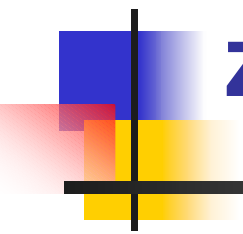


Zasebnost in nadzor na internetu, 4. del

Matej Kovačič,
http://www.ljudmila.org/matej

Uporaba PGP-ja

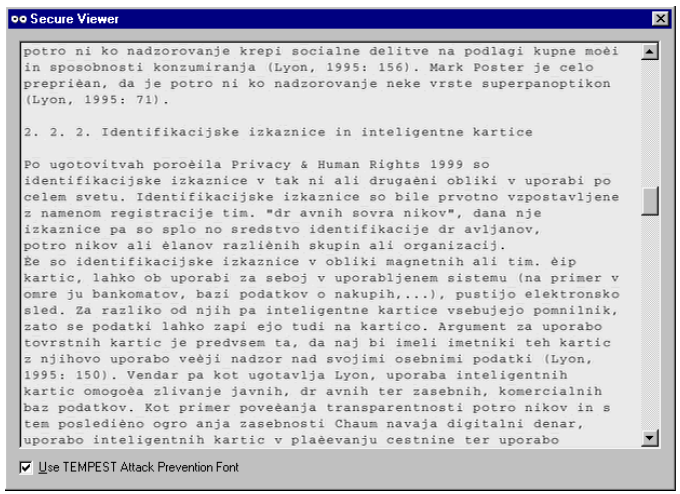
- **Enkripcija, dekripcija in digitalno podpisovanje elektronske pošte in datotek s programom PGP.**
- **Zagotovitev pristnosti javnih ključev (preverjanje prstnega odtisa in podpis ključa ter šele nato nastavitev stopnje zaupanja).**
- **Pomen varnostne kulture (izbira ustreznega gesla, redna uporaba).**
- **Hushmail.**

Lastnosti javnega ključa in njegov prstni odtis.

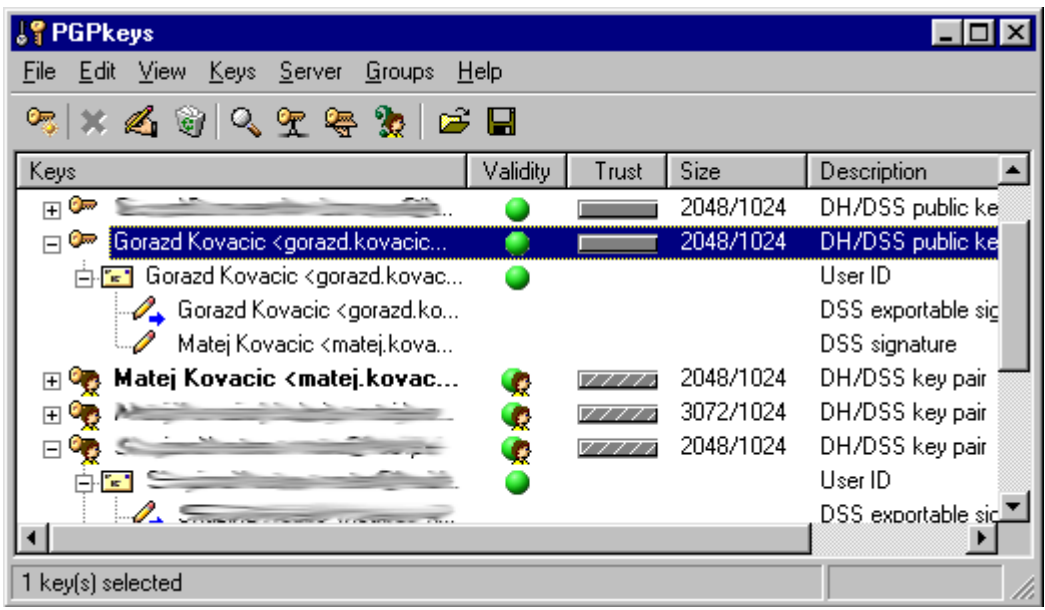
Uporaba PGP-ja

- **Visoka stopnja varnosti: preprečevanje napada "*tempest atack*".**
- **PGP disk.**

PGP tools.

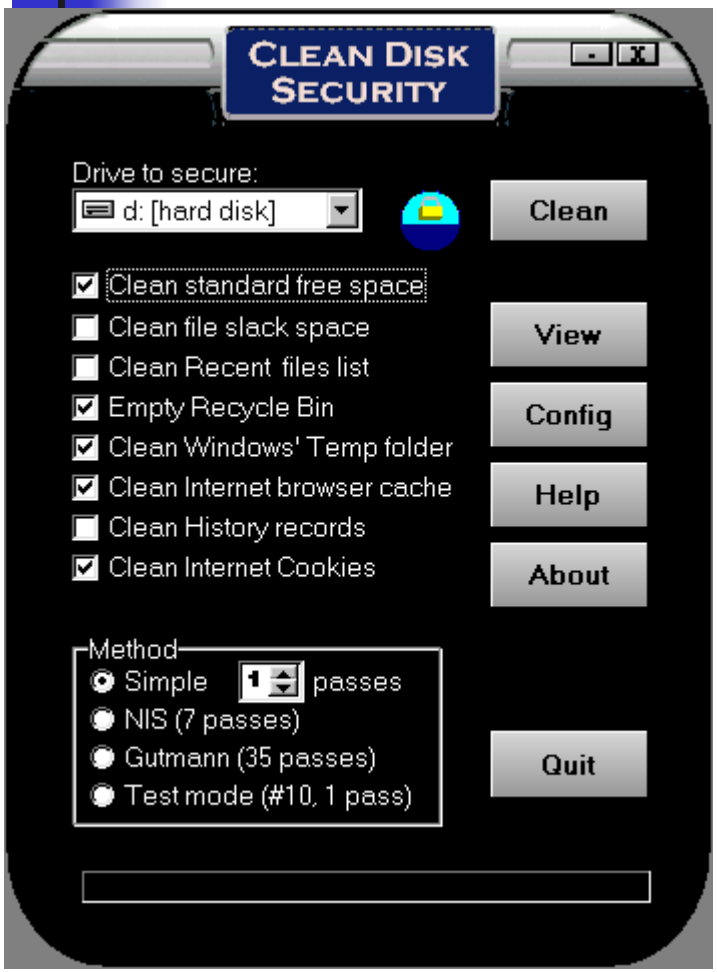


Secure viewer.



Podpisovanje javnih ključev pred nastavitvijo stopnje zaupanja.

Clean Disk Security

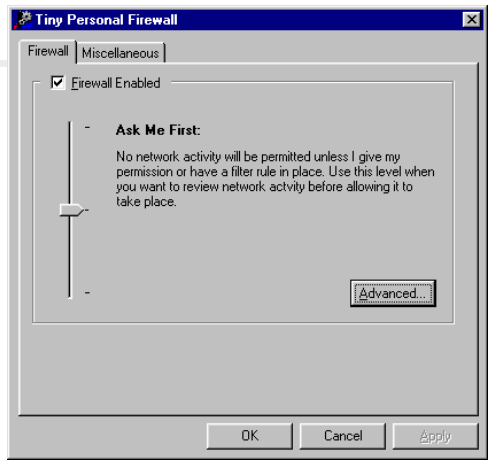


Clean Disk Security.

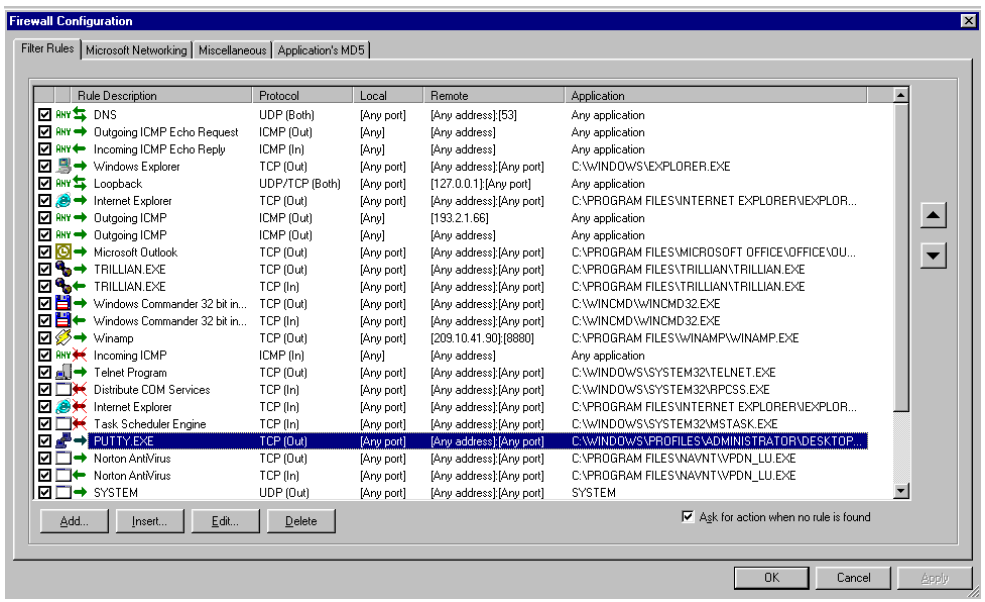
- **Brisanje sledov uporabe računalnika: *history files*, *cookies*, *swap file*.**
- **Nepovratno brisanje vsebine datotek (*wipe, number of passes*).**
- **Priporočeno število prehodov pri brisanju:**
- **priporočila PGP:**
  - **3x za osebno rabo;**
  - **10x za komercialno uporabo;**
  - **18x za vojaško uporabo;**
  - **26x za največjo varnost;**
- **priporočila Clean Disk Security (posebne metode)**
  - **metoda NIS (*US Department of Defense*): 7x;**
  - **Guttmanova metoda: 35x.**

Personal Tiny Firewall

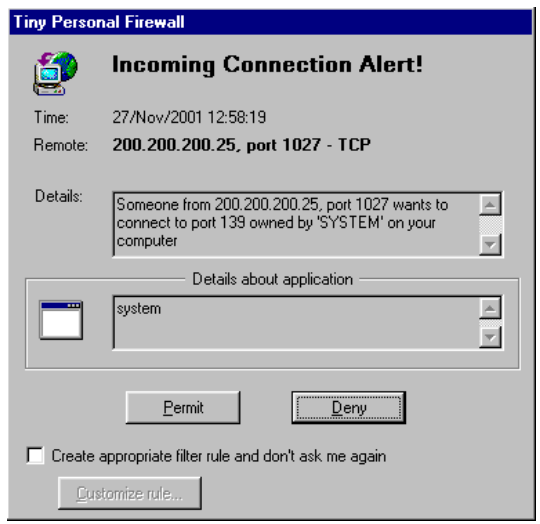
- **Preprečuje neželeno vhodno in izhodno komunikacijo.**
- **Omejitev dostopa glede na program (MD5 podpis), IP naslov in vrata (*port*).**



Nastavitev stopnje zaščite.



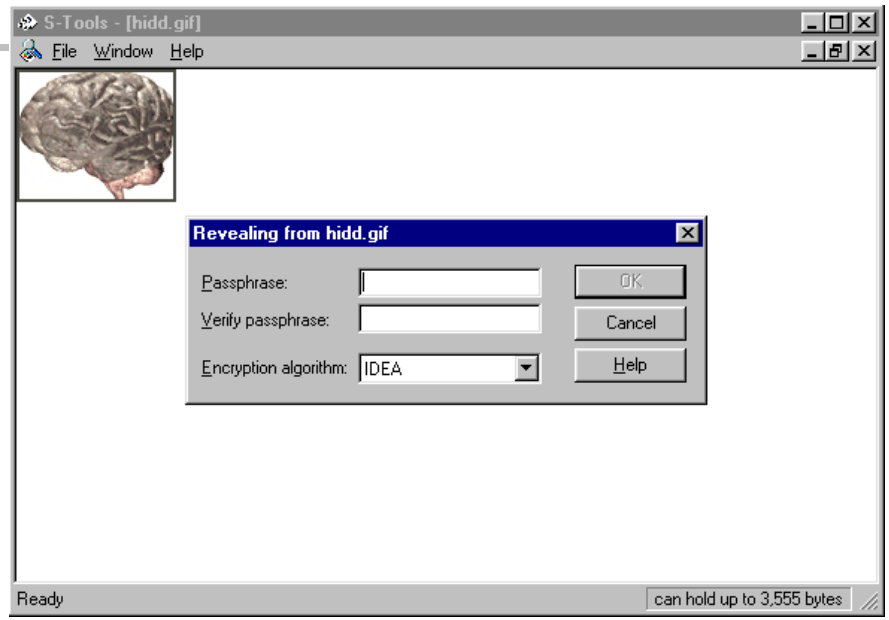
Pregled pravil.



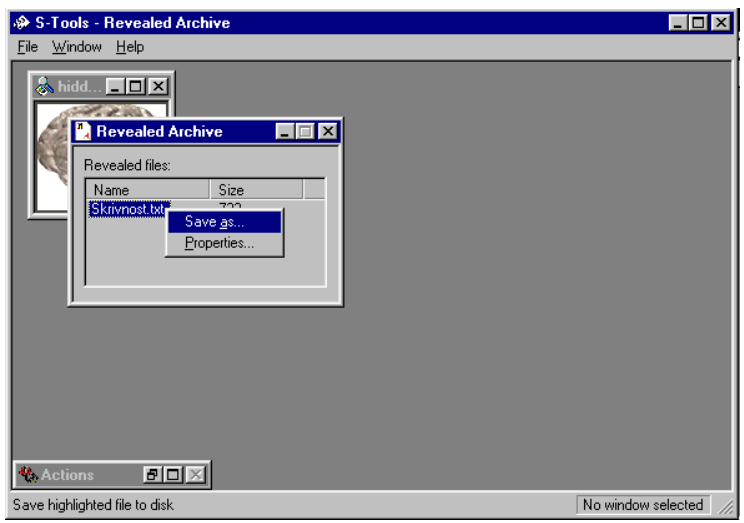
Požarni zid je zaznal poiskus vdora.

S-Tools

- **Steganografija - skrivanje sporočil, nevidno kodiranje, označevanje datotek z digitalnim vodnim tiskom ter digitalnimi serijskimi številkami.**



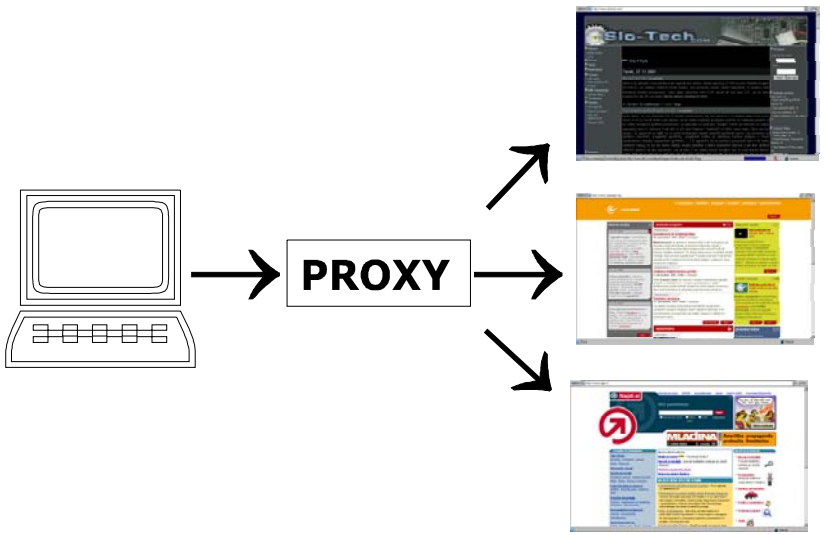
V datoteki HIDD.GIF se nahaja skrito sporočilo.



Shranjevanje skrite datoteke na disk.

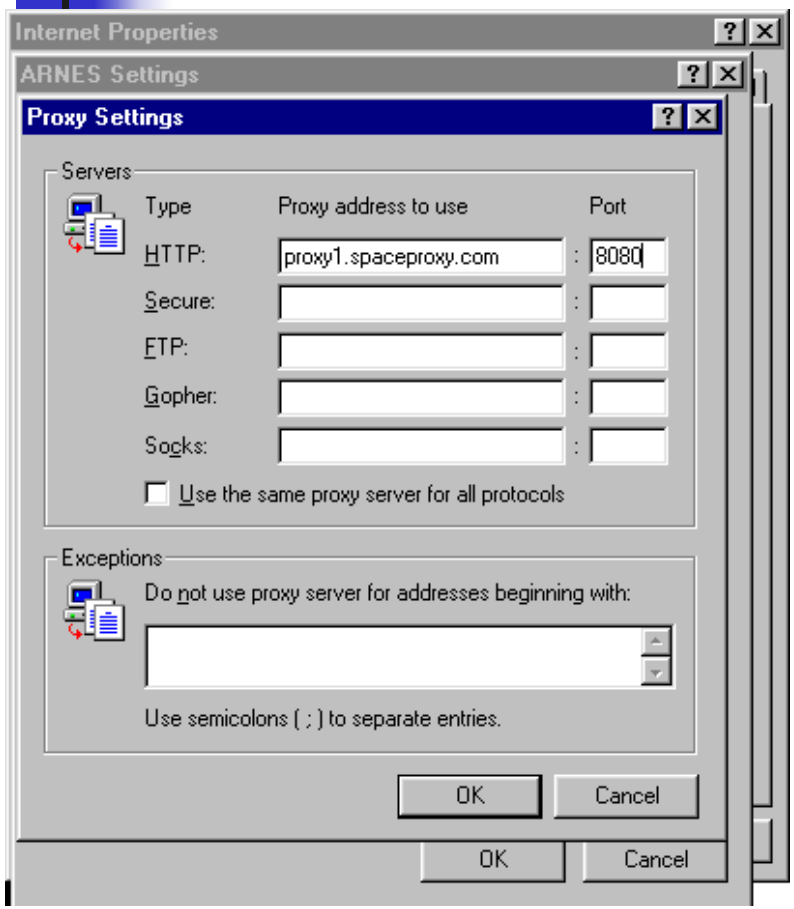
- Možnosti: sporočilo najprej zakriptiramo, nato pa skrijemo v zvočno ali slikovno datoteko.

Anonimni proxy



- Proxy ali zastopniški program je točka preko katere komuniciramo z internetom. Proxy v uporabnikovem imenu pošilja zahtevke za dostop do spletnih strani, podatke pa nato posreduje uporabniku.
- Proxy lahko posreduje tudi podatke in medpomnilnika (*cache*-ja).
- Proxy se v internetu predstavlja s svojim IP naslovom. Anonimni proxy tako skrije identiteto pravega uporabnika interneta.

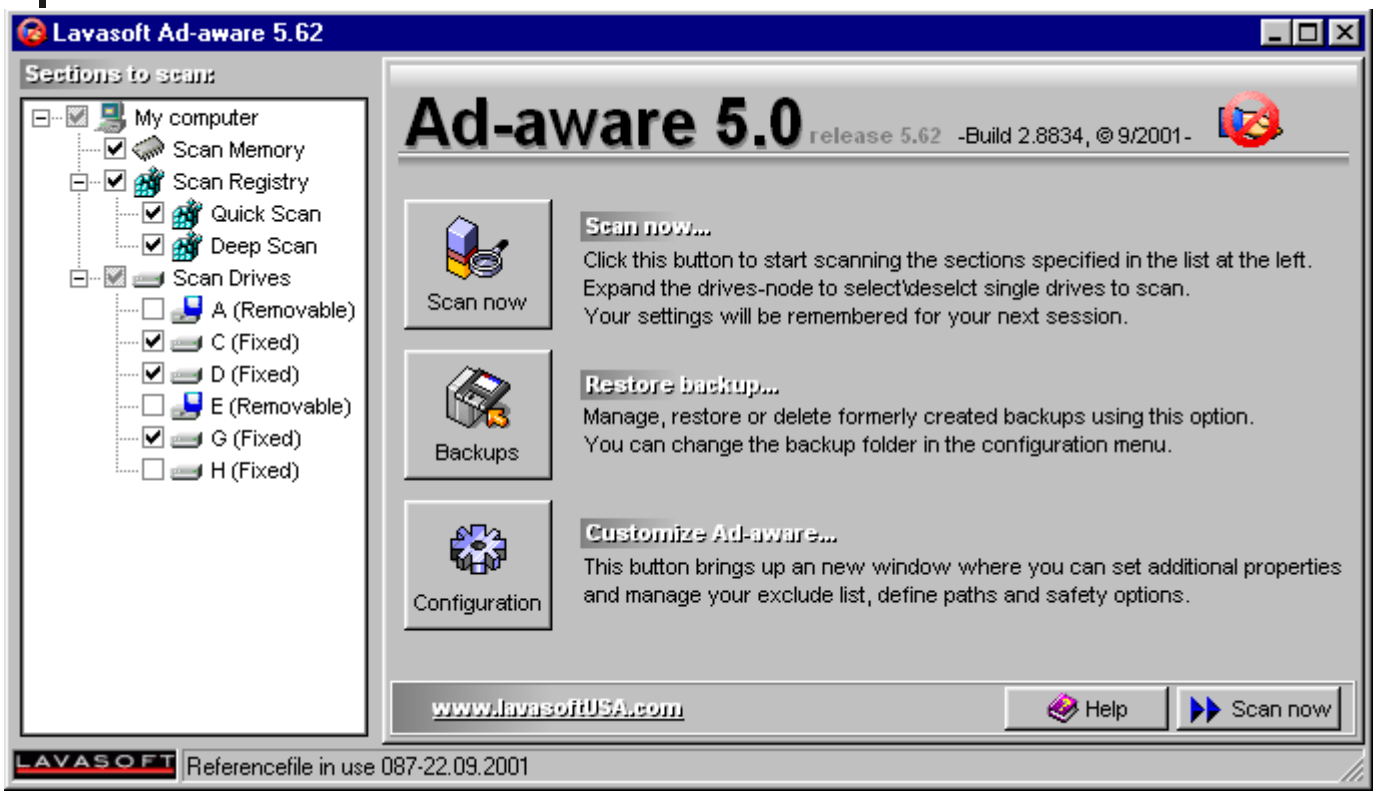
Anonimni proxy



- **Ločimo navadne anonimne proxy-e (*standalone anonymous proxy*) in spletne anonimne proxy-e (*web-based anonymous proxy*).**
- **Anonimni proxy skrije identiteto uporabnika *samo* obiskanemu spletnemu strežniku. Ponudnik dostopa do interneta pa še vedno lahko spremlja promet uporabnika.**
- **Če uporabnik do proxya uporablja kriptirano povezavo (npr. SSL), pa še vedno obstaja možnost analize prometa (kateri proxy je uporabljen in količina prenešenih podatkov).**

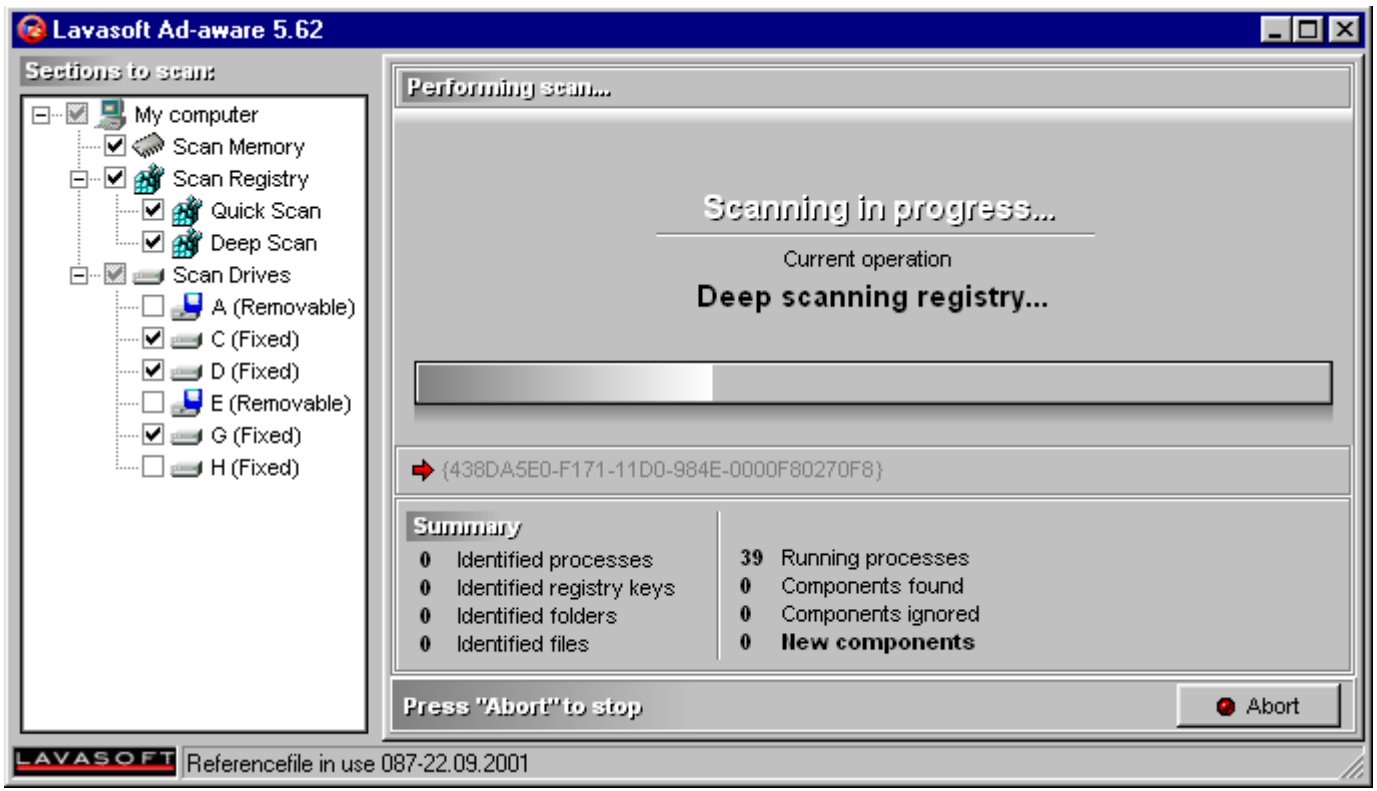
Nastavitve za uporabo proxy-a. Proxy je potrebno nastaviti za vsakega izmed klicnih ali omrežnih dostopov posebej.

Odstranjevanje vohunskih programov



Program Ad-aware za odstranjevanje vohunskih programov (spyware-a).

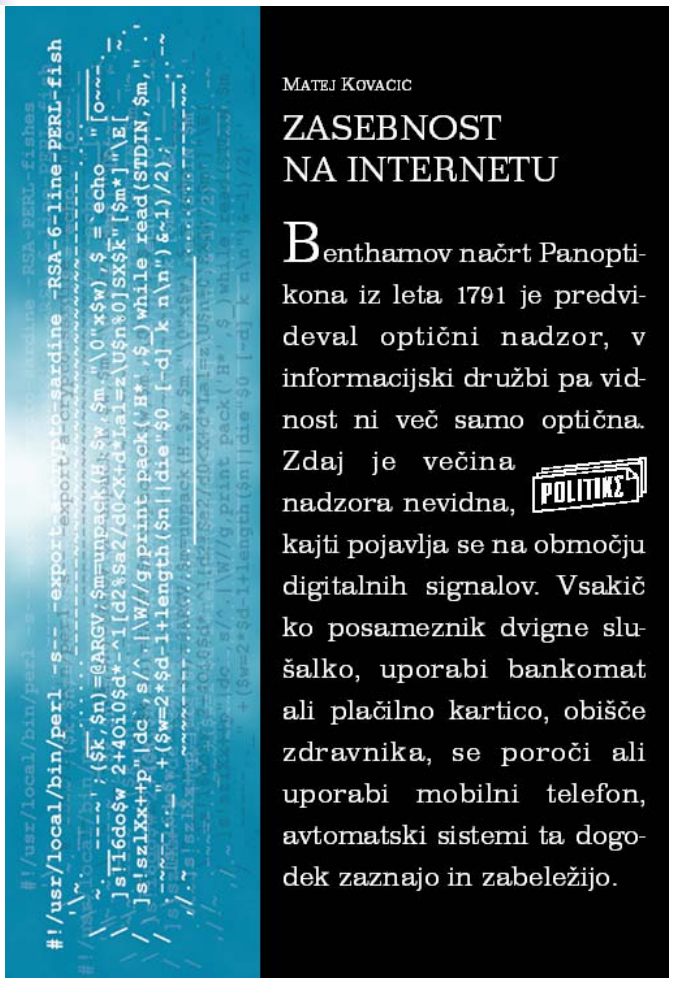
Odstranjevanje vohunskih programov



Ad-Aware preiskuje računalnik...

Knjiga: Zasebnost na internetu

http://www.ljudmila.org/matej/knjiga

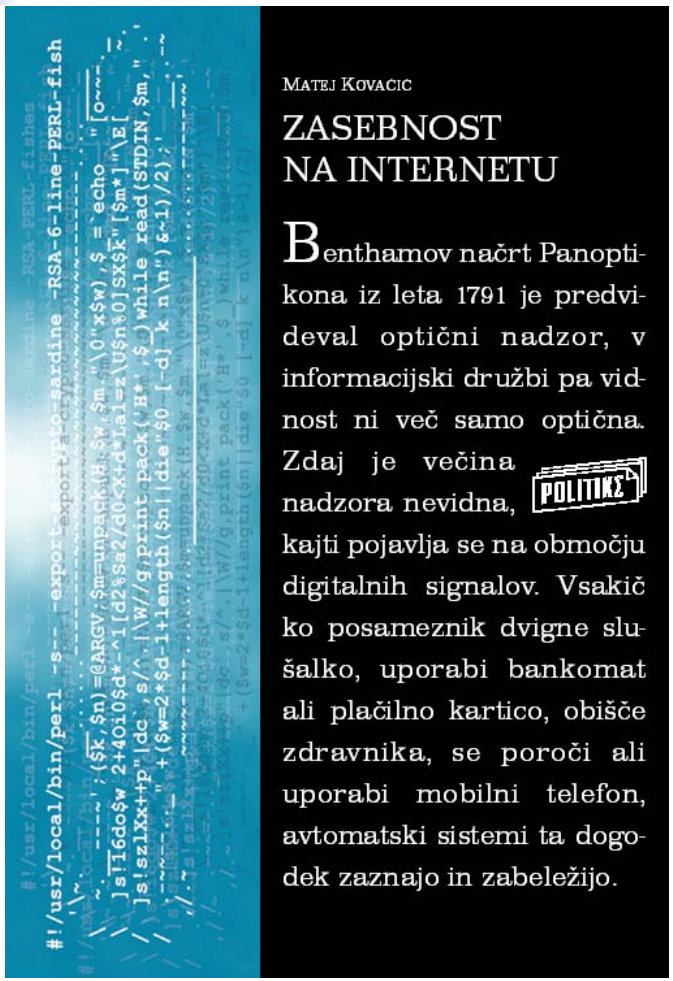


O knjigi

Knjiga govori o problemu zasebnosti v sodobni informacijski in potrošniški družbi, predvsem pa o problemu zasebnosti na internetu. Problem zasebnosti in nadzora v virtualnem prostoru obravnava tako v sociološkem, pravnem, kot tudi tehničnem smislu. Knjiga pa ima tudi praktični vidik, saj so v njej opisani tako konkretni primeri možnih zlorab zasebnosti na internetu, kot tudi nekatere zaščitne tehnike. Knjiga je izšla v slovenskem in angleškem jeziku Knjiga bo izšla pri Mirovnem inštitutu, naročiti pa jo bo mogoče pri Študentski založbi, Beethovnova 9, 1000 Ljubljana, telefon (01) 2510-332.

Knjiga: Zasebnost na internetu

http://www.ljudmila.org/matej/knjiga



Naslovnica

Naslovnica knjige (oblikovala jo je Irena Wölle) vsebuje *kripto sardino*. Gre za novo vrsto "živali" *sardina cryptographicus*, ki sta jo odkrila Alex Stewart in Rui Mendez. V resnici seveda ne gre za žival, pač pa za programsko implementacijo RSA šifrirnega algoritma v jeziku Perl, ki izgleda kot sardina (na naslovnici je postavljena pokončno). Če boste programsko kodo pretipkali in pognali, boste ugotovili, da program dejansko deluje!