

Varnost informacijskih sistemov

(CC) 2019



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:

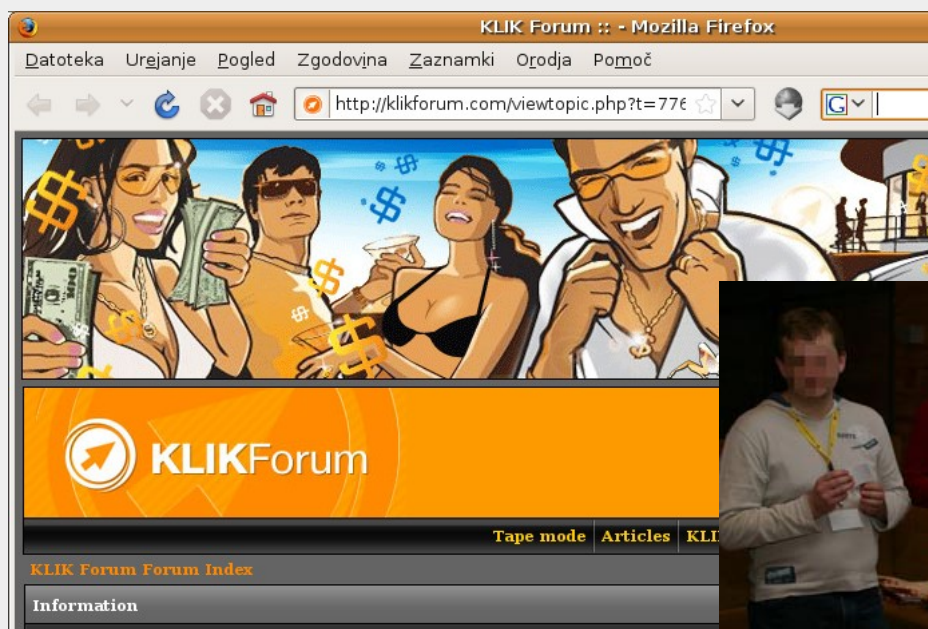
- raziskovanje,
- radovednost,
- samodokazovanje,
- zabava,
- vandalizem, ...



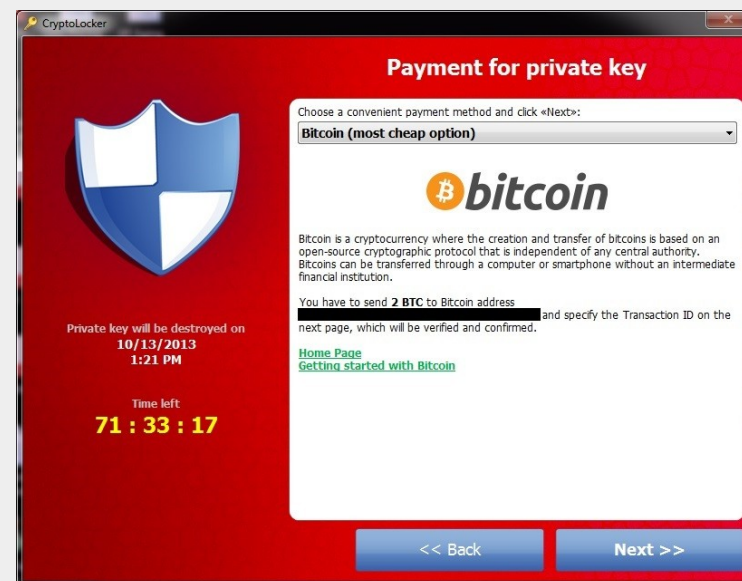
Kiberkriminal

Danes:

- posel in denar!



Spletna stran "podjetja".



Šifrirno-izsiljevalski virus Cryptolocker.



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

Nepooblaščen dostop do podatkov.

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

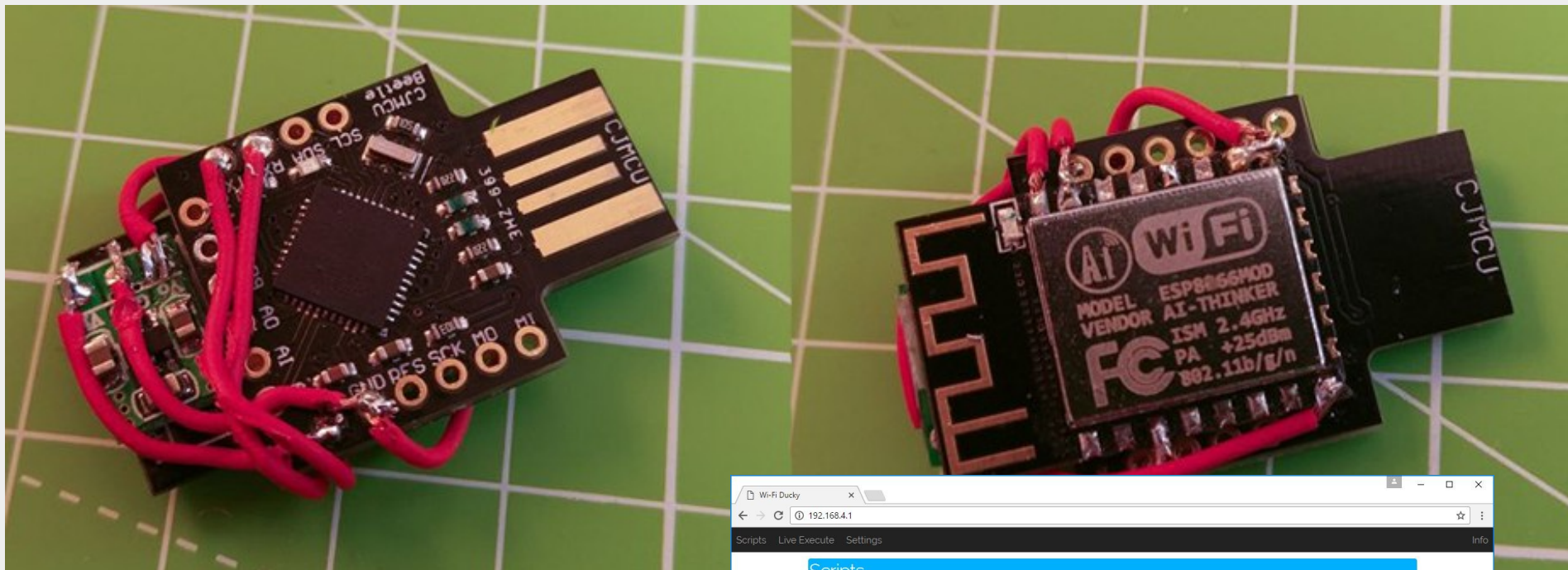
Zavržene računalniške komponente, ki vsebujejo nosilce podatkov (trdi diski, tiskalniki, mobilni telefoni,...).

Nameščanje aplikacij z »dvojno funkcijo«.

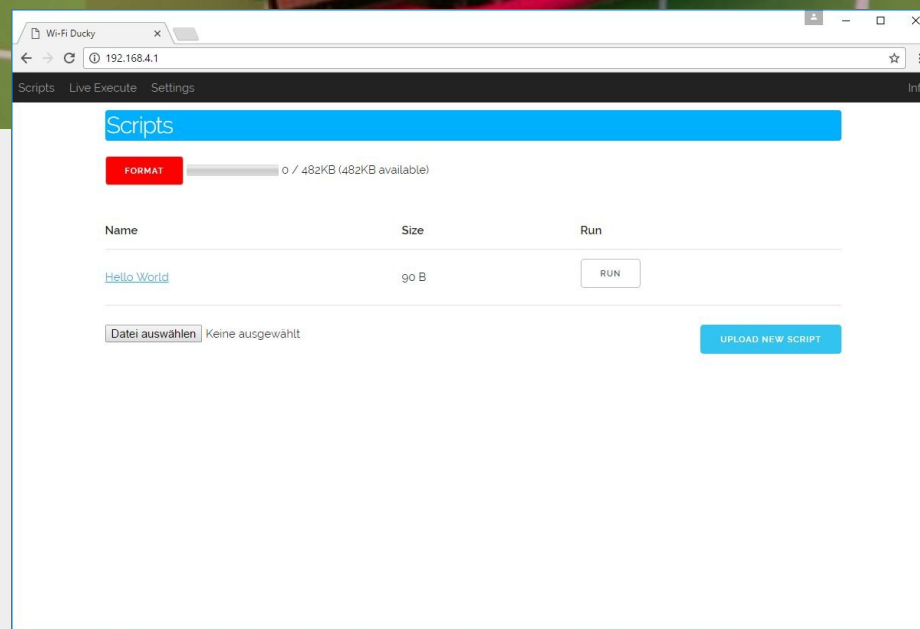
Priklapljanje neznanih naprav na sistem (najdeni USB ključki, »polnjenje« mobilnih telefonov,...)

Večuporabniška okolja (eskalacija privilegijev).

Navarni USB ključki



BadUSB z Wi-Fi podpora.

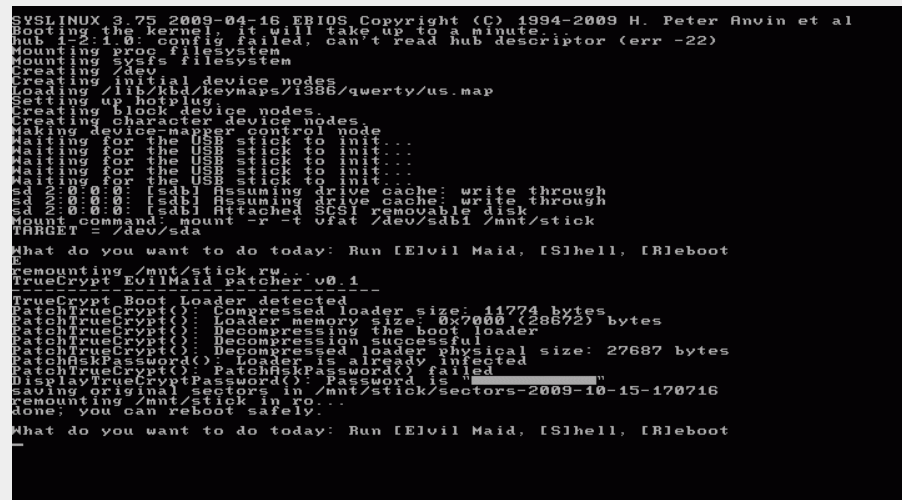


Upravljanje preko Wi-Fi.

Podtikanje prikritih mehanizmov



Programski prestrezniki tipkanja.



Evil Maid napad na TrueCrypt in...

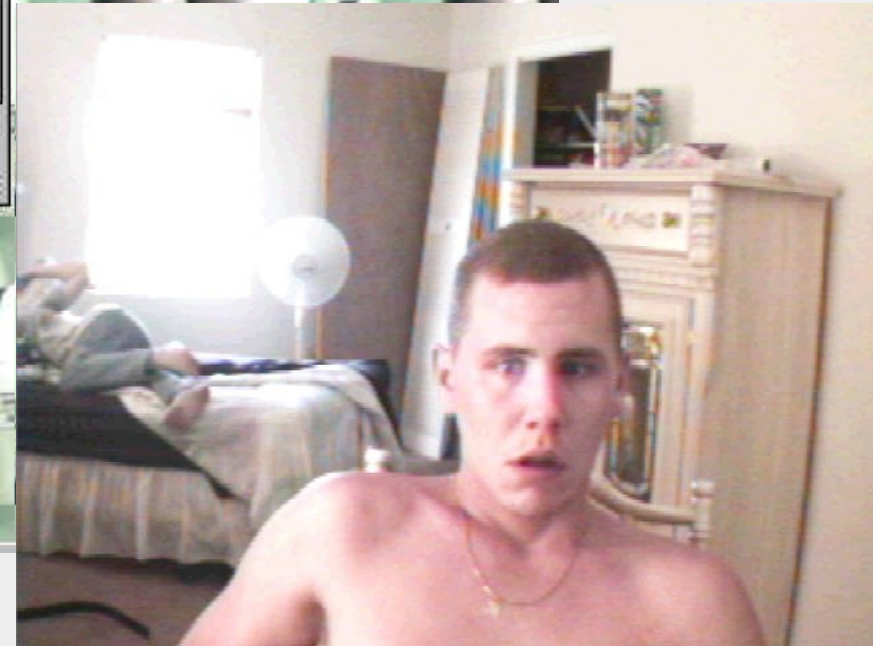
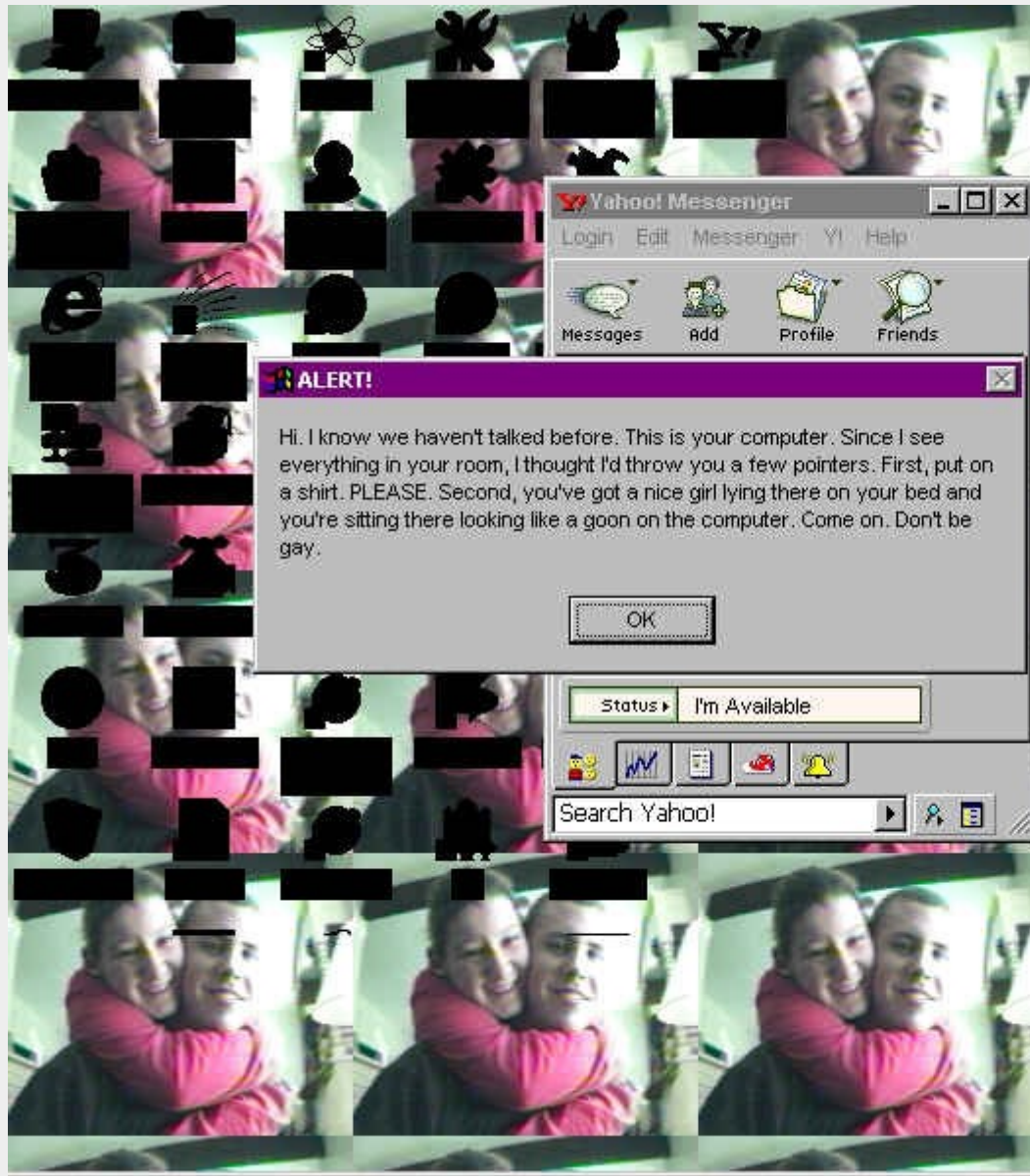


Strojni prestrezniki tipkanja.



...ostanki sirskega jedrskega reaktorja al-Kibar.

Posledice...



Ranljivi niso samo računalniki...



Ranljivi niso samo računalniki...

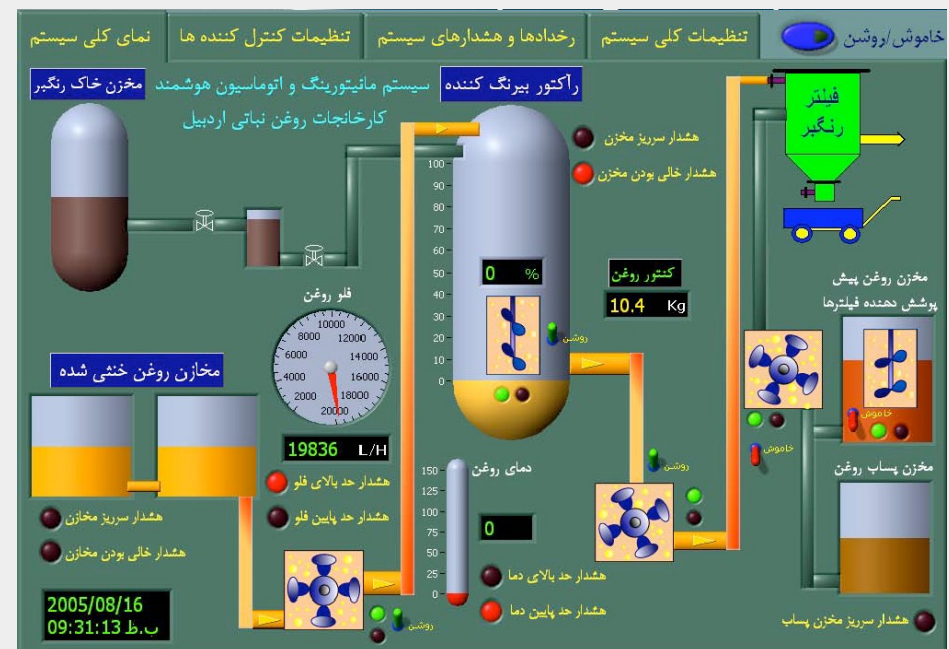
The screenshot shows a web browser window with the address bar displaying `http://10.254.60.43/index.html`. The main content area shows the **Tenovis WebTerminal** interface, which includes a **WebTerminal** section with a PIN input field (displayed as `****`) and a **Status** of `Connected`. Below this is an **Abort** button. A **T3IP WebTerminal : mainmenu** overlay is visible, displaying system information: **Own call number: 5711**, **MAC address: 00-04-0d-f5-09-6a**, **Application file: T112_Sp3.bin**, and **Boot- file: T100**. It also features buttons for **Bootline**, **Registration & admission**, and **IP audio settings**, along with a **Status** field showing `Data unc...`. At the bottom of the overlay, it states **VoIP Manager active: Configuration access limited!** and includes **Send data** and **Cancel** buttons. A terminal window titled **matej@cryptopia: ~** is open, showing the command `nmap 10.254.60.43` and its output: `Starting Nmap 5.21 ( http://nmap.org ) at 2010-11-...`, `Nmap scan report for 10.254.60.43`, `Host is up (0.0014s latency).`, `Not shown: 999 filtered ports`, `PORT STATE SERVICE`, `80/tcp open http`, and `Nmap done: 1 IP address (1 host up) scanned in 5.4...`. The browser's status bar at the bottom shows **Applet started.**, **Retrieving your IP address...**, and **Anonimizacija izključena**.

Napad na VOIP telefon.

Ranljivi niso samo računalniki...

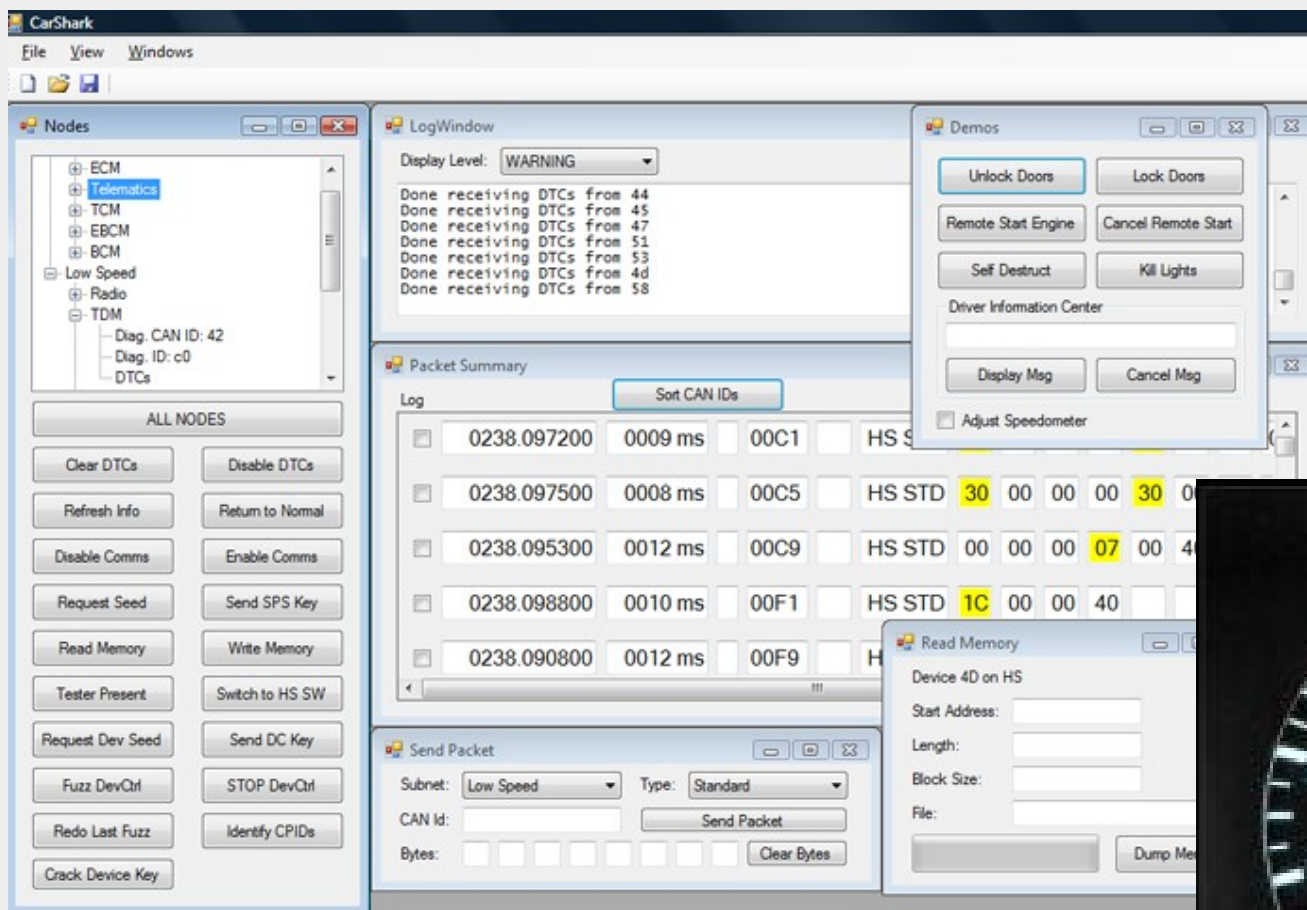


Napadi na RFID potne liste.



Napadi na SCADA sisteme.

Ranljivi niso samo računalniki...



Napadi na avtomobile.



Ranljivi niso samo računalniki...

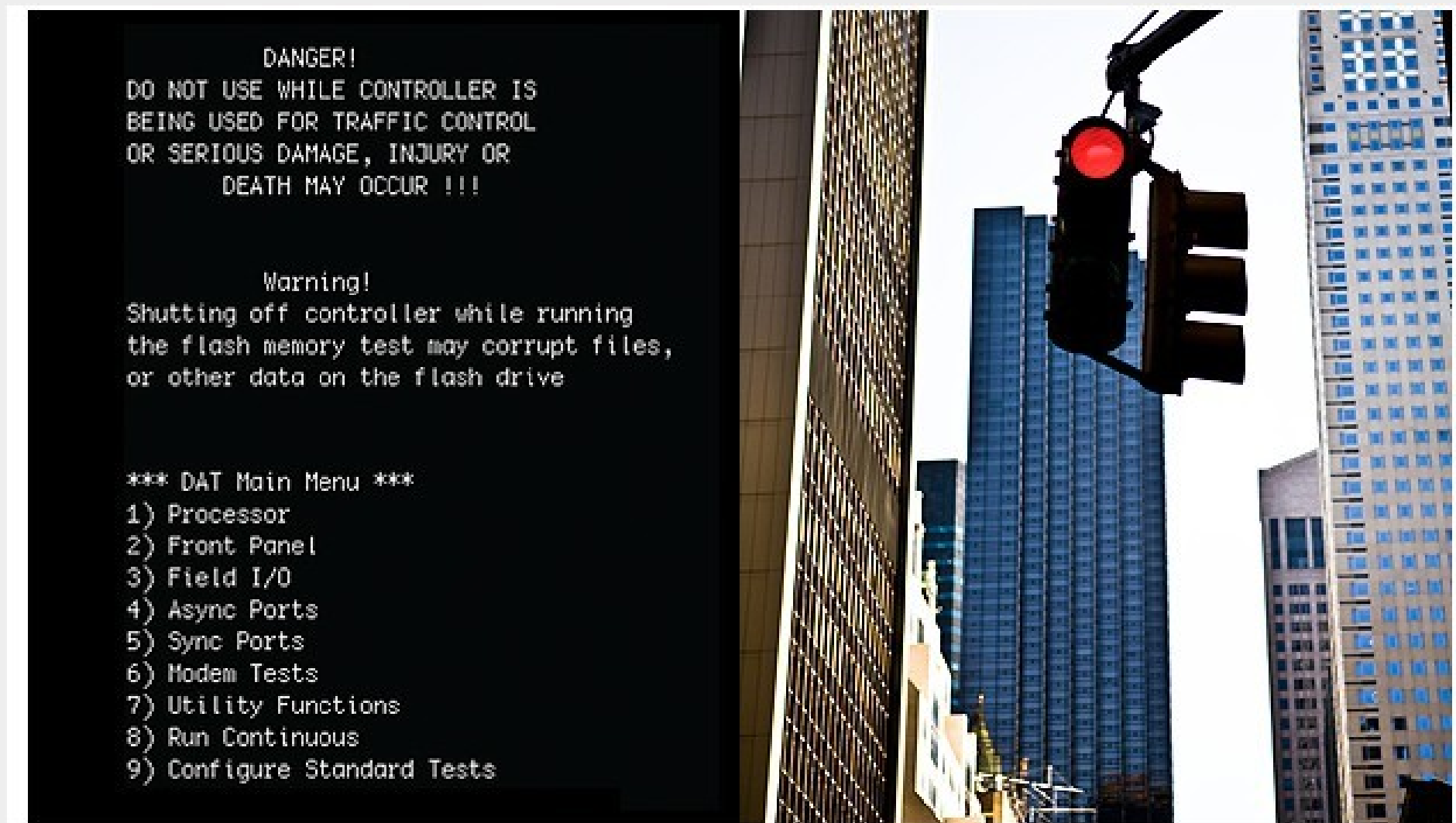


foto: Dan Tentler.

Prestrezanje komunikacij

The image displays two windows from a network analysis tool, Wireshark, and a VoIP RTP Player.

Wireshark Window (sip.pcap - Wireshark):

- Filter:** sip
- Table:**

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

Packet Details (Frame 82):

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

Packet Bytes:

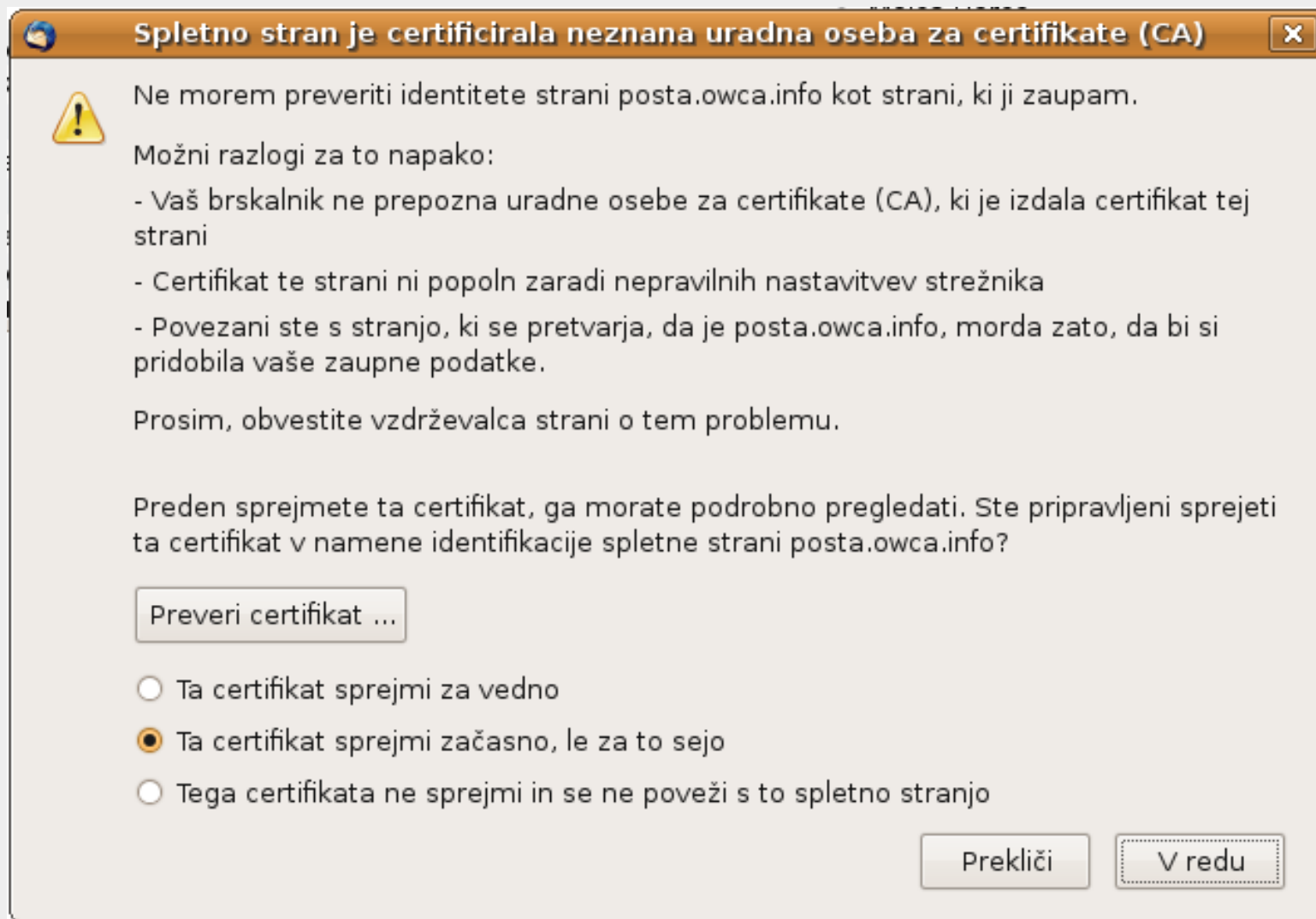
Offset	Hex	ASCII
0000	00 18 73 a3 4e 48 00 15 af e5 25 c8 08 00 45	
0010	04 b5 00 00 40 00 40 11 5f 95 99 05 85 5b d4	
0020	e4 34 13 c4 13 c4 04 a1 de c4 49 4e 56 49 54	
0030		
0040		
0050		
0060	20 32 38 20 4d 61 79 20 32 30 30 39 20 31 32	
0070	32 36 3a 35 31 20 47 4d 54 0d 0a 43 53 65 71	
0080	20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

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

VoIP RTP Player Window (sip_govor.pcap - VoIP - RTP Player):

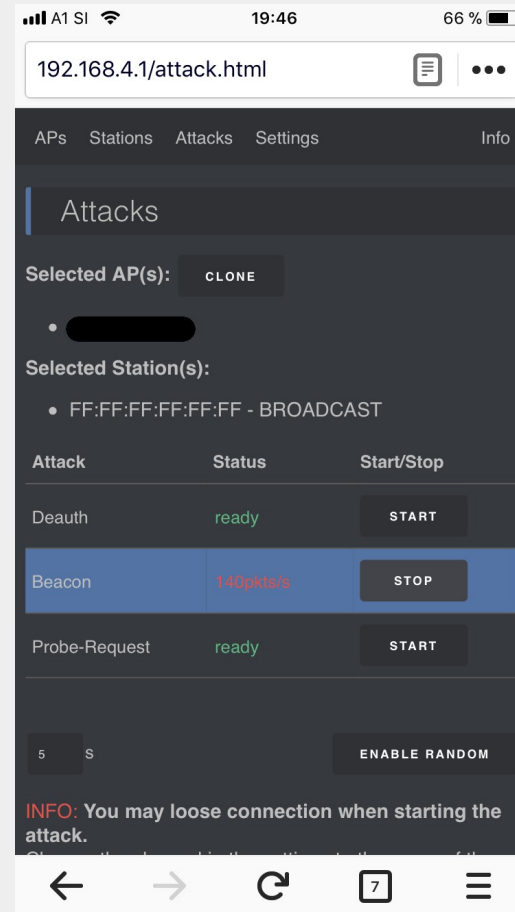
- Audio Waveform:** Shows two audio segments. The first segment is from 14 to 21 seconds, and the second is from 14 to 21 seconds. Both segments show a green background with a black waveform.
- Duration:** 11.76 (Drop by Jitter Buff: 0(0.0%) Out of Seq: 0(0.0%))
- Duration:** 12.04 (Drop by Jitter Buff: 0(0.0%) Out of Seq: 1(0.2%))
- Controls:** jitter buffer [ms] 50, Decode, Play, Pause, Stop, Zapri.

Prestrezanje komunikacij



Previdno pri sprejemanju neznanih digitalnih potrdil!

Wifi omrežja?



Zbiranje javnih (?) informacij

uni-lj.si - Iskanje Google - Mozilla Firefox

Datoteka Urejanje Pogled Zgodovina Zaznamki Orodja Pomoč

http://www.google.si/search?hl=sl&client=firefox-a&rls=com.ubuntu%3Asl%3Au

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

Google

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

Išči po: ☒ celotnem spletu ☐ straneh v državi Slovenija

Splet

[xLS] [Ocene 08](#)
Oblika datoteke: Mid
Ocene dne 22.4.2008
10 točk, Preizkušnja
_dok

[xLS] [Ocene redni](#)
Oblika datoteke: Mid
Ocene redni_EJS_1
periodika, seminar,
_dok

[xLS] [OCENE](#)
Oblika datoteke: Mid
2, STUDENT ID, soc
40 točk, SKUPAJ, C
_dok

[xLS] [Sheet1](#)
Oblika datoteke: Mid
6, 19440552, 100. 7
19454945, 20. 12, 19
_dok

[Podobne strani](#)

[xLS] [Sheet1](#)
Oblika datoteke: Mid
4, 10.11. 5, 1939850
19453361. 11, 19454
_dok

[Podobne strani](#)

[xLS] [Sheet1](#)
Oblika datoteke: Mid
8, 19452140, 50. 9,
19455168, 100. 14,
_dok

[Podobne strani](#)

ocene_april_pr (samo za branje) - OpenOffice.org Calc

Datoteka Uredi Pogled Vstavi Oblika Orodja Podatki Okno Pomoč

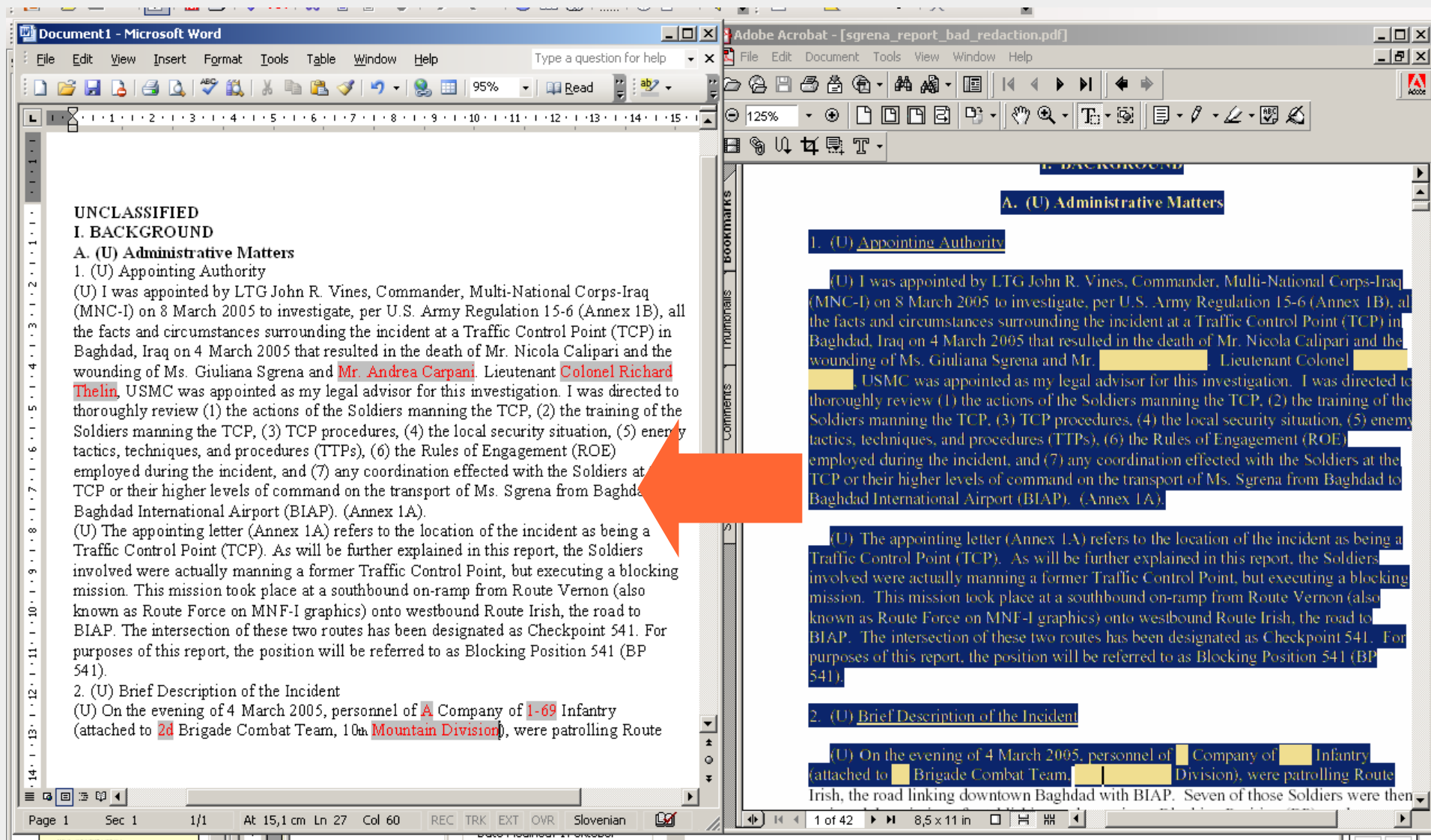
B2 $f(x)$ Σ = Vpis_st

	A	B	C	D	E	M	N	O	P
1			TRŽENJE V TRGOVINI NA DROBNO Letni semester 2008 Ocene dne 22.4.2008						
2		Vpis st	analiza gosta 1 10 točk	analiza gosta 2 10 točk	Preizkušnja 30 točk				
3		19326554			13,5				
4		19398834	5		16,5				
5		19401312	7,5	6	25,5				
6		19401331	6	7	25,5				
7		19401473	7,5	10	25,5				
8		19401806							
9		19402546	8	9	24				
10		19404113			21				
11		19405597	9	8	21				
12		19405690	5		22,5				
13		19405760	9	8	15				

Ocene 08 / PODPISI / Seznam studentov 2

Delovni list 1 / 3 PageStyle_Ocene 08 STA Vsota=0

Zbiranje javnih (?) informacij



Document1 - Microsoft Word

File Edit View Insert Format Tools Table Window Help Type a question for help

95% Read

UNCLASSIFIED

I. BACKGROUND

A. (U) Administrative Matters

1. (U) Appointing Authority

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

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

2. (U) Brief Description of the Incident

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

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

Adobe Acrobat - [sgrena_report_bad_redaction.pdf]

File Edit Document Tools View Window Help

125%

I. BACKGROUND

A. (U) Administrative Matters

1. (U) Appointing Authority

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

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

2. (U) Brief Description of the Incident

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

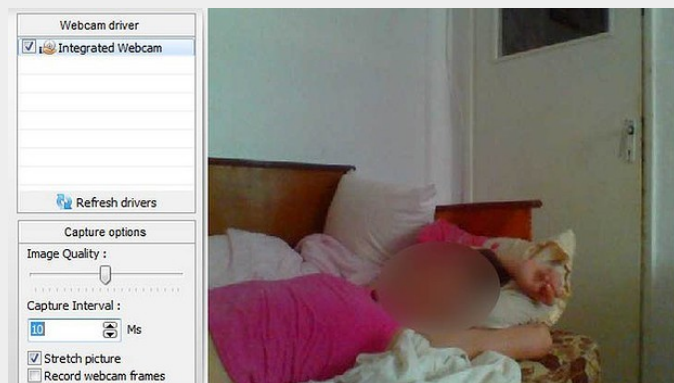
1 of 42 8,5 x 11 in

Zbiranje javnih (?) informacij



22.5.2008 11:27:31.514
Nočni trezor

Zbiranje javnih (?) informacij



← → ↺ ↻ 212 [redacted] eb/guest/en/websys/webArch/mainFrame.cgi

RICOH MP C4503 Web Image Monitor

← Home

Print Job List

Back

Print Delete

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

[redacted] SARA. Spol: Datum roj.: z. [redacted] imek 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.

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...39.pdf

1 of 1

100%

RAČUN ŠT: 1...39

Sklic na: _____
Jesenice, dne: 04.03.2019 10:19
Datum valute: 18.03.2019
Datum opravljene storitve: 04.03.2019 10:19

Vesna _____

Tel: _____ ID za DDV: _____
Kontakt: _____

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

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

Browser address bar: [https://portia-erotica.com/wp-admin/post.php?post=\[REDACTED\]&action=edit](https://portia-erotica.com/wp-admin/post.php?post=[REDACTED]&action=edit)

Page header: Portia Erotica sex shop 14 Nov Kallyas Options Živjo, sexadm

Left sidebar menu:

- Custom Product Tabs
- Documentation Items
- Page Layouts
- Page Builder Smart Areas
- AddThis
- MA Connector
- PixelYourSite
- Store Manager Connector
- All Export
- All Import
- Zendesk Chat
- Kallyas Theme Dashboard
- Loco Translate
- Easy Forms

Main content area:

Plačnik
Andraž [REDACTED]
[REDACTED]
[REDACTED]
Telefon: [REDACTED]
E-poštni naslov: [vroca-nina](#) [REDACTED]

Dostava
[REDACTED]
[REDACTED]
[REDACTED]
Strankina opomba:
Paketomat

Izdelek	Cena	Količina	Znesek	DDV 22%
 KISS-209 - 14 Šifra: KISS209/BP/M ID različice: 53764	€ 84,23	× 1	€ 84,23	€ 18,53
 Pleated Mini Skirt - L Šifra: OR-27700671041 ID različice: 163522	€ 29,95	× 1	€ 29,95	€ 6,59
 Hold-up Stockings - L Šifra: OR-25204601041	€ 15,95	× 1	€ 15,95	€ 3,51

Hvala za potrditev... novi znesek za plačilo 238,06 eur + naročilo iz portia-shop (majica) 4,50 = 280,10 eur za nakazilo .
Hvala

dodano [REDACTED] od irenap [Izbrišite opombo](#)

Pozdravljeni, sporočamo vam da je žal replika penisa COLT IUKE pri nobenem dobavitelju ni nedobavljiv in ga ni možno več dobiti. Priporočamo vam <https://portia-erotica.com/shop/lovetoy/s/dildos/king-cock-cock-10-inch-with-balls-flesh/>
PROSIM POTRDITE SPREMEMBO.
OZIROM NAS LAHKO TUDI PIKLIČIT
[REDACTED]

dodano [REDACTED] od irenap [Izbrišite opombo](#)

Zadržana Bančna nakazila Stanje naročila spremenjeno iz Plačilo v teku v Zadržano.

dodano [REDACTED] [Izbrišite opombo](#)

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

POTRDILO O IZVRŠENIH PLAČILNIH TRANSAKCIJAH

PLAČNIK
Naziv:
Naslov:

Eva

Račun:
Referenčna številka:
Banka:
Naziv banke:

SI56
SI99
BAKOSI2X
BANKA INTESA SANPAOLO D.D.

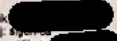
PLAČILNI NALOG
Številka transakcije:
Vrsta:
Nujnost:
Način plačila:
Datum prejema naloga:
Datum obremenitve računa:
Znesek:
Nadomestilo:
Znesek nadomestila:
Koda namena:
Namen:
Status SEPA:
Plačnik stroškov:

Plačilni nalog
Ne nujno
Mobilna BankaIN
13.03.2019
13.03.2019
60,00 EUR
Nalog do 50.000 EUR na drugo banko - Banka IN
0,40 EUR
OTHR
Članarina 2019 - Eva
SP01
Oba (SHA)

PREJEMNIK PLAČILA
Naziv:
Naslov:
Naslov:
Račun:
Referenčna številka:
Banka:
Naziv banke:

DRUŠTVO PSIHOLOGOV SLOVENIJE
TRG PREKOMORSKIH BRIGAD 1
1000 LJUBLJANA
SI56 6100 0001 5938 417
SI002019
HDELSI22
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, d.ž. l. reg. vpisa: 1/00490/00, osnovni kapital: 22.173.218,16 EUR, BIC: BAKOSI2X, poravnalni rač. un: SI56 0100 0000 1000 153.

Podpisnik
Izdajatelj: 
Številka certifikata
Potek veljavnosti
Čas podpisa: 05. 10. 2019



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

1433 RADEČE

Številka: 

Datum: 2018

Zveza:

Obrazec: PotrdiloOPrijavi.dobx

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

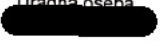
Oseba  (a)  stanujoč(a)  vodi v evidenci brezposelnih oseb pri Zavodu Republike Slovenije za zaposlovanje.

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).



Uradna oseba




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

← → FDV www.fdv.uni-lj.si/Kontakti/telefonski_imenik.asp ☆ ↻ Google

 **Fakulteta za družbene vede**
Univerza v Ljubljani

SPLETNI REFERAT URNIKI PEDAGOGI PREDMETI PROGRAMI KLUB DIPLOMANTOV



Kontakti

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

TELEFONSKI IMENIK
A B C Č D Đ E F G H I J K L M N O P R S Š T U V Z Ž
V primeru nejasnosti ali informacije pokličite **5805-100**

	Prilimek 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 Po

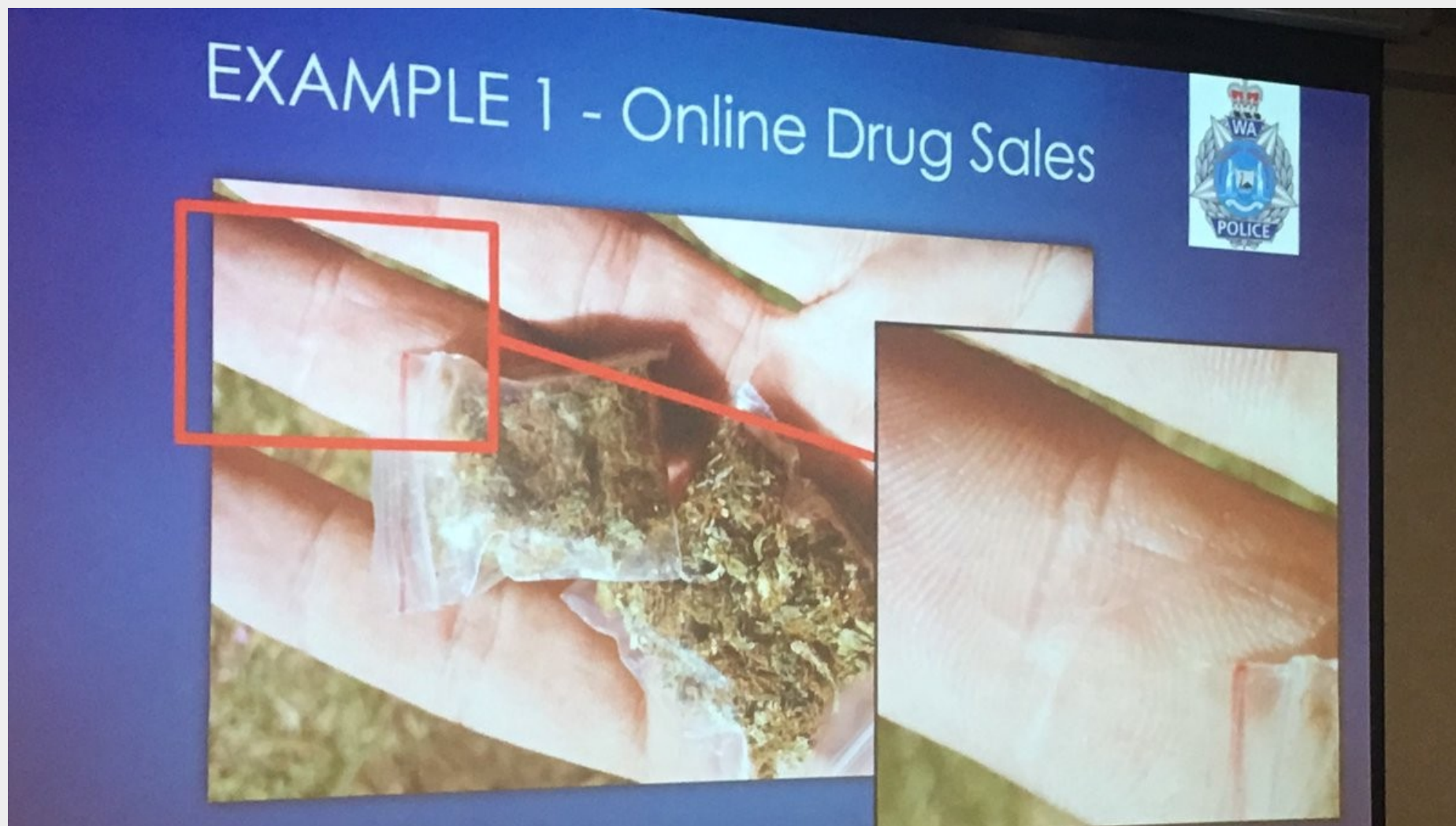
Arial 10

A1 f(x) Σ = Priimek in ime

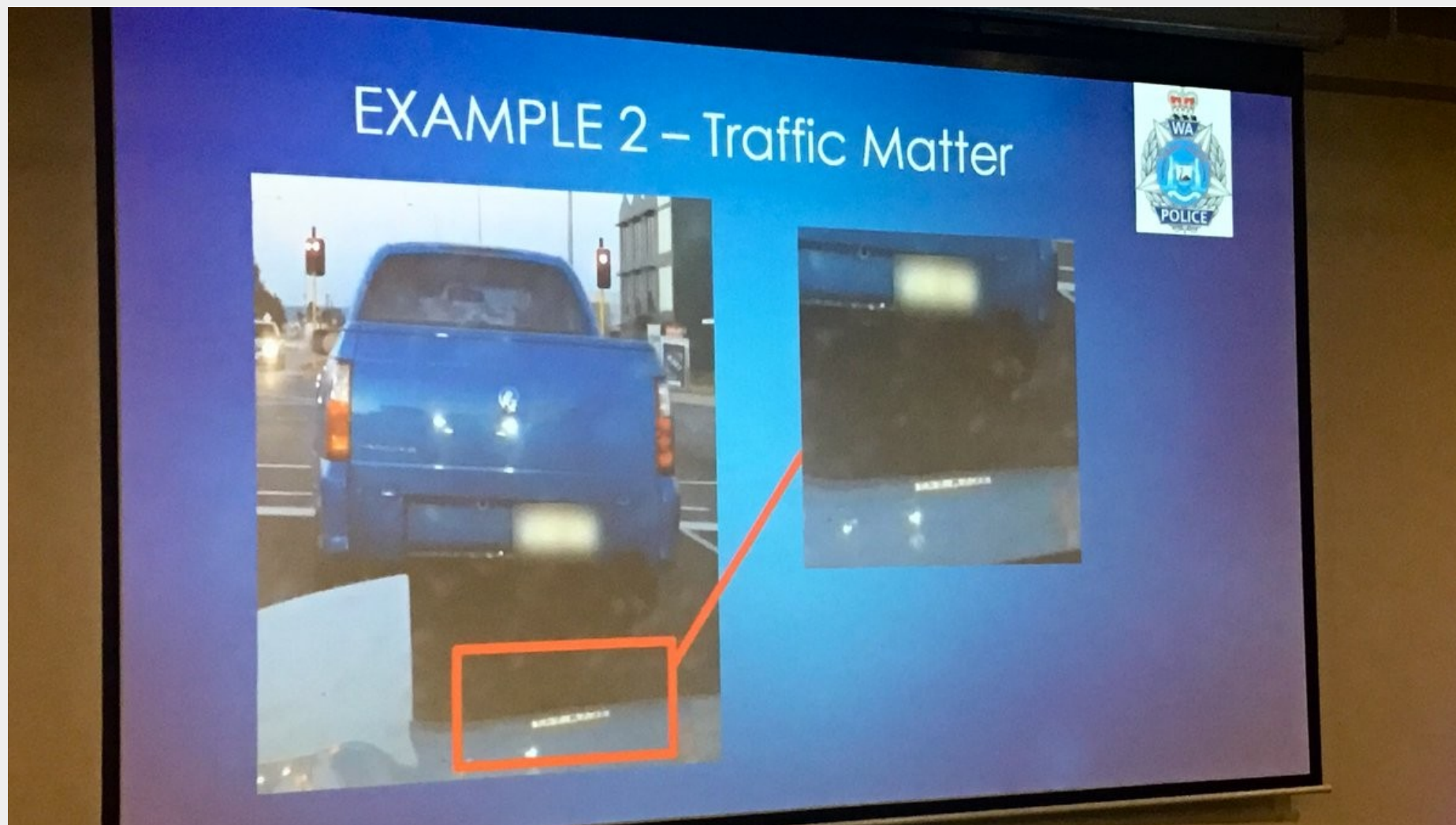
	A	B
239	UHAN dr. Samo	296
240	VEHOVAR dr. Vasja	297
241	TOŠ dr. Niko	298
242	GREGORČIČ dr. Marta	299
243	VELIKONJA dr. Mitja	299
244		300
245	BERNIK dr. Ivan	301
246	JOGAN dr. Maca	302
247		303
248	KOS dr. Drago	304
249	DIMC Neli	305
250	MALI dr. Franc	306
251	MENCIN-ČEPLAK dr. Marjeta	307
252	MIHELJAK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

Delovni list 1 / 3 Privzeto STA Vgota=0

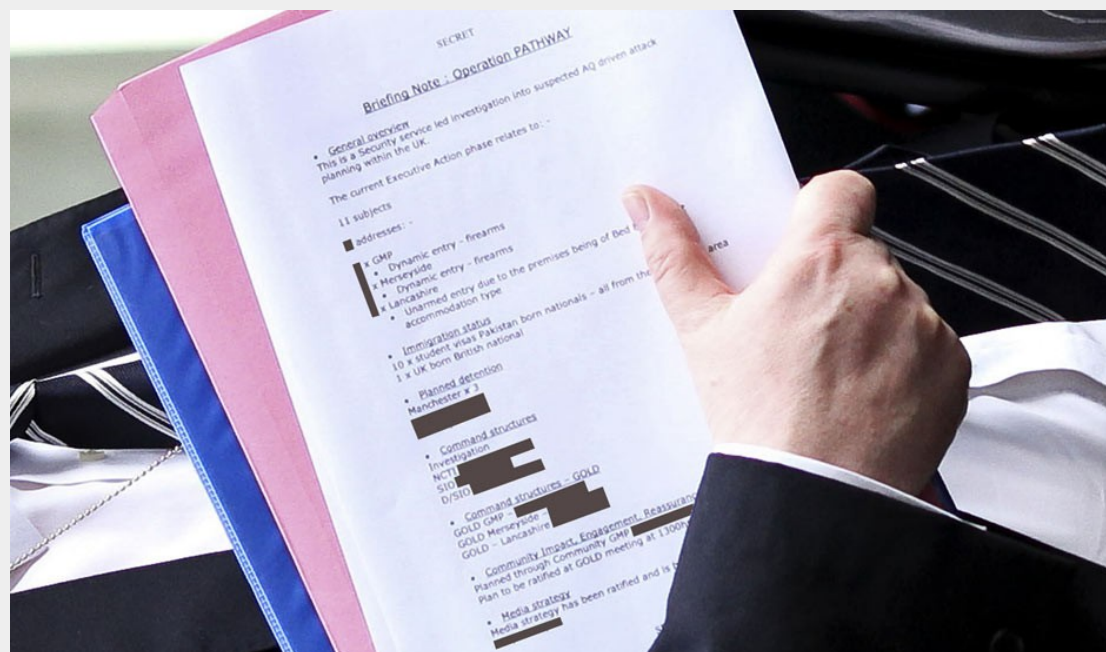
Zbiranje javnih (?) informacij



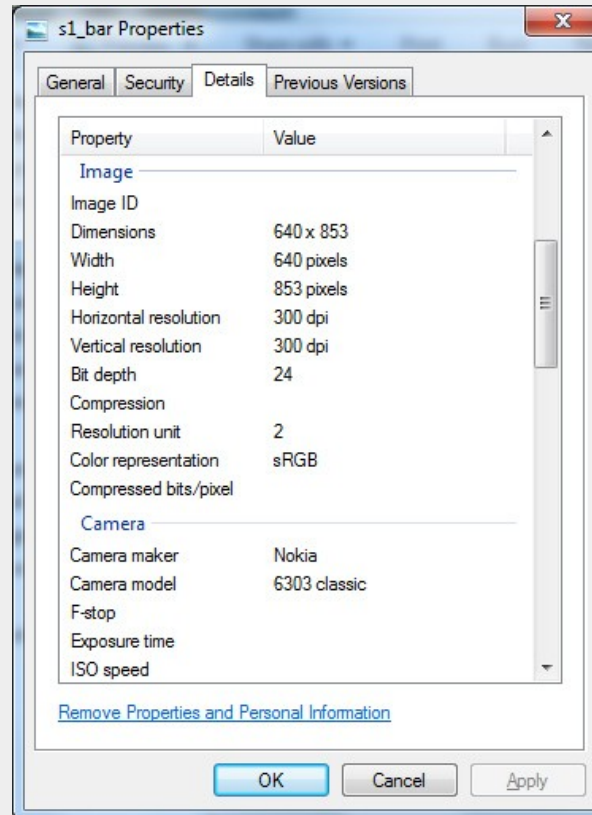
Zbiranje javnih (?) informacij



Zbiranje javnih (?) informacij



Metapodatk



Metapodatki

IP-RS - FOCA Free 3.0

Project Tools Options TaskList About Donate

FOCA

Clean your OpenOffice documents with OOMetaExtractor

Attribute | **Value**

Users

Nataša Pirc

Folders

C:\Program%20Files\Microsoft%20Office\MEDIA\CAGCAT10\
d:\osebno\Moj%20dokumenti\My%20Pictures\Microsoftov%20organizator%20izrezk...
C:\Documents%20and%20Settings\NPirc\Local%20Settings\Temporary%20Internet...

Software

Microsoft Office
Microsoft Office 2007

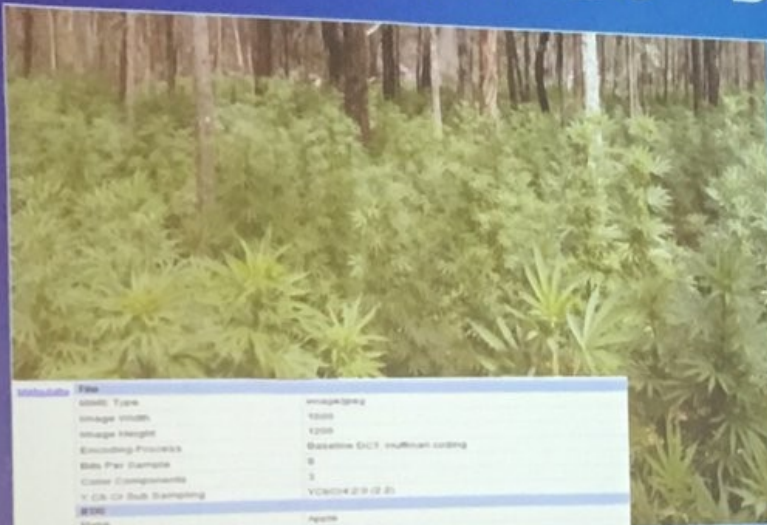
Time	Source	Severity	Message
8:24:13	MetadataSearch	low	Document metadata extracted: C:\Documents and Settings\kpkMacF\Local Settings\Temp\Smernic...
8:24:13	MetadataSearch	low	Document metadata extracted: C:\Documents and Settings\kpkMacF\Local Settings\Temp\Smernic...
8:24:13	MetadataSearch	low	Document metadata extracted: C:\Documents and Settings\kpkMacF\Local Settings\Temp\ZAKON...
8:24:13	MetadataSearch	low	Document metadata extracted: C:\Documents and Settings\kpkMacF\Local Settings\Temp\vzorec...
8:24:13	MetadataSearch	low	Document metadata extracted: C:\Documents and Settings\kpkMacF\Local Settings\Temp\Tersek...
8:24:14	MetadataSearch	low	Document metadata extracted: C:\Documents and Settings\kpkMacF\Local Settings\Temp\QP_in...
8:24:14	MetadataSearch	low	Document metadata extracted: C:\Documents and Settings\kpkMacF\Local Settings\Temp\Priloga...

Conf Deactivate AutoScroll Clear Save log to File

Metadata analyzed !

Metapodatki

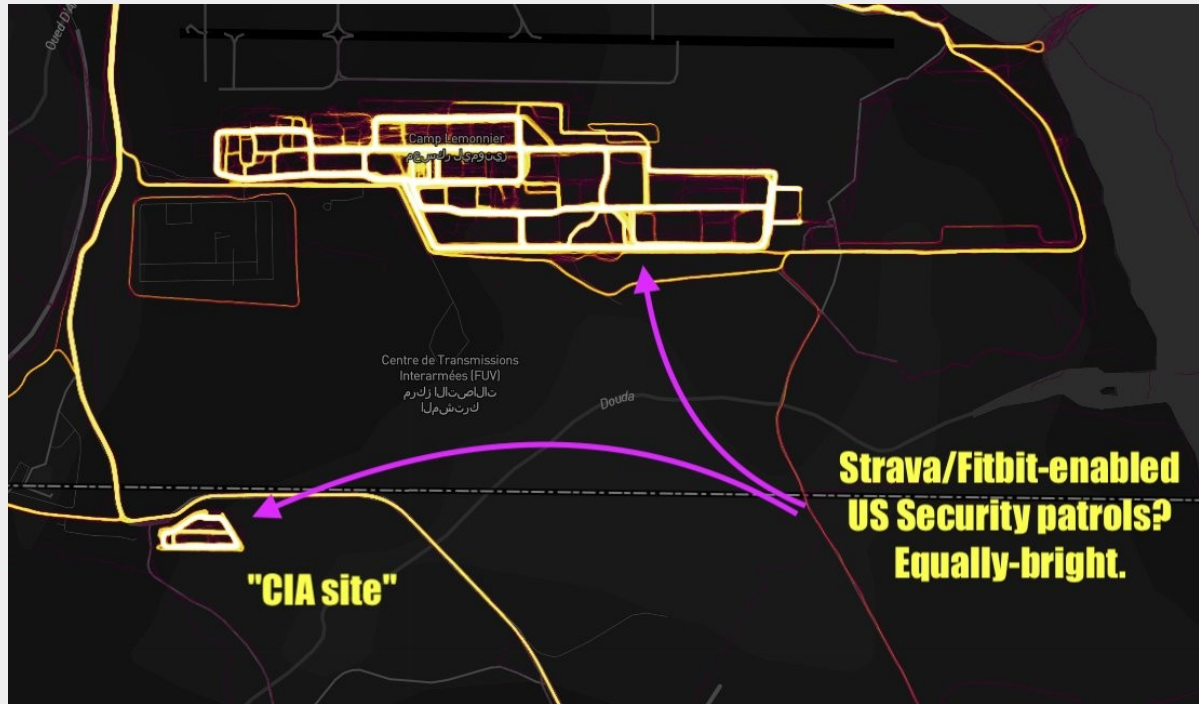
EXAMPLE 3 – Drug Crop



Metadata		
File		
Image Type	image/jpeg	
Image Width	1200	
Image Height	1200	
Encoding Process	Baseline DCT, Huffman coding	
Bits Per Sample	8	
Color Components	3	
V Co Co Sub Sampling	YCbCr4:2:2 (2 2 2)	
EXIF		
Make	Apple	
Camera Model Name	iPhone	
Orientation	Horizontal (normal)	
X Resolution	72	
Y Resolution	72	
Resolution Unit	inches	
Modify Date	2009:09:17 11:18:38	
V Co Co Processing	Centered	
EXIF		
F Number	2.8	
Exif Version	0021	
DateTime Original	2009:09:17 11:18:38	
DateTime Original	2009:09:17 11:18:38	
Create Date	V Co Co -	
Components Configuration	0100	
Flashpix Version	0100	
Color Space	0000	
Exif Image Width	1200	
GPS		
Location	34° 29' 20" S, 150° 54' 50" E, 08	

Exif Image Height	1200
GPS	
Location	34° 29' 20" S, 150° 54' 50" E, 08

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 [\[a8\]](#)

⁴⁴ 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. [\[Djibouti: a new U.S. ally has denied for\]](#)

Metapodatki

US bombs terror HQ after ISIS 'moron' takes selfie there

By Yaron Steinbuch

June 5, 2015 | 4:11pm

Type to Search



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



Slo 

PRIJAVA

 IŠČEM

 ODDAJAM

 REGISTRIRAM

 BONITETNE STORITVE

O AJPES

Naročilnice, vloge in pooblastila

Poročila in načrt objav

Cenik storitev

Pomoč

Vprašanja in odgovori

Kazalo

 JOLP
Javna objava letnih poročil

Letna poročila / Javna objava / JOLP

Vnos iskalnih pogojev

Rezultati

Izbrano podjetje

Pomoč in pogoji uporabe 

Rezultati iskanja

Število zadetkov: 1

ime poslovnega subjekta	naslov	pošta	kraj	okrožno sodišče	vložna številka
6	7	9	XYZQSTART	587173	XYZQSTOP

NAZAJ NA ISKANJE

Domov

Elektronsko podpisovanje

Za razvijalce programske opreme

KONTAKT

OBVESTILO O UPORABI PIŠKOTKOV

Spletni portal uporablja piškotke za izboljšanje delovanja spletnih storitev. Ali se strinjate, da na vaš računalnik naložimo piškotke za ta namen?

ŽELIM IZVEDETI VEČ

STRINJAM SE

Napadi preko spletnih aplikacij

The screenshot shows a Mozilla Firefox browser window titled "Net.Stik - Mozilla Firefox". The address bar displays the URL `https://netstik.sparkasse.si/eb/index.asp`. The page content includes a red stamp and a yellow circle highlighting a URL parameter in the address bar: `https://netstik.sparkasse.si/eb/kartica.asp?x=...&y=...&z=...&q=...&k=...&s=...`.

MasterCard kartični račun: [redacted]

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

Za preklic kartice, prosimo, pokličite 01/583 41 83.

© 2002-2009, BANKA SPARKASSE d.d. Pravica do napak in sprememb pridržana.

Napadi preko spletnih aplikacij

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

Datoteka Urganje Pogled Pojdi Zaznamki Orodja Pomoč

http://lgl.esiti.com/si/prevzem.php?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

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

Lutkovno gledališče Ljubljana

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

segment	vrsta	Številka	količina	cena
Veliki oder	6	7b	1	3,24 EUR
Veliki oder	6	7a	1	3,24 EUR
Veliki oder	6	6b	1	3,24 EUR
Veliki oder	6	6a	1	3,24 EUR
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 prireditelj 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.

Končano

Anonimizacija izključena

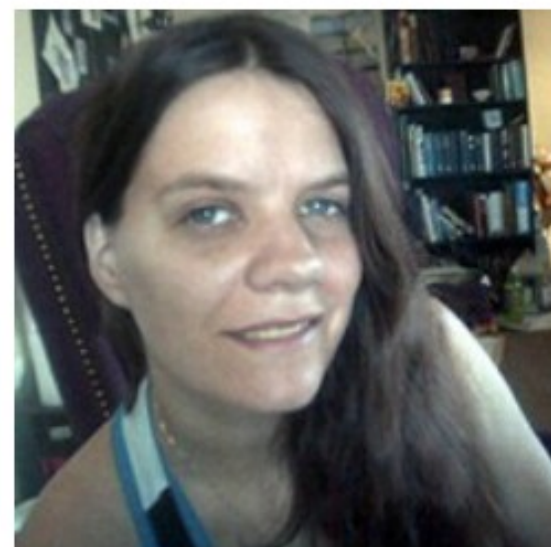
Start prevze... The GIMP Layers, ... Untitled... LGL - LU... http://l... 10:19

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...

e-RISK DUNZ

Uporabnik: Matej Kovačič / KOMISIJA ZA PREPREČEVANJE KORUPCIJE
Četrtek, 10. marec, 2011 /
[O aplikaciji](#) | [Omožiti](#) | [Odjava](#)

Iskanje

Podatki o strani - https://erisk.sigov.si/erisk/index.faces

Splošno Večpredstavnost Dovoljenja Varnost

Mozilla Firefox

Podatki o strani - https://erisk.sigov.si/erisk/logoff

Splošno Dovoljenja Varnost

Identiteta spletne strani

Spletna stran: erisk.sigov.si
Ta spletna stran ne vsebuje podatkov o lastništvu, state-institutions

Preglej digitalno potrdilo

Zasebnost in zgodovina

Ali sem to stran obiskal še kdaj pred današnjim dnem? Ne

Ali ta spletna stran shranjuje podatke (piškote) na moj računalnik? Da

Ali sem shranil kakšno geslo za to stran? Ne

Preglej piškote

Preglej shranjena gesla

Stran	Ime
erisk.sigov.si	JSESSIONID
erisk.sigov.si	UtpaToken
erisk.sigov.si	UtpaToken2

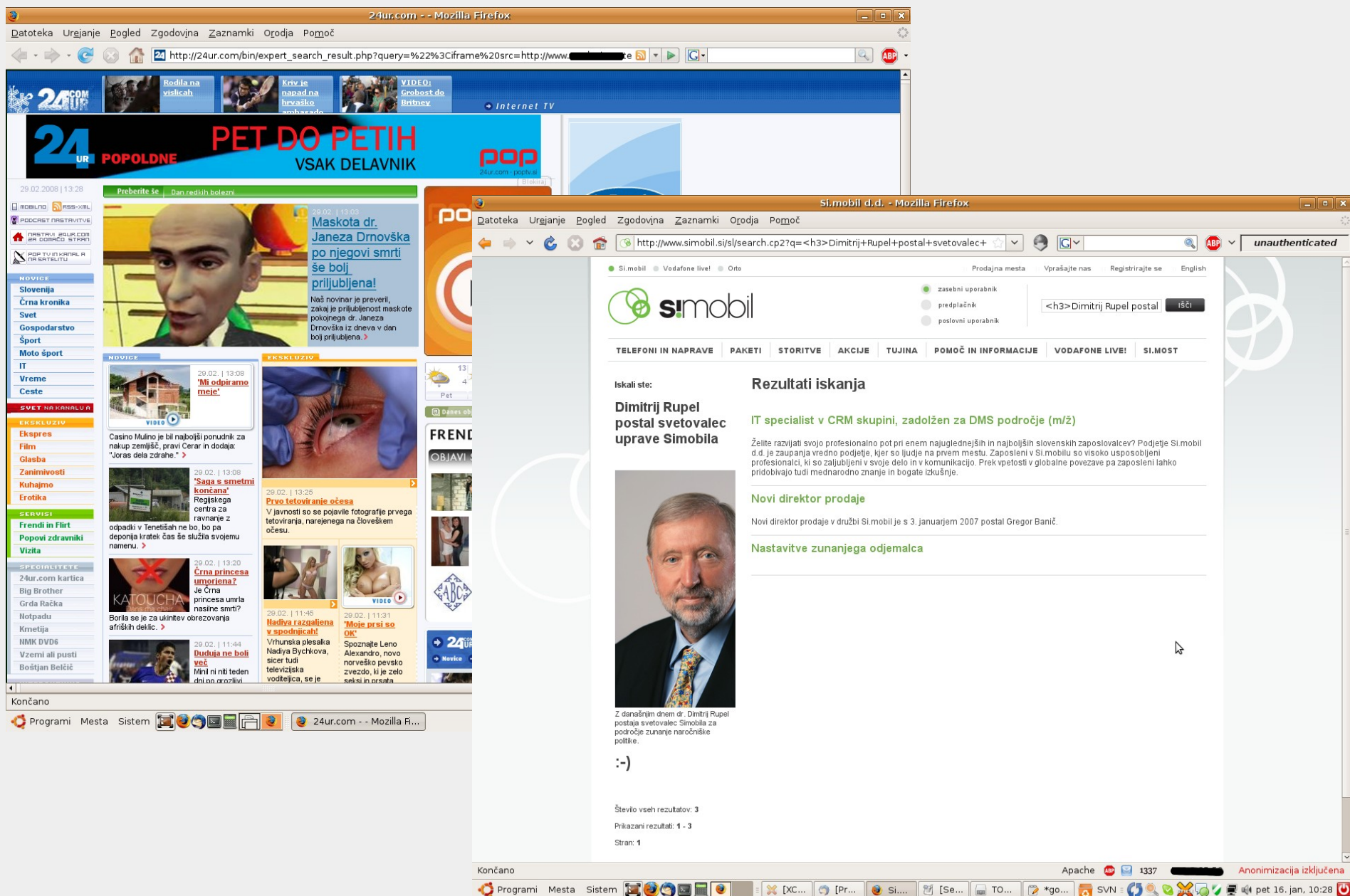
Ime: JSESSIONID
Vsebina: 0000IXLMzITJWUJZUQTVL_er6b:C075CB88E4DE8449000001B00
Gostitelj: erisk.sigov.si
Pot: /
Poslan za: Vse povezave
Preteče: na koncu seje

Odstrani piškot Odstrani vse piškote Zapri

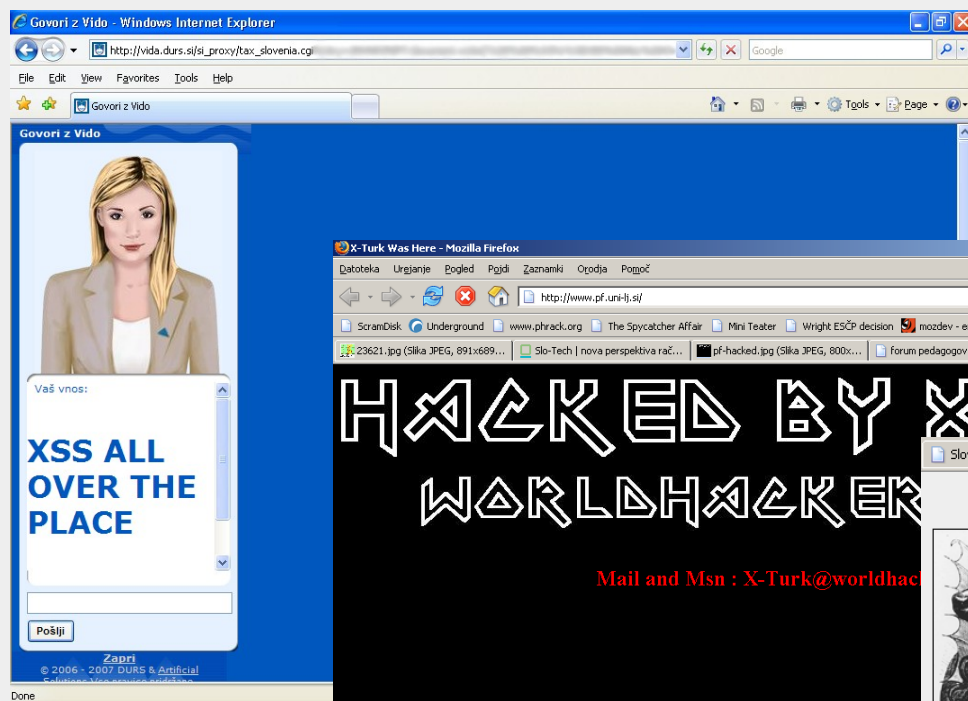
Ali pa... :)

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.

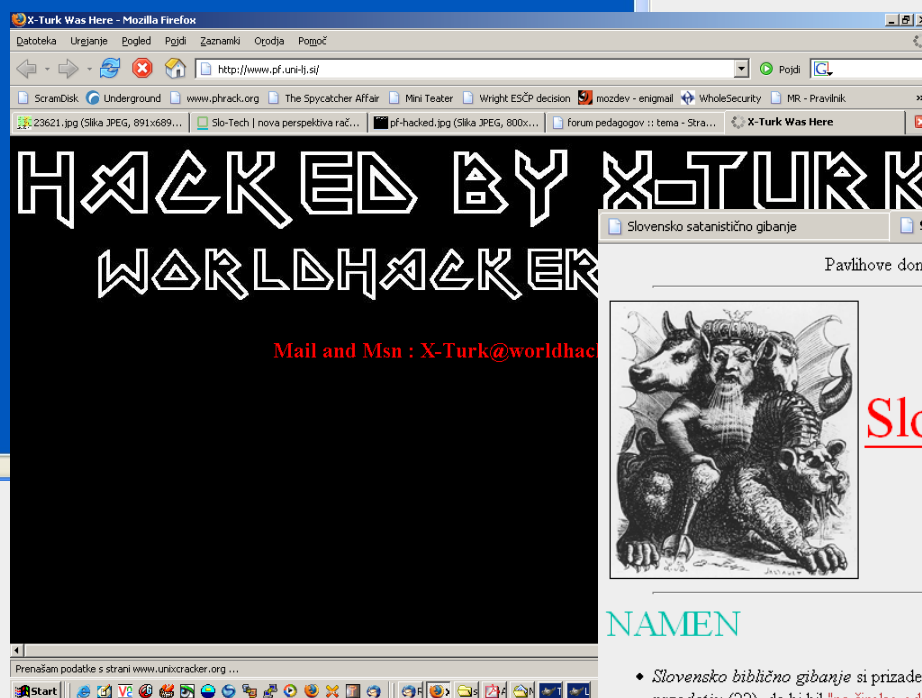
According to Assistant Chief Mike Allen, **a fax was sent to the jail** which stated *"Upon decision between Judge Rainey and the West Memphis Police Department CID Division Tristian Wilson is to be released immediately on this date of October 30, 2004 with a waiver of all fines, bonds and settlements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



Zaupanje vsebini na spletu?



XSS napad na
"davčno Vido".



Pravna fakulteta, Univerza v
Ljubljani, februar 2007



NAMEN

- Slovensko biblično gibanje si prizadeva po besedah 2. vatikanskega cerkvenega zbora v dogmatični konstituciji *O Božjem razodetju* (22), da bi bil "na široko odprt dostop do Svetega pisma".
- Zato hočemo *Sveto pismo* vsem ljudem predstaviti, ponuditi, posebej vernim pa pomagati, da ga bodo mogli zavestno sprejemati kot Božjo besedo znotraj živega izročila celotne Cerkve.

NALOGE

- povezovati svetopisemske ali biblične skupine,
- spodbujati nastajanje novih in jim pomagati pri delu
- prirejati biblične tečaje, razstave, predavanja

Razobličenje spletne strani
rimokatoliške cerkve.

Zaupanje vsebini na spletu?

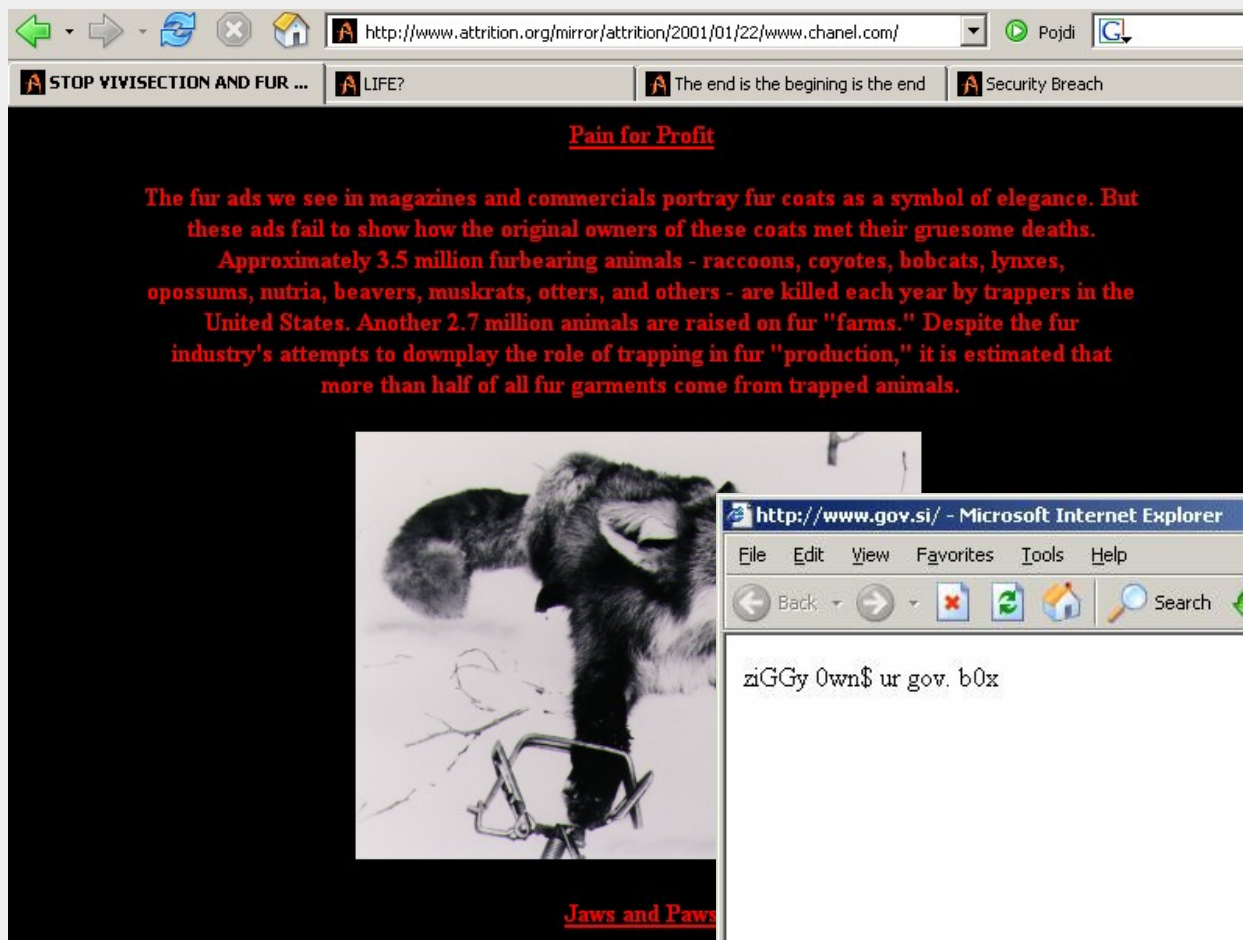
The left screenshot shows a Windows Internet Explorer window displaying the 'DELO' website. The address bar contains a URL with a malicious script: `http://www.delo.si/index.php?sv_path=43,50&query=<script%20src=`. The search bar on the page contains the text `<script src=`. The search results show a list of articles, including one titled 'Hakerji vdrlj v eno izmed Slovenskih bank'.

The right screenshot shows a Mozilla Firefox window displaying a 'Big Brother' meme on the website '24ur.com'. The address bar contains a URL with a malicious script: `http://24ur.com/bb/bb_search.php`. The search bar on the page contains the text `<script src=`. The meme features a portrait of a man with the text 'Fools... BIG BROTHER IS WATCHING YOU'.

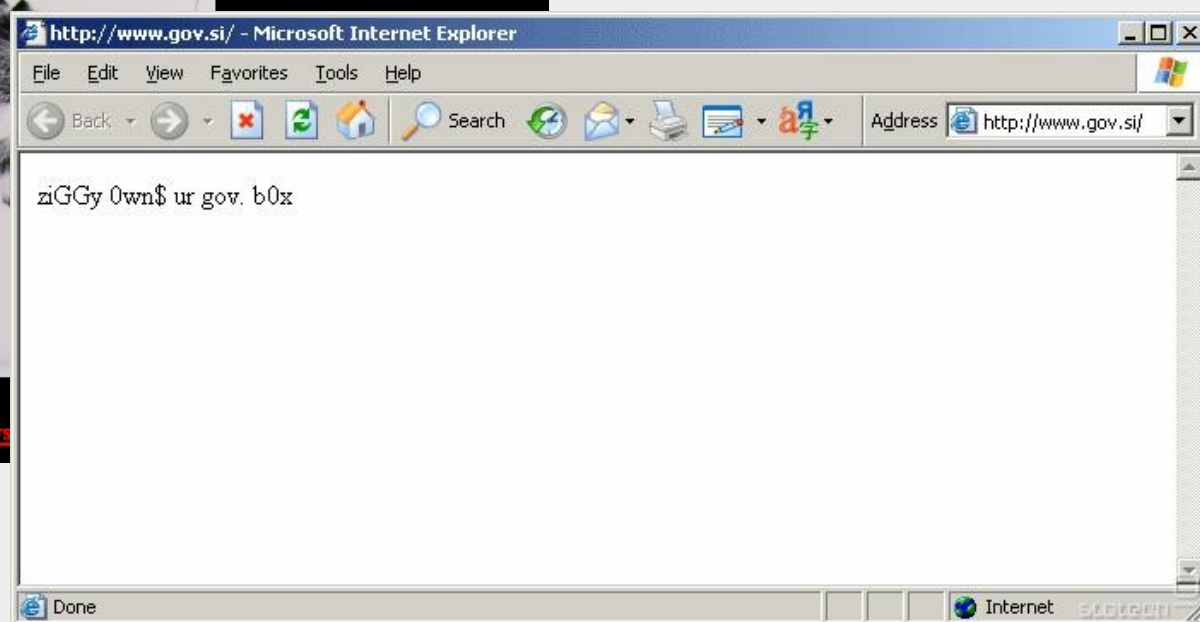
Lažna novica na spletni strani časnika DELO (XSS napad).

"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 (antispymware) 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? Niiiiiice.

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 šifriranje?

```
Follow TCP Stream

Stream Content

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

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

```
Follow TCP Stream

Stream Content

.....X...y...z(h.MO.t.-M.+..L\....O.*....9.8.5.3.2.../.....
.....www.google.com...P...L.H.)>..Z...>..y..F.....o:..{/..k..u/.....l.'...z...
.../...3.....Y...U..R..%O...!O.....<:d...s.....0
...*.H...
.....0L1.0...U...ZA1%0#.U...
...Thawte Consulting (Pty) Ltd.1.0...U...
Thawte SGC CA0..
080502170255Z.
090502170255Zoh1.0...U...US1.0...U...
California1.0...U...
Mountain View1.0...U...
Google Incl.0...U...www.google.com0..0
...*.H...
.....0.....].V.If.y...xNO.....K...%...e.....OG.P.....G...S.....\...g.J....h..TG.
$0.....?.....^r8I.t.7.....0..0(U.%10...+.....H..B..06..U.../0-0+..)'..%http://
crl.thawte.com/ThawteSGCCA.crl0r...+.....f0d0*...+.....0..http://ocsp.thawte.com0>...+.....0..2http://www.thawte.com/
repository/Thawte_SGC_CA.crt0...U.....0.0
...*.H...
.....1
l...T..h...C.k...l.....+oP...*6(..LV m.=B...W)..2.PEQn...*8..R(..W..d.M...=...fL..DR.|
<...7a.....i.c.F.o.r./7D...^#0.....0...0
...*.H...
.....0.1.0...U...US1.0...U...
...VeriSign, Inc.1705..U...Class 3 Public Primary Certification Authority0..
040513000000Z.
140512235959ZOL1.0...U...ZA1%0#.U...
...Thawte Consulting (Pty) Ltd.1.0...U...
Thawte SGC CA0..0
...*.H...
.....0.....g.....1}...?<...d.c.2K...o.../...3..3#..+tq...../...C..H.....-2..6.
{.dj;u..p}.b..i.6.1u...l...|...u.,zh....X'.....0...U.....0...U.....0...H...B.....0(U...!
0...0.1.0...U...PrivateLabel3-1501..U...*0(06.$.. http://crl.verisign.com/pca3.crl02..+.....60$0*...+.....0...http://
ocsp.thawte.com04..U...-0+...+.....+.....H..B...
^H...E...0
...*.H...
.....U.c....._..v..Q...+..wK.iP.....9...ry/...p...S4...S...V+...7.H.B%>...o..m.t...|
{<w..H.../.7.*6...?To.....[ZF6Au..i.....]..n.t6.0.J..uK.....NcP6b.G
$D.P..7G...-...t.@MP.*.G...*8...<.094.S:U...DV...m.. (.e1.i.c.Z...6...C.....$#G1.S;...f.....e.2P^K)-Cs
[...Y..rw.R...$......Q.....7.....#.....V}.....B..31.g...G.3.b.T.Y.....#Z...s...
$.)..R.....;f.....W.L.>..i...;h.b.....67...PW0Q...k..l'.FS...c..vtb..3.uvd..lx..g...RB.....=31
$.y0...>..w...j...3G!...>..(..W.Lu
>bqa+).V]A...o..l./<..!2..*..b.....V.B..=
...41n3H. ...)r=...^...M<..1H..X.Un....kV..7.....(v..
)...Y..C..A...$......
).....
```

Šifriranje »priporočča« tudi NSA!

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

Capabilities Development Risk Matrix (II)

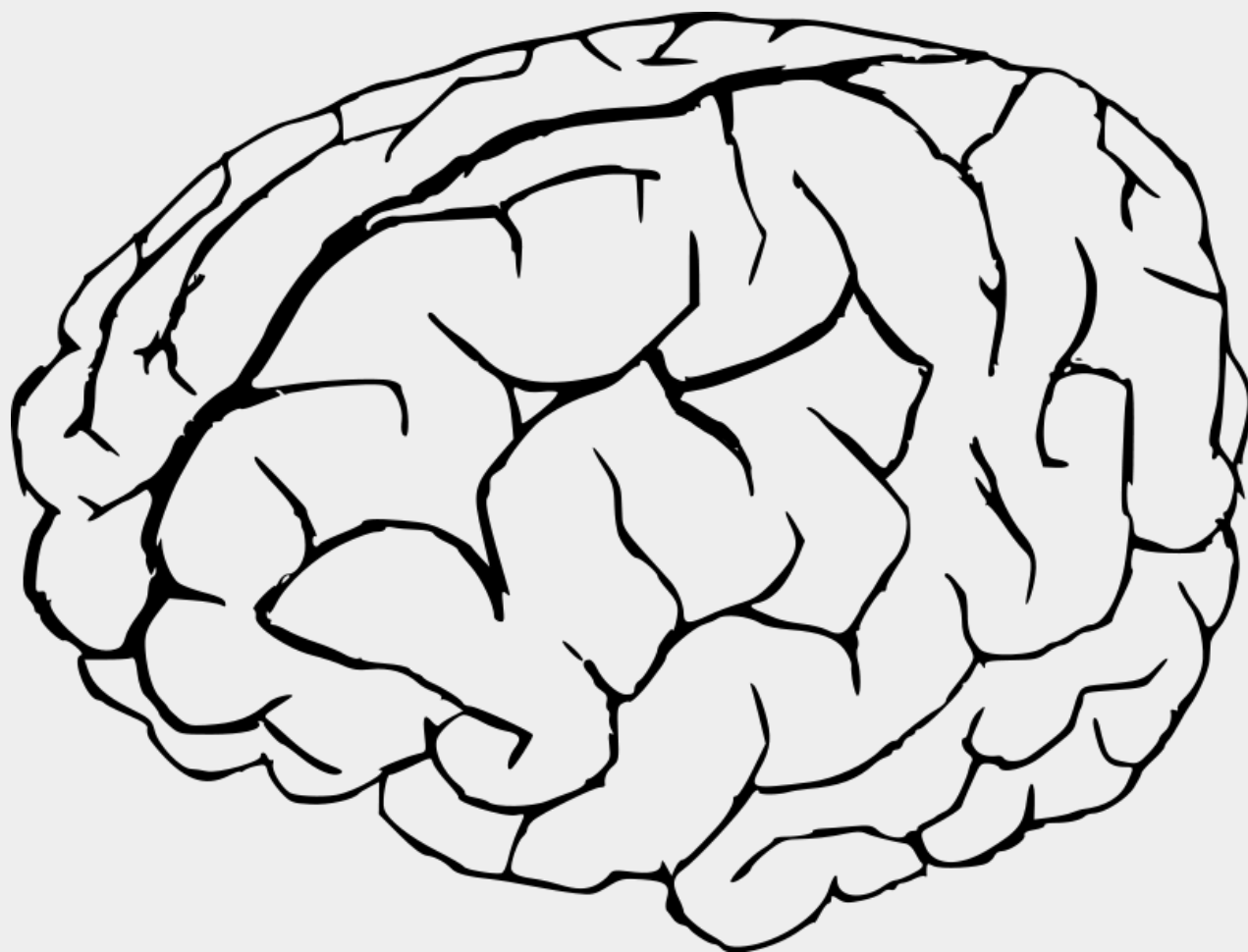
Impact > to production Use Risk v	TRIVIAL Loss/lack of insight to small aspect of target communications , presence	MINOR Loss/lack of insight to significant aspect of target communication s, presence	MODERATE Loss/lack of insight to large component of target communications, presence	MAJOR Loss/lack of insight to majority of target communications , presence	CATASTROPHIC 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, Experimentation					

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 changemel23 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 HISTFILE
[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

The image shows a Wireshark packet capture of a GSM TAP. The top pane displays a list of packets, with packet 34 selected. The middle pane shows the packet details, and the bottom pane shows the packet bytes.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
24...	56.627398...	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH)	(RR) Paging Request Type 1
34...	81.125671...	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH)	(RR) Paging Request Type 1

Packet Details (Packet 34):

- User Datagram Protocol, Src Port: 57272, Dst Port: 4729
- GSM TAP Header, ARFCN: 0 (Downlink), TS: 0, Channel: CCCH (5)
- GSM CCCH - Paging Request Type 1
 - L2 Pseudo Length
 - 0110 = Protocol discriminator: Radio Resources Management messages (0x6)
Message Type: Paging Request Type 1
 - Page Mode
 - Channel Needed
 - Mobile Identity - Mobile Identity 1 - IMSI (██████████)
 - Length: 8
 - 0010 = Identity Digit 1: 2
 - 1... = Odd/even indication: Odd number of identity digits
 -001 = Mobile Identity Type: IMSI (1)
 - IMSI: ██████████**
 - Mobile Country Code (MCC): Slovenia (293)
 - Mobile Network Code (MNC): SI Mobil (40)
 - P1 Rest Octets

Packet Bytes:

Offset	Hex	ASCII
0010	00 43 70 31 40 00 40 11 cc 76 7f 00 00 01 7f 00	.Cp10. @. .V.....
0020	██████████	██████████
0030	██████████	██████████
0040	██████████ 2b 2b	██████████ ++
0050	2b	+

Status Bar: International mobile subscriber identity(IMSI) (e212.imsi), 8 bytes | Packets: 4196 · Displayed: 2 (0.0%) · Load time: 0:0.83 · Profile: Default

Vprašanja...



Matej Kovačič

`matej.kovacic@telefoncek.si`

`https://infosec-seminar.si`

`https://telefoncek.si`