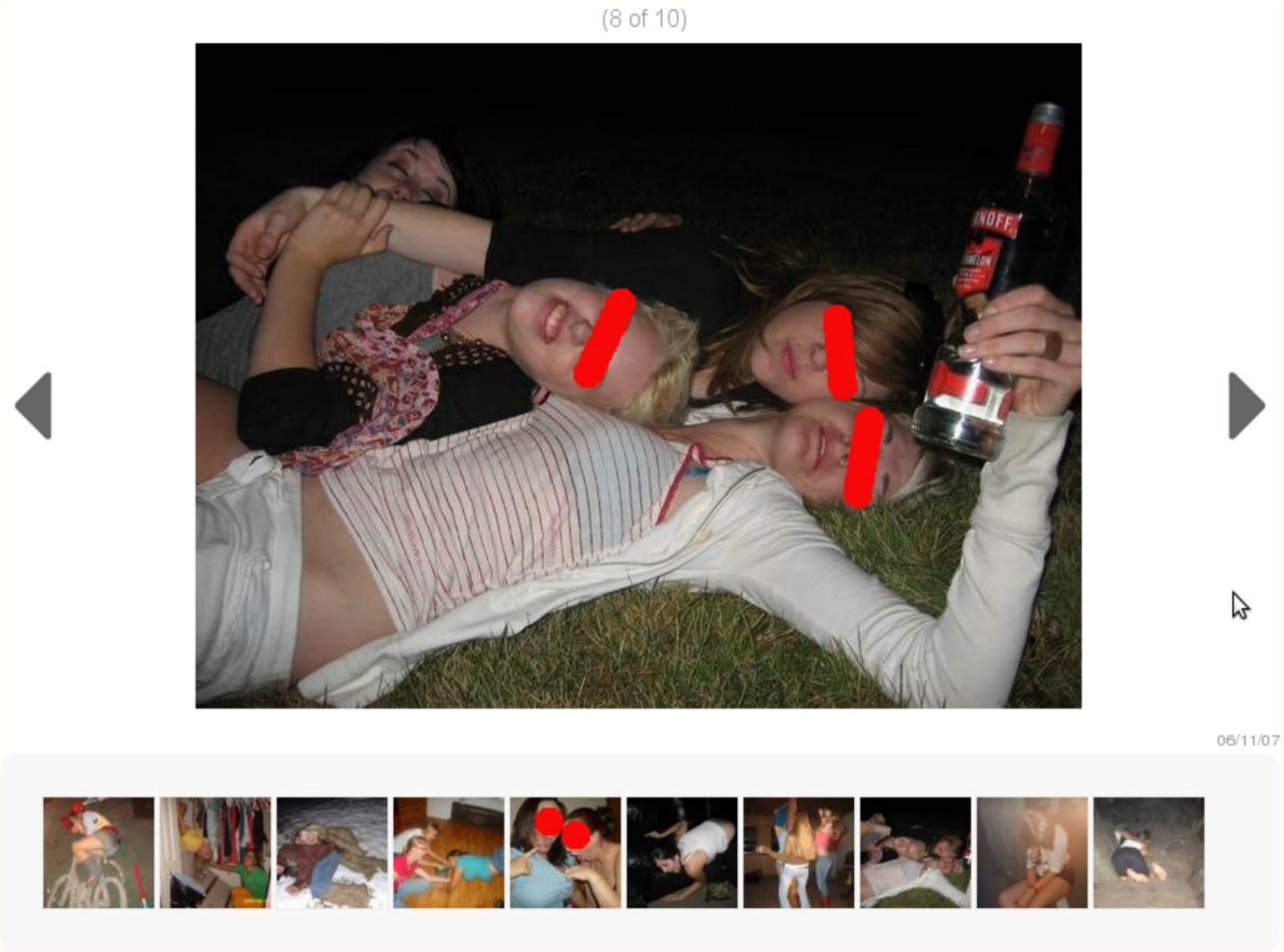
Vir in avtorstvo: dedected.org

Je dostop do lokalnega omrežja res zavarovan?



Javni ali zasebni prostor?

Socialna omrežja: zasebni ali javni prostor?

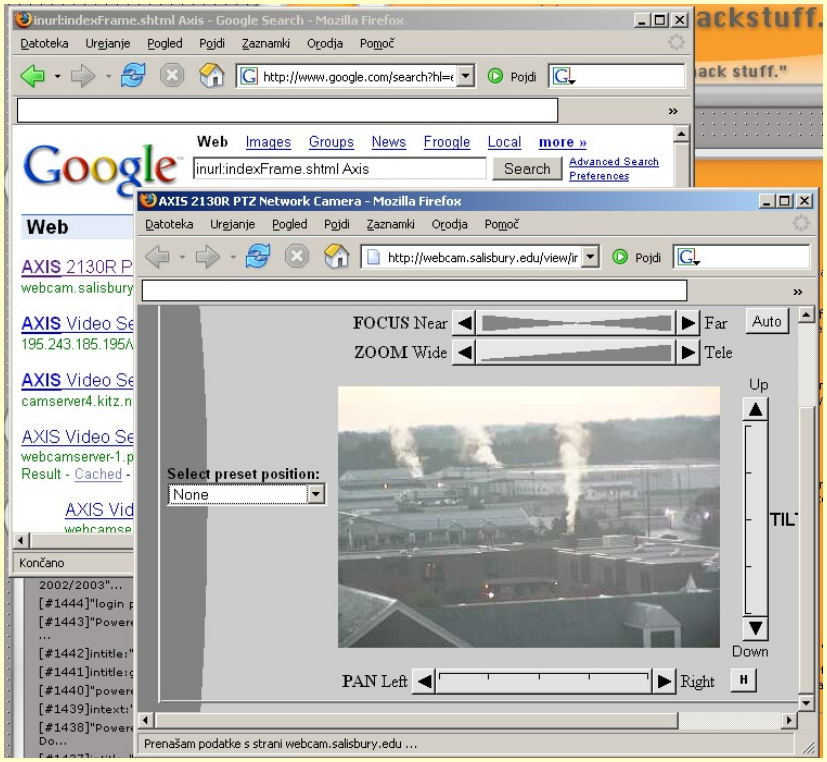


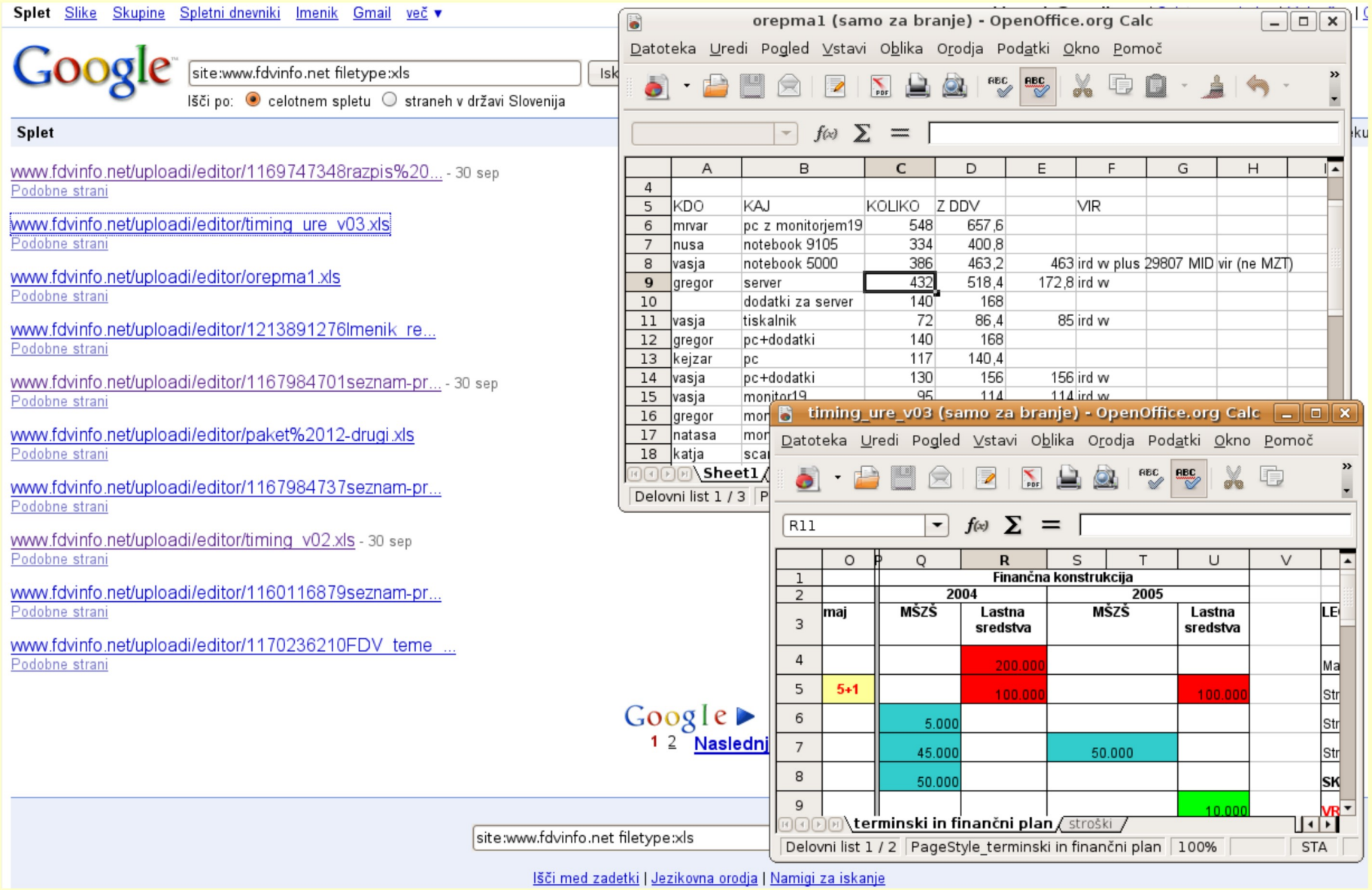
Ko *zaseben* podatek postane *javen*

- 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")

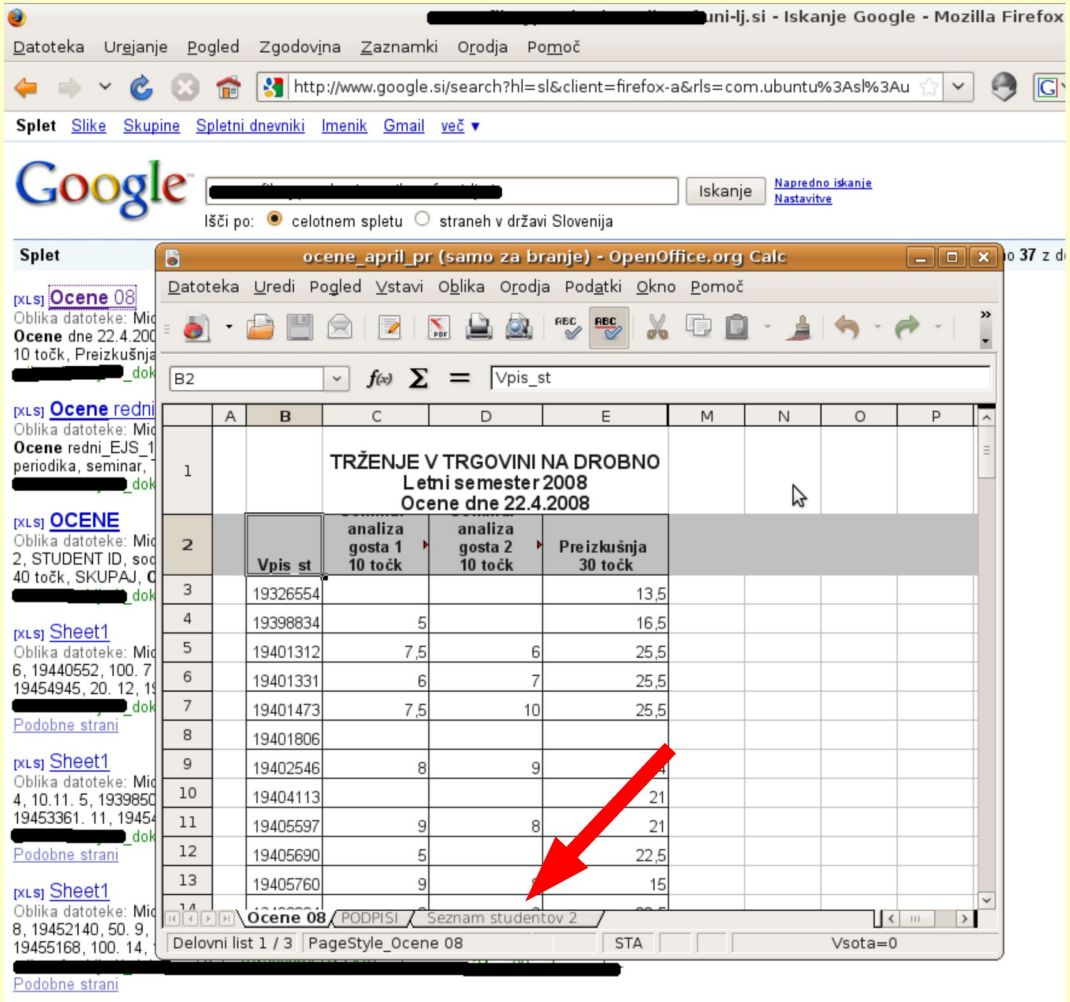
“Google hacking”

- 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).



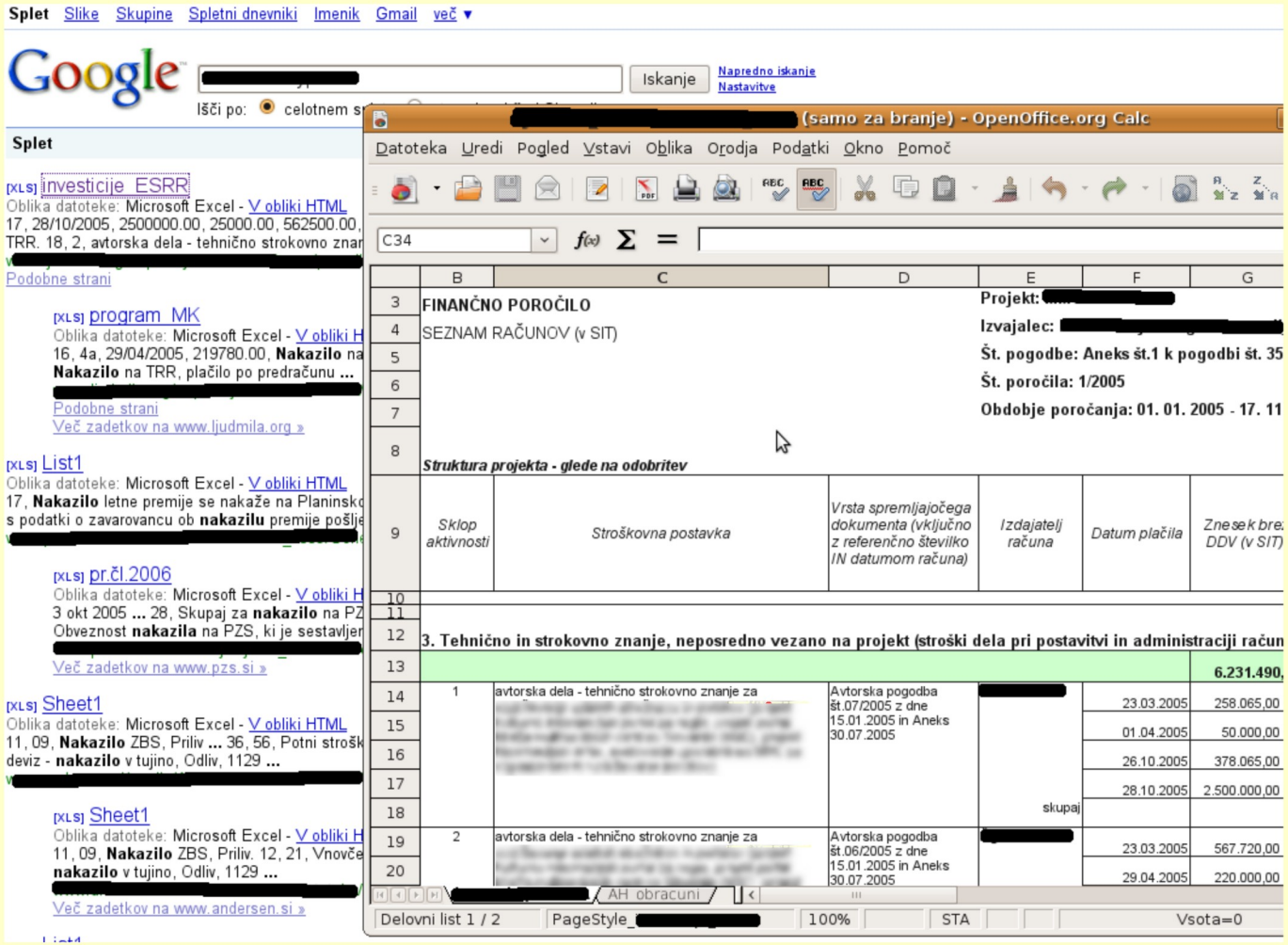

Splet Slike Skupine Spletni dnevniki Imenik Gmail več
Google
site:www.fdvinfo.net filetype:xls
Išči po: celotnem spletu straneh v državi Slovenija
Splet
www.fdvinfo.net/uploadi/editor/1169747348razpis%20... - 30 sep
Podobne strani
www.fdvinfo.net/uploadi/editor/timing_ure_v03.xls
Podobne strani
www.fdvinfo.net/uploadi/editor/orepma1.xls
Podobne strani
www.fdvinfo.net/uploadi/editor/1213891276lmenik_re...
Podobne strani
www.fdvinfo.net/uploadi/editor/1167984701seznam-pr... - 30 sep
Podobne strani
www.fdvinfo.net/uploadi/editor/paket%2012-drugi.xls
Podobne strani
www.fdvinfo.net/uploadi/editor/1167984737seznam-pr...
Podobne strani
www.fdvinfo.net/uploadi/editor/timing_v02.xls - 30 sep
Podobne strani
www.fdvinfo.net/uploadi/editor/1160116879seznam-pr...
Podobne strani
www.fdvinfo.net/uploadi/editor/1170236210FDV_teme ...
Podobne strani
Google
1 2 Naslednj
orepma1 (samo za branje) - OpenOffice.org Calc
Datoteka Uredi Pogled Vstavi Oblika Orodja Podatki Okno Pomoč
KDO KAJ KOLIKO Z DDV VIR
mrvar pc z monitorjem19 548 657,6
nusa notebook 9105 334 400,8
vasja notebook 5000 386 463,2 463 ird w plus 29807 MID vir (ne MZT)
gregor server 432 518,4 172,8 ird w
dodatki za server 140 168
vasja tiskalnik 72 86,4 85 ird w
gregor pc+dodatki 140 168
kejzar pc 117 140,4
vasja pc+dodatki 130 156 156 ird w
Sheet1
Delovni list 1 / 3
timing_ure_v03 (samo za branje) - OpenOffice.org Calc
Datoteka Uredi Pogled Vstavi Oblika Orodja Podatki Okno Pomoč
R11
Finančna konstrukcija
2004
2005
maj
MŠZŠ
Lastna sredstva
MŠZŠ
Lastna sredstva
200.000
5+1
100.000
100.000
5.000
45.000
50.000
50.000
10.000
terminski in finančni plan
stroški
Delovni list 1 / 2
PageStyle_terminski in finančni plan
100%
STA
site:www.fdvinfo.net filetype:xls
Išči med zadetki | Jezikovna orodja | Namigi za iskanje

Javno ali zasebno?



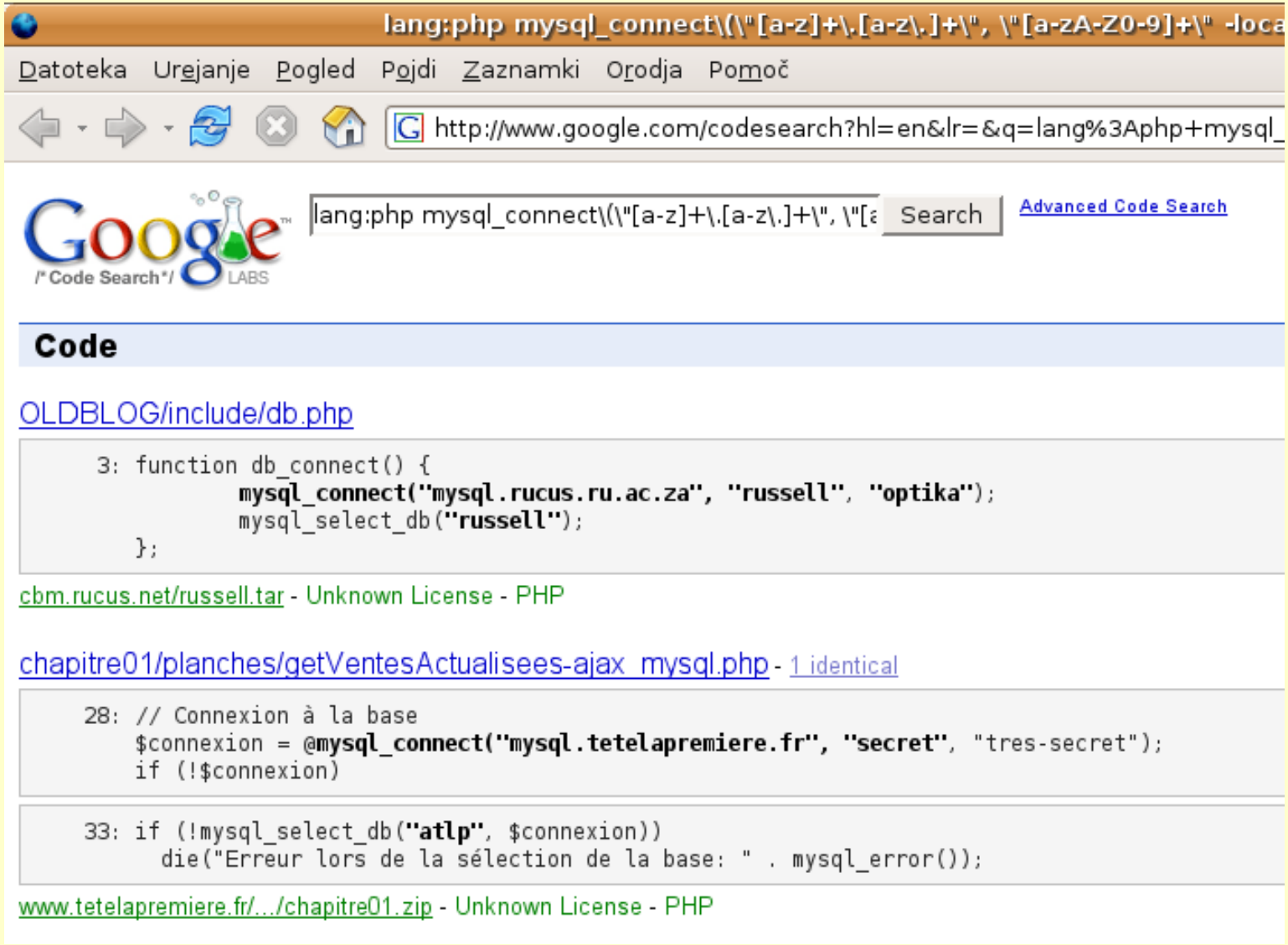
"Google hacking"

Javno ali zasebno?

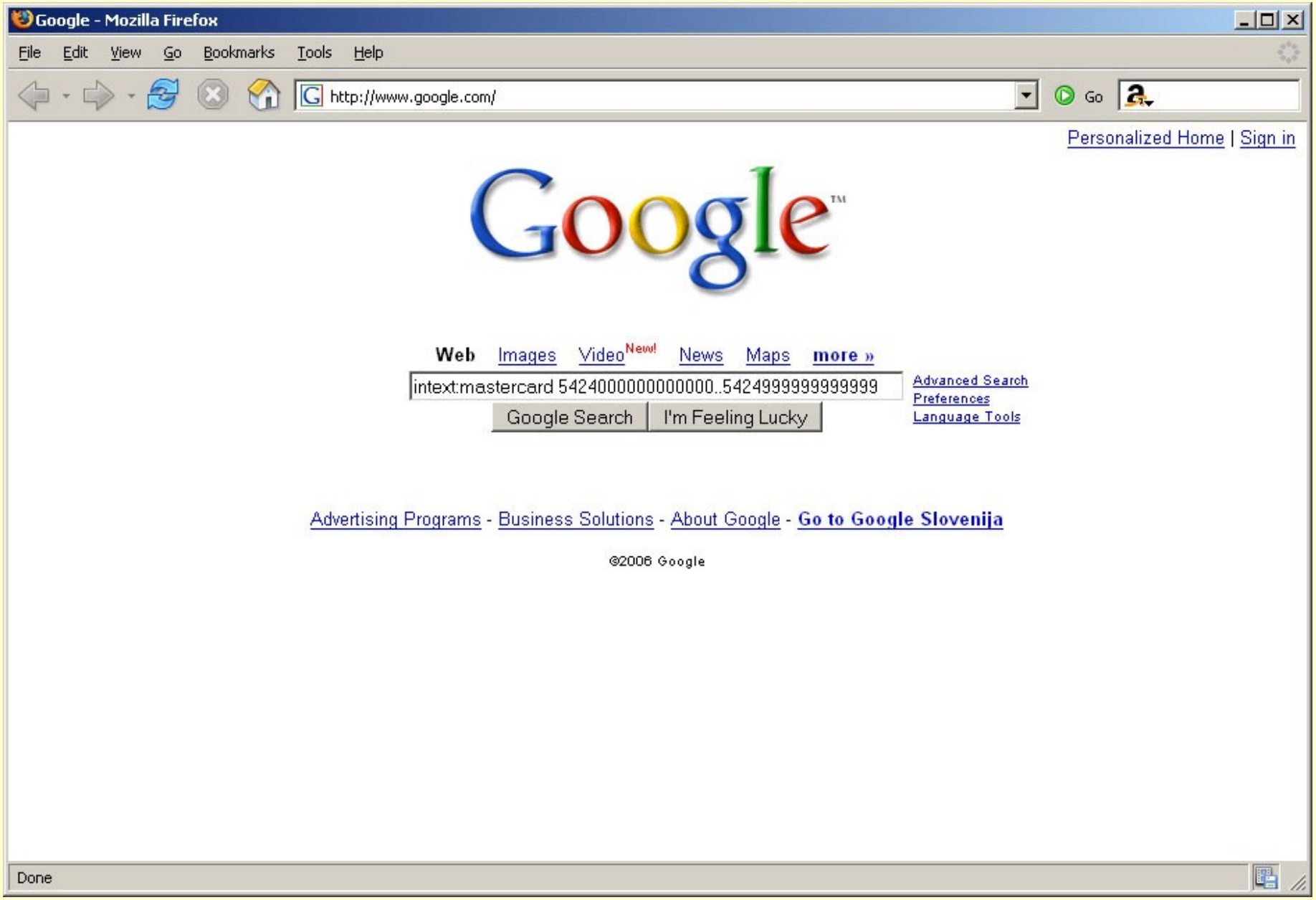


"Google hacking"

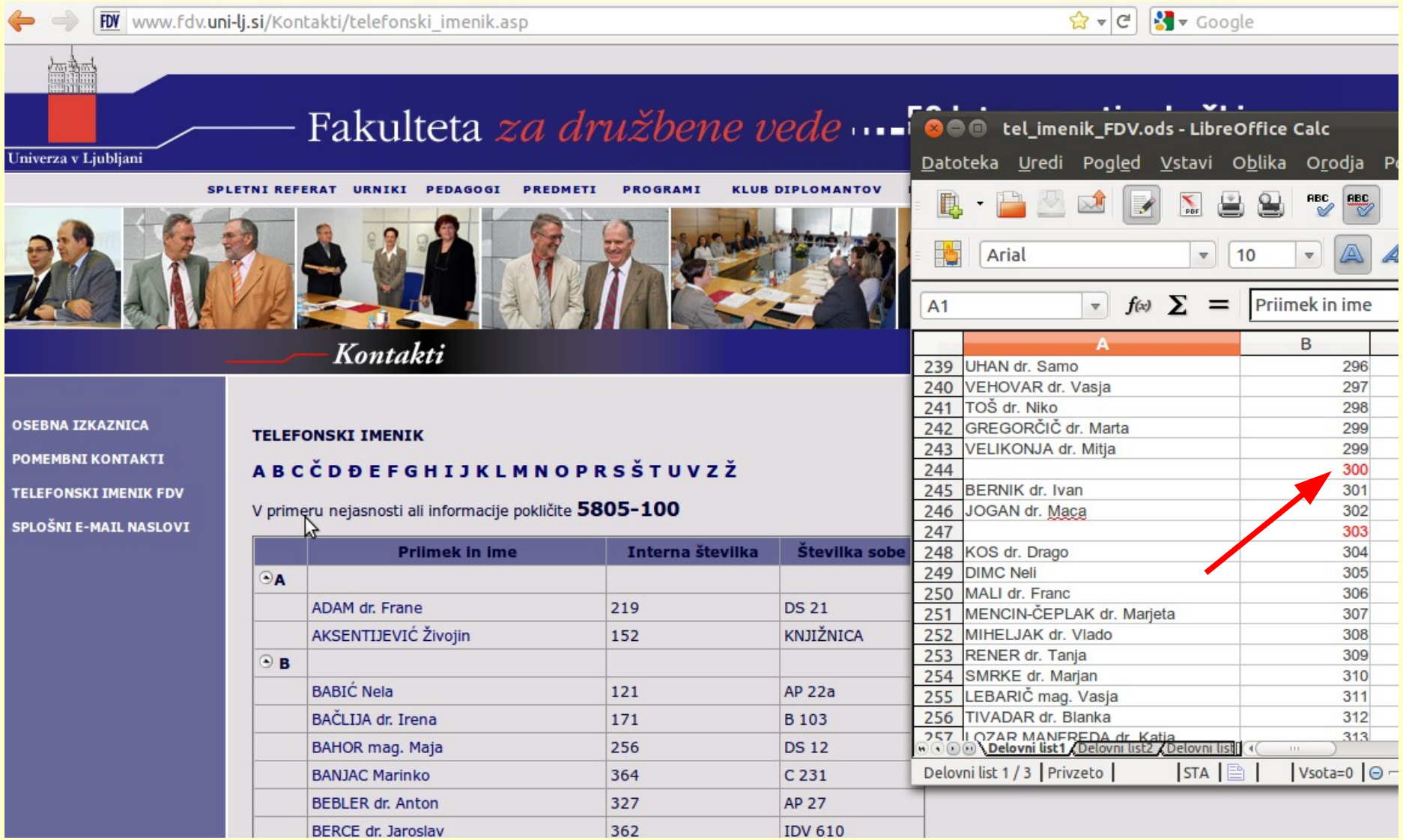
“Google hacking”

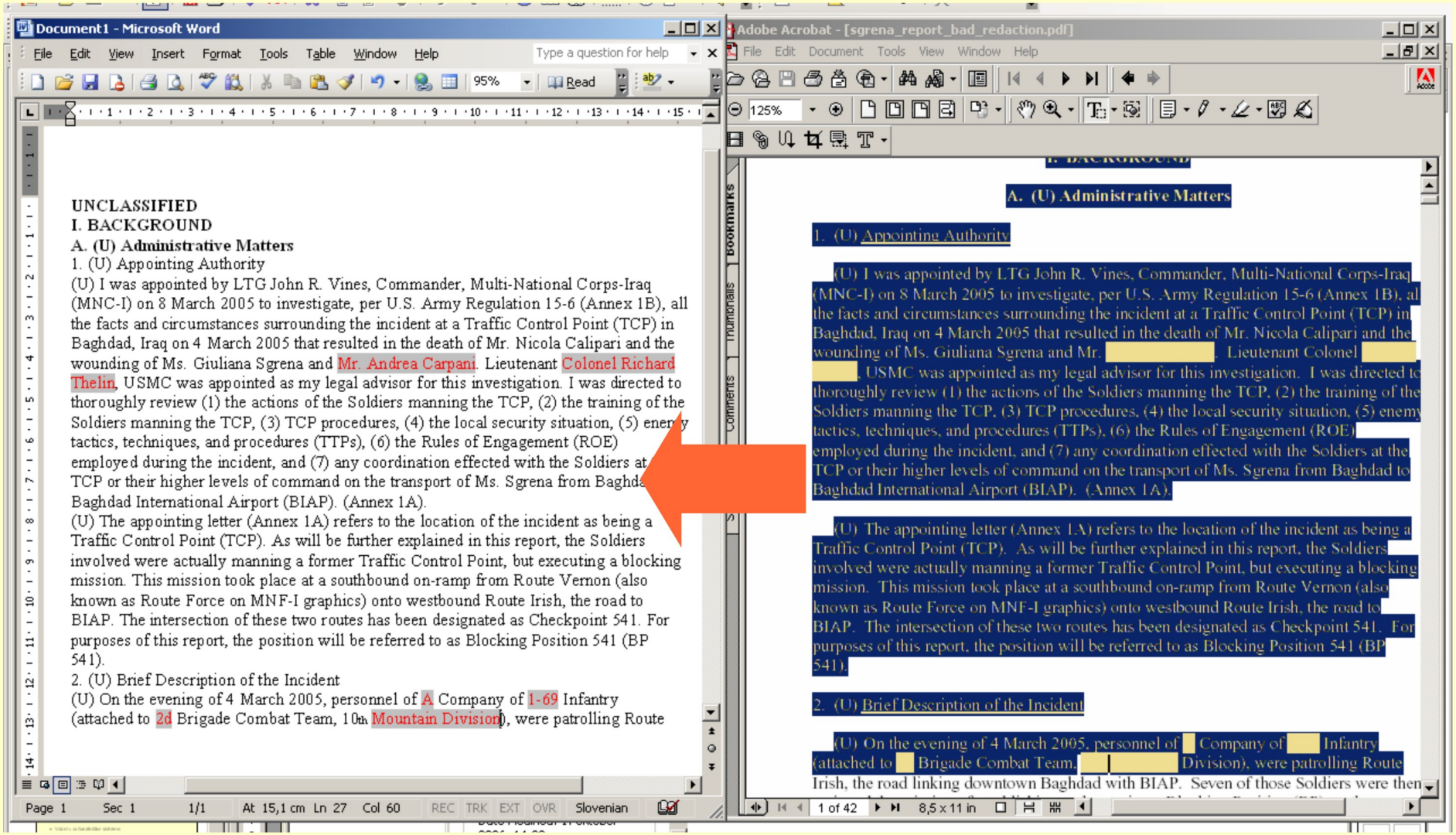


Iskanje gesel za vdor s pomočjo “Google hacking-a”.


Google - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.google.com/
Go
Personalized Home | Sign in
Google™
Web Images Video New! 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 Slovenija
©2006 Google
Done

Javno ali zasebno?


www.fdv.uni-lj.si/Kontakti/telefonski_imenik.asp
Google
Univerza v Ljubljani
Fakulteta za družbene vede
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
Priimek in ime | Interna številka | Številka sobe
A
ADAM dr. Frane | 219 | DS 21
AKSENTIJEVIĆ Živojin | 152 | KNJIŽNICA
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
Arial
10
A1
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. Maca 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
Delovni list1 Delovni list2 Delovni list
Delovni list 1 / 3 Privzeto STA Vsota=0


Document1 - Microsoft Word
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 Baghda 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]
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), al 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. . Lieutenant Colonel , 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 Company of Infantry (attached to Brigade Combat Team, 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

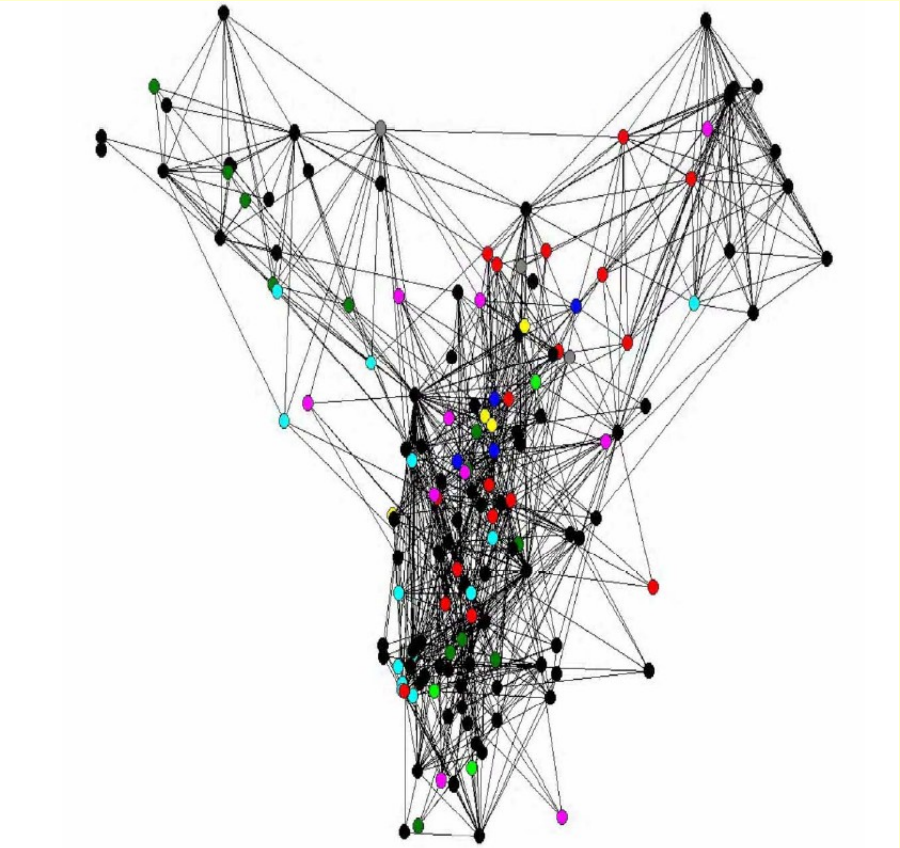
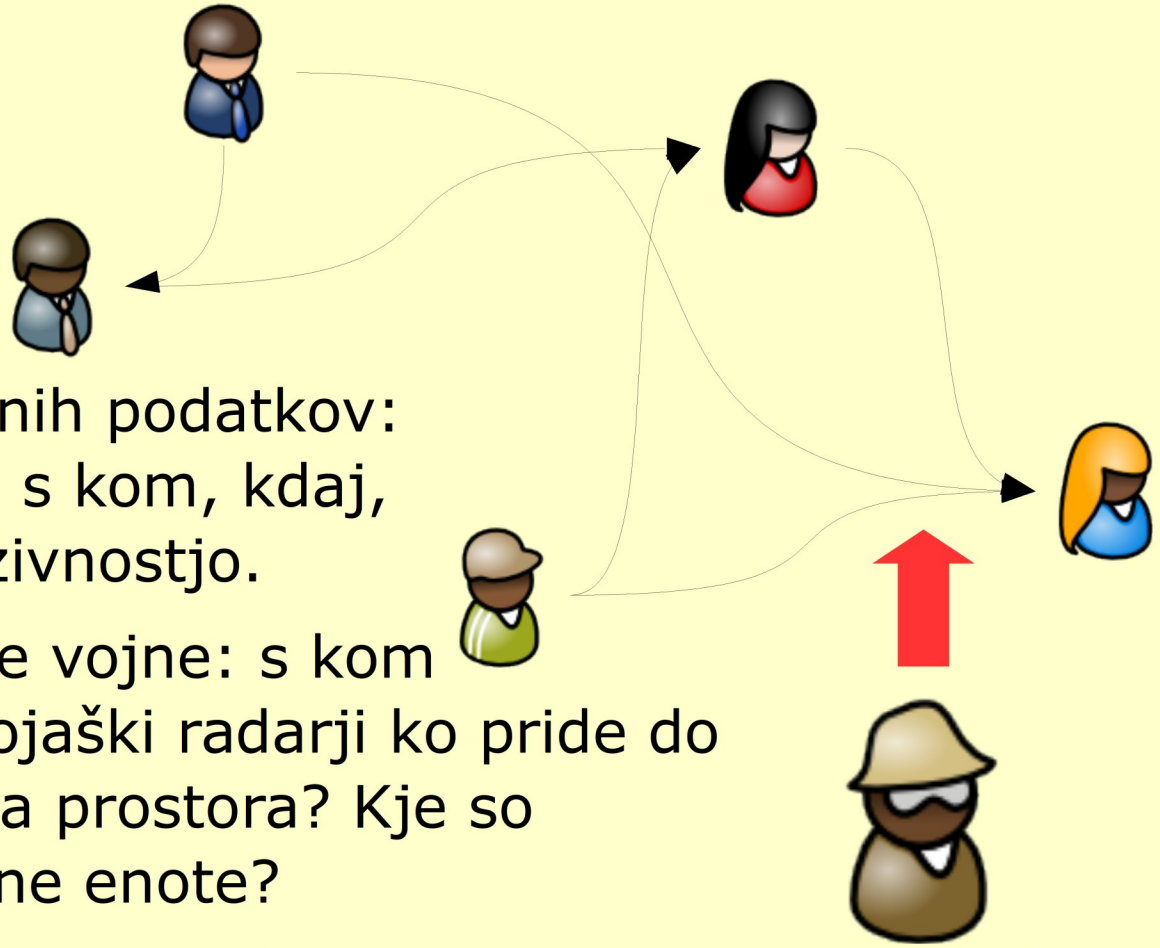


Figure 7: Network showing how the ex employees were connected
Red: Vice President, Blue: President, Black: Employee (non managerial), Grey: In House Lawyer, Pink: Manager, Dark Green: Trader, Light Green: Managing Director, Light Blue: Director, Yellow: CEO

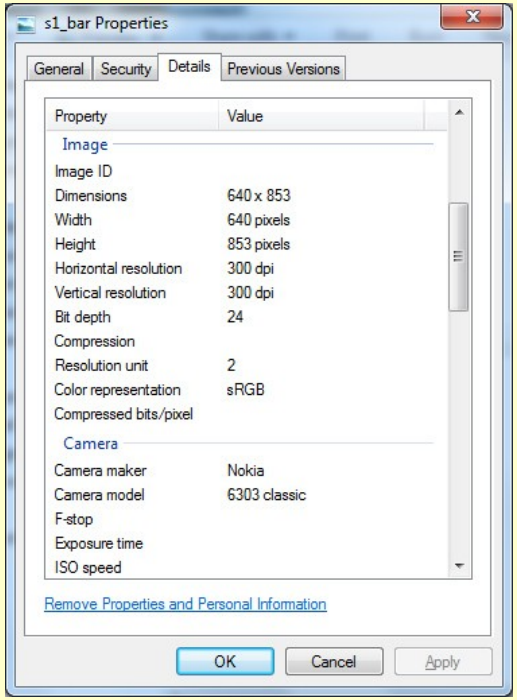
Kdo v Enronu je s kom komuniciral – socialno omrežje zaposlenih.
Vir in avtorstvo: *Shetty in Adibi, The Enron Email Dataset - Database Schema and Brief Statistical Report, 2004*.

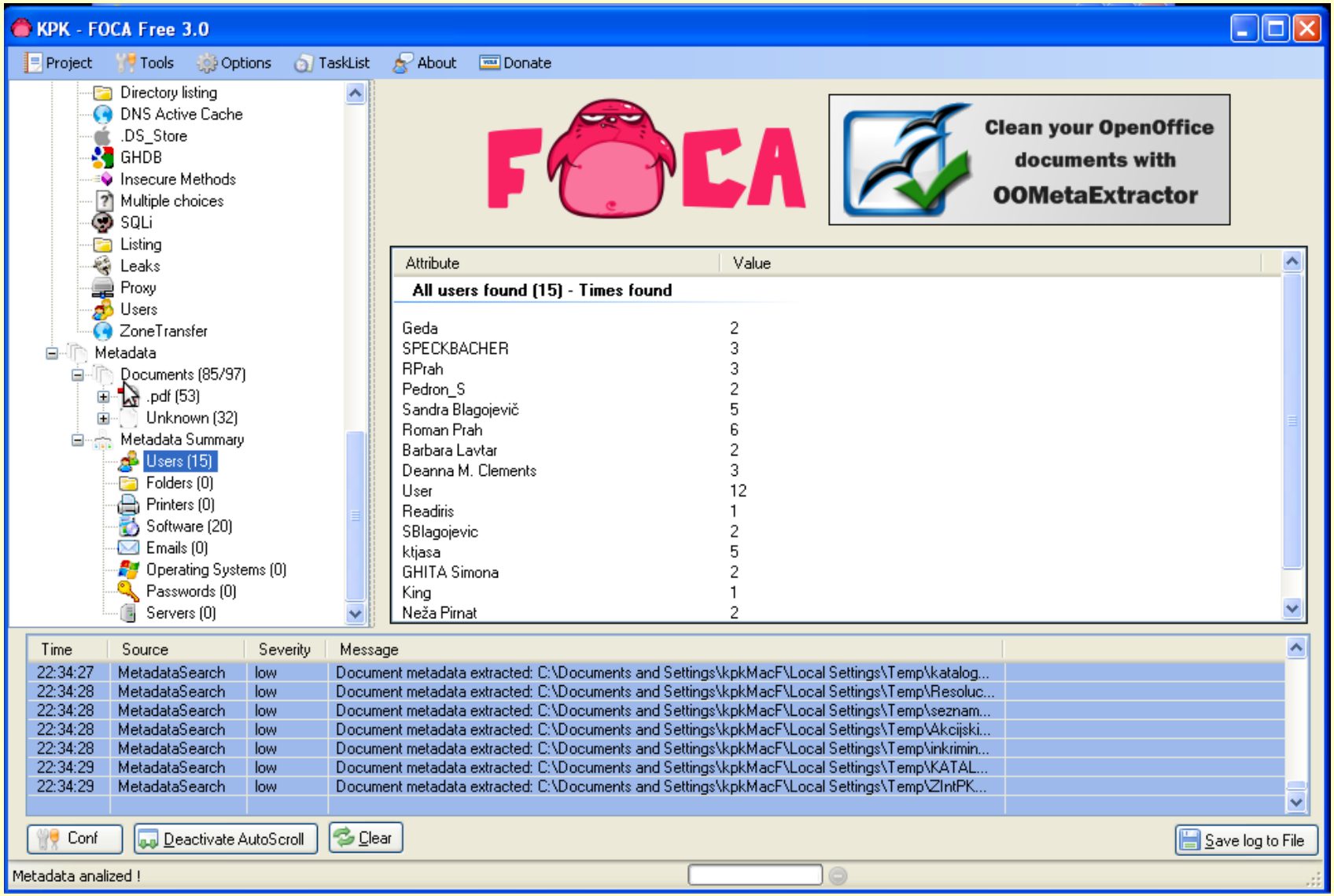
Analiza prometa



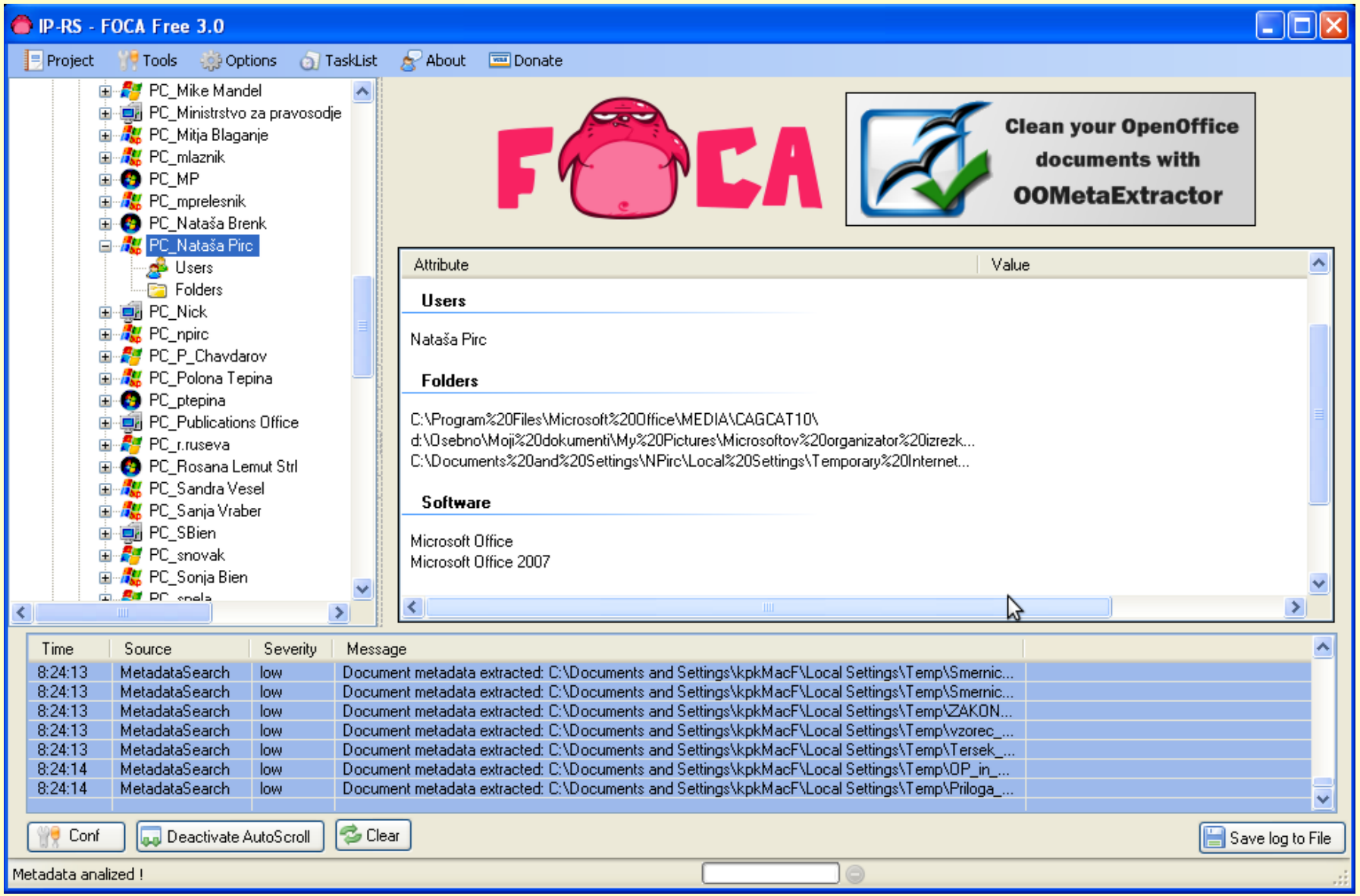
- Analiza prometnih podatkov: kdo komunicira s kom, kdaj, s kakšno intenzivnostjo.
- Primer iz hladne vojne: s kom komunicirajo vojaški radarji ko pride do kršitve zračnega prostora? Kje so locirane sovražne enote?
- Deluje tudi kadar je vsebina komunikacije šifrirana.

Skriti metapodatki...





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



FOCA – analiza www.ip-rs.si

```
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 repo
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up)
```

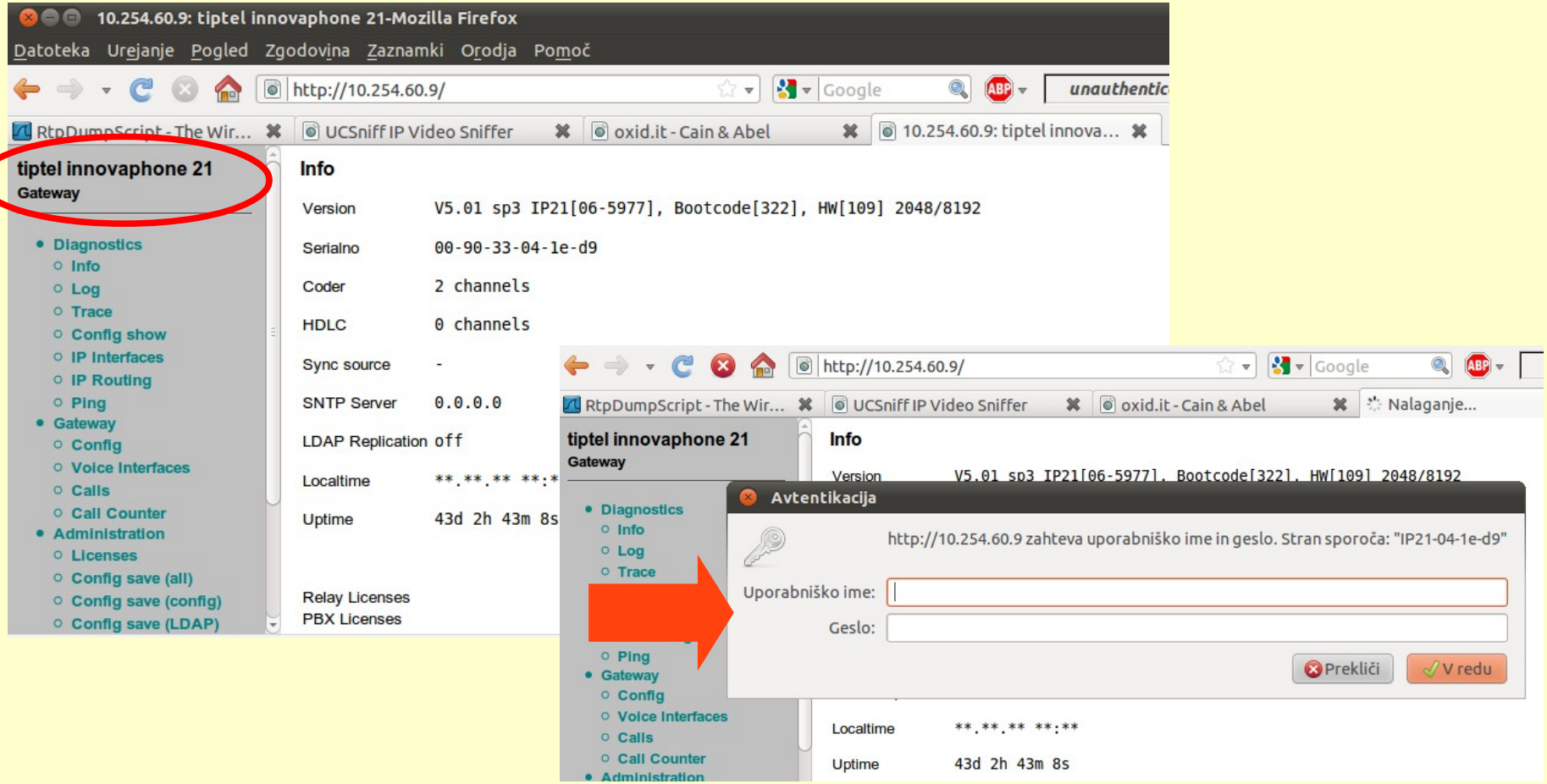
```
dig kpk-rs.si MX

; <<>> 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
```

```
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
```

Identifikacija strežnikov organizacije s standardnimi omrežnimi orodji...

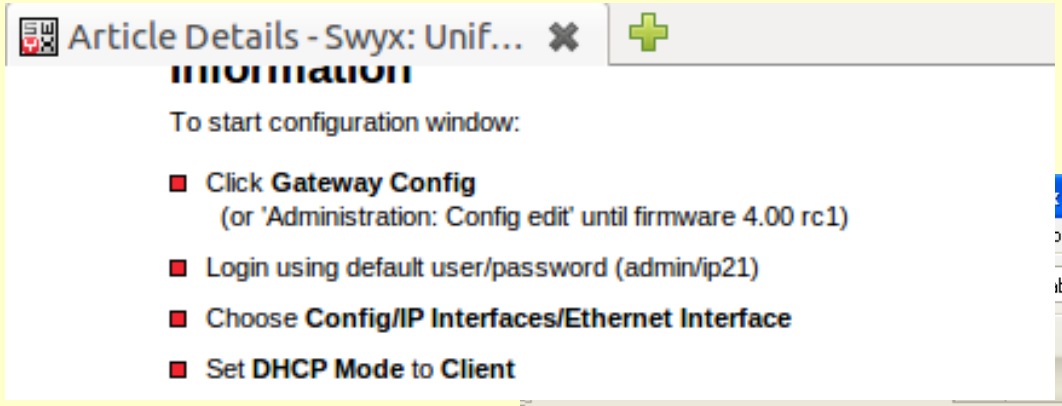
Gesla

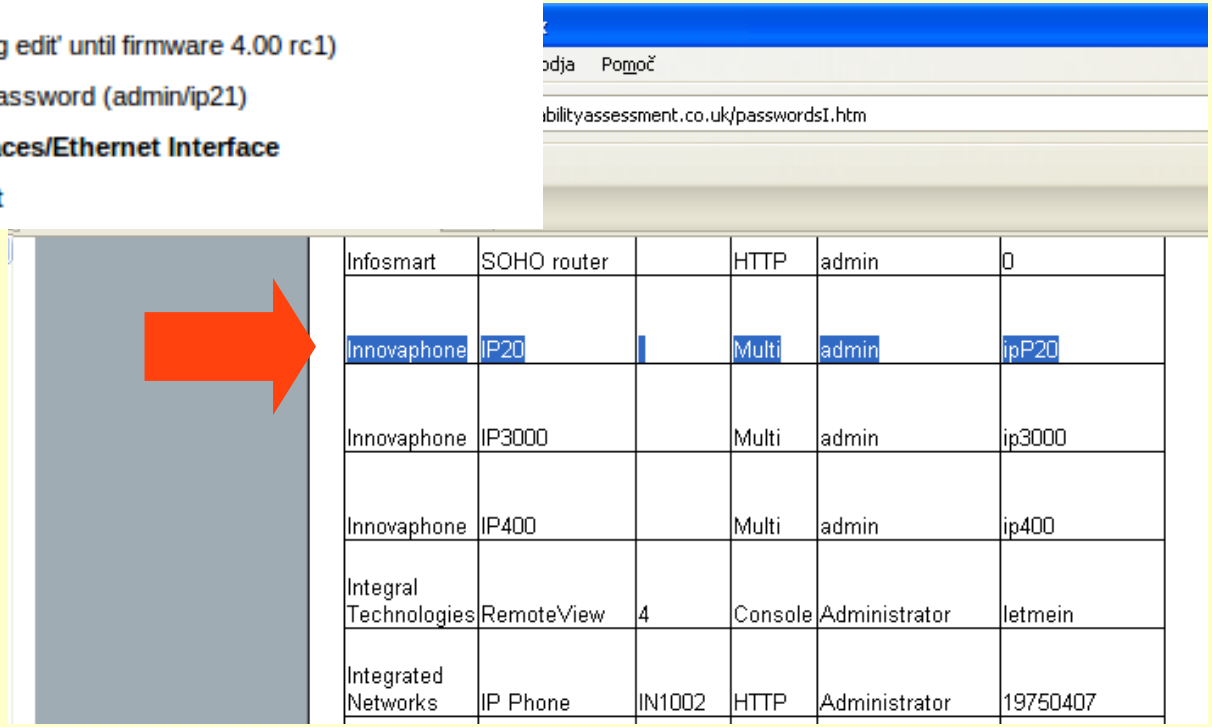
Uporaba privzetih gesel



Uporaba privzetih gesel

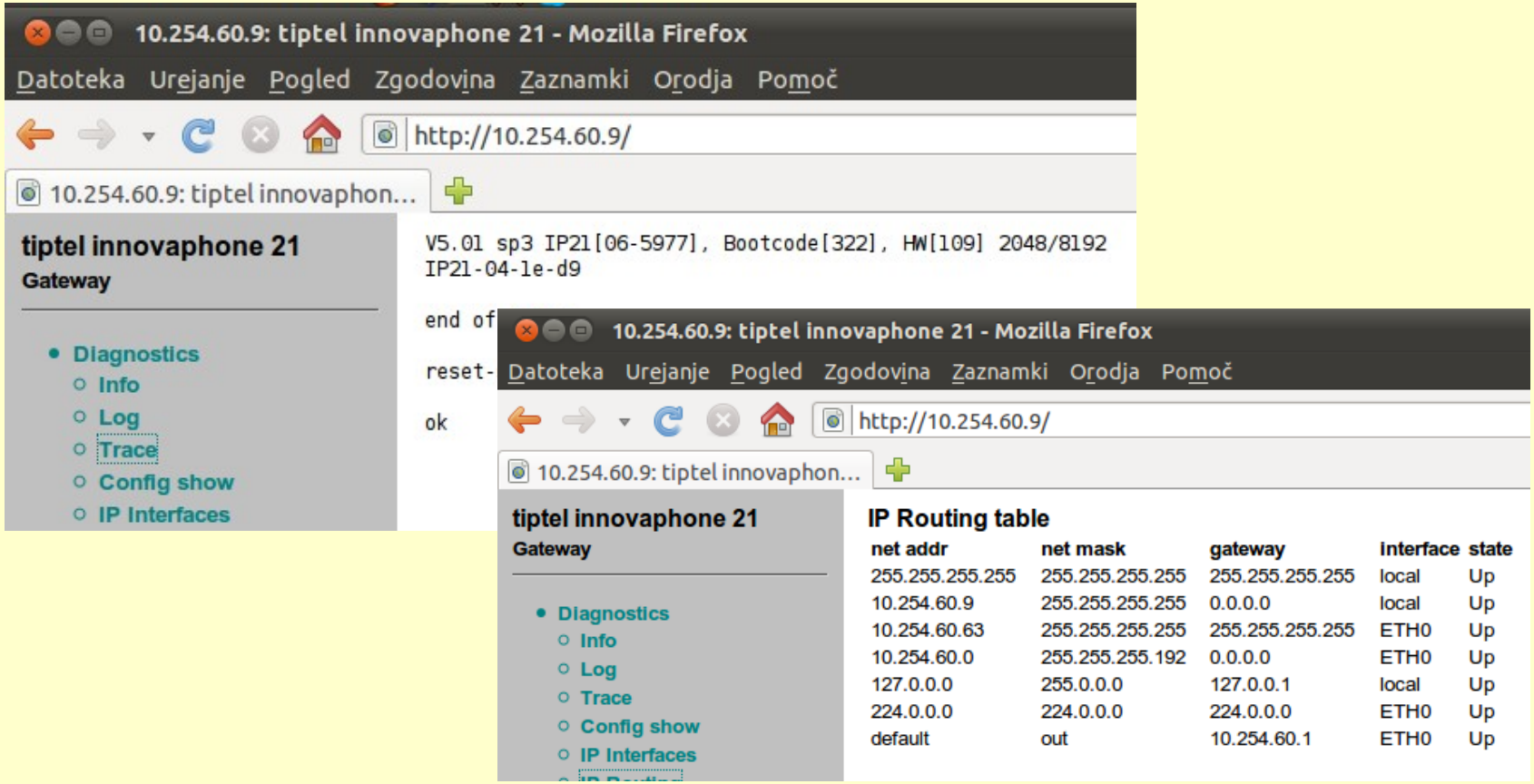
Google: “Tiptel Innovaphone 21”

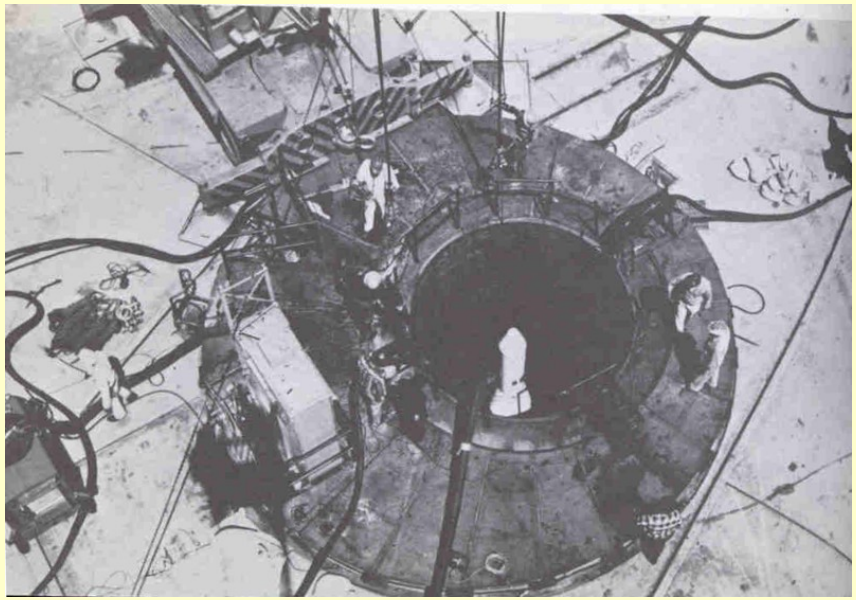




Infosmart	SOHO router		HTTP	admin	0
Innovaphone	IP20		Multi	admin	ipP20
Innovaphone	IP3000		Multi	admin	ip3000
Innovaphone	IP400		Multi	admin	ip400
Integral Technologies	RemoteView	4	Console	Administrator	letmein
Integrated Networks	IP Phone	IN1002	HTTP	Administrator	19750407

Uporaba privzetih gesel





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 OOOOOOOO.**

Bruce G. Blair. 2004. Keeping Presidents in the Nuclear Dark. <http://www.cdi.org/blair/permissive-action-links.cfm>

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.

https://sites.google.com/site/zeroforowned/dan-kaminsky-1

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

```
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
```

```
...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?

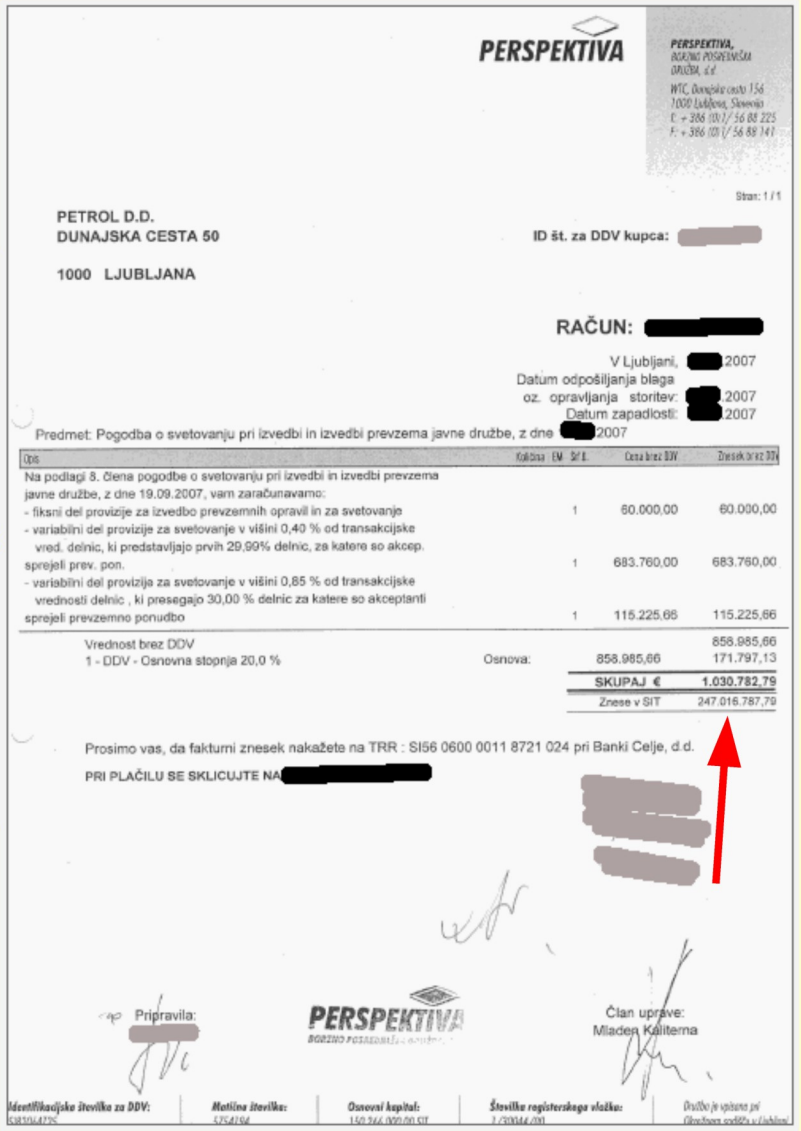
Zadeva: Remote Download server ;)
Od: [redacted]
Datum: 09. 07. 2007 01:52
Za: matej.kovacic@gmail.com

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

PETROL D.D.
DUNAJSKA CESTA 50
1000 LJUBLJANA

ID št. za DDV kupca: [redacted]

RAČUN: [redacted]

V Ljubljani, [redacted].2007
Datum odpošiljanja blaga
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	Količina	EM	Šif. E.	Cena brez DDV	Znesek brez DDV
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
1 - DDV - Osnovna stopnja 20,0 %			Osnova:	858.985,66	171.797,13
				SKUPAJ €	1.030.782,79
				Znese 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 SKLICUJTE NA [redacted]

Pripravila: [redacted]

PERSPEKTIVA

Član uprave:
Mladen Kaliterna

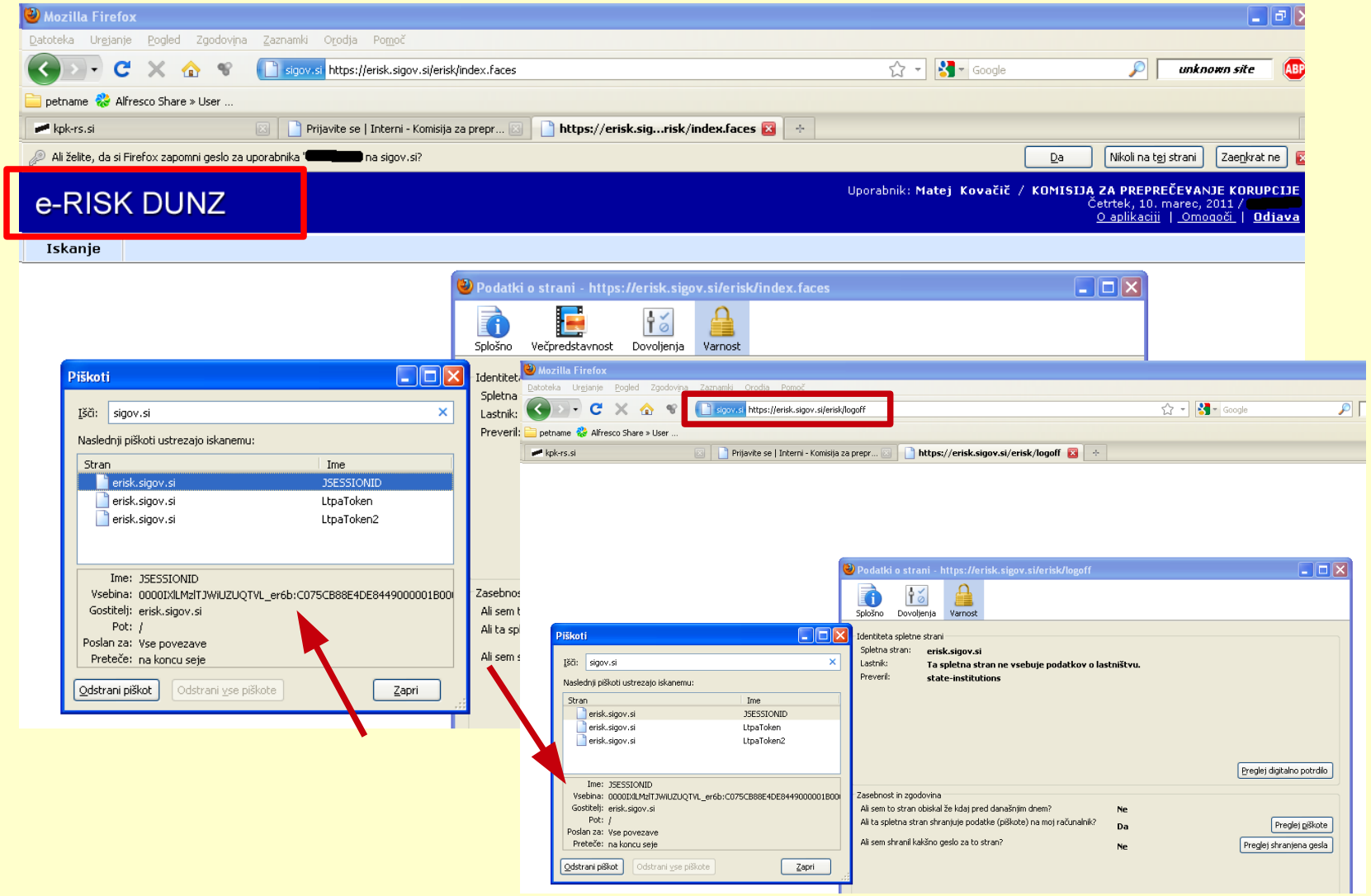
Primer sporočil prispelih na moj Gmail račun...

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.

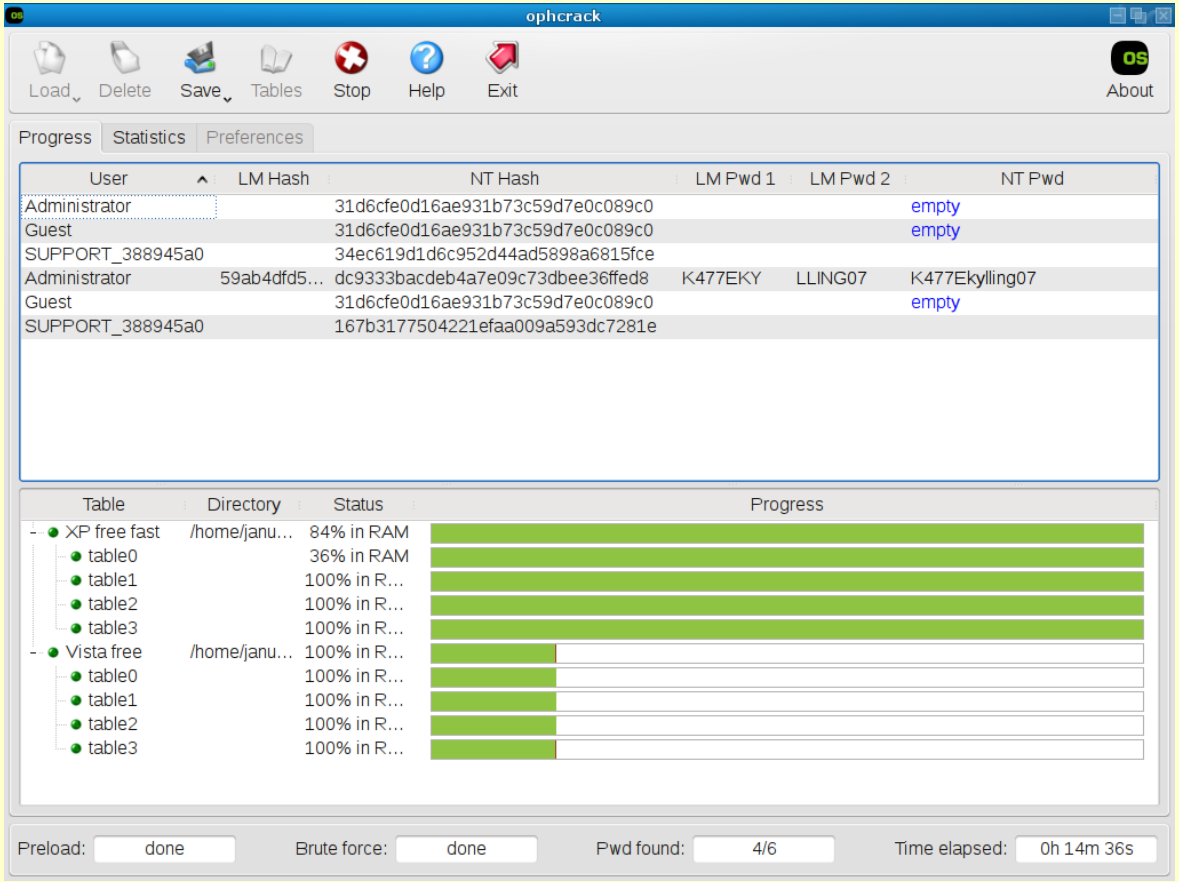
According to Assistant Chief Mike Allen, a fax was sent to the jail which stated "*Upon decision between Judge Rainey and the West Memphis Police Department CID Division Tristian Wilson is to be released immediately on this date of October 30, 2004 with a waiver of all fines, bonds and settlements per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

Vir: https://www.schneier.com/blog/archives/2004/11/hacking_faxes.html

Neustrezna avtentikacija



Razbijanje gesel



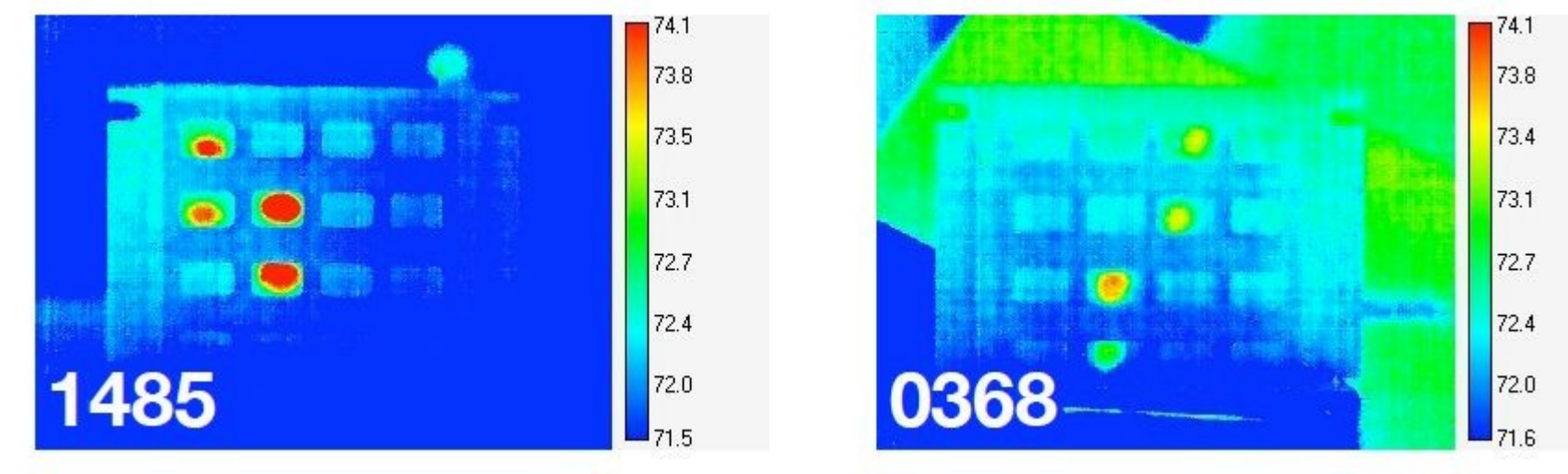
- Napad s slovarjem: seznami besed (“wordliste”).
- Mavrične tabele (MD5, LM, NTLM...).

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>.

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>.

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 laže prebrati s plastičnih, saj toploto odvajajo počasneje od kovinskih.

Napadi na strojno opremo

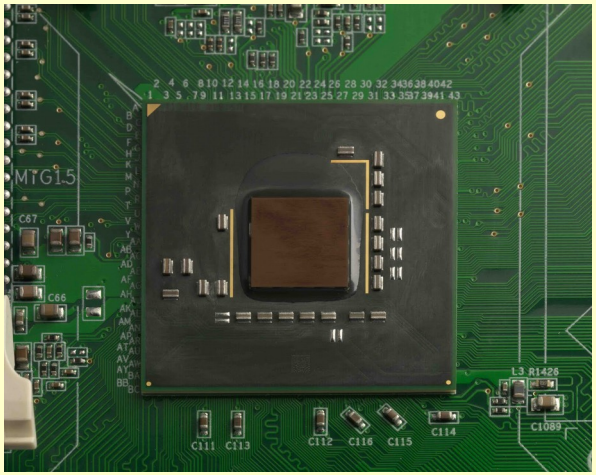
Napad na krmilnik trdega diska, mrežne kartice,...

```
Default
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:~$
```

```
ROXTerm
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.

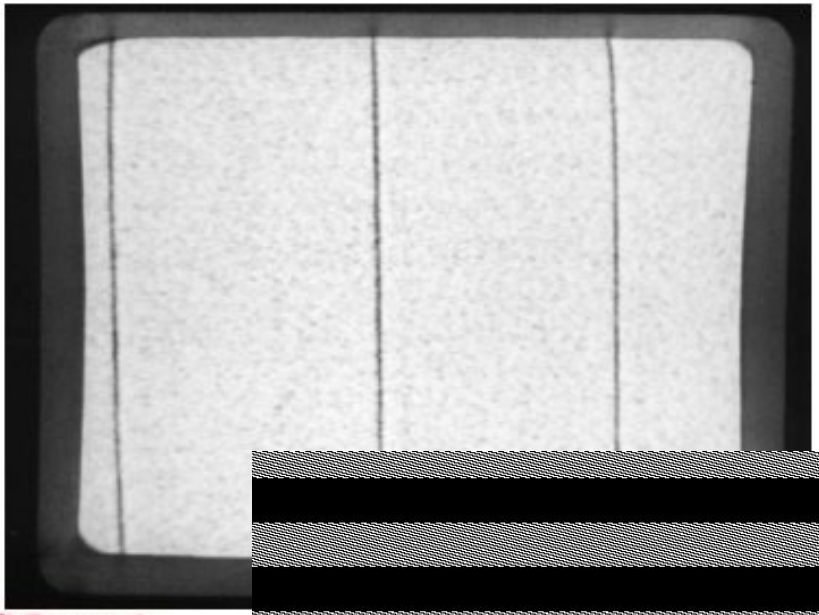


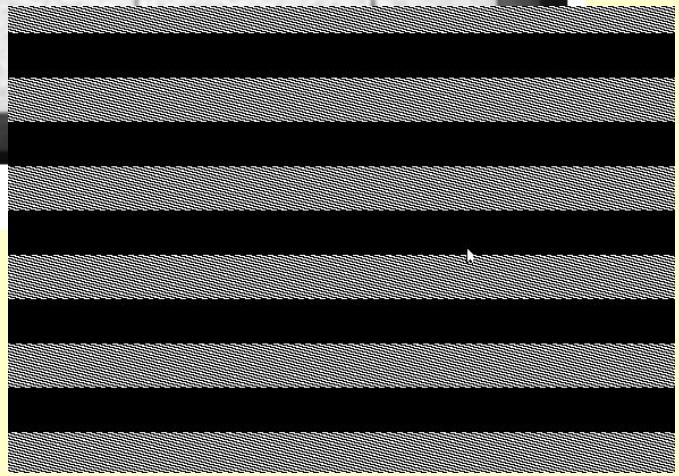
Slika Q35 čipa (MCH) v katerega so namestili korenski komplet. Več informacij: <https://slo-tech.com/novice/t369218>

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>, 2000.
- **Hit by a Bus: Physical Access Attacks with Firewire**, <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>, 2006.

Tempest napad

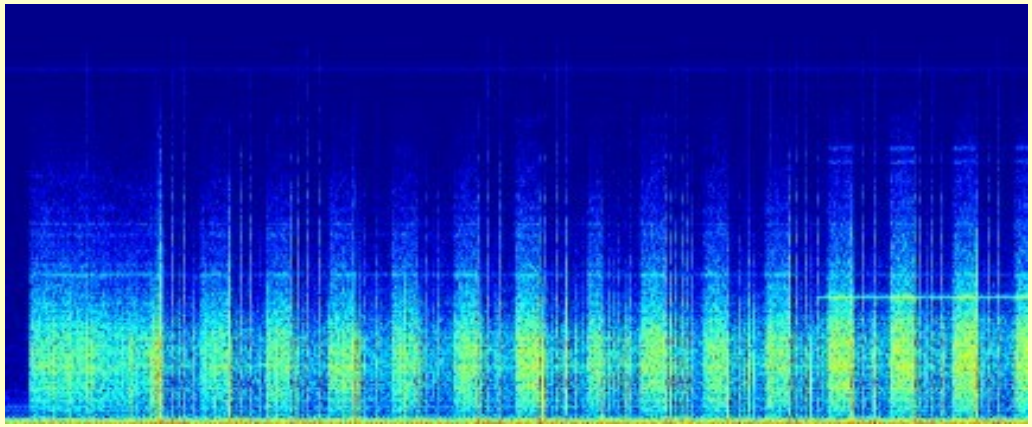




Vir: prosojnice Markusa G. Kuhna in Rossa J. Andersona "Soft Tempest: Hidden Data Transmission Using Elecromagnetic Emanations"

Tempest napad

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



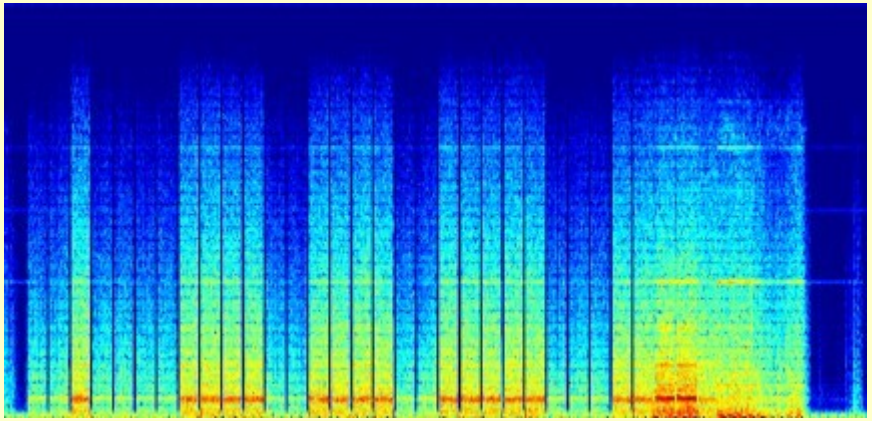
- Sonogram elekgromagnetnih signalov ob pisanju na trdi disk. Avtor je na podlagi spremljanja elektromagnetnih signalov lahko rekonstruiral kdaj se zapisujejo enke in kdaj ničle. Vir in avtorstvo: Oğuz Berke Durak, Hidden Data Transmission by Controlling Electromagnetic Emanations of Computers, <http://abaababa.ouvaton.org/tempest/>.

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

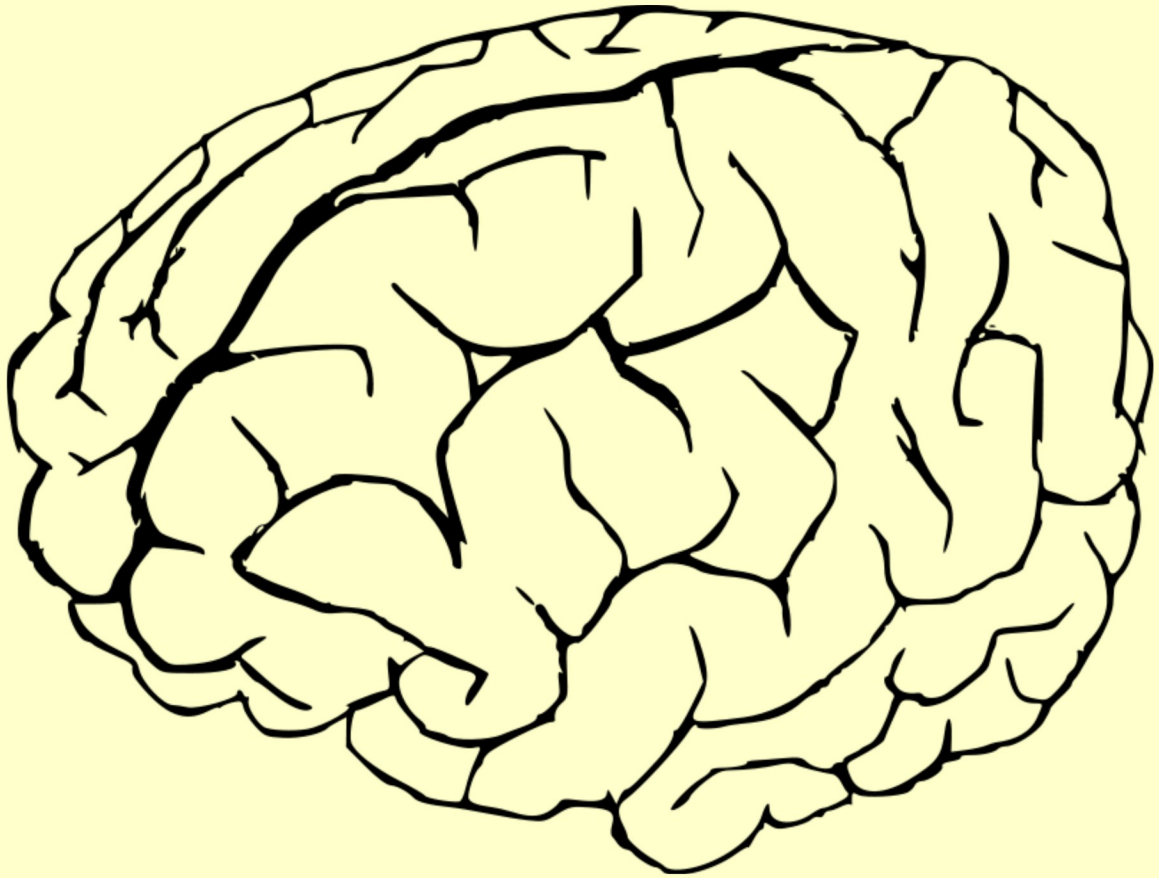
- **Nekatere tehnike osnovne zaščite računalniških sistemov**:
  - uporaba ustreznih gesel;
  - pazljivost pri večuporabniških sistemih;
  - redno posodobljen sistem;
  - požarni zid;
  - uporaba protivirusnih in protismetnih (antispyware) programov;
  - ustrezna varnostna kultura;
  - fizična varnost;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

Naprednejša zaščita

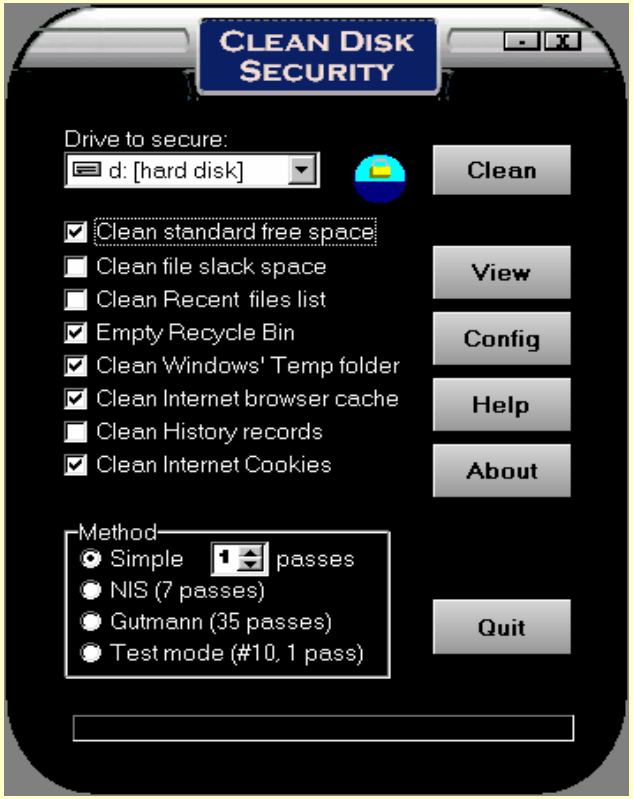
- **Nekatere tehnike naprednejše zaščite**:
  - varno brisanje podatkov;
  - šifriranje:
    - šifriranje razdelkov trdih diskov kjer so shranjeni občutljivi podatki (tudi začasnega "swap" pomnilnika);
    - šifriranje elektronske pošte;
  - anonimizacija uporabe interneta (preprečimo analizo prometnih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

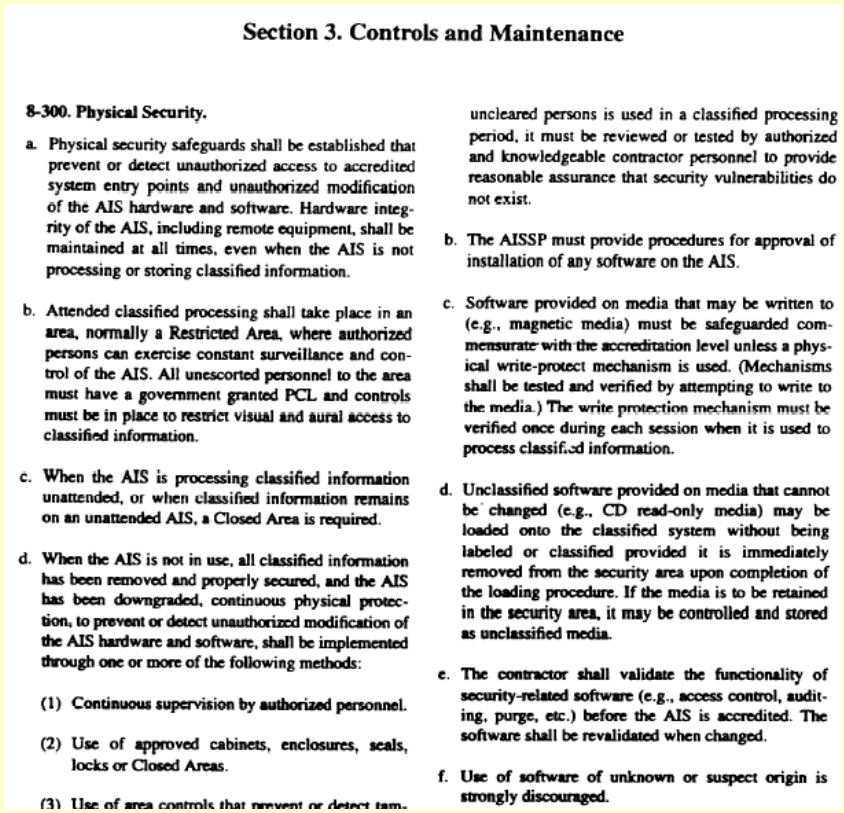
Še bolj napredna zaščita

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



Trajno brisanje podatkov





Section 3. Controls and Maintenance

8-300. Physical Security.

a. Physical security safeguards shall be established that prevent or detect unauthorized access to accredited system entry points and unauthorized modification of the AIS hardware and software. Hardware integrity of the AIS, including remote equipment, shall be maintained at all times, even when the AIS is not processing or storing classified information.

b. Attended classified processing shall take place in an area, normally a Restricted Area, where authorized persons can exercise constant surveillance and control of the AIS. All unescorted personnel to the area must have a government granted PCL and controls must be in place to restrict visual and aural access to classified information.

c. When the AIS is processing classified information unattended, or when classified information remains on an unattended AIS, a Closed Area is required.

d. When the AIS is not in use, all classified information has been removed and properly secured, and the AIS has been downgraded, continuous physical protection, to prevent or detect unauthorized modification of the AIS hardware and software, shall be implemented through one or more of the following methods:

(1) Continuous supervision by authorized personnel.

(2) Use of approved cabinets, enclosures, seals, locks or Closed Areas.

(3) Use of area controls that prevent or detect tam-

uncleared persons is used in a classified processing period, it must be reviewed or tested by authorized and knowledgeable contractor personnel to provide reasonable assurance that security vulnerabilities do not exist.

b. The AISSP must provide procedures for approval of installation of any software on the AIS.

c. Software provided on media that may be written to (e.g., magnetic media) must be safeguarded commensurate with the accreditation level unless a physical write-protect mechanism is used. (Mechanisms shall be tested and verified by attempting to write to the media.) The write protection mechanism must be verified once during each session when it is used to process classified information.

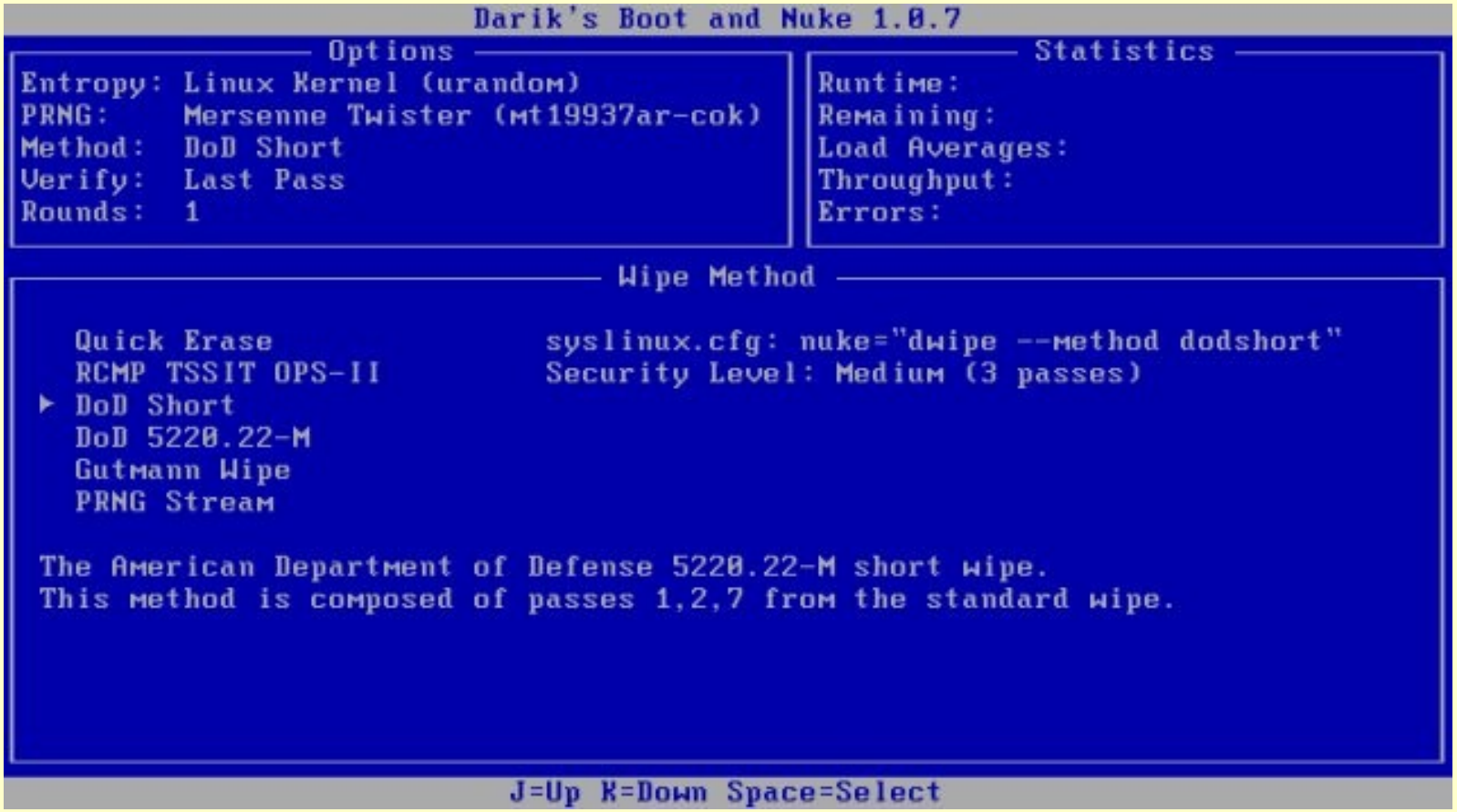
d. Unclassified software provided on media that cannot be changed (e.g., CD read-only media) may be loaded onto the classified system without being labeled or classified provided it is immediately removed from the security area upon completion of the loading procedure. If the media is to be retained in the security area, it may be controlled and stored as unclassified media.

e. The contractor shall validate the functionality of security-related software (e.g., access control, auditing, purge, etc.) before the AIS is accredited. The software shall be revalidated when changed.

f. Use of software of unknown or suspect origin is strongly discouraged.

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

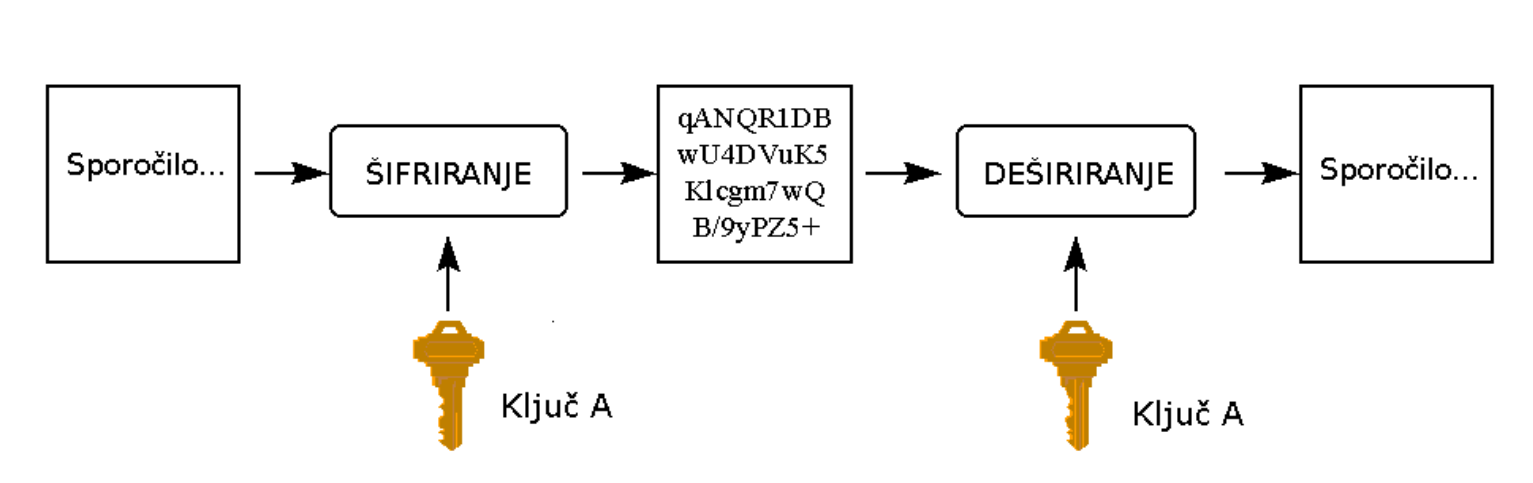


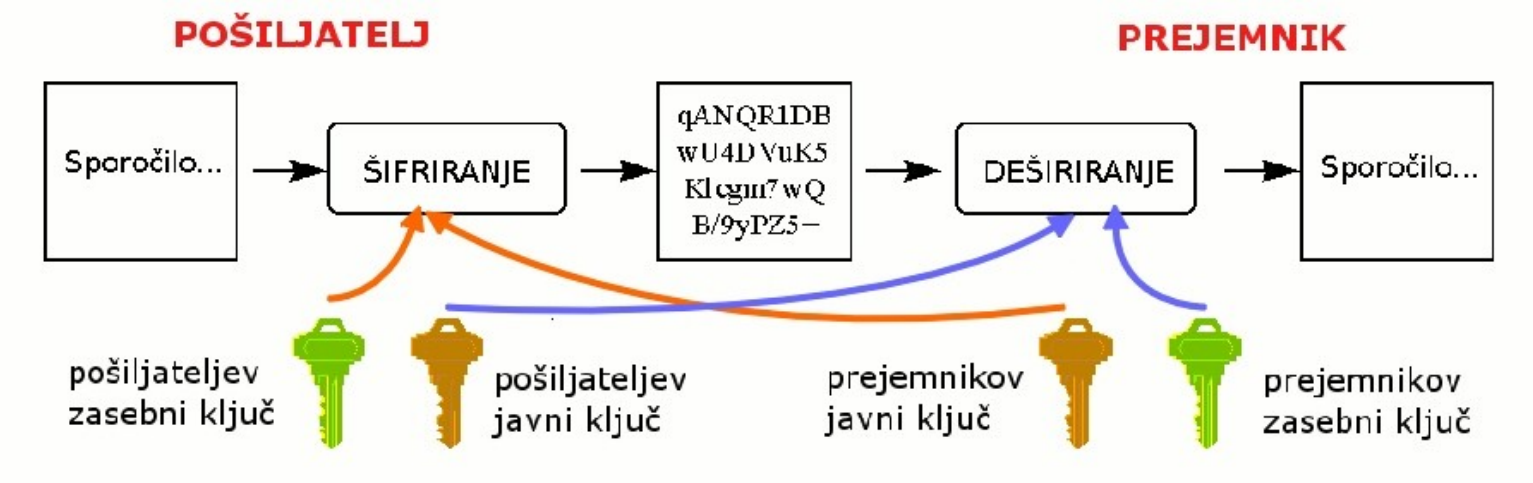
DBAN - Darik's Boot and Nuke, orodje namenjeno uničevanju vsebine trdih diskov. Zažene se iz zagonske diskete. < http://dban.sourceforge.net/>. Vir in avtorstvo: dokumentacija programa.

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

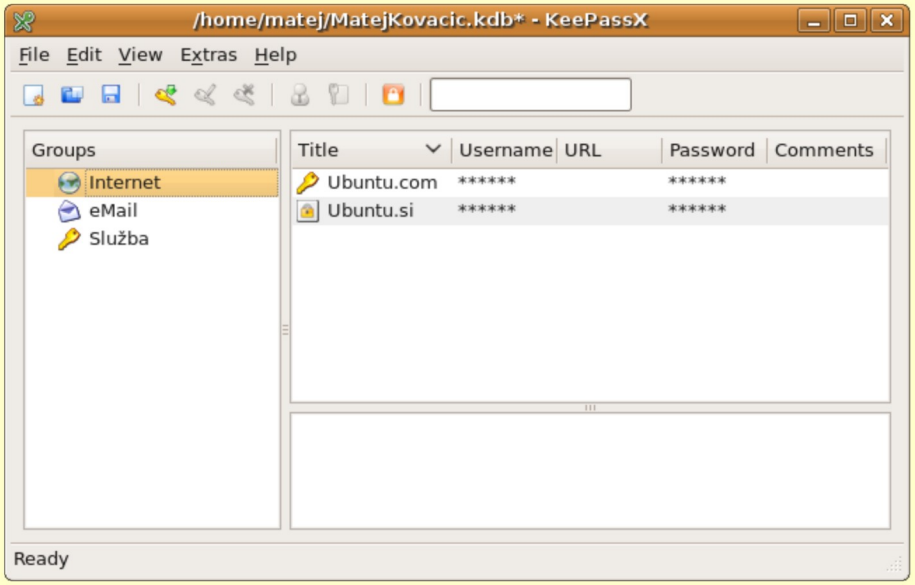




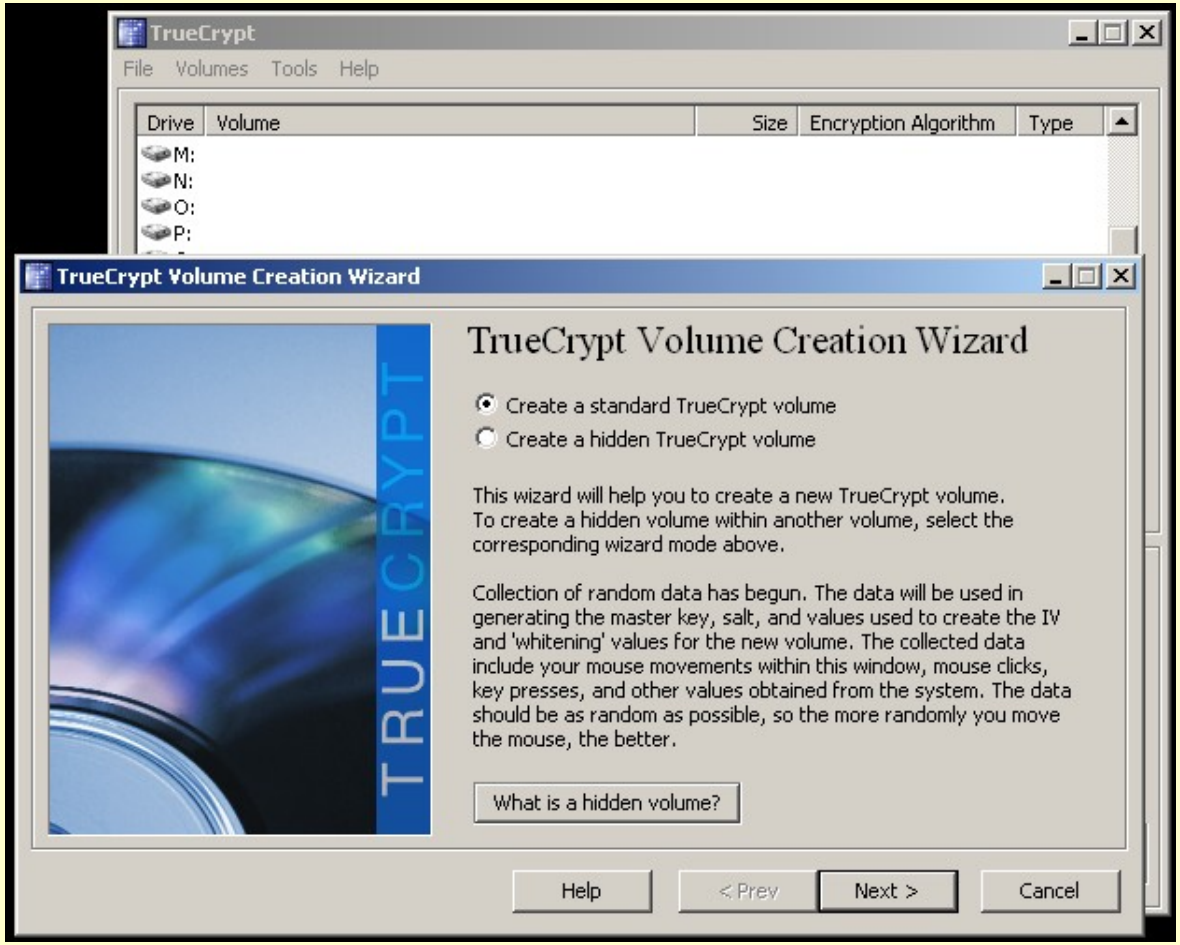
Shematski prikaz simetrične kriptografije in kriptografije z javnimi ključi.

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



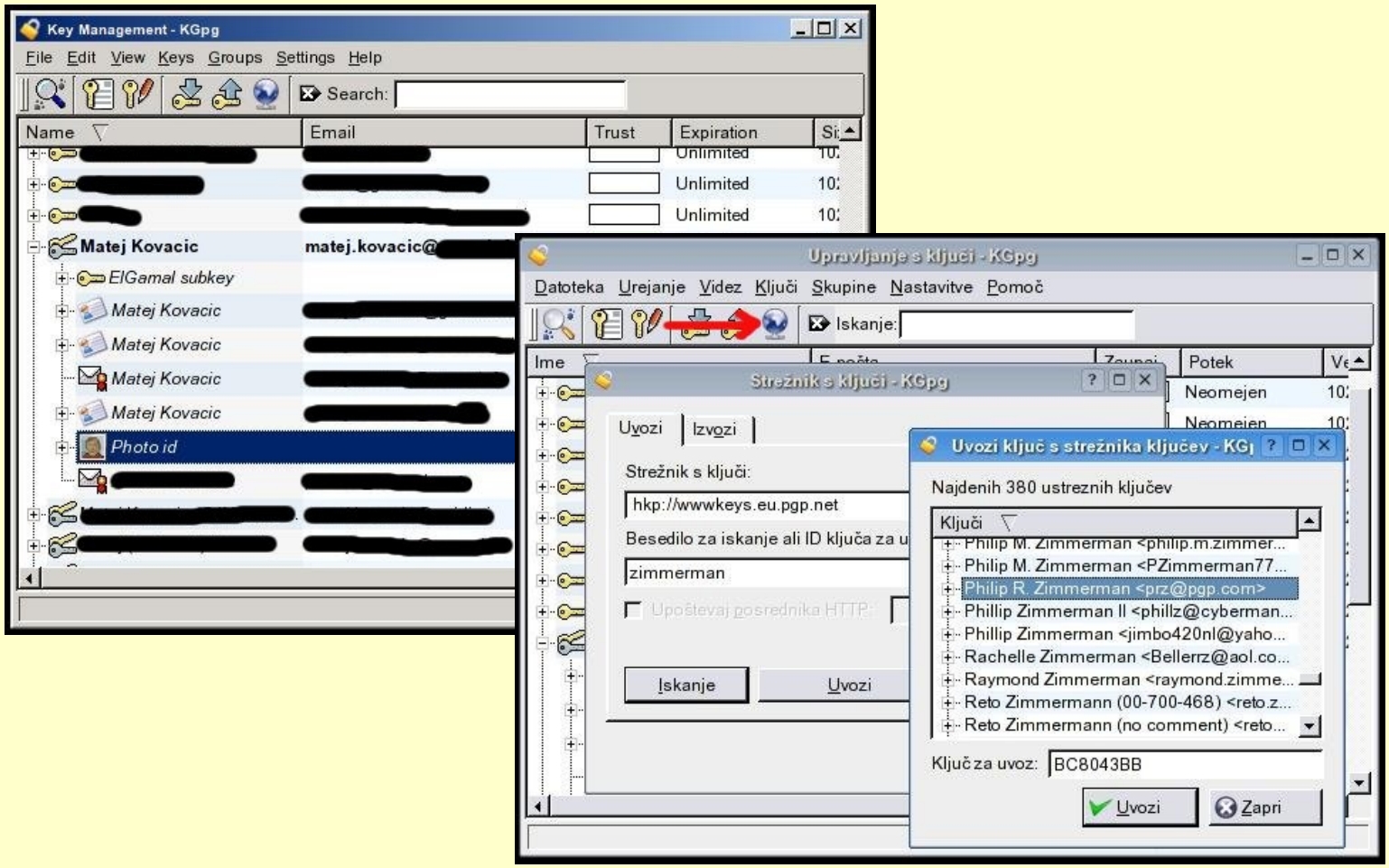
Šifriranje (navideznih) diskovnih particij s programom *TrueCrypt*.
Program omogoča tudi skrite šifrirane particije.

Šifrirni kontejner v LUKS formatu

Omogoča tudi menjavo gesel:

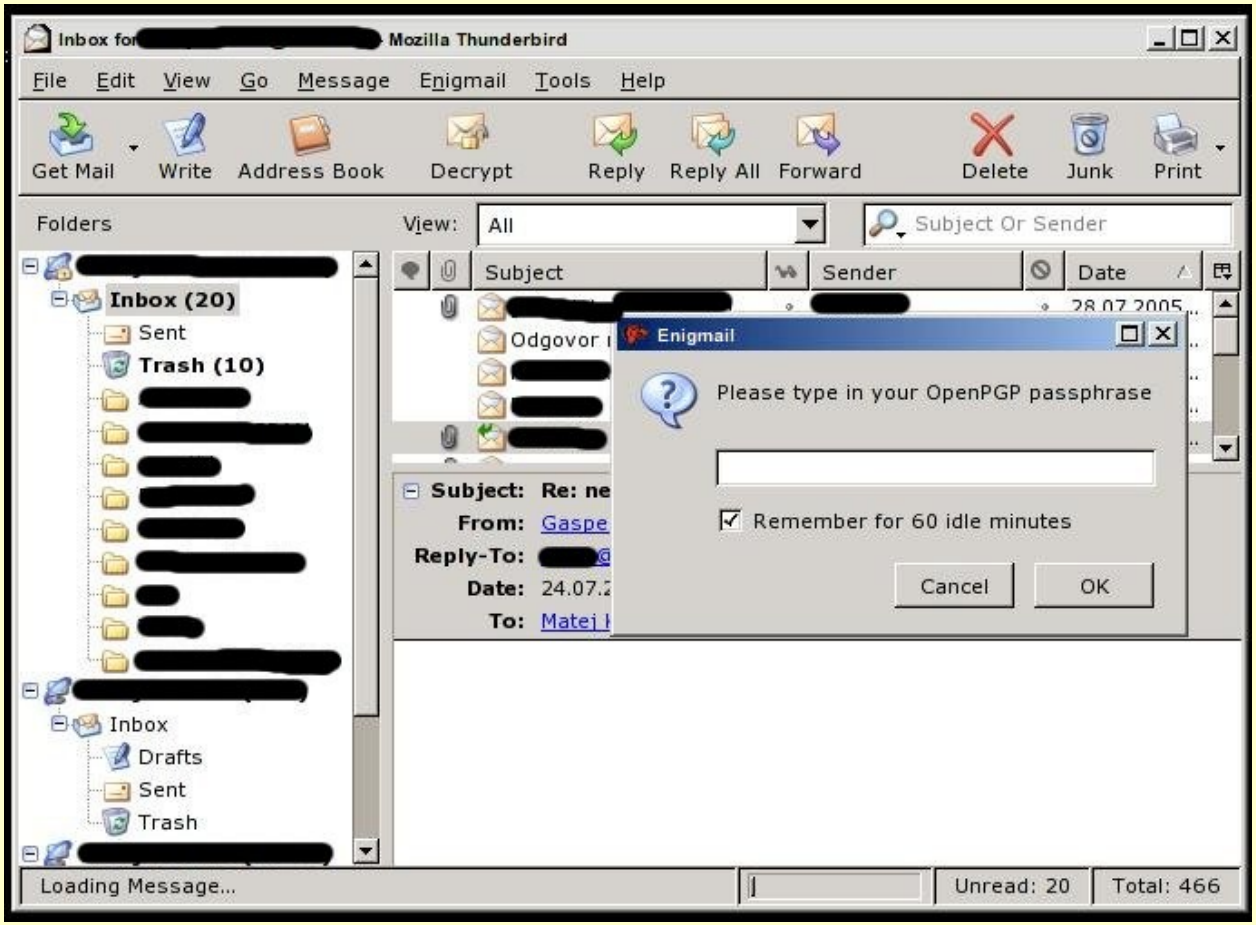
- dodamo novo geslo
- odstranimo starega.

Šifriranje e-pošte



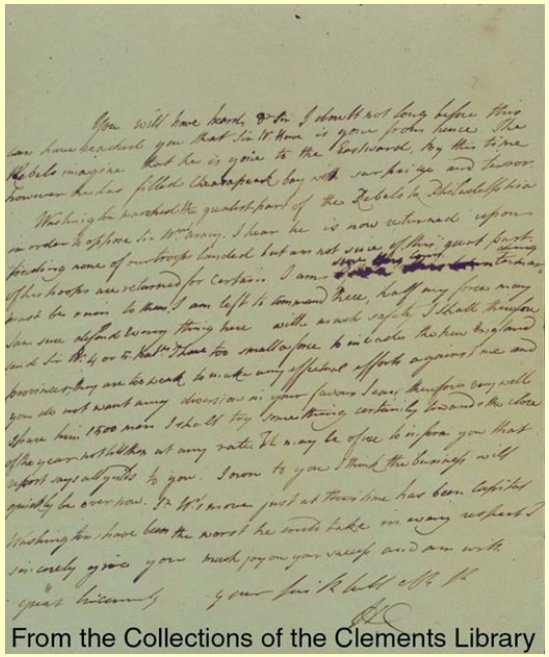
Šifrirni program *GPG* (*GNU Privacy Guard*) - upravljanje s šifrirnimi ključi v okolju Linux.

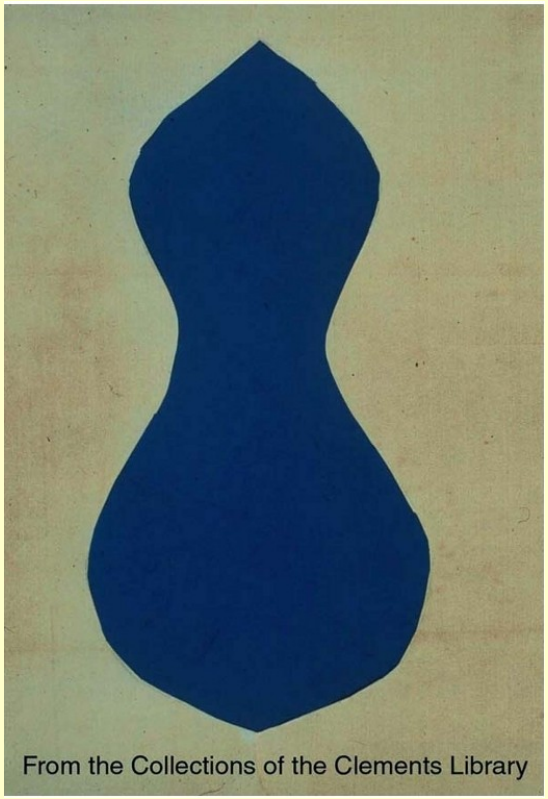
Šifriranje e-pošte

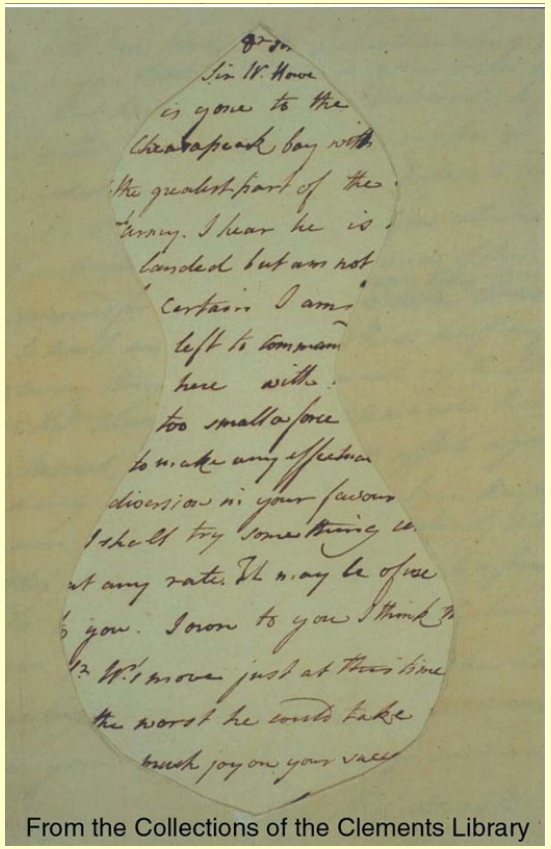


Šifriranje elektronske pošte v odprtokodnem odjemalcu elektronske pošte *Mozilla Thunderbird* z dodatkom *Enigmail*.

Skrivanje podatkov

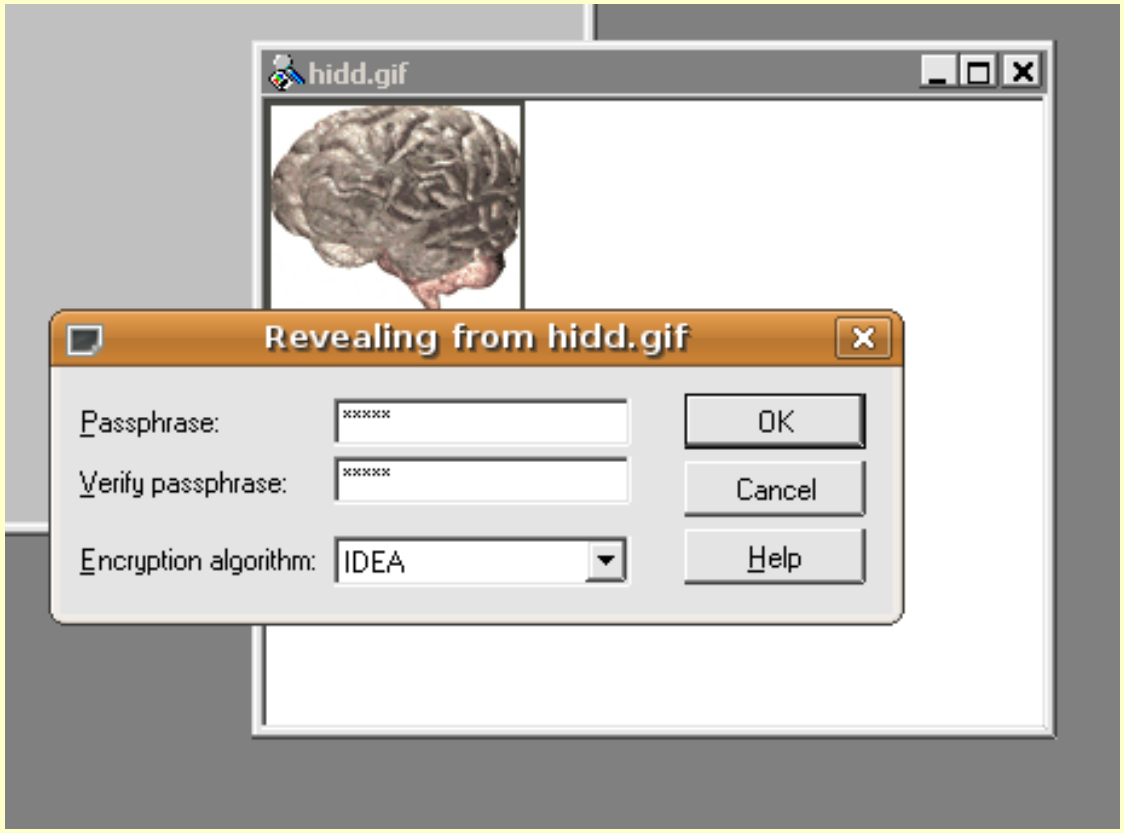

From the Collections of the Clements Library


From the Collections of the Clements Library


From the Collections of the Clements Library

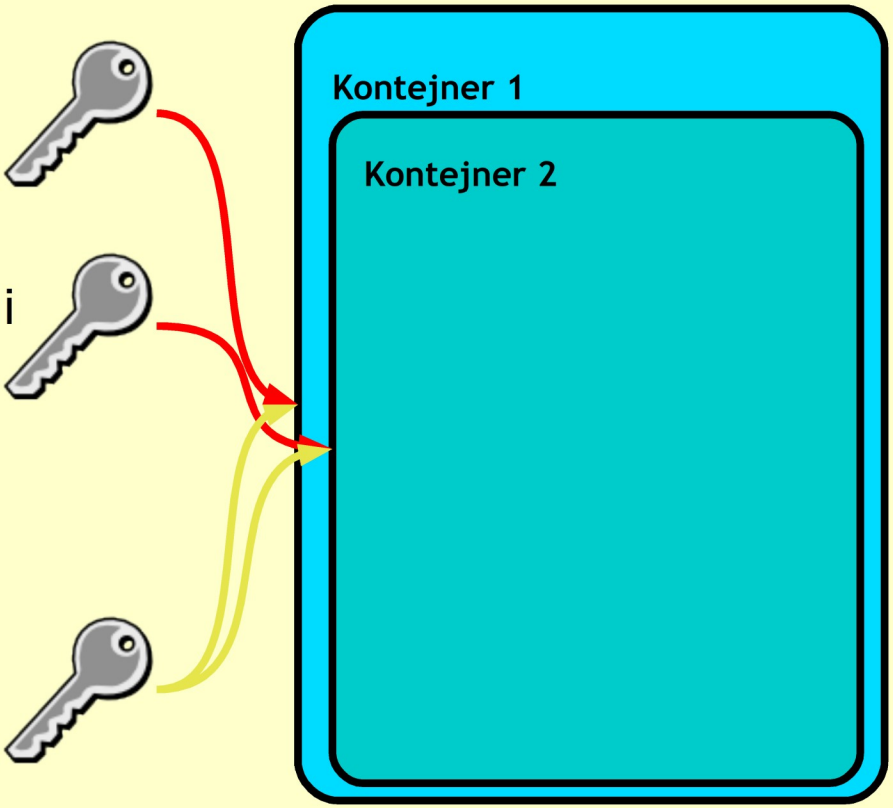
Maskirano pismo: 10. avgust 1777, Henry Clinton -> John Burgoyne.
http://www.si.umich.edu/spies/letter-1777august10-1.html

S-Tools

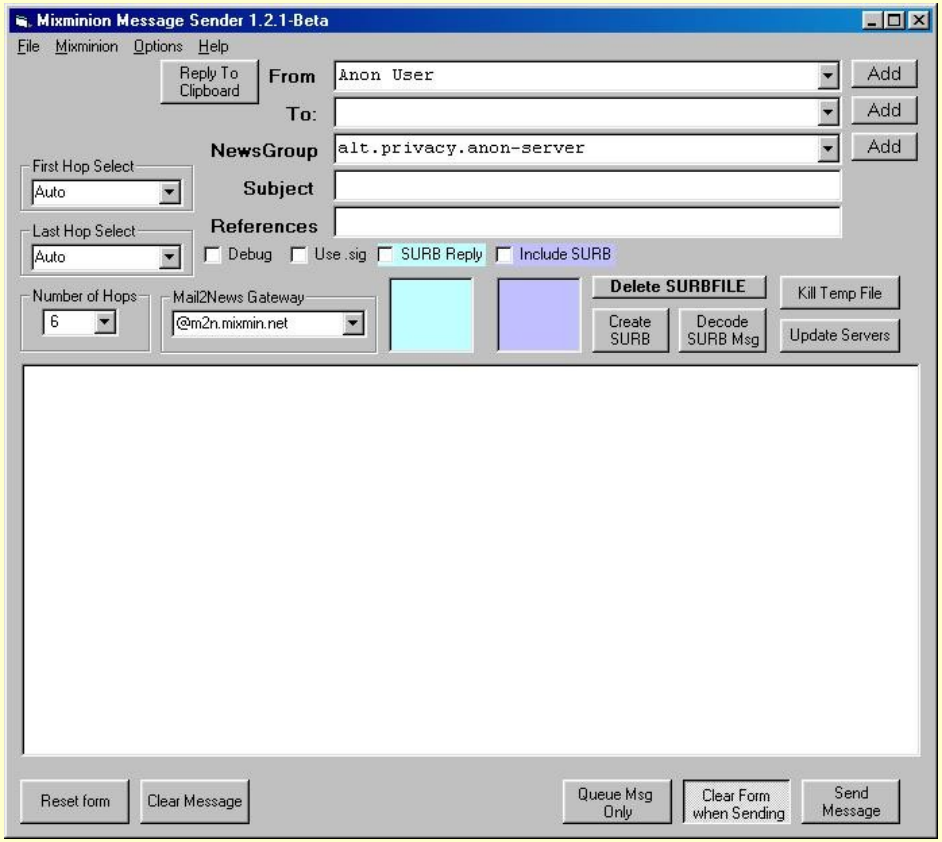

hidd.gif
Revealing from hidd.gif
Passphrase:
*****
Verify passphrase:
*****
Encryption algorithm:
IDEA
OK
Cancel
Help

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.

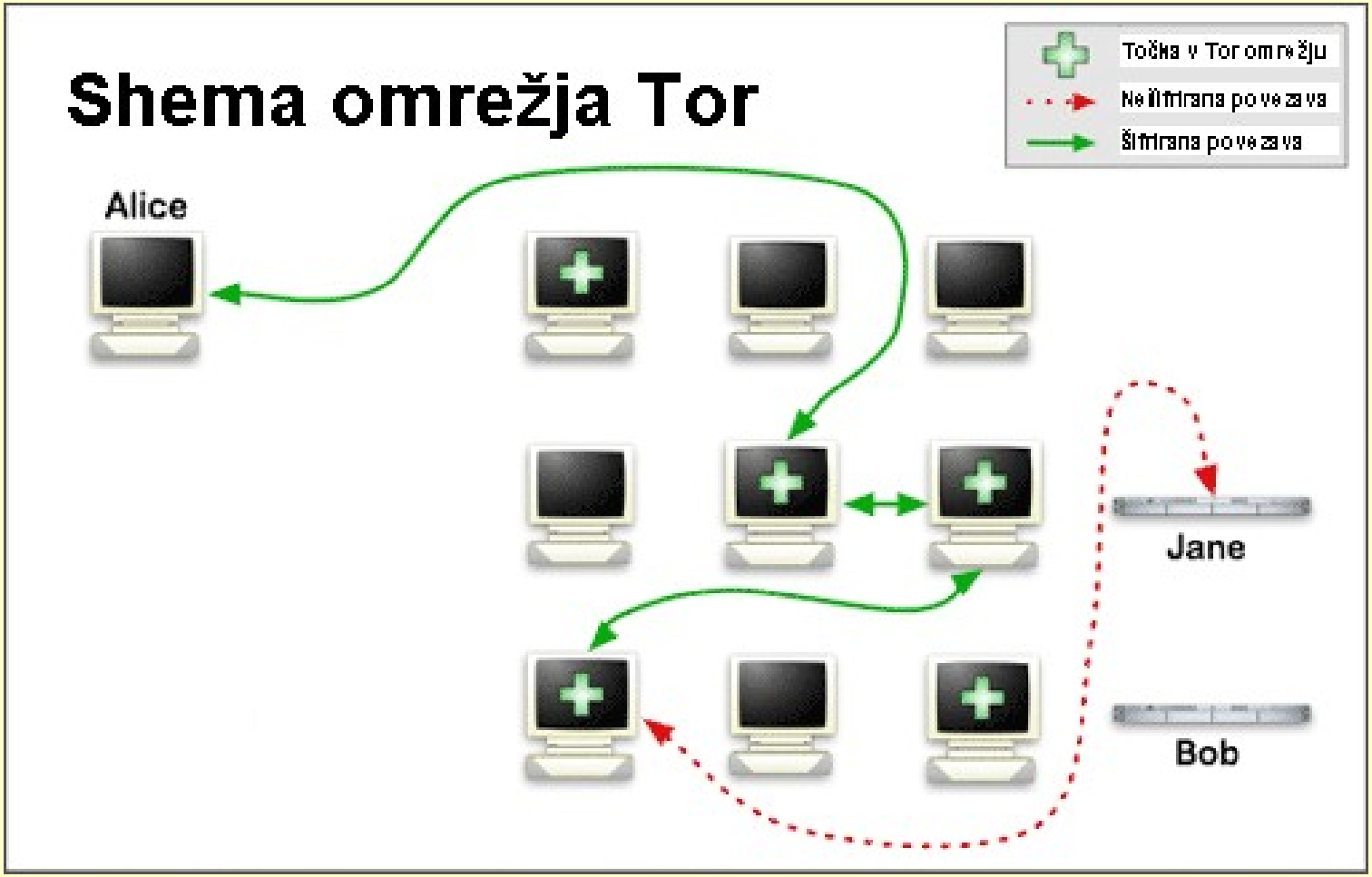


Anonimno pošiljanje e-pošte



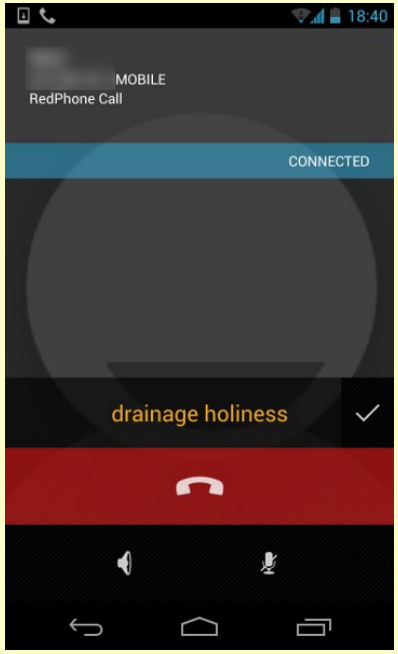
Pošiljanje elektronske pošte preko s pomočjo "remailer-ja" *Mixminion*. Uporaba programa omogoča tudi anonimno odgovarjanje na anonimna sporočila. Sporočila potujejo čez več anonimizacijskih strežnikov (tim. *mixi*) v šifrirani obliki.

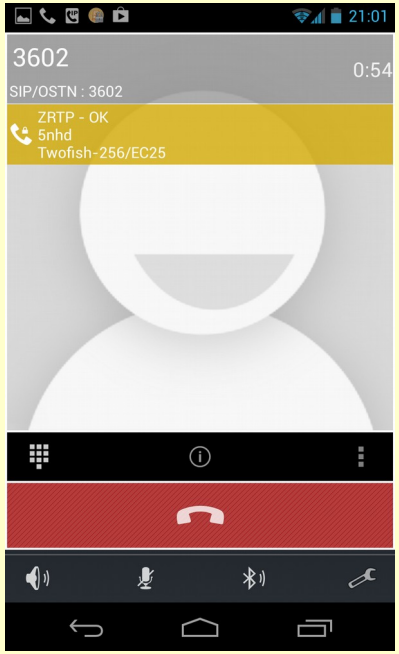
Anonimizacijsko omrežje Tor

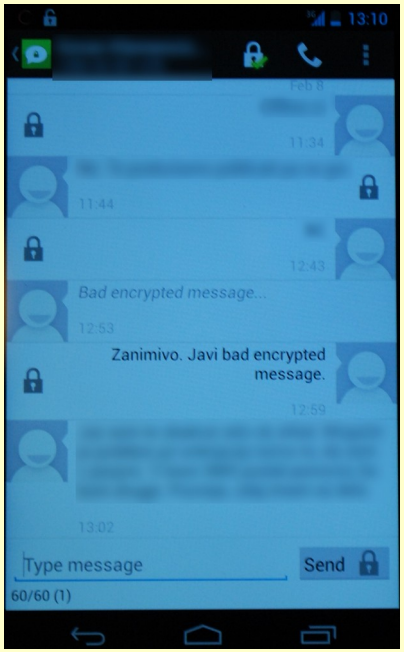


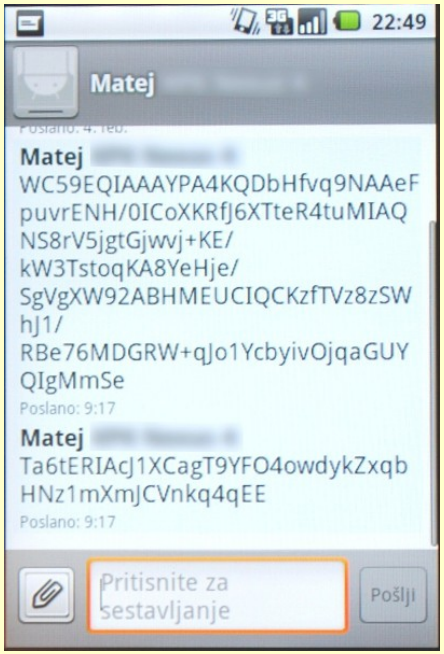
Prikaz delovanja anonimizacijskega omrežja *Tor*.

Varnost mobilne telefonije









Vprašanja?