

“The Disk Busters”

Forenzika pomnilniških sistemov

Infosek 2006

Koren Gašper, Kovačič Matej in Škrablin Jožko
Fakulteta za družbene vede

(CC) 2006

Delo je izdano pod Creative Commons licenco: "Priznanje avtorstva-Nekomercialno-Deljenje pod enakimi pogoji 2.5 Slovenija". Celotno pravno besedilo licence je dostopno na spletni strani: <<http://creativecommons.org/licenses/by-nc-sa/2.5/si/legalcode>>, ali na poštnem naslovu: Inštitut za intelektualno lastnino, Streliška 1, 1000 Ljubljana.

Možnosti zasega podatkov

- Prodane ali zavržene računalniške komponente, ki vsebujejo trajne pomnilnike (trdi diski, tiskalniki, mobilni telefoni,...).
- (Ne)pooblaščen fizični dostop do strojne opreme:
 - priklop trdega diska na drug računalnik;
 - uporaba "živega CD-ja" (ang. *live CD*), ki omogoča zagon operacijskega sistema Linux iz CD enote:
 - razbijanje Windows gesel;
 - dostop do vsebine diska;
 - izdelava kopije diska: `"dd if=/dev/hda1 of=kopija_diska.img"`

Možnosti zasega podatkov

PPA 1.50 - Brute Force attack - 2.54% (7)

Attack type: Brute-force Mask Dictionary

Hashes: Brute-force attack Recovery

Statistics

Current password: UGYEERA
NT passwords found: 25/103
Passwords checked: 203.899.016
Passwords total: 8.031.810.176 (7)

User name	User...	Computer	Hash type
<input type="checkbox"/> Stephen Hill...	0093		LM+NTLM
<input checked="" type="checkbox"/> Stephen Lars...	0094		LM+NTLM
<input type="checkbox"/> Stephen Wils...	0095		LM+NTLM
<input type="checkbox"/> Susan Ilston	0096		LM+NTLM
<input checked="" type="checkbox"/> Suzanne Segal	0097		LM+NTLM
<input checked="" type="checkbox"/> Terry Hatter	0098		LM+NTLM
<input checked="" type="checkbox"/> Thelton Hen...	0099		LM+NTLM
<input type="checkbox"/> Thomas Whe...	0100		LM+NTLM

Timestamp Message

03.06.2005 18:01:04	Found first half of LM password for us
03.06.2005 18:01:04	Found NT password for user "Charles
03.06.2005 18:01:14	Found first half of LM password for us
03.06.2005 18:01:14	Found NT password for user "William

Proactive Password Auditor 1.50, Copyright (c) 2003-2005 ElcomS

CIA Commander for Windows NT/2000/XP v1.0

Accounts

- 01F4: Administrator
- 01F5: Guest
- 03E8: HelpAssistant
- 03EA: SUPPORT_388945a0
- 03EB: [redacted]

CIA User Manager

5.1 b.2600
SYSKEY is In-Registry

ERD Commander 2003 Locksmith Wizard

Select New Password

Locksmith needs to know the name of the account to be modified, and the new password you desire.

Please select the account for which you would like the password to be changed, and type in the new password.

Account: Administrator

New Password: Administrator
Guest
HelpAssistant
Kilian
SUPPORT_388945a0

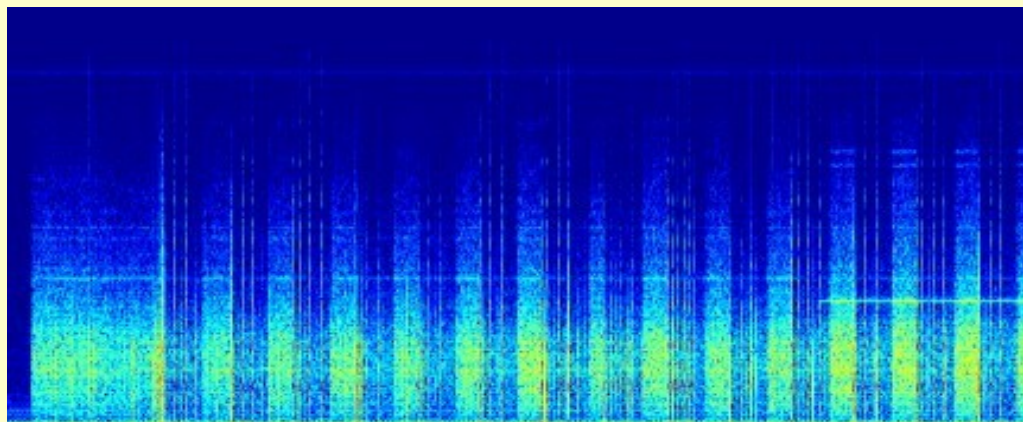
Confirm Password: [redacted]

< Back Next > Cancel

“Obnavljanje” Windows gesel s pomočjo živih CD-jev.

Možnosti zasega podatkov

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



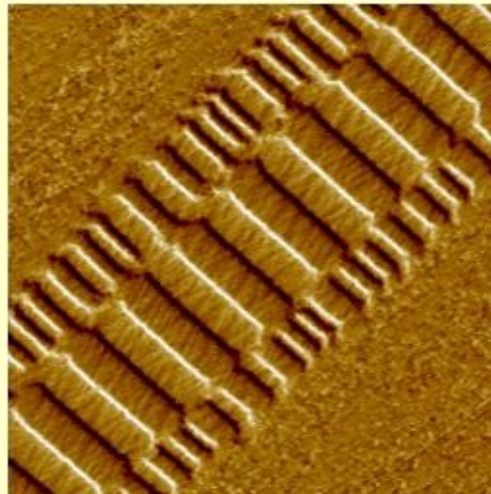
- Sonogram elektromagnetnih signalov ob pisanju na trdi disk. Avtor je na podlagi spremljanja elektromagnetnih signalov lahko rekonstruiral kdaj se zapisujejo enke in kdaj ničle. Vir: Oğuz Berke Durak, Hidden Data Transmission by Controlling Electromagnetic Emanations of Computers, <<http://abaababa.ouvaton.org/tempest/>>.

Problem brisanja podatkov

- Običajno brisanje datotek in celo formatiranje trdih diskov podatkov ne izbriše trajno.
- Podatki iz pomnilnika lahko ostanejo shranjeni tudi v začasnem pomnilniku (ang. *swap, cache*) na trdem disku.
 - Hibernacija računalnika.
- Raziskava podjetja Pointsec iz leta 2004 je pokazala da je mogoče podatke na razmeroma enostaven način rekonstruirati na do 70% rabljenih trdih diskov kupljenih preko interneta.

Rekonstrukcija izbrisanih podatkov

- Mikroskopiranje magnetnih sil - v nekaterih primerih je mogoče enkratno oziroma tudi večkratno prepisane podatke zaradi temperaturnega krčenja in širjenja diska rekonstruirati s pomočjo elektronskega mikroskopa.

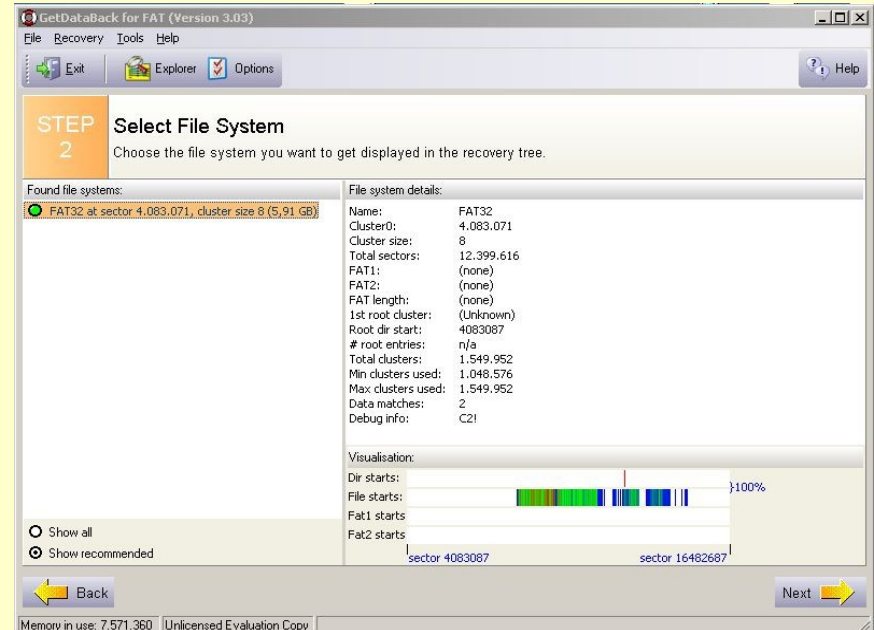
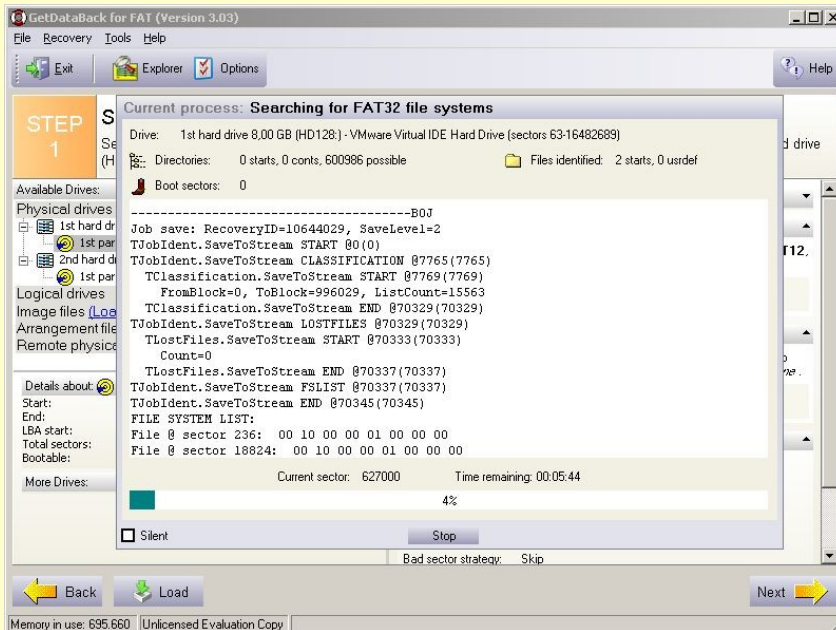


- Ostanki prepisanih informacij na magnetnih diskih na robovih zapisovalnih sledi. Vir in avtorstvo: Venema in Farmer, Forensic Discovery, 2004.

Rekonstrukcija izbrisanih podatkov

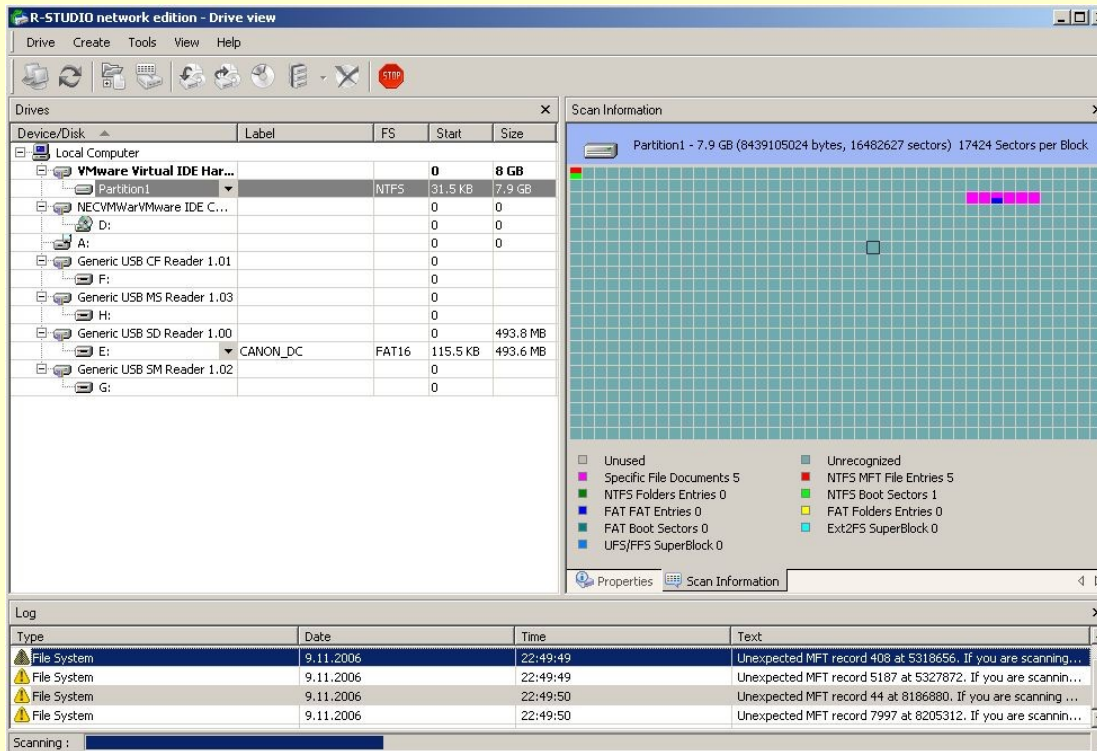
- V nekaterih primerih je mogoče izbrisane podatke rekonstruirati celo zgolj s pomočjo programskih orodij in to celo mesece ali leta po tem, ko so bili izbrisani.
- Orodja:
 - **GetDataBack**, preprosto orodje namenjeno obnavljanju izgubljenih datotek v okolju Windows.
 - **R-Studio**, orodje za obnavljanje izgubljenih podatkov v okolju Windows.
 - **TestDisk**, namenjen obnavljanju izgubljenih particij. <<http://www.cgsecurity.org/wiki/TestDisk>>.
 - **PhotoRec**, namenjen obnavljanju izgubljenih datotek. <<http://www.cgsecurity.org/wiki/PhotoRec>>.
 - **Autopsy Forensic Browser**, namenjen forenzični analizi pomnilniških sistemov. <<http://www.sleuthkit.org/autopsy/>>.

Rekonstrukcija izbrisanih podatkov



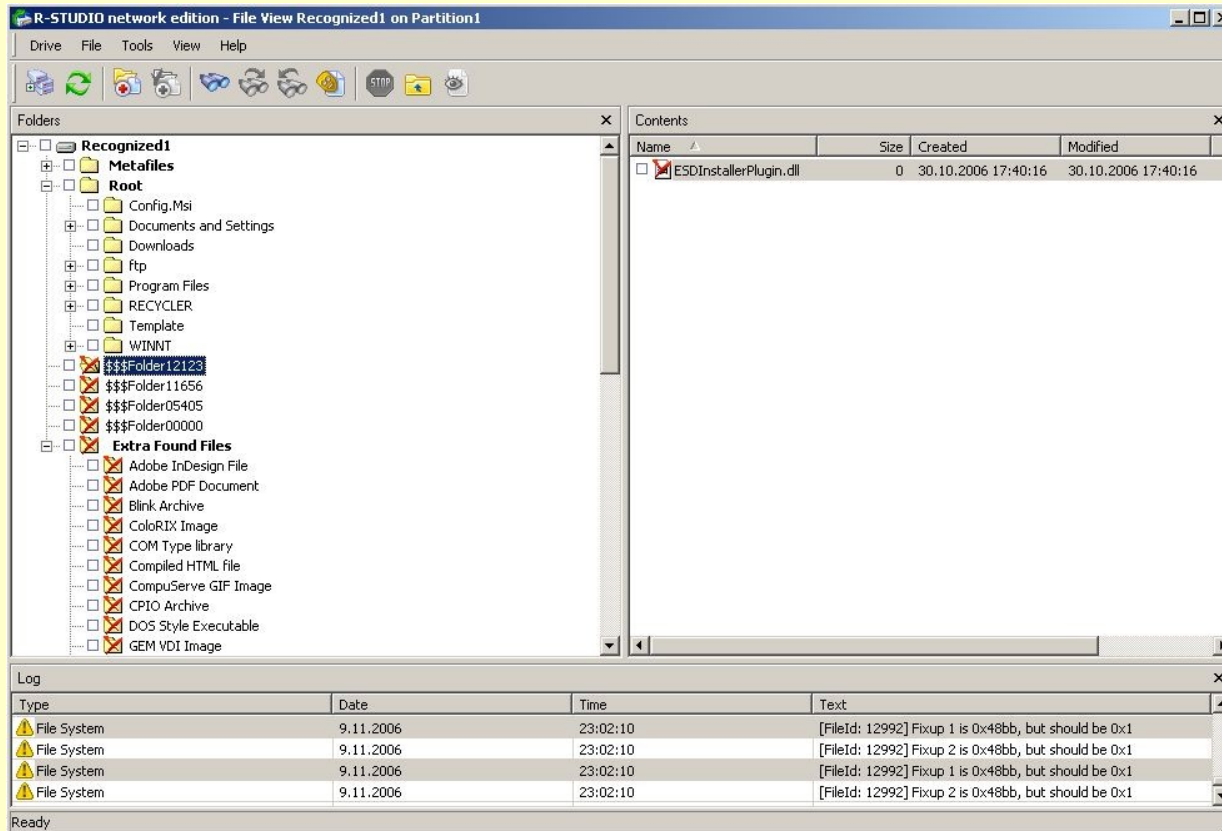
- **GetDataBack**, komercialno orodje za rekonstrukcijo izbrisanih podatkov v okolju Windows.

Rekonstrukcija izbrisanih podatkov



- **R-Studio**, komercialno orodje za rekonstrukcijo izbrisanih podatkov v okolju Windows.

Rekonstrukcija izbrisanih podatkov



- **R-Studio**, komercialno orodje za rekonstrukcijo izbrisanih podatkov v okolju Windows.

Rekonstrukcija izbrisanih podatkov



```
matej@KOVACIC-M: ~  
Datoteka Uredi Pogled Terminal Tabs Pomoč  
TestDisk 6.1, Data Recovery Utility, October 2005  
Christophe GRENIER <grenier@cgsecurity.org>  
http://www.cgsecurity.org  
  
Disk /dev/sdc - 992 MB - CHS 1024 32 62  
Analyse cylinder 276/1023: 26%  
  
Stop
```

- **TestDisk**, prosto orodje namenjeno obnavljanju izgubljenih particij, deluje v več operacijskih sistemih in pozna številne datotečne sisteme. <<http://www.cgsecurity.org/wiki/TestDisk>>.

Rekonstrukcija izbrisanih podatkov



```
matej@KOVACIC-M: ~  
Datoteka Uredi Pogled Terminal Tabs Pomoč  
PhotoRec 6.1, Data Recovery Utility, October 2005  
Christophe GRENIER <grenier@cgsecurity.org>  
http://www.cgsecurity.org  
  
Disk /dev/sdc - 992 MB - CHS 1024 32 62  
Partition      Start      End      Size in sectors  
1 * FAT16 >32M    0  0 33 1023 31 62    2031584 [NO NAME]  
  
Reading sector      260728/2031584, 389 pictures or videos found  
Elapsed time 0h00m07s - Estimated time for achievement 0h00m47  
  
Stop
```

- **PhotoRec**, prosto orodje namenjeno obnavljanju izgubljenih datotek; deluje tudi v primeru poškodbe datotečnega sistema; pozna več datotečnih sistemov.
<<http://www.cgsecurity.org/wiki/PhotoRec>>.

Forenzična analiza

- Autopsy:
 - analiza datotečnega sistema;
 - neposreden pregled vsebine diska (po sektorjih);
 - iskanje ključnih besed;
 - identificiranje programske opreme (tudi zlonamerne) z uporabo NIST National Software Reference Library (NSRL);
 - pregled datotek in izbrisanih datotek;
 - itd.

Forenzična analiza

The image shows a forensic analysis interface. On the left, a list of disk sectors is displayed, including Sector 129606, 129607, 129608, 145409, 145410, 145411, and 145698. Each sector entry includes a hex address and a file name, with some parts redacted with black boxes. On the right, a detailed view of Sector 195123 is shown. It is identified as 'Allocated' and contains an ASCII text file. The file's content is an email header and body, with several fields redacted. The email header includes fields like 'Subject', 'From', 'To', 'Date', 'Message-Id', 'Mime-Version', 'X-Mailer', 'X-Virus-Scanned', and 'X-Sanitizer'. The body of the email is partially visible, showing a reference to '143.219))' and a mention of 'Postfix'.

ASCII (display - [report](#)) Hex (display - [report](#)) ASCII Strings (display - [report](#))

File Type: ASCII text, with CRLF line terminators

Sector: 195123
Allocated
[Find Meta Data Address](#)

ASCII Contents of Sector 195123 in sdc-32-507391

```
143.219))
    by posta. [redacted] (Postfix) with ESMTP id 2DF35F00B2
    for <matthai@[redacted]>; Thu, 10 Mar 2005 [redacted] +0100 (CET)
Subject: [Fwd: [redacted]]
From: Primoz <primoz@[redacted]>
To: matthai@[redacted]
Content-Type: multipart/mixed; boundary="--OaA5XraW0KdWrjjFIku"
Date: Thu, 10 Mar 2005 [redacted] +0100
Message-Id: <[redacted]>
Mime-Version: 1.0
X-Mailer: Evolution 2.0.3
X-Virus-Scanned: by amavisd-new at posta.[redacted]
X-Sanitizer: Advosys
```

- Forenzična analiza diska z orodjem **Autopsy**. Orodje je našlo izbrisano elektronsko sporočilo v ostanku v datotečnega sistema, tim. "slack space".

Forenzična analiza

```
.....H...p.....lf..X...Book....CDCa....HistP...Inte@.
.HostName....w.w.w...[REDACTED]...o.r.g...r.....vk
.
.

E.3.B.B.1.F.6.4.0.6.D.3.E.4.F.8.B.C.4.1.1.A.8.B.1.C.F.B.1.3.3.1.3.D.2.8.3.9.3.6.6.D.6
.....@...x.....*...v.e.....matej@193.[REDACTED]...o.r..

.UserName....[REDACTED].....vk.....PingType....nk ..n.....
```

- Forenzična analiza diska z orodjem **Autopsy**. Orodje je na disku našlo podatke o dostopih uporabnika na oddaljene strežnike preko protokola ssh in telnet.

Trajno brisanje podatkov

- Trajno brisanja (ang. *wiping*), vsebino datotek izbriše s prepisovanjem novih (navadno naključnih) podatkov čez stare.
- Trajno brisanje znotraj obstoječega datotečnega sistema na nekaterih datotečnih sistemih (tim. *journal file systems*) ni učinkovito!
- Najbolj zanesljivo je trajno brisanje celotnega trdega diska, ki povezi obstoječi datotečni sistem.

Trajno brisanje podatkov

- Praviloma se uporablja večkratno prepisovanje (ang. *number of passes*):
 - PGP za običajne uporabnike priporoča **tri prehode**, kot zgornjo mejo pa navaja **26 prehodov**;
 - priporočilo ameriškega obrambnega ministrstva iz januarja 1995 priporoča **sedem prehodov** (U.S. Department of Defense, 1995: 8-306);
 - postopek nepovratnega brisanja podatkov, ki ga je opisal Peter Gutmann v članku *Secure Deletion of Data from Magnetic and Solid-State Memory* zahteva **35-kratno prepisovanje** podatkov po posebnem postopku.

Trajno brisanje podatkov

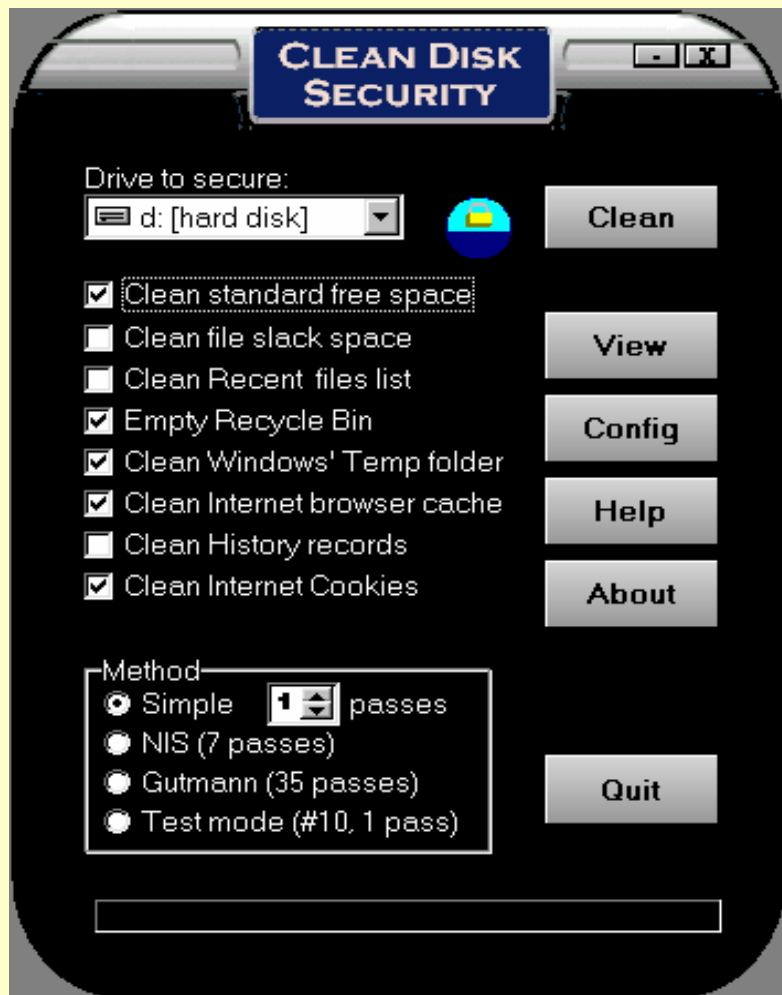
Section 3. Controls and Maintenance

8-300. Physical Security.

- a. Physical security safeguards shall be established that prevent or detect unauthorized access to accredited system entry points and unauthorized modification of the AIS hardware and software. Hardware integrity of the AIS, including remote equipment, shall be maintained at all times, even when the AIS is not processing or storing classified information.
 - b. Attended classified processing shall take place in an area, normally a Restricted Area, where authorized persons can exercise constant surveillance and control of the AIS. All unescorted personnel to the area must have a government granted PCL and controls must be in place to restrict visual and aural access to classified information.
 - c. When the AIS is processing classified information unattended, or when classified information remains on an unattended AIS, a Closed Area is required.
 - d. When the AIS is not in use, all classified information has been removed and properly secured, and the AIS has been downgraded, continuous physical protection, to prevent or detect unauthorized modification of the AIS hardware and software, shall be implemented through one or more of the following methods:
 - (1) Continuous supervision by authorized personnel.
 - (2) Use of approved cabinets, enclosures, seals, locks or Closed Areas.
 - (3) Use of area controls that prevent or detect tam-
- uncleared persons is used in a classified processing period, it must be reviewed or tested by authorized and knowledgeable contractor personnel to provide reasonable assurance that security vulnerabilities do not exist.
- b. The AISSP must provide procedures for approval of installation of any software on the AIS.
 - c. Software provided on media that may be written to (e.g., magnetic media) must be safeguarded commensurate with the accreditation level unless a physical write-protect mechanism is used. (Mechanisms shall be tested and verified by attempting to write to the media.) The write protection mechanism must be verified once during each session when it is used to process classified information.
 - d. Unclassified software provided on media that cannot be changed (e.g., CD read-only media) may be loaded onto the classified system without being labeled or classified provided it is immediately removed from the security area upon completion of the loading procedure. If the media is to be retained in the security area, it may be controlled and stored as unclassified media.
 - e. The contractor shall validate the functionality of security-related software (e.g., access control, auditing, purge, etc.) before the AIS is accredited. The software shall be revalidated when changed.
 - f. Use of software of unknown or suspect origin is strongly discouraged.

Ameriški vojaški priročnik *National Industrial Security Program Operating Manual (NISPOM 1995)*, poglavje 8, sekcija 3 (Controls and Maintenance), ki opredeljuje varno brisanje.

Trajno brisanje podatkov



Clean Disk Security – orodje namenjeno trajnemu brisanju podatkov v okolju Windows. Orodje briše datoteke znotaj datotečnega sistema, omogoča pa tudi samodejno brisanje začasnega pomnilnika (*swap*) ob zaustavitvi sistema.

V okolju Linux je na voljo podobno konzolno orodje *wipe*.

Previdnost pri uporabi tovrstnih orodij, saj uničenih podatkov ni več mogoče obnoviti!

Trajno brisanje podatkov

```
Darik's Boot and Nuke 1.0.7

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

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

----- Wipe Method -----

Quick Erase                syslinux.cfg: nuke="dwipe --method dodshort"
RCMP TSSIT OPS-II         Security Level: Medium (3 passes)
▶ DoD Short
DoD 5220.22-M
Gutmann Wipe
PRNG Stream

The American Department of Defense 5220.22-M short wipe.
This method is composed of passes 1,2,7 from the standard wipe.

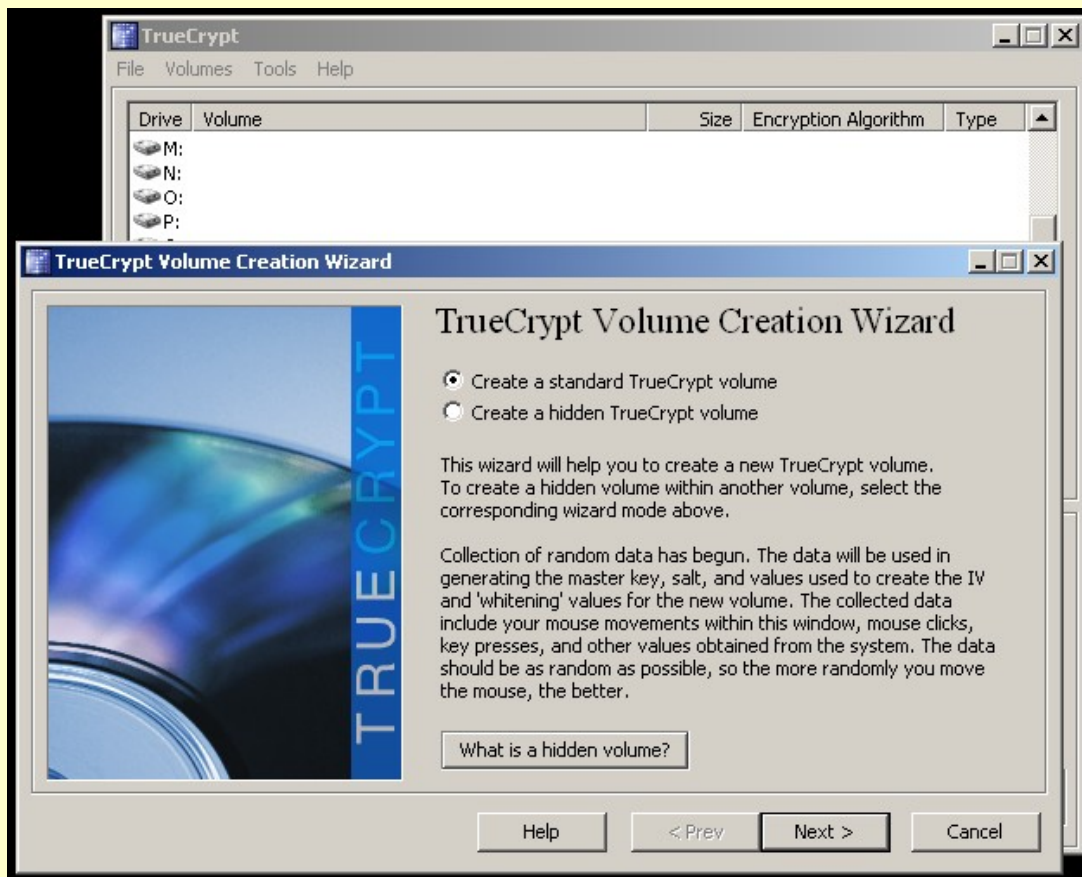
J=Up K=Down Space=Select
```

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

Onemogočanje "forezničnih napadov"

- Najbolj zanesljiva metoda je uporaba šifriranja nosilcev občutljivih podatkov. Ob tem je potrebno poskrbeti za zanesljive rezervne kopije!
- Šifriranje datotek s pomembnimi ali občutljivimi podatki.
- Šifriranje particij ali virtualnih particij pomnilniških nosilcev.
- Problem: začasni pomnilnik (swap, cache).
- Rešitev: šifriranje celotnega sistema.

Onemogočanje “forezničnih napadov”



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

Onemogočanje "forezničnih napadov"

- Šifriranje celotnega sistema je pod Linuxom razmeroma enostavno dostopno. Z izbiro Ubuntu Linuxa si zagotovimo tudi uporabniško prijaznost sistema. Potrebna orodja:
 - **Ubuntu** "alternate install" namestitveni CD (zaradi enostavnosti najprej namestimo strežniško različico sistema, po končani namestitvi šifrirne sheme pa še grafični del);
 - **Cryptsetup**, orodje za konfiguracijo in delo s šifriranimi diskovnimi particijami;
 - **Yaird**, orodje za ustvarjanje zagonske slike sistema (*tim. initial boot image*).

Šifriranje celotnega sistema

- Delovanje šifrirne sheme:
 - ob zagonu sistema iz particije /boot je potrebno vnesti geslo;
 - s pomočjo gesla se dešifriran in priklopi korenska particija (root) in začne se nalaganje jedra operacijskega sistema;
 - particija z uporabniškimi podatki (/home) se samodejno naloži s pomočjo ključa shranjenega v posebni datoteki (ključ vsebuje naključno generirane podatke);
 - geslo za /swap particijo se generira ob vsakem zagonu sistema naključno (/dev/random ali /dev/urandom).

Šifriranje celotnega sistema

Priklopna točka	Velikost	Razdelek
/boot	118 Mb	Partition 1 Disc IDE/ATA 1 (Primary) [hda1]
/	2 Gb	Partition 2 Disc IDE/ATA 1 (Primary) [hda2]
	100 Gb	Partition 3 Disc IDE/ATA 1 (Primary) [hda3]
	10 Gb	Partition 4 Disc IDE/ATA 1 (Primary) [hda4]

Priklopna točka	Velikost	Razdelek
/boot	118 Mb	Partition 1 Disc IDE/ATA 1 (Primary) [hda1]
/swap	2 Gb	Partition 2 Disc IDE/ATA 1 (Primary) [hda2]
/home	100 Gb	Partition 3 Disc IDE/ATA 1 (Primary) [hda3]
/root	10 Gb	Partition 4 Disc IDE/ATA 1 (Primary) [hda4]

Shema diska pred in po vzpostavitvi šifriranja na celotnem sistemu.

Dobre prakse varnega uničevanja nosilcev podatkov



Vir: *Slo-Tech.com*, 2001; članek: "Radostna destrukcija".

Dobre prakse varnega uničevanja nosilcev podatkov

Orodja za forenzično analizo so dostopna in razmeroma enostavna za uporabo!

Priporočila za zavarovanje kritičnih nosilcev podatkov in njihovo varno uničevanje:

- Nadzorovanje fizičnega dostopa do računalniške opreme.
- Previdnost pri servisiranju pri zunanjih serviserjih.
- Dobre prakse uničevanja in prodajanja odsluženih ali odpisanih računalniških komponent.
- Dobre prakse pri uporabi prenosnih pomnilniških sistemov in prenosnih računalnikov.
- Uporaba šifriranja.