# Varnost informacijskih sistemov



Matej Kovačič
https://telefoncek.si

# 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.

# Napadi na informacijske sisteme...

**...in ljudi!**

Napadi, ki zahtevajo fizični dostop do sistema.

Omrežni napadi (napadi na komunikacije ter napadi na »virtualni prostor«).

Zbiranje različnih (javno objavljenih) informacij na internetu.

Posredni napadi - napadi na uporabnika (socialni inženiring, prevare).

# Kiberkriminal

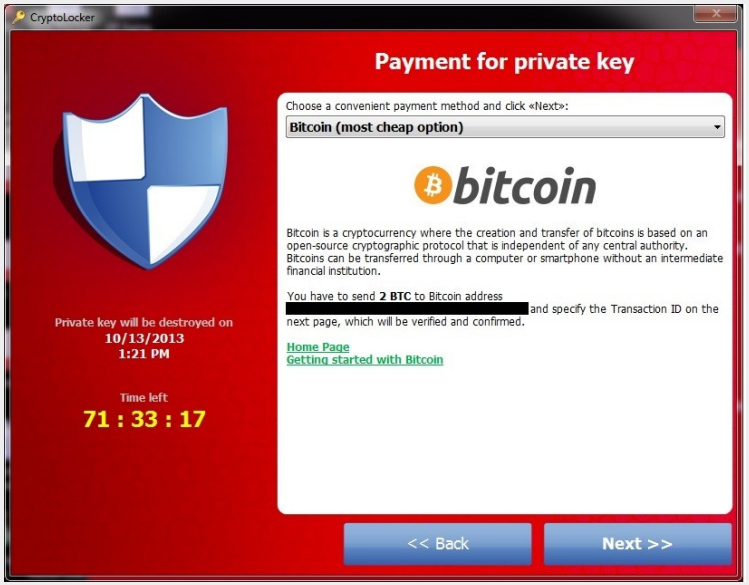
Včasih:

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

# Kiberkriminal

Danes:

- posel in denar!




Šifrirno-izsiljevalski virus Cryptolocker.


Spletna stran "podjetja".

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

# »Etično hekanje«

Informacijski sistemi kot organizmi z imunskimi sistemi.

Odkrivanje varnostnih ranljivosti ima za posledico njihovo odpravo ter povišano varnostno kulturo uporabnikov.

Etično hekanje krepi »imunski sistem« interneta in zmanjšuje verjetnost, da bi nekoč prišlo do katastrofalnega napada.

# Fizični dostop do sistema

Nepooblaščeni dostop do podatkov.

Podtikanje prikritih mehanizmov za oddaljeni dostop ali krajo šifriranih podatkov (npr. programske aplikacije ali strojni dodatki).

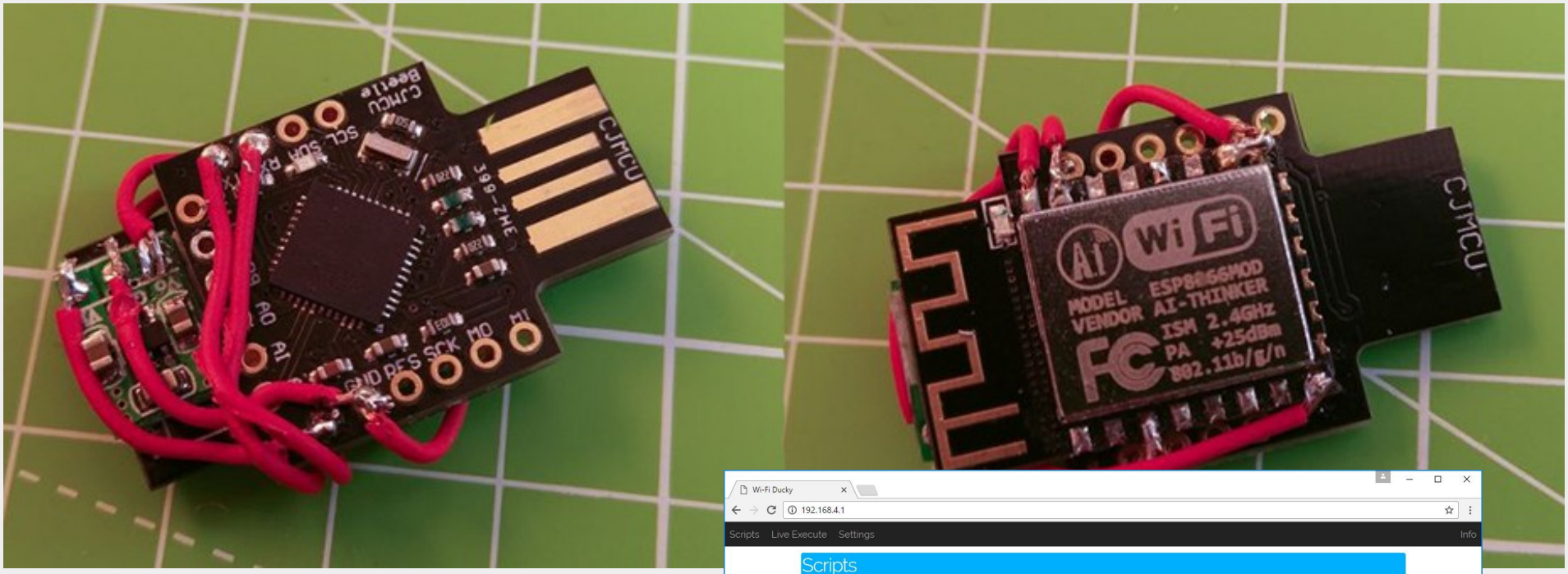
Zavržene računalniške komponente, ki vsebujejo nosilce podatkov (trdi diski, tiskalniki, mobilni telefoni,...).

Nameščanje aplikacij z »dvojno funkcijo«.

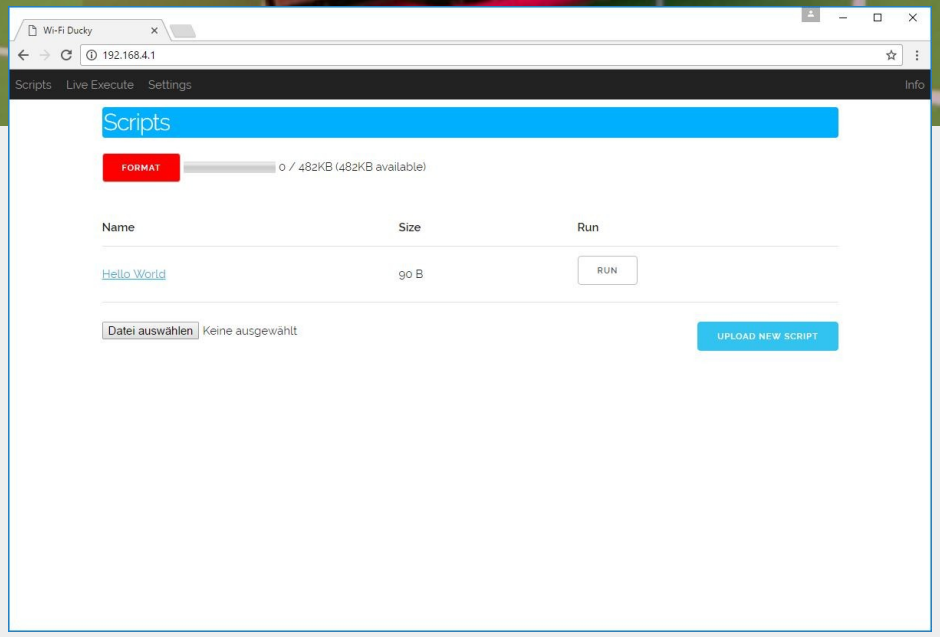
Priklapljanje neznanih naprav na sistem (najdeni USB ključki, »polnjenje« mobilnih telefonov,...)

Večuporabniška okolja (eskalacija privilegijev).

# Navarni USB ključki



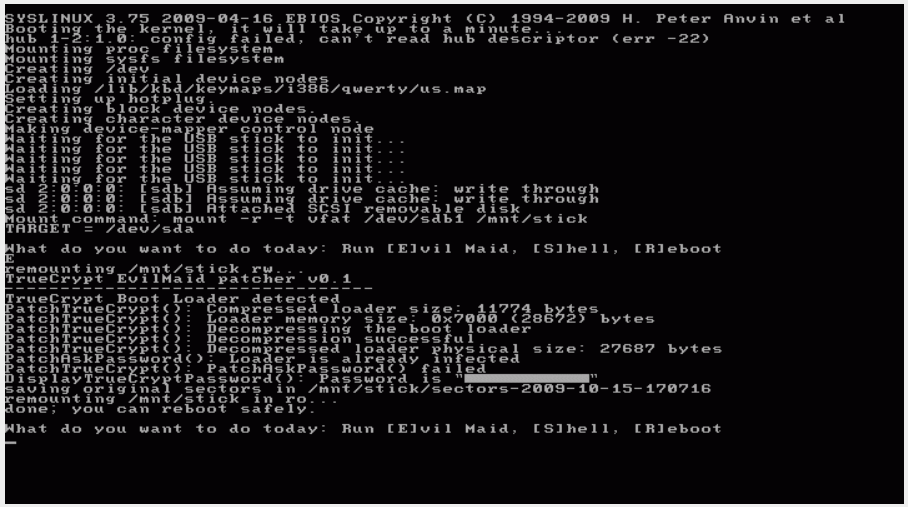

BadUSB z Wi-Fi podporo.




Upravljanje preko Wi-Fi.

# Podtikanje prikritih mehanizmov


Programski prestrezniki tipkanja.

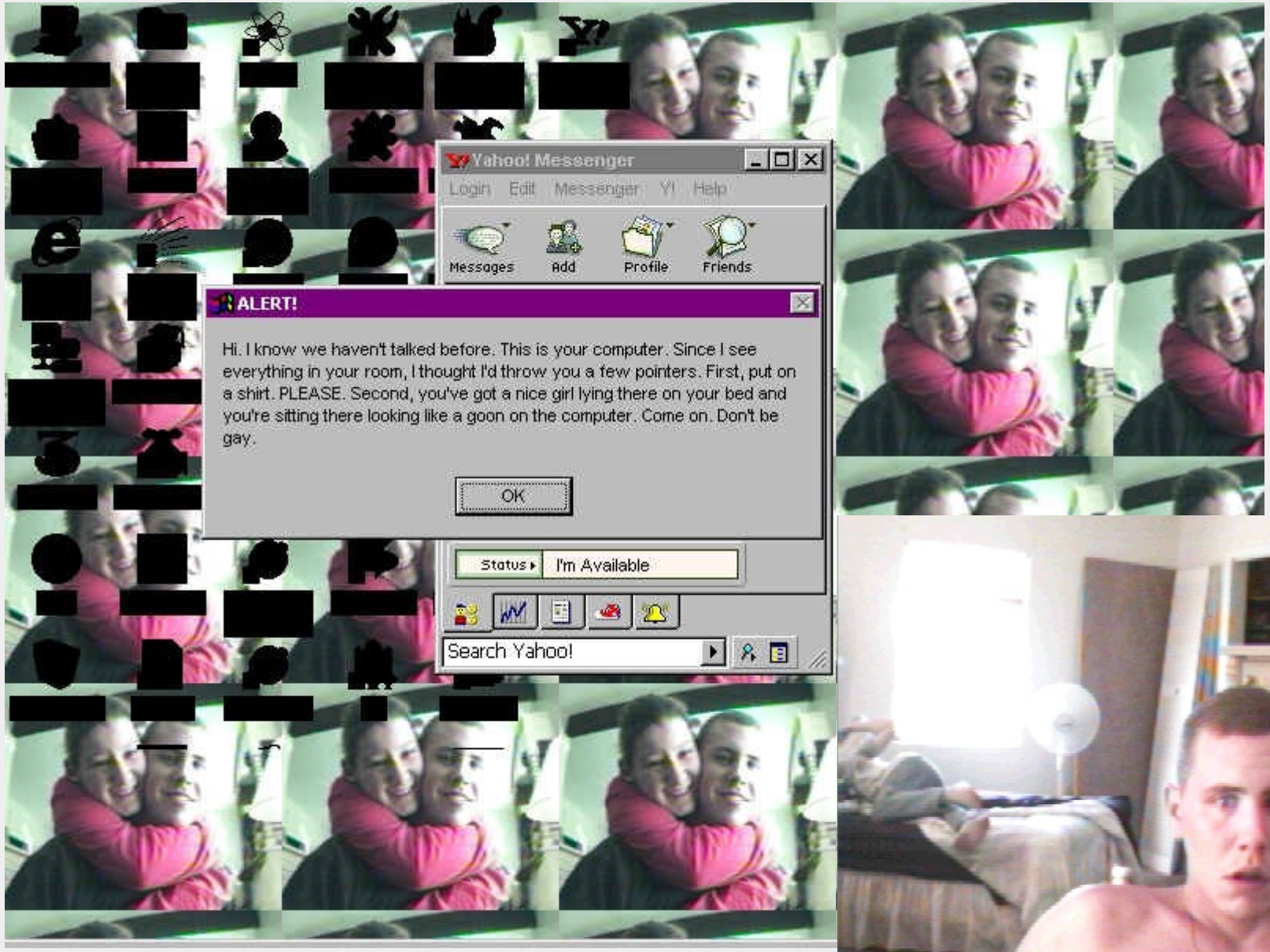



Evil Maid napad na TrueCrypt in...

Strojni prestrezniki tipkanja.


...ostanki sirskega jedrskega reaktorja al-Kibar.

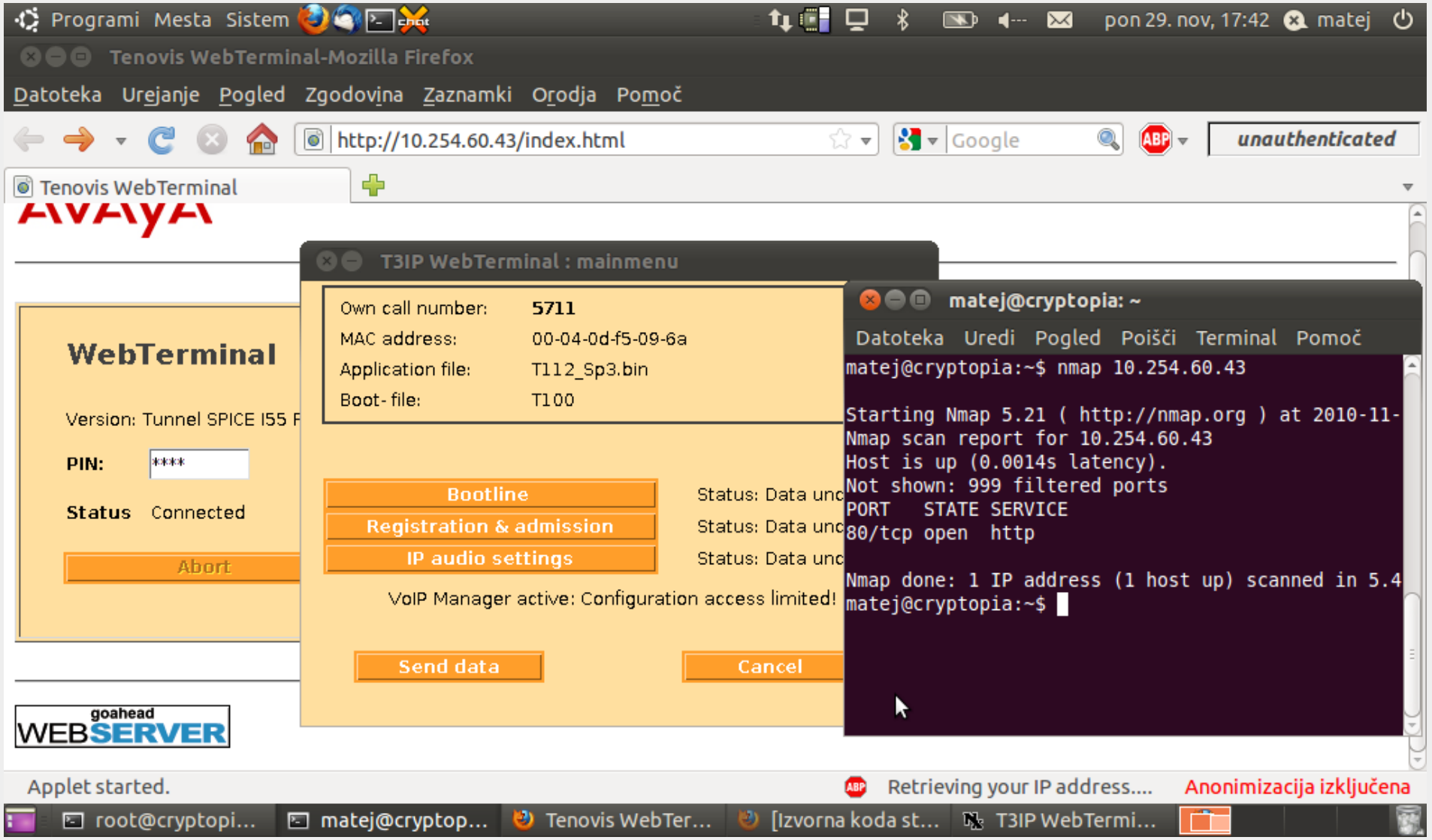
# Posledice...


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!

# Ranljivi niso samo računalniki...

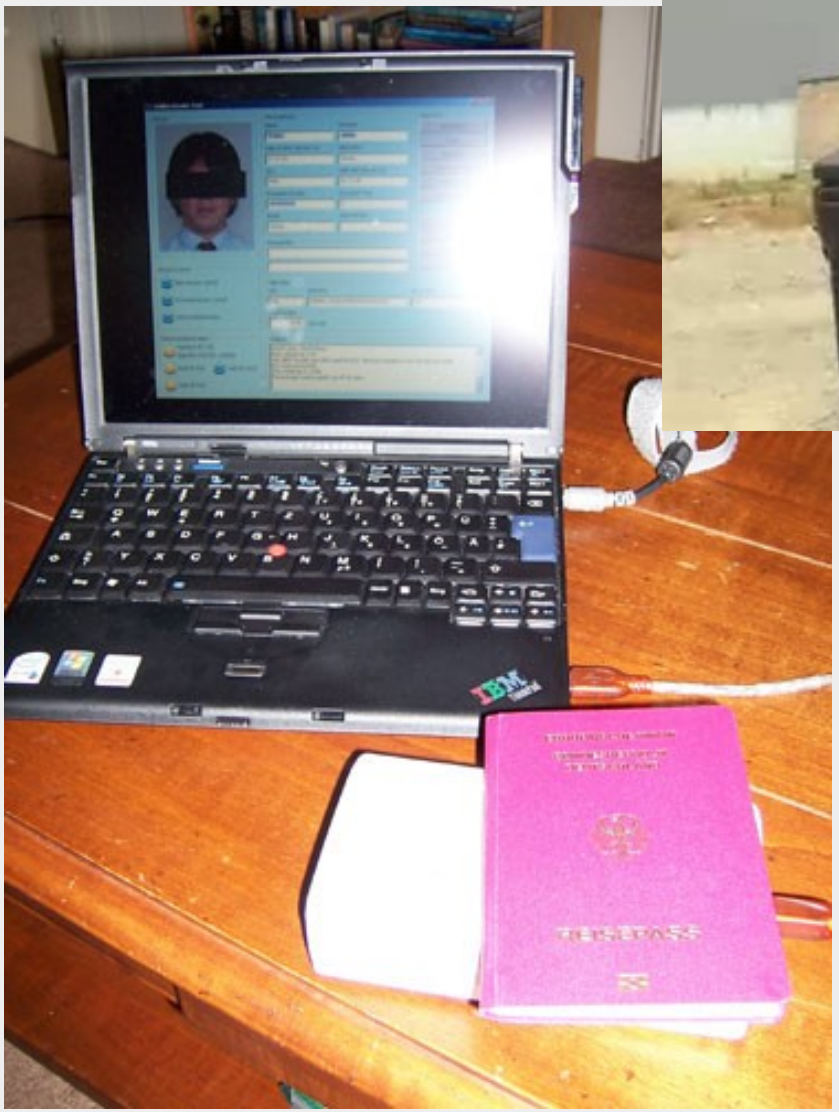



# Ranljivi niso samo računalniki...

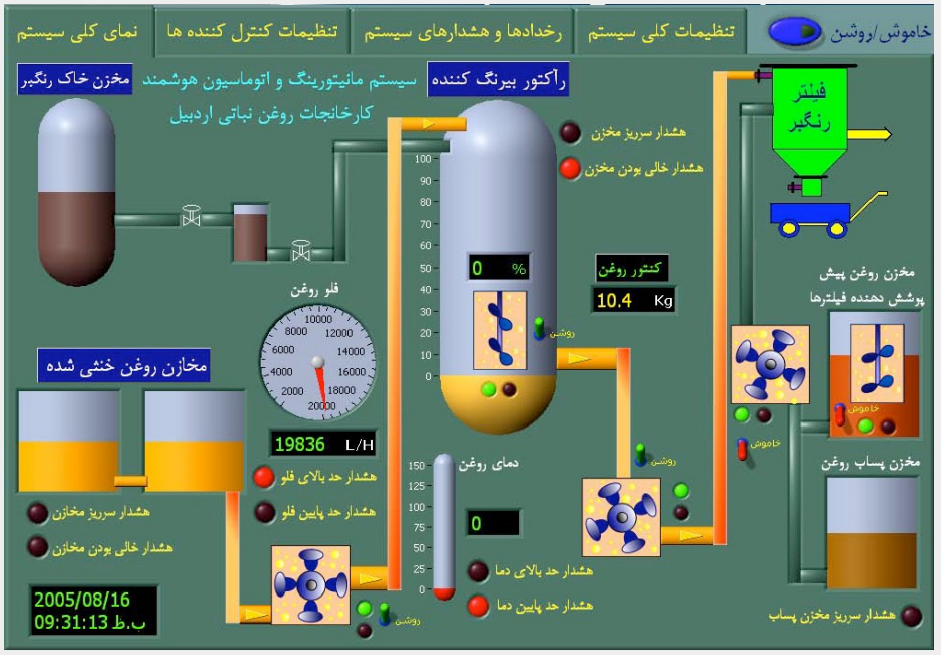



Napad na VOIP telefon.

# Ranljivi niso samo računalniki...

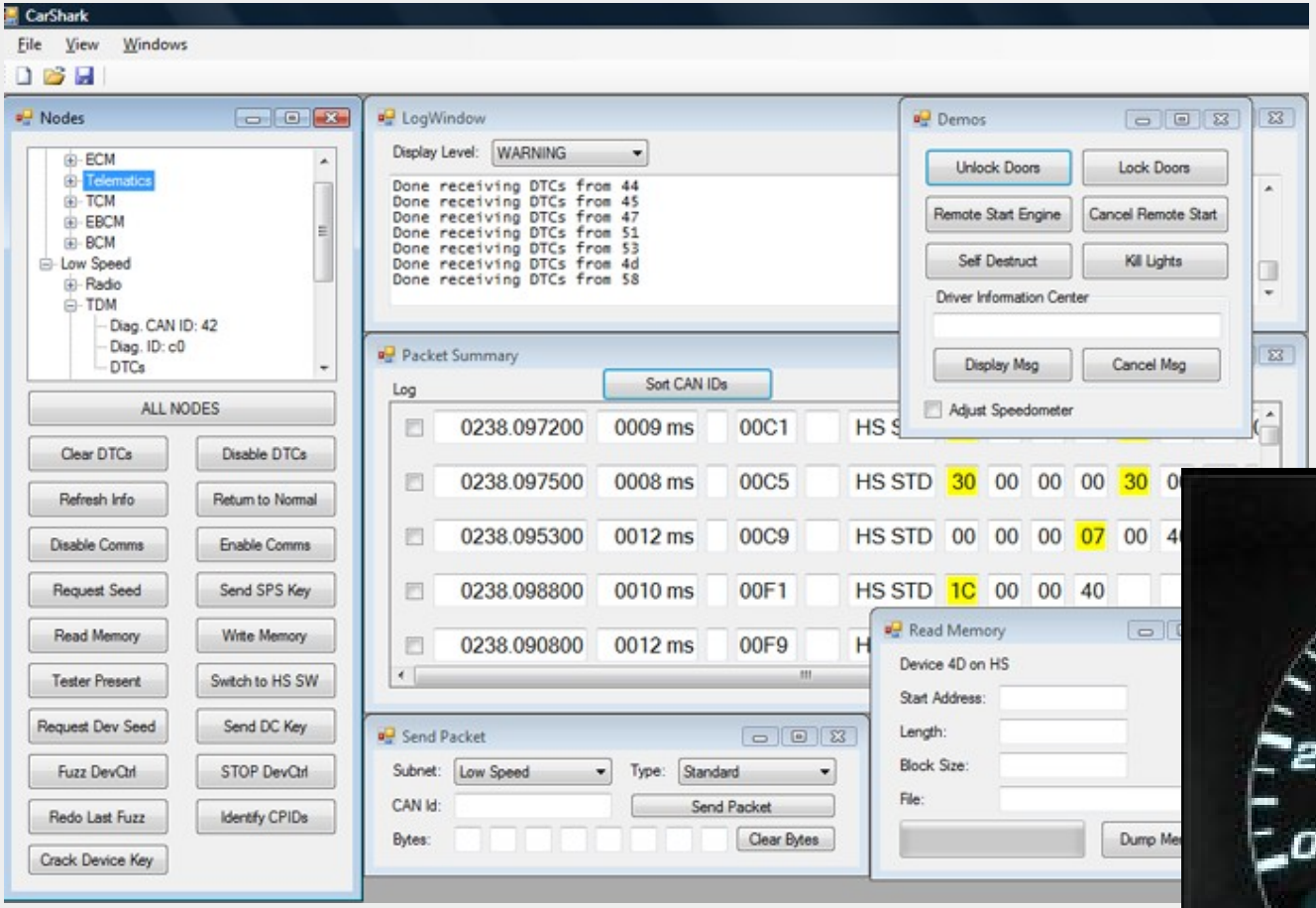


Napadi na RFID potne liste.




Napadi na SCADA sisteme.

# Ranljivi niso samo računalniki...




Napadi na avtomobile.

# Ranljivi niso samo računalniki...

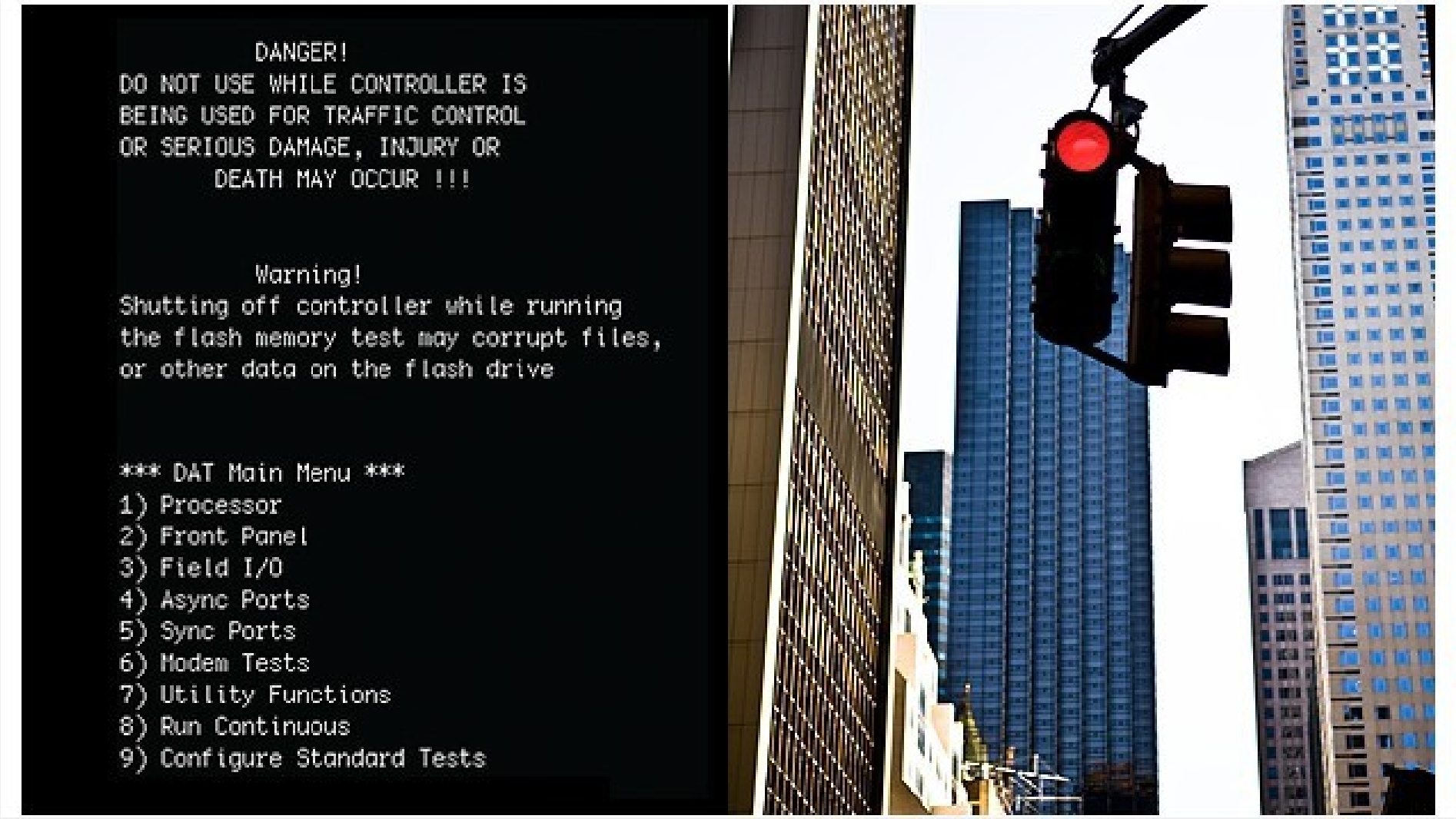
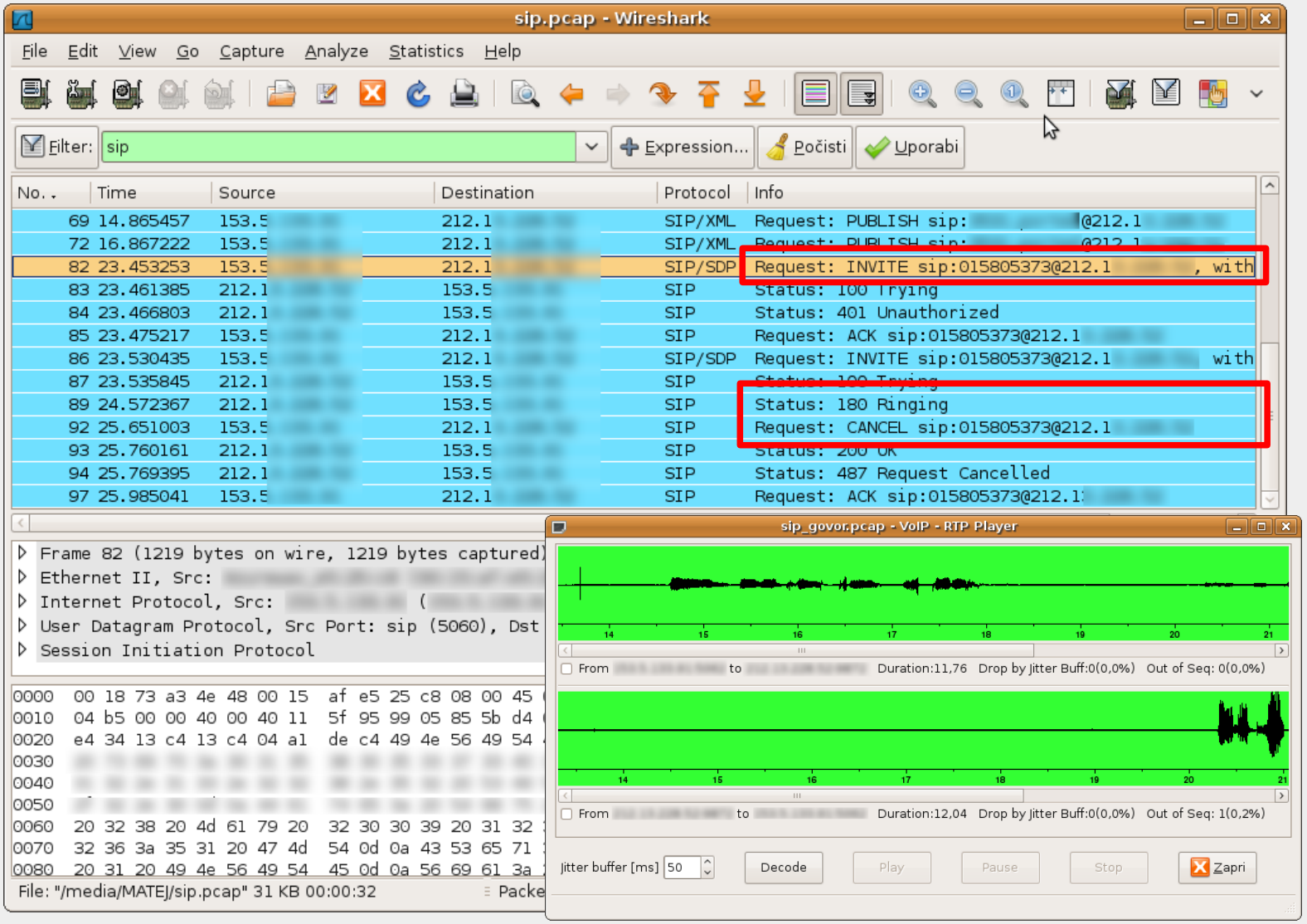
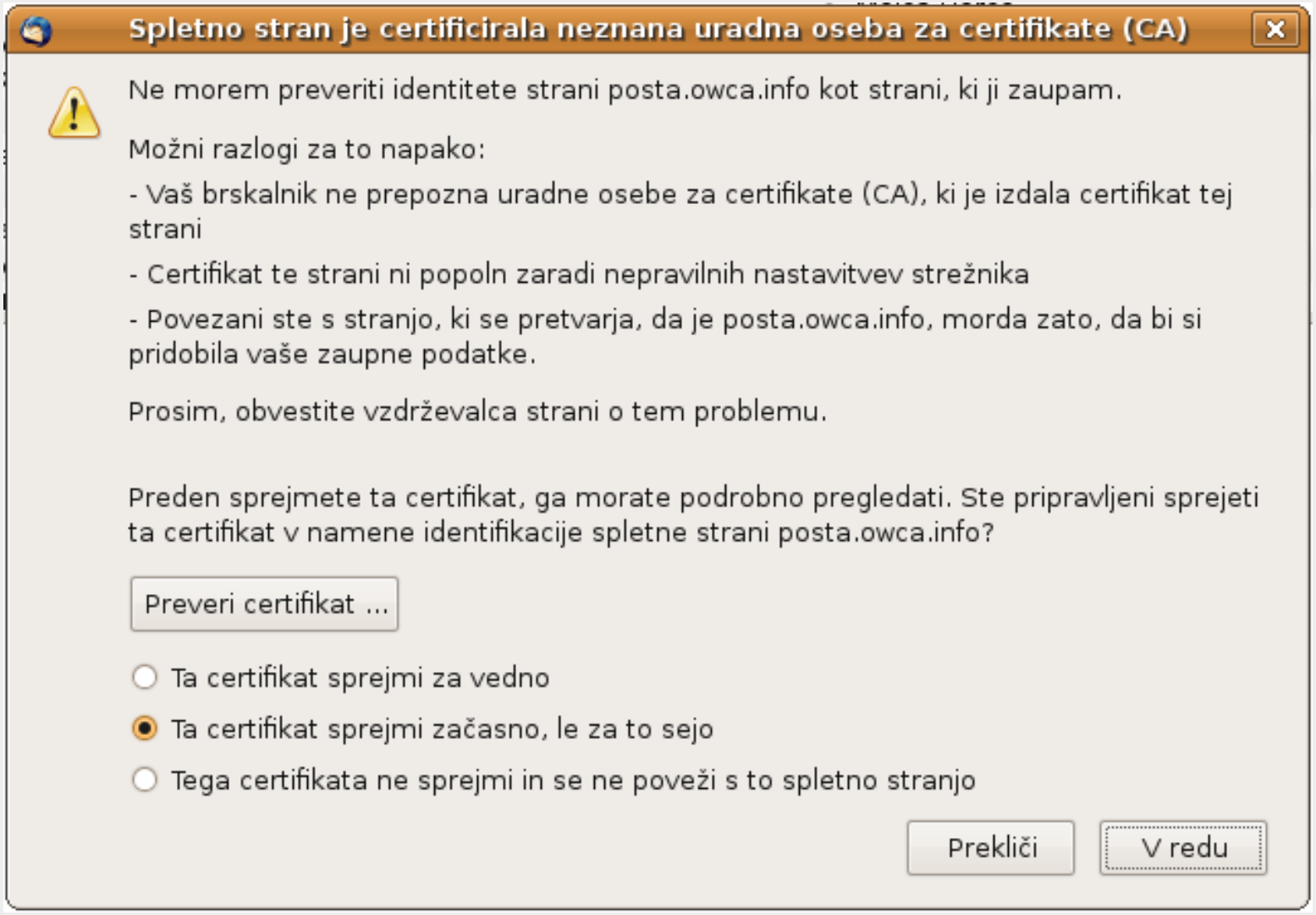



foto: Dan Tentler.

# Prestrezanje komunikacij

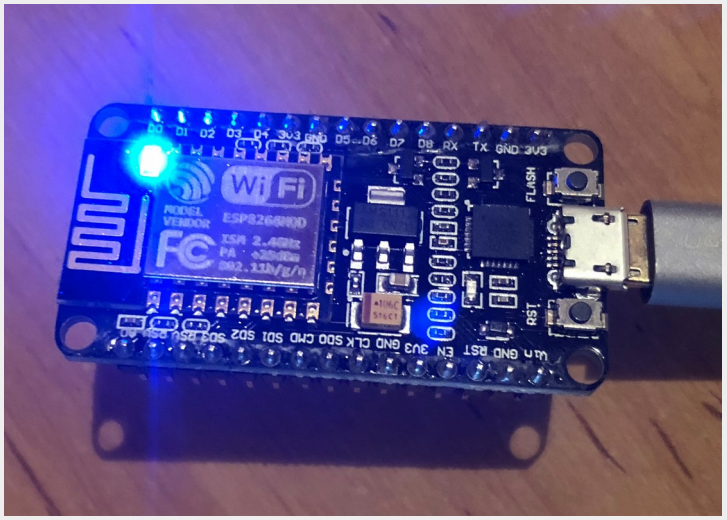


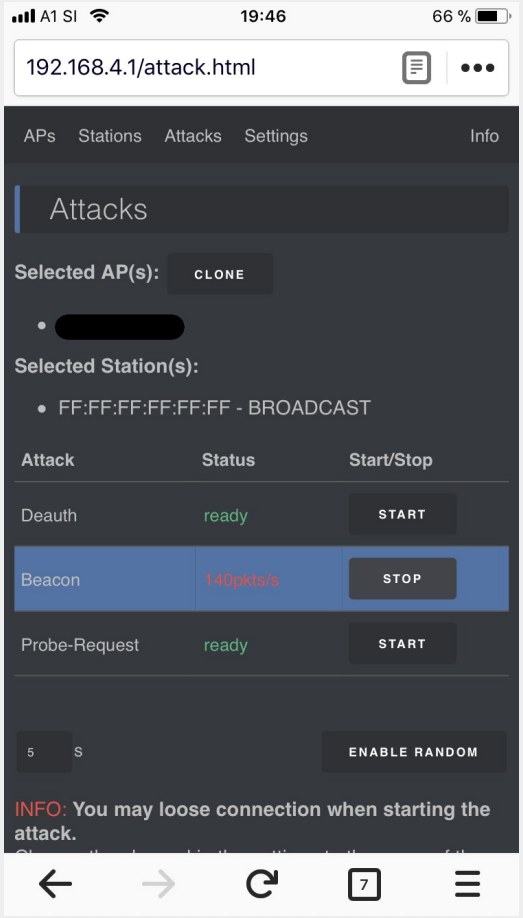
# Prestrezanje komunikacij

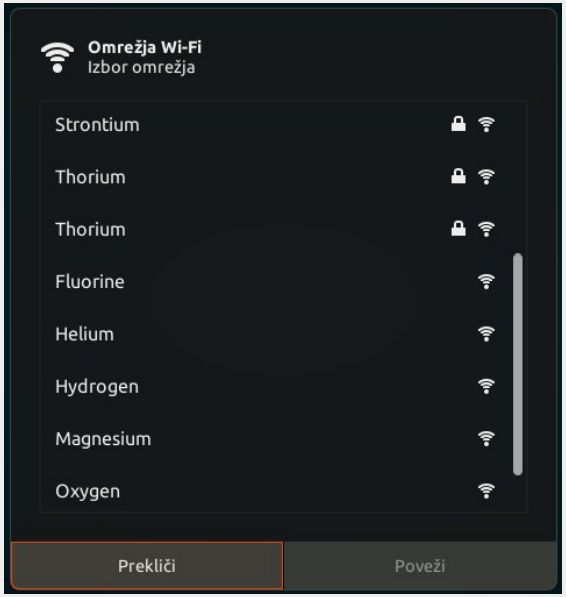



Previdno pri sprejemanju neznanih digitalnih potrdil!

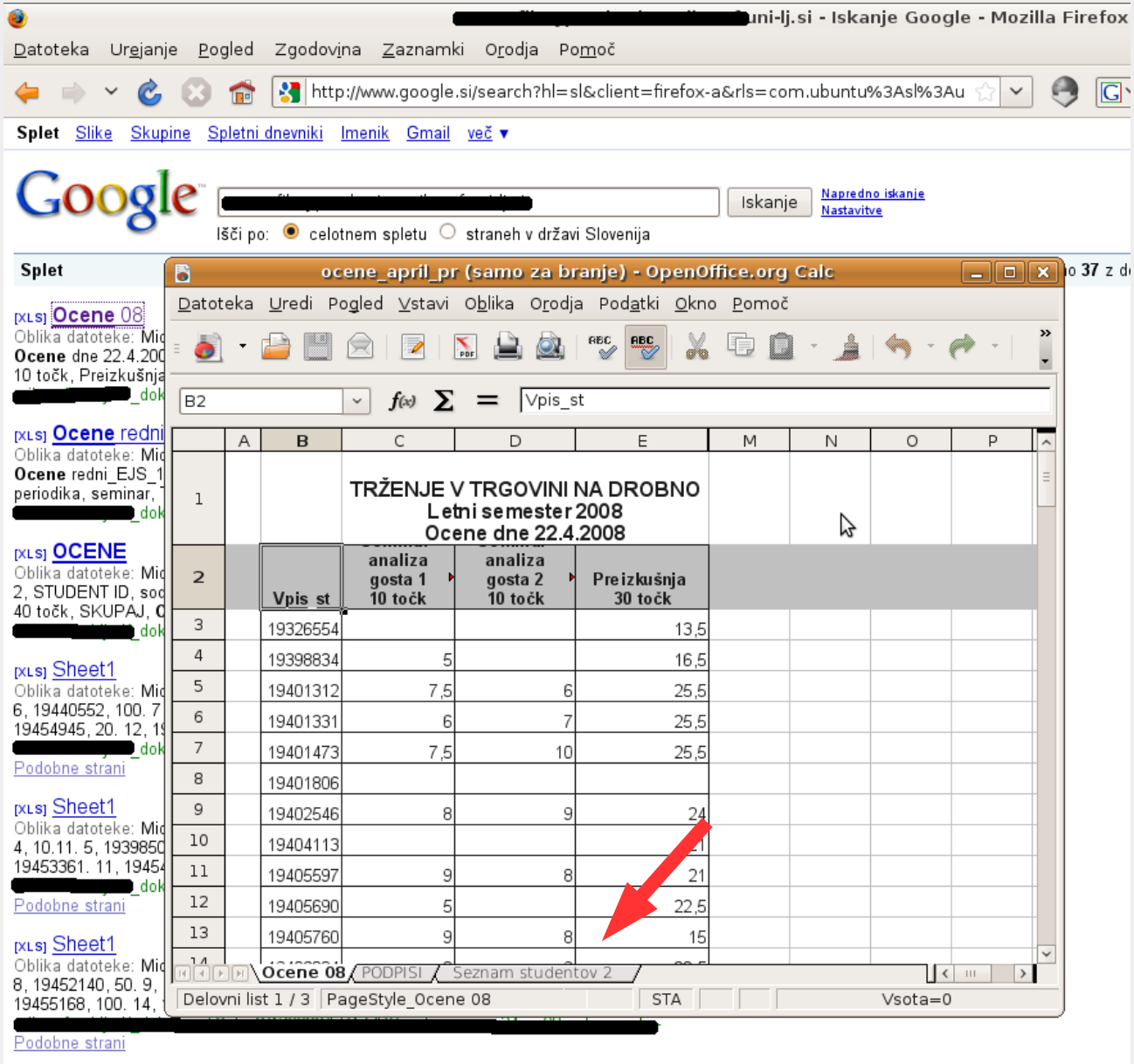
# Wifi omrežja?



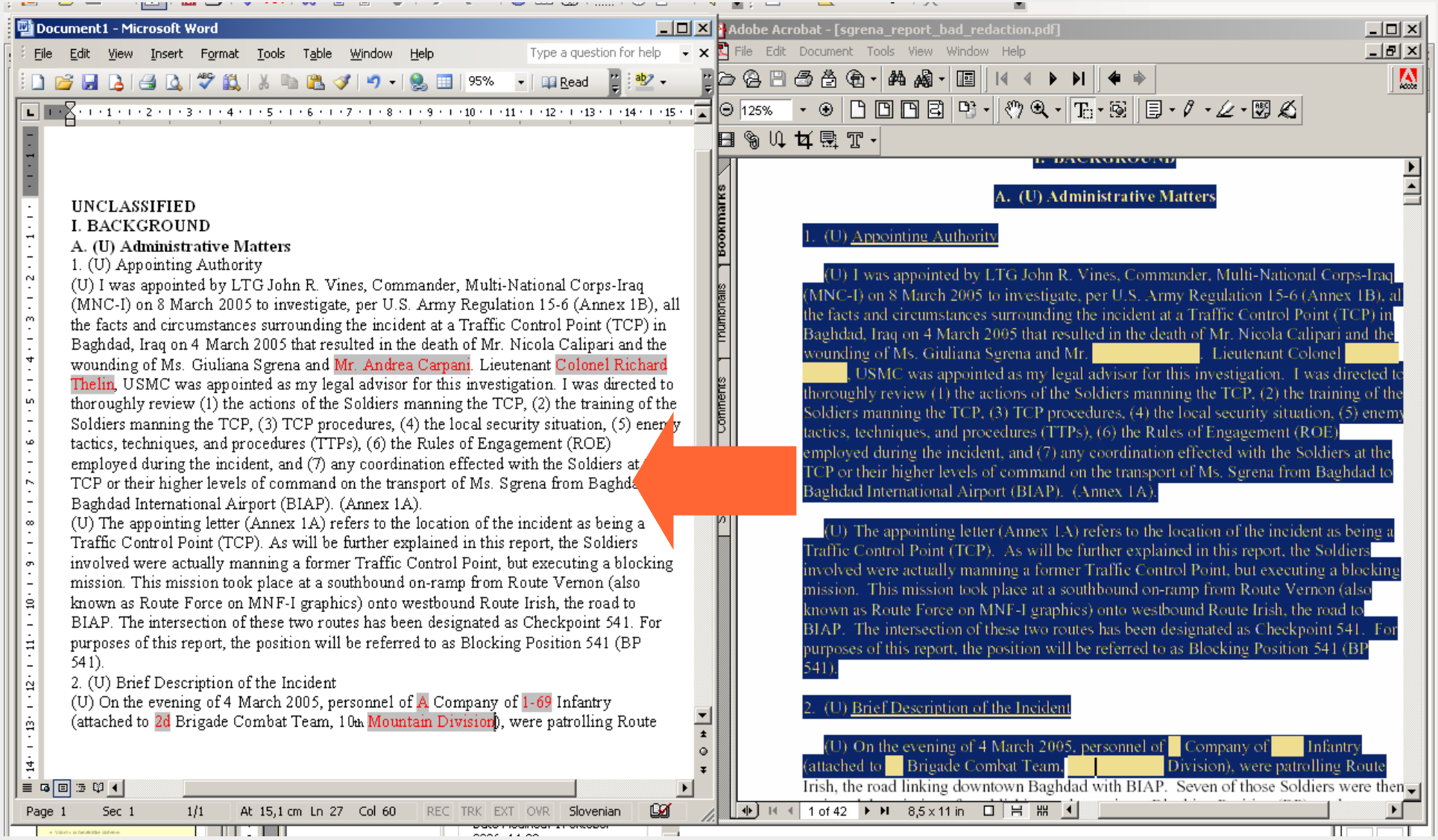


# Zbiranje javnih (?) informacij

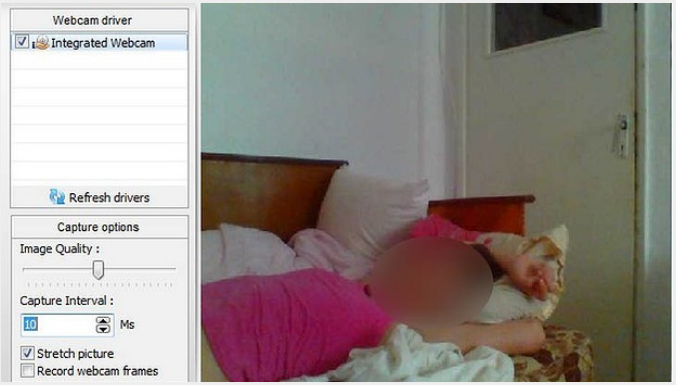


# Zbiranje javnih (?) informacij



# Zbiranje javnih (?) informacij

# Zbiranje javnih (?) informacij




[redacted]**SARA**. Spol: Datum roj.: z. [redacted]iimek in ime:
Naroe ilo sprejema :[redacted]
12:04:07. AMBULANTA[redacted] ...

Untitled
https://www.sb-izola.si/wp-content/uploads/2018/01/izvid.pdf
Sedež: [redacted]. Enota: [redacted]
GINEKOLOŠKA AMBULANTA.[redacted] **Sara**, rojena [redacted] ul. 16, 6000 Koper.

Untitled
https://www.sb-izola.si/wp-content/uploads/2017/05/doc04315520170511074250.pdf
9. maj 2017 -[redacted] **SARA**.[redacted] 6274 ŠMARJE.

212[redacted]eb/guest/en/websys/webArch/mainFrame.cgi

RICOH **MP C4503** Web Image Monitor

Home

**Print Job List**

Back

Print Delete

Go to [Printer Job History] >>

View : All Select User ID : *** All ***

1/1 Display Items : 10

Job(s) : 8 Selected : 0 Select All Clear All

| | Type | | User ID | File Name | Created At | Print Start Time | Page(s) | Copies |
|---|---|---|---|---|---|---|---|---|
| | Hold Print | | ZBORNICA | Microsoft Word - Izjava-ekskurzija-3.doc | 14/3/2019 11:02:14 | --- | 2 | --- |
| | Hold Print | | ZBORNICA | Microsoft Word - Izjava-ekskurzija-2.doc | 14/3/2019 10:58:41 | --- | 2 | --- |
| | Hold Print | | ZBORNICA | Microsoft Word - Izjava-ekskurzija-2.doc | 14/3/2019 10:57:42 | --- | 2 | --- |
| | Hold Print | | ZBORNICA | Microsoft Word - Izjava-ekskurzija-1.doc | 14/3/2019 10:56:52 | --- | 2 | --- |
| | Hold Print | | zborn2 | Microsoft Word - LISTA PRISOTNOSTI NA 1.docx | 12/3/2019 12:23:11 | --- | 1 | --- |
| | Hold Print | | sobRAZGO | Microsoft Word - Dokument1 | 8/3/2019 12:15:48 | --- | 1 | --- |
| | Hold Print | | sobRAZGO | FiSS_Formule.pdf | 5/2/2019 11:28:11 | --- | 4 | --- |
| | Hold Print | | sobRAZGO | Dohod_VirDat_Obvestilo_2018_[redacted].pdf | 31/1/2019 11:45:38 | --- | 1 | --- |

Back

# Zbiranje javnih (?) informacij

https://kidstar.si/wp-content/uploads/2018/02/

## Index of /wp-content/uploads/2018/02

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| Dobavnica-12018.pdf | 2018-02-13 21:31 | 1.1M | |
| Dobavnica-22018.pdf | 2018-02-15 07:51 | 1.1M | |
| Dobavnica-32018.pdf | 2018-02-15 07:51 | 1.1M | |
| Dobavnica-42018.pdf | 2018-02-15 07:51 | 1.1M | |
| Dobavnica-52018.pdf | 2018-02-15 07:51 | 1.1M | |
| Dobavnica-62018.pdf | 2018-02-16 07:45 | 1.1M | |
| Dobavnica-72018.pdf | 2018-02-16 07:45 | 1.1M | |
| Dobavnica-82018.pdf | 2018-02-16 07:45 | 1.1M | |
| Dobavnica-92018.pdf | 2018-02-16 07:45 | 1.1M | |
| Dobavnica-102018.pdf | 2018-02-16 07:46 | 1.1M | |
| Dobavnica-112018.pdf | 2018-02-16 07:46 | 1.1M | |
| Dobavnica-122018.pdf | 2018-02-20 07:12 | 1.1M | |
| Dobavnica-132018.pdf | 2018-02-20 07:12 | 1.1M | |
| Dobavnica-142018.pdf | 2018-02-20 07:12 | 1.1M | |
| Dobavnica-152018.pdf | 2018-02-20 07:12 | 1.1M | |
| Dobavnica-162018.pdf | 2018-02-20 07:12 | 1.1M | |
| Dobavnica-172018.pdf | 2018-02-21 08:29 | 1.1M | |
| Dobavnica-182018.pdf | 2018-02-21 08:29 | 1.1M | |
| Dobavnica-192018.pdf | 2018-02-21 08:29 | 1.1M | |
| Dobavnica-202018.pdf | 2018-02-21 08:29 | 1.1M | |

izpis.proteini.si/1[redacted]39.pdf

1 of 1 — 100%

**RAČUN ŠT: 1[redacted]39**

Sklic na: [redacted]
Jesenice, dne: 04.03.2019 10:19
Datum valute: 18.03.2019
Datum opravljene storitve: 04.03.2019 10:19

PROTEINI.SI SPORT NUTRITION CENTER

**ROLnet d.o.o.**
Blejska Dobrava 42
SI-4273 Blejska Dobrava

**TRR:** SI56 3000 0001 6408 944
**Banka:** Sberbank banka d.d.
**ID za DDV:** SI 44085206
**Matična številka:** 2024691

**E:** info@proteini.si
www.proteini.si

**Vesna**[redacted]

Tel:
Kontakt:
ID za DDV:

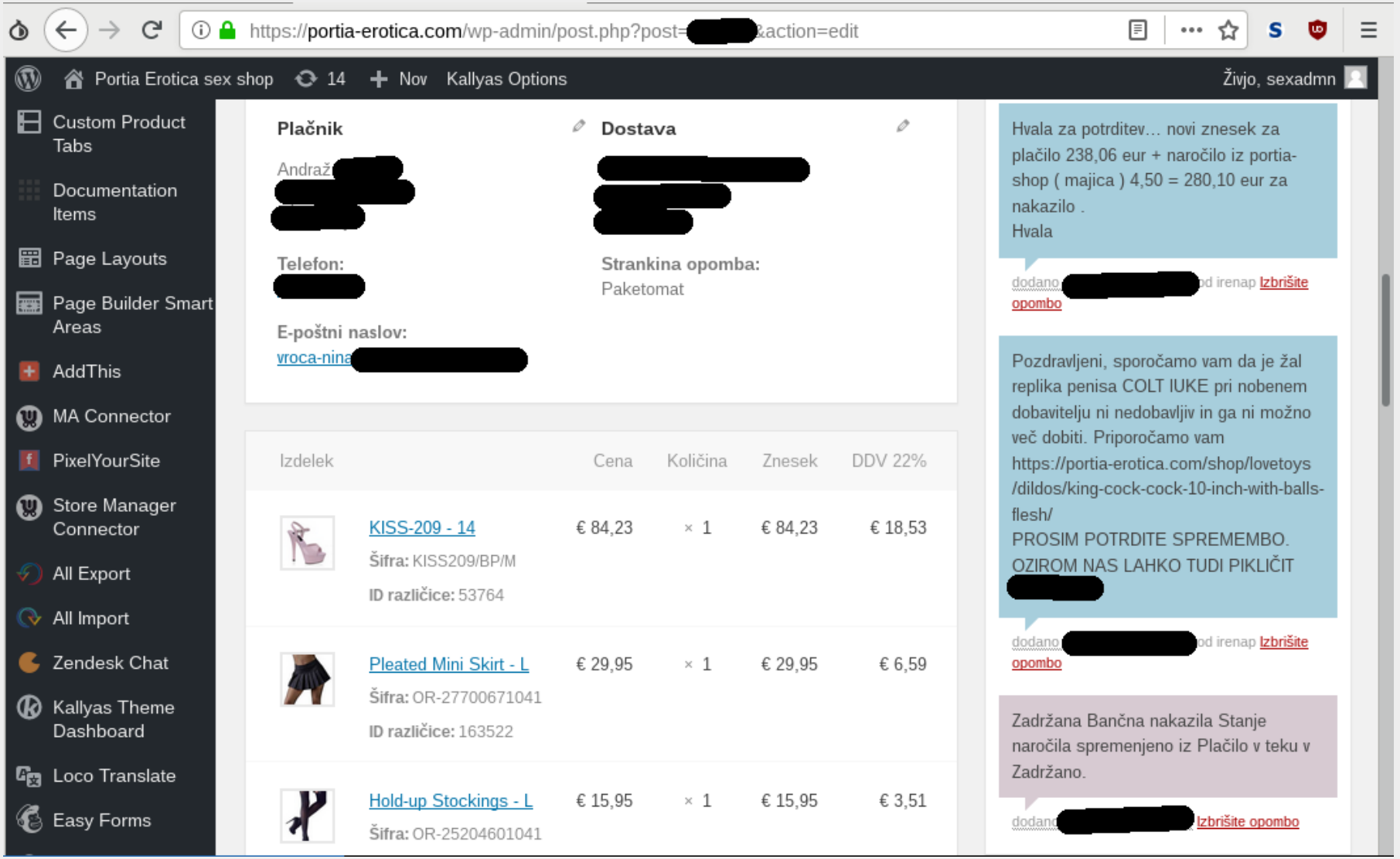
| Naziv storitve | Količina | Cena | Popust % | Brez DDV | DDV % | Skupaj |
|---|---|---|---|---|---|---|
| PROTEINI.SI 100% NATURAL WHEY PROTEIN, 500g, White Choc. Straw. | 2 | 10,04 | 0,00 | 10,04 | 9,50 | **21,98** |
| Dostava Pošta Slovenije SLOVENIA | 1 | 2,45 | 0,00 | 2,45 | 22,00 | **2,99** |

| | |
|---|---|
| Skupaj bruto znesek: | 22,53 |
| Popust: | 0,00 |
| Skupaj neto znesek: | 22,53 |
| Davek: | 2,44 |
| **Skupaj:** | **24,97 EUR** |

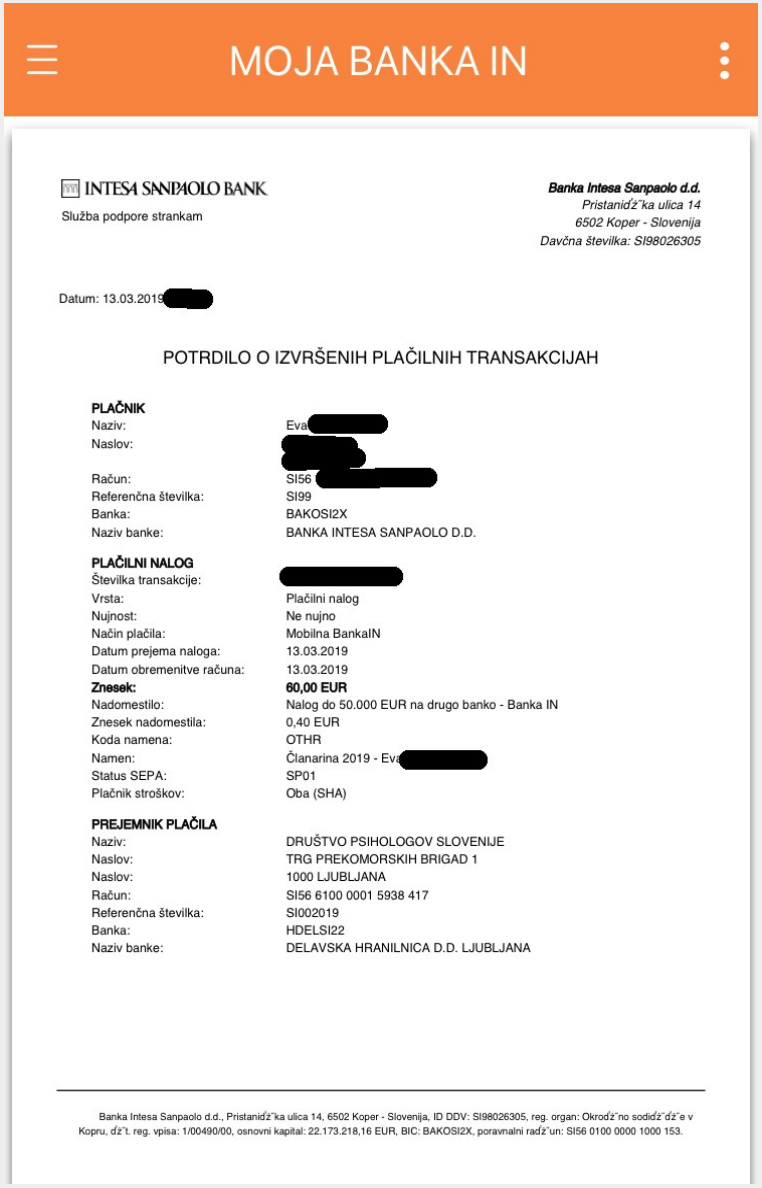
**Obračun DDV:**

| Stopnja | Osnova | Davek |
|---|---|---|
| 9,50% | 20,08 | 1,90 |

# Zbiranje javnih (?) informacij



# Zbiranje javnih (?) informacij



MOJA BANKA IN

INTESA SANPAOLO BANK
Služba podpore strankam

*Banka Intesa Sanpaolo d.d.*
*Pristaniška ulica 14*
*6502 Koper - Slovenija*
*Davčna številka: SI98026305*

Datum: 13.03.2019[redacted]

POTRDILO O IZVRŠENIH PLAČILNIH TRANSAKCIJAH

**PLAČNIK**

| | |
|---|---|
| Naziv: | Eva[redacted] |
| Naslov: | [redacted] |
| Račun: | SI56 [redacted] |
| Referenčna številka: | SI99 |
| Banka: | BAKOSI2X |
| Naziv banke: | BANKA INTESA SANPAOLO D.D. |

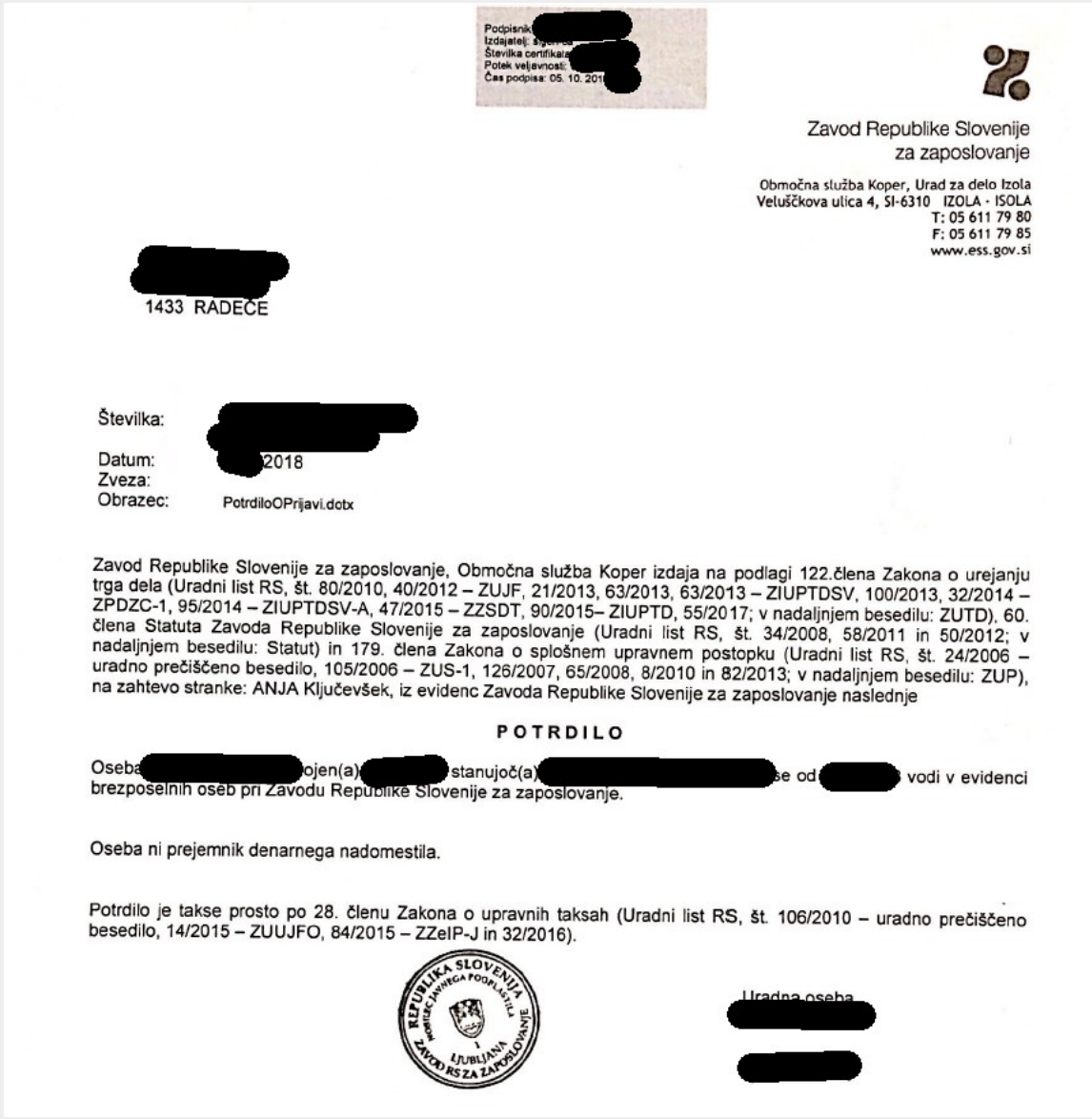
**PLAČILNI NALOG**

| | |
|---|---|
| Številka transakcije: | [redacted] |
| Vrsta: | Plačilni nalog |
| Nujnost: | Ne nujno |
| Način plačila: | Mobilna BankaIN |
| Datum prejema naloga: | 13.03.2019 |
| Datum obremenitve računa: | 13.03.2019 |
| **Znesek:** | **60,00 EUR** |
| Nadomestilo: | Nalog do 50.000 EUR na drugo banko - Banka IN |
| Znesek nadomestila: | 0,40 EUR |
| Koda namena: | OTHR |
| Namen: | Članarina 2019 - Eva[redacted] |
| Status SEPA: | SP01 |
| Plačnik stroškov: | Oba (SHA) |

**PREJEMNIK PLAČILA**

| | |
|---|---|
| Naziv: | DRUŠTVO PSIHOLOGOV SLOVENIJE |
| Naslov: | TRG PREKOMORSKIH BRIGAD 1 |
| Naslov: | 1000 LJUBLJANA |
| Račun: | SI56 6100 0001 5938 417 |
| Referenčna številka: | SI002019 |
| Banka: | HDELSI22 |
| Naziv banke: | DELAVSKA HRANILNICA D.D. LJUBLJANA |

Banka Intesa Sanpaolo d.d., Pristaniška ulica 14, 6502 Koper - Slovenija, ID DDV: SI98026305, reg. organ: Okrožno sodišče v Kopru, vl. reg. vpisa: 1/00490/00, osnovni kapital: 22.173.218,16 EUR, BIC: BAKOSI2X, poravnalni račun: SI56 0100 0000 1000 153.



Podpisnik: [redacted]
Izdajatelj: [redacted]
Številka certifikata: [redacted]
Potek veljavnosti: [redacted]
Čas podpisa: 05. 10. 201[redacted]

Zavod Republike Slovenije
za zaposlovanje

Območna služba Koper, Urad za delo Izola
Veluščkova ulica 4, SI-6310 IZOLA - ISOLA
T: 05 611 79 80
F: 05 611 79 85
www.ess.gov.si

[redacted]
1433 RADEČE

Številka: [redacted]
Datum: [redacted]2018
Zveza:
Obrazec: PotrdiloOPrijavi.dotx

Zavod Republike Slovenije za zaposlovanje, Območna služba Koper izdaja na podlagi 122.člena Zakona o urejanju trga dela (Uradni list RS, št. 80/2010, 40/2012 – ZUJF, 21/2013, 63/2013, 63/2013 – ZIUPTDSV, 100/2013, 32/2014 – ZPDZC-1, 95/2014 – ZIUPTDSV-A, 47/2015 – ZZSDT, 90/2015– ZIUPTD, 55/2017; v nadaljnjem besedilu: ZUTD), 60. člena Statuta Zavoda Republike Slovenije za zaposlovanje (Uradni list RS, št. 34/2008, 58/2011 in 50/2012; v nadaljnjem besedilu: Statut) in 179. člena Zakona o splošnem upravnem postopku (Uradni list RS, št. 24/2006 – uradno prečiščeno besedilo, 105/2006 – ZUS-1, 126/2007, 65/2008, 8/2010 in 82/2013; v nadaljnjem besedilu: ZUP), na zahtevo stranke: ANJA Ključevšek, iz evidenc Zavoda Republike Slovenije za zaposlovanje naslednje

**POTRDILO**

Oseba [redacted] ojen(a) [redacted] stanujoč(a) [redacted] se od [redacted] vodi v evidenci brezposelnih oseb pri Zavodu Republike Slovenije za zaposlovanje.

Oseba ni prejemnik denarnega nadomestila.

Potrdilo je takse prosto po 28. členu Zakona o upravnih taksah (Uradni list RS, št. 106/2010 – uradno prečiščeno besedilo, 14/2015 – ZUUJFO, 84/2015 – ZZelP-J in 32/2016).

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA DELO, DRUŽINO, SOCIALNE ZADEVE IN ENAKE MOŽNOSTI
ZAVOD RS ZA ZAPOSLOVANJE
1
LJUBLJANA

Uradna oseba
[redacted]

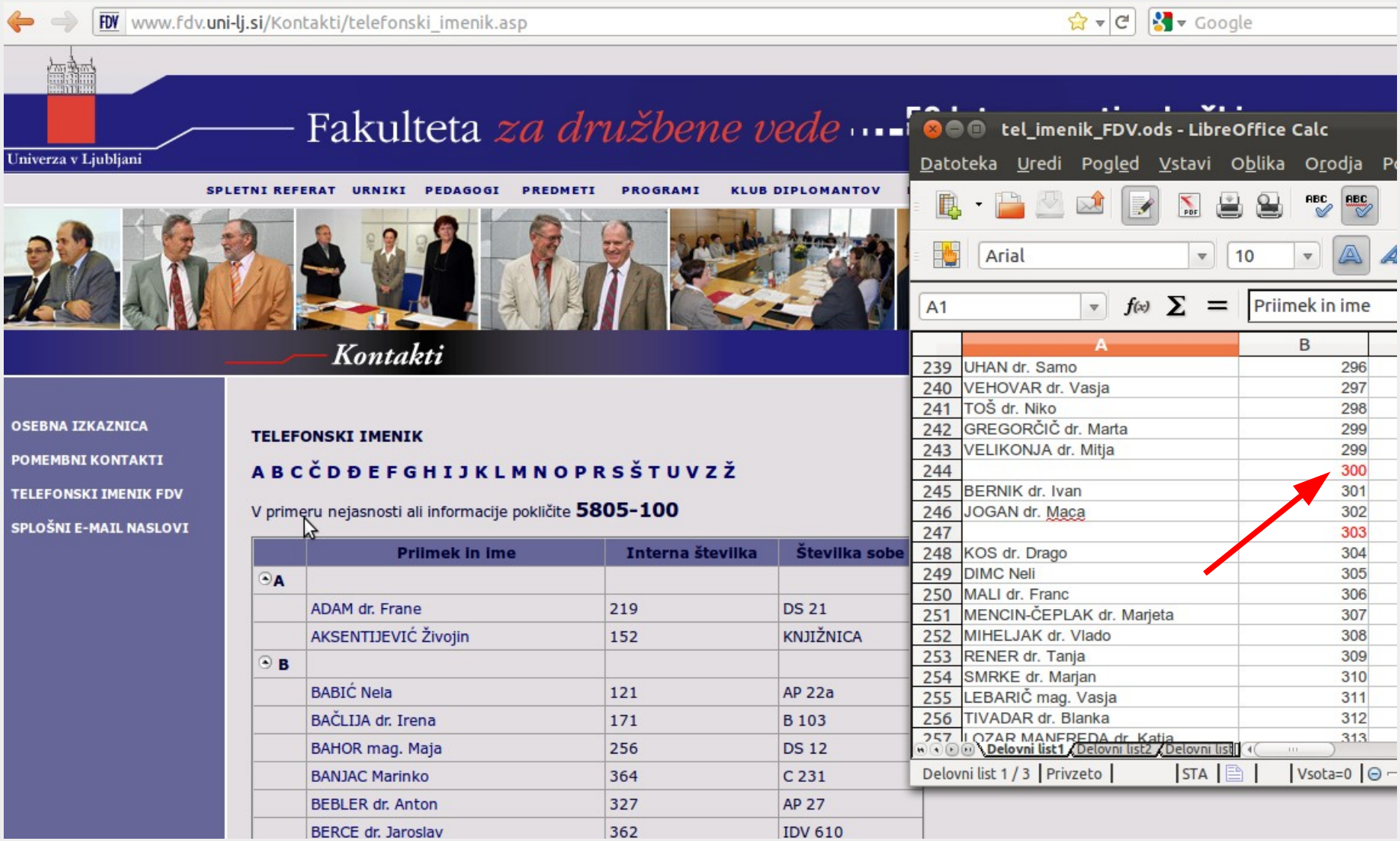
# Zbiranje javnih (?) informacij

(8 of 10)

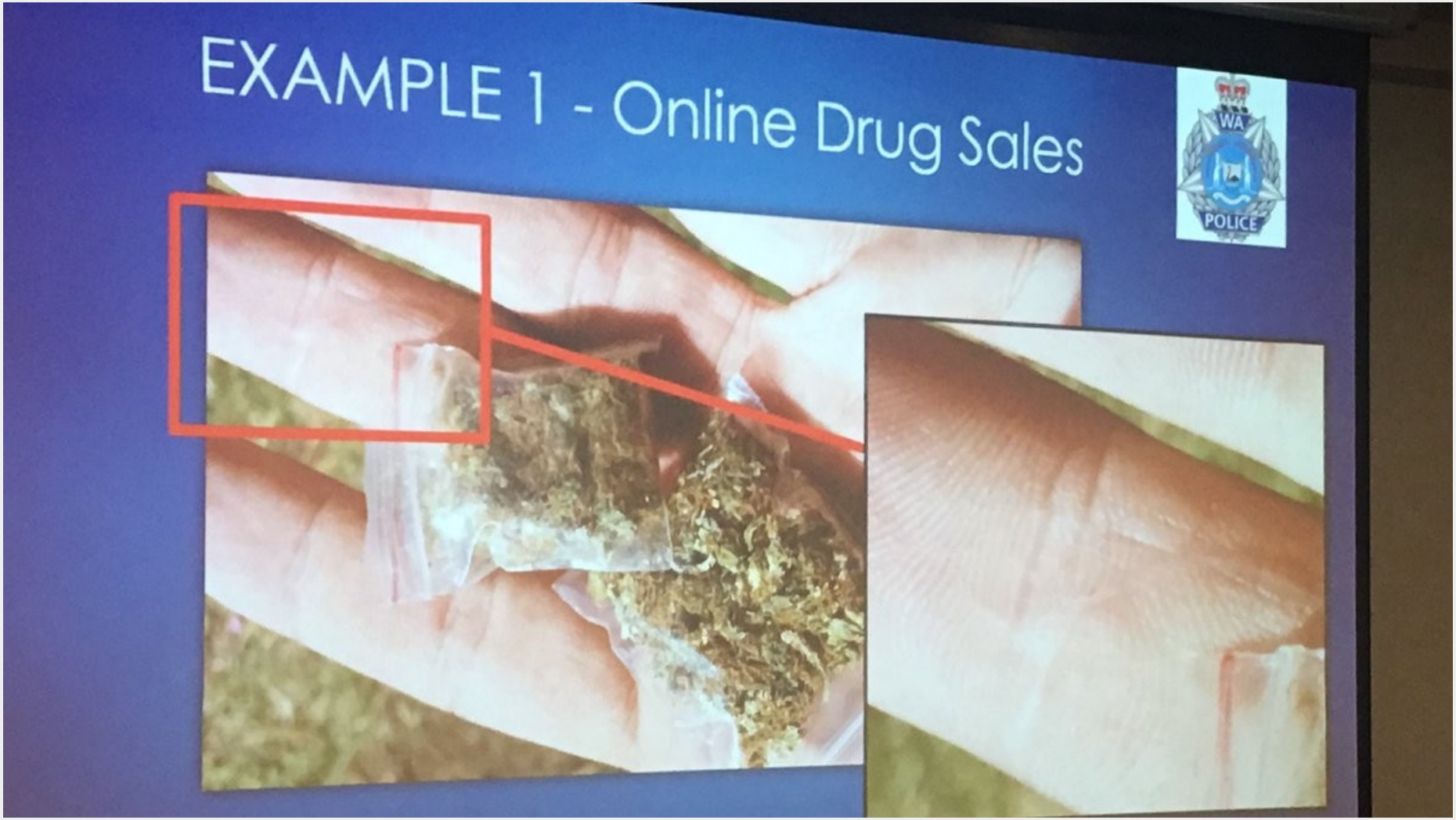
My sweethearts! ❤💋🥂🎈🎁 #birthday #birthdaygirl #friends #lovethem #womanpower #specialmoments #thankful #love

A post shared by Sabina Remar (@sabinaremar) on Dec 3, 2017 at 5:34am PST

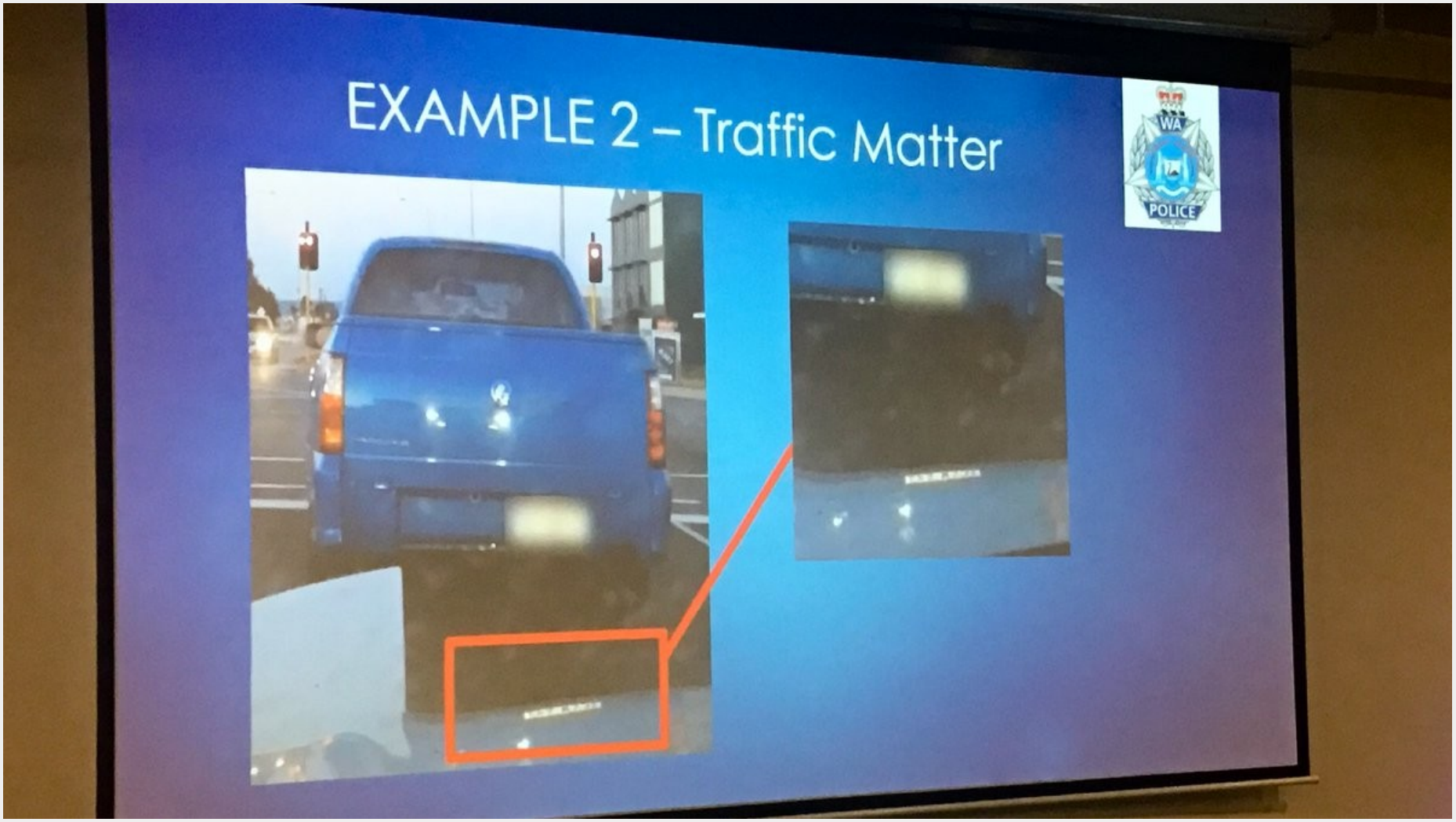
# Zbiranje javnih (?) informacij



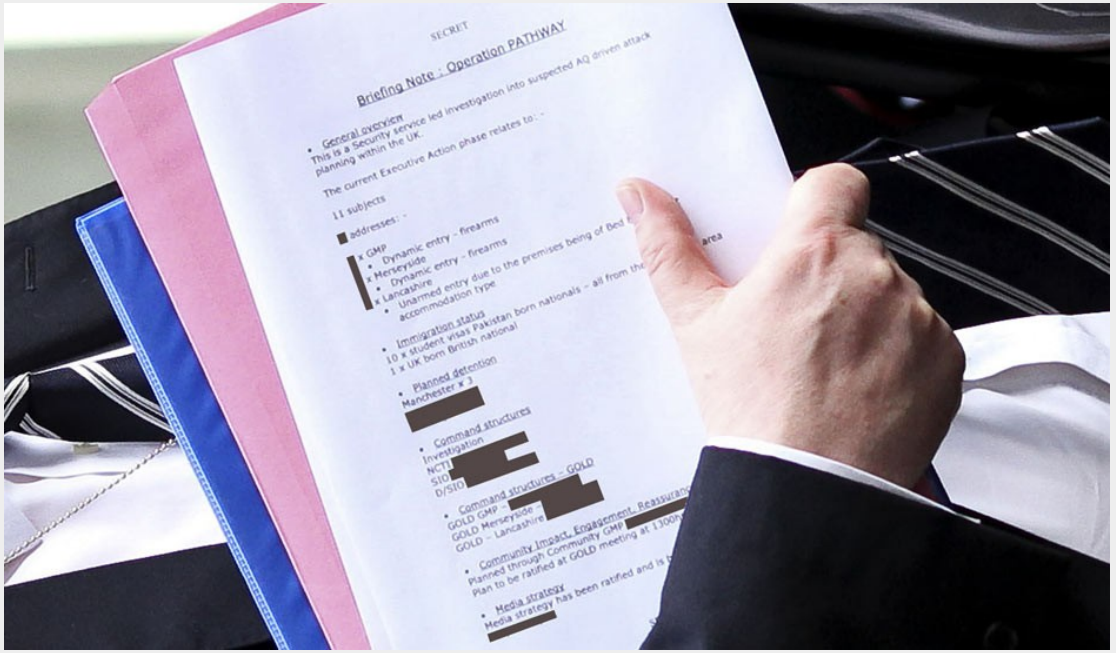
# Zbiranje javnih (?) informacij



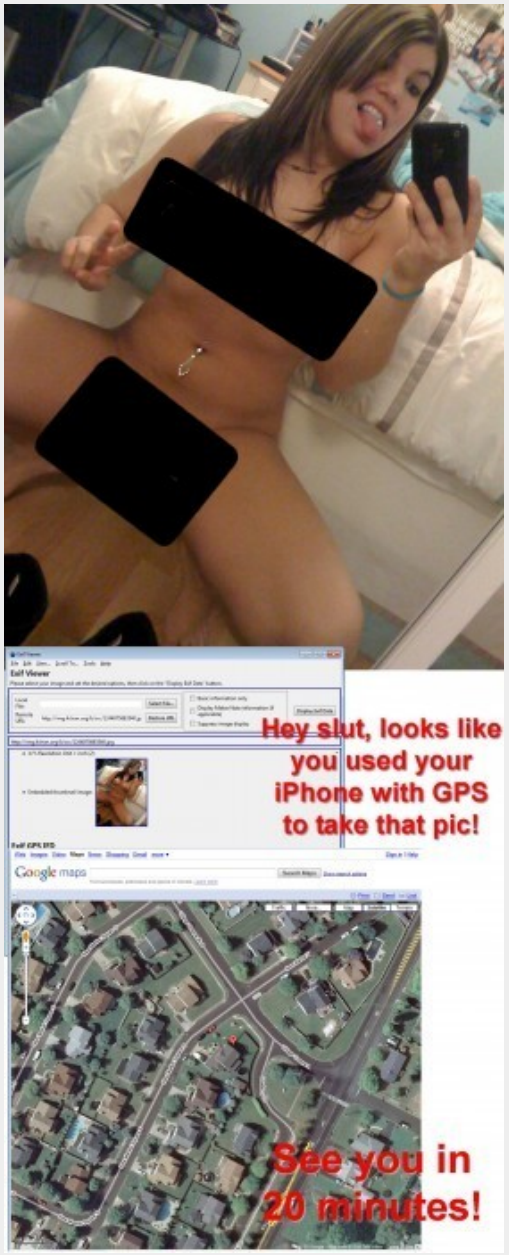
# Zbiranje javnih (?) informacij

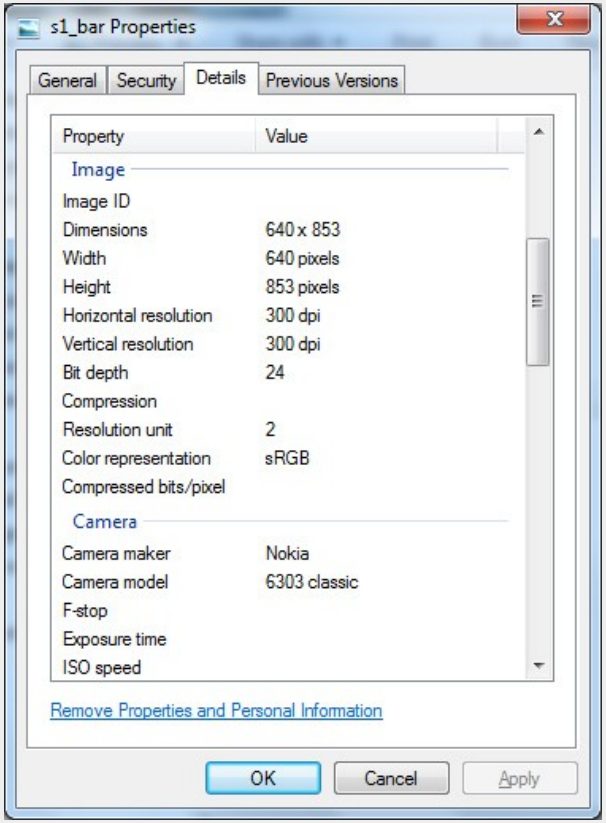


# Zbiranje javnih (?) informacij

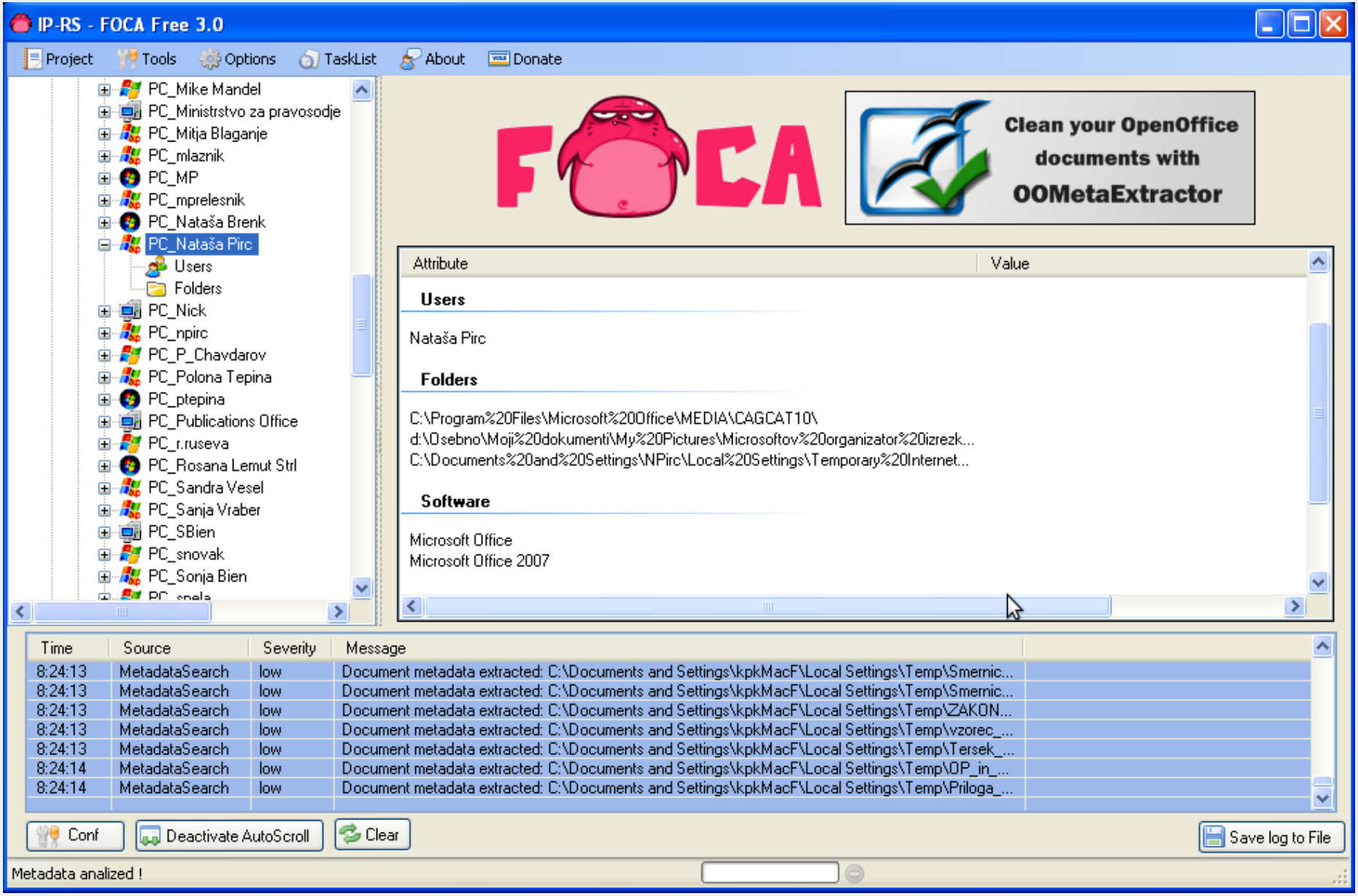


# Metapodatki

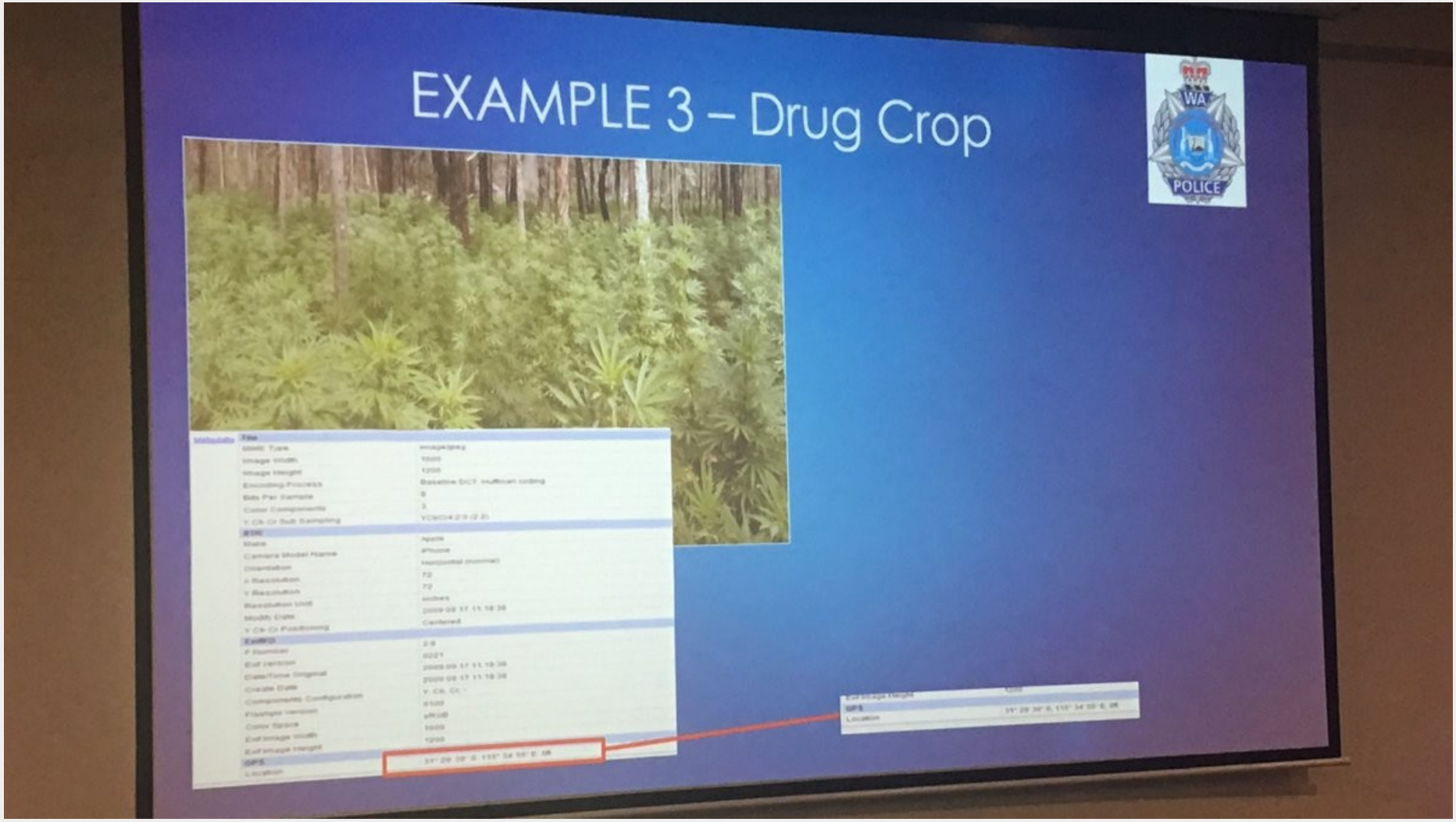


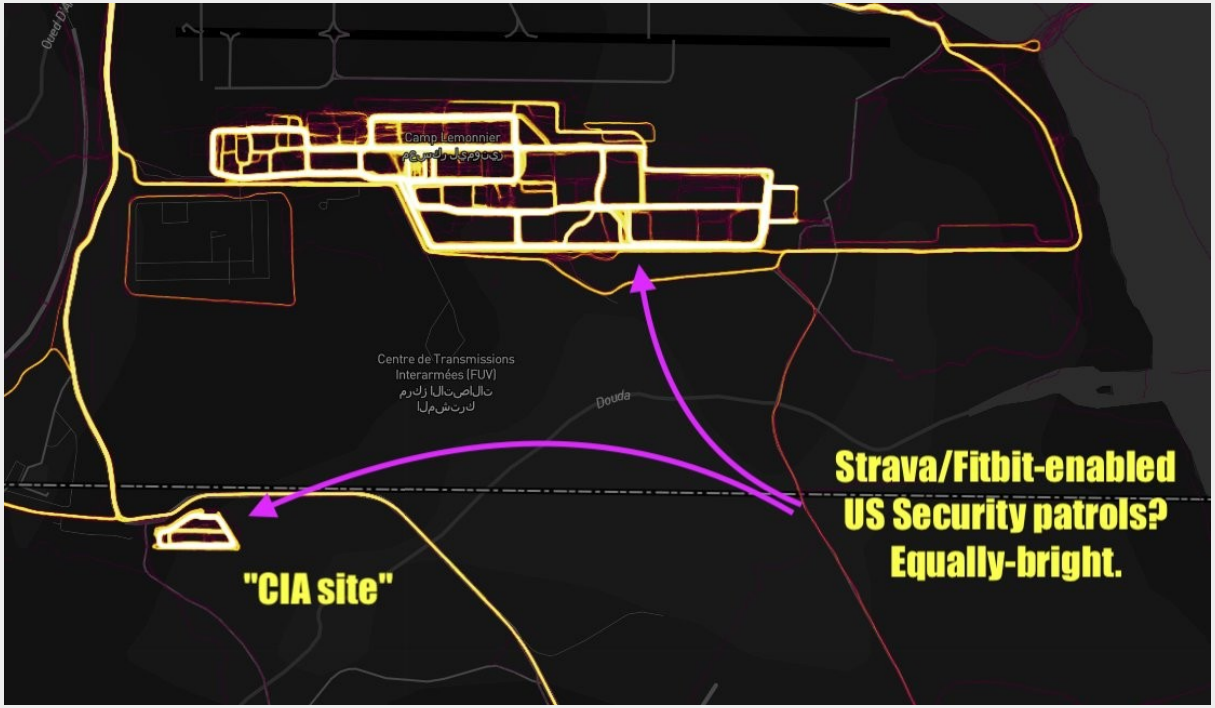
# Metapodatki



# Metapodatki



# Metapodatki




7) The article said there were a lot of other militaries living side-by-side up in Djibouti, let's scan around with Google maps and see what else is there.

8) Well, looky here: about a half mile from the camp, a short hop, but isolated: [google map link]

Wow, that was a bit too easy. Look the nice cleared perimeter, walls, crash-trenches so nobody can ram a truck-bomb through, complex gate to defeat assaults or truck-bombs. Expensive security. Good security. And the architectural tone looks pretty familiar, too; for one thing, only Americans spend money like that. [stderr]

9) Google "CIA black site djibouti" and you find [alj]

> The legal case of a former CIA detainee suing the government of Djibouti for hosting the facility where he says he was detained could be helped by the contents of a still-classified Senate report. Djibouti, a key U.S. ally, has denied for

# Metapodatki

# US bombs terror HQ after ISIS ‘moron’ takes selfie there

By Yaron Steinbuch

June 5, 2015 | 4:11pm

ype to Search

SEARCH

NEW YORK POST

A U.S. Navy F-18E Super Hornet used in airstrikes against the Islamic State.
AP

MORE ON:
ISIS

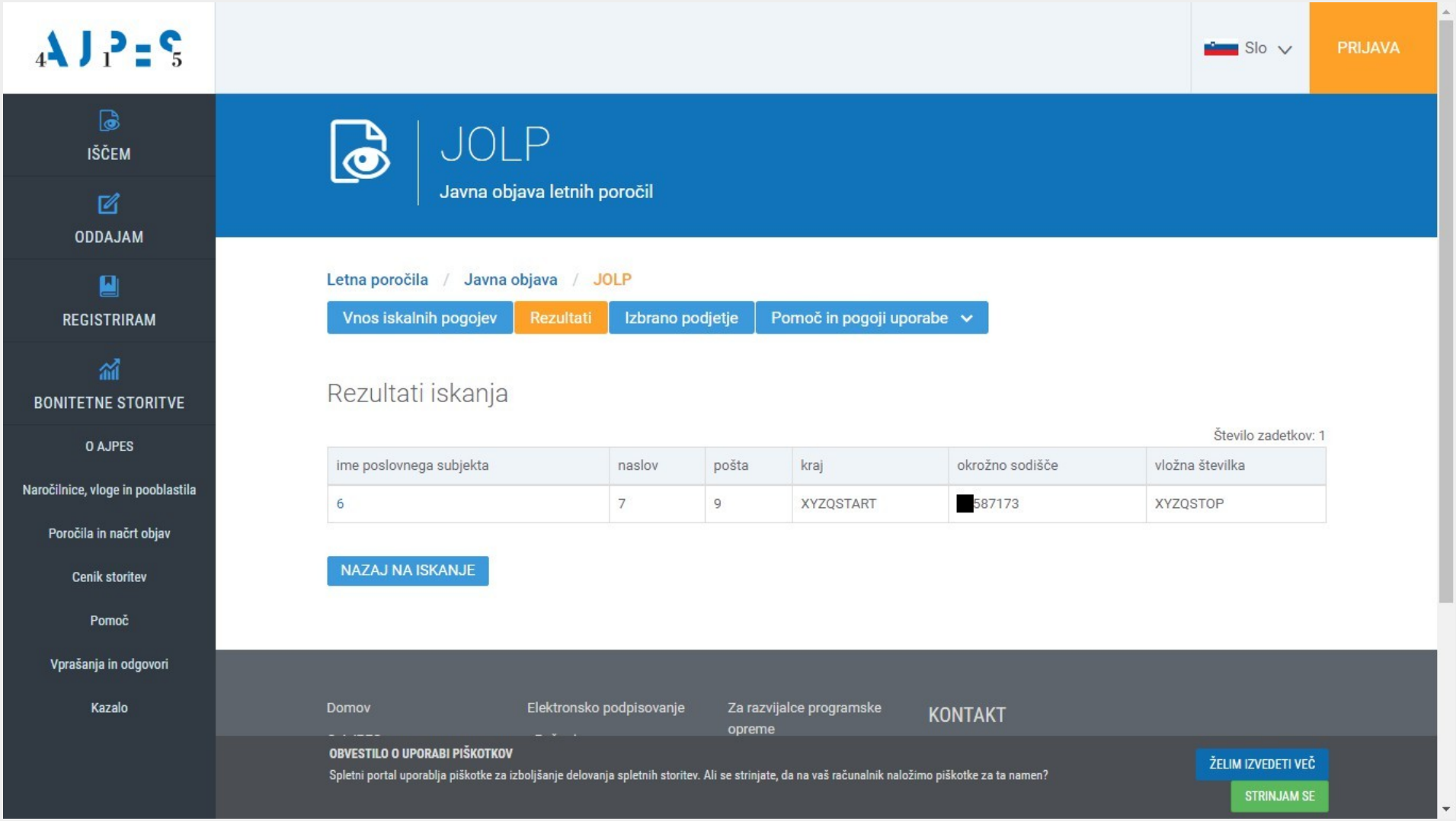
ISIS supporter gets at least 30 years for plot to kill Theresa May

US soldier to plead guilty to trying to help ISIS

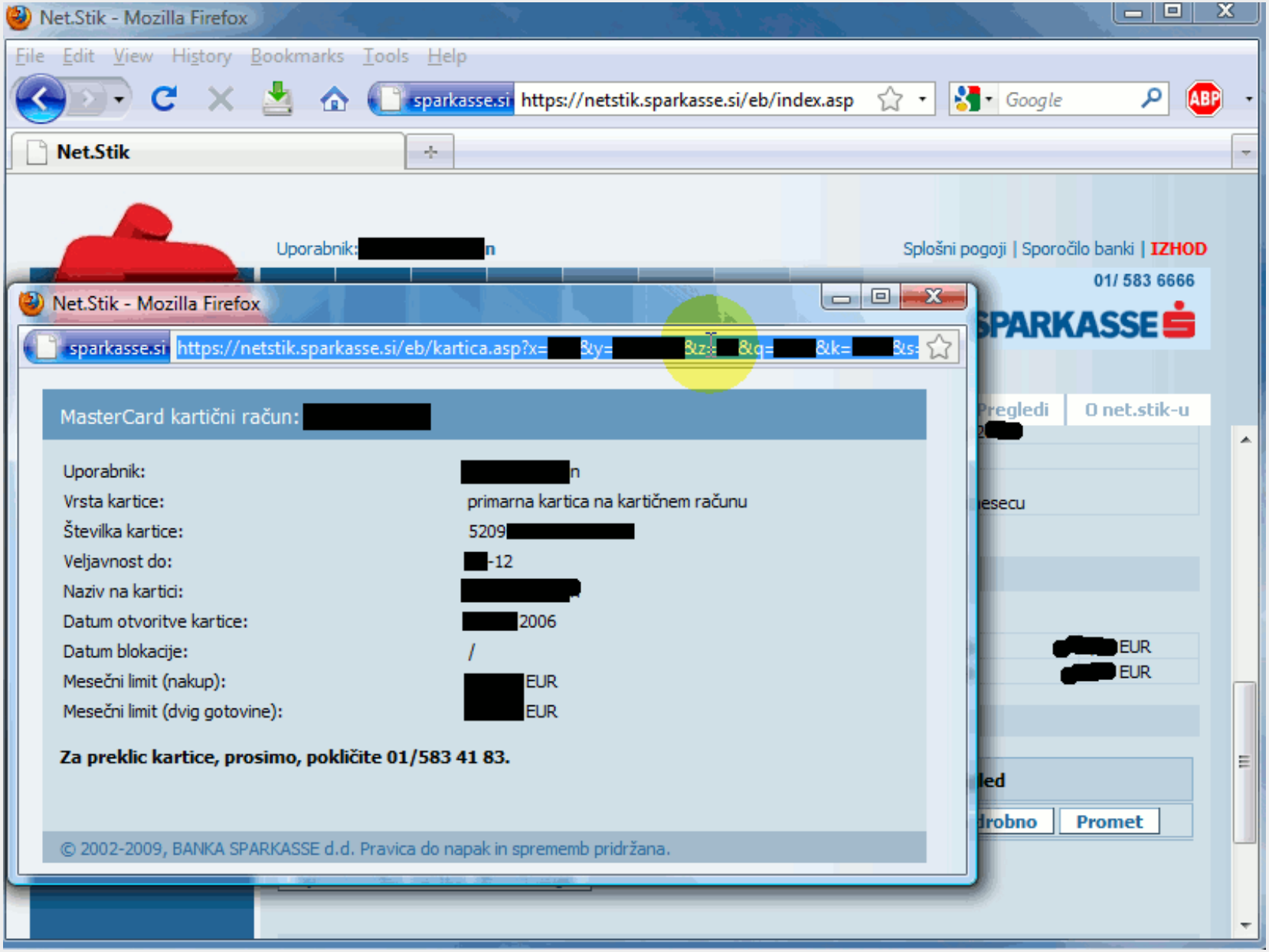
Islamic State thugs can blame the destruction of a headquarters building on a social media “moron” in their ranks who posted a selfie that pinpointed the site.

Air Force Gen. Hawk Carlisle, head of Air Combat Command, said that eagle-eyed airmen with a recon and surveillance group in Hurlburt Field, Florida, spotted the telltale post, Defense Tech reported via Military.com.

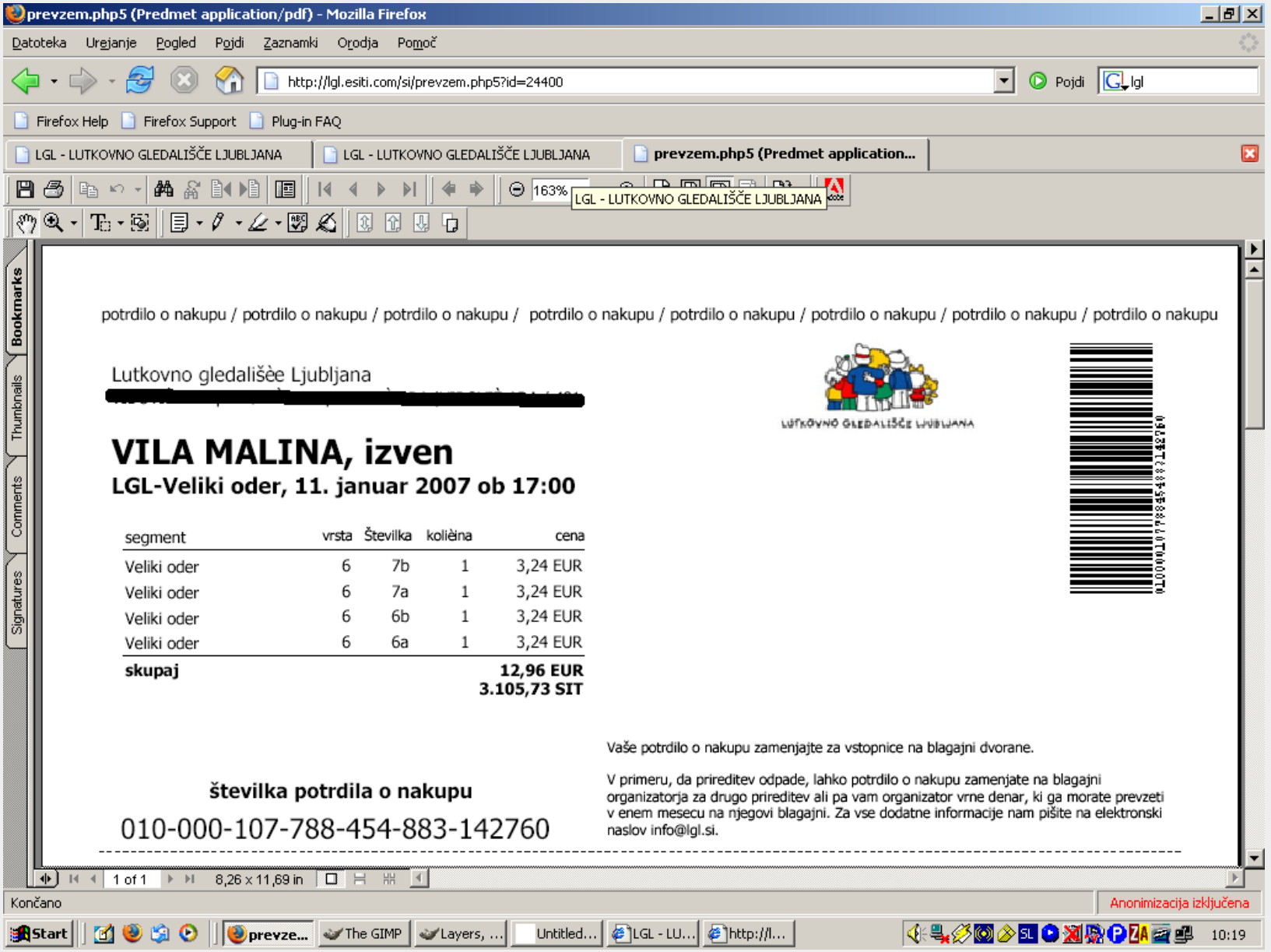
# Napadi preko spletnih aplikacij



# Napadi preko spletnih aplikacij



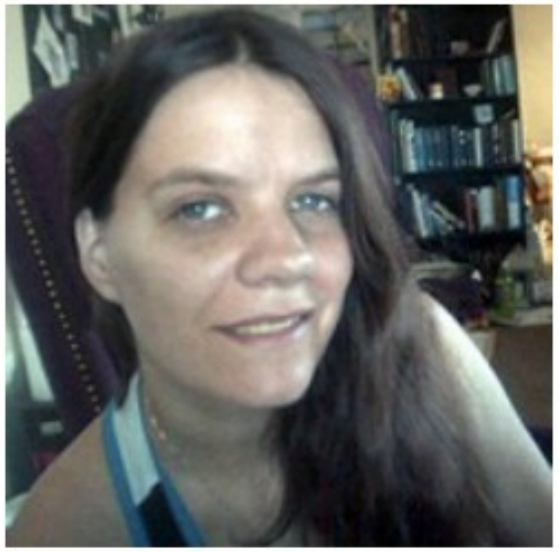
# Napadi preko spletnih aplikacij



# Napadi preko spletnih aplikacij

## Hackers embed flashing animations on epilepsy support forum

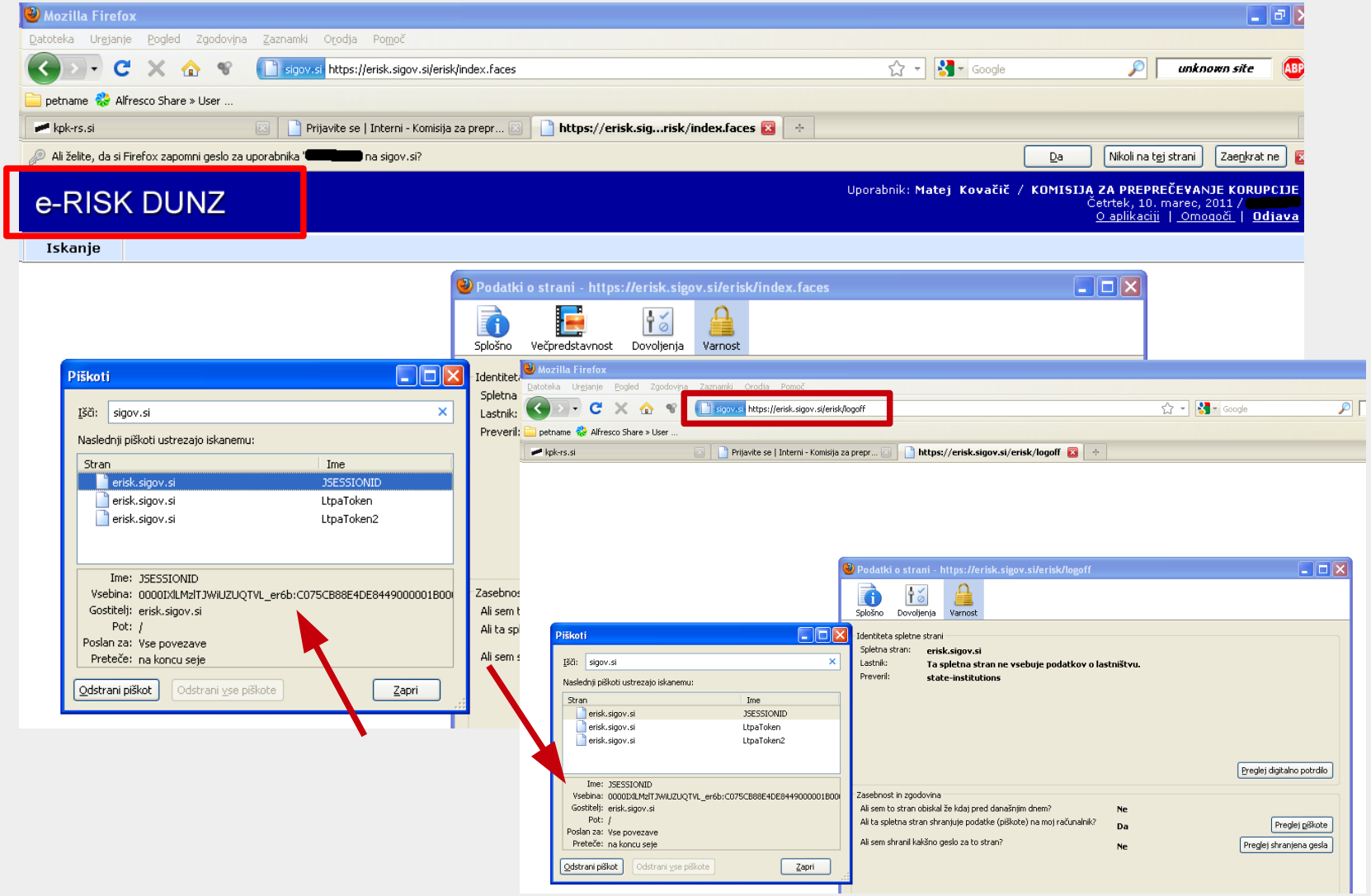
*By Darren Murph posted March 29th 2008 8:50PM*



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/

# Interne aplikacije...



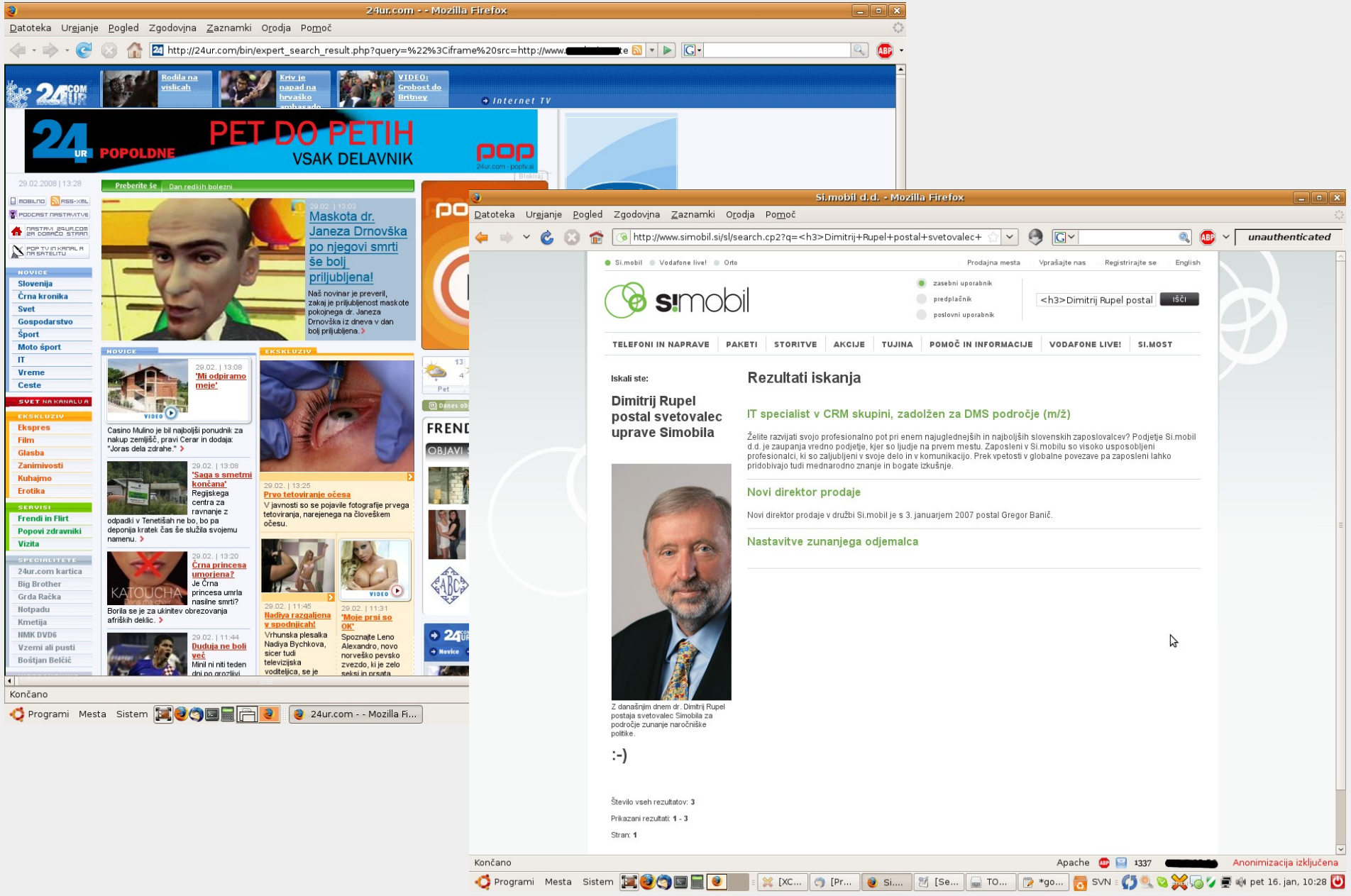
# Ali pa... :)

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.

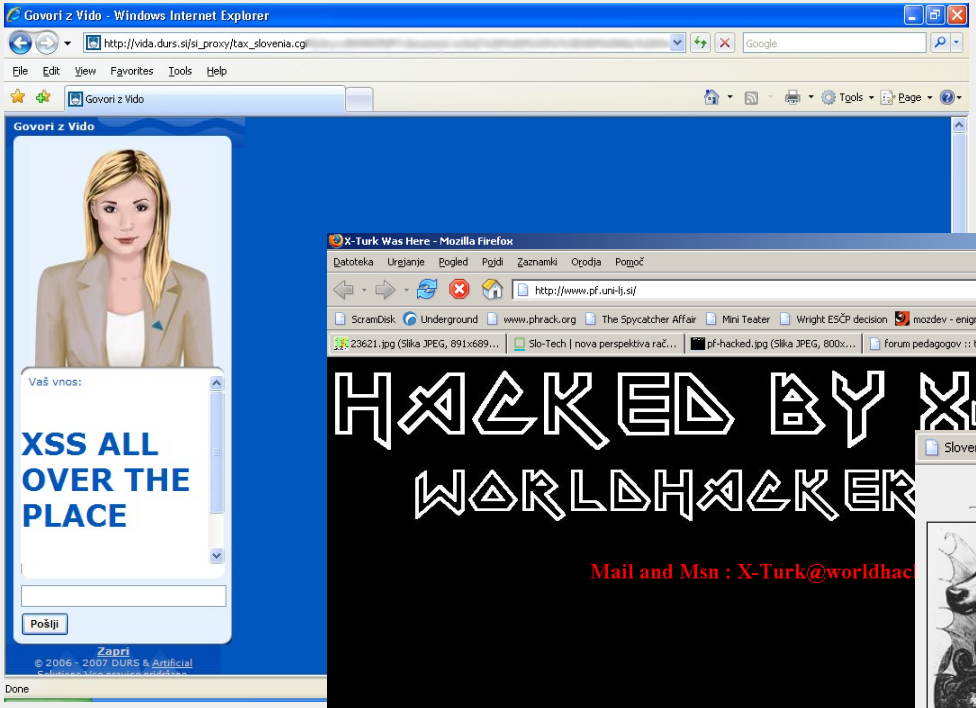
According to Assistant Chief Mike Allen, a fax was sent to the jail which stated "*Upon decision between Judge Rainey and the West Memphis Police Department CID Division Tristian Wilson is to be released immediately on this date of October 30, 2004 with a waiver of all fines, bonds and settlements per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

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

# Zaupanje vsebini na spletu?

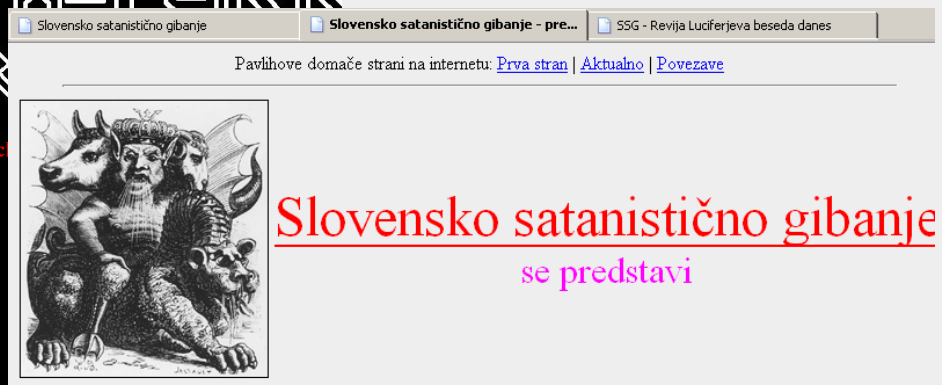


# Zaupanje vsebini na spletu?



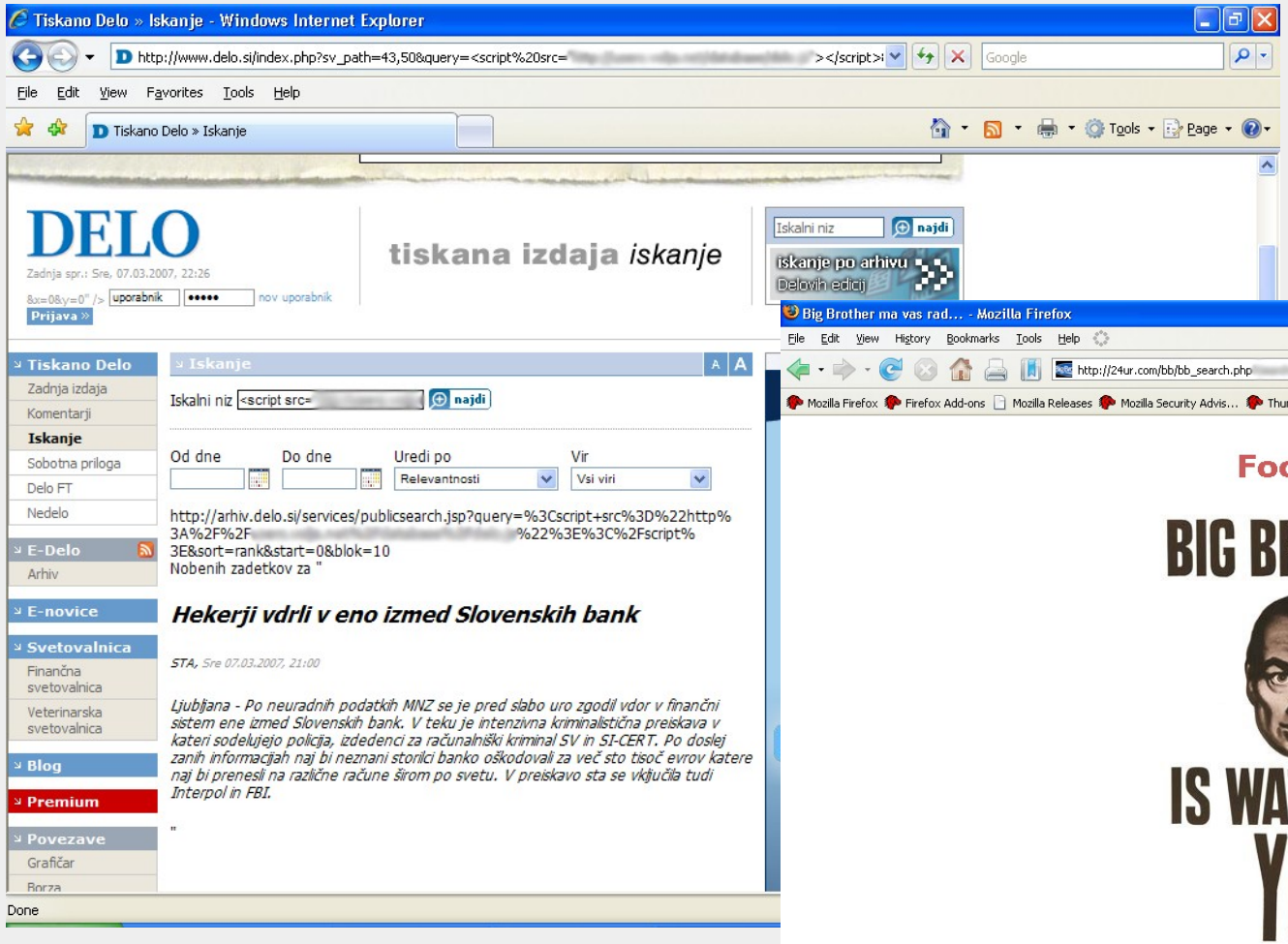

XSS napad na "davčno Vido".


Pravna fakulteta, Univerza v Ljubljani, februar 2007




Razobličenje spletne strani rimokatoliške cerkve.

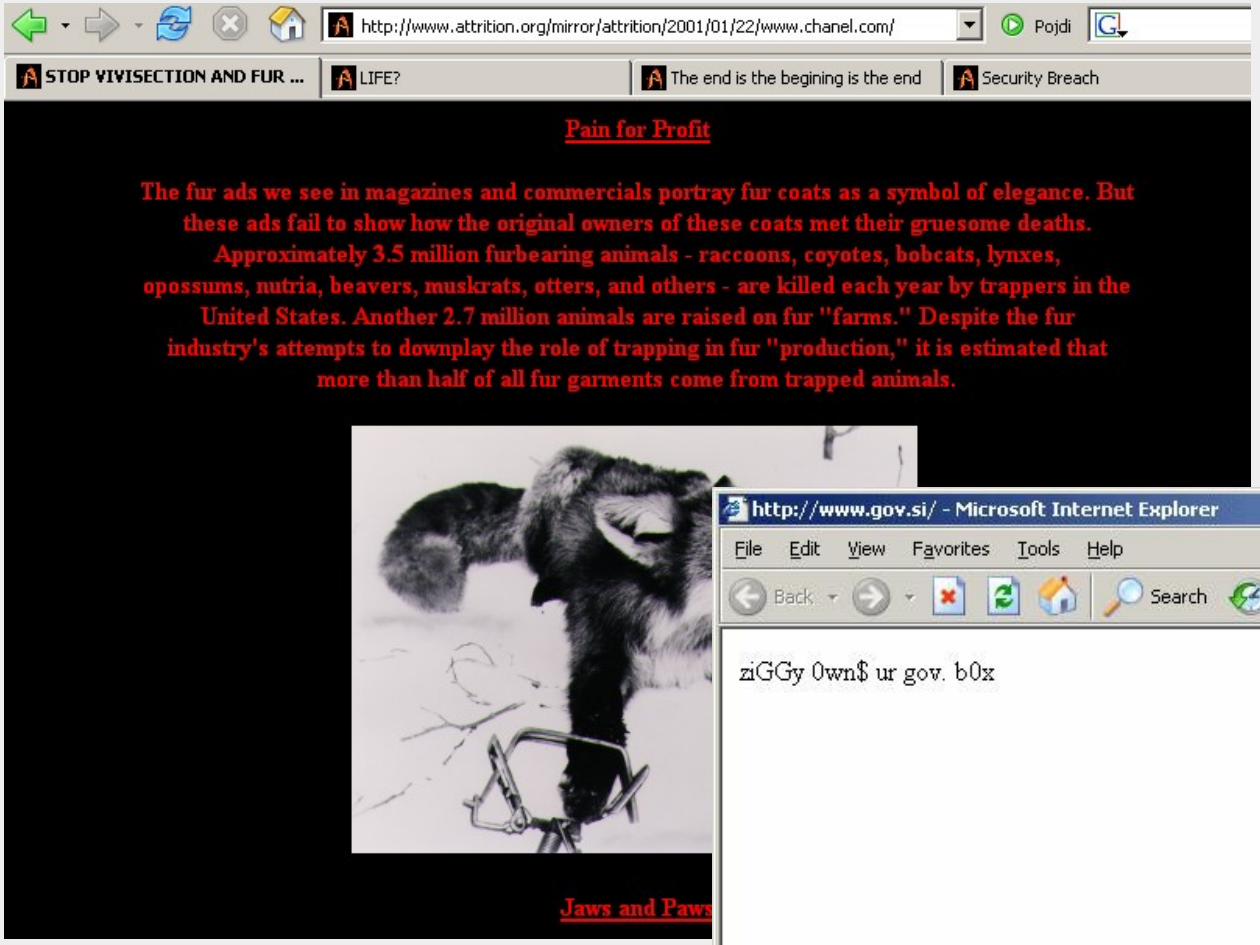
# Zaupanje vsebini na spletu?



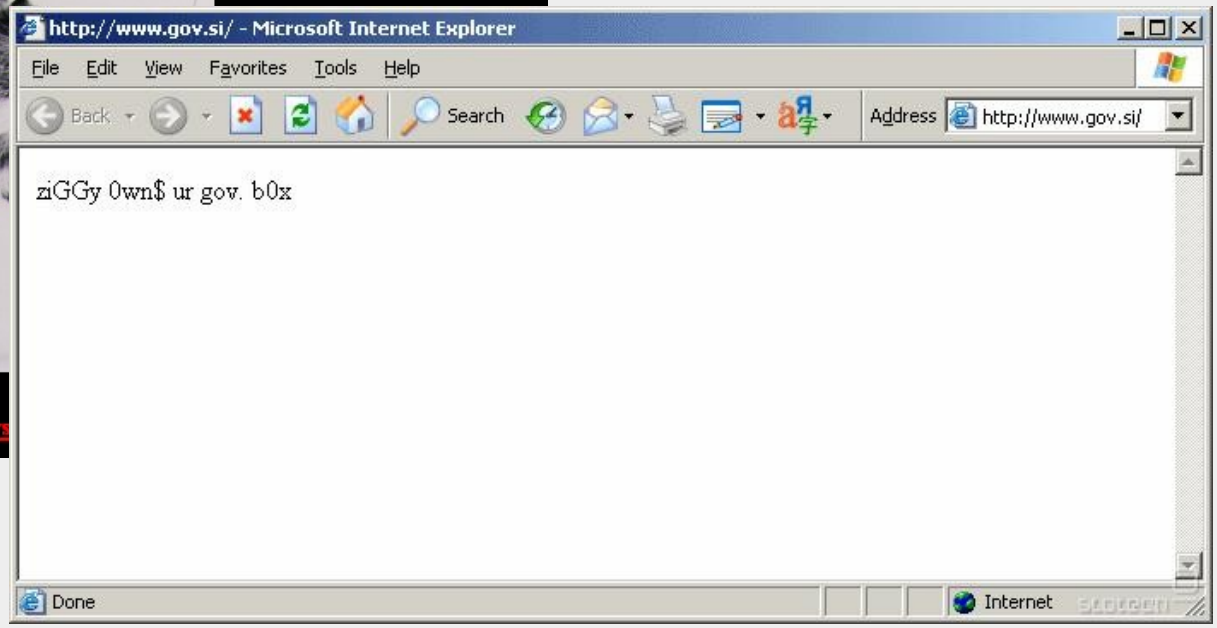

Lažna novica na spletni strani časnika DELO (XSS napad).


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

# Zaupanje vsebini na spletu?




Razobličenje spletne strani modne hiše Chanell.com




Razobličenje vladne strani (gov.si).

# 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;
- ...

# Gesla...



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.

# Ustrezna uporaba gesel?

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

`fuck.hackers`, `øhnøz` (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.

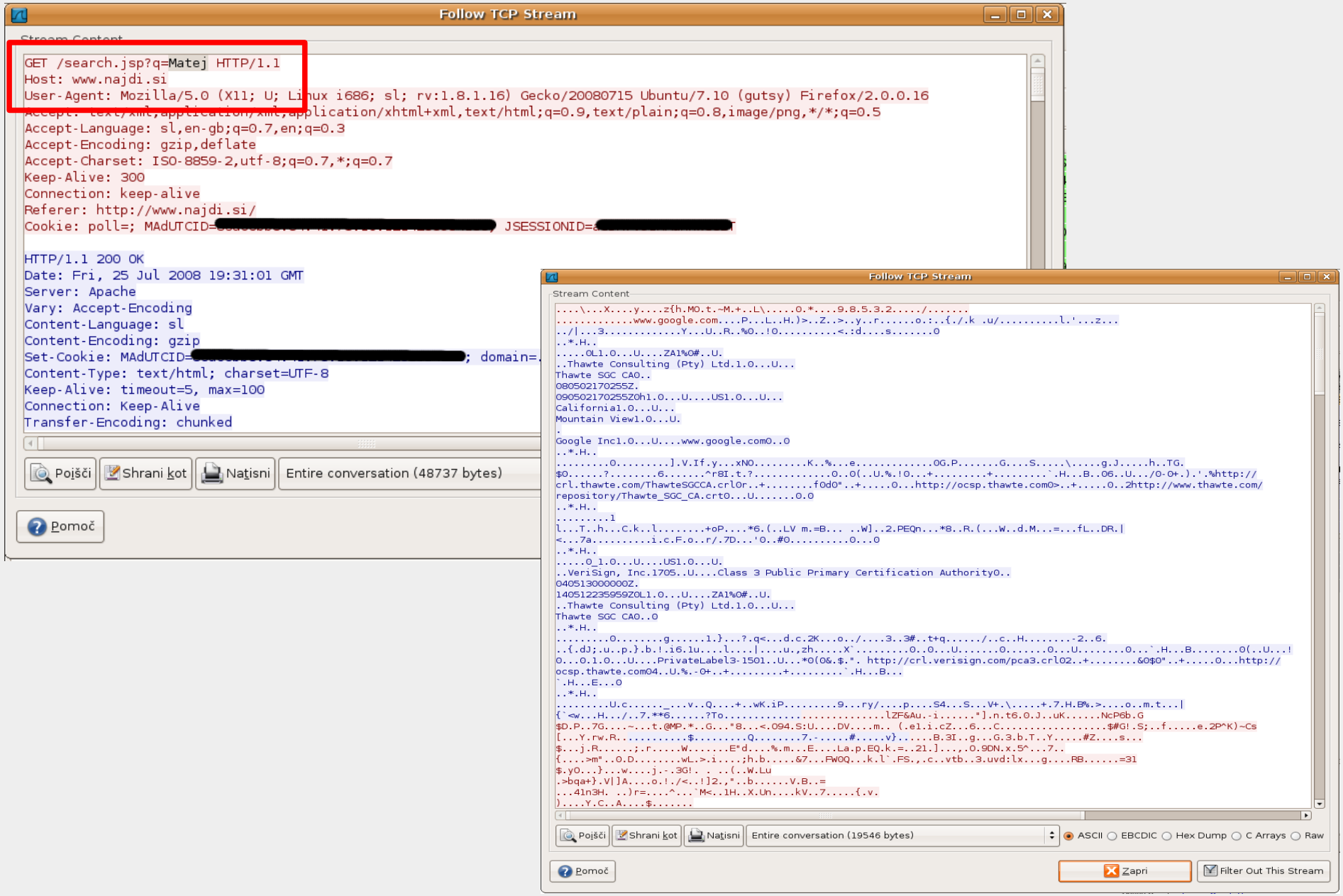
`https://sites.google.com/site/zeroforowned/dan-kaminsky-1`

# Naprednejša zaščita

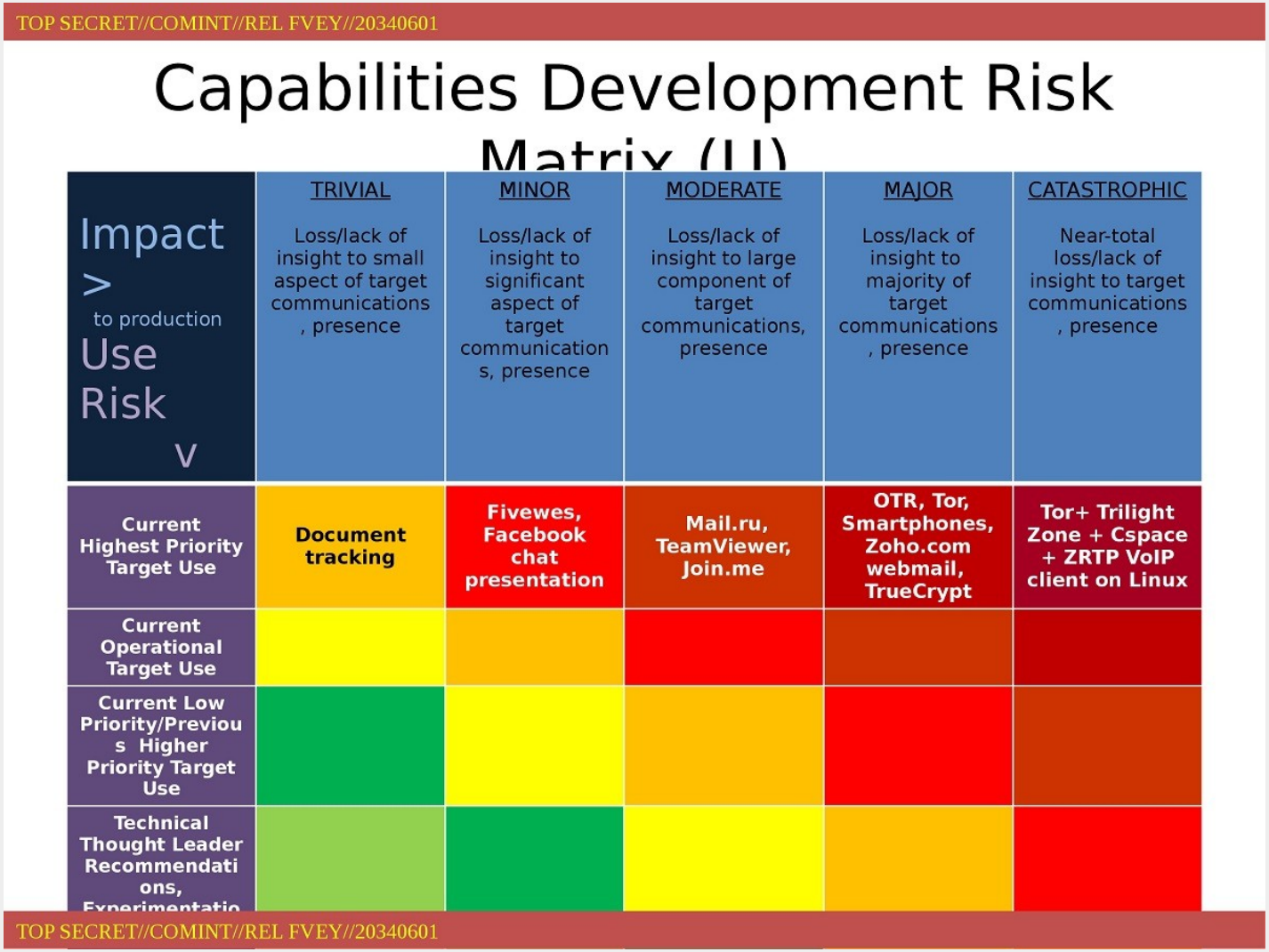
Nekatere tehnike naprednejše zaščite:

- **trajno brisanje podatkov**,
- **šifriranje** (*preprečimo dostop do vsebine*):
  - šifriranje nosilcev podatkov,
  - šifriranje elektronske pošte, neposrednih/hipnih sporočil, govorne in video komunikacije,
  - uporaba šifriranih povezav in protokolov (HTTPS,...),
- **anonimizacija** uporabe interneta (*preprečimo analizo prometnih podatkov*):
  - anonimizacijska omrežja,
  - "remailerji",
- **VPN**

# Zakaj šifiriranje?



# Šifriranje »priporoča« tudi NSA!



TOP SECRET//COMINT//REL FVEY//20340601

## Capabilities Development Risk Matrix (U)

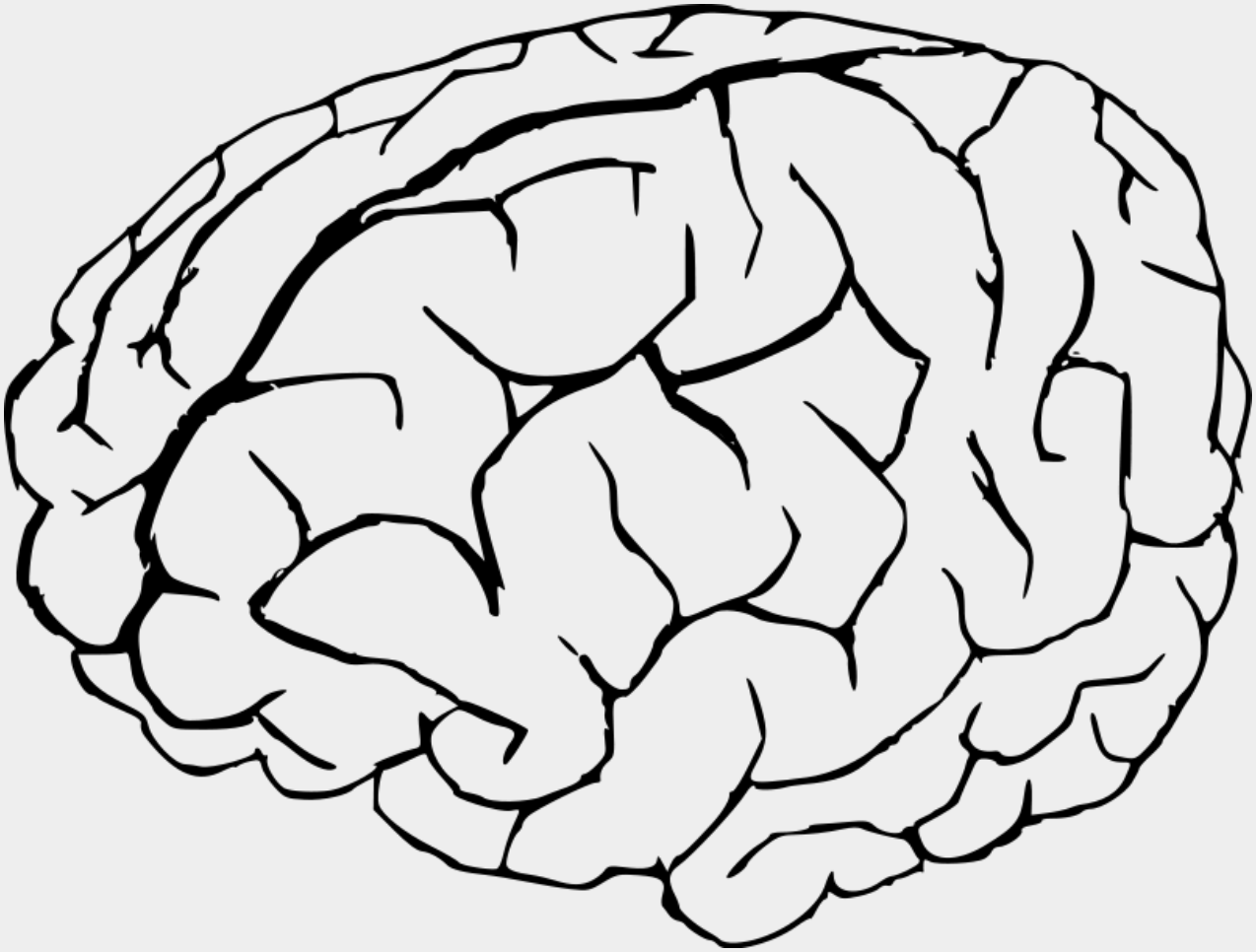
| Impact > to production Use Risk v | TRIVIAL<br>Loss/lack of insight to small aspect of target communications, presence | MINOR<br>Loss/lack of insight to significant aspect of target communications, presence | MODERATE<br>Loss/lack of insight to large component of target communications, presence | MAJOR<br>Loss/lack of insight to majority of target communications, presence | CATASTROPHIC<br>Near-total loss/lack of insight to target communications, presence |
|---|---|---|---|---|---|
| **Current Highest Priority Target Use** | **Document tracking** | **Fivewes, Facebook chat presentation** | **Mail.ru, TeamViewer, Join.me** | **OTR, Tor, Smartphones, Zoho.com webmail, TrueCrypt** | **Tor+ Trilight Zone + Cspace + ZRTP VoIP client on Linux** |
| **Current Operational Target Use** | | | | | |
| **Current Low Priority/Previous Higher Priority Target Use** | | | | | |
| **Technical Thought Leader Recommendations, Experimentatio** | | | | | |

TOP SECRET//COMINT//REL FVEY//20340601

Things become "catastrophic" for the NSA at level five - when, for example, a subject uses a combination of Tor, another anonymization service, the instant messaging system CSpace and a system for Internet telephony (voice over IP) called ZRTP. This type of combination results in a "near-total loss/lack of insight to target communications, presence," the NSA document states. (Der Spiegel)

# Še bolj napredna zaščita

Nekaj znanja, doslednosti in zdrava pamet. ;-)



# Primer phishing napada

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

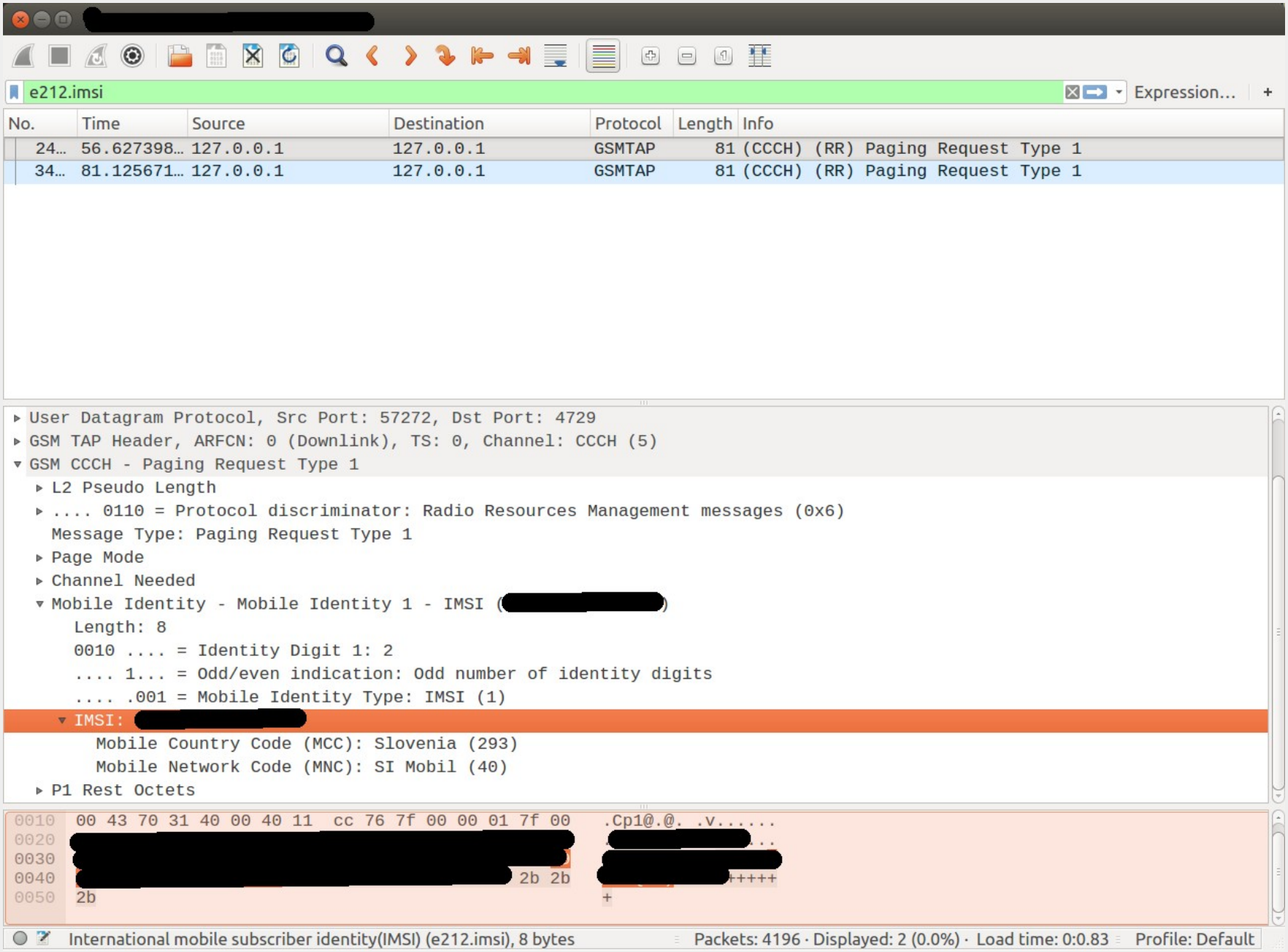
Napad na informacijsko-varnostno podjetje HBGary (podjetje je za ameriško vlado izvajalo "napade" proti skupini Anonymous).

...a little later:

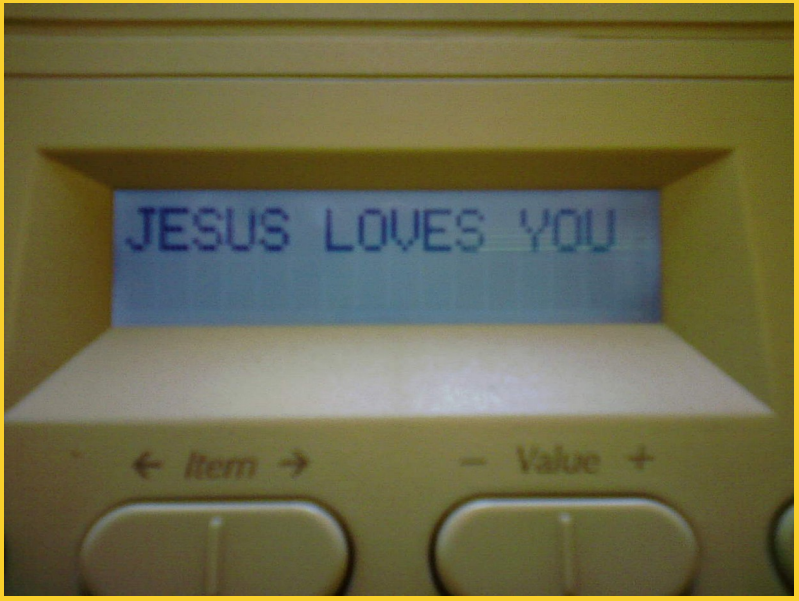
```
bash-3.2# ssh hoglund@65.74.181.141 -p 47152
[unauthorized access prohibited]
hoglund@65.74.181.141's password:
[hoglund@www hoglund]$ unset
[hoglund@www hoglund]$ unset HIST
[hoglund@www hoglund]$ unset HISTFLE
[hoglund@www hoglund]$ unset HISTFILE
[hoglund@www hoglund]$ uname -a;hostname
Linux 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
```

# Varnost mobilnih komunikacij

# Varnost mobilnih komunikacij



# Vprašanja...




**Matej Kovačič**
matej.kovacic@telefoncek.si

https://infosec-seminar.si

https://telefoncek.si