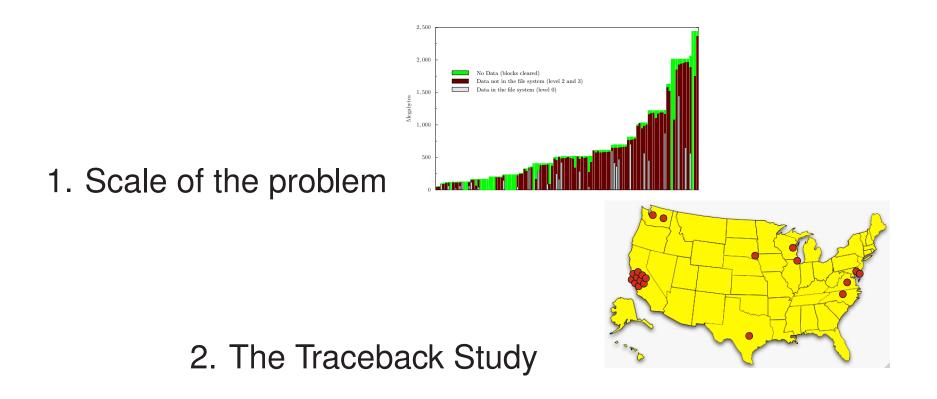
**Information Leakage and Computer Forensics** 

Simson L. Garfinkel Center for Research on Computation and Society Harvard University

February 17, 2006

#### The disk sanitization problem.



### **Disk Sanitization**

Recall some of the goals of computer security:

- Availability
- Confidentiality
- Data Integrity
- Control
- Audit

### Confidentiality means preventing unauthorized disclosure.

Data can be:

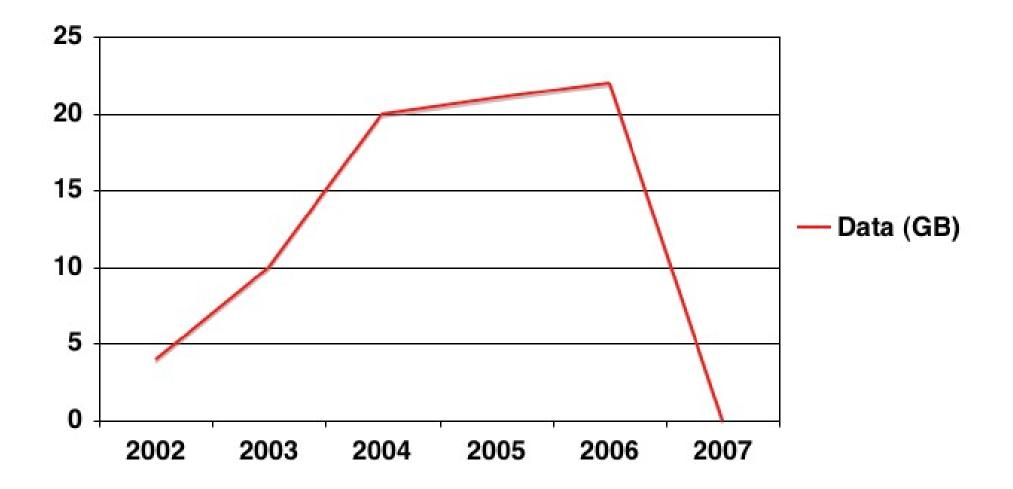
- In flight
- Stored



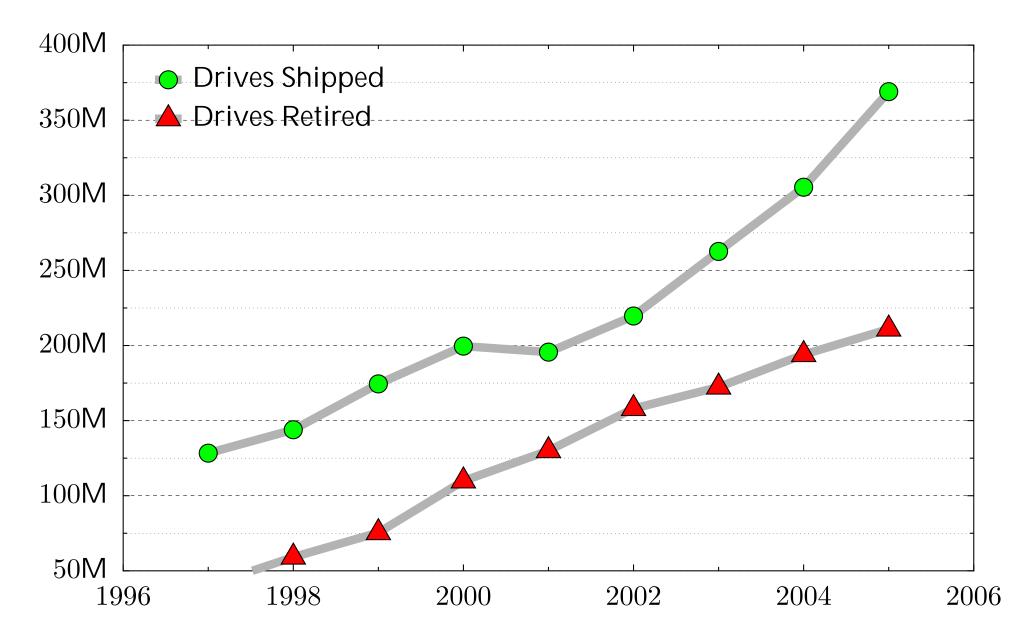


Most data spends most of its time in storage.

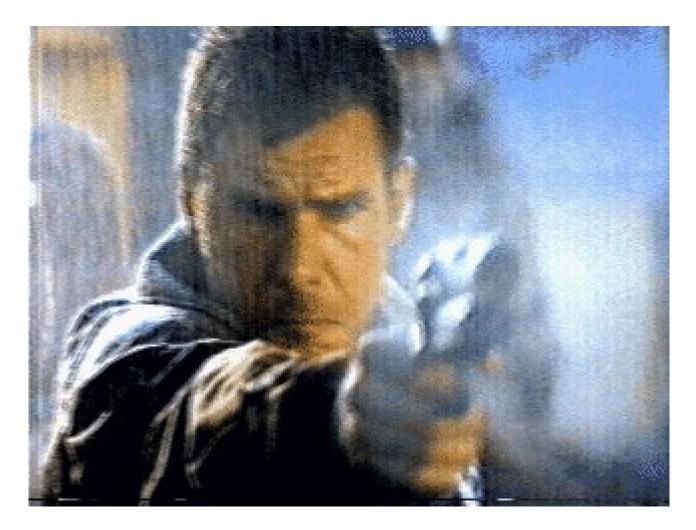
#### **Data over time: Conceptual**



#### 210 million drives will be retired this year.







### Deckard (Harrison Ford) retiring a replicant. "Blade Runner" (1982)

#### Hard drives pose special problem for computer security

Do not forget data when power is removed.

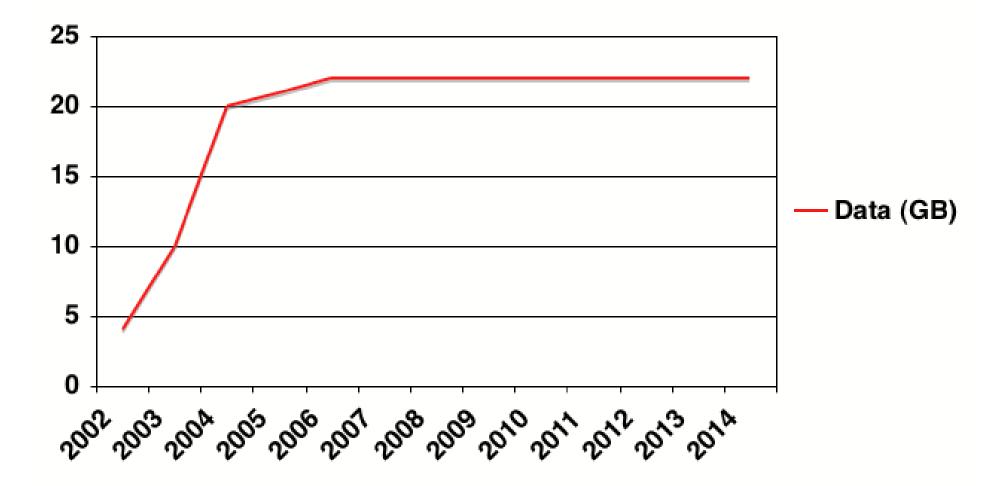
Contain data that is not immediately visible.

Today's computers can read hard drives that are 15 years old!

- Electrically compatible (IDE/ATA)
- Logically compatible (FAT16/32 file systems)
- Very different from tape systems



#### **Data over time: Actual**



#### There is a significant secondary market for used disk drives.

Retired drives are:

- Re-used within organizations
- Given to charities
- Sold at auction

350 items f	Second for hand drives         net ending first   peerly fisted   lowest priced   highest priced	iced		Save this search	
Picture	Item Tide	Price	Dids	Time Left	
đ	Lot of hard and floppy drives	\$5.50	2	14n	
đ	Lot of hard and floppy drives	\$5.50	2	22n	
đ	Lot of hard and floppy drives	\$5.50	2	256	
đ	Lot of 2 hard drives IDE	\$8.00	12	29n	
	3.2 gig Hard Drives	\$180.00		59n	
đ	(5) 1.2 hard drives & (15) 10/100 network	\$25.00	1	1h 00p	
	Lot of 3 Quantum 9.1 gig SCSI Hard Drives	\$26.00	6	1h 25p	
	IDE HARD DRIVES (3)	\$6.50	6	1h 46n	
đ	LOT OF 5 Hard Drives! 3.2 Oig Western Digital	\$120.00 \$124.95 #	Ly I Nor	1h 50p	
	OTY 3 IDE Hard Drives 2.5 Gg	\$20.50	5	2h 02n	
đ	5 WESTERN DIGITAL 2.5 GIG HARD DRIVES	\$30.00	4	2h 03a	
	QTY 3 IDE Hard Drives 1.0 Gig	\$9.99	1	2h 04n	
	Western Digital 850 meg IDE Hard Drives dutch	\$6.00	1	2h 57n	
	WINDOWS		6.00	- 3h 18n	

About 1000 used drives/day sold on eBay.

Today there are three primary techniques for assuring data confidentiality.

- 1. Physical security.
- 2. Logical access controls. (operating system)
- 3. Cryptography (disk & link)

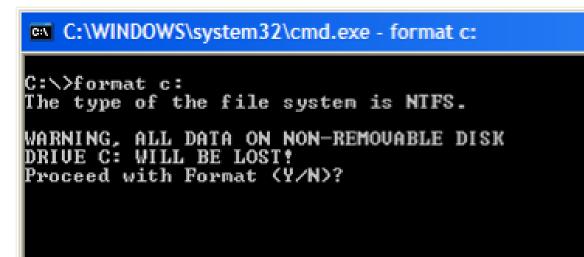
When a disk is thrown out or repurposed, most of these techniques don't work.

3. Cryptography (disk & link)

And most people don't encrypt their data.

#### More bad news.

FORMAT C: doesn't erase the hard drive.



FORMAT just writes a new root directory.

#### **DEL doesn't delete files**

C:\WINDOWS\system32\cmd.exe

C:\tmp>dir Volume in drive C has no label. Volume Serial Number is 1410-FC4A Directory of C:\tmp 10/15/2004 09:20 PM <DIR> 09:20 PM <DIR> 10/15/2004 10/03/2004 11:34 AM 27,262,976 big\_secret.txt 1 File(s) 27,262,976 bytes 2 Dir(s) 4,202,078,208 bytes free C:\tmp>del big\_secret.txt C:∖tmp>dir Volume in drive C has no label. Volume Serial Number is 1410-FC4A Directory of C:\tmp 10/15/2004 09:22 PM <DIR> 09:22 PM 10/15/2004 <DIR> Ø File(s) 0 bytes 4,229,296,128 bytes free 2 Dir(s) C:\tmp>\_

#### **DEL simply removes the file's name from the directory.**

These failings are shared by all modern file systems.

- FAT12 DOS Floppy disks
- FAT16, FAT32 DOS, Windows, USB Drives
- NTFS Windows NT/XP/Longhorn
- UFS, FFS, EXT2/3 Unix
- HFS, HFS+ MacOS
- Novell

# Compressed and Encrypted file systems complicate recovery of data.

# A typical hard disk

#### Factory-Fresh Hard disk: All Blank

0	0	0	0	0	0	0	
0	0	0	0	0	0	0	
0	0	0	0	0	0	0	
0	0	0	0	0	0	0	
0	0	0	0	0	0	0	

Each block is 512 bytes

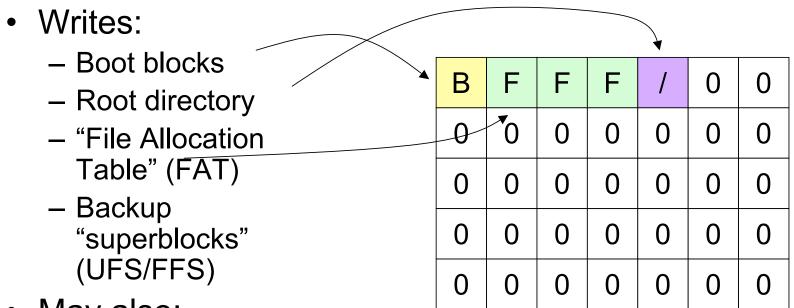
A 20G disk has 40M blocks.

Disk blocks (not to scale)

### "All Blank"

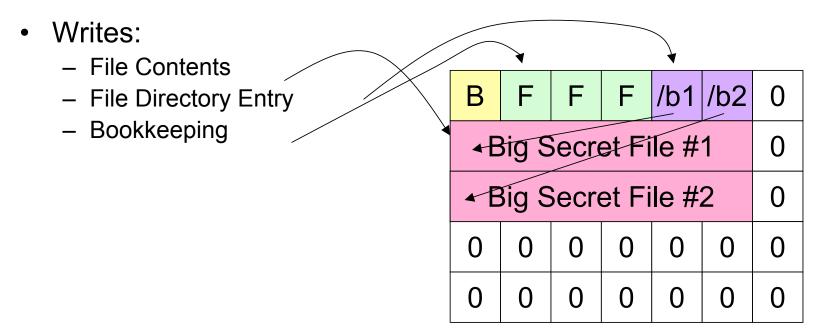
#### Each block has 512 ASCII NULs:

### % format C:\*



- May also:
  - Validate surface
- \* Examples based on FAT32 running under Unix

# % cp bfs1 /mnt/b1 % cp bfs2 /mnt/b2



• root directory:

b1\_\_\_\_\_ jan 1 2004 block 7 b2 . jan 1 2004 block 14

# % rm /mnt/b1 % rm /mnt/b2

• Writes:	oot directory							
– Bookke		В	F	F	F	/?1	/?2	0
		E	Big S	Secr	et Fi	le #	1	0
		E	Big S	Secr	et Fi	le #	2	0
		0	0	0	0	0	0	0
• new root	directory:	0	0	0	0	0	0	0

new root directory.

21			1	2004	block	7
• -	•	) um	-	2001	DIOCK	,
?2	٠	jan	1	2004	block	14

# % cp Madonna.mp3 /mnt/mp3

<ul> <li>Writes:</li> <li>– New root directory</li> </ul>		•					
– madonna.mp3	В	F	F	F	/mp3	/?2	0
<ul> <li>Bookkeeping</li> </ul>	Ma	don	ina	et Fi	le #	1	0
	< E	Big S	Secr	et Fi	le #2	2	0
	0	0	0	0	0	0	0
new root directory:	0	0	0	0	0	0	0

Madonna	.mp3	jan	2	2004	block	7
?2	•	jan	1	2004	block	14

# What's on the disk?

- Madonna.mp3
- Madonna.mp3's directory entry
- All of B2
- Most of B2's directory entry

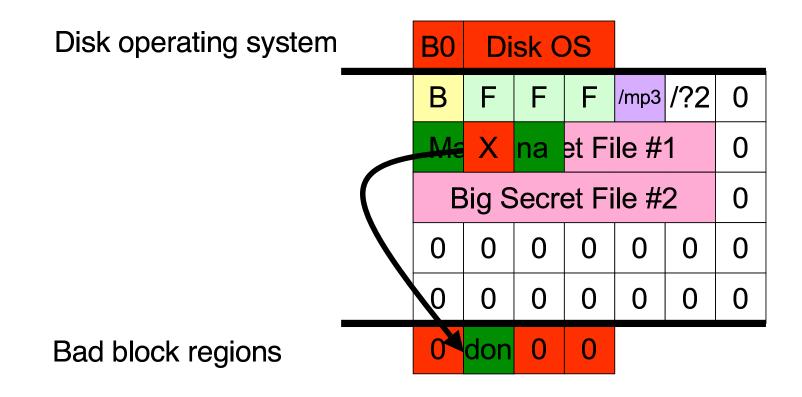
В	F	F	F	/mp3	/?2	0
Ma	Madonna et File #1				0	
E	Big Secret File #2				0	
0	0	0	0	0	0	0
0	0	0	0	0	0	0

• Part of B1

# Taxonomy of hard disk data

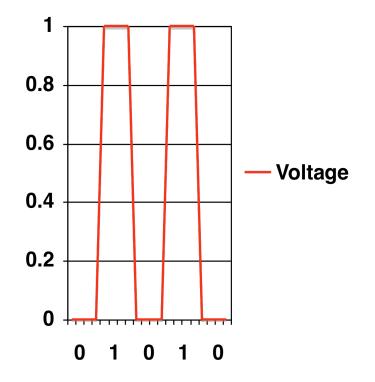
Level 0	Files in file system
Level 1	Temp files (/tmp, /windows/tmp, etc)
Level 2	Recoverable deleted files
Level 3	Partially over-written files
Level 4	Data accessible by vendor commands
Level 5	Overwritten data

### Level 4 Data: Vendor Area



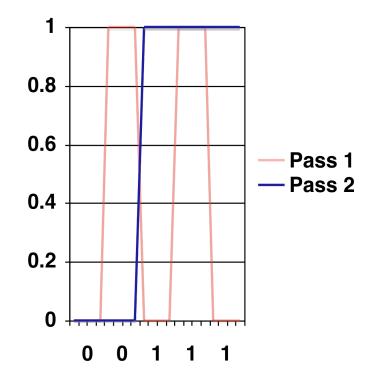
### Level 5: Overwritten Data

 Disk Drives are analog devices



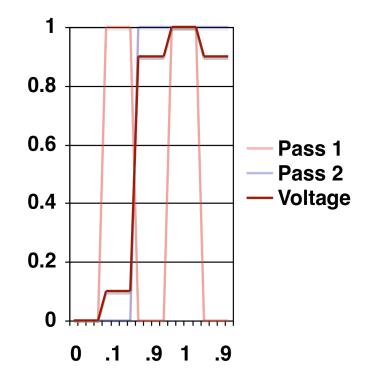
### Level 5: Overwritten Data

- Disk Drives are analog devices
- Overwritten data doesn't just die...



### Level 5: Overwritten Data

- Disk Drives are analog devices
- Overwritten data doesn't just die...
- Read data should be a function of all previous data values...



# Level 5: What to do?

- DOD 5220.22-M
  - "Degauss with a Type I degausser"
  - "Degauss with a Type II degausser"
  - "Overwrite all locations with a character, it's complement, then a random character and verify"
  - Destroy, Disintegrate, incinerate, pulverize, shred, or melt

# Type 1 Degausser

<u>....</u>

- Model HD-2000
- 73 seconds cycle time
- 260 lbs
- \$13,995
- Monthly rental \$1,400
- Note:
  - Your hard disk won't work after it's been degaussed (why not?)

#### http://www.datadev.com/v90.htm

-

# **Drive Slagging**

 Melting down the drives works just fine



http://driveslag.eecue.com/

# Drive Slagging Cont...





# **Drive Slagging**

### • "Good luck removing data from this."





#### Punching a hole also works.



#### The bad news: Most people aren't using these techniques.

#### **Purchased used from a computer store in August 1998:**



### Computer #1: 486-class machine with 32MB of RAM

A law firm's file server...

...with client documents!

Computers #2 through #10 had:

- Mental health records
- Home finances
- Draft of a novel...

#### Was this a chance accident or common occurrence?



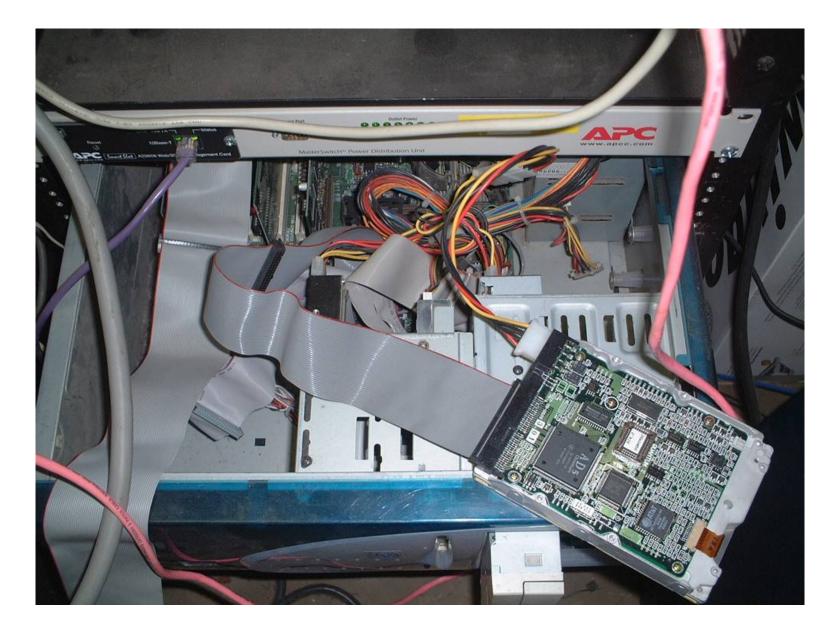
### Between January 1999 and April 2002, I acquired 236 hard drives on the secondary market.



# **Drives arrived by UPS**



#### Data on drives "imaged" using FreeBSD



dd if=/dev/ad0 of=file.img bs=65536 conv=noerror,sync

## **Images stored on a RAID**



# For every drive, I cataloged:

- Disk SN, date of manufacture, etc.
- Every readable sector on the drive..
- All visible files.
- MD5 of every file.
- MD5 of the image.



## Example: Disk #70: IBM-DALA-3540/81B70E32

Purchased for \$5 from a Mass retail store on eBay Copied the data off: 541MB

Initial analysis:

Total disk sectors:	1,057,392
Total non-zero sectors:	989,514
Total files:	3

The files:

drwxrwxrwx	0 root	0 Dec 31	1979 ./
-r-xr-xr-x	0 root	222390 May 11	1998 IO.SYS
-r-xr-xr-x	0 root	9 May 11	1998 MSDOS.SYS
-rwxrwxrwx	0 root	93880 May 11	1998 COMMAND.COM

## Clearly, this disk had been FORMATed...

C:\WINDOWS\system32\cmd.exe - format c:

C:\>format c: The type of the file system is NTFS.

WARNING, ALL DATA ON NON-REMOUABLE DISK DRIVE C: WILL BE LOST! Proceed with Format (Y/N)?

## Windows FORMAT doesn't erase the disk... FORMAT just writes a new root directory.

#### UNIX "strings" reveals the disk's previous contents...

Insert diskette for drive and press any key when ready Your program caused a divide overflow error. If the problem persists, contact your program vendor. Windows has disabled direct disk access to protect your lo To override this protection, see the LOCK /? command for m The system has been halted. Press Ctrl+Alt+Del to restart You started your computer with a version of MS-DOS incompa version of Windows. Insert a Startup diskette matching thi

OEMString = "NCR 14 inch Analog Color Display Enchanced SV Graphics Mode: 640 x 480 at 72Hz vertical refresh. XResolution = 640 YResolution = 480 VerticalRefresh = 72

## 70.img con't...

ling the Trial Edition

IBM AntiVirus Trial Edition is a full-function but time-li evaluation version of the IBM AntiVirus Desktop Edition pr may have received the Trial Edition on a promotional CD-RC single-file installation program over a network. The Tria is available in seven national languages, and each languag provided on a separate CC-ROM or as a separa EAS.STCm

EET.STC

ELR.STCq

ELS.STC

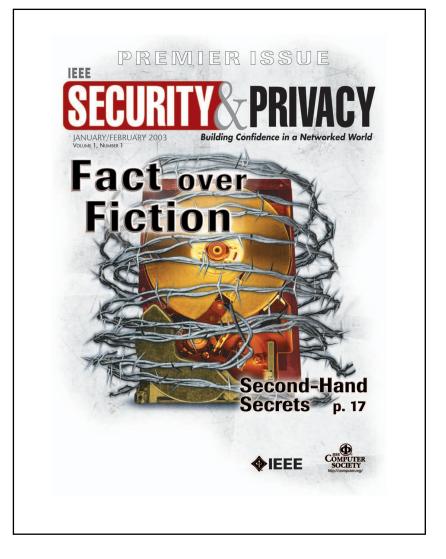
# 70.img con't...

MAB-DEDUCTIBLE MAB-MOOP MAB-MOOP-DED **METHIMAZOLE** INSULIN (HUMAN) COUMARIN ANTICOAGULANTS CARBAMATE DERIVATIVES AMANTADINE MANNITOL MAPROTILINE CARBAMAZEPINE CHLORPHENESIN CARBAMATE ETHINAMATE FORMALDEHYDE MAFENIDE ACETATE

# [Garfinkel & Shelat 03] established the scale of the problem.

We found:

- Thousands of credit card numbers (many disks)
- Financial records
- Medical information
- Trade secrets
- Highly personal information



## We did not determine why the data had been left behind.

# There are roughly a dozen documented cases of people purchasing old PCs and finding sensitive data.

- A woman in Pahrump, NV bought a used PC with pharmacy records [Markoff 97]
- Pennsylvania sold PCs with "thousands of files" on state employees [Villano 02]
- Paul McCartney's bank records sold by his bank [Leyden 04]
- O&O Software GmbH 200 drives.





### Why don't we hear more stories?

- Hypothesis #1: Disclosure of "data passed" is exceedingly rare because most systems are properly cleared.
- Hypothesis #2: Disclosures are so common that they are not newsworthy.
- Hypothesis #3: Systems aren't properly cleared, but few people notice the data.

# I think that data left behind on hard drives is a serious social problem.

Large numbers of drives are being sold and given away.

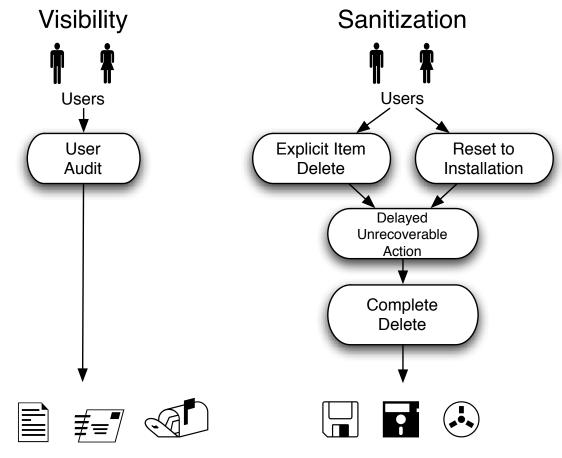
Many of them appear to have hidden confidential information.





## We are morally obligated to solve this problem!

# [Garfinkel '05] presents five distinct patterns for addressing the sanitization problem



Document Files, Applications, and Media

http://www.simson.net/thesis/

# To be effective, a solution must address the root cause

#### Usability Problem:

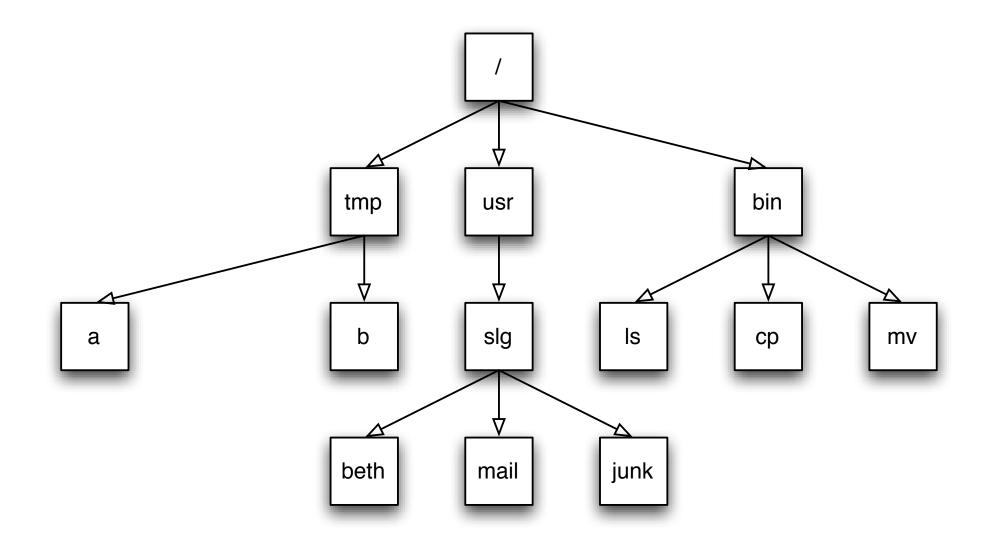
- Effective audit of information present on drives.
- Make DEL and FORMAT actually remove data. [Bauer & Priyantha 01]
- Provide alternative strategies for data recovery.

## Education Problem:

- Add training to the interface. [Whitten 04]
- Regulatory requirements. [FTC 05, SEC 05]
- Legal liability.

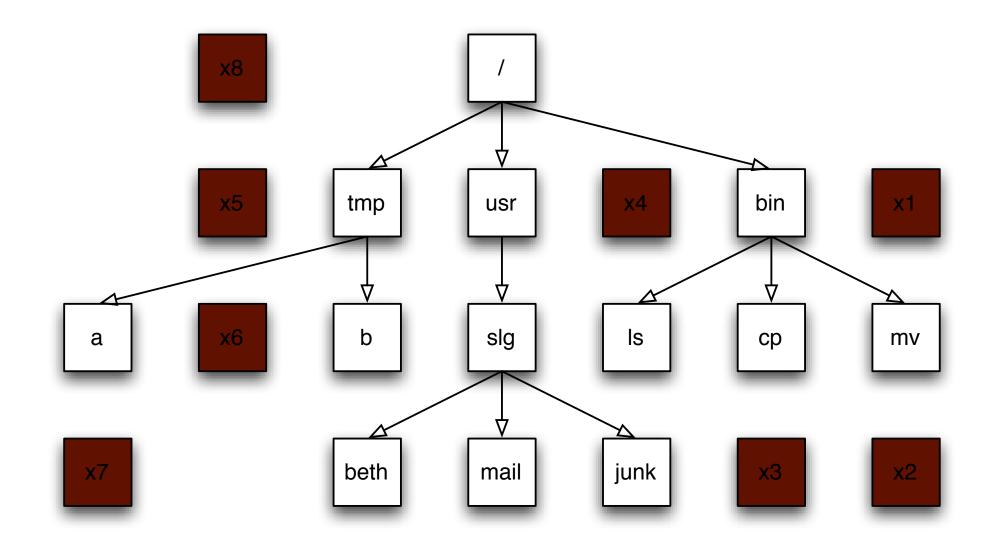
## To find that cause, I looked on the drives and contacted the data subjects.

## Data on a hard drive is arranged in sectors.



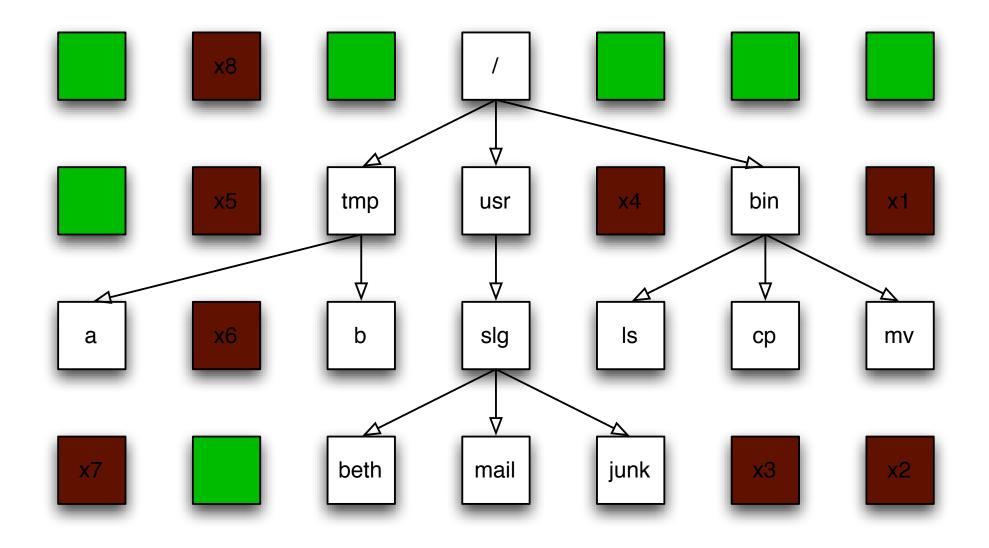
The white sectors indicate directories and files that are visible to the user.

## Data on a hard drive is arranged in sectors.



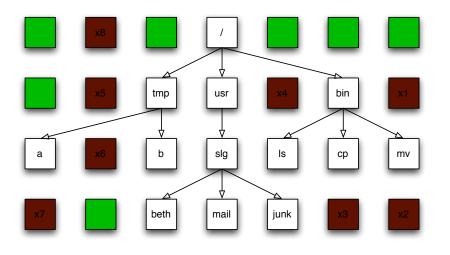
#### The brown sectors indicate files that were deleted.

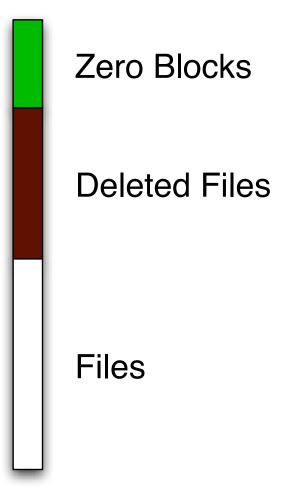
## Data on a hard drive is arranged in sectors.



The green sectors indicate sectors that were never used (or that were wiped clean).

#### Stack the disk sectors:





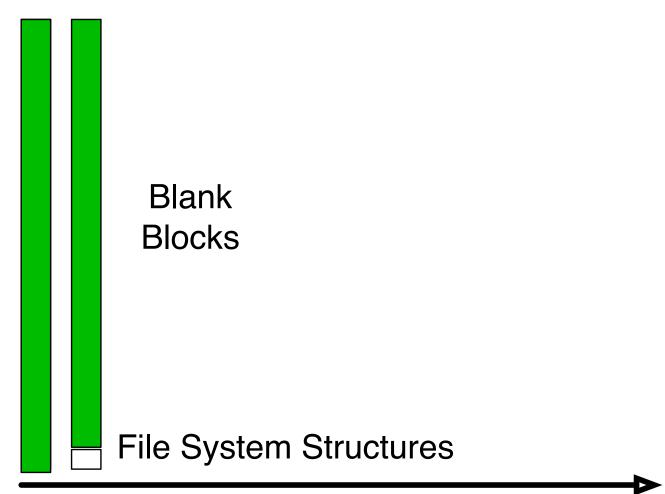
•

## **NO DATA: The disk is factory fresh.**

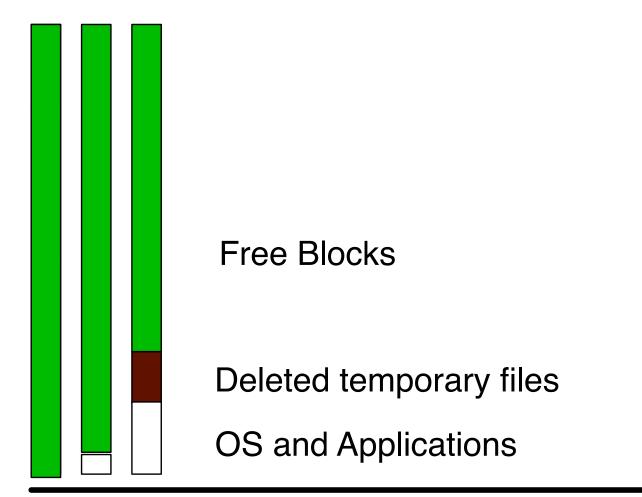
All Blocks are Zero

.

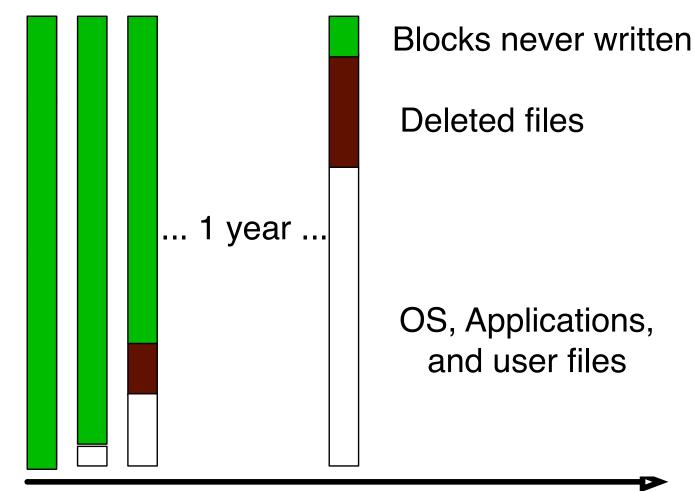
# FORMATTED: The disk has an empty file system



# **AFTER OS INSTALL: Temp. files have been deleted**

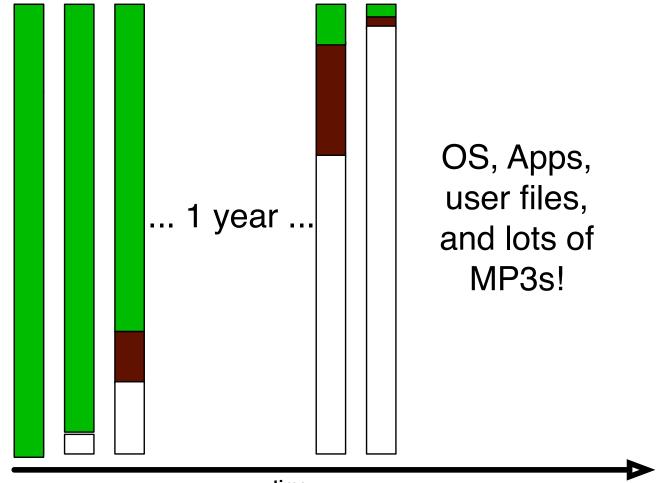


# **AFTER A YEAR OF SERVICE**

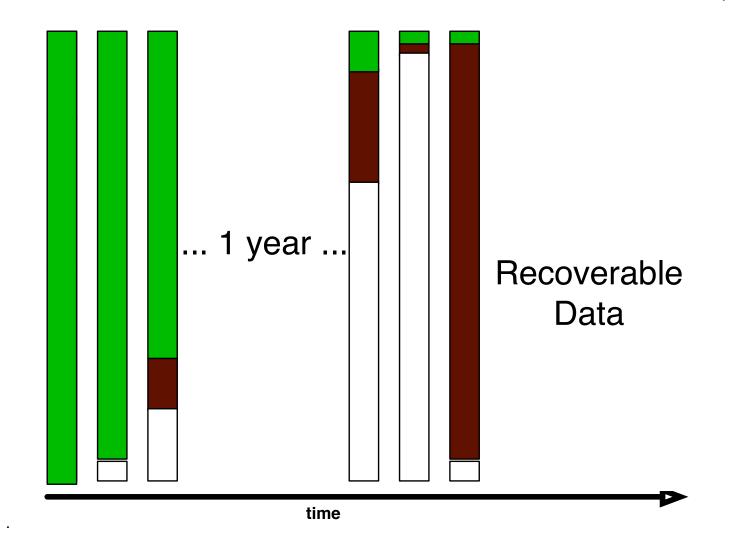


# **DISK NEARLY FULL!**

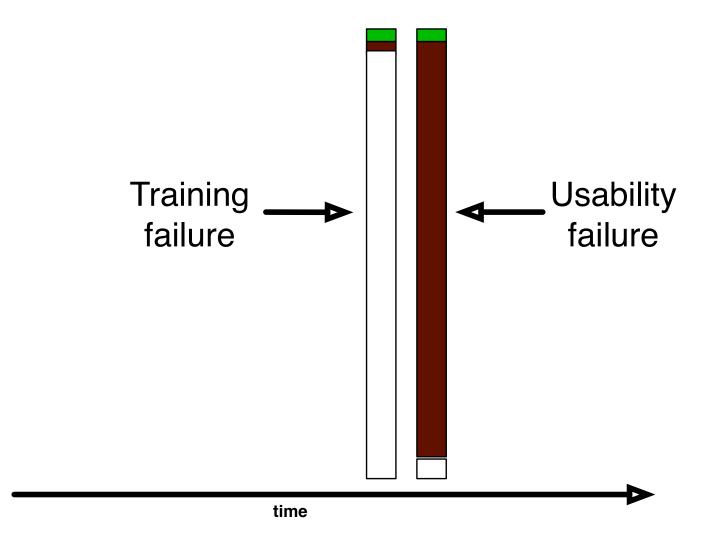
.



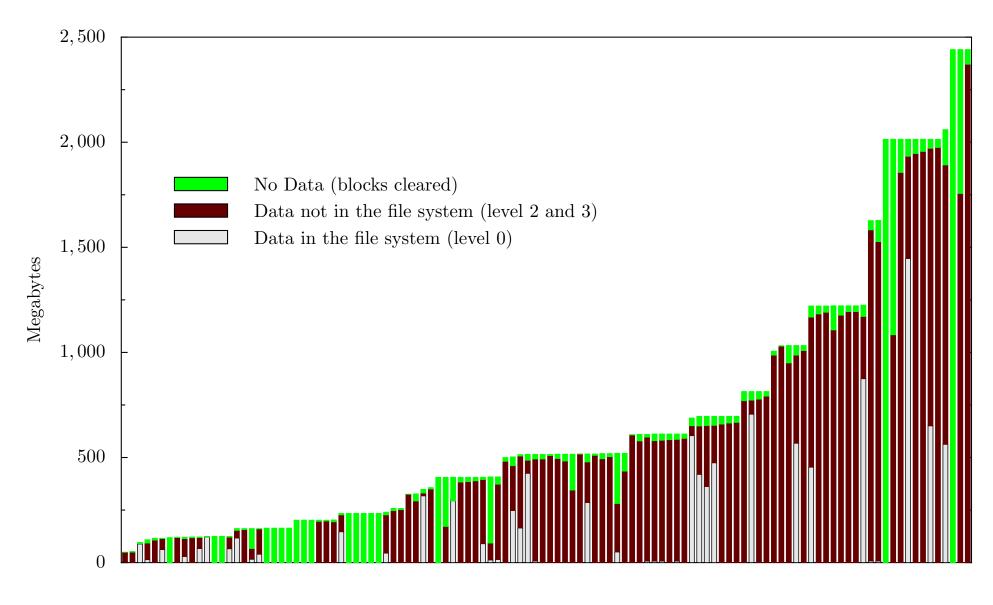
# FORMAT C:\ (to sell the computer.)



#### We can use forensics to reconstruct motivations:



## The drives are dominated by failed sanitization attempts...



..but training failures are also important.

## **Overall numbers**

Drives Acquired:	236
Drives DOA:	60
Drives Images:	176
Drives Zeroed:	11
Drives "Clean Formatted:"	22
Total files:	168,459
Total data:	125G

## Only 33 out of 176 working drives were properly cleared!

- 1 from Driveguys but 2 others had lots of data.
- 18 from pcjunkyard but 7 others had data.
- 1 from a VA reseller 1 DOA; 3 dirty formats.
- 1 from an unknown source 1 DOA, 1 dirty format.
- 1 from Mr. M. who sold his 2GB drive on eBay.

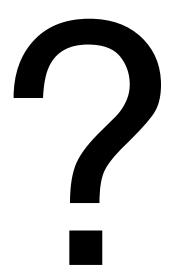
# MD5 hashing allows the identification of files.

Interestingly, few unique files that had not been deleted:

File type	Unique Files
Microsoft Word files:	783
Microsoft Excel files:	184
Microsoft PowerPoint files:	30
Outlook PST files:	11
audio files:	977

Conclusion: *most users* DELeted their files before discarding their drives.

## But what *really* happened?



#### I needed to contact the original drive owners.

# The *Remembrance of Data Passed Traceback Study.* [Garfinkel 05]

- 1. Find data on hard drive
- 2. Determine the owner
- 3. Get contact information for organization
- 4. Find the right person *inside* the organization
- 5. Set up interviews
- 6. Follow guidelines for human subjects work

06/19/1999 /:dir216/Four H Resume.doc
03/31/1999 /:dir216/U.M. Markets & Society.doc
08/27/1999 /:dir270/Resume-Deb.doc
03/31/1999 /:dir270/Deb-Marymount Letter.doc
03/31/1999 /:dir270/Links App. Ltrdoc
08/27/1999 /:dir270/Resume=Marymount Udoc
03/31/1999 /:dir270/NCR App. Ltrdoc
03/31/1999 /:dir270/Admissions counselor, NCR.doc
08/27/1999 /:dir270/Resume, Deb.doc
03/31/1999 /:dir270/UMUC App. Ltrdoc
03/31/1999 /:dir270/Ed. Coordinator Ltrdoc
03/31/1999 /:dir270/American Collegedoc
04/01/1999 /:dir270/Am. U. Admin. Dirdoc
04/05/1999 /:dir270/IR Unknown Lab.doc
04/06/1999 /:dir270/Admit Slip for Modernism.doc
04/07/1999 /:dir270/Your Honor.doc

#### This was a lot harder than I thought it would be.

# Ultimately, I contacted 20 organizations between April 2003 and April 2005.



## The leading cause: betrayed trust.

## Trust Failure: 5 cases

- ✓ Home computer; woman's son took to "PC Recycle"
- Community college; no procedures in place
- Church in South Dakota; administrator "kind of crazy"
- Auto dealership; consultant sold drives he "upgraded"
- ✓ Home computer, financial records; same consultant

This specific failure wasn't considered in [GS 03]; it was the most common failure.

## Second leading cause: Poor training and supervision

Trust Failure: 5 cases

Lack of Training: 3 cases

- California electronic manufacturer
- Supermarket credit-card processing terminal
- ✓ ATM machine from a Chicago bank

Alignment between the interface and the underlying representation would overcome this problem.

#### Sometimes the data custodians just don't care.

Trust Failure: 5 cases Lack of Training: 3 cases

Lack of Concern: 2 cases

- Bankrupt Internet software developer
- ✓ Layoffs at a computer magazine

**Regulation on resellers might have prevented these cases.** 

#### In seven cases, no cause could be determined.

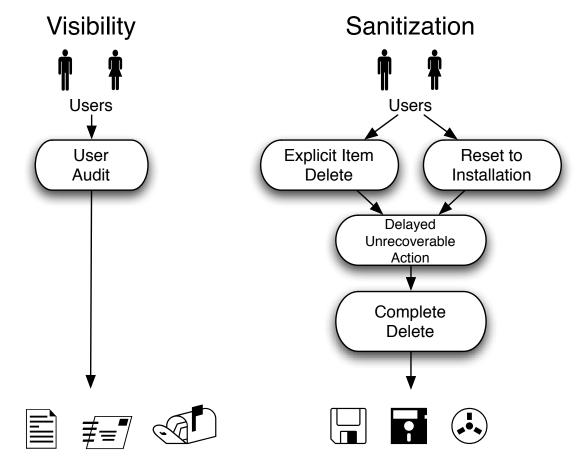
Trust Failure: 5 cases Lack of Training: 3 cases Lack of Concern: 2 cases

#### Unknown Reason: 7 cases

- ✗ Bankrupt biotech startup
- X Another major electronics manufacturer
- **X** Primary school principal's office
- ✗ Mail order pharmacy
- ✗ Major telecommunications provider
- X Minnesota food company
- **X** State Corporation Commission

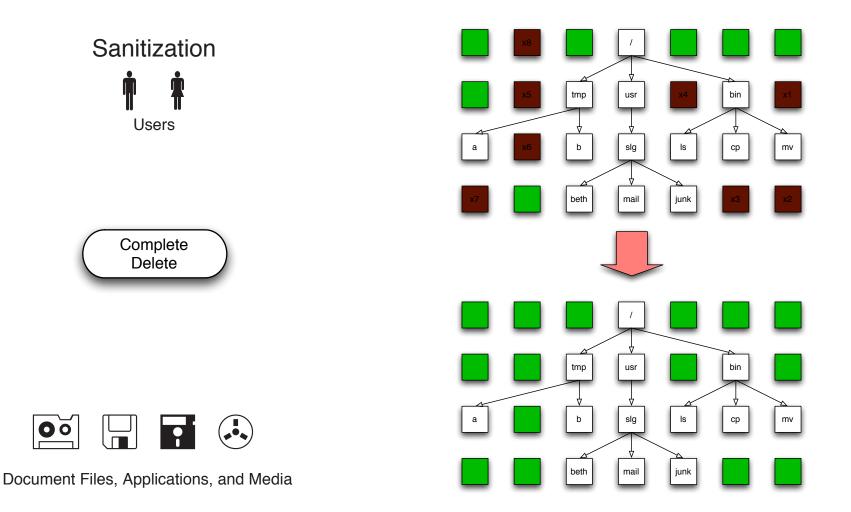
## **Regulation might have helped here, too.**

# I have identified five distinct patterns for addressing the sanitization problem.



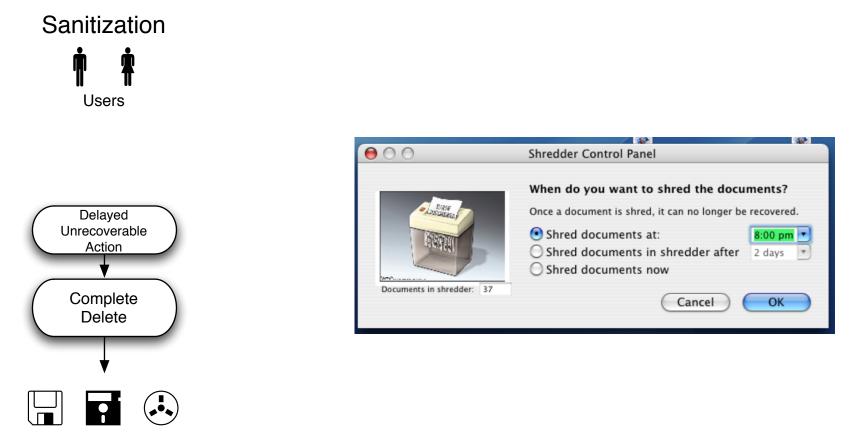
Document Files, Applications, and Media

*Complete Delete*: assure that deleting the *visible* representation deletes the *hidden* data as well.



# Naming this pattern lets us discuss its absence in modern operating systems.

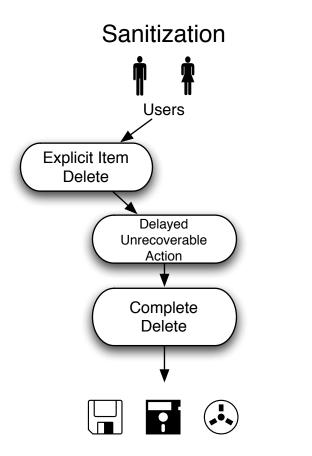
# **Delayed Unrecoverable Action:** give the users a chance to change their minds.



Document Files, Applications, and Media

# [Norman 83] and [Cooper 99] both suggest this functionality, but they do not name or integrate it.

### Two ways to delete information. #1: Explicit Item Delete

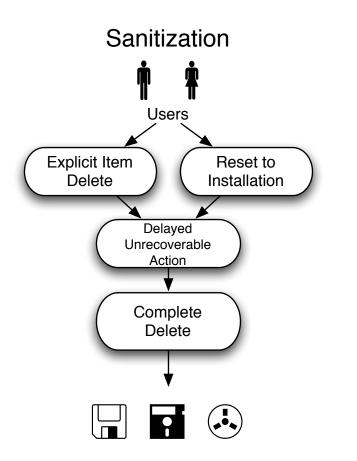


C:\WINDOWS\system32\cmd.exe
C:\tmp>dir Volume in drive C has no label. Volume Serial Number is 1410-FC4A
Directory of C:\tmp
10/15/2004 09:20 PM <dir> 10/15/2004 09:20 PM <dir> 10/03/2004 11:34 AM 27,262,976 big_secret.txt 1 File(s) 27,262,976 bytes 2 Dir(s) 4,202,078,208 bytes free</dir></dir>
C:\tmp>del big_secret.txt
C:\tmp>dir Volume in drive C has no label. Volume Serial Number is 1410-FC4A
Directory of C:\tmp
10/15/2004 09:22 PM <dir> 10/15/2004 09:22 PM <dir> 0 File(s) 0 bytes 2 Dir(s) 4,229,296,128 bytes free</dir></dir>
C:\tmp>_

Document Files, Applications, and Media

# "Provide a means for deleting information where the information is displayed."

### Reset to Installation: Get rid of everything



C:\WINDOWS\system32\cmd.exe - format c:

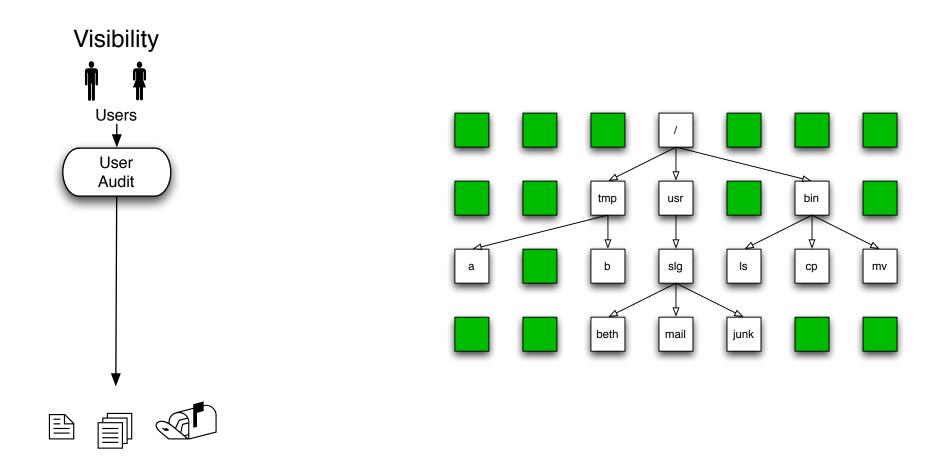
C:\>format c: The type of the file system is NTFS.

WARNING, ALL DATA ON NON-REMOUABLE DISK DRIVE C: WILL BE LOST! Proceed with Format (Y/N)?

Document Files, Applications, and Media

Reset/reinstall functionality is common (Windows; PalmOS; etc.). This pattern framework clarifies *Reset's* security property.

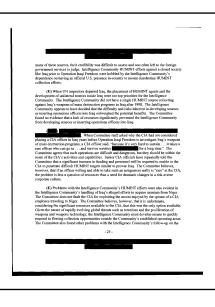
## User Audit: If the information is present, make it visible.



With files, this happens automatically when the *Complete Delete* pattern is implemented.

# The power of these patterns is that they apply equally well to other sanitization problems.

#### Document Files



• Web Browsers

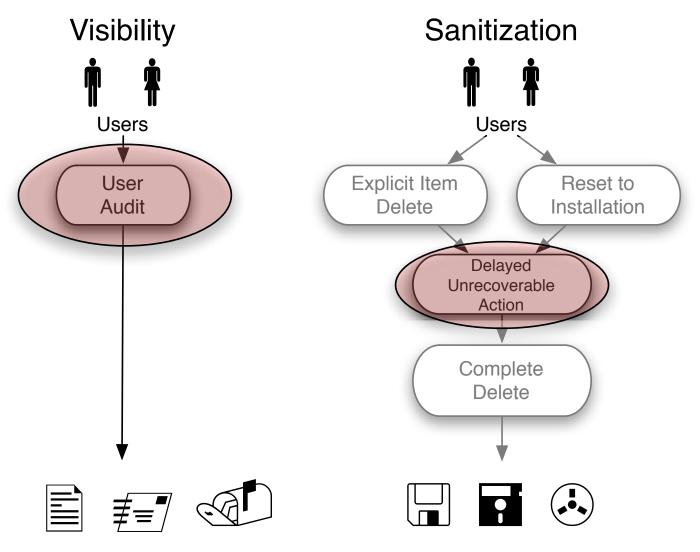
Congle Search Web C Debted C Autori C Debtes C C Congle C C C C C C C C C C C C C C C C C C C	2				
File       Edit       Wow       Favorites       Tools Help         Addes	<sup>tec</sup> 🗿 MIT WebMail - Microsoft Internet	Explorer - [Working Offline]		- 🗆 🖂	
Image:	File Edit View Favorites Tools H	felp		<b></b>	
Congle	🧯 😋 Back 🝷 🐑 🔺 📓 🏠	🔎 Search 🤺 Favorites 🚱 🔗 -	🎍 🗷 • 🔜 🏭 🦓		
MIT WebMail       41.18       More         An email service form Information Bervices & Technology       53.58       None         1NBOX       Empty Trash       Compose       Folders       Search       Directory       Heb       Logout       Open Folder         1NBOX       Empty Trash       Compose       Folders       Search       Directory       Heb       Logout       Open Folder         1NBOX       Empty Trash       Compose       Folders       Search       Directory       Heb       Logout       Open Folder         1718       None       20.88       None       20.88       None       20.88       None         1718       None       Expand All (Collapse All #       Image: All # All All (Collapse All #       Image: All # All All (Collapse Scientific Scient       None	Ex Address 🚵 https://webmail.mit.edu/horde)			Links »	ogle • 🛛 💙
An email switce from Information Barrylees & Technology Network Barrylees & Technology Network Barrylees & Technology Network Barrylees & Technology Expand All Collapse All #  Student House Fielder Navigation Fielder Navigati	Google -	防 Search Web 🔹 🐗 🔁 O blocked 🔚	AutoFil 🏾 Notions 🥒		Size Expires 🔥
An email service from Information Services & Technology       Boild Services (Services)         An email service from Information Services & Technology       Boild Services (Services)         INBOX       Empty Trash       Compose Poliders         Mailbor quotes: 175 8MB Used/244 14MB Tobal (72.02%)       Folder         Folder Navigator       Imailbor quotes: 175 8MB Used/244 14MB Tobal (72.02%)         Folder Navigator       Imailbor quotes: 175 8MB Used/244 14MB Tobal (72.02%)         Folder Navigator       Imailbor quotes: 175 8MB Used/244 14MB Tobal (72.02%)         Folder Navigator       Imailbor quotes: 175 8MB Used/244 14MB Tobal (72.02%)         Folder Navigator       Imailbor quotes: 175 8MB Used/244 14MB Tobal (72.02%)         Folder Navigator       Imailbor quotes: 175 8MB Used/244 14MB Tobal (72.02%)         Folder Navigator       Imailbor quotes: 175 8MB Used/244 14MB Tobal (72.02%)         Imailbor quotes: 175 8MB Used/244 14MB Tobal (72.02%)       Imailbor guotes: 185 8MB Used/244 14MB Tobal (72.02%)         Imailbor quotes: 175 8MB Used/244 14MB Tobal (72.02%)       Imailbor guotes: 185 8MB Used/244 14MB Tobal (72.02%)         Imailbor quotes: 175 8MB Used/244 14MB Tobal (72.02%)       Imailbor guotes: 185 8MB Used/244 14MB Tobal (72.02%)         Imailbor quotes: 175 8MB Used/244 14MB Tobal (72.02%)       Imailbor guotes: 185 8MB Used/244 14MB Tobal (72.02%)         Imailbor quotes: 175 8MB Used/244 14MB Tobal (72.02%)       Imailbor	MIT WebMail				
INBOX       Empty Trash       Compose       Folders       Options       Search       Directory       Help       Logout       Open Folder         INBOX       Mailbox quota: 175 84MB Used / 244 14MB Total (72.02%)       Folder       Nave       178       Mne         Folder       Navigator       Choose Action:       Image: Choose Ac		on Services & Technology			
INBOX       Empty Trash       Compose       Folders       Options       Search       Directory       Help       Logout       Oppin Folder       1758       Nee         Mailbox quots       175       S4MB       Used/244.14MB       Total (72.02%)       Folder       1758       Nee         Folder       Navigator       Image: Search       Expand All Collapse All       Image: Search       2018       Nee         Choose Action:       Image: Search       Image: Search       Image: Search       Image: Search       2018       Nee         Image: Search       Image: Search       Image: Search       Image: Search       Image: Search       2018       Nee         Image: Search       Image: Search       Image: Search       Image: Search       Image: Search       2018       Nee         Image: Search       Image: Search       Image: Search       Image: Search       Image: Search       2018       Nee       2018       Nee       2018       Nee       2018       Nee       2018       Nee       2018       3018       Nee       2018       3018       3018       Nee       2018       3018       3018       3018       Nee       2018       3018       3018       3018       3018       3018       3018 <th></th> <th>an bervices a reenhology</th> <th></th> <th></th> <th></th>		an bervices a reenhology			
TNBOX       Empty Trash       Compose       Folders       Search       Directory       Help       Logout       Open Folder         Malloor quote       1758       Here       State       Help       Logout       Open Folder         Folder       Navigator       State       Expand All Collapse All       III       III       Here         Choose Action:       III       Expand All Collapse All       III       IIII       Here         IIII       Here       State       IIIIIII       Here       State       Here         IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	4 🕅 🗰	<b>2</b> 22 0 0	2 🖪 📥		
Mailbor quota. 17.5.84MB Used / 244.14MB Total (72.02%)       17.58         Folder Navigator **       **         Choose Action: **       **         Expand All Collapse All #       **         **       ** <th>INBOX Empty Trach Compos</th> <th>e Folders Options Search Directo</th> <th></th> <th>lder</th> <th></th>	INBOX Empty Trach Compos	e Folders Options Search Directo		lder	
Mailton quota 175.84MB Used / 244 14MB Total (72.02%)       244 14MB Total (72.02%)         Folder Navigator **       **         Choose Action: **       **         Expand All Collapse All #*       355 8         Home       356 None         State Navigator **       **         **       **	8				
Folder Navigator       0       Expand All Collapse All # C         Choose Action: <ul> <li></li></ul>					
Chose Action: <ul> <li>Expand All Collapse All #</li> <li>Chose Action:</li> <li>Chose Action:</li></ul>		box quota: 175.84MB Used / 244.14MB Total (	72.02%)		
Image: Section in the sectio	Folder Navigator 🌳 📃				35 KB None 🔤
Image: State of the sent set o	Chaose Action:		Evnand All I Collanse All		26 KB 4/24/2005 5:58
Image: Section of the section of t		8	Expand Air Conspire Air		4 KB 4/24/2005 4:58
□       Image: Section 1       Image: Sectio			1367	0	
Image: State of the sent set of the set of the sent set of the set of the sent set of the sen					
Image: Constraint of the sector of the se					
Image: Standard House       12 to None         Image: Standard House       Image: Standard House					
Image: State of All Mode Scale       33 48       4/AlMODE Scale         Image: State of All Mode Scale       35 48       4/AlMODE Scale         Image: State of All Mode Scale       35 48       4/AlMODE Scale         Image: State of All Mode Scale       35 48       4/AlMODE Scale         Image: State of All Mode Scale       35 48       4/AlMODE Scale         Image: State of All Mode Scale       35 48       4/AlMODE Scale         Image: State of All Mode Scale       35 48       4/AlMODE Scale         Image: State of All Mode Scale       35 48       4/AlMODE Scale         Image: State of All Mode Scale       35 48       4/AlMODE Scale         Image: State of All Mode Scale       35 48       4/AlMODE Scale         Image: State of All Mode Scale       35 48       4/AlMODE Scale         Image: State of All Mode Scale       35 48       4/AlMODE Scale         Image: State of All Mode Scale       35 48       4/AlMODE Scale         Image: State of All Mode Scale       35 48       4/AlMODE Scale         Image: State of All Mode Scale       35 48       4/AlMODE Scale         Image: State of All Mode Scale       35 48       4/AlMODE Scale         Image: State of All Mode Scale       35 48       4/AlMODE Scale         Image: State of All Mode Scale       <					
Image: Student House       2719       451/0005       231         Image: Student House       2719       451/0005       231         Image: Image: Student House       2719       451/0005       231         Image: Im					
Image: Student House       3k B 4/k70005 521					
Student House Student House Studen	🗖 🗖 🖓 sent				
Image: State of the state o	Ctudent House				
Image: State of the state o	1				
Image: Second all tash     17.18 Name       Image: Second all tash     Image: Second all tash	Ultimate				35 KB 4/24/2005 5:21
Image: Second and and and an analysis       Image: Second and and an analysis       Image: Second an analysis       Image: Se					
Choose Action:					
R B B D Internet	Work				<b>&gt;</b>
	Choose Action:	2	Expand All   Collapse All #		
				<b>▼</b>	
y Starit 🔰 🗿 MIT WebMai - Micros 🍙 Temporary Internet F 👌 libi - Paint 🖉 😨 🔏 💓 📢 🕲	ê)	5	💈 🤮 👔 Internet		
	start	🛅 Temporary Internet F 🍟 lib1 - Paint	E CONTRACTOR OF THE OWNER		/ / 🐺 🔬 🏹 🗟 😣

### Information is left in document files.

- The *New York Times* published a **PDF file** containing the names of Iranians who helped with the 1953 coup. [Young 00]
- US DoJ published a **PDF file** "diversity report" containing embarrassing redacted information. [Poulsen 03]
- SCO gave a Microsoft Word file to journalists that revealed its Linux legal strategy. [Shankland 04]
- Multinational Force-Iraq report

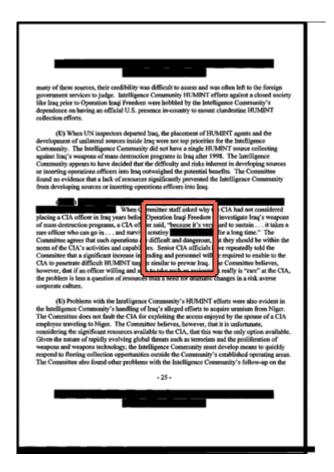
UNCLASSIFIED
UNCLASSIFIED
TABLE OF CONTENTS
L (U) BACKGROUND 1
A. (U) Administrative Matters 1
1. (U) Appointing Authority
B. (U) Constraints and Limitations 2
C. (U) Format of the Report
II. (U) ATMOSPHERICS
A. (U) Introduction
B. (U) Local Security Situation
1. (10) Frag
C. (U) Known Insurgent Tactics, Techniques, and Procedures 5
1. (U) Methods of Attack
D. (U) Recent Incidents in the Vicinity of Checkpoint 541
E. (U) Unit Experience in the Baghdad Area of Responsibility
1. (U)         Division         8           2. (U)         Brigade,         Division         9           3. (U)         Battalion         9           4. (U)         Battalion         10
F. (U) Findings
III. (U) TRAFFIC CONTROL POINTS, BLOCKING POSITIONS, AND TRAINING
i
UNCLASSIFIED

# The information leaked because two patterns were not implemented.



Document Files, Applications, and Media

The Senate Foreign Intelligence Committee accomplished this goal by *scanning* the redacted report on pre-war Iraq intelligence to create the PDF that it distributed.



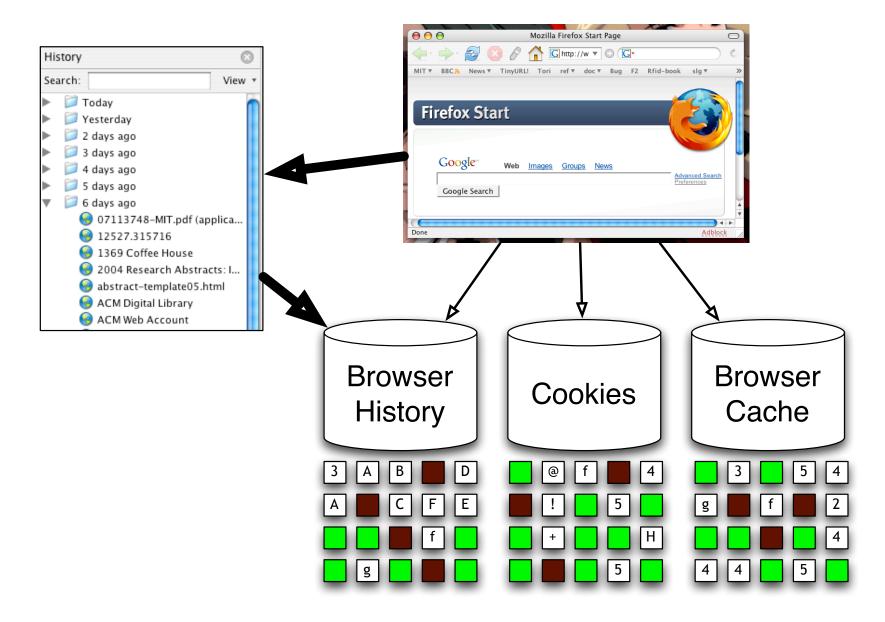
nittee staff asked v
eration Iraqi Freed
said, "because it's
rutiny
ifficult and danger
Senior CIA offic
ling and personnel
imilar to prewar Ir

# Microsoft has tried to solve this problem with "Remove Hidden Data" tool.

💐 Remove Hidden Data		
	our document without comments, revisions, file properties, or other u should only use this feature when you are ready to publish your	
Enter a file name for the new version 🗟 Ren	ove Hidden Data	
File name: Remo	ve Hidden Data is automatically checking for hidden data.	
Recommended: Use a different file na its original name. Chec	ing Done!	
	inish to close this document and display a log file of results.	
WAR data	IING: If you open this file f Rhd2.log - Notepad	×
	File Edit Format View Help V:\current\Blast_Notes.doc scanned at 8:35:21 PM on 3/5/2005 Personal summary information found and removed. Different revisions of document not found. Comments not found. Early document versions not found. VB Macro Comments failed to remove. Reason: If the "Trust Access to Visual Basic Project" security setting is SendForReview RCIDs not found. Printer path not found. V:\current\Blast_Notes.doc scanning completed	
		~
	Ln 1, Col 1	

RHD doesn't integrate into the flow of document preparation. The patterns-based analysis predicts that RHD will fail in many cases.

#### Information is left behind in web browsers.



# Two key problems: 1 Deleted files; 2 The cache

## In fact, a lot of information is left behind in web browsers.



Deck       Or product       Product Settings/Luck (Local Settings/Life=propring Internet Piles       Deck       Dig Copy       Size       Explore         Folder Tasks       Copy the Ren	
Folder Tasks     Type     Size     Expression       Copy the Izm     Expression     Expression     1111     Boundeder/Y     4118     None       Copy the Izm     Expression     Expression     1111     Boundeder/Y     4111     None     4118     None       Copy the Izm     Expression     Expression     1111     Boundeder/Y     4111     None     4118     None       Delete this Izm     Expression     Expression     1111     Doubleder/Y     11111     Doubleder/Y     11111     Doubleder/Y     11111     Doubleder/Y     11111     Doubleder/Y     11111     Doubleder/Y     11111     11111     11111     11111     11111     11111     11111     11111     11111     11111     11111     11111     11111     11111     11111     11111     111111	
Folder Tasks       2         Copy the Ren       3howFolder Yh         Delete this Ren       3howFolder Yh         Diver Hares       3howFolder Yh         Other Places       3howFolder Yh         Diver Hares       3howFolder Yh	
Copy this item       Shourfolder thu:       http://us.f530.mail.ydoc.com/jm/Showfolder/thu-bibodr       HTML Document       6618       Nore         Dielete this item       Shourfolder thu:       http://us.f530.mail.ydoc.com/jm/Showfolder/thu-bibodr       HTML Document       5318       Nore         Dielete this item       Shourfolder thu:       http://us.f530.mail.ydoc.com/jm/Showfolder/thu-bibodr       HTML Document       5318       Nore         Dielete this item       Shourfolder thu:       http://uw.medocidstre.com/book/SearchResults.apptc       HTML Document       1718       Nore         Dielete this item       Shourfolder thu:       http://uw.medocidstre.com/book/SearchResults.apptc       HTML Document       1718       Nore         My Documents       SearchResults       http://uw.medocidstre.com/book/SearchResults.apptc       HTML Document       1718       Nore         Signorf docr thu:       http://uw.medocidstre.com/book/SearchResults.apptc       HTML Document       1718       Nore         Signorf docr thu:       http://uw.medocidstre.com/book/SearchResults.apptc       HTML Document       1718       Nore         Signorf docr thu:       http://uw.medocidstre.com/book/SearchResults.apptc       HTML Document       1518       Nore         Signorf docr thu:       http://uw.medocidocider.com/book/SearchResults.apptc       HTML Docum	
Composition     Compositent     Compositent     Compositent     Compositent     Composite	
Delete this item         Image: Stand St	
Cher Places       Composition       Thip://www.netdookstore.com/books/SearchResults.asp/tx       HTIL Document       17.80       None         Cher Places       Composition       Composition       Composition       17.80       None         Composition       My Documents       Composition       Composition       17.80       None         My Documents       Composition       Composition       Composition       17.80       None         My Network Roces       My Network Roces       Mathematics       Composition       17.80       None         My Network Roces       Mathematics       Composition       None       17.80       None         My Network Roces       Mathematics       Mathematics       None       17.80       None         Thip://www.netbookstore.com/books/Searcheauts.asp/tx       HTIL Document       24.80       None       47	
Other Places       SearchResults       http://www.medbookstore.com/books/SearchResults.apt/tz       HTML Document       17.8       None         Local Settings       My Documents       SearchResults       http://www.medbookstore.com/books/SearchResults.apt/tz       HTML Document       21/8       None         My Documents       PhotoLifeEds       http://www.medbookstore.com/books/SearchResults.apt/tz       HTML Document       21/8       None         My Network Places       PhotoLifeEds       http://www.medbookstore.com/books/Product/Beaks.apt/tz       HTML Document       21/8       None         My Network Places       PhotoLifeEds       http://www.medbookstore.com/photols/Product/Beaks.apt/tz       HTML Document       21/8       None         BoorGadery T-E       http://www.medbookstore.com/photols/Product/Beaks.apt/tz       HTML Document       26/8       None         BoorGadery T-E       http://www.medbocom/photocom/photols/Product/Beaks/phot/HTML Document	
Other Places       Image: SearchBeaults       http://www.medbookstore.com/books/SearchBeaults.apt7tc       HTML Document       12/8       None         Image: My Documents       Image: SearchBeaults       http://www.medbookstore.com/books/SearchBeaults.apt7tc       HTML Document       2/16       None         Image: My Documents       Image: SearchBeaults       Http://www.medbookstore.com/books/SearchBeaults.apt7tc       HTML Document       2/16       None         Image: My Documents       Image: SearchBeaults       Http://www.medbookstore.com/books/ProductDeals.apt7tc       HTML Document       2/16       None         Image: My Documents       Image: SearchBeaults       Http://www.medbookstore.com/books/ProductDeals.apt7tc       HTML Document       2/16       None         Image: My Documents       Image: SearchBeaults       Http://www.medbookstore.com/books/ProductDeals.apt7tc       HTML Document       2/16       None         Image: My Documents       Image: SearchBeaults       Http://www.medbookstore.com/books/ProductDeals.apt7tc       HTML Document       2/16       None         Image: My Documents       Image: SearchBeaults       Http://www.medbookstore.com/books/ProductDeals.apt7t       HTML Document       2/16       None         Image: My Documents       Image: My Document       Http://www.medbookstore.com/minitescaphrophytemy Document       2/16       None	
Local Settings     My Decuments     My Decuments     My Network Places     My Network     My Network Places     My Network	
W Documents       Bits://www.medicoksice.com/booksi/ProductDetails.esp?C       HTML Document       2918       None         W Notwork Paces       Bits://www.medicoksice.com/booksi/ProductDetails.esp?C       HTML Document       2918       None         W Notwork Paces       Bits://www.medicoksice.com/booksi/ProductDetails.esp?C       HTML Document       2918       None	
Image: State	
Wy Network Places <ul> <li>Mark Mark Places</li> <li>Mark Mark Places</li> <li>Mark Mark Mark Mark Mark Mark Mark Mark</li></ul>	
My Network Places         Phtp://mail.yaboo.com/jr.kip/ilog/i7.and=/gmla70dmfga         2514         4/24/2           Bogn?         http://u.s.f530.mail.yaboo.com/jr.wilog/i7.and=/gmla70dmfga         HTML Document         2418         4/24/2           Bogn?         http://u.s.f530.mail.yaboo.com/jr.wilog/i7.and=/gmla70dmfga         HTML Document         2618         None           Bogn?         http://u.s.f530.mail.yaboo.com/jr.Wilog/i7.and=/gmla70dmfga         HTML Document         3618         None           Brokones/YY=68.1         http://u.s.f530.mail.yaboo.com/jr.Wilog/i7.and=/gmla70dmfga         HTML Document         6418         M/264           Brokones/YY=68.1         http://u.s.f530.mail.yaboo.com/jrw/locomes/YY=6849         HTML Document         6418         M/264           Compose/YH=         http://u.s.f530.mail.yaboo.com/jrw/locomes/YY=6849         HTML Document         5418         None           Brokones/YH=         http://u.s.f530.mail.yaboo.com/jrw/locomes/YH=6849         HTML Document         5418         None           Brokones/YH=         http://u.s.f530.mail.yaboo.com/jrw/locomes/YH=6849         HTML Document         5418         None           Brokones/YH=         http://webmal.mt.edu/horde/jmp/maboo.pht/phramal.po         HTML Document         2548         4/2/2           Brokones.ppb?//webmal.mt.edu/horde/jmp/masboo.phtp?mas=2190         HTML	
Image: Program         http://liu.ftS30.mail.yaboo.com/ym/logn?.arad-qualo70drigd         HTML Document         418         4/24/2           Image: Program         http://liu.ftS30.mail.yaboo.com/ym/lio.org/m/mistoc/mc969478         HTML Document         4518         Home           Image: Program         http://liu.ftS30.mail.yaboo.com/ym/lio.org/m/instoc/mc969478         HTML Document         4618         Home           Image: Program         http://liu.ftS30.mail.yaboo.com/ym/liot.org/more304	05 5:58
Image: http:///withun.fs30.mail.yebo.com/m/webcne?YY=8315         HTML Document         381 Kone           Image: http://withun.staff         http://withun.staff         HTML Document         381 Kone           Image: http://withun.staff         http://withun.staff         HTML Document         581 Kone           Image: http://withun.staff         http://withun.staff         http://withun.staff         181 Kone           Image: http://withun.staff         http://withun.staff         181 Kone         181 Kone           Image: http://withun.staff         http://withun.staff         181 Kone         181 Kone           Image: http://withun.staff         http://withun.staff         181 Kone         181 Ko	
Androcompose? http://u.fr.530.mail.ychoo.com/ym/ShowForder?/v-=64972 HTML Document 6418 More Indtacompose? http://u.fr.530.mail.ychoo.com/ym/Capose?Yi=64972 HTML Document 6418 4/26/2 Compose?Yi= http://u.fr.530.mail.ychoo.com/ym/Capose?Yi=64972 HTML Document 2418 More Orgone?Yi= http://u.fr.530.mail.ychoo.com/ym/Capose?Yi=64972 HTML Document 2418 More Orgone?Yi= http://u.fr.530.mail.ychoo.com/ym/Capose?Yi=64972 HTML Document 2418 More Orgone?Yi=0.00000000000000000000000000000000000	
Impose?         Mitty://wr.fS30.mail.yebo.com/m/infratecompos?.c_Dol1         H110. Documert         6414         4/6/2           Impose?         Mitty://wr.fS30.mail.yebo.com/m/infratecompos?.c_Dol1         H110. Documert         6414         2418         H010.           Impose?         Mitty://wr.fS30.mail.yebo.com/m/infratecompos?.c_Dol1         H110. Documert         5418         H020.           Impose?         Mitty://wr.fS30.mail.yebo.com/m/infratecompos?.c_Dol1         H110. Documert         518         H020.           Impose?         Mitty://wr.fs30.mail.yebo.com/m/infratecompos?.c_Dol1         H110. Documert         518         H020.           Impose.         Mitty://wr.fs30.mail.yebo.cm/primabox-lp0.mabox.ip/primabox-lp0.mabox.ip/primabox-lp0.mabox.ip/primabox-lp0.mabox.ip/primabox-lp0.mabox.ip/primabox-lp0.mabox.ip/primabox-lp0.mabox.ip/primabox-lp0.mabox.ip/primabox-lp0.mabox.ip/prim/mabox.ip/prim/mabox.ip/primabox.ip/prim/mabox.ip/primabox.ip/pr	
Query http://web.mail.mit.edu/horde/imp/masbcz.php?masb49     HTML Document 2918 None     yrod=11143a     Http://web.mat.edu/stytopics/mail/ouery.html     HTML Document 2918 None     Yord=11143a     Http://web.mat.edu/stytopics/mail/ouery.html     HTML Document 2918 None     Yord=1143a     Http://web.mat.edu/stytopics/mail/ouery.html     HTML Document 2918 None     Yord=1143a     Html://webmail.mit.edu/horde/imp/masbcz.php?masb2     Html://webmail.mit.edu/horde/imp/masbcz.php?masb2     Html://webmail.mit.edu/horde/imp/masbcz.php?masb2     Html://webmail.mit.edu/horde/imp/masbcz.php?masb2     Html://hocument 2918 4/2/2     masbcx     Http://webmail.mit.edu/horde/imp/masbcz.php?masb2     Html:/hocument 2918     Yord=291     Html:/hocument 2918     Yord=291     Html:/hocument 2918     Yord=291     Html:/hocument 291     Yord=291     Html:/hocument 291     Yord=291     Html:/hocument 291     Yord=291     Html:/hocument 291     Yord=291     Yo	05 5:58
And Section 2014 11438 http://webmail.ne.edu/horde/ine/jas/bass.ph/socom/8123109 II HTIL Document 512 None 1218 Non	
Image: State	
Implicit         https://webmail.mit.edu/horder/imp/matbcox.php?matbbcox/mit.         331.8         4/24/2           Implicit         https://webmail.mit.edu/horder/imp/matbcox.php?mexmal_po         HTML Document         331.8         4/24/2           Implicit         https://webmail.mit.edu/horder/imp/matbcox.php?mexmal_po         HTML Document         351.8         4/24/2           Implicit         https://webmail.mit.edu/horder/imp/matbcox.php?nexmal_po         HTML Document         351.8         4/24/2           Implicit         https://webmail.mit.edu/horder/implications.php?nexmal_po         HTML Document         351.8         4/24/2           Implicit         https://webmail.mit.edu/horder/implications.php?nexm2/194         HTML Document         351.8         4/24/2           Implicit         https://webmail.mit.edu/horder/implications.php?start=S93         HTML Document         351.8         4/24/2           Implicit         https://webmail.mit.edu/horder/implications.php?start=S93         HTML Document         351.8         4/24/2           Implicit         https://webmail.mit.edu/horder/implications.php?start=S93         HTML Document         351.8         4/24/2           Implicit         https://webmail.mit.edu/horder/implications.sego.php?imications=20-192         HTML Document         351.8         4/24/2	
Iddars         https://webmal.mit.edu/horde/imp/ifolders.php         HTML Document         27 K8         4/24/2           Imalbox.php?m.         https://webmal.mit.edu/horde/imp/imalbox.php?memal_po.         HTML Document         36 K9         4/24/2           Imalbox.php?m.         https://webmal.mit.edu/horde/imp/imalbox.php?memal_po.         HTML Document         36 K9         4/24/2           Imalbox         https://webmal.mit.edu/horde/imp/imalbox.php?memal_po.         HTML Document         36 K9         4/24/2           Imalbox         https://webmal.mit.edu/horde/imp/imalbox.php?idart=S3         HTML Document         26 K9         4/24/2           Imalbox         https://webmal.mit.edu/horde/imp/imalbox.php?idart=S3         HTML Document         25 K8         4/24/2           Imalbox         https://webmal.mit.edu/horde/imp/imalbox.php?idart=S3         HTML Document         25 K8         4/24/2           Imalbox         https://webmal.mit.edu/horde/imp/imalbox.php?idart=S3         HTML Document         26 K8         4/24/2           Imalbox         https://webmal.mit.edu/horde/imp/imalbox.php?idart=S3         HTML Document         24 K8         4/24/2	05 5:20
Analysis of the second se	
Imalbox         https://webmail.mit.edu/horde/mp/maibox.php?page=60         HTML Document         36 kB         4/24/2           Imalbox         https://webmail.mit.edu/horde/mp/maibox.php?page=60         HTML Document         26 kB         4/24/2           Imalbox         https://webmail.mit.edu/horde/mp/maibox.php?stat=633         HTML Document         26 kB         4/24/2           Imalbox         https://webmail.mit.edu/horde/mp/maibox.php?stat=633         HTML Document         36 kB         4/24/2           Imalbox         https://webmail.mit.edu/horde/mp/maibox.php?stat=632         HTML Document         26 kB         4/24/2	
maissage https://webmail.mit.edu/horde/imp/message.php?index=2194 HTML Document 2618 4/24/2     maisco: https://webmail.mit.edu/horde/imp/maisco.php?start=959     maisco: https://webmail.mit.edu/horde/imp/massage.php?index=2192 HTML Document 2418 4/24/2     message	
Maibox https://webmail.mit.edu/horde/imp/maibox.php?start=593 HTML Document 35 KB 4/24/2     Marce https://webmail.mit.edu/horde/imp/message.php?index=2192 HTML Document 24 KB 4/24/2	
message https://webmail.mit.edu/horde/imp/message.php?index=2192 HTML Document 24 KB 4/24/2	
	00 0:21
	>

#### **MIT Humanities Library, April 25, 2005**

# 4 out of 4 computers inspected had significant quantities of personal email in their browser caches.

MIT WebMail - Microsoft Inter	net Explorer - [Working Offline]					
ile Edit View Favorites Tools	Help				A*	
🕞 Back 🝷 🐑 🚽 🛃 🌔	🏠 🔎 Search 🤺 Favorites	) 🗟 · 🖕 🔟 · 🗔 🎎 🦓				
ddress 🥘 https://webmail.mit.edu/ho	rde/imp/folders.php	✓ →	Go Links »	ogle -	×	>
Google -	👻 👸 Search Web 🔹 ø 🗗 0 b	locked 🔚 AutoFill 🛛 🛃 Options 🥒		Size	Expires	•
MIT WebMail				: 41 KB	None	
An email service from Inform	ation Services & Technology			: 66 KB	None	
	,			53 KB 26 KB	None None	
🗻 🕉 👳	> 🔁 🏦 🔎	🧳 ? 📲 📊	a 📊	17 KB	None	
INBOX Empty Trash Comp	oose Folders Options Search	n Directory Help Logout Open	Folder	: 17 KB	None	
				: 17 KB	None	
N	1ailbox quota: 175.84MB Used / 244.14	4MB Total (72.02%)		: 24 KB	None	
Folder Navigator 🔍				: 20 KB	None	
				: 35 KB	None	2
Choose Action:	<mark>∽</mark> ?	Expand All   Collapse All 🕴	¥ 🖂 🖌	26 KB 4 KB	4/24/2005 5:58 4/24/2005 4:58	
		13	67 0	38 KB	None	
		13	07 0	66 KB	None	
ACF				: 84 KB	4/26/2005 5:58	
				: 29 KB	None	
Home				: 5 KB	None	
🗖 👘 🐨 мітос				: 12 KB	None	
				: 33 KB	4/24/2005 5:20	
🗖 👘 🗣 sent				27 KB 36 KB	4/24/2005 5:21 4/24/2005 5:21	
□ - Student House					4/24/2005 5:21	
					4/24/2005 5:21	
🗖 👘 🖑 Ultimate					4/24/2005 5:21	
— — · · · · ·				24 KB	4/24/2005 5:21	
🗆 👘 🧐 webmail-trash				: 17 KB	None 💊	
Work				_	> .:	i.
Choose Action:	✓ 2	Expand All   Collapse All	¥ 🖂			
-						
		🗝 🔒 🥑 Internet				

The American Library Association recommends software that automatically purges caches on a *daily* basis.[ALA 05] (It would be better to purge after each use.)

## Legislative reactions to this research: "Fair and Accurate Credit Transactions Act of 2003" (US)

- Introduced in July 2003. Signed December 2003.
- Regulations adopted in 2004, effective June 2005.
- Amends the FCRA to standardize consumer reports.
- Requires destruction of paper or electronic "consumer records."

**Testimony:** http://tinyurl.com/cd2my

# Technical reactions to this research: "Secure Empty Trash" in MacOS 10.3.

6	Finder	File	Edit	View	Go	١
	About	Finde	r			
	Prefere	ences.		ж,		
	Empty	Trash		¥ 🛛		
	Secure	Empt	y Trasl	1		
	Service	es		•		
	Hide F	inder		жн		
	Hide C	thers	٦	жн		
	Show /	411				

# Unfortunately, "Secure Empty Trash" is incomplete.

- Implemented in Finder (inconsistently)
- Locks trash can
- Can't change your mind





#### MacOS 10.4 "Erase Free Space" makes a big file.

000	USB2	$\bigcirc$
Burn New Image Convert Verify	Enable Journaling Info Unmount Eject	Log
S5.9 GB Hitachi IC25N0 Macintosh HD 233.8 GB Maxtor OneT USB2	First Aid       Erase       RAID       Restore         To erase a disk or volume, select its icon, specify a format and name, and         • Erasing a disk erases all data and volumes on a disk, leaving the disk er selected volume erases that volume only, leaving other volumes on the di         • To securely erase data, click Security Options and select an option before         Erase.         • To help prevent recovery of deleted files, click the Erase Free Space buttom	mpty. Erasing a isk unchanged. re clicking
•	Volume Format: Mac OS Extended (Case-sensitiv Name: USB2	ve, Jo 🛟
	Erase Free Space Security Options	Erase
Mount Point : <u>No</u> Format : Mac Owners Enabled : No Number of Folders : 5	lumes/USB2 OS Extended (Case-sensitive, Journaled) Used : 97.7 GB (104,90 Number of Files : 32	955,315,712 Bytes)

### MacOS "File Vault" gives users an encrypted file system.

00	Security	
	how All	Q
	FileVault FileVault secures your home folder by encrypting encrypts and decrypts your files while you're usin WARNING: Your files will be encrypted using your login password and you don't know the master pa A master password is set for this compute This is a "safety net" password. It lets you unlock FileVault account on this computer. FileVault protection is on for this account. Turning off FileVault may take a while.	g them. login password. If you forget your assword, your data will be lost. er. any Change
	<ul> <li>Require password to wake this computer</li> <li>For all accounts on this computer:</li> <li>Disable automatic login</li> <li>Require password to unlock each secure</li> <li>Log out after 60 (1) minutes of inaction</li> <li>Use secure virtual memory</li> </ul>	e system preference
Click	the lock to prevent further changes.	?

### **Future Work: Deploying Compete Delete**

- Make FORMAT actually erase the disk.
- Make "Empty Trash" actually overwrite data.
- Integrate this functionality with web browsers, word processors, operating systems.
- Address usability dangers of clean delete.
- Analysis of "one big file" technique.

# Let's put this in Linux!

### **Future Work: 2500 Drive Corpus**

- Automated construction of stop-lists.
- Detailed analysis of false positives/negatives in CCN test.
- Explore identifiers other than CCNs.
- Support for languages other than English.

More than 500 drives are standing by...

### **Future Work: Toolkit**

- Easy-to-use, reliable, disk imaging software.
- New file format for disk images.
- Web-based database of hash codes.

Initial version is available for download.

## **Future Work: Economics and Society**

- Who is buying used hard drives and why?
- Hard drive honeypot.
- Compliance with FACT-A

This is a lot of work...

### **Future Work: Summary**

- Improved cross-drive forensics
- 2500 Drive Corpus
- Open-Source Toolkits
- Economics and Society

#### **Questions?**