

# Napadi na informacijske sisteme (in ljudi)

---

(CC) 2021



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 in  
kiberkriminalci

# Kiberkriminal

---

Kiberkriminal ni zgolj samo uporaba informacijsko-komunikacijske tehnologije v kriminalne namene, pač pa je bistveni element kiberkriminala v tem, da ta kriminal ne bi bil mogoč brez uporabe tehnologije, vsaj ne v takem obsegu.

# »Heker«

---

Eden izmed slovenskih hekerjev, je v pogovoru povedal: *“Ne razumem zakaj ljudje izraz hekanje vedno povezujejo z vdiranjem in asocialnimi tipi. Ta termin ne pomeni nič drugega kot da si zelo dober v neki stvari, pa naj si bo to računalništvo ali kaj drugega. sem mnenja da je to bolj način razmišljanja, želja po znanju, izziv...”*.

Bruce Schneier hekanje razume kot **stanje duha**, pri čemer način razmišljanja povsem ločuje od namena uporabe le-tega: *“Heker je nekdo, ki razmišlja izven okvirov. Je nekdo, ki opusti običajno modrost in namesto tega naredi nekaj drugega. Je nekdo, ki gleda na rob in se sprašuje kaj je na oni strani. Je nekdo, ki vidi niz pravil in se sprašuje, kaj se zgodi, če jim ne slediš. Heker je nekdo, ki eksperimentira z omejitvami sistema zaradi intelektualne radovednosti. ...”*

# »Heker«

---

*“Računalniki so odlično igrišče za hekerje. Računalniki in računalniška omrežja so ogromni zakladi skrivnega znanja. Internet je brezmejna pokrajina neodkritih informacij. Več kot veš, več lahko storiš. ... To je varnostno hekanje: vdiranje v sisteme s pomočjo razmišljanja na drug način. ‘Heker’ je stanje duha in nabor veščin; kako to uporabiš, pa je drugo vprašanje.”*  
(Bruce Schneier).

Richard Pryce, »Datastream Cowboy«, ki je leta 1994 v starosti 16 let vdrl v več visoko zaupnih ameriških vojaških sistemov: *“Nekateri so gledali televizijo po šest ur na dan, jaz pa sem hekal računalnike.”*

# Kiberkriminal

Včasih:

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





# Kiberkriminal

Danes:

- posel in denar!



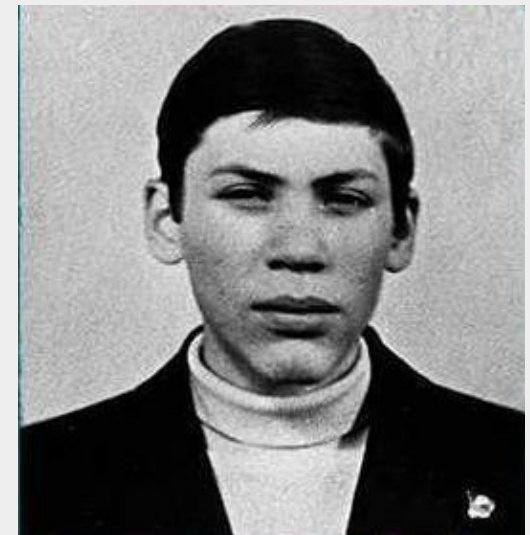
Spletna stran "podjetja".



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



Šifrirno-izsiljevalski virus Cryptolocker.



Vladimir Leonidovič Levin je leta 1994 vdrl v Citibank in ukradel 10,7 milijona USD.

# »Etično hekanje«

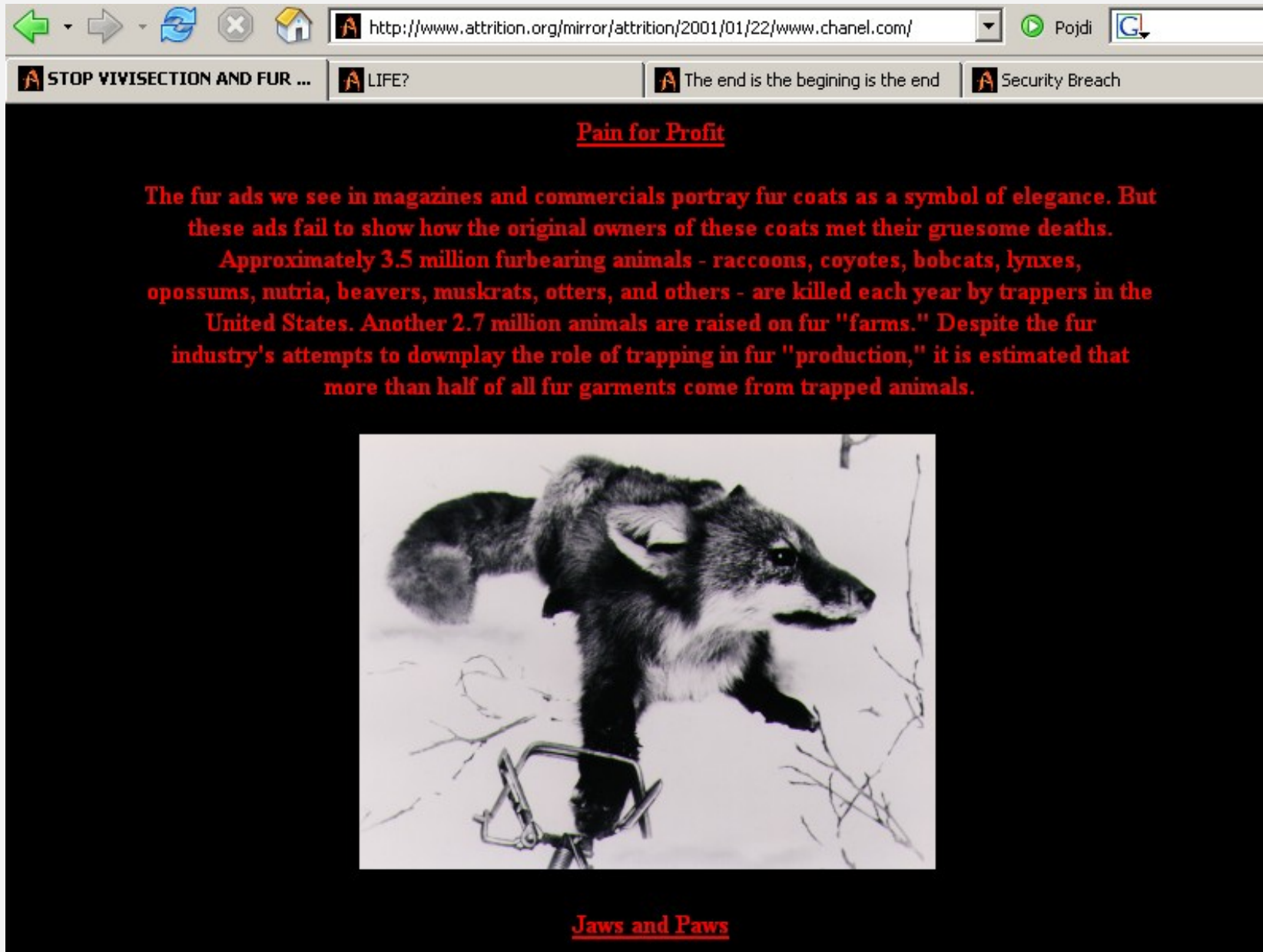
---

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.

# Haktivizem




The screenshot shows a web browser window with the address bar containing the URL <http://www.atrition.org/mirror/atrition/2001/01/22/www.chanel.com/>. The browser has several tabs open, including "STOP VIVISECTION AND FUR ...", "LIFE?", "The end is the begining is the end", and "Security Breach". The main content area has a black background with red text. The text is as follows:

**Pain for Profit**

**The fur ads we see in magazines and commercials portray fur coats as a symbol of elegance. But these ads fail to show how the original owners of these coats met their gruesome deaths.**

**Approximately 3.5 million furbearing animals - raccoons, coyotes, bobcats, lynxes, opossums, nutria, beavers, muskrats, otters, and others - are killed each year by trappers in the United States. Another 2.7 million animals are raised on fur "farms." Despite the fur industry's attempts to downplay the role of trapping in fur "production," it is estimated that more than half of all fur garments come from trapped animals.**



**Jaws and Paws**

# Kiberterrorizem in kibersabotaža

---

## **Kiberterrorizem in kibersabotaža:**

- uporaba hekerskih tehnik v aktivistične ali vojaške, a destruktivne namene (povzročanje ekonomske škode ali ogrožanje življenja ljudi);

## **Primeri:**

- Morris worm, 2. november 1988 (bolj vandalizem);
- 1990-ta leta: večinoma pošiljanje SPAM sporočil;
- 911 worm (leta 2000), računalniški virus, ki je po uspešni okužbi skušal z modemom klicati na številko za klic v sili;
- napad na pristaniške v Houstonu (leta 2003): motnje v delovanju pristanišča;
- pogojno: napad SQL Slammerja na jedrsko elektrarno v Ohio leta 2003.

# Kiberterrorizem in kibersabotaža

---

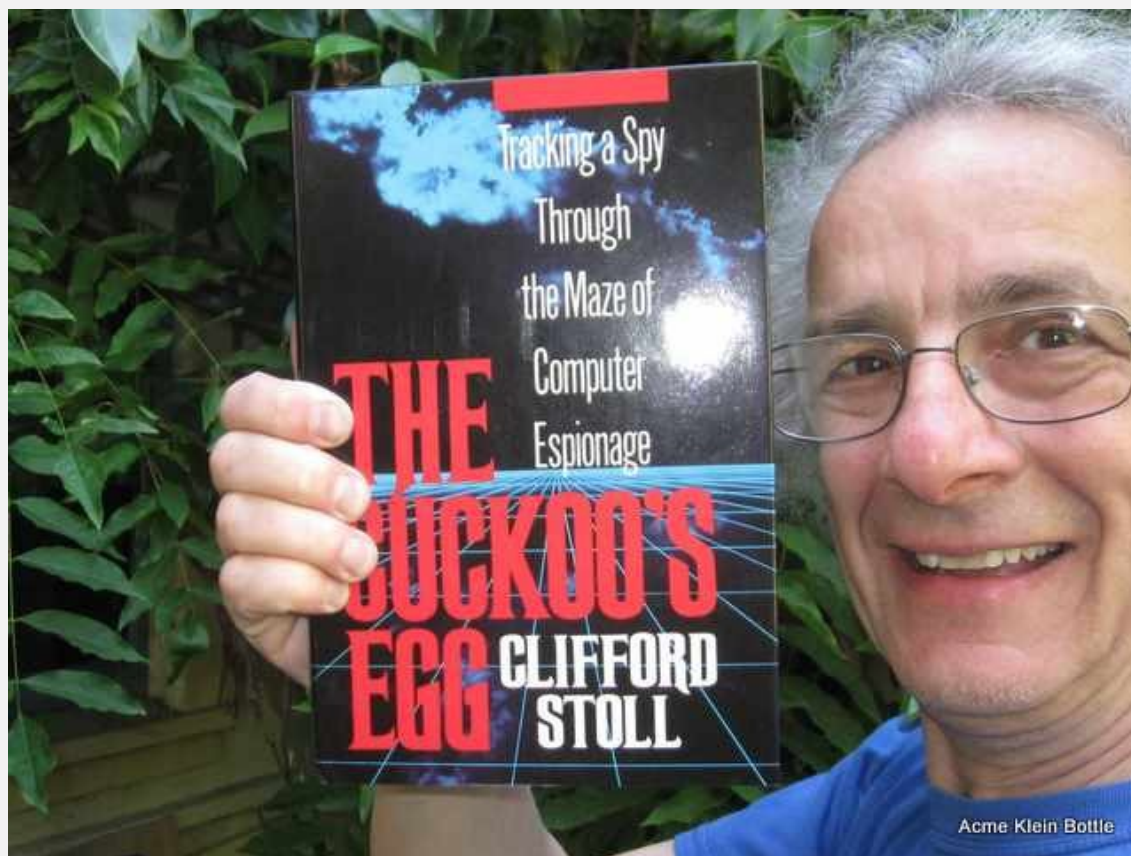
## Primeri:

- DoS napad na NATO strežnike leta 1999 kot znak protesta proti bombardiranju kitajske ambasade v Beogradu;
- leta 2000 bivši zaposleni v Maroochy Shire v Avstraliji povzroči izpust 800.000 litrov odpadnih voda v okolje;
- kibernapad na Estonijo leta 2007 zaradi odstranitve spomenika sovjetskemu vojaku;
- v zadnjih letih napadi na finančni sektor, vladne službe, kritično infrastrukturo,...

# Kiberkriminal in država

## Informacijsko-obveščevalni napadi:

- »Cuckoo's Egg« (KGB hack)



# Kiberkriminal in država

---

## Informacijsko-obveščevalni napadi:

- ZDA (NSA, industrijska špijonaža);
- Rusija (industrijska špijonaža, APT napadi na zahodne države, vojaško-obveščevalno hekanje (Ukrajina, Estonija...), virusi, FancyBear);
- Stuxnet (napad na iranski jedrski program);
- Severna Koreja (Mirrim College, Lazarus Group);
- Kitajska (sile kibernetike varnosti («Blue Army»), Enota 61398, APT napadi na zahodne države, napadi na politične aktiviste).

# Kiberkriminal in država

---

## **Kibervojna:**

- DDoS napadi na Gruzijo julija 2008 s strani Rusije (napad na medijske organizacije, državne spletne strani,...);
- v Ukrajini so leta 2014 ruske sile za nekaj časa prevzele nadzor nad več središči s TK opremo - s tem naj bi preprečili uporabo mobilnih telefonov članom parlamenta in drugim pomembnim posameznikom;
- decembra 2015 je 80.000 gospodinjstev na zahodu Ukrajine ostalo brez električne energije, saj so napadalci izključili razdelilne transformatorske postaje;
- konec 2014: napadi na turške državne strežnike, telekomunikacijski in finančni sektor, zaradi sestrelitve Ruskega letala na meji s Sirijo.



# Kiberkriminal in država

---

**Zmoglјivosti kibernetiskih napadov kot sredstvo odvračanja kibernetiskih napadov:**

*»In 2016, the US was successfully deterred from attacking Russia in cyberspace because of fears of Russian capabilities against the US.«*

(Bruce Schneier, <[https://www.schneier.com/blog/archives/2018/06/an\\_example\\_of\\_d.html](https://www.schneier.com/blog/archives/2018/06/an_example_of_d.html)>)

# Napadi na informacijske sisteme

# Fizični dostop do sistema

---

Nepooblaščen dostop do podatkov.

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

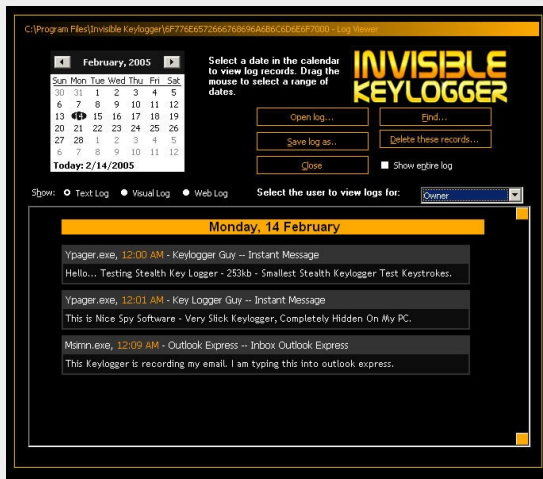
Zavržene računalniške komponente, ki vsebujejo nosilce podatkov (trdi diski, tiskalniki, mobilni telefoni,...).

Nameščanje aplikacij z »dvojno funkcijo«.

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

Večuporabniška okolja (eskalacija privilegijev).

# Podtikanje prikritih mehanizmov



Programski prestrezniki tipkanja.

```
SVSLINUX 3.75 2009-04-16 ERIOS 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...
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

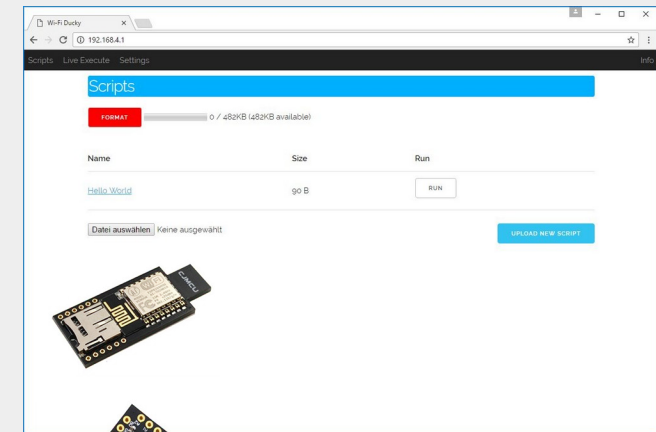
What do you want to do today: Run [E]vil Maid, [S]hell, [R]leboot
P
remounting /mnt/stick rw...
TrueCrypt EvilMaid_patcher v0.1
-----
TrueCrypt Boot Loader detected
PatchTrueCrypt(): Compressed loader size: 41773 bytes
PatchTrueCrypt(): Loader memory size: 8x7000 (28672) bytes
PatchTrueCrypt(): Decompressing the boot loader
PatchTrueCrypt(): Decompression successful
PatchTrueCrypt(): Decompressed loader physical size: 27687 bytes
PatchHskPassword(): Loader is already infected
PatchTrueCrypt(): PatchHskPassword() failed
DisplayTrueCryptPassword(): Password is "
saving original sectors in /mnt/stick/sectors-2009-10-15-170716
remounting /mnt/stick in ro...
done; you can reboot safely.

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

Evil Maid napad na TrueCrypt in...

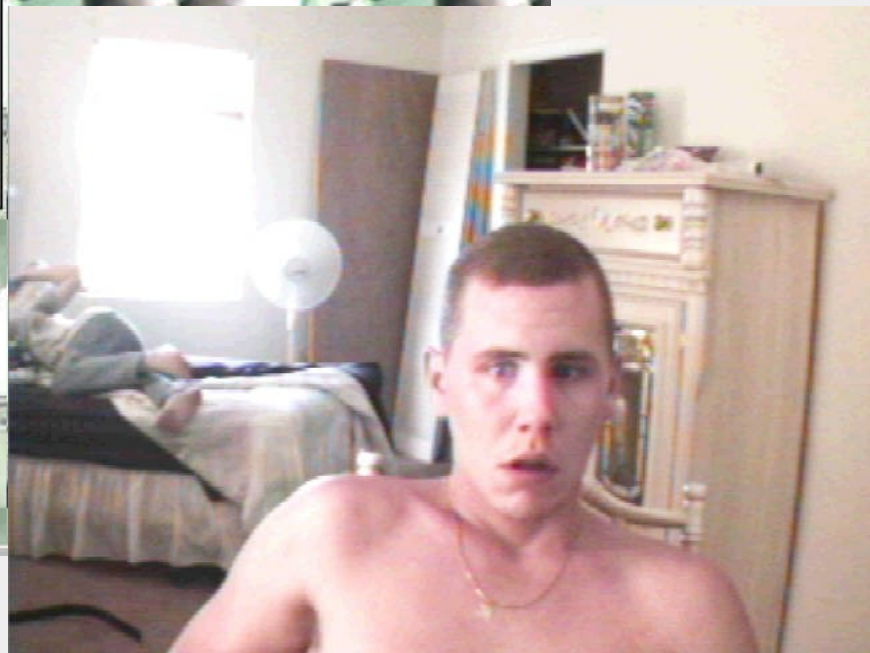
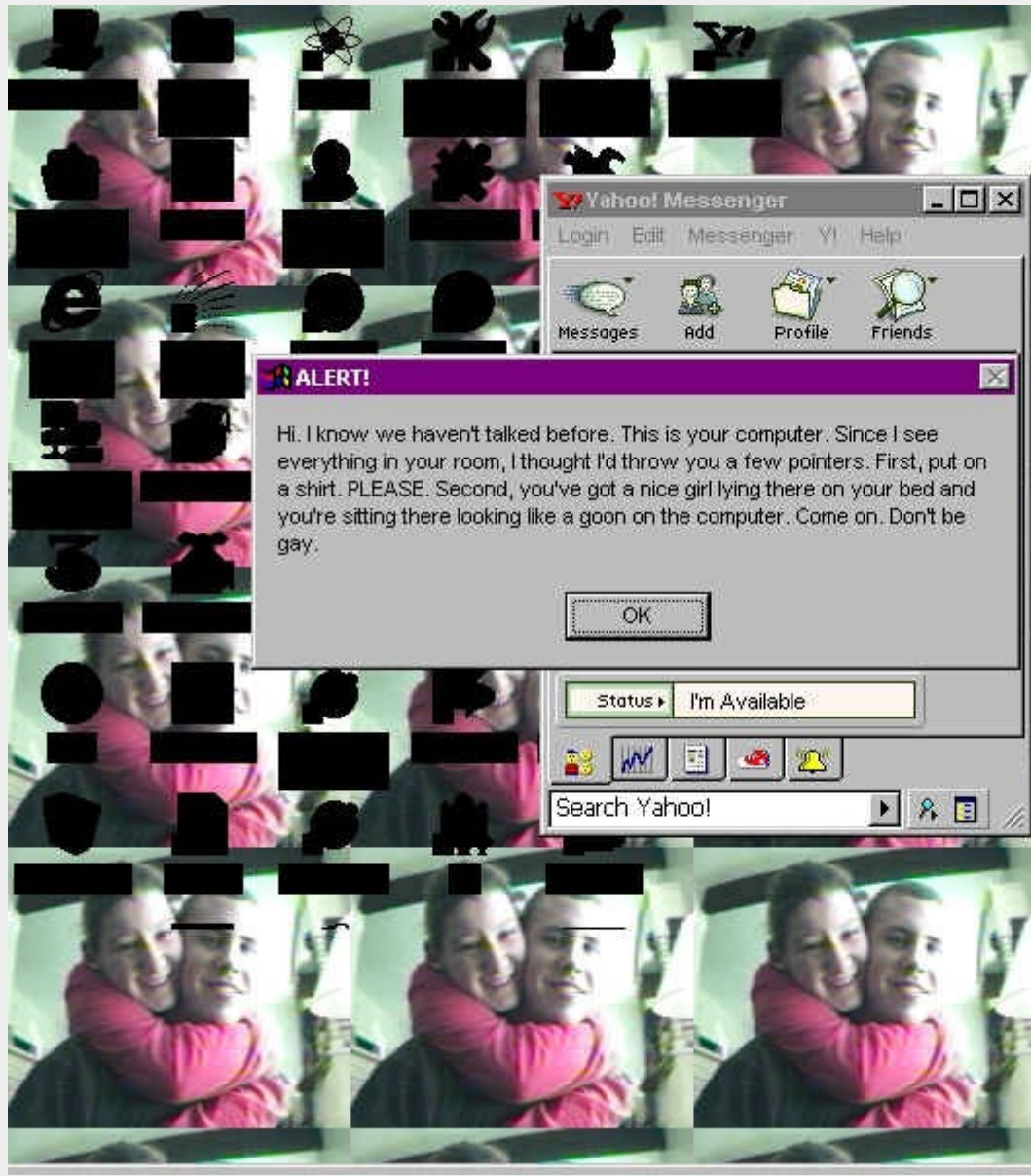


Strojni prestrezniki tipkanja.



BadUSB z Wi-Fi podporo.

# Posledice...



# Ranljivi niso samo računalniki...



# Ranljivi niso samo računalniki...

The screenshot shows a web browser window displaying the Tenovis WebTerminal interface. The browser's address bar shows the URL `http://10.254.60.43/index.html`. The page content includes the Avaya logo and a "WebTerminal" section with a "PIN:" field containing "\*\*\*\*" and a "Status" of "Connected". A "T3IP WebTerminal : mainmenu" dialog box is overlaid on the page, displaying system information:

- Own call number: 5711
- MAC address: 00-04-0d-f5-09-6a
- Application file: T112\_Sp3.bin
- Boot-file: T100

Below this information are buttons for "Bootline", "Registration & admission", and "IP audio settings". A "Send data" button is at the bottom left, and a "Cancel" button is at the bottom right. The status "VoIP Manager active: Configuration access limited!" is visible. A terminal window titled "matej@cryptopia: ~" is open in the foreground, showing the execution of the command `nmap 10.254.60.43`. The terminal output indicates that the host is up and that port 80/tcp is open for http. The terminal also shows the Nmap version (5.21) and the scan completion time (5.4 seconds).

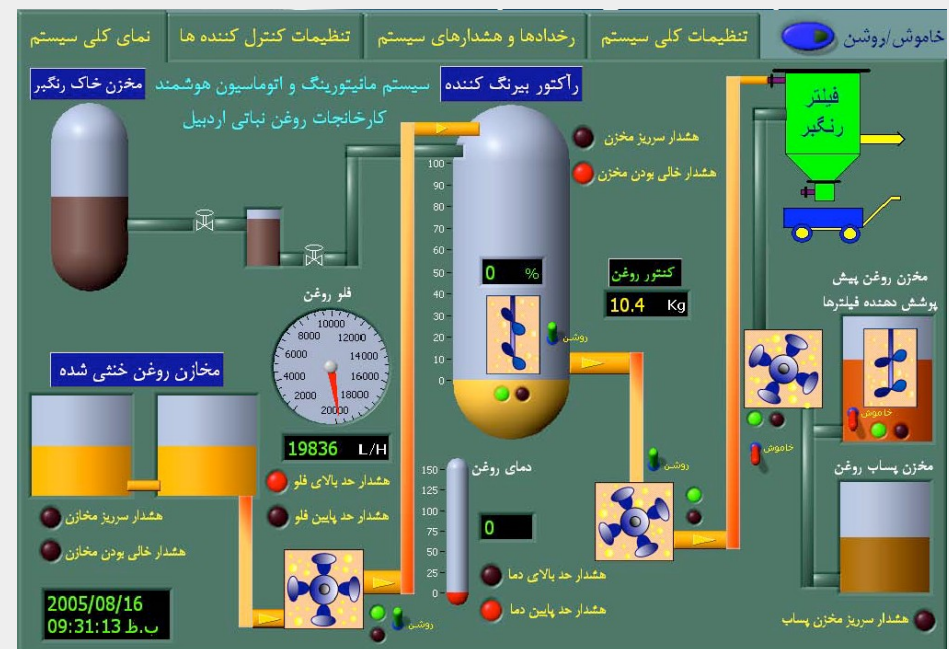
At the bottom of the browser window, a status bar displays "Applet started." and "Retrieving your IP address... Anonimizacija izključena". The taskbar at the bottom shows several open applications, including "root@cryptopi...", "matej@cryptop...", "Tenovis WebTer...", "[Izvorna koda st...", and "T3IP WebTermi..."

Napad na VOIP telefon.

# Ranjivi niso samo računalniki...



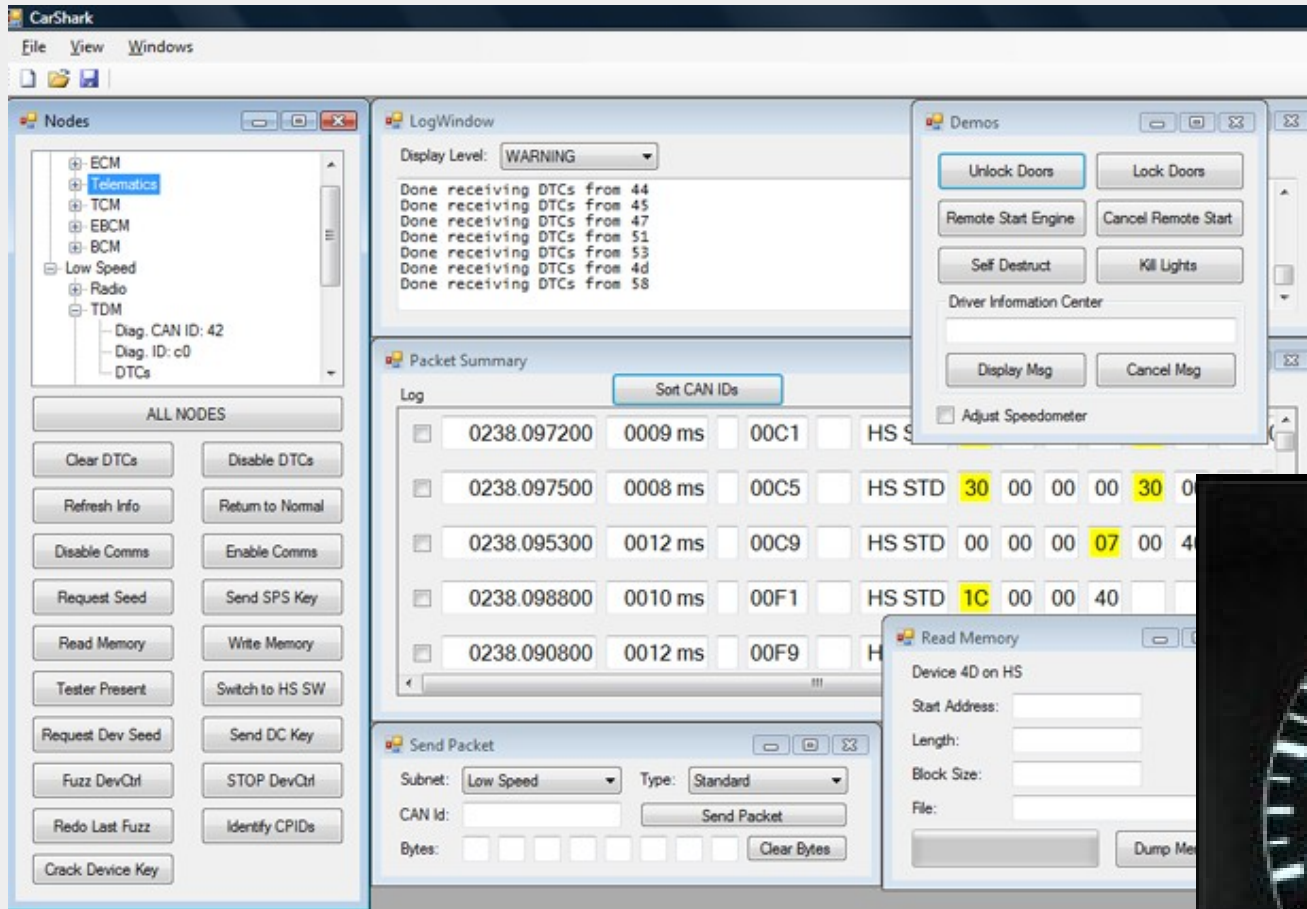
Napadi na RFID potne liste.



Napadi na SCADA sisteme.



# Ranljivi niso samo računalniki...



Napadi na avtomobile.



# Ranljivi niso samo računalniki...

```
DANGER!  
DO NOT USE WHILE CONTROLLER IS  
BEING USED FOR TRAFFIC CONTROL  
OR SERIOUS DAMAGE, INJURY OR  
DEATH MAY OCCUR !!!
```

```
Warning!  
Shutting off controller while running  
the flash memory test may corrupt files,  
or other data on the flash drive
```

```
*** DAT Main Menu ***  
1) Processor  
2) Front Panel  
3) Field I/O  
4) Async Ports  
5) Sync Ports  
6) Modem Tests  
7) Utility Functions  
8) Run Continuous  
9) Configure Standard Tests
```



foto: Dan Tentler.

# Nekoč, pred davnimi časi...

---

*»LOpht Heavy Industries was a hacker collective active between 1992 and 2000 and located in the Boston, Massachusetts area. The LOpht was one of the first viable hackerspaces in the US, and a pioneer of Responsible disclosure.«*



# ...je živel Mudge

---

Mudge has written a program to scan utility companies' Web sites for words like

»*confidential*« or

»*password*.« »*I'm not breaking any laws by doing this, I'm just grabbing public stuff,*« he is quick to point out. »*They don't realize that they're putting it up there for the world to see.*«



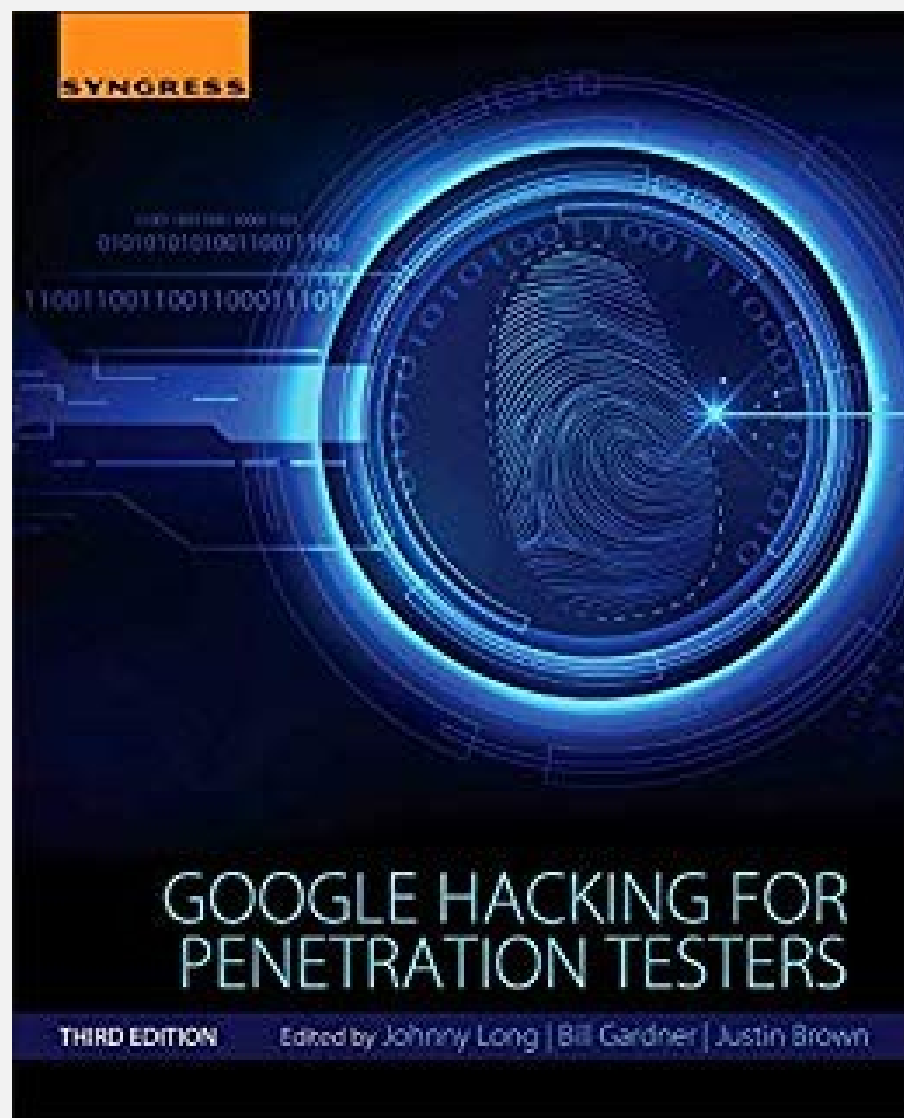
# In potem je prišel »Google hacking«...

---

Vincent Gaillot,  
»How to use Google  
to find confidential  
informations«, 2001

Google hacking je prvič  
omenjen avgusta 2003  
na Defconu.

Johnny Long je leto  
kasneje o tem napisal  
še knjigo »Google Hacking  
for Penetration Testers«.



# Javno dostopne naprave



RTSP/1.0 200 OK  
CSeq: 1  
Server: Hipcam RealServer/V1.0  
Public: OPTIONS, DESCRIBE, SETUP, TEARDOWN, PLAY, SET\_PARAMETER, GET\_PARAMETER

# Javno dostopne naprave

212...eb/guest/en/websys/webArch/mainFrame.cgi

**RICOH MP C4503** Web Image Monitor

Home

## Print Job List

Refresh

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
<input type="checkbox"/>	Hold Print		ZBORNICA	Microsoft Word - Izjava-ekskurzija-3.doc	14/3/2019 11:02:14	---	2	---
<input type="checkbox"/>	Hold Print		ZBORNICA	Microsoft Word - Izjava-ekskurzija-2.doc	14/3/2019 10:58:41	---	2	---
<input type="checkbox"/>	Hold Print		ZBORNICA	Microsoft Word - Izjava-ekskurzija-2.doc	14/3/2019 10:57:42	---	2	---
<input type="checkbox"/>	Hold Print		ZBORNICA	Microsoft Word - Izjava-ekskurzija-1.doc	14/3/2019 10:56:52	---	2	---
<input type="checkbox"/>	Hold Print		zborn2	Microsoft Word - LISTA PRISOTNOSTI NA 1.docx	12/3/2019 12:23:11	---	1	---
<input type="checkbox"/>	Hold Print		sobRAZGO	Microsoft Word - Dokument1	8/3/2019 12:15:48	---	1	---
<input type="checkbox"/>	Hold Print		sobRAZGO	FISS_Formule.pdf	5/2/2019 11:28:11	---	4	---
<input type="checkbox"/>	Hold Print		sobRAZGO	Dohod_VirDat_Obvestilo_2018_...pdf	31/1/2019 11:45:38	---	1	---

Back

# Varnost IoT

- Mirai botnet (napadal je domače usmerjevalnike in – IP kamere)...
- tiskalniki
- IP telefoni
- pametne pisarne,
- alarmi...

SIP Open Door Settings

Enable SIP Open Door:

Key to Open the Door:

Delay Lock Time(Second):

Save

Phone List

Phone Number	Remark Name	Remove
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Check All

Add... Remove

Note: You must restart the device to apply the changes.

```
CamCheck
[REDACTED]
#3:32 | Drag in Combo File.
#25235
#3:32 | Error Loading.
#3:32 | Drag in Combo File.
C:\Users\[REDACTED]\Desktop\combo.txt
#3:32 | Loaded 1579025 Combos.
select Proxy Type:
#1] | HTTPS
#2] | SOCKS4
#3] | SOCKS5
#0] | Proxyless
#3:32 | Drag in Proxy File.
C:\Users\[REDACTED]\Desktop\HTTP_12-06-19 15:47 PM.txt"
#3:32 | Loaded 2511 Proxies.
#3:32 | Thread Count?
#00
```





# Prestrezanje komunikacij

The image shows two windows from a network analysis tool. The top window, titled "sip.pcap - Wireshark", displays a list of captured packets. The bottom window, titled "sip\_govor.pcap - VoIP - RTP Player", shows the audio waveform for the selected packet.

**Wireshark Packet List:**

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

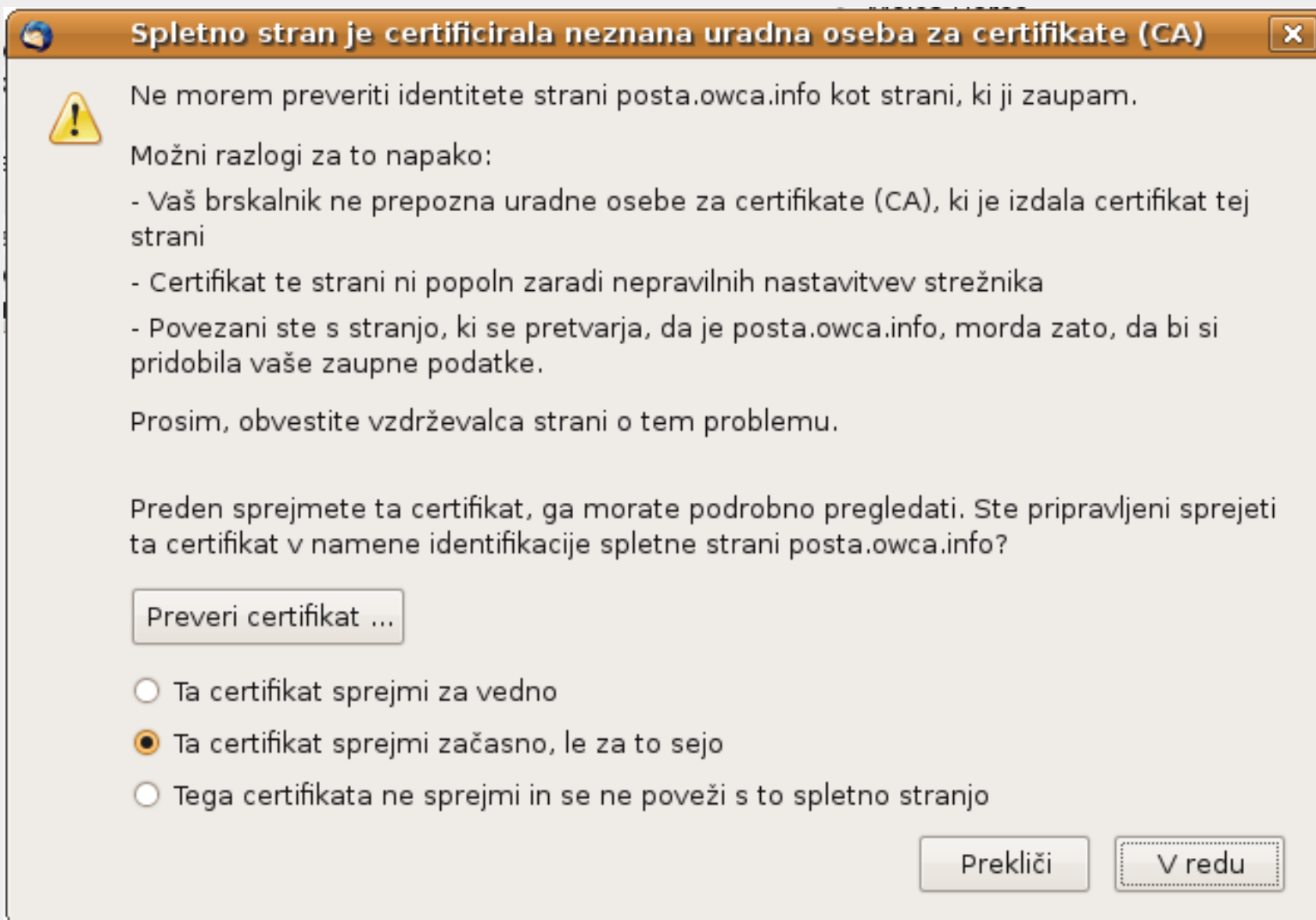
**Wireshark Packet Details (Frame 82):**

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

**RTP Player Audio Playback:**

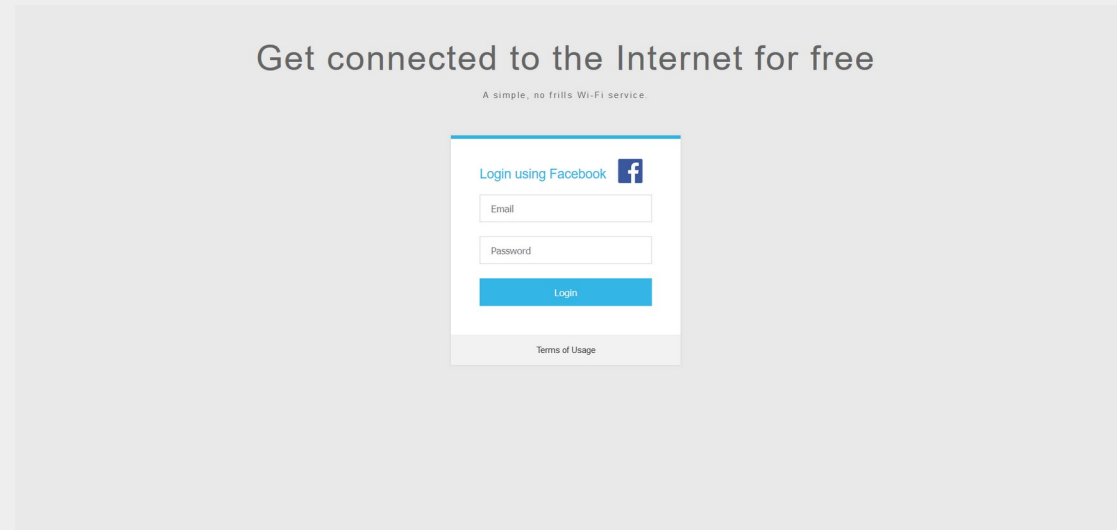
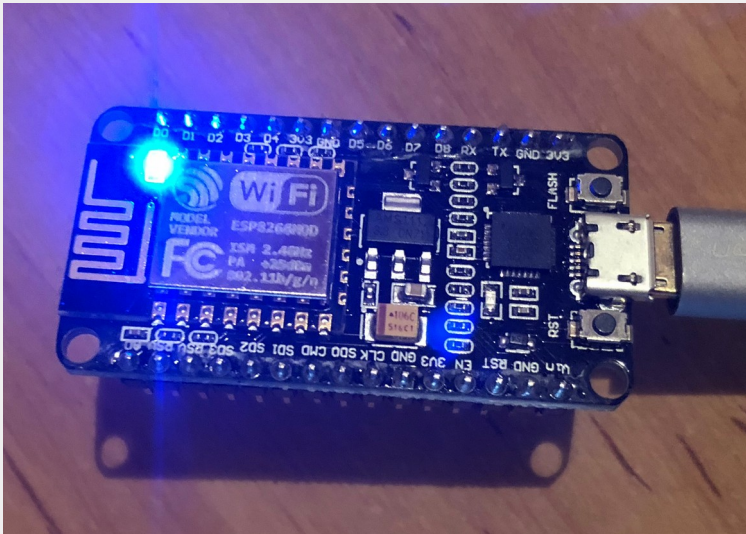
- Duration: 11.76 (top waveform), 12.04 (bottom waveform)
- Drop by Jitter Buff: 0(0.0%)
- Out of Seq: 0(0.0%) (top), 1(0.2%) (bottom)
- Buttons: Decode, Play, Pause, Stop, Zapri

# Prestrežanje komunikacij



Previdno pri sprejemanju neznanih digitalnih potrdil!

# Javno dostopna (Wifi) omrežja...



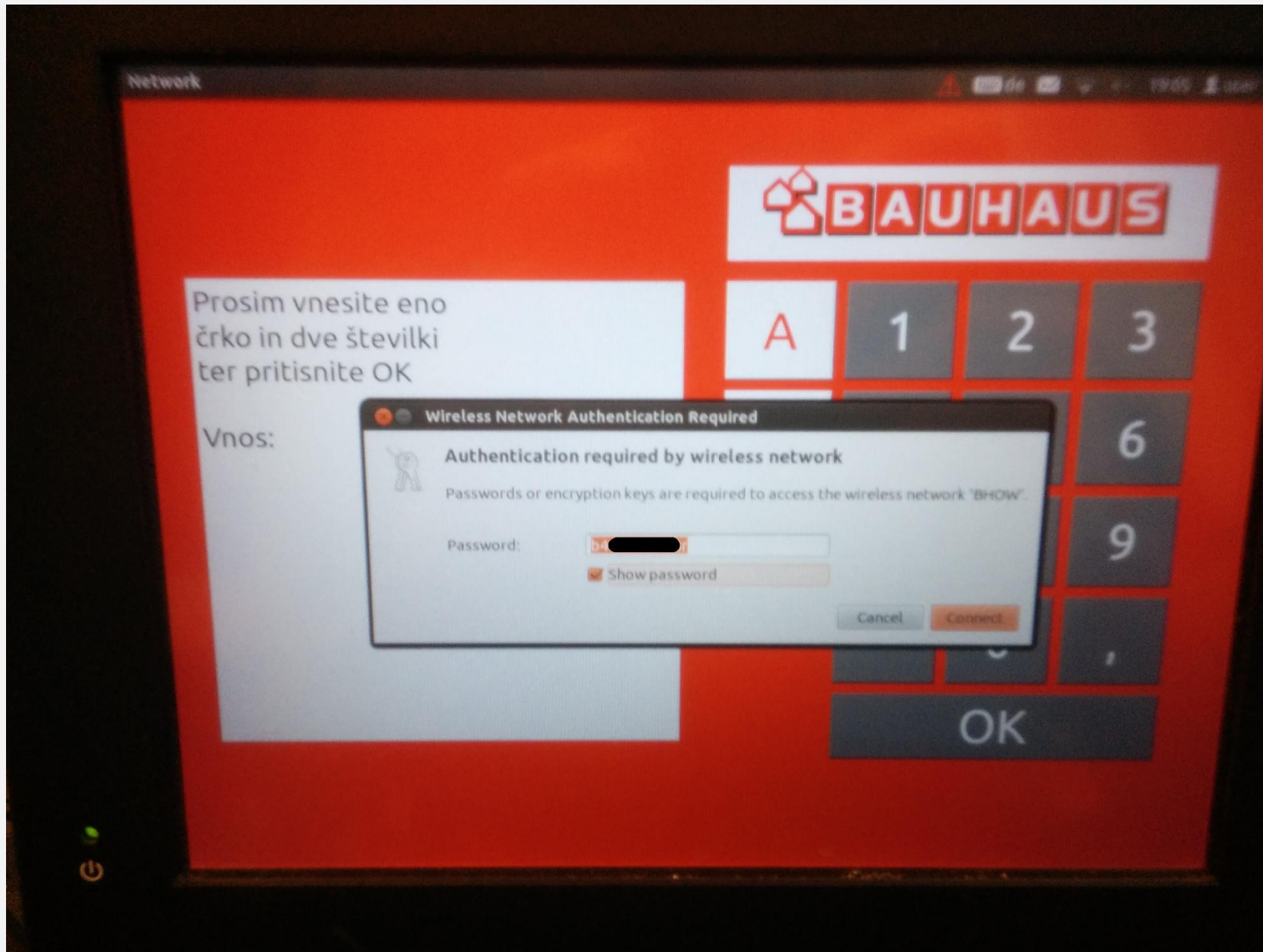
```
Extensions feed:
Sending 60 known beacons (OnAir ... HAM AIRPORT FREE WIFI)
Sending 60 known beacons (AEROPUERTO WIFI ... XFINITY)
Sending 60 known beacons (cablewifi ... backup)
Victim f4:91:  probed for WLAN with ESSID: 'Stargate' (KARMA)
Victim 40:f3:  probed for WLAN with ESSID: 'Telekom_FON' (Known Beacons)
DHCP Leases:
1533330793 40:f3  android-6c  01:40

Wifiphisher 1.4GIT
ESSID: Free WiFi
Channel: 6
AP interface: wlan0
Options: [Esc] Quit

HTTP requests:
[*] GET request from 10.0.0.94 for http://clients3.google.com/generate_204
[*] GET request from 10.0.0.94 for http://clients3.google.com/generate_204
[*] POST request from 10.0.0.94 with wfphshr-email=Victim@victim.com&wfphshr-password=crippledblackphoenix
[*] GET request from 10.0.0.94 for http://clients3.google.com/generate_204
[*] GET request from 10.0.0.94 for http://clients3.google.com/generate_204
```

<https://github.com/wifiphisher/wifiphisher>

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

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

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 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 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

**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

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

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

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

izpis.proteini.si/1...39.pdf

1 of 1 100%

**PROTEINI.SI**  
SPORT NUTRITION CENTER

**RAČUN ŠT: 10000039**

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

**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 \_\_\_\_\_  
\_\_\_\_\_

Tel: \_\_\_\_\_ ID za DDV: \_\_\_\_\_  
Kontakt: \_\_\_\_\_

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



MOJA BANKA IN



INTESA SANPAOLO BANK

Služba podpore strankam

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

Datum: 13.03.2019

## POTRDILO O IZVRŠENIH PLAČILNIH TRANSAKCIJAH

### PLAČNIK

Naziv: Eva  
Naslov:  
Račun: SI56  
Referenčna številka: SI99  
Banka: BAKOSI2X  
Naziv banke: BANKA INTESA SANPAOLO D.D.

### PLAČILNI NALOG

Številka transakcije:  
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  
Naziv: Članarina 2019 - Eva  
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., Pristanišča ulica 14, 6502 Koper - Slovenija, ID DDV: SI98026305, reg. organ: Okrodž'no sodišč' d'z'e v Kopru, d'z'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: [redacted]  
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: [redacted]  
Datum: [redacted] 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 [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).



Uradna oseba

[redacted]



# Zbiranje javnih (?) informacij

FDV www.fdv.uni-lj.si/Kontakti/telefonski\_imenik.asp

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 D E F G H I J K L M N O P R S Š T U V Z Ž

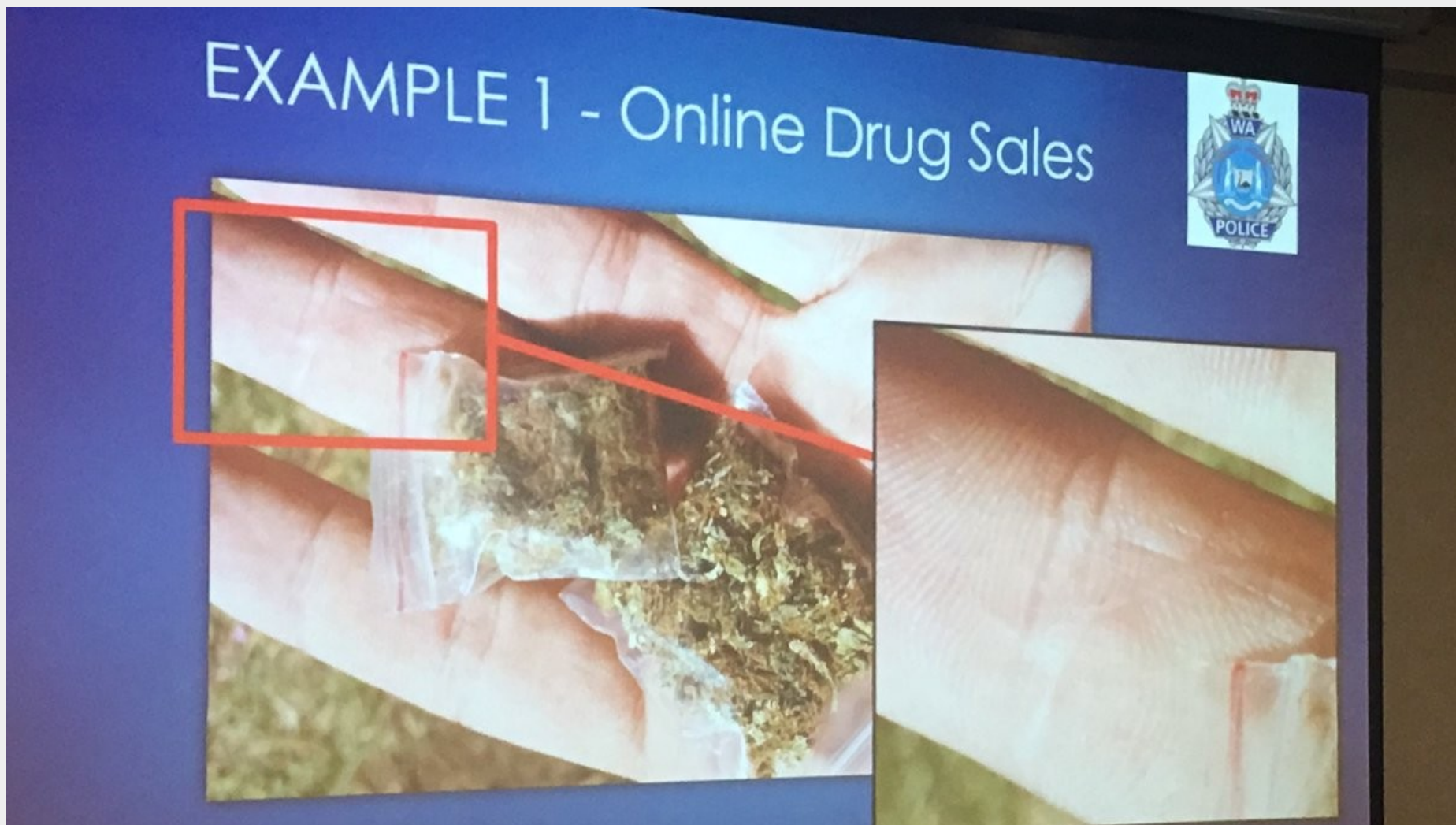
V primeru nejasnosti ali informacije pokličite **5805-100**

	Prilimek in ime	Interna številka	Številka sobe
A			
	ADAM dr. Frane	219	DS 21
	AKSENTIJEVIČ 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

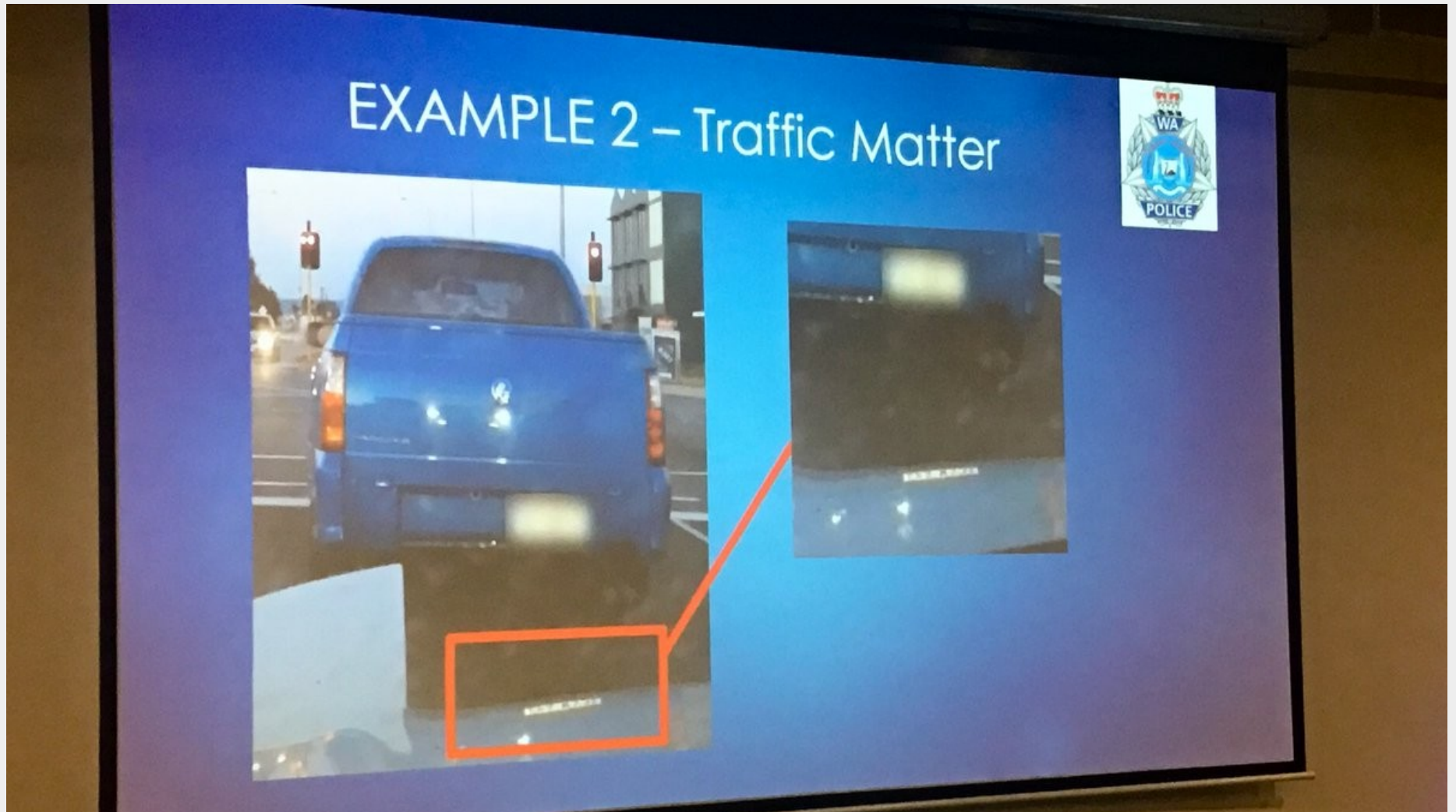
tel\_imenik\_FDV.ods - LibreOffice Calc

	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

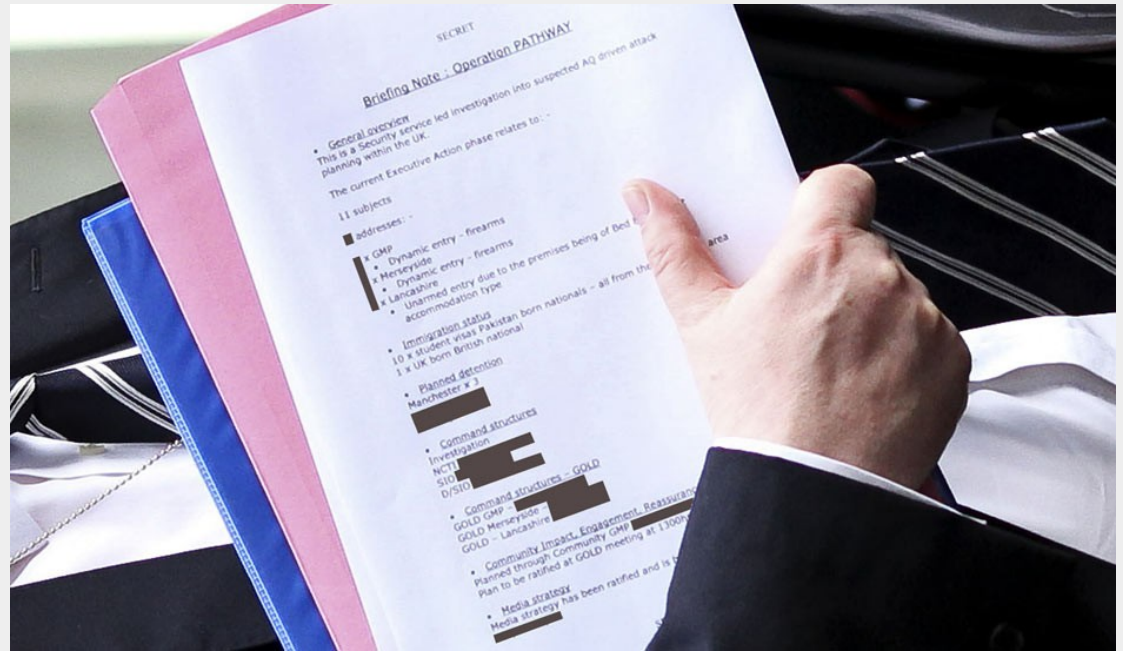
# Zbiranje javnih (?) informacij



# 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.

# Zbiranje javnih (?) informacij

VISOKOŠOLSKI STROKOVNI ŠTUDIJ  
Elektrotehnika – Telekomunikacije

## POROČILO PRAKTIČNEGA IZOBRAŽEVANJA

v podjetju  
[redacted]  
poslovna enota Maribor

Čas opravljanja: [redacted], 2009 do [redacted] 2010  
Mentor v podjetju: [redacted]  
Študent: [redacted]  
Vpisna številka: 9[redacted]  
E-pošta: [redacted]@gmail.com  
Telefon: 041 [redacted]

VISOKOŠOLSKI STROKOVNI ŠTUDIJ

## Računalništvo in informacijske tehnologije

## POROČILO PRAKTIČNEGA IZOBRAŽEVANJA

v podjetju  
[redacted]

Čas opravljanja: [redacted] 2010 - [redacted] 2010  
Mentor v GD: [redacted]  
Študent: [redacted]  
Vpisna številka: [redacted]  
E-pošta: [redacted]@uni-mb.si  
Telefon: 041 [redacted]



# Metapodatki

## Jeffrey's Exif Viewer

From Web  From File

Image URL:

[CLEAR IMAGE]

Jeffrey Friedl's Image Metadata Viewer  
(How to use)

Some of my other stuff

- [My Blog](#) · [Lightroom plugins](#) · [Pretty Photos](#)
- ["Photo Tech"](#)

### Basic Image Information

Target image: [http://www.wired.com/images\\_blogs/gadgetlab/2012/12/1b4ed71e0012f775d7dc621f5498bd731.jpg](http://www.wired.com/images_blogs/gadgetlab/2012/12/1b4ed71e0012f775d7dc621f5498bd731.jpg)

Camera:	Apple iPhone 4S
Lens:	4.3 mm
Exposure:	Auto exposure, Program AE, 1/20 sec, f/2.4, ISO 125
Flash:	Off, Did not fire
Date:	<b>December 3, 2012</b> 12:26:00PM (timezone not specified) (2 years, 3 months, 23 days, 9 hours, 3 minutes, 34 seconds ago, assuming image timezone of 6 hours behind GMT)
Location:	Latitude/longitude: <b>15° 39' 29.4" North, 88° 59' 31.8" West</b> ( 15.658167, -88.992167 )  Location guessed from coordinates: <i>Dumrey Road, Rio Dulce, Guatemala</i>
	Map via embedded coordinates at: <a href="#">Google</a> , <a href="#">Yahoo</a> , <a href="#">Wikimapia</a> , <a href="#">OpenStreetMap</a> , <a href="#">Bing</a> (also see the <a href="#">Google Maps</a> pane below)
	Altitude: 7 meters (23 feet)

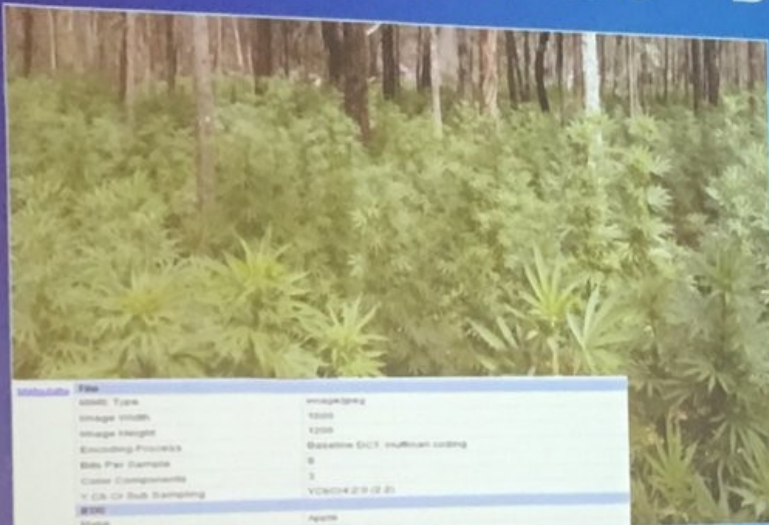


Click image to isolate; click this text to show histogram

# Metapodatki



## EXAMPLE 3 – Drug Crop



Metadata	
<b>File</b>	
Image Type	image/png
Image Width	1200
Image Height	1200
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
V. Ch. Ch. Sub Sampling	VC094 219 21 21
<b>EXIF</b>	
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. Ch. Ch. Processing	Canon2
<b>EXIF2</b>	
F Number	2.8
Exif Version	0021
CreateTime Original	2009:09:17 11:18:38
Create Date	2009:09:17 11:18:38
Components Configuration	V. Ch. Ch. -
Flashpix Version	1.0.0
Color Space	sRGB
Exif Image Width	1200
Exif Image Height	1200
<b>GPS</b>	
Location	34° 29' 20" S, 150° 34' 50" E, 08

Exif Image Height	1200
<b>GPS</b>	
Location	34° 29' 20" S, 150° 34' 50" E, 08

# Metapodatki

The screenshot shows the FOCA Free 3.0 application window. The title bar reads "IP-RS - FOCA Free 3.0". The menu bar includes "Project", "Tools", "Options", "TaskList", "About", and "Donate".

The left sidebar displays a file tree with the following items:

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

The main display area features the FOCA logo (a pink crab) and a text box that reads: "Clean your OpenOffice documents with OOMetaExtractor". Below this is a table of metadata attributes:

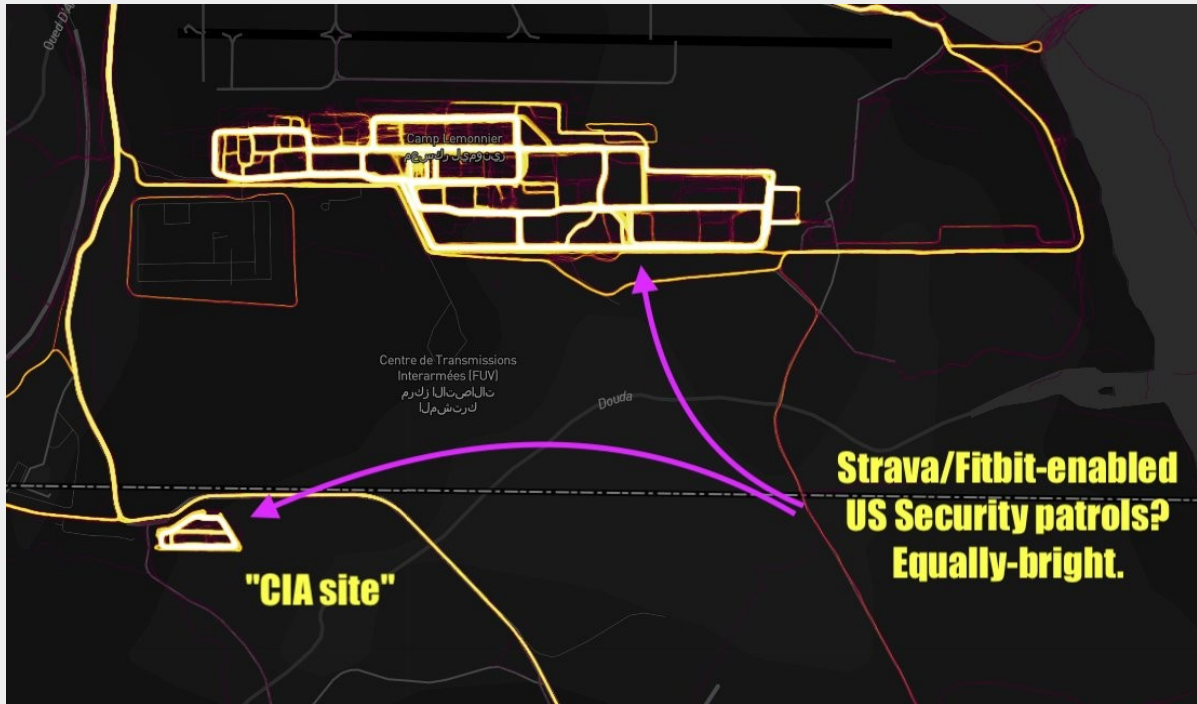
Attribute	Value
<b>Users</b>	
Nataša Pirc	
<b>Folders</b>	
C:\Program%20Files\Microsoft%20Office\MEDIA\CAGCAT10\	
d:\D.sebno\Moj%20dokumenti\My%20Pictures\Microsoftov%20organizator%20izrezk...	
C:\Documents%20and%20Settings\NPirc\Local%20Settings\Temporary%20Internet...	
<b>Software</b>	
Microsoft Office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

The bottom log window displays the following entries:

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\DP_in...
8:24:14	MetadataSearch	low	Document metadata extracted: C:\Documents and Settings\kpkMacF\Local Settings\Temp\Priloga...

At the bottom of the window, there are buttons for "Conf", "Deactivate AutoScroll", "Clear", and "Save log to File". The status bar at the very bottom shows "Metadata analyzed !".

# 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 [a]

<sup>44</sup> 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 low 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

**4AJPE5** Slo PRIJAVA

**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 image shows a Mozilla Firefox browser window displaying a banking application interface. The browser's address bar shows the URL `https://netstik.sparkasse.si/eb/index.asp`. The page content includes a user login field with the text "Uporabnik: [redacted]n", a phone number "01/ 583 6666", and the SPARKASSE logo. A pop-up window is overlaid on the main page, displaying the following information:

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

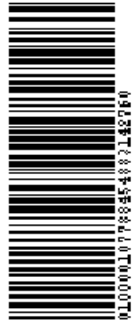

Firefox Help Firefox Support Plug-in FAQ

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

163% LGL - LUTKOVNO GLEDALIŠČE LJUBLJANA

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

Lutkovno gledališče Ljubljana



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

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

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.

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

Končano

Anonimizacija izključena

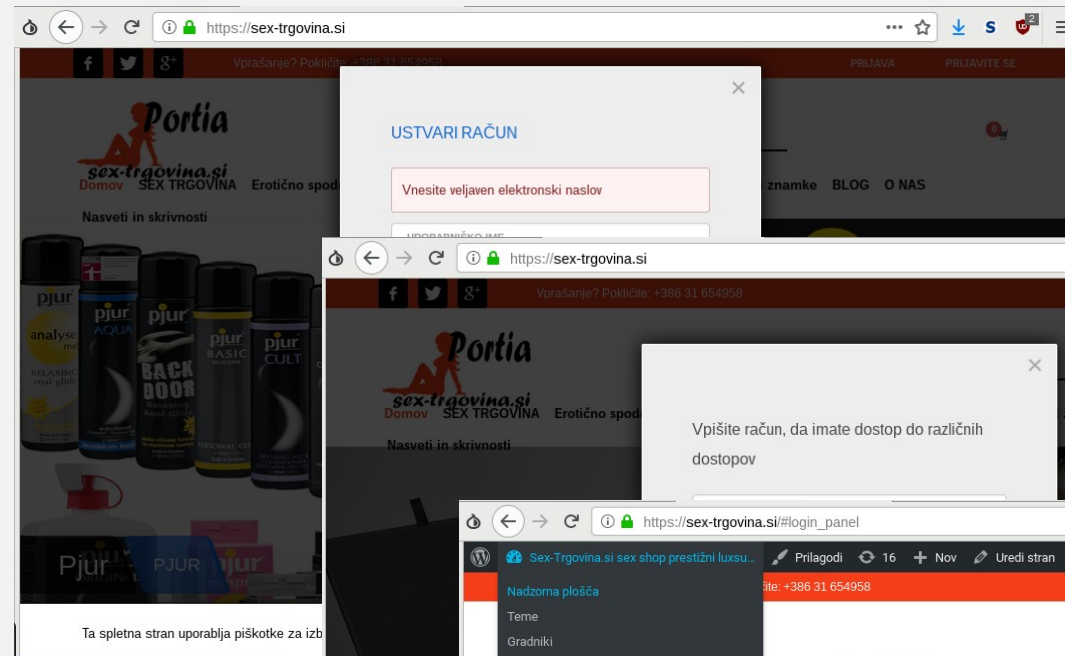
Start prevze... The GIMP Layers, ... Untitled... LGL - LU... http://l... 10:19



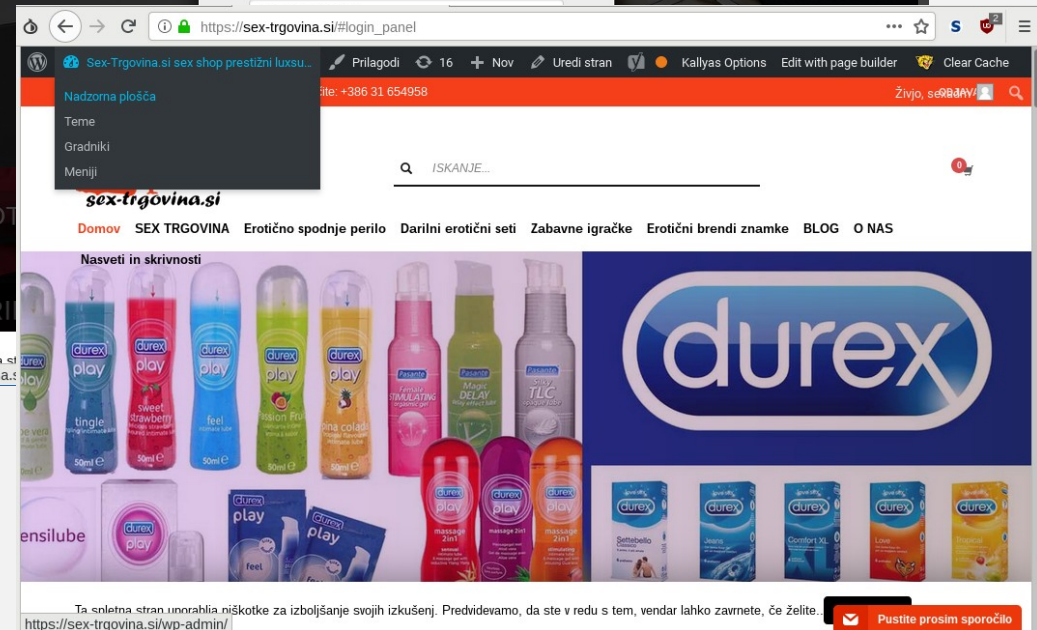
# Napadi preko spletnih aplikacij

How to become a hacker?

1. Register.



2. Login.



3. Become an admin!

# Napadi preko spletnih aplikacij



The screenshot shows a WordPress admin interface for 'sex-trgovina.si'. The main content area displays order details for order number [REDACTED]. The order was paid via PayPal in VISA and MASTERCARD. The status is 'Zaključeno'. The order includes 'K-Y Lubricating Jelly' and 'Osnovna POŠTA PTT'. The sidebar contains various plugins like SEO, AddThis, and MA Connector.

**Podrobnosti za Naročilo št. [REDACTED]**  
Plačilo preko PayPal in VISA in MASTERCARD [REDACTED] Plačano [REDACTED]/2018 ob [REDACTED]  
IP stranke: [REDACTED]

**Splošno**  
Datum ustvaritve: 2018 [REDACTED] @ [REDACTED]  
Status: Zaključeno  
Stranka: Gost

**Plačnik**  
Slovenija  
Telefon: 04 [REDACTED]  
E-poštni naslov: [REDACTED]

**Dostava**  
Slovenija

Izdelek	Cena	Količina	Znesek	DDV
 <a href="#">K-Y Lubricating Jelly</a> Šifra: EP-E20674	8,95 €	x 1	8,95 €	1,97 €
 Osnovna POŠTA PTT Elementi: K-Y Lubricating Jelly x 1			5,50 €	1,21 €
			Dostava:	5,50 €
			DDV:	3,18 €
			Znesek:	17,63 €

**NS8 Order Analysis**  
EQ8 Score: [REDACTED]  
Recommendation: accept ✓  
[Details](#) [Approve](#) [SMS check](#)

**Dejanja za Naročilo**  
Izberite dejanje ...  
[Premakni v smeti](#) [Posodobi](#)

**Opombe za Naročilo**  
Stanje naročila spremenjeno iz V obdelavi v Zaključeno.  
dodana [REDACTED] od irenap  
[Izbršite opombo](#)  
Stanje naročila spremenjeno iz V obdelavi v Zaključeno.  
dodana [REDACTED] od irenap  
[Izbršite opombo](#)  
[NS8] Order approved  
dodana [REDACTED] od irenap  
[Izbršite opombo](#)  
Izdelek je danes prispel, jutri odposlano.

# Napadi preko spletnih aplikacij

<input type="checkbox"/>	Customer Name	Date	Status	Amount
<input type="checkbox"/>	[redacted]rena [redacted]	Feb 5, 2019	Zadržano	€ 133,54
<input type="checkbox"/>	[redacted]	Jan 12, 2019	Zaključeno	€ 238,06
<input type="checkbox"/>	[redacted]	Jan 9, 2019	Zaključeno	€ 46,98
<input type="checkbox"/>	[redacted]Milos [redacted]	Jan 8, 2019	Preklicano	€ 39,18
<input type="checkbox"/>	[redacted]	Jan 8, 2019	Preklicano	€ 39,18
<input type="checkbox"/>	[redacted]	Jan 8, 2019	Preklicano	€ 39,18
<input type="checkbox"/>	[redacted]	Dec 17, 2018	V obdelavi	€ 84,19
<input type="checkbox"/>	[redacted]Jernej [redacted]	Nov 19, 2018	Zaključeno	€ 75,04
<input type="checkbox"/>	[redacted]	Nov 13, 2018	V obdelavi	€ 17,64
<input type="checkbox"/>	[redacted]	Nov 13, 2018	V obdelavi	€ 73,64
<input type="checkbox"/>	[redacted]	Okt 17, 2018	V obdelavi	€ 35,99
<input type="checkbox"/>	[redacted]Barbara [redacted]	Sep 14, 2018	Plačilo v teku	€ 52,78

# Napadi preko spletnih aplikacij

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 title: Portia Erotica sex shop

Navigation: 14 + Nov Kallyas Options Živo, sexadm

Left sidebar (plugins/widgets):

- 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]

**Dostava** [redacted]  
[redacted]  
[redacted]

**Telefon:** [redacted]

**Strankina opomba:** Paketomat

**E-poštni naslov:** [vroca-nina@\[redacted\]](mailto:vroca-nina@[redacted])

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

Chat messages:

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](#)

# Interne aplikacije...

Mozilla Firefox browser window showing the URL `https://erisk.sigov.si/erisk/index.faces`. The page title is "e-RISK DUNZ". The user is logged in as "Matej Kovačič / KOMISIJA ZA PREPREČEVANJE KORUPCIJE". The date is "Četrtek, 10. marec, 2011". The page includes a search bar and a navigation menu with "Iskanje".

Podatki o strani - `https://erisk.sigov.si/erisk/index.faces`. The dialog shows tabs for "Splošno", "Večpredstavnost", "Dovoljenja", and "Varnost".

Piškoti dialog box for the domain `sigov.si`. It lists cookies for `erisk.sigov.si` with names `JSESSIONID`, `LtpaToken`, and `LtpaToken2`. The `JSESSIONID` cookie details are shown below:

Ime:	JSESSIONID
Vsebina:	0000IXLMzITJWIUZUQTVL_er6b:C075CB88E4DE844900001B00
Gostitelj:	erisk.sigov.si
Pot:	/
Poslan za:	Vse povezave
Preteče:	na koncu seje

Buttons: "Odstrani piškot", "Odstrani vse piškote", "Zapri". A red arrow points to the "Vsebina" field.

Mozilla Firefox browser window showing the URL `https://erisk.sigov.si/erisk/logoff`. The page title is "Podatki o strani - https://erisk.sigov.si/erisk/logoff". The dialog shows tabs for "Splošno", "Dovoljenja", and "Varnost".

The "Piškoti" dialog box is also open, showing the same list of cookies as in the previous screenshot. A red arrow points to the "Vsebina" field.

The "Podatki o strani" dialog box shows the "Varnost" tab with the following text:

Identiteta spletne strani  
Spletna stran: **erisk.sigov.si**  
Lastnik: **Ta spletna stran ne vsebuje podatkov o lastništvu.**  
Preveril: **state-institutions**

Buttons: "Preglej digitalno potrdilo", "Preglej piškote", "Preglej shranjena gesla".

# 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?

The image shows a screenshot of a Mozilla Firefox browser window displaying a search result on the website **simobil.si**. The search query is `<h3>Dimitrij+Rupel+postal+svetovalec+</h3>`. The search results show a profile for **Dimitrij Rupel postal svetovalec uprave Simobila**, identified as an **IT specialist v CRM skupini, zadolžen za DMS področje (m/ž)**. The profile includes a photo of a man and a short biography stating that he is a former director of sales at Simobil, who has been working in CRM since January 2007. The browser's address bar shows the URL `http://www.simobil.si/sl/search.cp2?q=<h3>Dimitrij+Rupel+postal+svetovalec+</h3>`. The browser's taskbar at the bottom shows various system icons and the date **pet 16. jan. 10:28**.

# Zaupanje vsebini na spletu?

Vaš vnos:  
**XSS ALL OVER THE PLACE**

Mail and Msn : X-Turk@worldhac

Slovensko satanistično gibanje  
Pavlihove domače strani na internetu: [Prva stran](#) | [Aktualno](#) | [Povezave](#)

**Slovensko satanistično gibanje**  
se predstavi

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 dogmatski 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

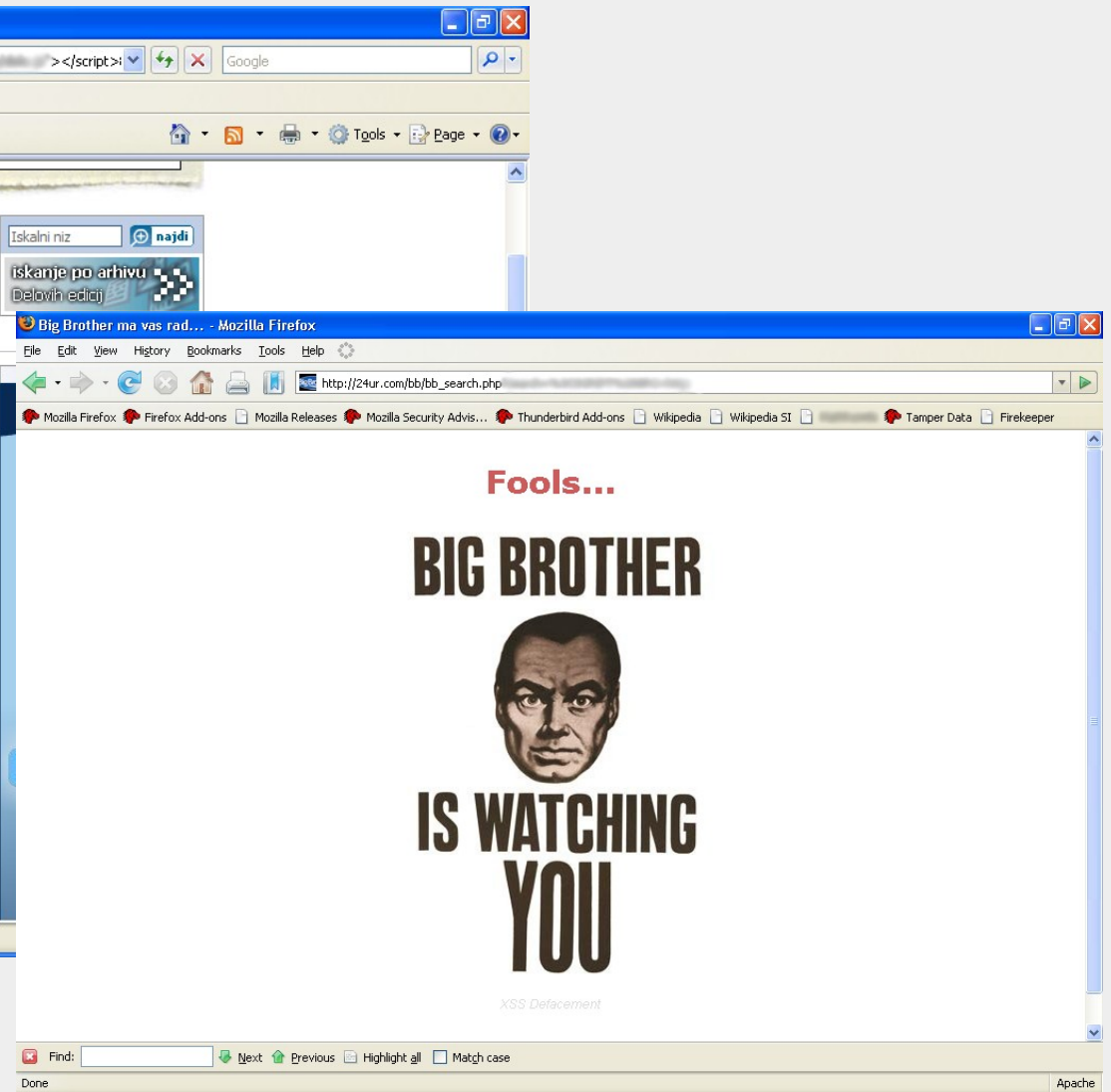
Razobličenje spletne strani  
rimokatoliške cerkve.



# Zaupanje vsebini na spletu?

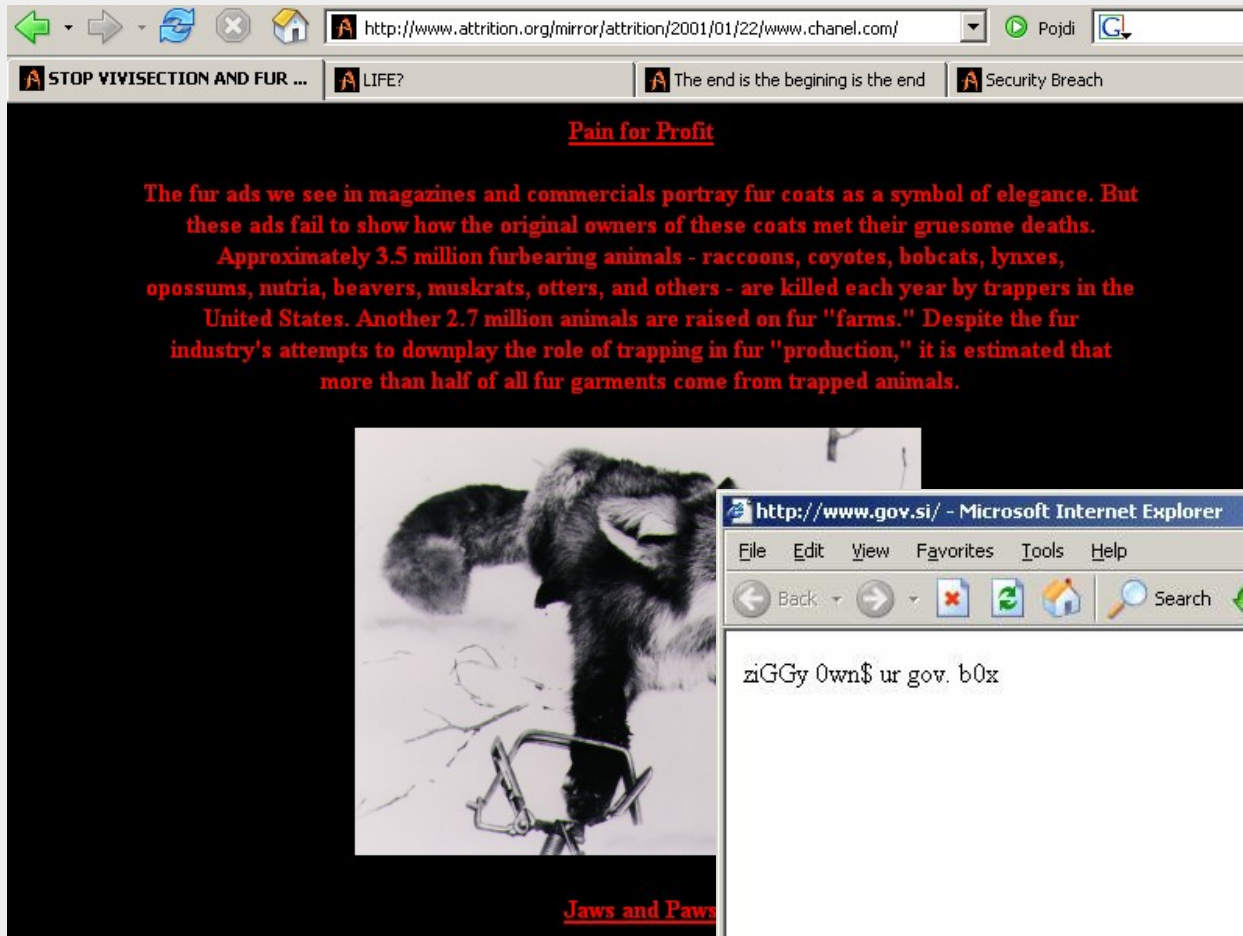


Lažna novica na spletni strani časnika DELO (XSS napad).

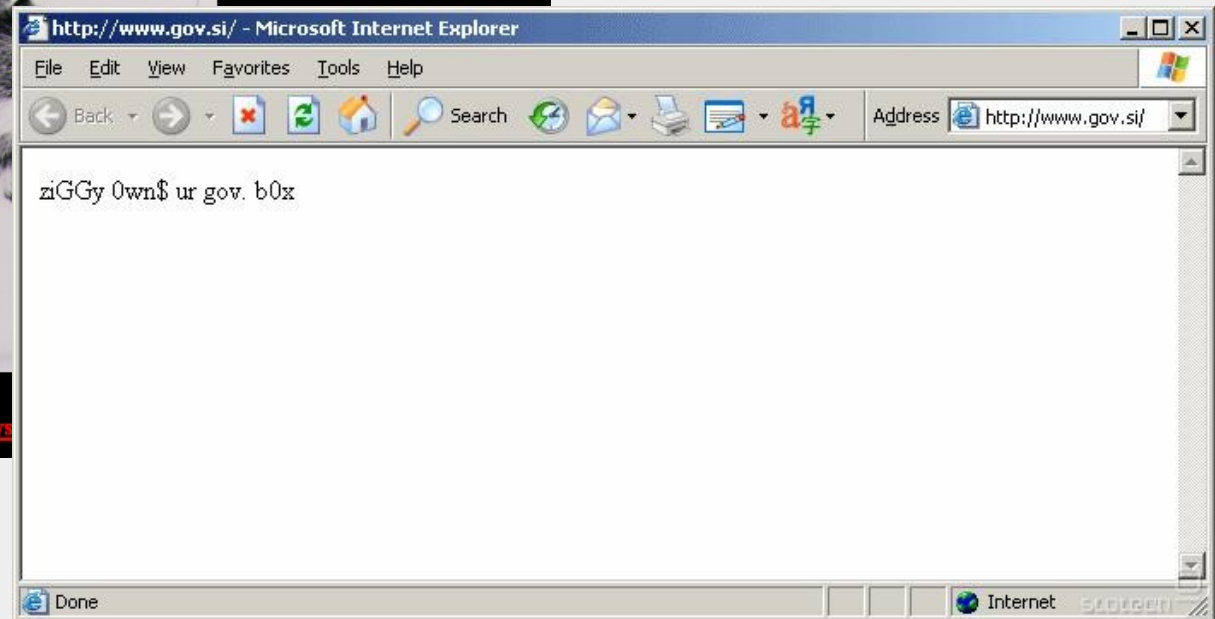


"Big Brother" na 24ur.com (XSS napad).

# Zaupanje vsebini na spletu?



Razobličenje spletne strani  
modne hiše Chanell.com



Razobličenje vladne strani (gov.si).

Prevare (scam) in socialni  
inženiring

# Scam (prevara)

---

A scam is a deceptive scheme or trick used to cheat someone out of something, especially money. Scam is also a verb meaning to cheat someone in such a way.

**noun:** *a confidence game or other fraudulent scheme, especially for making a quick profit; swindle.*

**verb** (*scammed, scamming*): *to cheat or defraud (someone) with a scam.*

# Tipi prevar

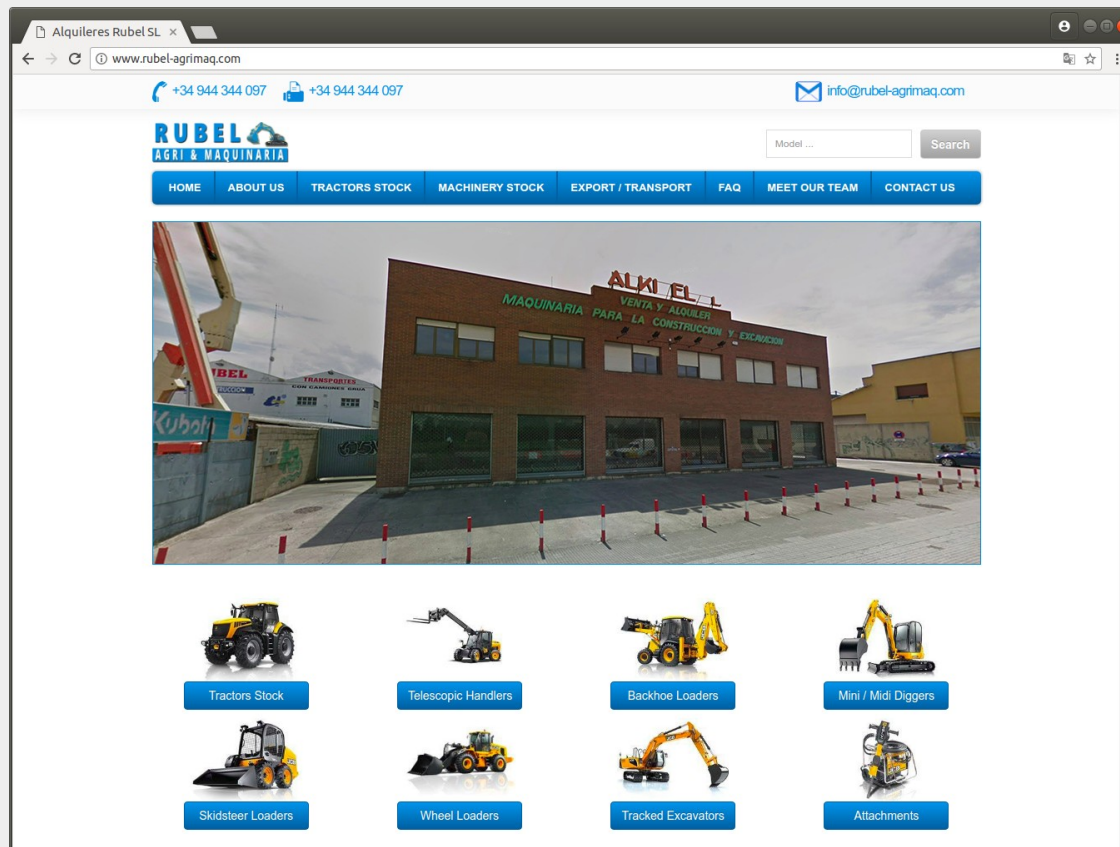
---

- Poskusi pridobivanja osebnih podatkov.
- Prodaja ali nakup.
- Zmenki in romantika.
- Lažna dobrodelnost.
- Investicije.
- Službe in zaposlitev.
- Grožnje in izsiljevanje.
- Nepričakovan denar (dediščina, nagrade,...).
- Piramidne sheme.
- Prevare z lažnim predstavljanjem za državne organe.

# Prevarantska spletna trgovina #1

Zgodba:

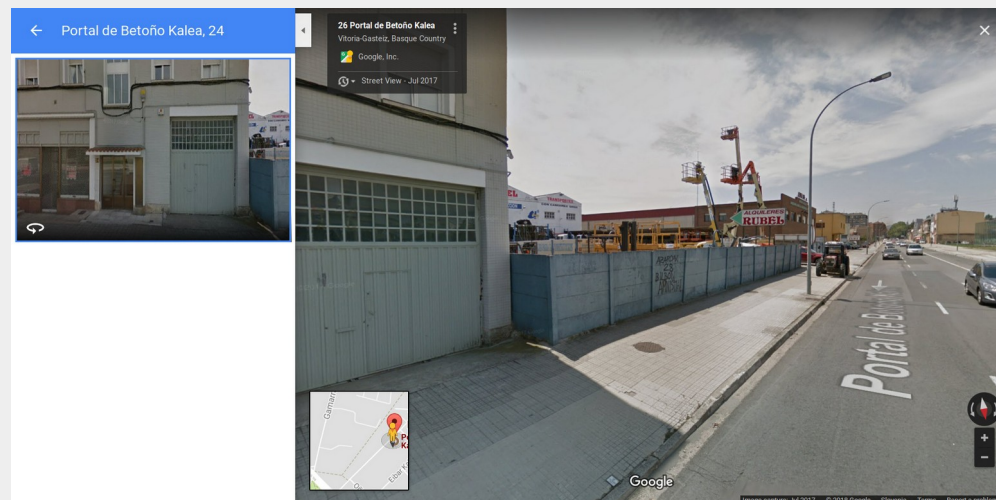
- Uporabnik je želel kupiti manjši bager. Našel je spletno trgovino z zelo ugodnimi cenami.



# Prevarantska spletna trgovina #1

Zgodba:

- Nizke cene so mu bile sumljive, zato se je odločil za dodatno preverjanje.
- Preveril je obstoj podjetja, pridobil bilanco podjetja, ki je vsebovala podatke o lastnikih, letni promet, število zaposlenih...
- Na Google StreetView je preveril celo sedež podjetja.



# Prevarantska spletna trgovina #1

---

Zgodba:

- Preko e-pošte je kontaktiral predstavnika podjetja. Komunikacija je bila hitra, profesionalna in v dobri angleščini.
- Vendar pa je podjetje želelo, da kupnino nakaže na bančni račun njihove podružnice na Portugalskem, *“da bi se izognili nekaj davkom”*.
- Ko je želel preveriti VIN številko delovnega stroja, se mu predstavniki podjetja niso več oglašali.



# Prevarantska spletna trgovina #1

---

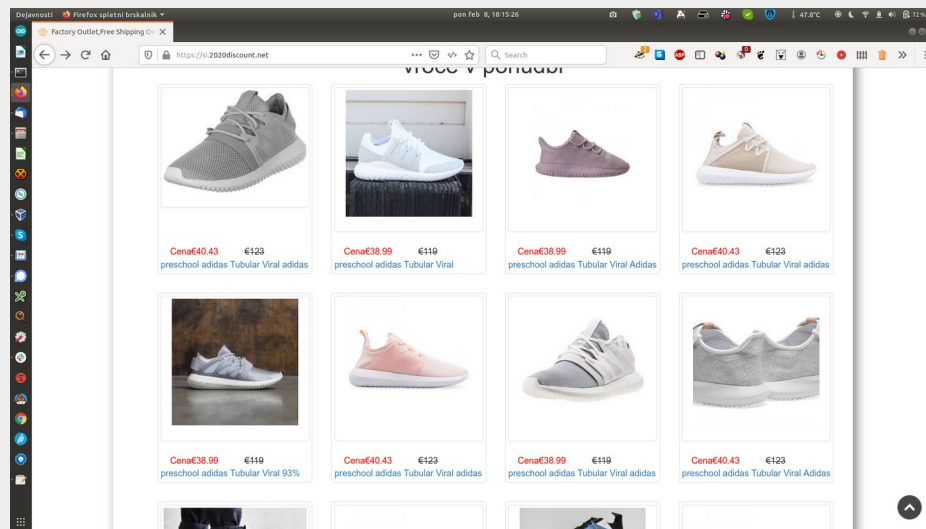
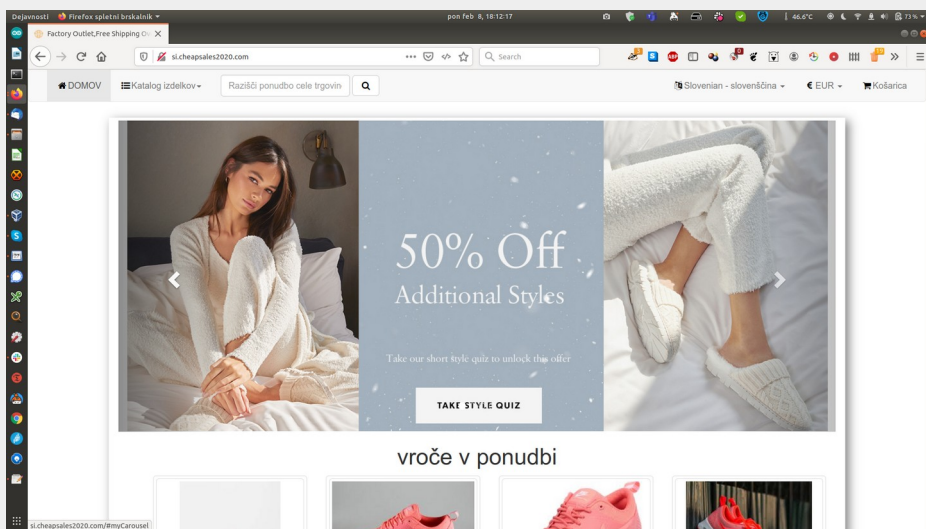
## Analiza:

- Spletni strežnik se je nahajal v Rusiji (omrežje *nic.ru*). Prav tako je bila v Rusiji registrirana domena.
- Iskanje je pokazalo, da je bila podobno zveneča domena (*rubel-maquinaria.com*) pred tem registrirana v Maleziji. Storitvi so upravljali tudi goljufivo spletno stran z gradbenimi stroji na domeni *budo-maszyny.com* (nahajala naj bi se na Poljskem). Uporabljali so enako spletno predlogo. Obe spletni strani sta bili razkriti kot prevarantski in umaknjeni s spleta.
- Danes domena *rubel-agrimaq.com* ni več dostopna.

# Prevarantska spletna trgovina #2

Preko neželjene e-pošte so storilci oglaševali več lažnih spletnih strani, ki so v slovenskem jeziku ponujale poceni blago.

Različne, a podobno zveneče domene: *si.2020discount.net*, *sisale2021.com*, *si.cheapsales2020.com*, itd.



# Prevarantska spletna trgovina #2

---

Prvi opozorilni znak:

- Zelo poceni izdelki (*“Če je preveč dobro, da bi bilo res, potem najverjetneje ni res”*).

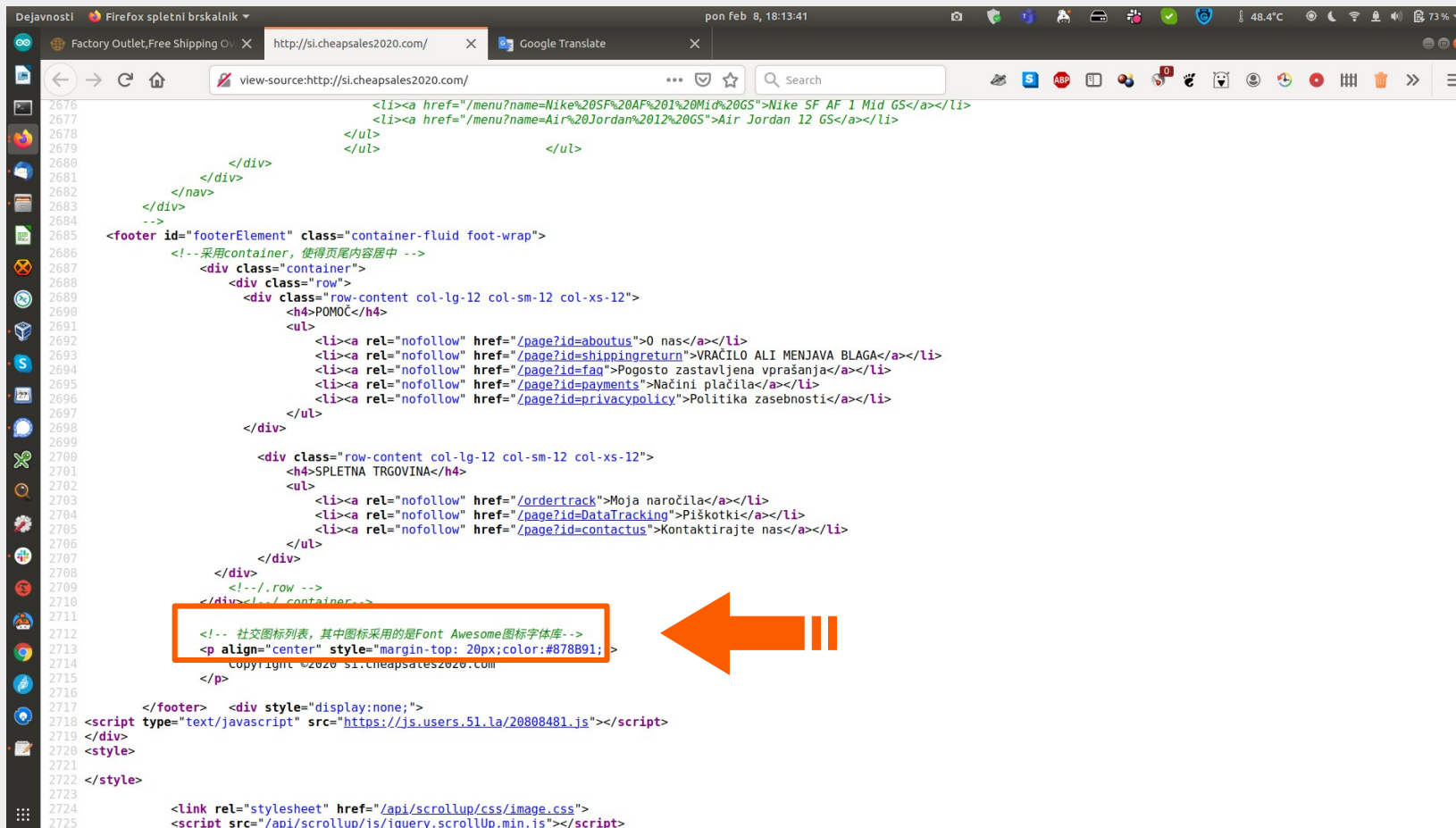
Poglobljena analiza:

- IP naslov skrit za Cloudflare omrežjem.
- Spletne strani so delovale preko HTTPS (zagotavljal ga je Cloudflare).

# Prevarantska spletna trgovina #2

## Poglobljena analiza:

- komentarji HTML kode v kitajščini.



```
2676 <li><a href="/menu?name=Nike%20SF%20AF%201%20Mid%20GS">Nike SF AF 1 Mid GS</a></li>
2677 <li><a href="/menu?name=Air%20Jordan%2012%20GS">Air Jordan 12 GS</a></li>
2678 </ul>
2679 </ul>
2680 </div>
2681 </div>
2682 </nav>
2683 </div>
2684 -->
2685 <footer id="footerElement" class="container-fluid foot-wrap">
2686 <!-- 采用container, 使得页尾内容居中 -->
2687 <div class="container">
2688 <div class="row">
2689 <div class="row-content col-lg-12 col-sm-12 col-xs-12">
2690 <h4>POMOČ</h4>
2691 <ul>
2692 <li><a rel="nofollow" href="/page?id=aboutus">0 nas</a></li>
2693 <li><a rel="nofollow" href="/page?id=shippingreturn">VRACILO ALI MENJAVA BLAGA</a></li>
2694 <li><a rel="nofollow" href="/page?id=fag">Pogosto zastavljena vprašanja</a></li>
2695 <li><a rel="nofollow" href="/page?id=payments">Načini plačila</a></li>
2696 <li><a rel="nofollow" href="/page?id=privacypolicy">Politika zasebnosti</a></li>
2697 </ul>
2698 </div>
2699
2700 <div class="row-content col-lg-12 col-sm-12 col-xs-12">
2701 <h4>SPLETNA TRGOVINA</h4>
2702 <ul>
2703 <li><a rel="nofollow" href="/ordertrack">Moja naročila</a></li>
2704 <li><a rel="nofollow" href="/page?id=DataTracking">Piškotki</a></li>
2705 <li><a rel="nofollow" href="/page?id=contactus">Kontaktirajte nas</a></li>
2706 </ul>
2707 </div>
2708 </div>
2709 <!-- /.row -->
2710 </div></div>
2711
2712 <!-- 社交图标列表, 其中图标采用的是Font Awesome 图标字体库 -->
2713 <p align="center" style="margin-top: 20px;color:#878B91;">
2714 Copyright ©2020 S1.cheapsales2020.com
2715 </p>
2716
2717 </footer> <div style="display:none;">
2718 <script type="text/javascript" src="https://js.users.51.la/20808481.js"></script>
2719 </div>
2720 <style>
2721
2722 </style>
2723
2724 <link rel="stylesheet" href="/api/scrollup/css/image.css">
2725 <script src="/api/scrollup/js/jquery.scrollUp.min.js"></script>
```



# Prevarantska spletna trgovina #2

Poglobljena analiza:

- ...ki je vodila na kitajske strežnike.

```
matej@cryptomania: ~  
Datoteka Uredi Pogled Poišči Terminal Pomoč  
  
matej@cryptomania:~$ ping -c1 ia.51.la  
PING d2cb5ad7002c4066.huaweisafedns.com (183.131.207.66) 56(84) bytes of data.  
64 bytes from 183.131.207.66 (183.131.207.66): icmp_seq=1 ttl=48 time=282 ms  
  
--- d2cb5ad7002c4066.huaweisafedns.com ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 282.793/282.793/282.793/0.000 ms  
matej@cryptomania:~$ ping -c1 51.la  
PING 51.la (14.17.102.104) 56(84) bytes of data.  
  
--- 51.la ping statistics ---  
1 packets transmitted, 0 received, 100% packet loss, time 0ms  
  
matej@cryptomania:~$ ^C  
matej@cryptomania:~$ ping -c1 uuid.users.51.la  
PING uuid.users.51.la (14.17.102.107) 56(84) bytes of data.  
64 bytes from 14.17.102.107 (14.17.102.107): icmp_seq=1 ttl=47 time=232 ms  
  
--- uuid.users.51.la ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 232.272/232.272/232.272/0.000 ms  
matej@cryptomania:~$
```

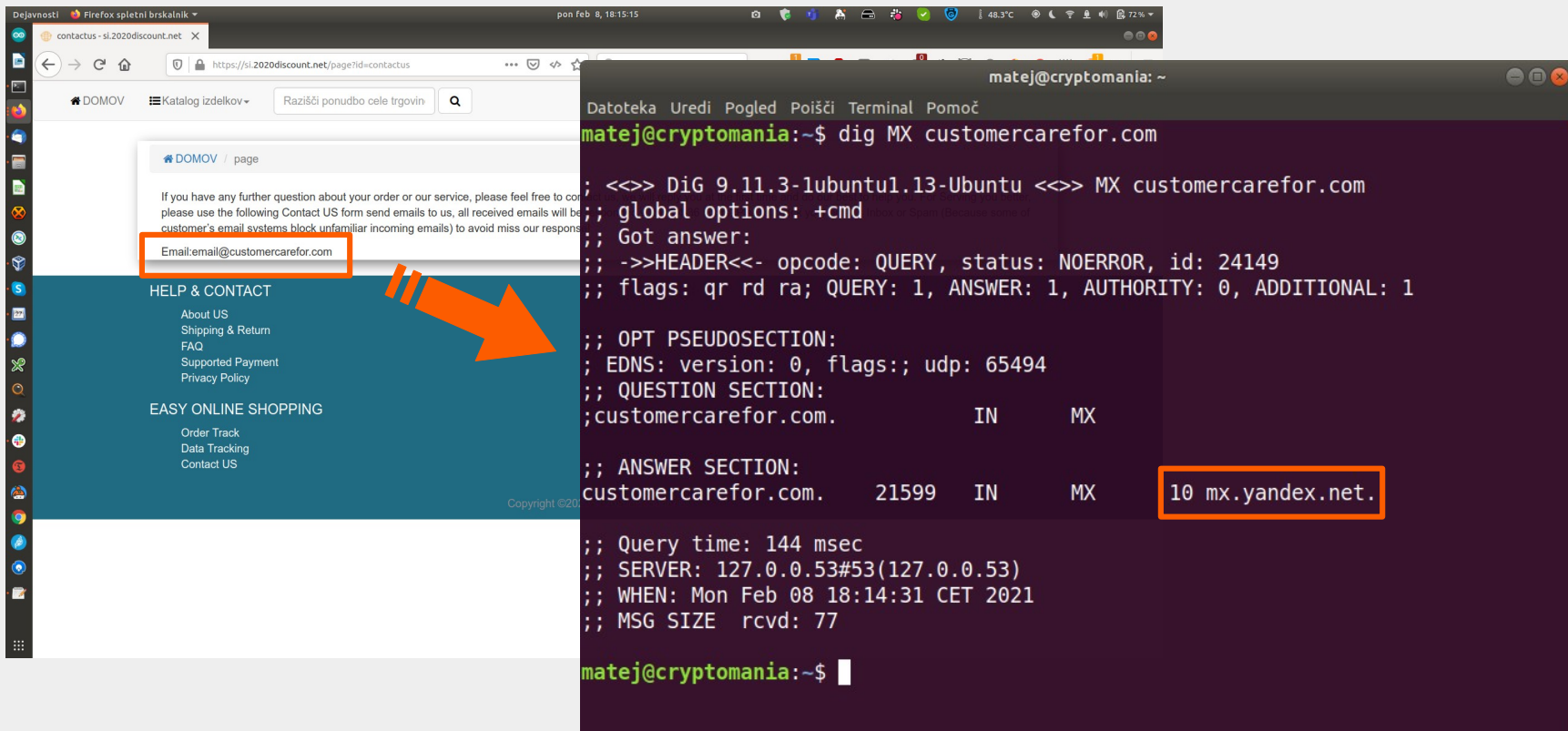
huaweisafedns.com  
lociran na švicarskem IP  
naslovu, domena registrirana  
pri Alibaba Cloud Computing  
(Peking)

IP naslovi 14.17.100.0/22  
dodeljeni CT-FOSHAN-IDC  
CHINANET Guangdong province  
network, CN

# Prevarantska spletna trgovina #2

## Poglobljena analiza:

- kontaktni e-naslov (email@customercarefor.com) na ruskih strežnikih (Yandex.net).



The image shows a screenshot of a website and a terminal window. The website is a contact page for 'DOMOV' with a contact form and a footer containing links like 'HELP & CONTACT' and 'EASY ONLINE SHOPPING'. The email address 'Email:email@customercarefor.com' is highlighted with a red box. A red arrow points from this box to a terminal window. The terminal window shows the command 'dig MX customercarefor.com' and its output, which includes the MX record '10 mx.yandex.net.' highlighted with a red box.

```
matej@cryptomania:~$ dig MX customercarefor.com
;<>> DiG 9.11.3-lubuntu1.13-Ubuntu <>> MX customercarefor.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 24149
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags::; udp: 65494
;; QUESTION SECTION:
;customercarefor.com.          IN      MX

;; ANSWER SECTION:
customercarefor.com.  21599  IN      MX      10 mx.yandex.net.

;; Query time: 144 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Feb 08 18:14:31 CET 2021
;; MSG SIZE rcvd: 77

matej@cryptomania:~$
```

# Zbiranje osebnih podatkov

---

Zgodba:

- Google Ads oglasi na spletnih straneh slovenskih medijev so oglaševali intervju z znano slovensko novinarko o njenih zdravstvenih težavah in lažnem zdravilu, ki ji je pomagalo.
- Lažni intervju je izgledal podobno kot bi bil objavljen na znani novičarski strani.
- Besedila so bila slovnično zelo pravilna (boljše kot prevodi z Google Translate).



# Zbiranje osebnih podatkov

Zgodba:

- Komentarji pod člankom so bili večinoma pozitivni (a tudi negativni!), napisani s strani lažnih uporabnikov s slikami in s slovensko zvenečimi imeni.



# Zbiranje osebnih podatkov

Analiza:

- Lažna spletna stran je gostovala na Github Pages.
- Uporabnike so vabili, da se registrirajo za prejem brezplačnega zdravila.
- Vnosni obrazec je zbiral osebne podatke, **ne pa tudi podatkov o kreditni kartici.**
- Vnosni obrazec je gostoval na ruskem spletnem strežniku.



POZOR!  
Nacionalni program

Izpolnite obrazec in pridobite promocijsko ceno! Oglasne enote so omejene!

Obrazec za registracijo

CENA promocijski **39 EUR**

**50** embalaža na zalogi!

Ime

Telefonska številka

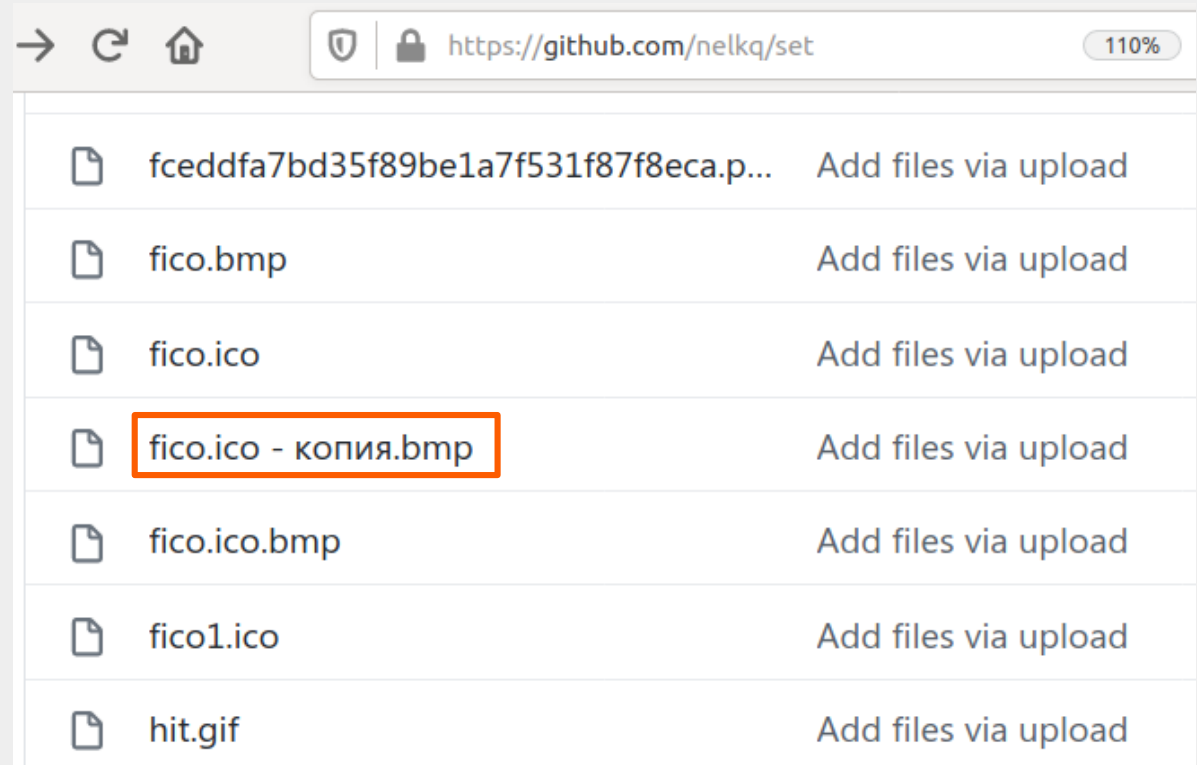
**HOČEM!**

\* cena na porcijo

# Zbiranje osebnih podatkov

Analiza:

- Najdena je bila datoteka z imenom v ruskem jeziku ("fico.ico - копия.bmp").
- Komentarji HTML kode v ruskem jeziku.



# Zbiranje osebnih podatkov

---

## Analiza:

- Z nadaljnjim iskanjem smo našli kontaktne informacije (e-naslov, mobilni telefon) osebe, ki je registrirala lažno domeno in ugotovili, da gre za Rusa, ki živi na območju Moskve.
- Ta oseba se je zahvaljevala prevajalcem na spletni strani *kwork.ru* za "hitre in točne prevode" v različne vzodnoevropske jezike (to razloži kvaliteto prevodov na lažnih spletnih straneh).

# Zbiranje osebnih podatkov

---

## Analiza:

- Našli smo podobne prevare, namenjene publiku na Poljskem in Češkem (lažni intervjuji v lokalnem jeziku, kjer so se pojavljale njihove lokalne slavne osebe,...).
- O lažnih straneh so bili obveščeni na Github Pages in lažne strani so bile umaknjene. Žal pa se novi lažni članki še vedno pojavljajo preko Google Ads oglasov, prevarantje pa odpirajo nove račune na Github Pages...

# Usmerjen napad preko Facebooka

---

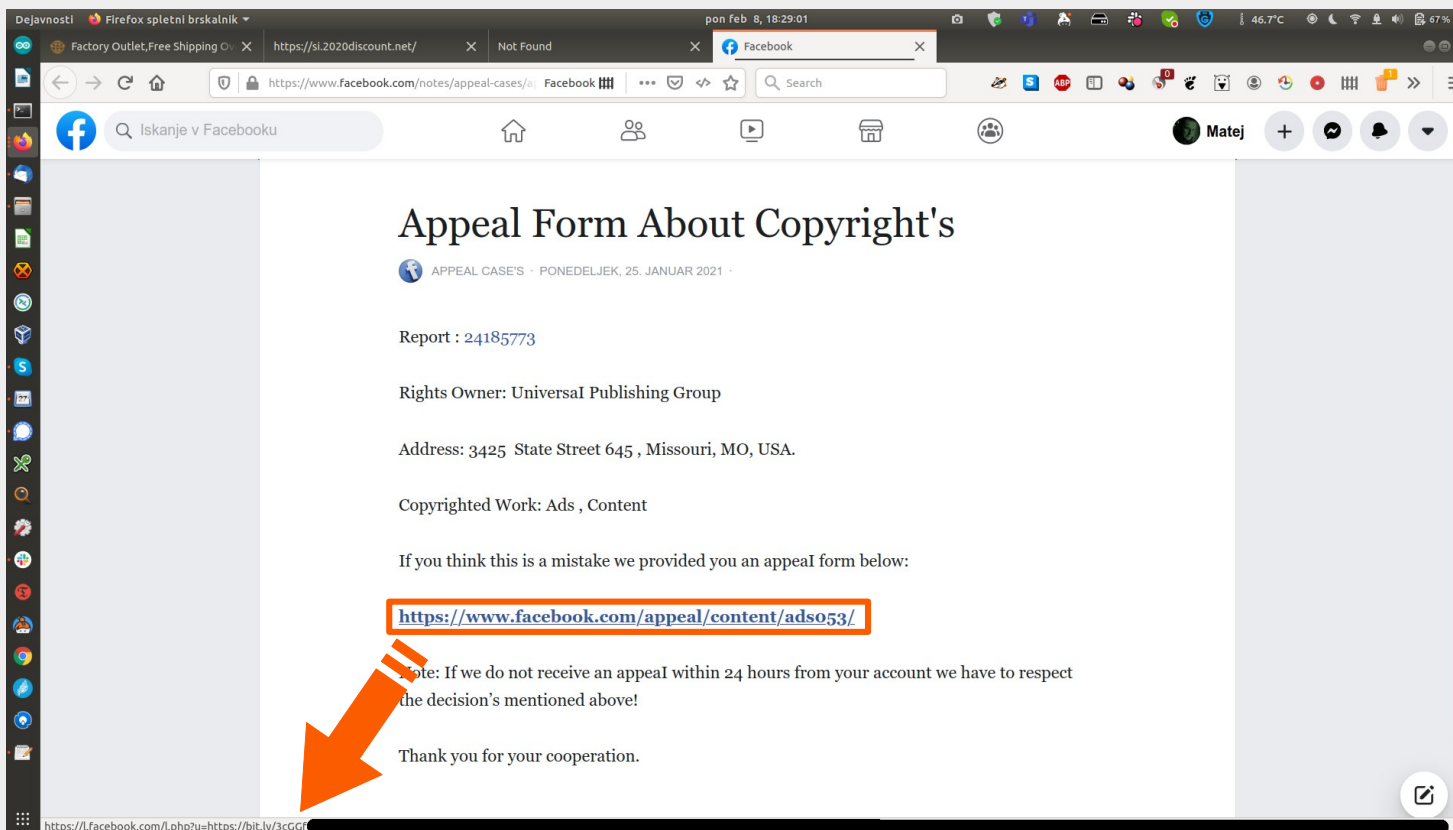
Zgodba:

- Uporabnik je na svojem Facebook profilu objavil sliko.
- Nekaj dni za tem (8. februarja 2021) je prejel obvestilo, da objava krši avtorske pravice in da se mora o kršitvi izjasniti.
- E-pošta je vsebovala povezavo na Facebook.
- Vendar pa je povezava kazala na Facebook Notes – gre za del Facebooka, ki ga ustvarjajo uporabniki (a se nahaja na Facebookovi domeni).

# Usmerjen napad preko Facebooka

Kaj se je v resnici zgodilo:

- Facebook Notes stran je vsebovala povezavo na "pritožbo". URL je kazal na bit.ly URL skrajševalec...



The screenshot shows a Facebook interface on a Firefox browser. The main content is a note titled "Appeal Form About Copyright's" posted by "APPEAL CASE'S" on January 25, 2021. The note contains the following text:

Report : 24185773

Rights Owner: Universal Publishing Group

Address: 3425 State Street 645 , Missouri, MO, USA.

Copyrighted Work: Ads , Content

If you think this is a mistake we provided you an appeal form below:

<https://www.facebook.com/appeal/content/ads053/>

Note: If we do not receive an appeal within 24 hours from your account we have to respect the decision's mentioned above!

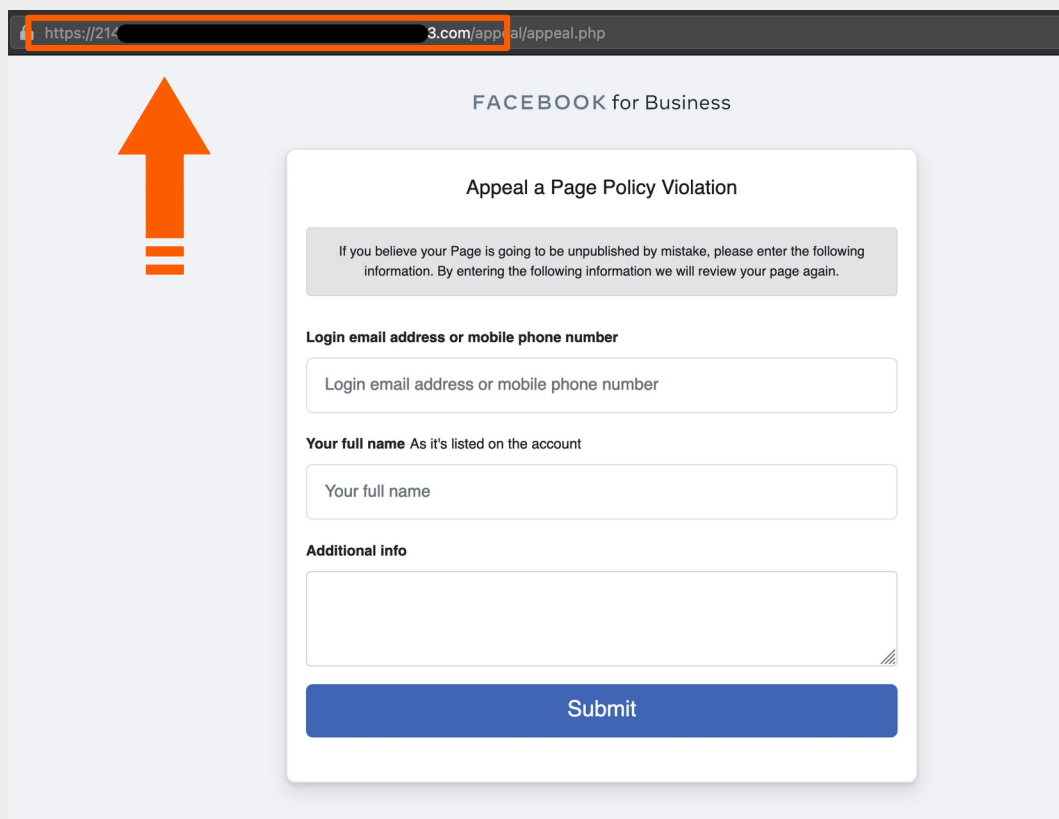
Thank you for your cooperation.

A red arrow points to the highlighted URL. The browser's address bar at the bottom shows the URL: <https://l.facebook.com/l.php?u=https://bit.ly/3cGG...>

# Usmerjen napad preko Facebooka

Kaj se je v resnici zgodilo:

- ...bit.ly je uporabnika preusmeril na storilčevo domeno, registrirano v ZDA (3. februarja 2021).



The screenshot shows a web browser address bar with the URL `https://213.com/appeal/appeal.php`. Below the browser, a red arrow points upwards towards the URL. The main content is a Facebook Business appeal form titled "Appeal a Page Policy Violation". The form includes a header "FACEBOOK for Business", a sub-header "Appeal a Page Policy Violation", and a grey instruction box: "If you believe your Page is going to be unpublished by mistake, please enter the following information. By entering the following information we will review your page again." The form contains three input fields: "Login email address or mobile phone number", "Your full name As it's listed on the account", and "Additional info". A blue "Submit" button is at the bottom.

https://213.com/appeal/appeal.php

FACEBOOK for Business

Appeal a Page Policy Violation

If you believe your Page is going to be unpublished by mistake, please enter the following information. By entering the following information we will review your page again.

**Login email address or mobile phone number**

Login email address or mobile phone number

**Your full name** As it's listed on the account

Your full name

**Additional info**

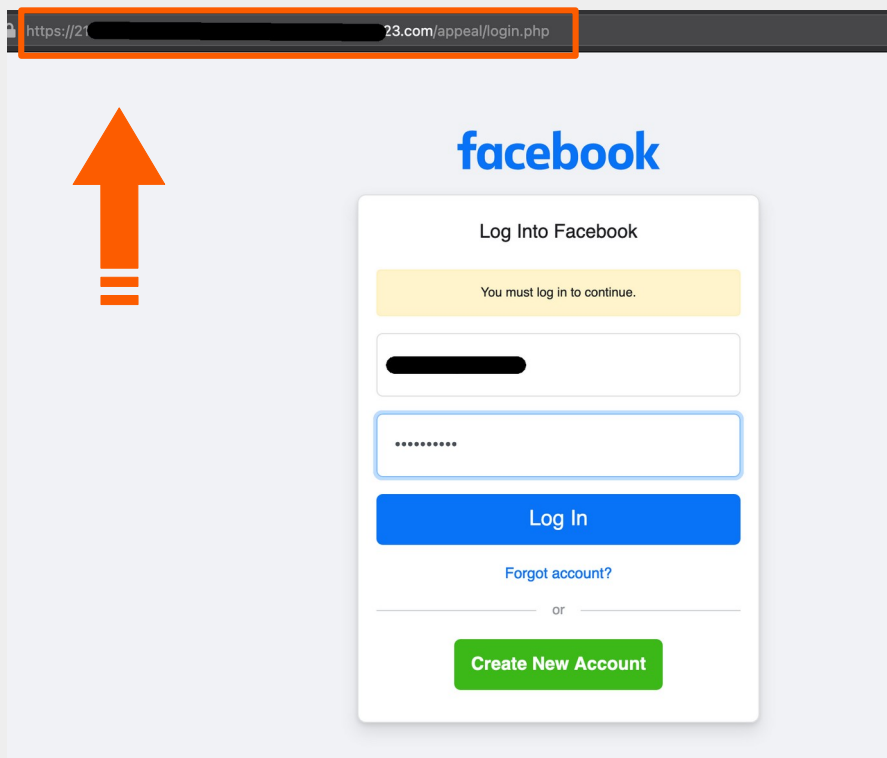
Submit



# Usmerjen napad preko Facebooka

Kaj se je v resnici zgodilo:

- ...ko je uporabnik oddal pritožbo, je stran od njega zahtevala, da se ponovno prijavi v Facebook ter mu ukradla geslo.



Ciljana oseba je bila lokalni poslovnež. Incident je bil posredovan na policijo, ki je začela s preiskavo.

# Phishing napad na HBGary

```
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 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
uid=0(root) gid=0(root)
groups=0(root),1200(varmistus)
```

# Zaščita pred prevarami

---

- Zavedajte se, da prevare na internetu obstajajo.
- Vedite s kom imate opravka oz. s kom komunicirate.
- Ne odpirajte sumljivih povezav ali priponk v e-pošti.
- Previdno pri spletnem nakupovanju.
- Pred vnosom gesla ali finančnih podatkov se prepričajte, da ste na pravi spletni strani, ki je dostopna na HTTPS povezavi.
- Ne odgovarjajte na sporočila ali telefonske klice, kjer vas sprašujejo za oddaljen dostop do vašega računalnika.
- Ne odgovarjajte na sporočila ali zgrešene klice iz števil, ki jih ne poznate.
- Hranite svoje osebne podatke in gesla (vključno z bančnimi podatki) na varnem mestu.
- Poskrbite za to, da bodo vaši računalniki in mobilne naprave ustrezno zavarovani.
- Redno pregledujte varnostne in zasebnostne nastavitve na socialnih omrežjih.
- Bodite pozorni, če kdo želi vaše osebne podatke ali denar.

**Če ponudba izgleda pre dobro, da bi bila resnična, potem najverjetneje tudi ni resnična.**

# Varovanje informacijskih sistemov

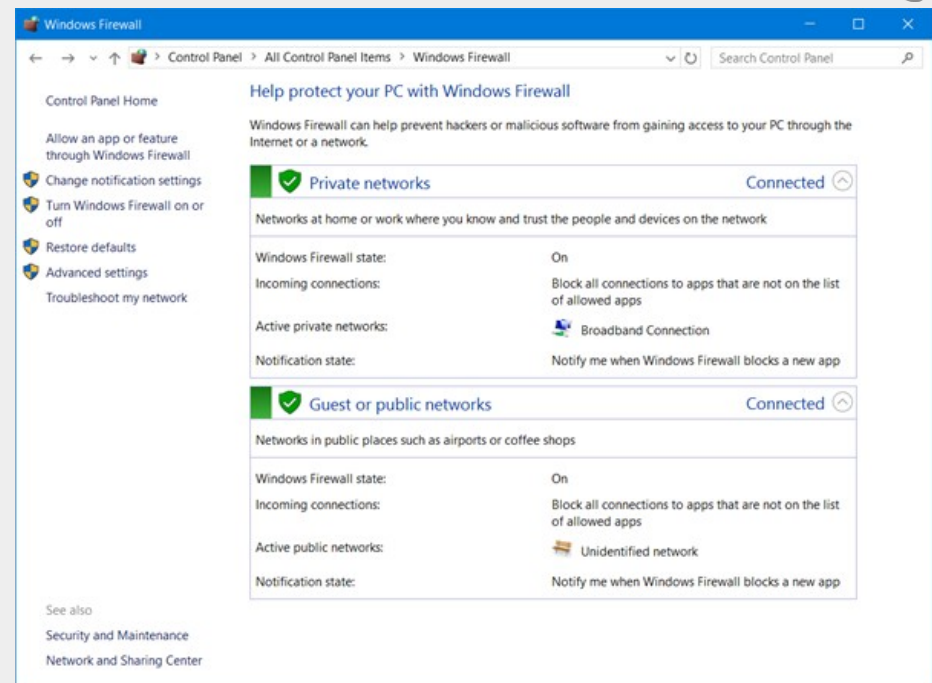
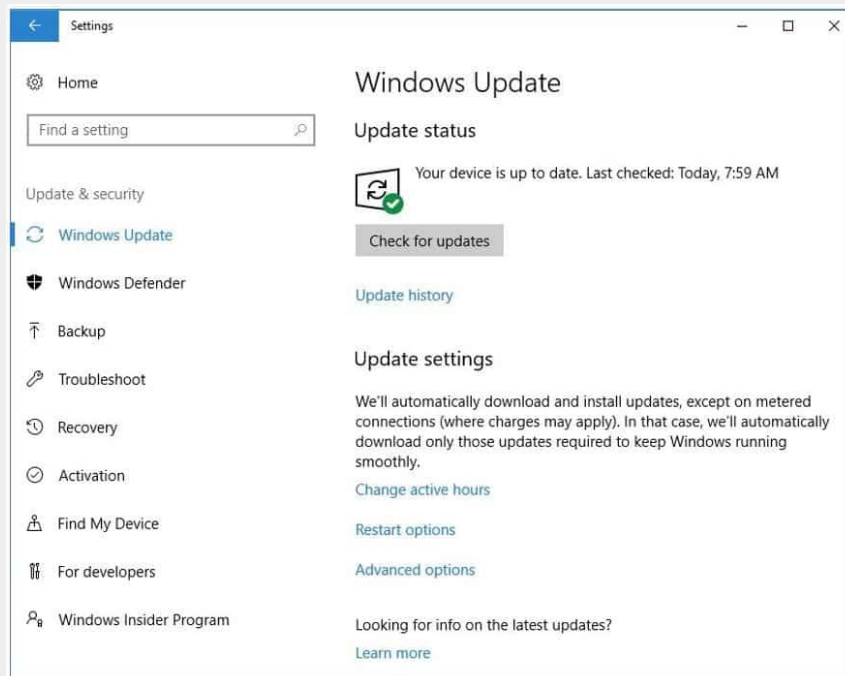
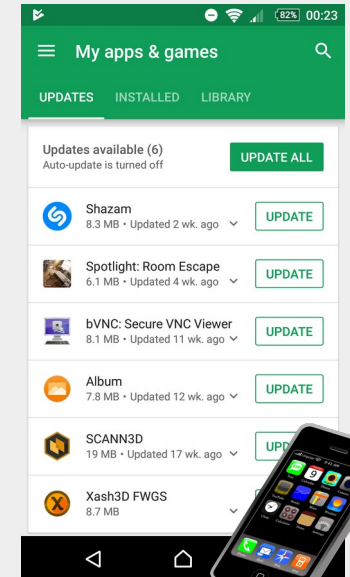
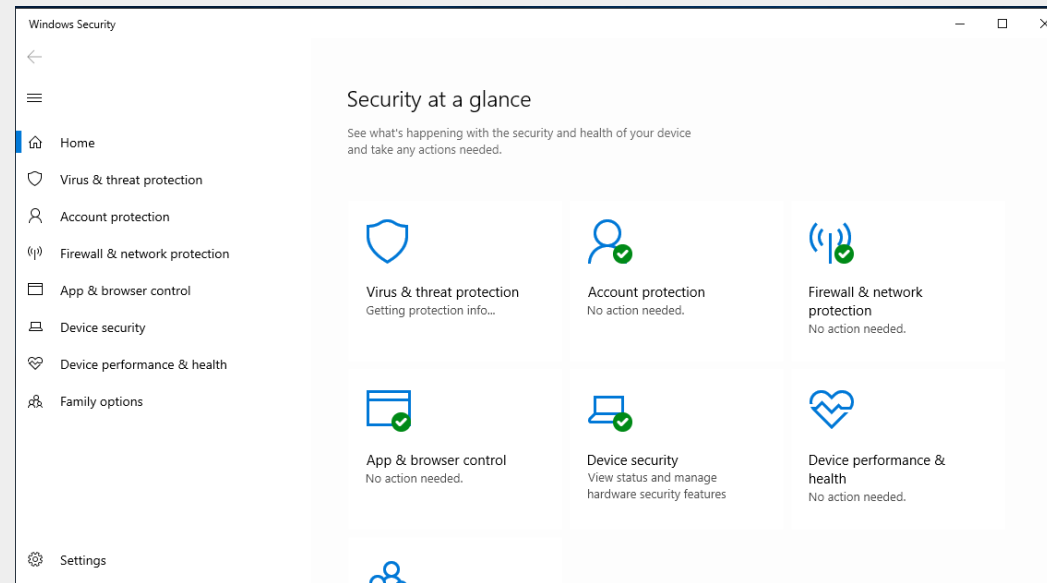
# Osnovna zaščita IT sistemov

---

Nekatere tehnike osnovne zaščite računalniških sistemov:

- uporaba ustreznih (in »nerecikliranih«) gesel;
- uporaba dvo- in multifaktorske avtentikacije kjer je mogoče (2FA, MFA);
- redno posodobljen sistem (vse aplikacije na vseh napravah);
- požarni zid;
- uporaba protivirusnih in protismetnih programov (blokada telemetrije?);
- varnostno arhiviranje;
- uporaba šifriranje kjer je mogoče;
- nameščanje samo tistih aplikacij, ki jih res potrebujemo;
- fizična varnost.

# Osnovna zaštita



# Gesla...



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

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

# Gesla

---

Pravilo:

- čim daljše
- čim bolj kompleksno (mešanica črk in števil, po možnosti tudi mešanica velikih in malih črk ter števil)

Kako pomembno je posamezno geslo (za kaj ga uporabljamo)?

Gesla morajo biti med seboj (dovolj) različna.



# Metode oblikovanja gesel

---

Pri **prvi metodi** geslo sestavimo iz stavka, oziroma je geslo enako stavku. Npr. "To je moje geslo". Na ta način ni težko ustvariti dovolj dolgega gesla. Izmislimo si lahko tudi neko (nesmiselno) zaporedje besed, npr. "gore Morje hrib Dolina". Smiselna je tudi uporaba številčk in drugih znakov.

Pri **drugi metodi** določene črke v besedah gesla zamenjamo s številčkami. Npr, "O" zamenjamo z nič, "L" z ena, "E" z tri, itd. Primer: "t0j3m0j3g3s10".

Pri **tretji metodi** pa geslo sestavimo iz prve (ali druge, ali zadnje,...) črke daljšega besedila. Tako iz "an ban pet podgan" nastane "abpp". Seveda so možne še druge kombinacije (npr. kombinacija besed in števil), pomembno je le, da je geslo dovolj dolgo in dovolj kompleksno, da ga ni mogoče uganiti.

# Gesla

---

Geslo mora biti čim bolj odporno na napad z metodo grobe sile ter na ugibanje.

Če gre za geslo za dostop do nekega sistema, ki ima **časovno omejitev** za ponovne poskuse vnosa gesla, ali če je **število poizkusov** vnosa gesla omejeno, je geslo lahko krajše.

Geslo mora imeti dovolj visoko stopnjo entropije (npr. vsaj 64 bitov entropije – mera za nedoločenost sistema sporočil).

**ASCII abeceda** ima približno okrog 5 bitov entropije. Zato za dosego 64 bitov entropije potrebujemo vsaj 13 znakov dolgo geslo ( $64/5 = 12,8$ ).

**Angleško besedilo** ima po nekaterih ocenah v povprečju približno 1,2 do 2 bita entropije na znak: geslo v angleškem jeziku mora biti dolgo med 32 in 54 znakov.

Povprečna entropija **slovenskih leposlovnih besedil** je 2,2 bita na znak: geslo v slovenskem jeziku mora biti dolgo vsaj 30 znakov.

# Gesla

---

Enkratna gesla

“Biometrična gesla”: biometričnih parametrov ni mogoče zamenjati oziroma preklicati, ponarejanje prstnih odtisov,...

Identiteta (“Kdo si?”) in avtentikacija (“Kako lahko to dokažeš?”) uporabnika morata ostaneta ločeni, kar pa pri uporabi biometričnih gesel ne velja.

Geslo, za katerega sumimo, da je bilo zlorabljeno je potrebno **takoj spremeniti**.

# 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?

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

# Varnostne kopije

---

## *The* **TAO** *Of* **BACKUP**

*A novice wanted to learn the Tao of Backup.  
The master said: "To become enlightened, you  
must master the seven heads of Backup. He who  
knows the heads will keep all his data forever.  
He who knows them not will lose all his data,"  
and with that, the lessons began...*



- uporaba (šifriranih?) oblačnih storitev (+/- dosegljivost,...);
- uporaba lokalnega NAS strežnika;
- arhiviranje samo pomembnih datotek;
- arhiviranje celotnega sistema (+ načrt okrevanja po katastrofi?);
- inkrementalne varnostne kopije.

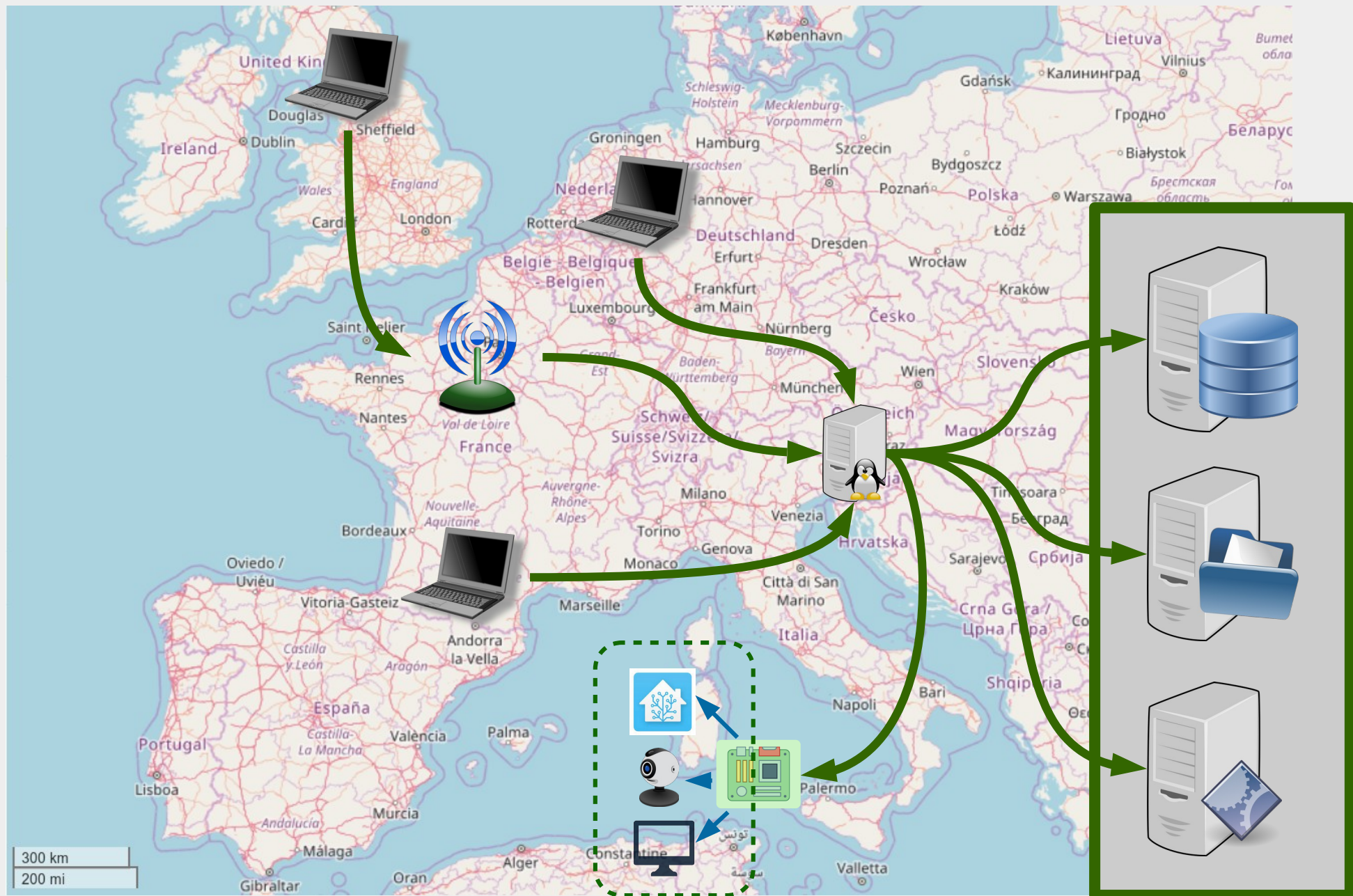
# Naprednejša zaščita

---

Nekatere tehnike naprednejše zaščite:

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

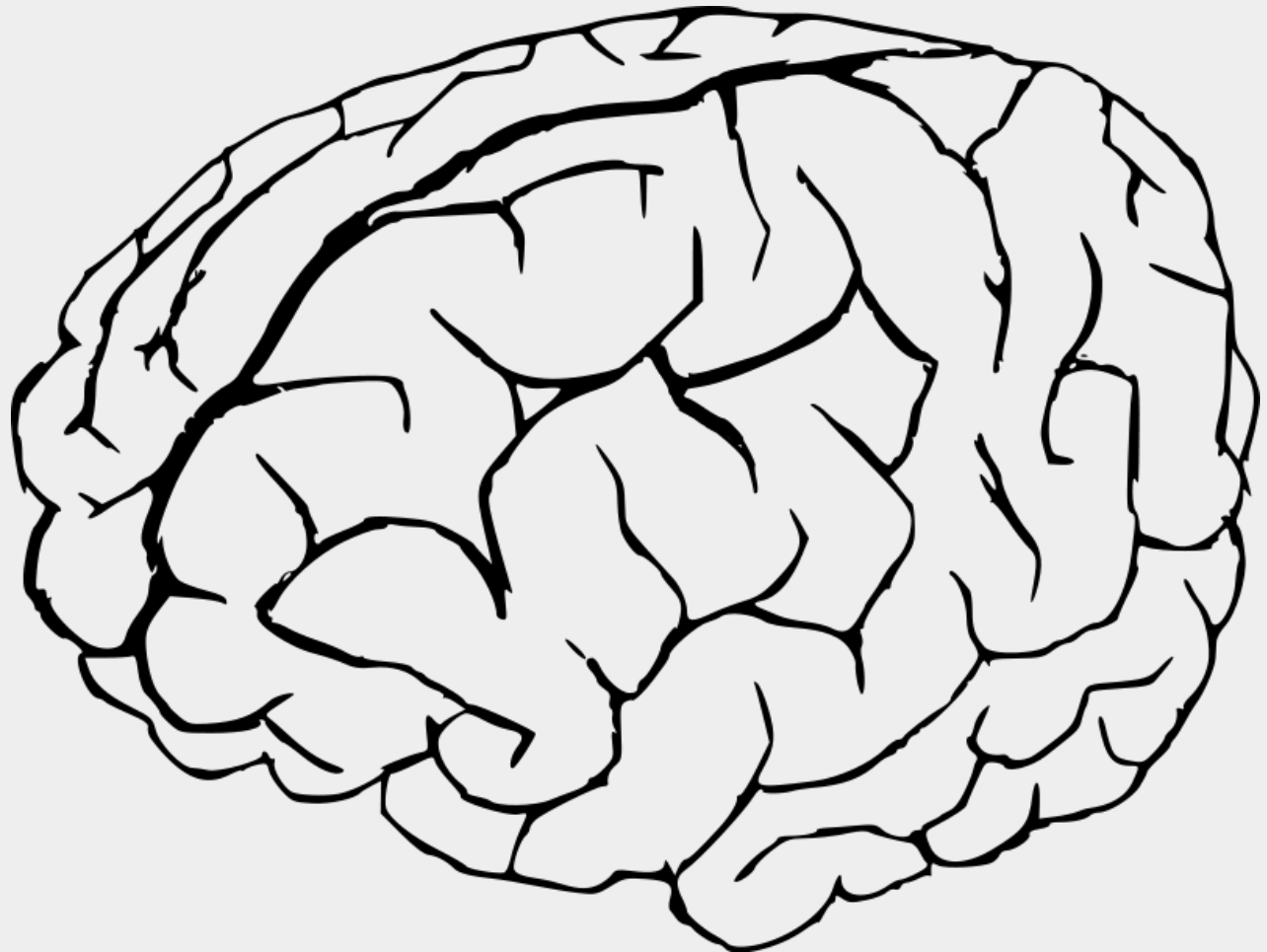
# VPN (Virtual Private Network)



# Še bolj napredna zaščita

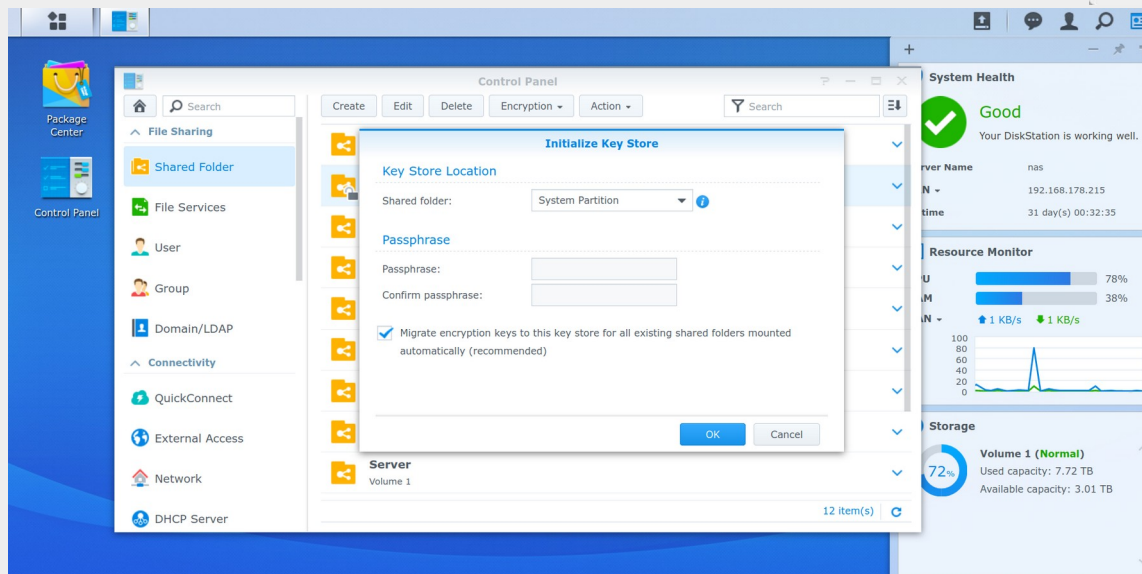
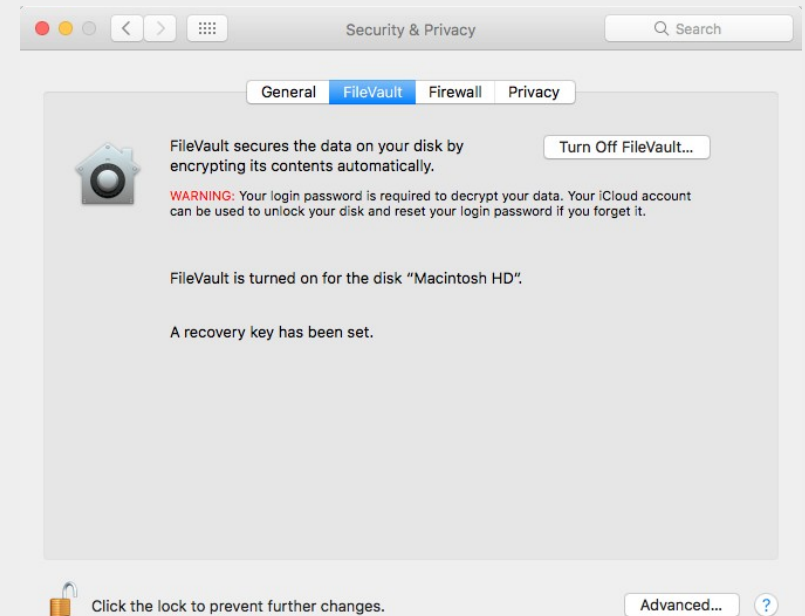
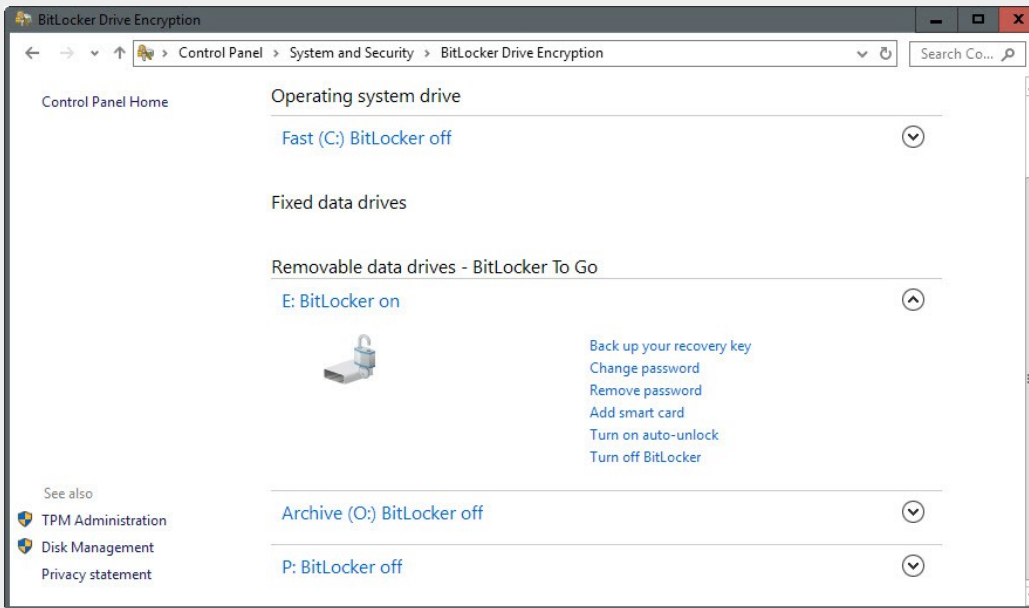
---

Nekaj znanja, doslednosti in zdrava pamet. ;-)





# Šifriranje nosilcev podatkov



# Dodatne aplikacije

---

Dodatki za brskalnik:

- HTTPS Everywhere,
- odstranjevalci spletnih tehnologij za sledenje (angl. *online trackers*): Ghostery, Privacy Badger, Adblock Plus, uBlock Origin,...),
- NoScript.

Odstranjevalci »nesnage« (BleachBit, CCleaner,...).

Blokada Windows telemetrije (Blackbird, WPD,... PiHole?).

Upravljevec gesel (angl. *password manager*): Keepass, Lastpass, Bitwarden, Lesspass...).

*Priporočljivo je, da so varnostni dodatki odprtokodni.*

# Zakaj šifriranje?

The image displays a network analysis session with three main windows:

- Follow TCP Stream:** Shows an HTTP 1.1 request to `/search.jsp?q=Matej` from `www.najdi.si`. The request includes headers such as `User-Agent: Mozilla/5.0 (X11; U; Linux i686; s; rv:1.8.1.16) Gecko/20080715 Ubuntu/7.10 (gutsy) Firefox/2.0.0.16` and `Accept-Language: sl,en-gb;q=0.7,en;q=0.3`. The response is a `200 OK` from Apache, with headers like `Content-Type: text/html; charset=UTF-8` and `Keep-Alive: timeout=5, max=100`.
- Wireshark:** Shows a list of captured packets. A filter is applied to `sip`. The packet list shows SIP messages including `PUBLISH sip:015805373@212.1`, `INVITE sip:015805373@212.1`, and `ACK sip:015805373@212.1`. The packet details pane shows the SIP message structure, with the `From` field highlighted in red.
- VoIP Calls:** A window showing detected VoIP calls. It lists two calls, both completed. The first call is from `172.16.0.116:5062` to `172.16.0.116` with a duration of 64.04 seconds. The second call is from `172.16.0.116:5062` to `172.16.0.116:5062` with a duration of 64.57 seconds. A waveform and jitter buffer graph are visible for the first call.

# Šifriranje »priporočča« tudi NSA!

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

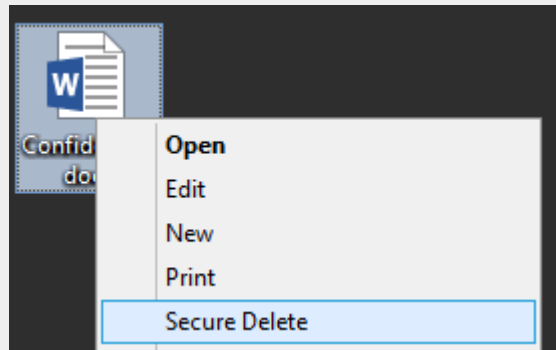
## Capabilities Development Risk Matrix (II)

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

# Trajno brisanje podatkov



```
Darik's Boot and Nuke 2.3.0

----- Options -----
Entropy: Linux Kernel (urandom)
PRNG:    Merseme Twister (mt19937ar-cok)
Method:  DoD Short
Verify:  Last Pass
Rounds:  1

----- Statistics -----
Runtime:
Remaining:
Load Averages:
Throughput:
Errors:

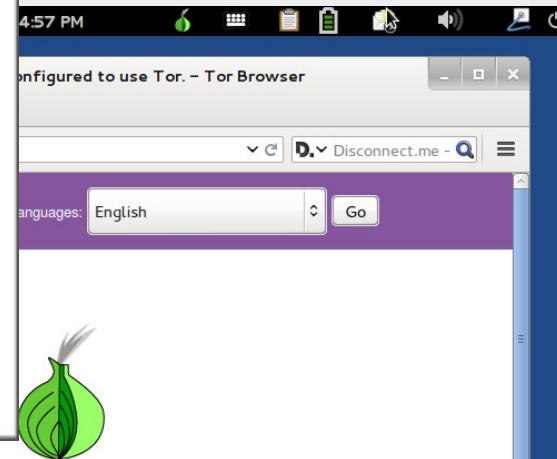
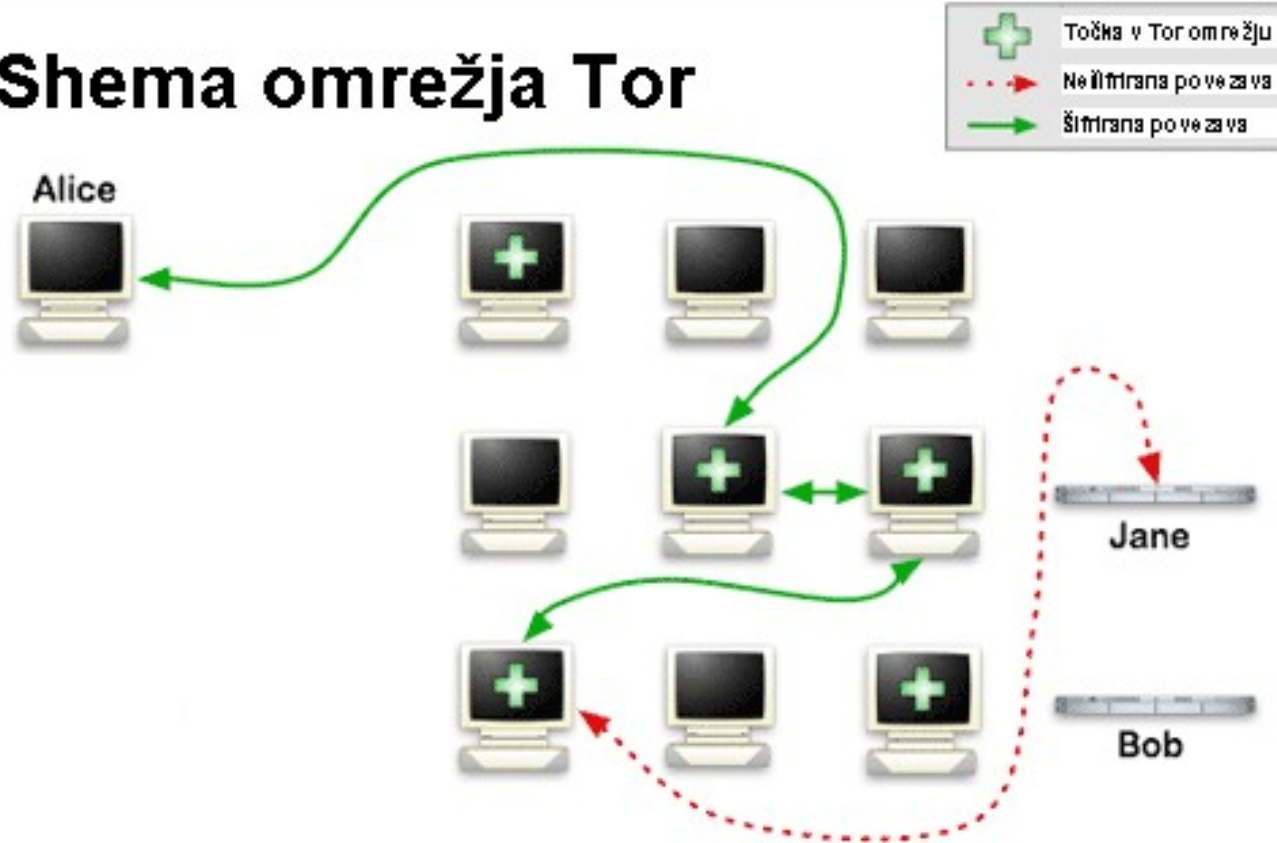
----- Disks and Partitions -----

▶ [wipe] ATA Disk Windows 8.1a-0 S SW7R 64GiB (68GB) 4SYNEQ6YU0P4F1NPKXHT

P=PRNG M=Method U=Verify R=Rounds, J=Up K=Down Space=Select, F10=Start
```

# Anonimizacija

## Shema omrežja Tor



Tails documentation



Report an error

**Congratulations. This browser is configured to use Tor.**

Your IP address appears to be: **209.126.110.113**

Please refer to the [Tor website](#) for further information about using Tor safely. You are now free to browse the Internet anonymously. For more information about this exit relay, see: [Atlas](#).

# Varnost e-pošte

---

Poštni strežnik:

- varnostni protokoli za preverjanje pristnosti e-pošte (SPF - Sender Policy Framework, DKIM - DomainKeys Identified Mail in DMARC - Domain-based Message Authentication, Reporting & Conformance),
- strežniški diski so šifrirani,
- protivirusni in protismetni filtri,
- podpora šifriranim protokolom (POP3s/IMAPs/SMTPs).

Poštni odjemalci:

- šifriranje e-pošte (GPG),
- dvofaktorska avtentikacija (Yubikey,...).

# Razpoložljivost

---

Razpoložljivost zagotavlja zanesljiv in pravočasen dostop do informacijskega sistema, ko ga uporabniki potrebujejo.

Zanesljiv in razpoložljiv informacijski sistem v organizaciji predstavlja temelj za nemoteno izvajanje delovnih in poslovnih procesov in ima zato ključno vlogo pri učinkovitosti poslovanja.

Delo na daljavo:

- infrastruktura v organizaciji (oddaljeni dostopi, videokonferenčni sistemi),
- infrastruktura pri zaposlenih (strojna in programska oprema (slušalke,...)),
- oddaljeno vzdrževanje,
- varnost terminalne opreme,
- trening.



# Delo na daljavo

---

Digitalizacija poslovanja in delo na daljavo niso možni v vseh gospodarskih panogah v enaki meri.

Kjer pa je to mogoče, pa je priprava na to smiselna.

Spremembe je treba uvajati premišljeno in sistematično.

1. Priprava ustrezne infrastrukture na strani organizacije.

2. Zagotovitev podpore delu na daljavo pri zaposlenih.

3. Izobraževanje zaposlenih.

4. Občasno izvajanje dela na domu/na daljavo (trening).

**Poseben poudarek na zagotavljanju varnosti.**

S tem bo organizacija bolje pripravljena na potencialno krizo, kar pa je bistvenega pomena za preživetje v primeru izrednih dogodkov.

# Varnost mobilnih komunikacij



# Varnost mobilnih komunikacij

The screenshot displays a network analysis tool interface. At the top, a search bar contains the text "e212.imsi". Below it, a table lists captured packets:

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

The selected packet (No. 34) is expanded to show the following details:

- ▶ 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

The P1 Rest Octets section shows a hex dump:

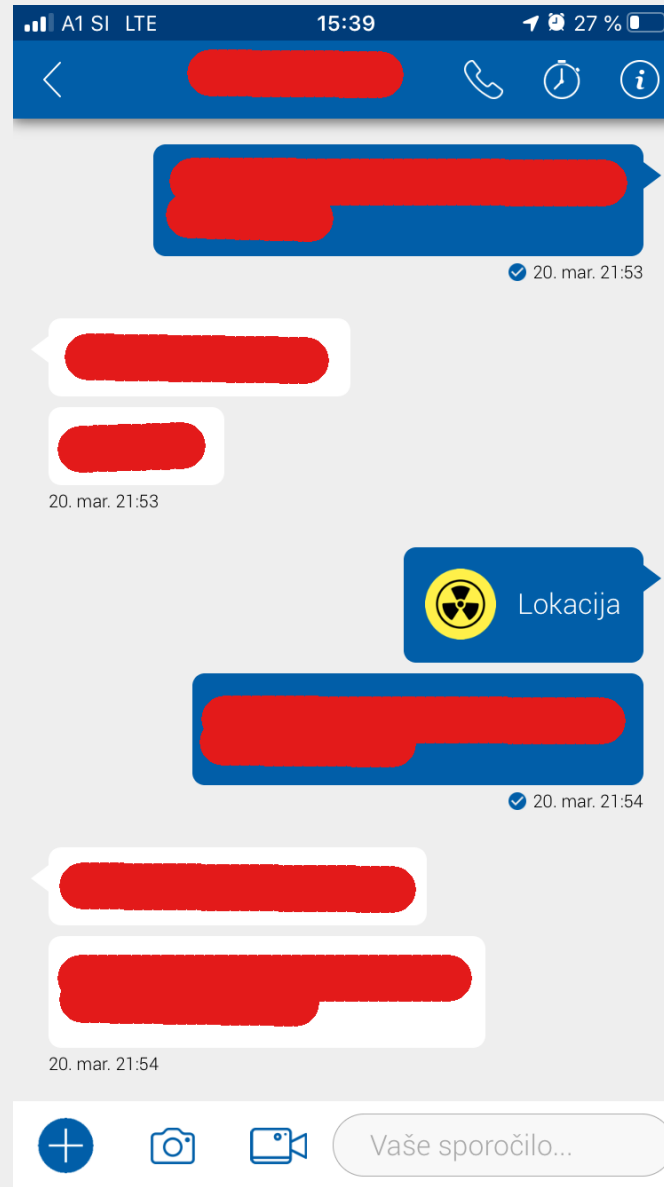
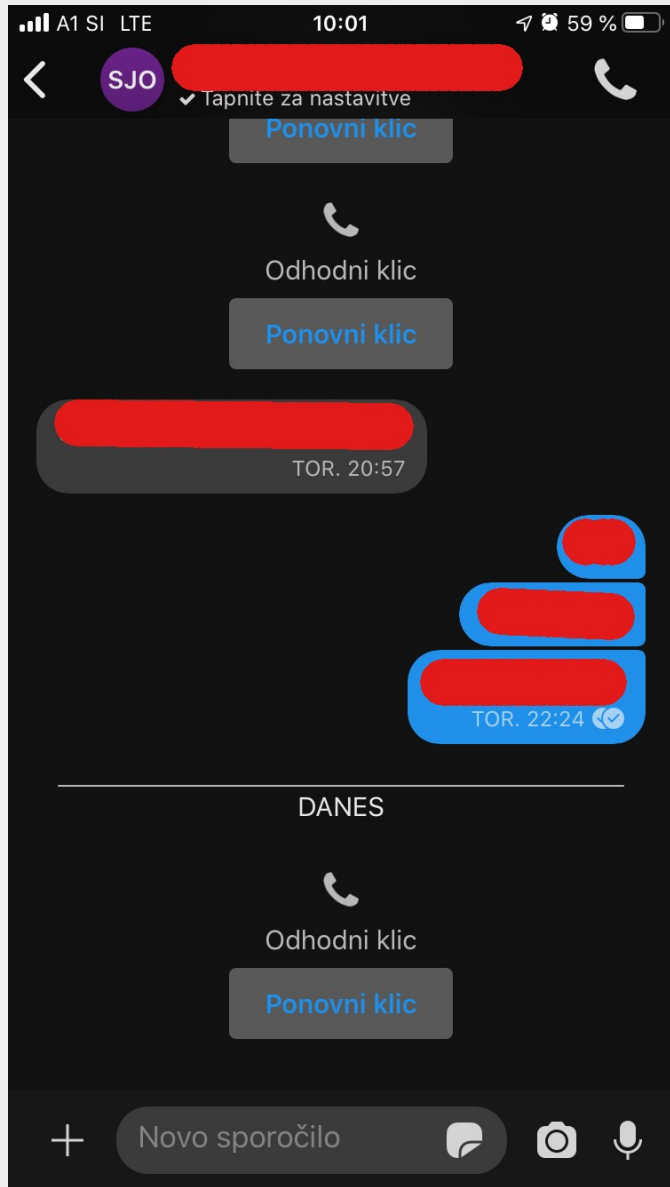
```
0010 00 43 70 31 40 00 40 11 cc 76 7f 00 00 01 7f 00 .Cp1@.@. .v.....
0020 ██████████ ██████████
0030 ██████████ ██████████
0040 ██████████ 2b 2b ██████████ +++++
0050 2b
```

# Varnost mobilnih komunikacij



Naprava podjetja NSO namenjena vdorom v mobilne telefone.

# Varnost mobilnih komunikacij



# Vidiki informacijske varnosti

---

Gradniki zagotavljanja informacijske varnosti:

- Tehnologija (pogosto se nanjo daje preveč poudarka, prepričanje, da samo s tehnologijo lahko zagotovimo varnost je napačno).
- Ljudje (pomemben del varnosti smo ljudje).
- Procesi, ki podpirajo tehnologijo in ljudi.
- Družbeni vidiki (širše družbene posledice uporabe informacijskih sistemov).

# Ljudje

---

Ljudje smo pomemben element pri zagotavljanju varnosti.

Ljudje smo nagnjeni h delanju napak.

Ljudje pogosto skušamo zaobiti varnostne protokole, ker nam to olajša življenje.





# Vprašanja?

<https://telefoncek.si>

This work is published under  
CC BY-NC-SA 4.0 License