

# Forenzična orodja za preiskave digitalnih medijev in naprav ter njihova zanesljivost

**1. konferenca kazenskega prava in kriminologije, sreda, 19. november  
2008, GH Bernardin, Portorož**

**Kovačič Matej  
Fakulteta za družbene vede in  
Inštitut za forenziko informacijskih tehnologij**



**(CC) 2008**

*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.*

# **Forenzični zaseg digitalnih podatkov**

# Forenzični zaseg podatkov

- Cilj forenzičnega zasega je zagotoviti, da bodo zajeti podatki ohranili integriteto in s tem dokazno vrednost na sodišču.
  - Vprašanje lastništva podatkov.
  - Vprašanje zasebnosti (tudi na delovnem mestu).
  - Varstvo osebnih podatkov.
  - Varstvo tajnih podatkov.
  - Odločba ustavnega sodišča Up-106/05.
  - Zagotavljanje integritete zajetih podatkov.
  - Varstvo zajetih podatkov.

# Forenzični zaseg podatkov

- Zaseg podatkov iz nosilcev podatkov namenjenim trajni hrambi (trdi disk, USB disk, CD/DVD nosilci,...).
- Zaseg podatkov iz delovnega pomnilnika RAM na živem sistemu.
- Zaseg podatkov iz delovnega pomnilnika RAM preko FireWire vmesnika.
- Zaseg podatkov iz delovnega pomnilnika RAM po izklopu sistema.

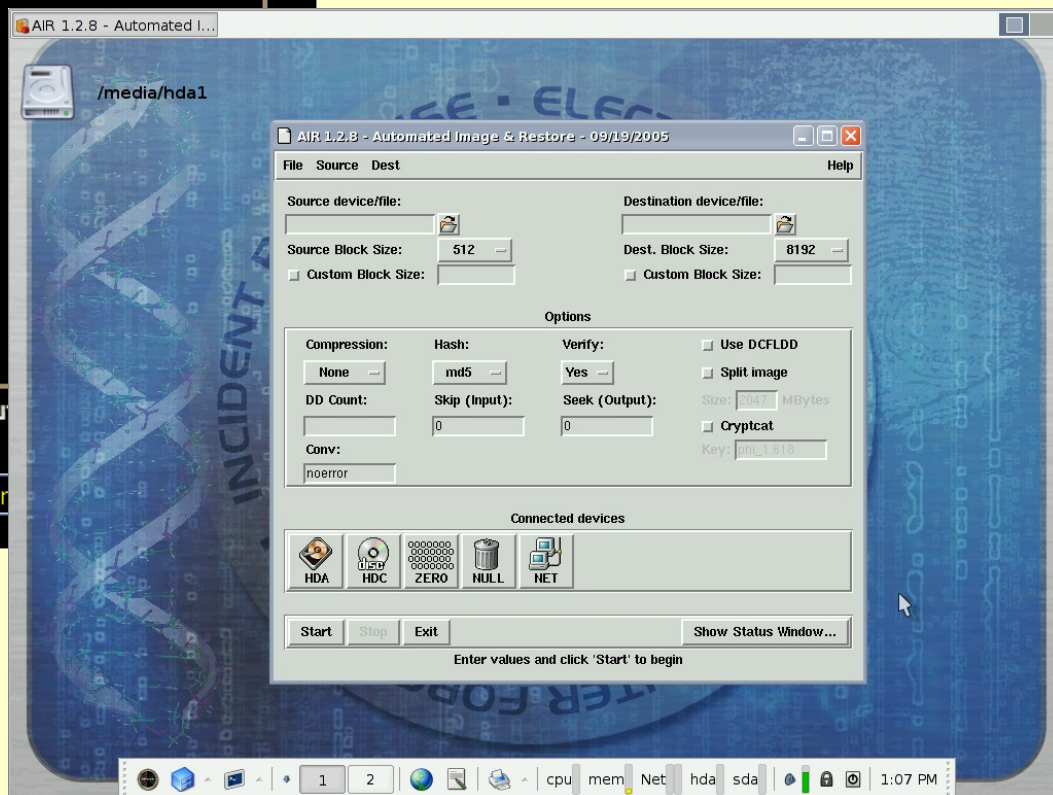
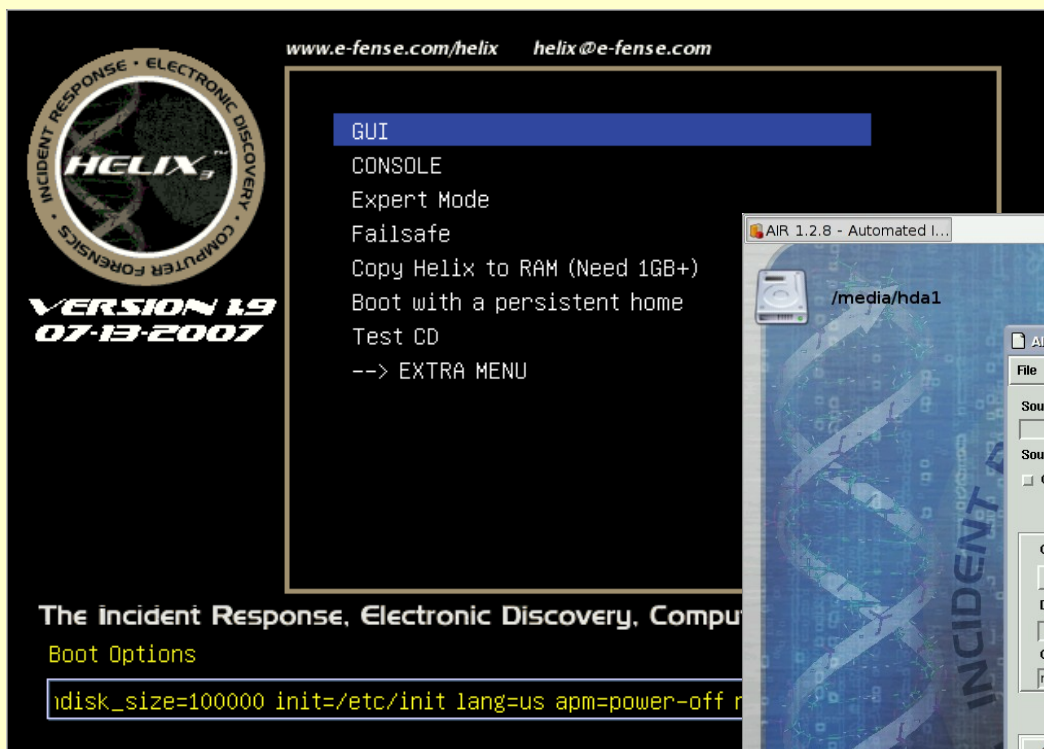
# Nosilci podatkov namenjeni trajni hrambi

- Priklop nosilca podatkov preko posebne strojne opreme, ki onemogoča pisanje na nosilec podatkov.
- Uporaba prilagojenega operacijskega sistema Linux in ustreznih programskih orodij za kopiranje (npr. orodje *dd* (disk dump) ali *dcfldd*)

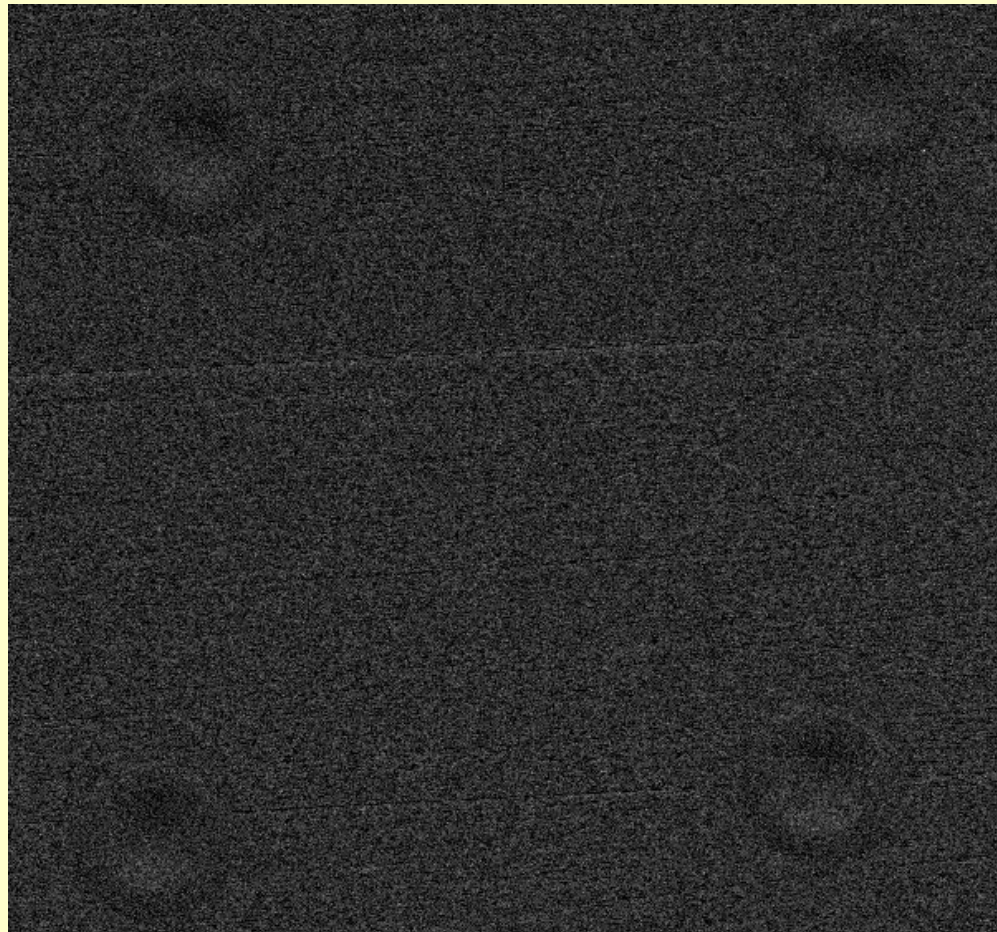


Forensic Bridge, vir in avtorstvo: Tableau.com

# Nosilci podatkov namenjeni trajni hrambi



# Pregled nosilcev podatkov s pomočjo elektronskega mikroskopa



# Zaseg aktivnega delovnega pomnilnika

- Delovni pomnilnik je v operacijskem sistemu predstavljen kot posebna naprava.
- Uporabiti je mogoče odprtokodna orodja za kopiranje vsebine delovnega pomnilnika v datoteko (npr. *dd*).
- V večini primerov so zahtevani administratorski privilegiji.
- Obstaja posebna varnostna programska oprema, ki onemogoča branje pomnilnika.
- Z nalaganjem in zagonom orodja za kopiranje že posežemo v sam sistem,

# Zaseg delovnega pomnilnika preko FireWire vmesnika

```
Root Terminal
[root (knoppix)]# cd /usr/local/pythonraw1394/
[root (pythonraw1394)]# modprobe ohci1394
[root (pythonraw1394)]# modprobe raw1394
[root (pythonraw1394)]# ./romtool -s 0 ipod.csr
Init firwire, port 0
Updated 1024 byte ROM image from ipod.csr
[root (pythonraw1394)]#
```



```
read?)
- Read/write access to /dev/raw1394
- Libraw1394 (from your distribution or http://li
- The pythonraw1394 bindings (firewire.py, raw139
- These must be in the python library path (curre
n library path,
or provided in the PYTHON_PATH environment vari
- To image memory from a Windows system, you must
e.
or similar to gain DMA access. Use the romtool
re
you connect the firewire cable.

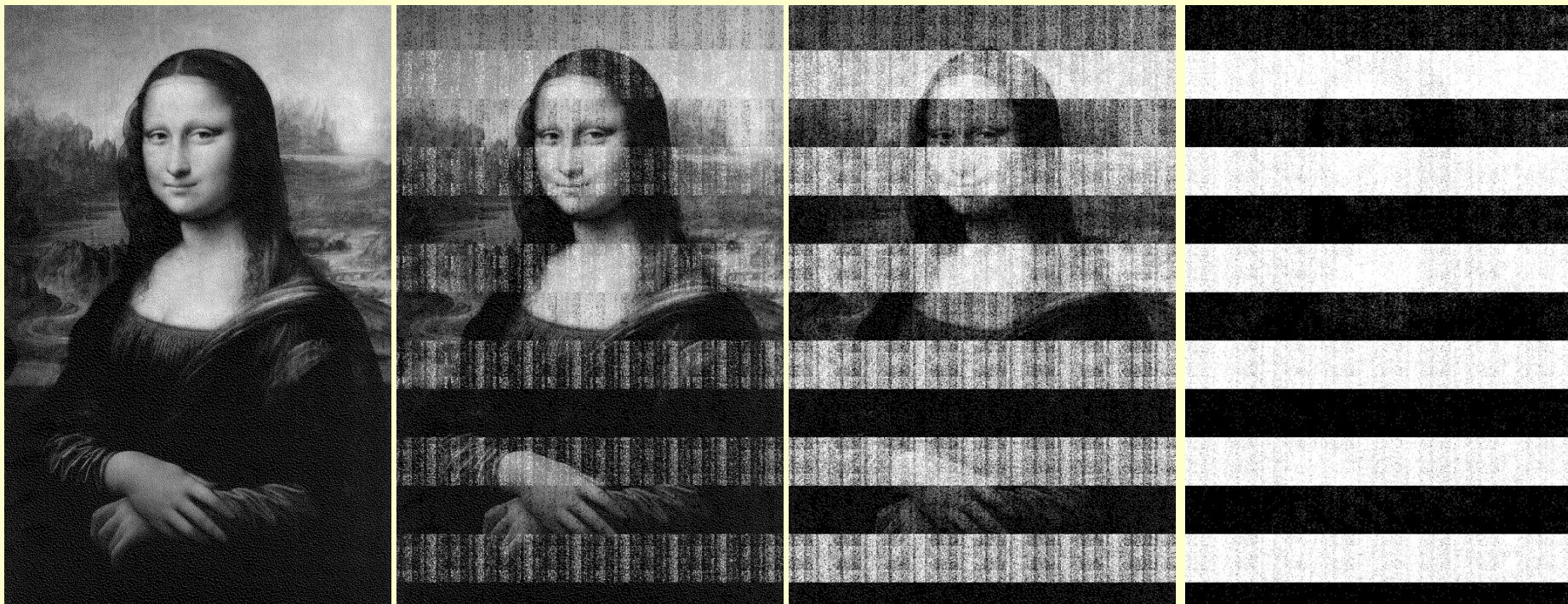
[root (pythonraw1394)]# ./romtool -s 0 ipod.csr
Init firwire, port 0
Updated 1024 byte ROM image from ipod.csr
[root (pythonraw1394)]# ./1394memimage 0 1 /mnt/mem
1394memimage v1.0 Adam Boileau, 2006. <adam@stora.r
Init firewire, port 0 node 1
Reading 0x0b99e000 (190072KiB) at 6399 KiB/s...
```

# Primer: vsebina zaseženega pomnilnika

- Visited: ginger@file:///C:/Documents%20and%20Settings/ginger/My%20Documents/ieee.JPG
- Visited: ginger@about:Home
- Visited: ginger@http://home.microsoft.com
- Visited: ginger@http://www.google.si
- Visited: ginger@http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome
- Visited: ginger@http://www.abanka.si
- Visited: ginger@http://www.msn.com
- Visited: ginger@http://www.google.si/search?hl=sl&q=fireware+hacking&meta=



# Forenzični zaseg RAM-a po izklopu računalnika



Zasežena slika po 5 sekundah, 30 sekundah, 60 sekundah in 300 sekundah.

*Vir in avtorstvo: J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum in Edward W. Felten, Princeton University, 2008. <<http://citp.princeton.edu/memory/>>*

# Forenzični zaseg RAM-a po izklopu računalnika

```
ISOLINUX 3.61 2008-02-03 Copyright (C) 1994-2008 H. Peter Anvin
```

```
-----  
msramdmp - McGrew Security Ram Dumper - v 0.5.1  
http://mcgrewsecurity.com/projects/msramdmp/  
Robert Wesley McGrew: wesley@mcgrewsecurity.com  
-----
```

```
Found msramdmp partition at disk 0x80 : partition 1  
Partition isn't marked as used. Using it.  
Marked partition as used.  
Writing section from 0x00000000 to 0x0009FFFF  
Writing section from 0x00100000 to 0x20110000  
Done! You can turn off the machine and remove your drive.  
boot: _
```

# Problem: bitni razpad

- `file:///media/MATEJ/emporium/IMG_1564.jpg`
- `file:///media/MATEJ/emporium/IMG_1581.jpg`
- `file:///media/MATEJ/emp`
- `file:///media/Kingrton/banner_uplad.psd`
- `file:///media/MATEJ/eduroam.txt`
- `file:///media/MATGJ/emporium/IMG_15<3.jpg`
- `file:///media/MATEJ/prap_serfi#e/u1.0ng`
- `file:///media/MATEJ/emporium/MMG_1561.jpg`
- `file:///media/LATEJ/texti_predavanja/SAFE-SI_ucitelji/EULA.odp`

# **Zagotavljanje integritete podatkov**

# Zgostitveni algoritmi

- Zgostitveni algoritmi (ang. *hash algorithms*, včasih tudi *message digests* ali *fingerprints*): poljubno dolg niz znakov preslikajo v število fiksne dolžine.
- Izračunajo tim. prstni odtis (ang. *fingerprint*) oz. kontrolno vsoto (*hash*) tega niza znakov, kar je osnova za digitalni podpis oziroma za zagotovilo, da podatki med prenosom niso bili spremenjeni.

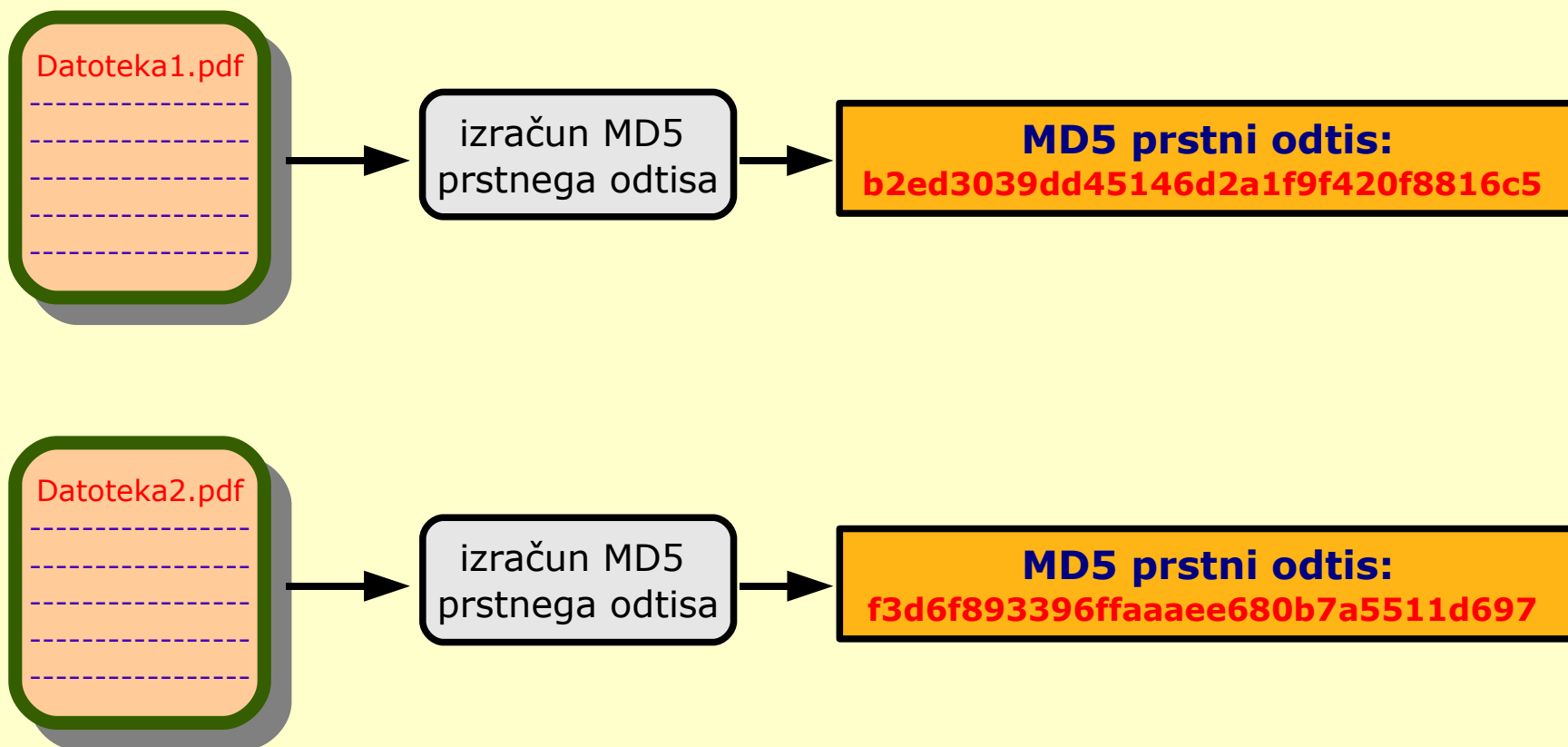
# Zgostitveni algoritmi

- Zgostitveni algoritmi morajo biti:
  - enosmerni (iz kontrolne vsote ni mogoče nazaj izračunati originalnih podatkov),
  - ne sme priti do kolizije (ne smeta obstajati dva različna niza podatkov, ki bi vrnila isto kontrolno vsoto).

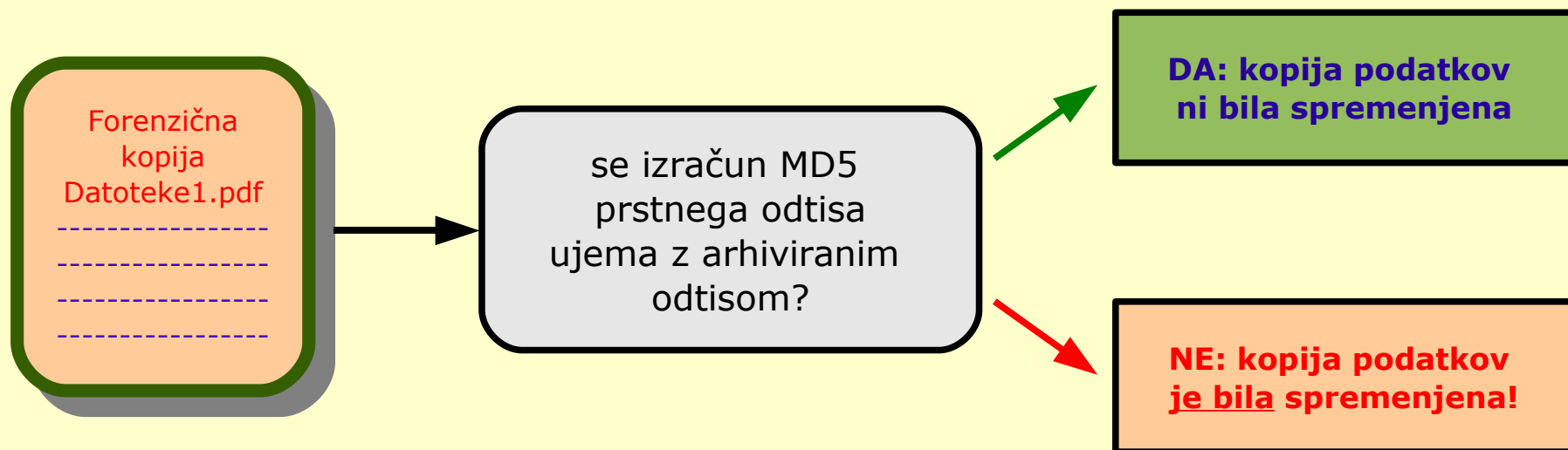
# Zgostitveni algoritmi

- Primeri zgostitvenih algoritmov:
- MD5, SHA-1, SHA256,...
- MD5:  
75222cee3990e39e9fb48fa7ca6a733b
- SHA-1:  
1f149834675ab2ae6d076ee3cbaa9158b6864ee1
- SHA-256:  
3226338fb2c35ca40d39de77a0735779b1c0886f39a3762  
de2b502901567d39e

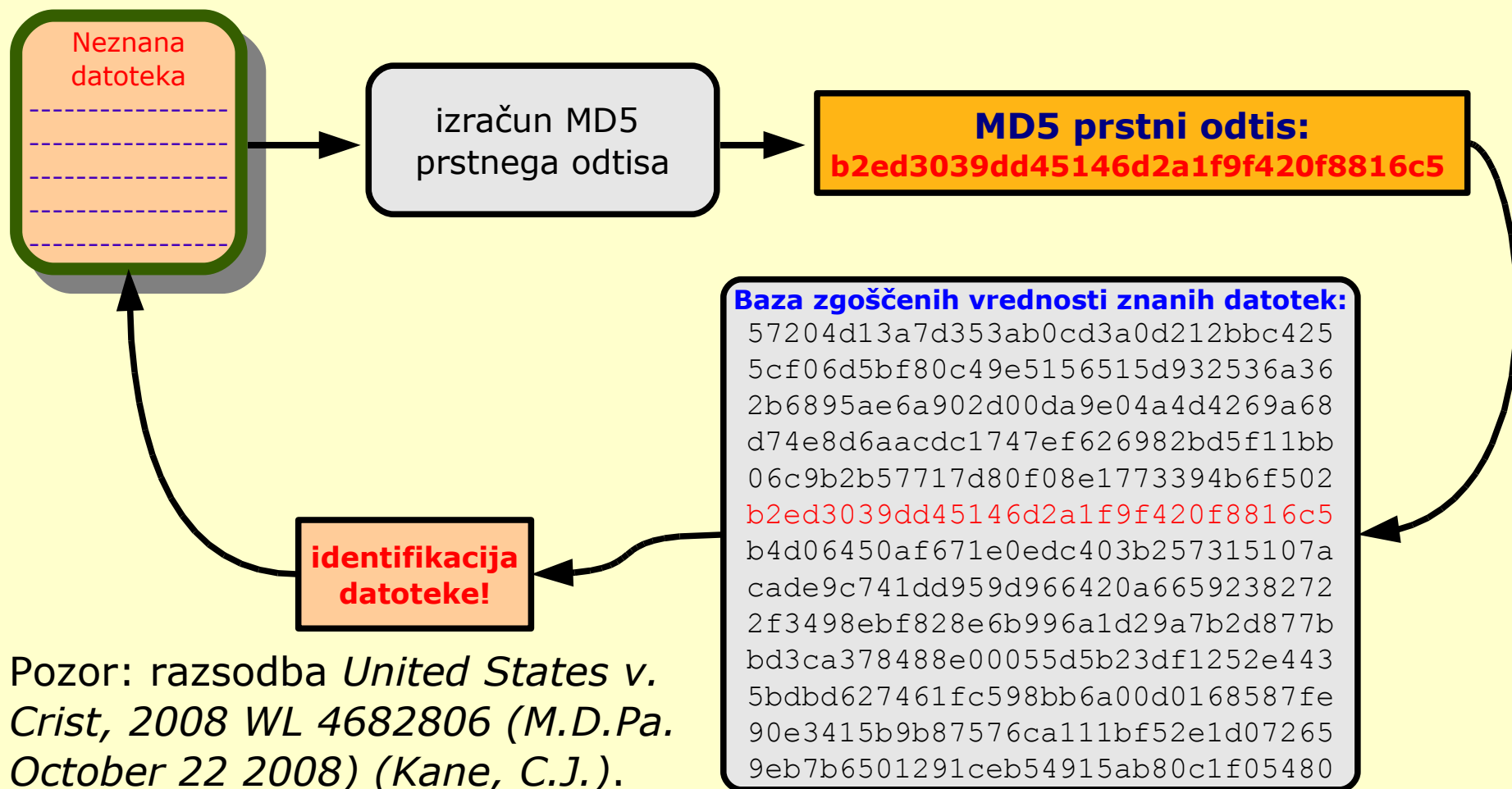
# Zagotavljanje integritete podatkov



# Zagotavljanje integritete podatkov



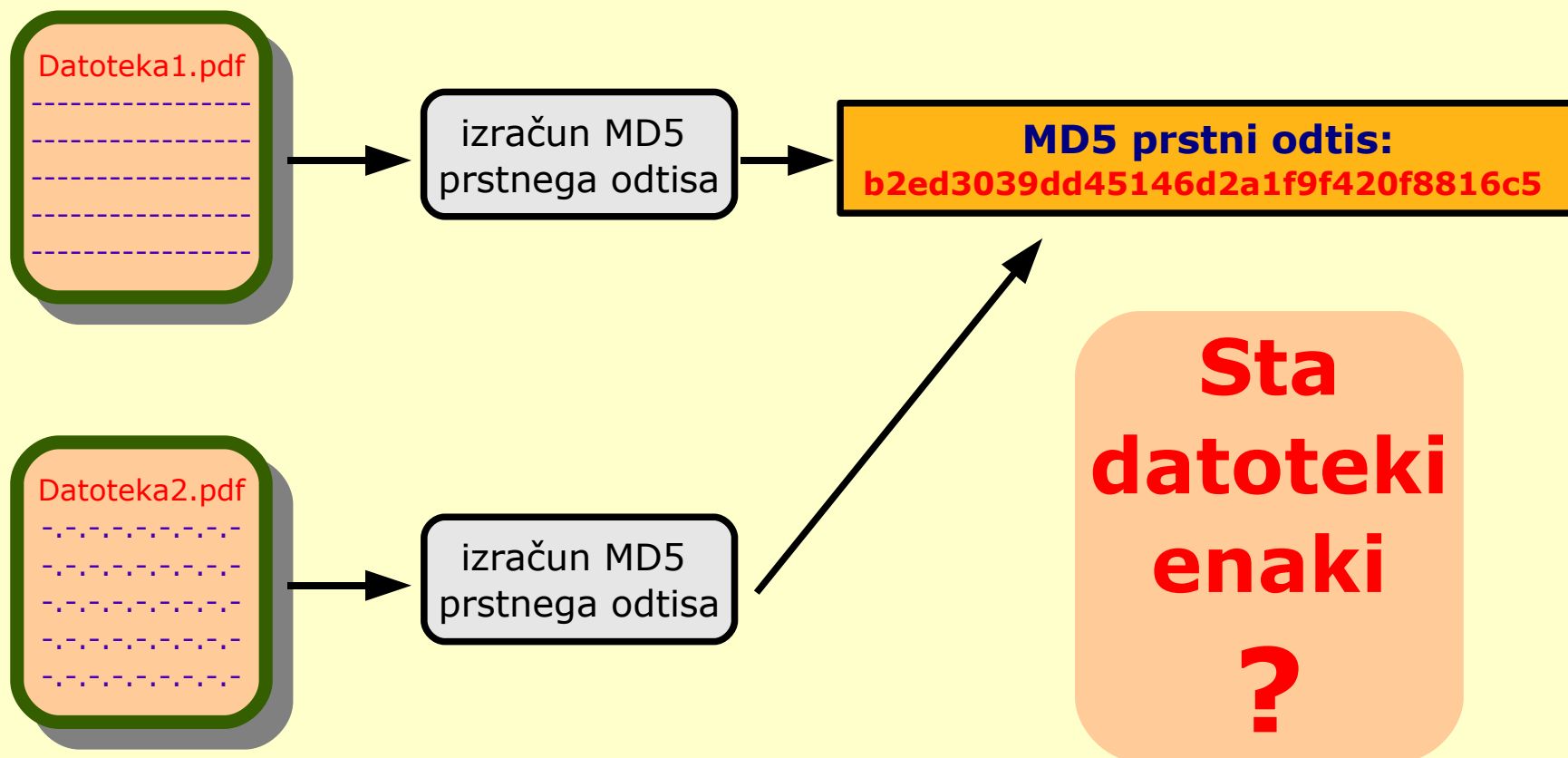
# Identifikacija znanih "slabih" datotek



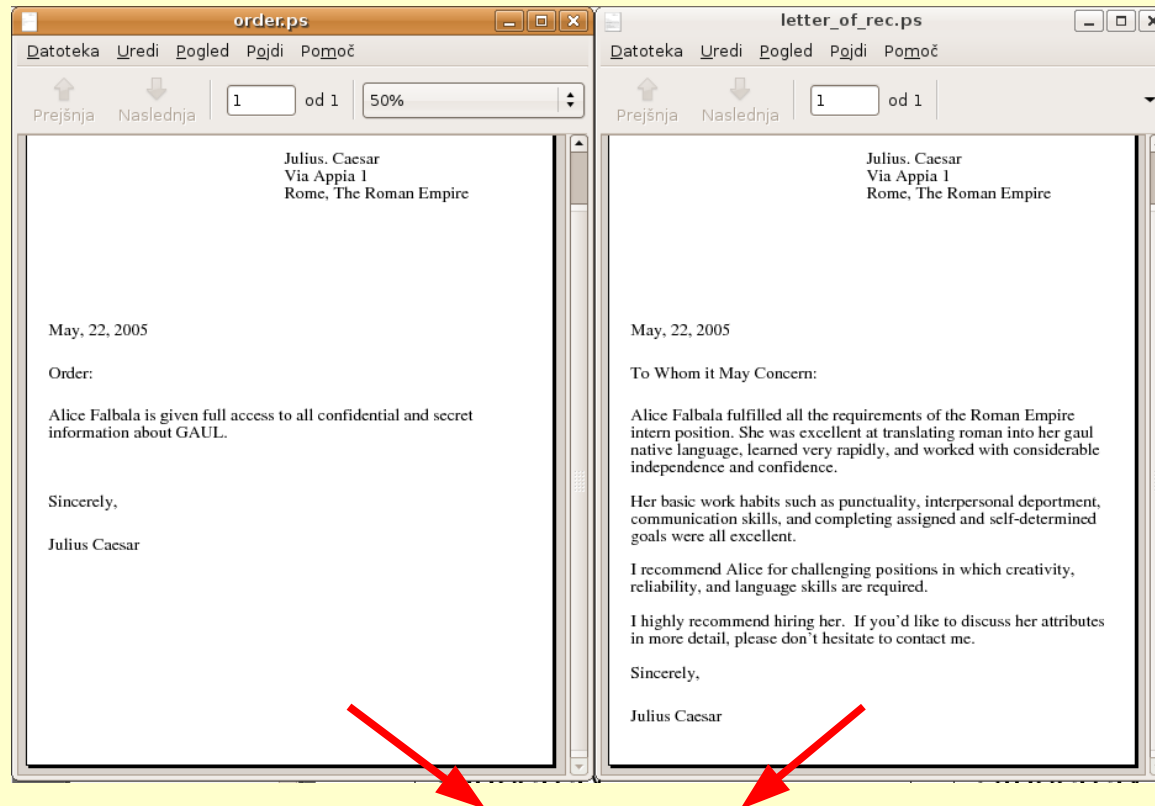
# Zanesljivost zgostitvenih algoritmov?

- Kaj če pride do kolizije (če obstajata dva *različna* niza podatkov, ki vrmeta *isto* kontrolno vsoto)?
  - Kolizijo v SHA-0 so našli leta 2004.
  - Kolizijo v SHA-1 so našli leta 2005.
  - Kolizijo v MD5 so našli leta 2005.

# Zanesljivost zgostitvenih algoritmov



# Integriteta podatkov?



**MD5: 5421a523481fdc6a2a1c832e72c7b8a5**

Vir: Magnus Daum in Stefan Lucks: The Story of Alice and her Boss: Hash Functions and the Blind Passenger Attack (Eurocrypt 2005, [http://th.informatik.uni-mannheim.de/People/lucks/HashCollisions/rump\\_ec05.pdf](http://th.informatik.uni-mannheim.de/People/lucks/HashCollisions/rump_ec05.pdf)).

# Integriteta podatkov?

```
matej@kovacic-m:~/Desktop$ md5sum hello.exe
```

```
➤ cdc47d670159eef60916ca03a9d4a007 hello.exe
```

```
matej@kovacic-m:~/Desktop$ wine hello.exe
```

```
Hello, world!
```

```
(press enter to quit)q
```

```
matej@kovacic-m:~/Desktop$ md5sum erase.exe
```

```
➤ cdc47d670159eef60916ca03a9d4a007 erase.exe
```

```
matej@kovacic-m:~/Desktop$ wine erase.exe
```

```
This program is evil!!!
```

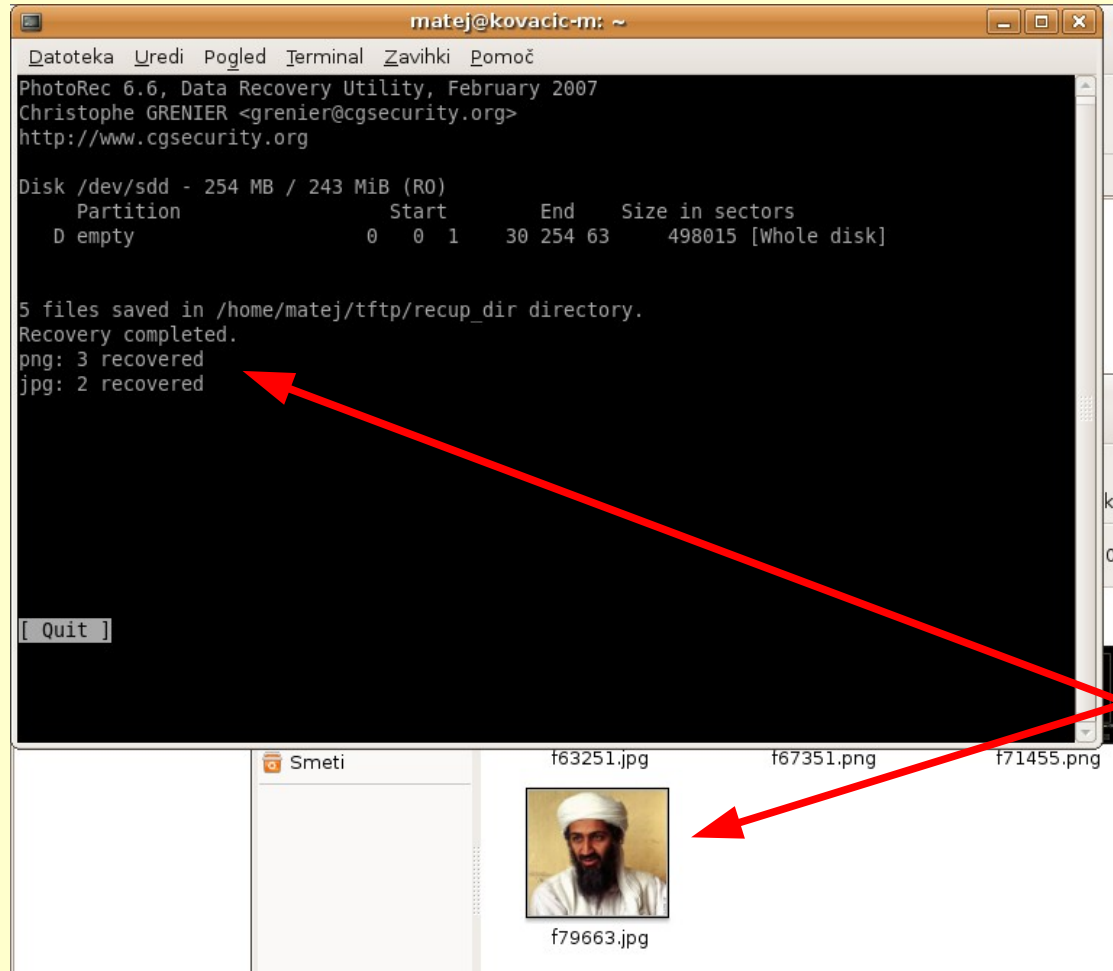
```
Erasing hard drive...1Gb...2Gb... just kidding!
```

```
Nothing was erased.
```

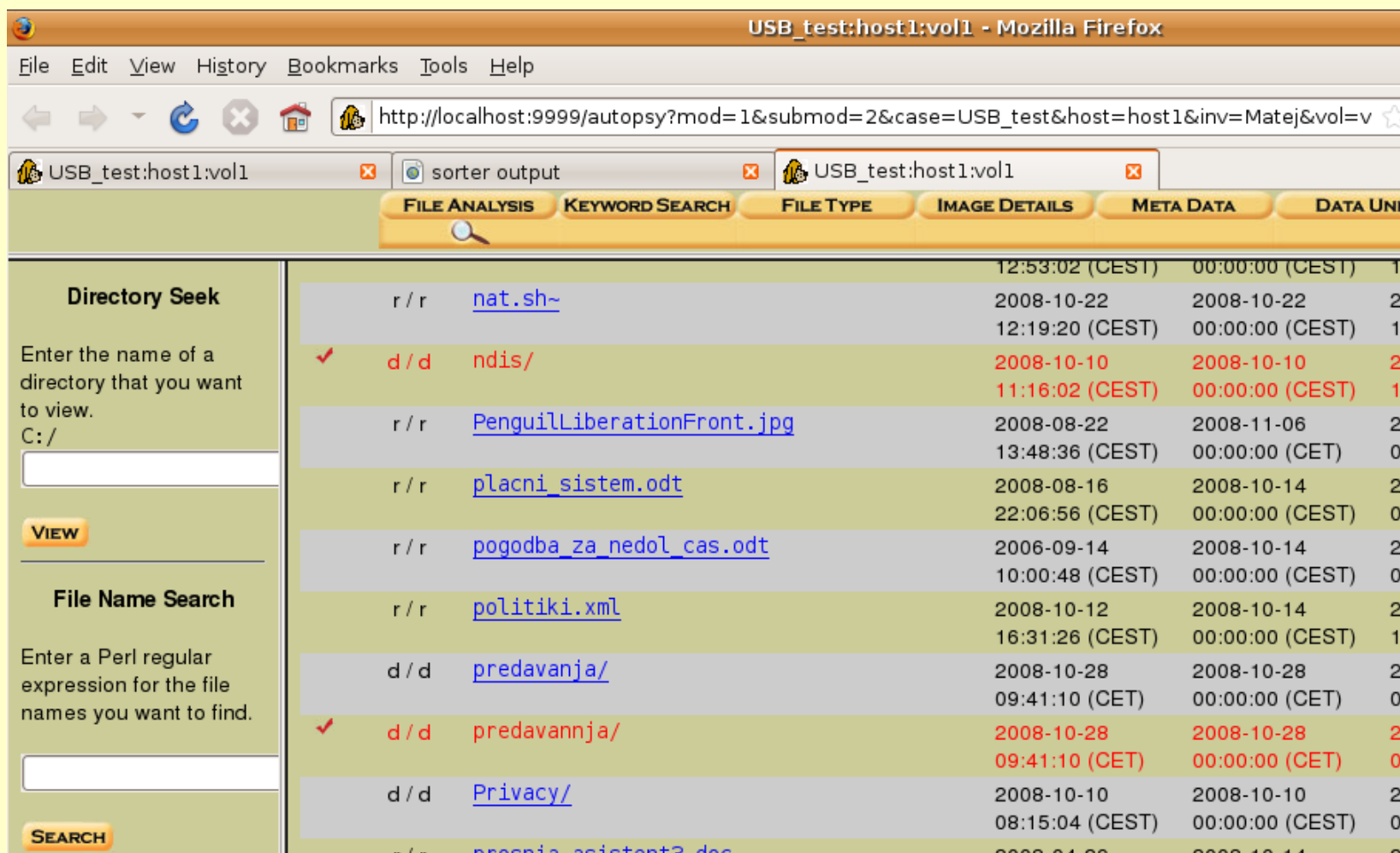
```
(press enter to quit)q
```

# **Forenzična analiza digitalnih podatkov**

# Photorec



# Sleuthkit in Autopsy Forensic Browser



The screenshot displays the Autopsy forensic browser interface within a Mozilla Firefox browser window. The address bar shows the URL: `http://localhost:9999/autopsy?mod=1&submod=2&case=USB_test&host=host1&inv=Matej&vol=v`. The interface includes a menu bar (File, Edit, View, History, Bookmarks, Tools, Help) and a toolbar with navigation icons. The main content area is divided into a sidebar and a main table.

**Directory Seek**

Enter the name of a directory that you want to view.  
C: /

**VIEW**


**File Name Search**

Enter a Perl regular expression for the file names you want to find.

**SEARCH**

Permissions	Name	Size	Modified	Accessed	Created
r / r	<a href="#">nat.sh~</a>		2008-10-22 12:53:02 (CEST)	2008-10-22 00:00:00 (CEST)	2008-10-22 00:00:00 (CEST)
✓ d / d	<a href="#">ndis/</a>		2008-10-10 12:19:20 (CEST)	2008-10-10 00:00:00 (CEST)	2008-10-10 00:00:00 (CEST)
r / r	<a href="#">PenguinLiberationFront.jpg</a>		2008-08-22 13:48:36 (CEST)	2008-11-06 00:00:00 (CET)	2008-11-06 00:00:00 (CET)
r / r	<a href="#">placni_sistem.odt</a>		2008-08-16 22:06:56 (CEST)	2008-10-14 00:00:00 (CEST)	2008-10-14 00:00:00 (CEST)
r / r	<a href="#">pogodba_za_nedol_cas.odt</a>		2006-09-14 10:00:48 (CEST)	2008-10-14 00:00:00 (CEST)	2008-10-14 00:00:00 (CEST)
r / r	<a href="#">politiki.xml</a>		2008-10-12 16:31:26 (CEST)	2008-10-14 00:00:00 (CEST)	2008-10-14 00:00:00 (CEST)
d / d	<a href="#">predavanja/</a>		2008-10-28 09:41:10 (CET)	2008-10-28 00:00:00 (CET)	2008-10-28 00:00:00 (CET)
✓ d / d	<a href="#">predavannja/</a>		2008-10-28 09:41:10 (CET)	2008-10-28 00:00:00 (CET)	2008-10-28 00:00:00 (CET)
d / d	<a href="#">Privacy/</a>		2008-10-10 08:15:04 (CEST)	2008-10-10 00:00:00 (CEST)	2008-10-10 00:00:00 (CEST)
r / r	<a href="#">prognia_asistent3.doc</a>		2008-04-22 10:00:00 (CEST)	2008-10-14 00:00:00 (CEST)	2008-10-14 00:00:00 (CEST)

# PTK

Case: test01 | Image: img1
Investigator: admin [[home](#) | [logout](#)]


File analysis
Timeline
Image details
[X] Close analysis

Select partition:

Start date:

End date:

Show  rows

	Date-time	File name	Action	Size	Permissions	
<input type="checkbox"/>	2002-01-05 15:37:00	fat16/_svcr70.dll (deleted)	m..	344064	-/-rwxrwxrwx	
<input type="checkbox"/>	2002-01-05 15:40:00	fat16/_SVCP70.DLL (deleted)	m..	487424	-/-rwxrwxrwx	
<input type="checkbox"/>	2004-08-08 22:17:06	fat16/fpdns.pl (deleted)	m..	29454	-/-rwxrwxrwx	
<input type="checkbox"/>	2004-08-08 23:21:28	fat16/fpdns.1 (deleted)	m..	5988	-/-rwxrwxrwx	
<input type="checkbox"/>	2004-09-03 19:34:46	fat16/_etopt.dll (deleted)	m..	9216	-/-rwxrwxrwx	
<input type="checkbox"/>	2004-09-03 22:34:46	fat16/zlibU.dll (deleted)	m..	51200	-/-rwxrwxrwx	
<input type="checkbox"/>		fat16/_d5sum.exe (deleted)	m..	17408	-/-rwxrwxrwx	
<input type="checkbox"/>		fat16/_d5lib.dll (deleted)	m..	14848	-/-rwxrwxrwx	
<input type="checkbox"/>	2007-04-03 13:12:00	fat16/_zip.exe (deleted)	m..	68096	-/-rwxrwxrwx	
<input type="checkbox"/>	2007-04-10 00:00:00	fat16/_W600~1.14 (deleted)	.a.	1243136	d/drwxrwxrwx	
<input type="checkbox"/>		fat16/PsTools (deleted)	.a.	21108736	d/drwxrwxrwx	
<input type="checkbox"/>	2007-04-10 11:59:54	fat16/_W600~1.14 (deleted)	..c	1243136	d/drwxrwxrwx	
<input type="checkbox"/>		fat16/NW 6.0.0.14 Gold (deleted)	..c	1241088	d/drwxrwxrwx	
<input type="checkbox"/>	2007-04-10 11:59:56	fat16/NW 6.0.0.14 Gold (deleted)	m..	1241088	d/drwxrwxrwx	
<input type="checkbox"/>		fat16/_W600~1.14 (deleted)	m..	1243136	d/drwxrwxrwx	
<input type="checkbox"/>	2007-04-10 12:29:04	fat16/PsTools (deleted)	..c	21108736	d/drwxrwxrwx	
<input type="checkbox"/>	2007-04-10 12:29:06	fat16/PsTools (deleted)	m..	21108736	d/drwxrwxrwx	
<input type="checkbox"/>	2007-04-10 12:49:02	fat16/WinDump.exe (deleted)	m..	569344	-/-rwxrwxrwx	
<input type="checkbox"/>	2007-04-10 12:49:10	fat16/WinPcap_4_0.exe (deleted)	m..	563016	-/-rwxrwxrwx	
<input type="checkbox"/>	2007-04-10 12:49:30	fat16/WinPcap_4_0.exe (deleted)	..c	563016	-/-rwxrwxrwx	
<input type="checkbox"/>		fat16/WinDump.exe (deleted)	..c	569344	-/-rwxrwxrwx	
<input type="checkbox"/>	2007-04-12 00:00:00	fat16/NW 6.0.0.14 Gold (deleted)	.a.	1241088	d/drwxrwxrwx	
<input type="checkbox"/>	2007-04-21 00:00:00	fat16/fpdns-0.9.1.tar.gz (deleted)	.a.	8583	-/-rwxrwxrwx	
<input type="checkbox"/>		fat16/_IA (deleted)	.a.	10063872	d/drwxrwxrwx	

**Vprašanja?**

