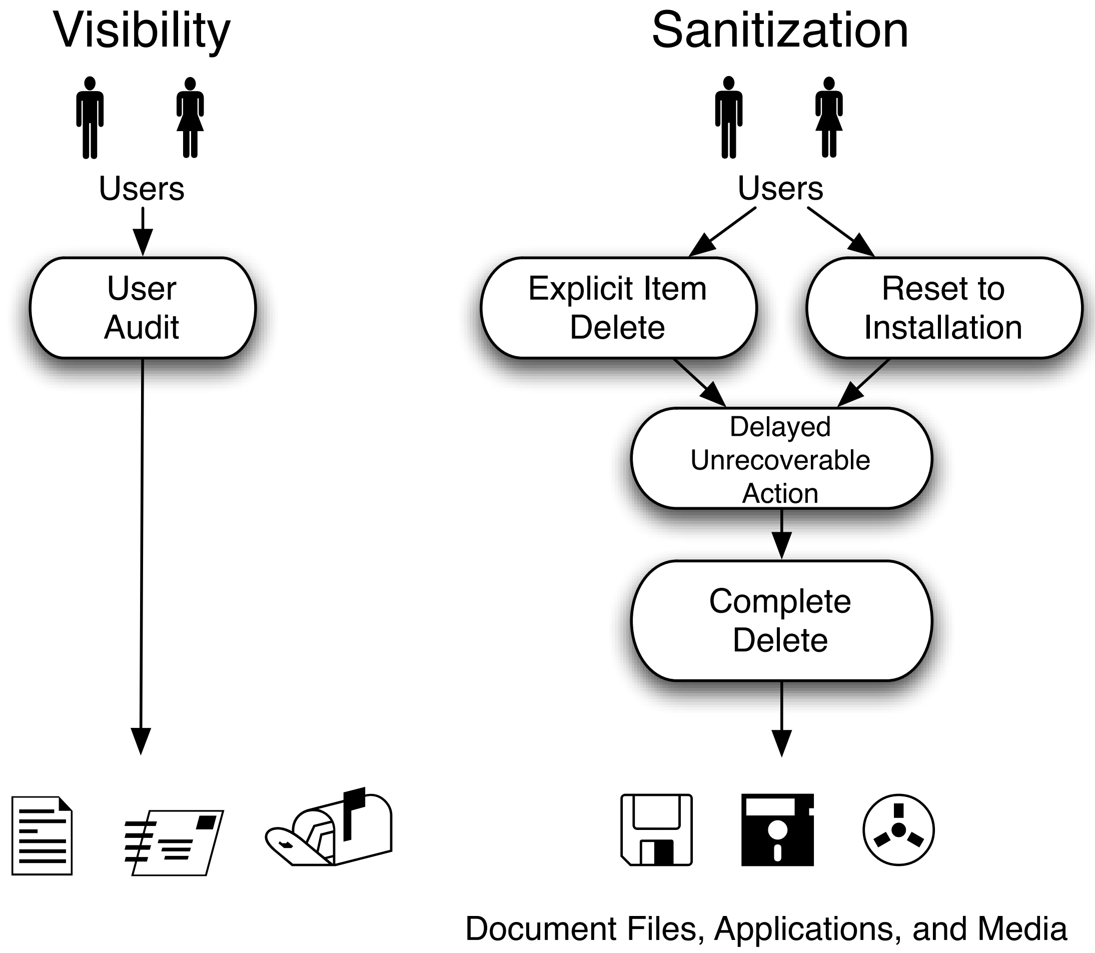
“Complete Delete” and Other Patterns for Information Eradication



Visibility

Users

User Audit

Sanitization

Users

Explicit Item Delete

Reset to Installation

Delayed Unrecoverable Action

Complete Delete

Document Files, Applications, and Media

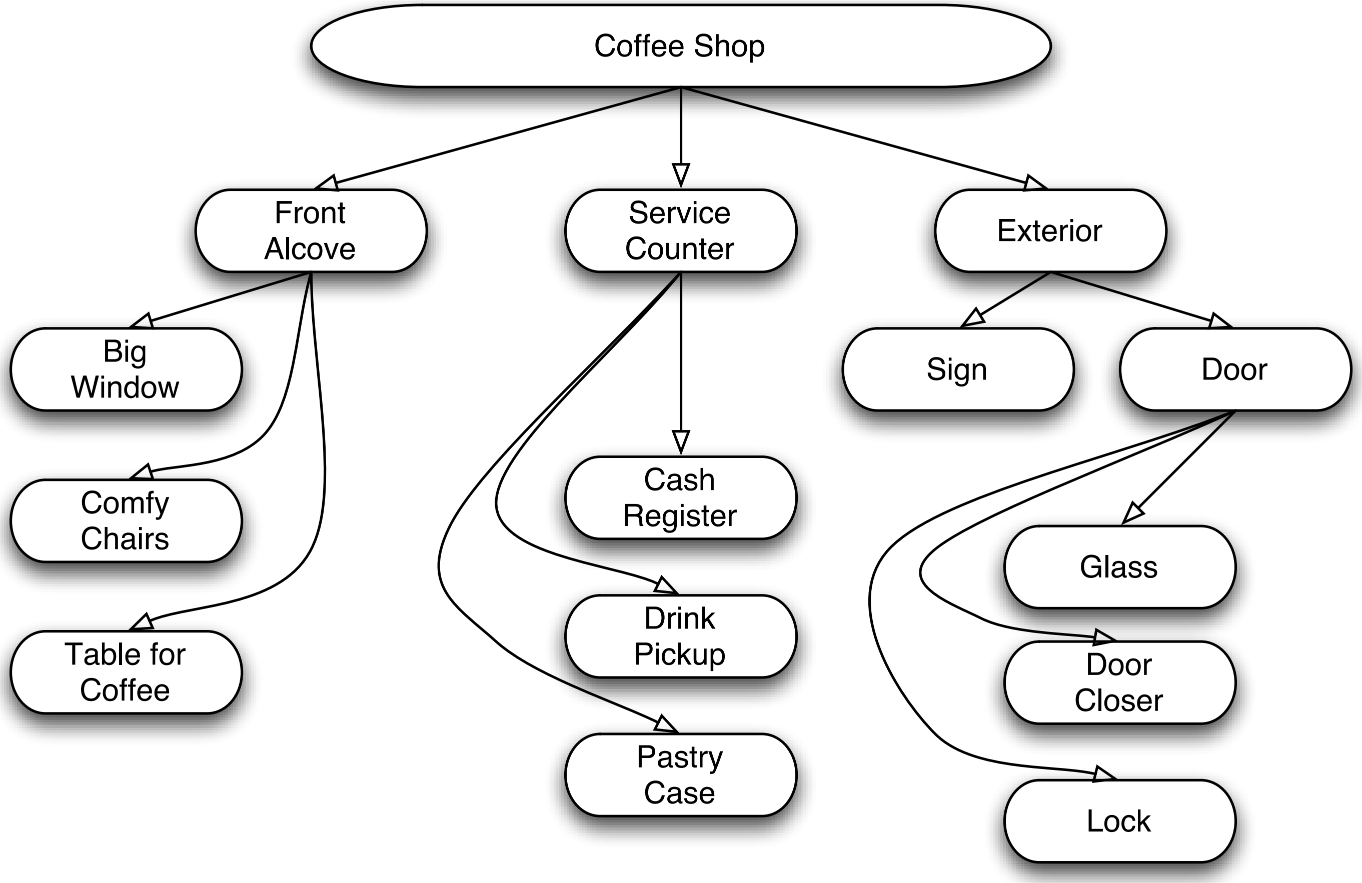
Simson L. Garfinkel

Center for Research on Computation and Society

Harvard University

October 11, 2005

A pattern is a recurring solution to a standard problem.



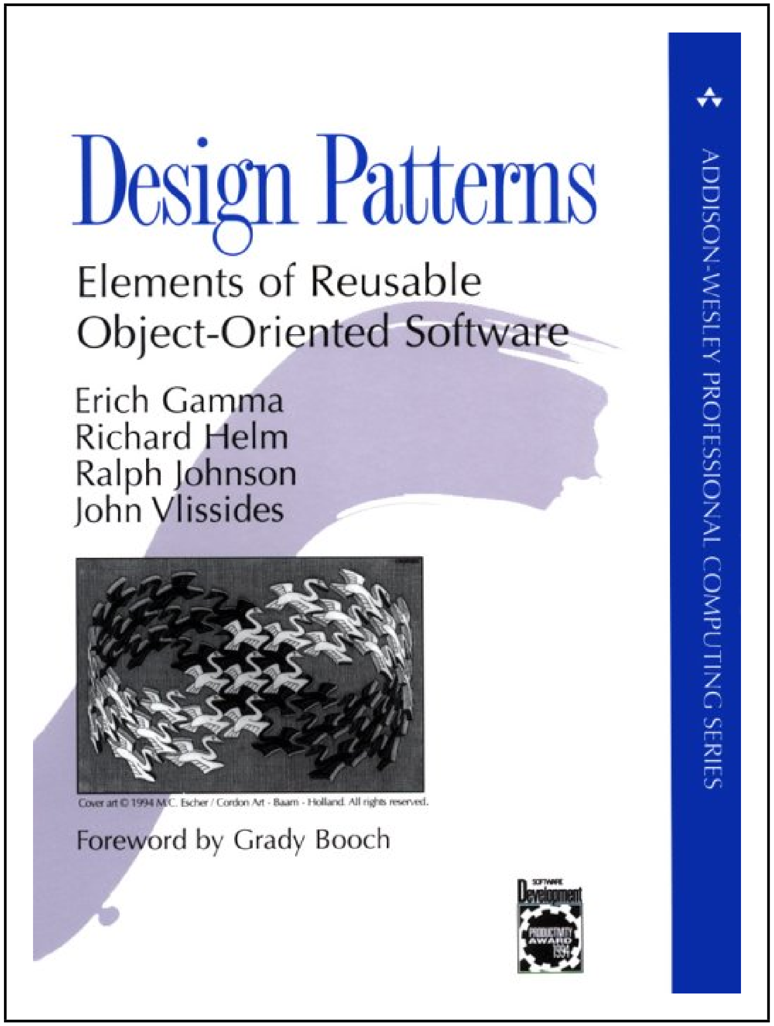
Patterns and “pattern languages” introduced by Architect Christopher Alexander in the 1970s.

Object Oriented Design adopted patterns in the 1990s.

Johnson *et al.*, [OOPSLA 91]; Coad [CACM, 92]; “Gang of four” [95]

Patterns help us to:

- reuse successful practices
- reason about what’s done and why
- document abstractions other than algorithms and data structures. [Schmidt *et al.*, 1996]



Design Patterns

Elements of Reusable Object-Oriented Software

Erich Gamma
Richard Helm
Ralph Johnson
John Vlissides

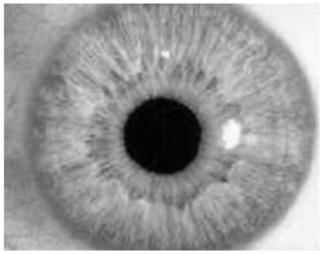
Cover art © 1994 M.C. Escher / Cordon Art - Baarn - Holland. All rights reserved.

Foreword by Grady Booch

ADDISON-WESLEY PROFESSIONAL COMPUTING SERIES

Patterns encapsulate knowledge and understanding, making it easier to teach and deploy solutions.

It has long been recognized that end-user security and usability are at odds in modern computer systems.



Username: simsong
Password: ••••••

ACCESS DENIED

ACCESS DENIED

ACCESS DENIED

The need to align end-user security and usability is recognized as a priority for both computing and the nation.

- CRA 2003 “Grand Challenge”
- PITAC 2005 “priority”
- Special publications
  [IEEE S&P 2004] [O’Reilly 2005]
- CHI 2005; SOUPS 2005

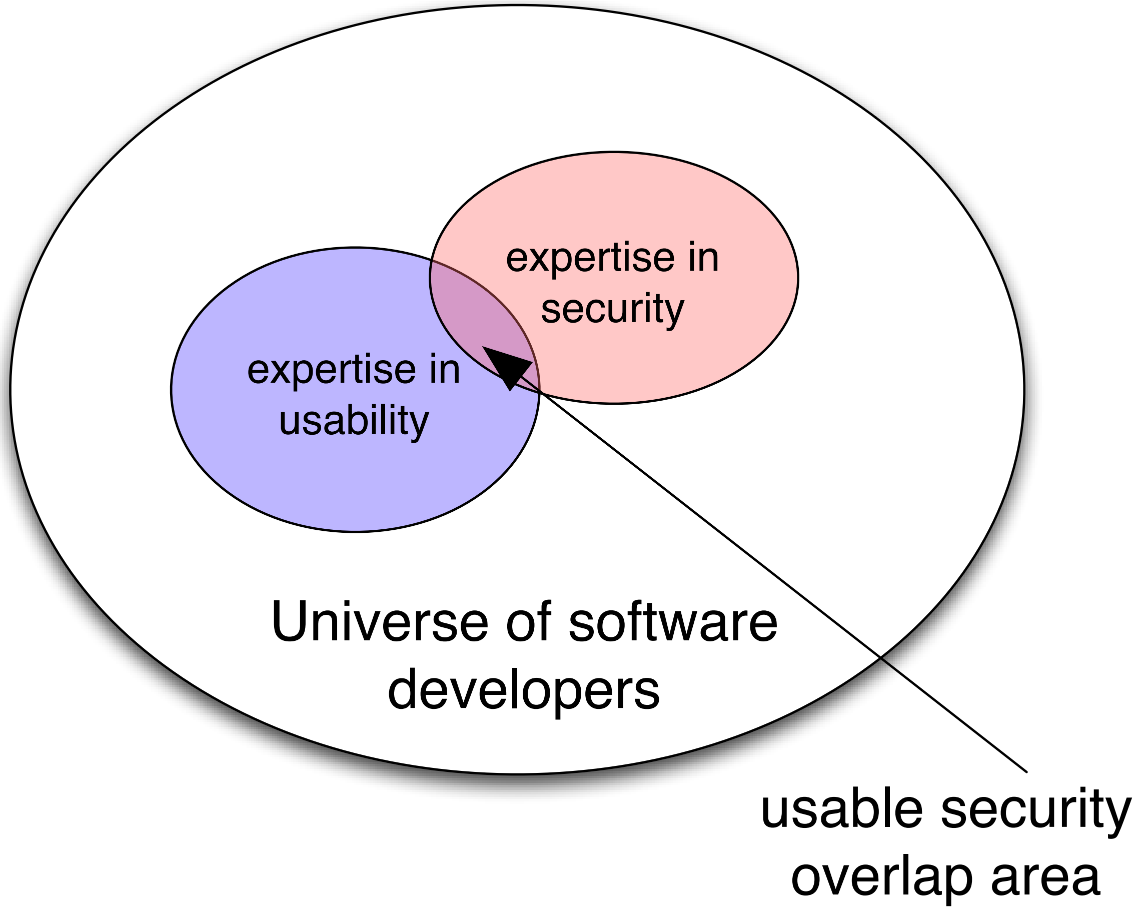
Honeypot Forensics • New: Basic Training • The Shellcode Generation
IEEE
SECURITY & PRIVACY
SEPTEMBER/OCTOBER 2004
Volume 2, Number 5
Building Confidence in a Networked World
Usability & Security
Computer Society
IEEE

Computing Research Association
CRA

President’s
Information Technology
Advisory Committee

HCI-SEC is the emerging field that seeks to align Human Computer Interfaces with Security.

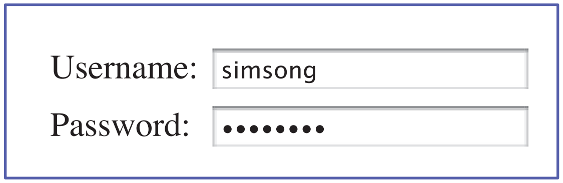
The root of the conflict: security and usability *must both be applied from the beginning*—but they are *different skills*.



Today computer security has many “principles,” “best practices” and “techniques.”

- Biometric authentication

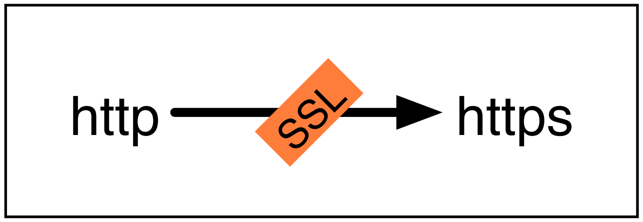
- The password field



Username: simsong

Password: ••••••••

- Wrapping plaintext protocols with SSL

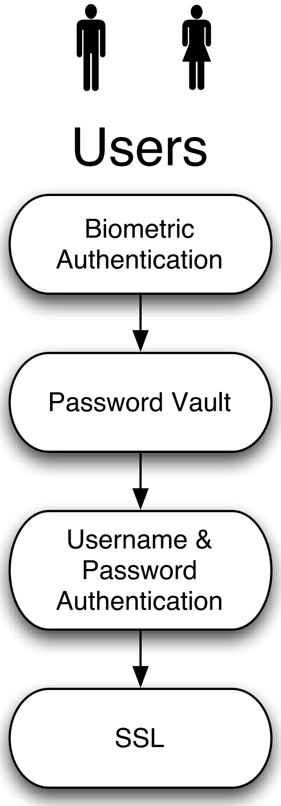


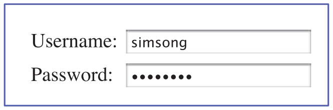
http

SSL

https

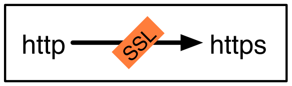
With patterns, we can decompose the problems and their solutions.





Username: simsong

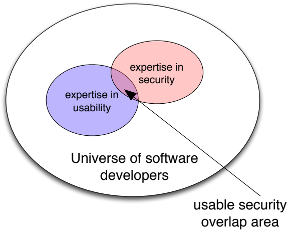
Password: ••••••••



Patterns make it easier to communicate solutions to students, implementors, and management.

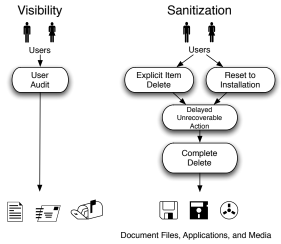
This talk presents set of patterns for destroying information.

1. Introduction to patterns. ✔

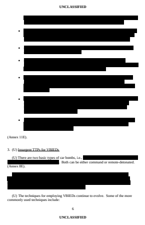


2. The Drives Study

3. Patterns for sanitization.



4. Applying these patterns.



UNCLASSIFIED

[redacted]

(Annex 11E).

3. (U) Insurgent TTPs for VBIEDs.

(U) There are two basic types of car bombs, i.e., [redacted]. Both can be either command or remote-detonated. (Annex 8E).

[redacted]

(U) The techniques for employing VBIEDs continue to evolve. Some of the more commonly used techniques include:

6

UNCLASSIFIED

The Sanitization Problem: Confidential information is left behind after it is no longer needed.

Data discovered on second-hand hard drives is an obvious case.

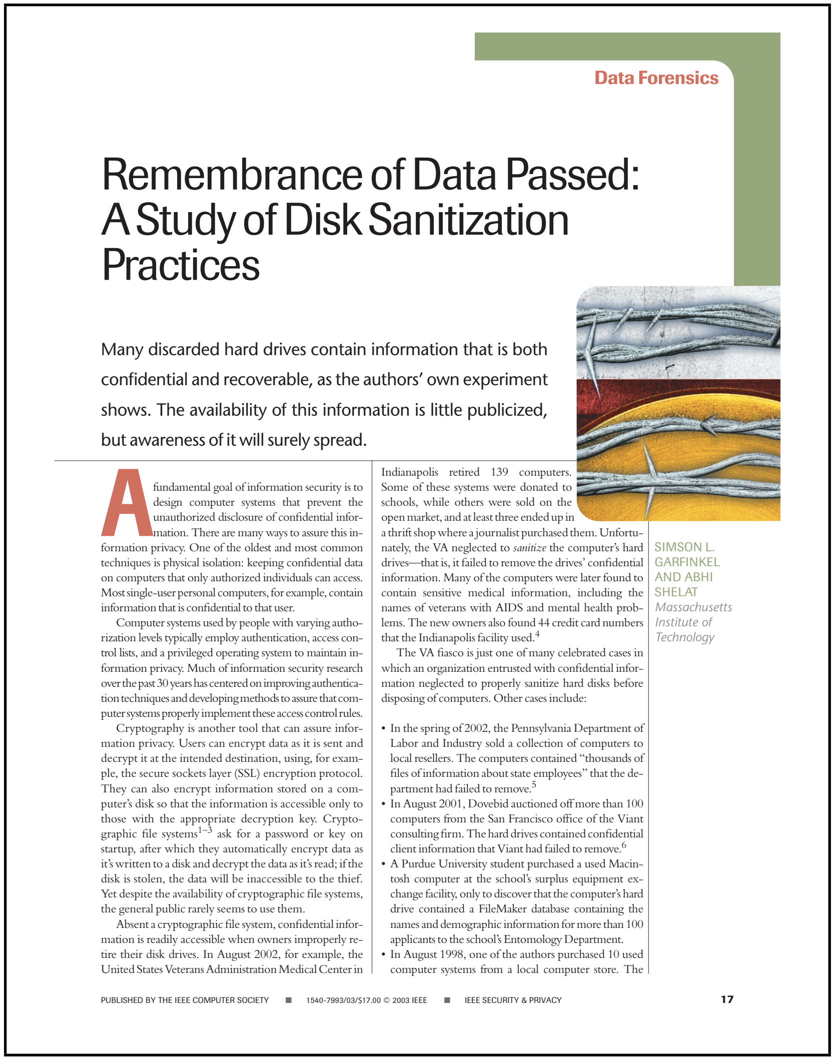
- Woman in Nevada bought a used PC with pharmacy records [Markoff 97]
- Paul McCartney’s bank records sold by his bank [Leyden 04]
- Pennsylvania sold PCs with “thousands of files” on state employees [Villano 02]

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

[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



Data Forensics

Remembrance of Data Passed: A Study of Disk Sanitization Practices

Many discarded hard drives contain information that is both confidential and recoverable, as the authors' own experiment shows. The availability of this information is little publicized, but awareness of it will surely spread.

SIMSON L. GARFINKEL AND ABHI SHELAT
Massachusetts Institute of Technology

A fundamental goal of information security is to design computer systems that prevent the unauthorized disclosure of confidential information. There are many ways to assure this information privacy. One of the oldest and most common techniques is physical isolation: keeping confidential data on computers that only authorized individuals can access. Most single-user personal computers, for example, contain information that is confidential to that user.

Computer systems used by people with varying authorization levels typically employ authentication, access control lists, and a privileged operating system to maintain information privacy. Much of information security research over the past 30 years has centered on improving authentication techniques and developing methods to assure that computer systems properly implement these access control rules.

Cryptography is another tool that can assure information privacy. Users can encrypt data as it is sent and decrypt it at the intended destination, using, for example, the secure sockets layer (SSL) encryption protocol. They can also encrypt information stored on a computer's disk so that the information is accessible only to those with the appropriate decryption key. Cryptographic file systems[1–3] ask for a password or key on startup, after which they automatically encrypt data as it's written to a disk and decrypt the data as it's read; if the disk is stolen, the data will be inaccessible to the thief. Yet despite the availability of cryptographic file systems, the general public rarely seems to use them.

Absent a cryptographic file system, confidential information is readily accessible when owners improperly retire their disk drives. In August 2002, for example, the United States Veterans Administration Medical Center in Indianapolis retired 139 computers. Some of these systems were donated to schools, while others were sold on the open market, and at least three ended up in a thrift shop where a journalist purchased them. Unfortunately, the VA neglected to *sanitize* the computer's hard drives—that is, it failed to remove the drives' confidential information. Many of the computers were later found to contain sensitive medical information, including the names of veterans with AIDS and mental health problems. The new owners also found 44 credit card numbers that the Indianapolis facility used.[4]

The VA fiasco is just one of many celebrated cases in which an organization entrusted with confidential information neglected to properly sanitize hard disks before disposing of computers. Other cases include:

- In the spring of 2002, the Pennsylvania Department of Labor and Industry sold a collection of computers to local resellers. The computers contained "thousands of files of information about state employees" that the department had failed to remove.[5]
- In August 2001, Dovebid auctioned off more than 100 computers from the San Francisco office of the Viant consulting firm. The hard drives contained confidential client information that Viant had failed to remove.[6]
- A Purdue University student purchased a used Macintosh computer at the school's surplus equipment exchange facility, only to discover that the computer's hard drive contained a FileMaker database containing the names and demographic information for more than 100 applicants to the school's Entomology Department.
- In August 1998, one of the authors purchased 10 used computer systems from a local computer store. The

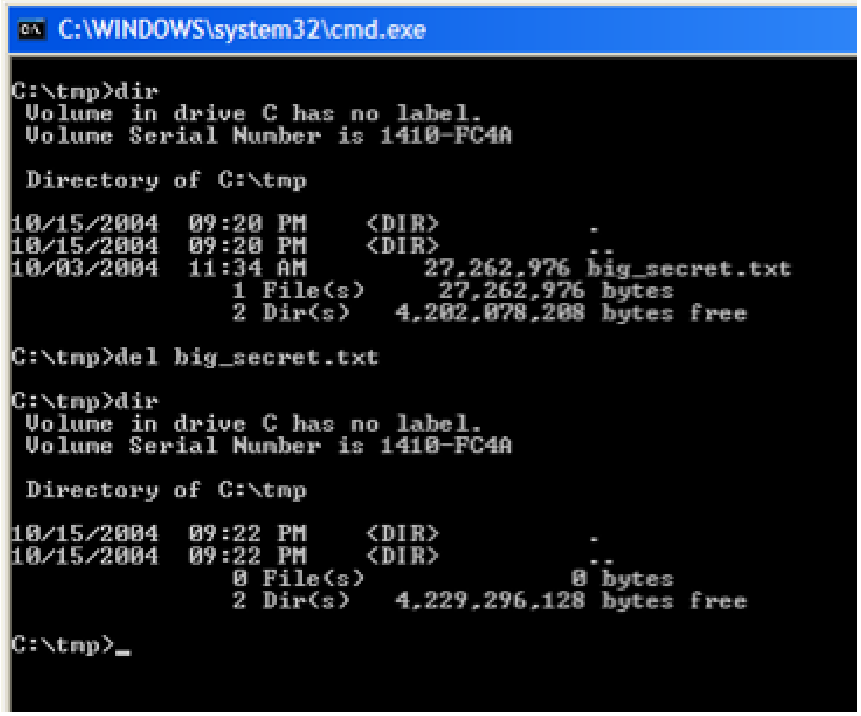
PUBLISHED BY THE IEEE COMPUTER SOCIETY ■ 1540-7993/03/$17.00 © 2003 IEEE ■ IEEE SECURITY & PRIVACY 17

We did not determine if this was a *usability* problem or an *education* problem.

Evidence for the usability problem: Computers *lie* when users delete data.

DEL removes file names

—but not file contents.

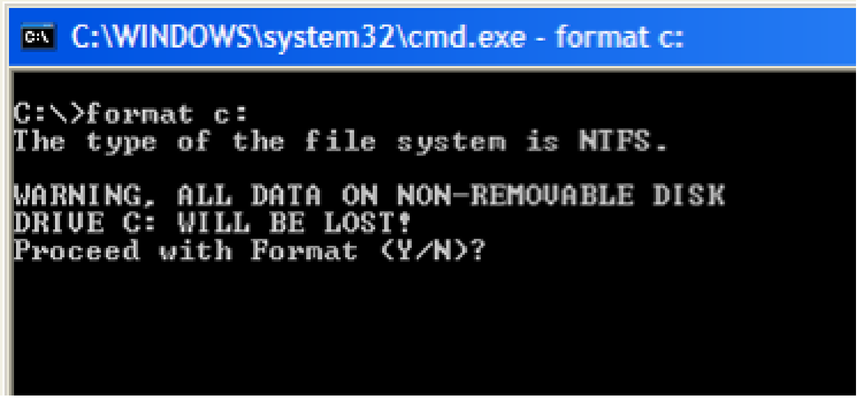


```
C:\tmp>dir
 Volume in drive C has no label.
 Volume Serial Number is 1410-FC4A

 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

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

C:\tmp>_
```

FORMAT claims

"ALL DATA ... WILL BE LOST"

—but it's not.



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

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

This violates the principle of "Psychological Acceptability." [SS '75]

Psychological Acceptability: “... avoid a fundamental mismatch between software capabilities and the user’s mental models.”

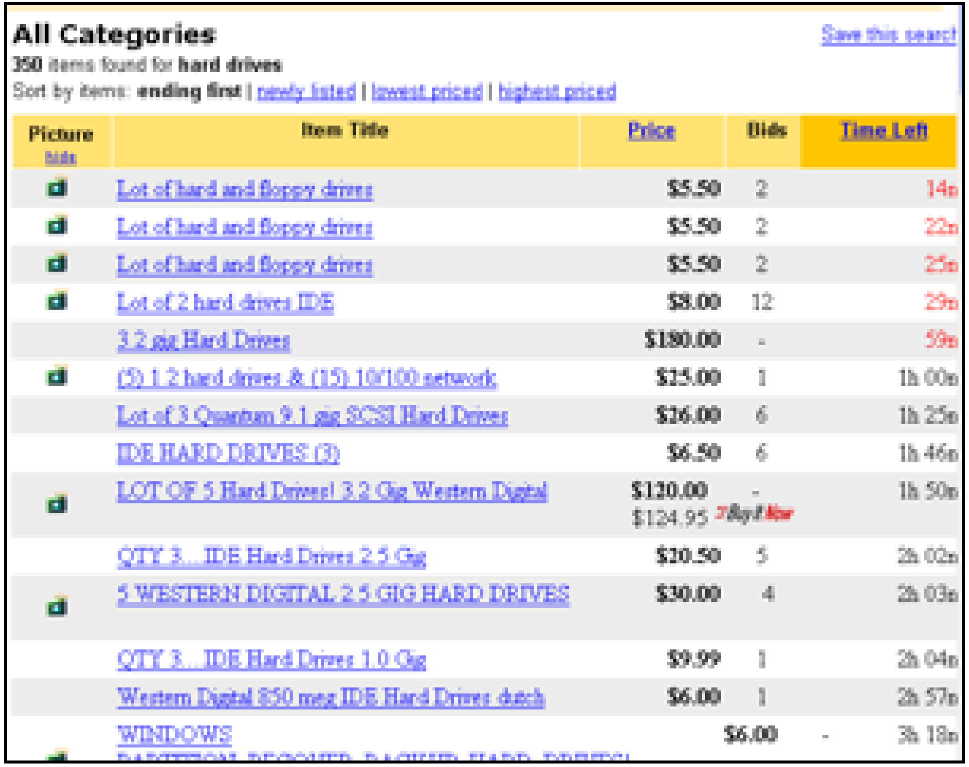
“We all sincerely believed that when we ... pressed the button ’delete’ that it was gone forever.

Wow, were we wrong.”
— Oliver North, 1987

Oliver North had a mismatched mental model.

Evidence for an educational problem:
There is a huge secondary market for used disk drives.

- Re-used within organizations
- Given to charities
- Sold on eBay



All Categories Save this search

350 items found for **hard drives**

Sort by items: **ending first** | newly listed | lowest priced | highest priced

Picture hide	Item Title	Price	Bids	Time Left
📷	Lot of hard and floppy drives	$5.50	2	14m
📷	Lot of hard and floppy drives	$5.50	2	22m
📷	Lot of hard and floppy drives	$5.50	2	25m
📷	Lot of 2 hard drives IDE	$8.00	12	29m
	3.2 gig Hard Drives	$180.00	-	59m
📷	(5) 1.2 hard drives & (15) 10/100 network	$25.00	1	1h 00m
	Lot of 3 Quantum 9.1 gig SCSI Hard Drives	$26.00	6	1h 25m
	IDE HARD DRIVES (3)	$6.50	6	1h 46m
📷	LOT OF 5 Hard Drives! 3.2 Gig Western Digital	$120.00 $124.95 =Buy It Now	-	1h 50m
	QTY 3....IDE Hard Drives 2.5 Gig	$20.50	5	2h 02m
📷	5 WESTERN DIGITAL 2.5 GIG HARD DRIVES	$30.00	4	2h 03m
	QTY 3....IDE Hard Drives 1.0 Gig	$9.99	1	2h 04m
	Western Digital 850 meg IDE Hard Drives dutch	$6.00	1	2h 57m
📷	WINDOWS PARTITION, RECOVER, BACKUP, HARD DRIVES!	$6.00	-	3h 18m

People could just be discarding disk drives without thinking about the consequences.

To be effective, patterns should address the root cause of the problem.

Usability Problem:

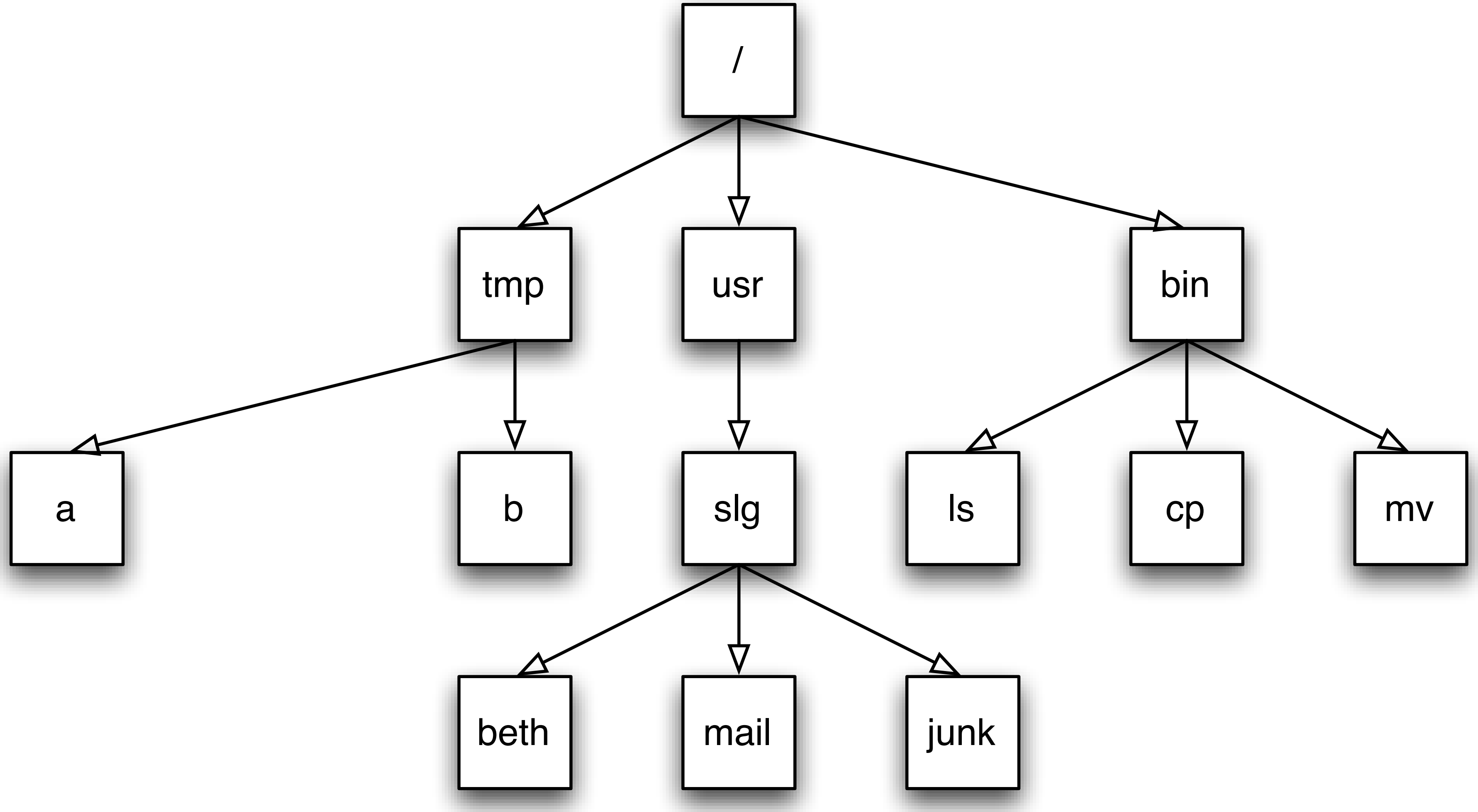
- Effective audit of information present on drives.
- Make DEL and FORMAT actually remove data. [Bauer & Priyantha 01]
- Provide alternative strategies for data recovery.

Education Problem:

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

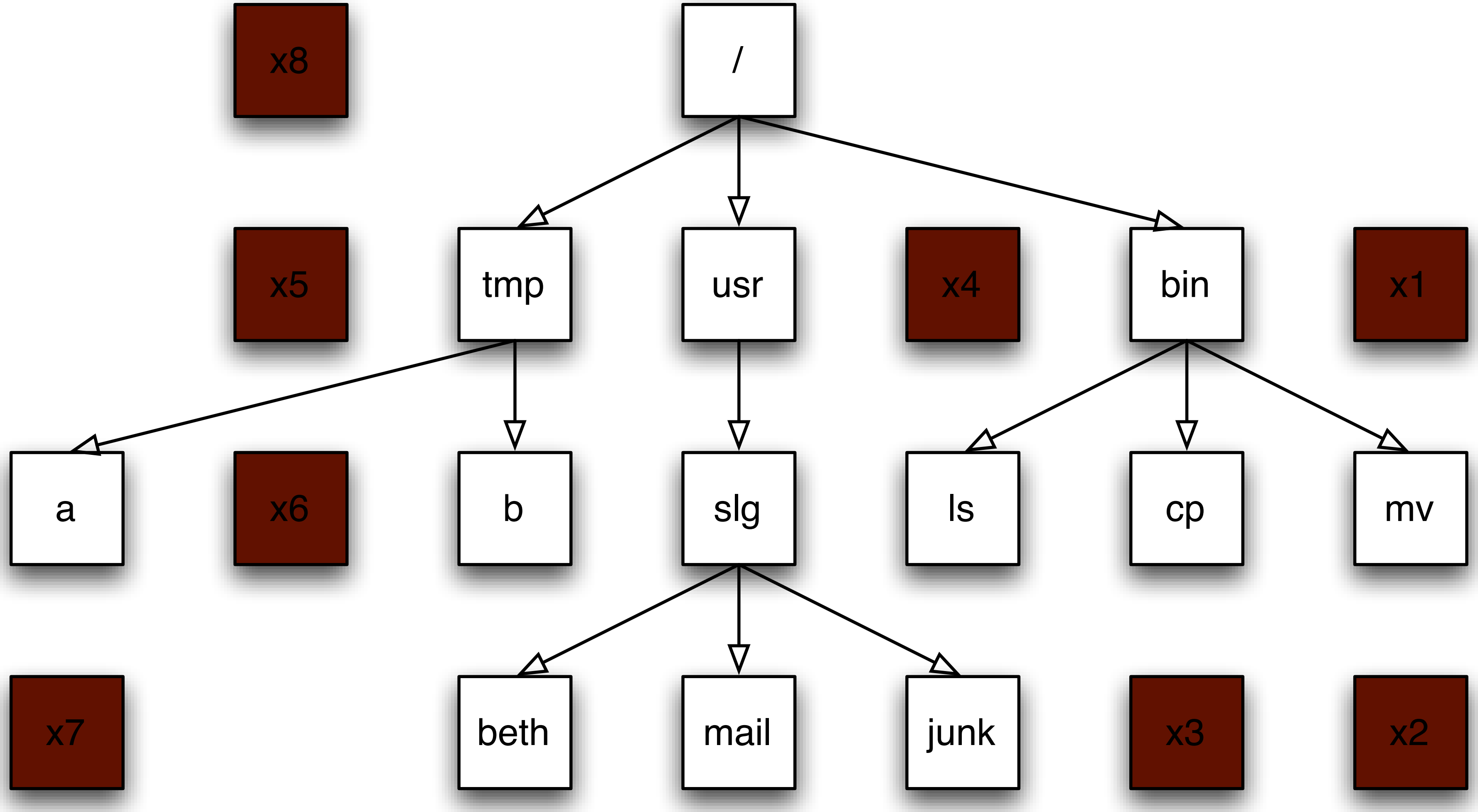
To determine the root cause, I looked *on the drives* and *contacted the data subjects*.

Data on a hard drive is arranged in blocks.



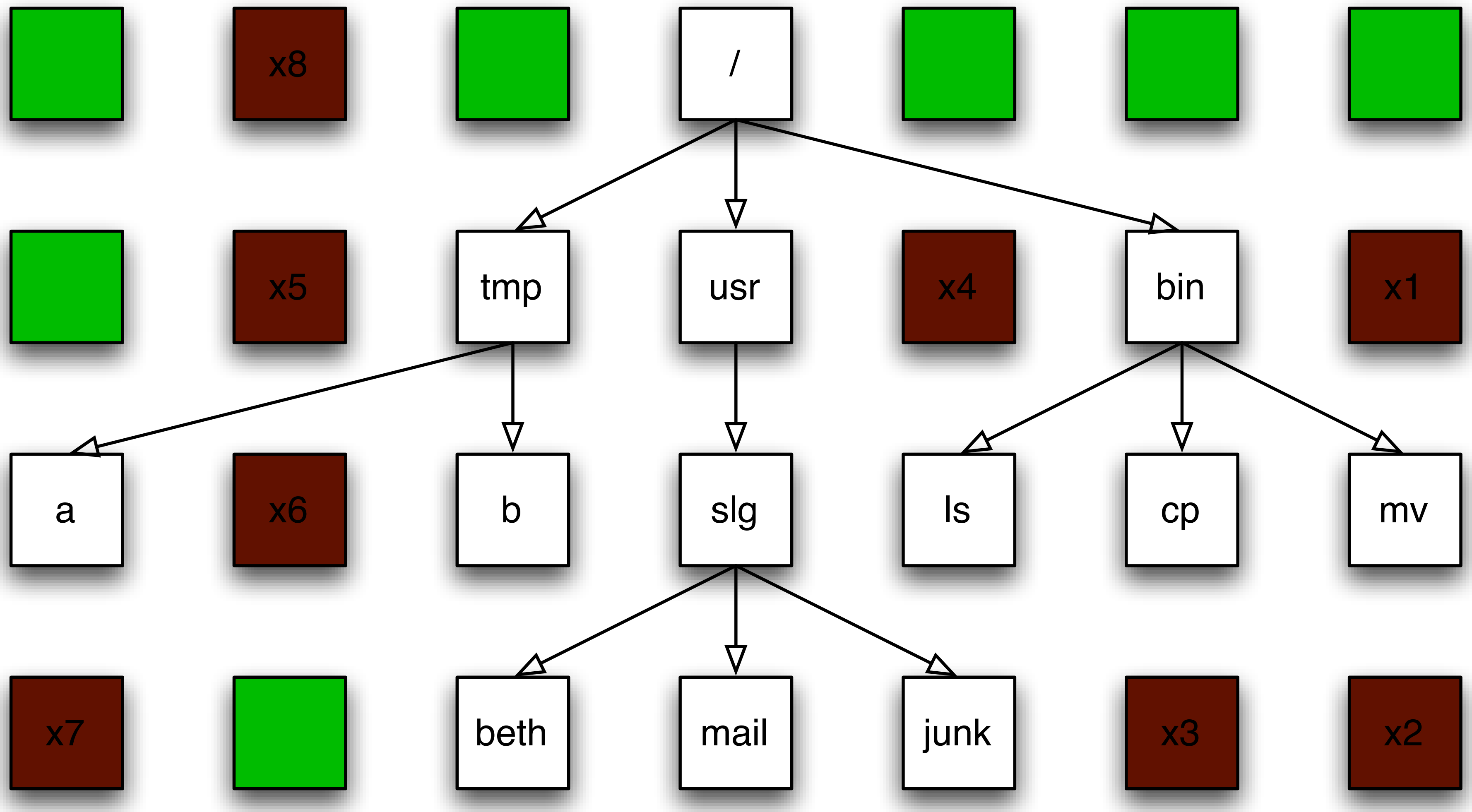
The white blocks indicate directories and files that are visible to the user.

Data on a hard drive is arranged in blocks.



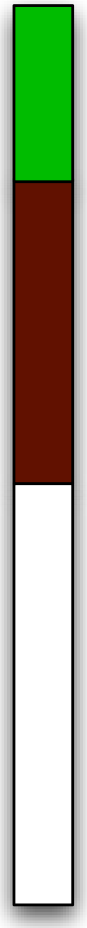
The brown blocks indicate files that were deleted.

Data on a hard drive is arranged in blocks.



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

Stack the disk blocks:

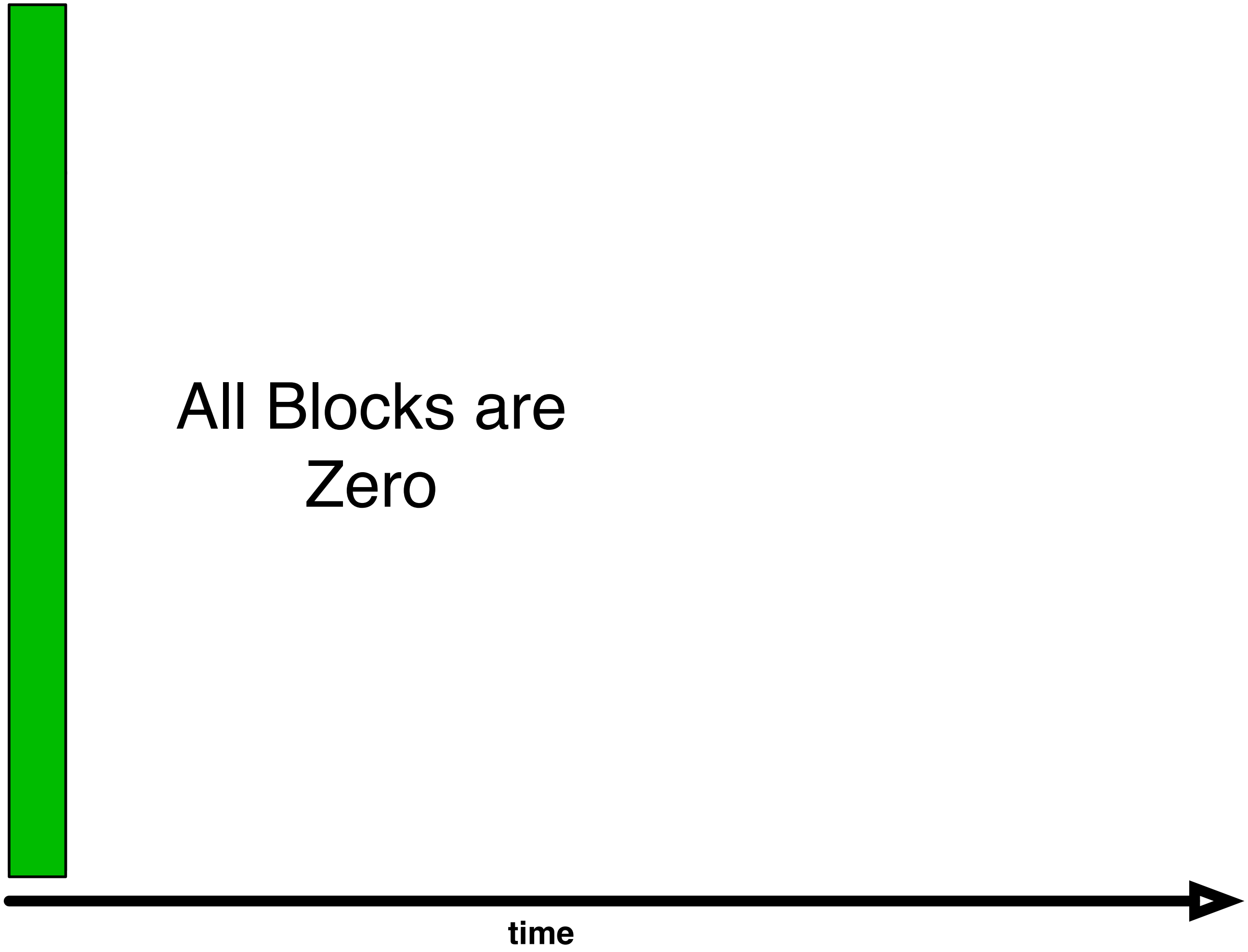


Zero Blocks

Deleted Files

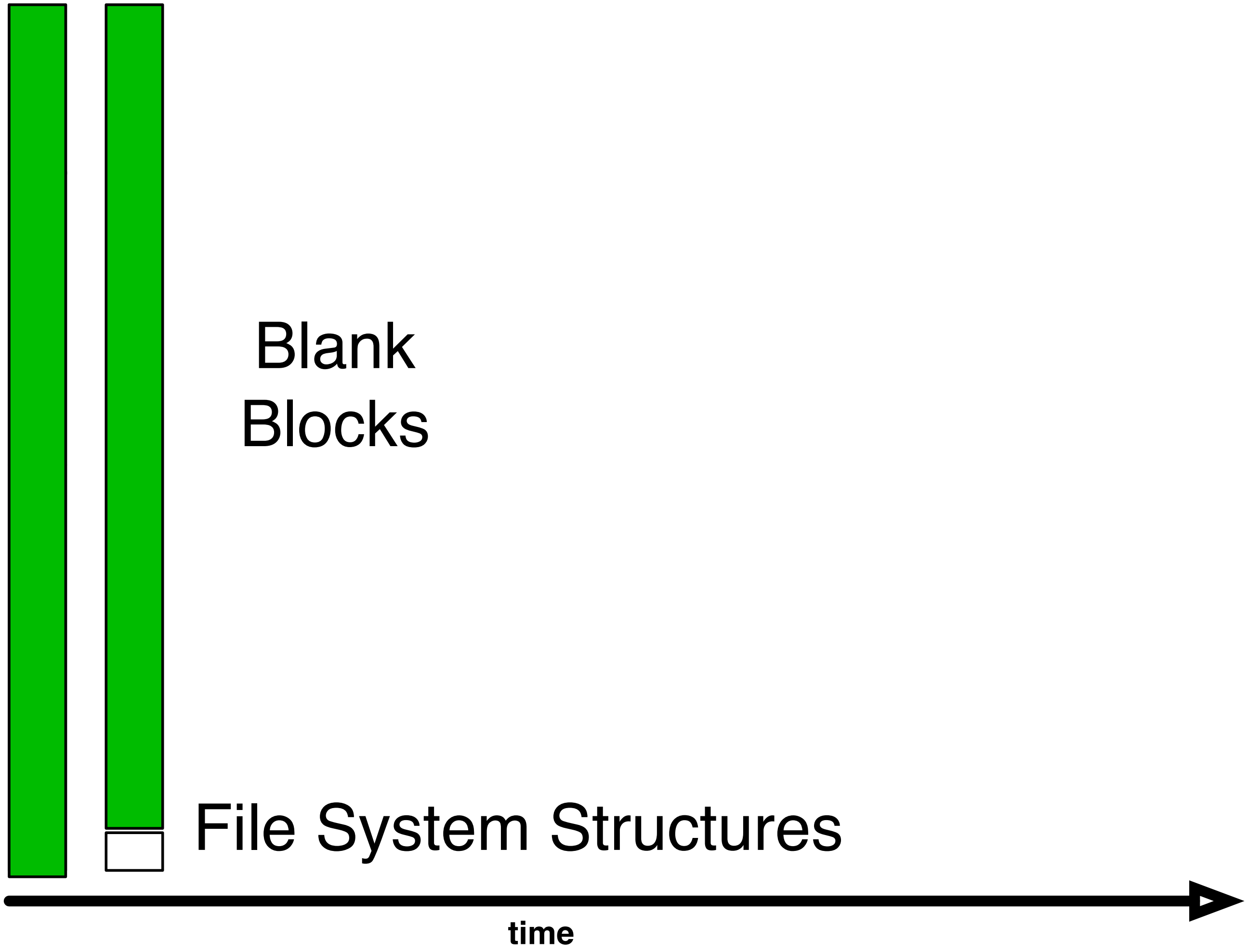
Files

NO DATA: The disk is factory fresh.

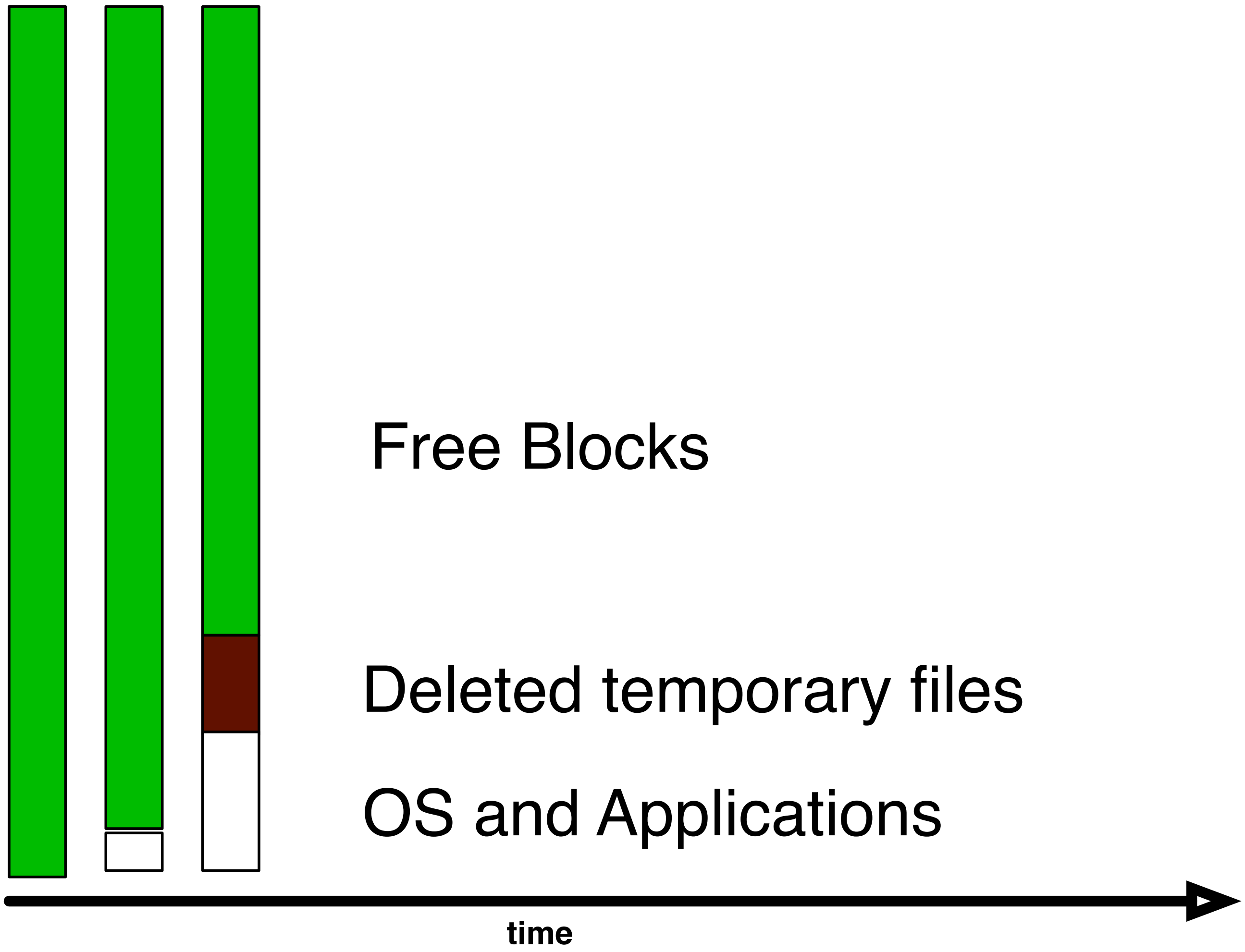


All Blocks are Zero

FORMATTED: The disk has an empty file system



AFTER OS INSTALL: Temp. files have been deleted



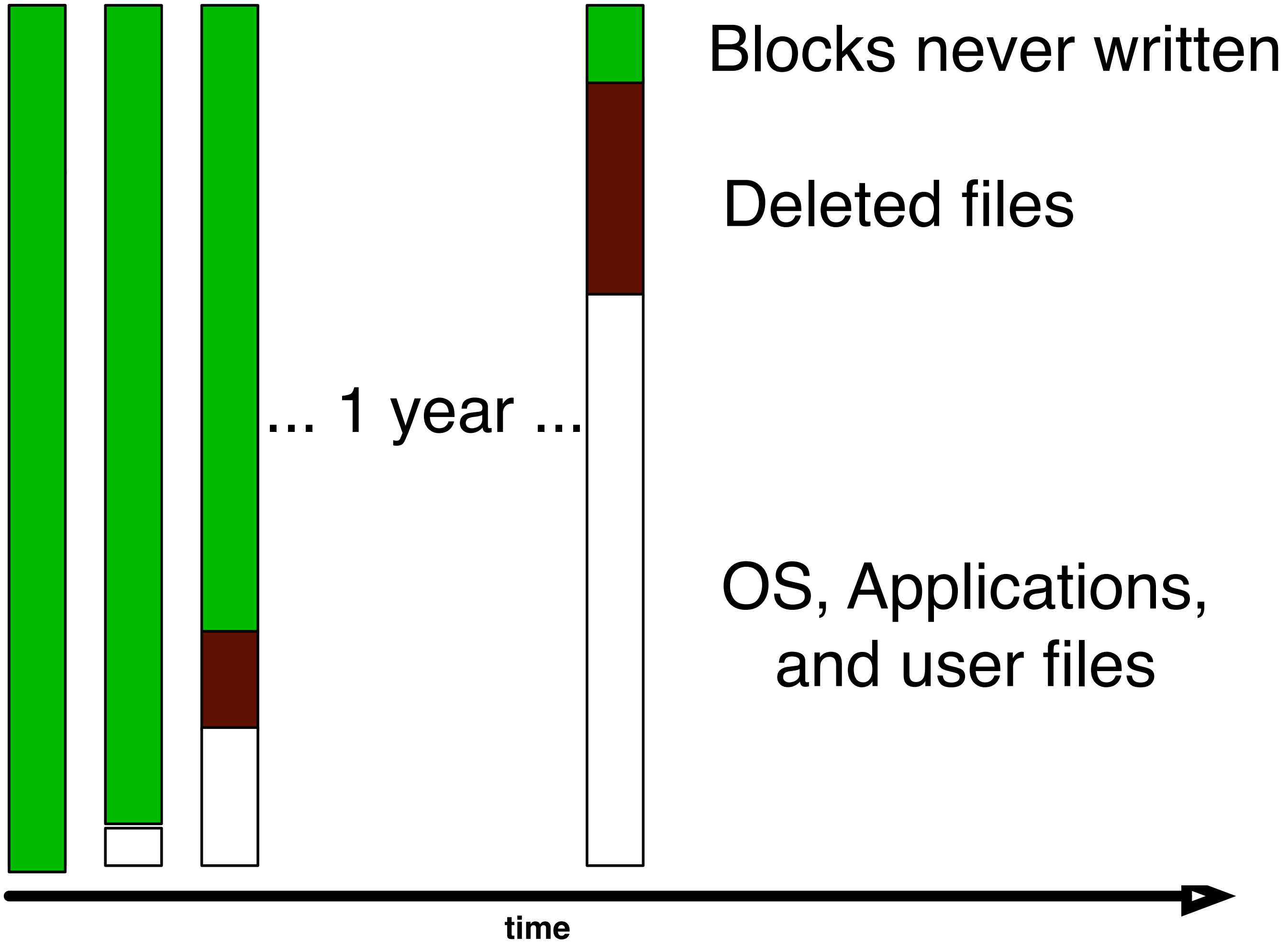
Free Blocks

Deleted temporary files

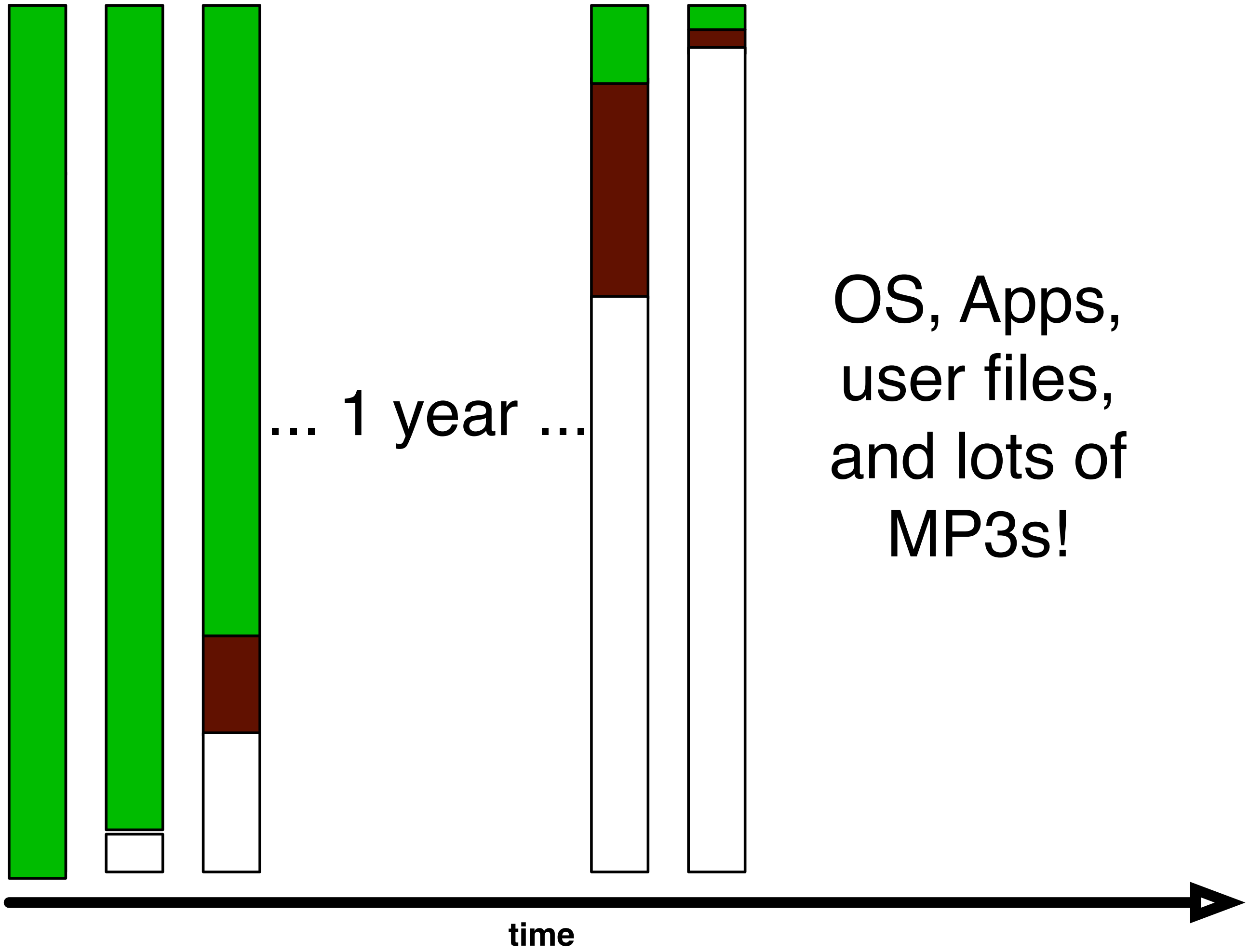
OS and Applications

time

AFTER A YEAR OF SERVICE

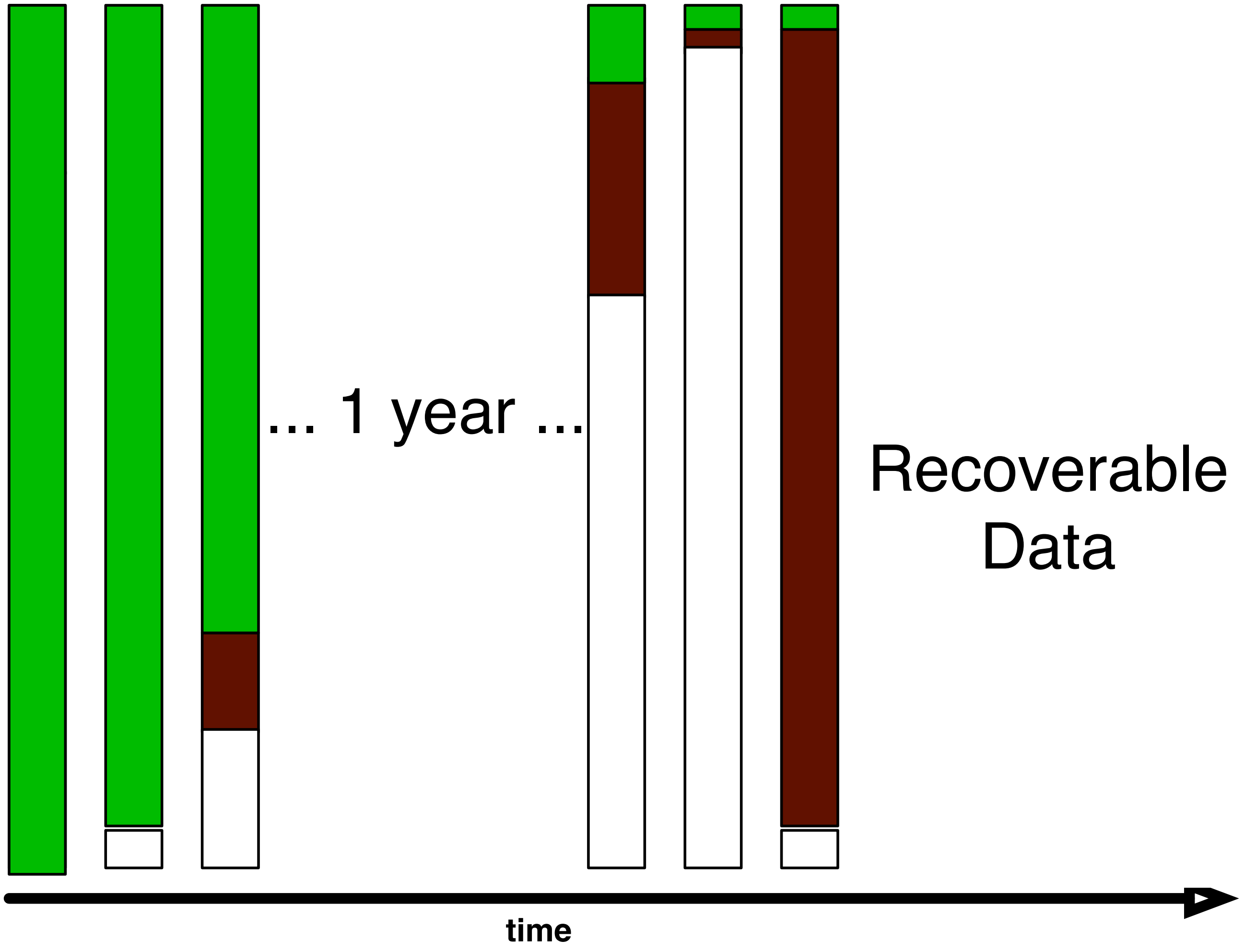


DISK NEARLY FULL!

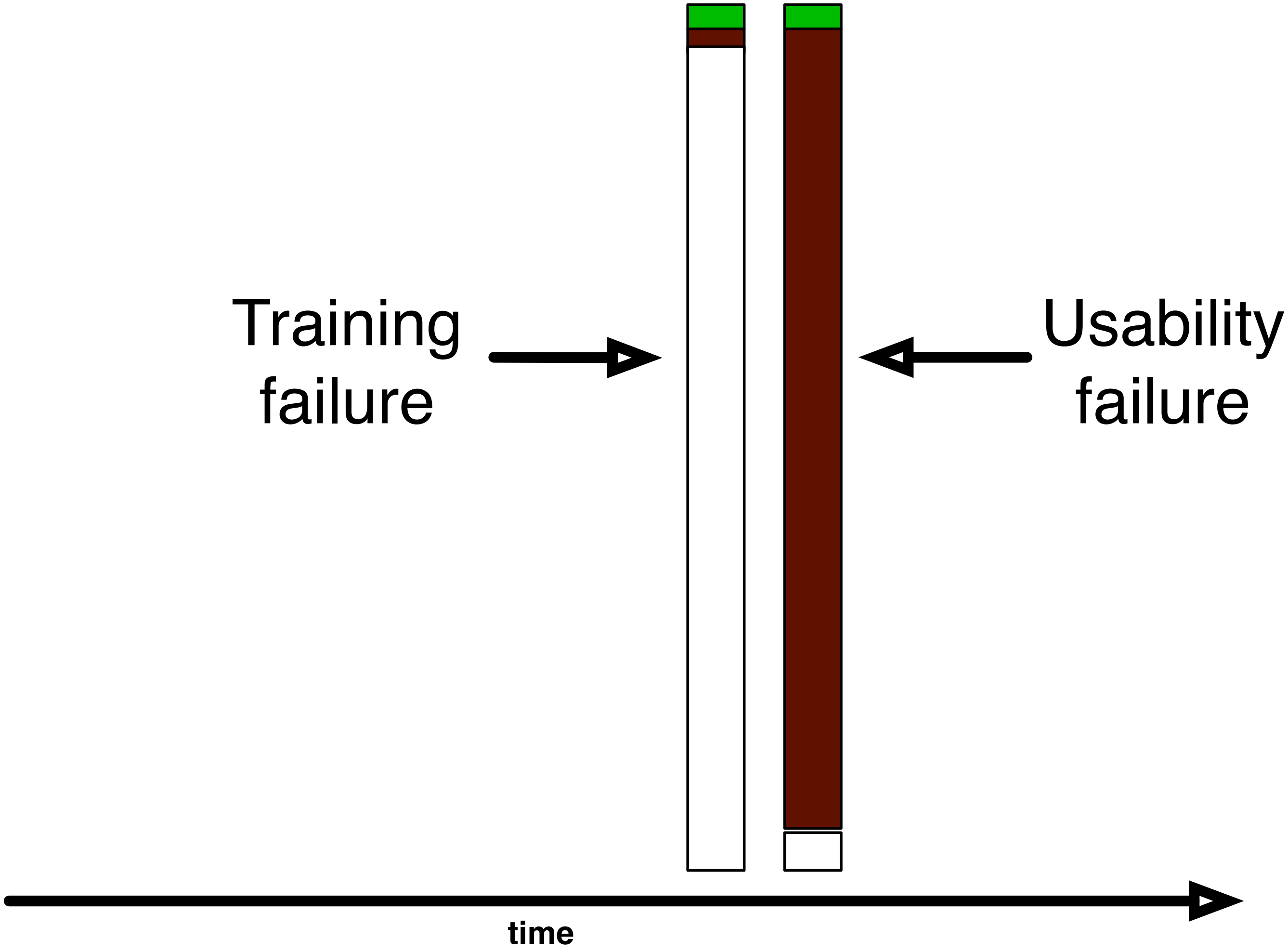


OS, Apps,
user files,
and lots of
MP3s!

FORMAT C:\ (to sell the computer.)



We can use forensics to reconstruct motivations:

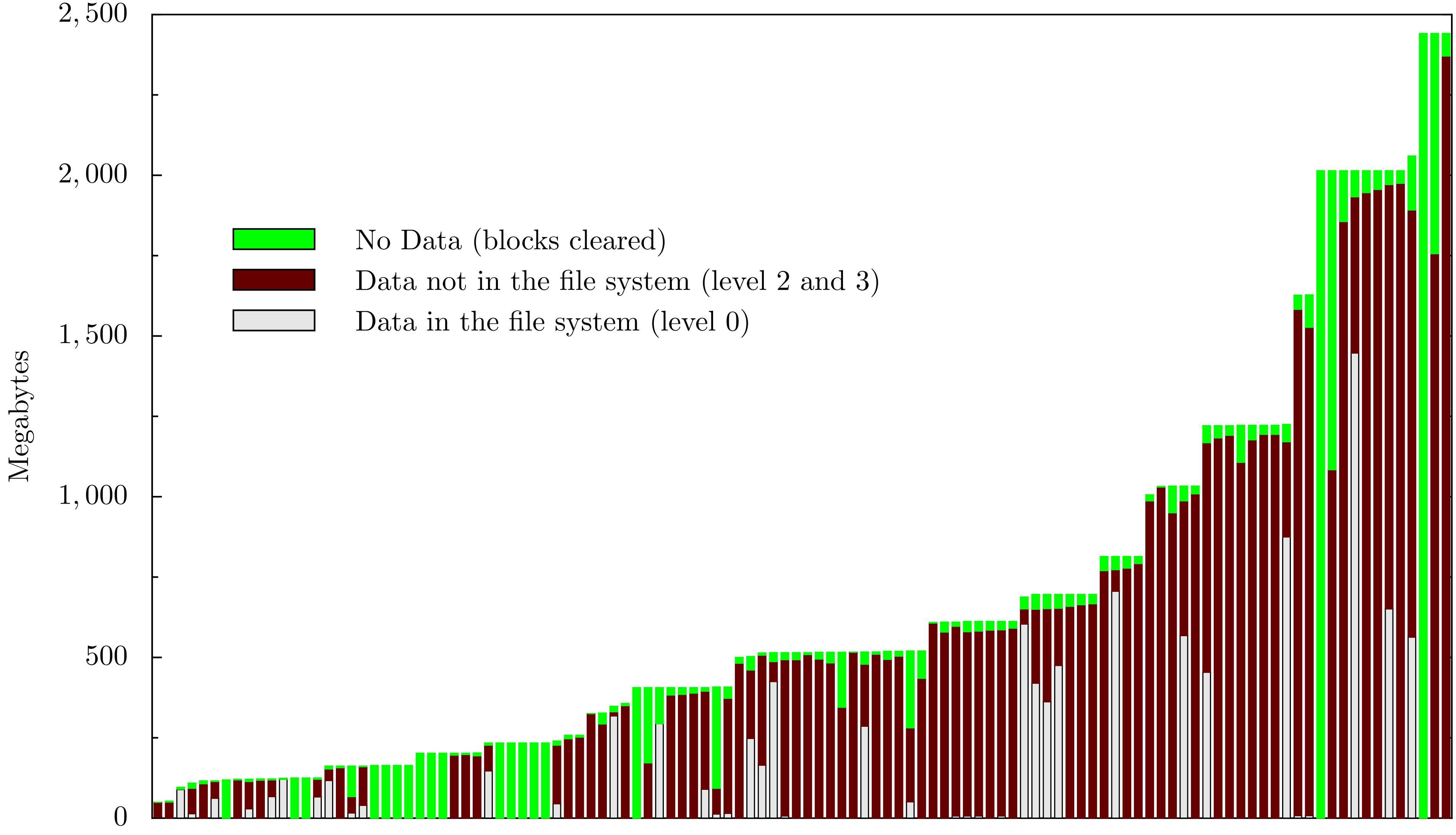


Training failure

Usability failure

time

The 236 drives are dominated by failed sanitization attempts.



But training failures are also important.

But what *really* happened?

?

To answer this question, I needed to contact the original drive owners.

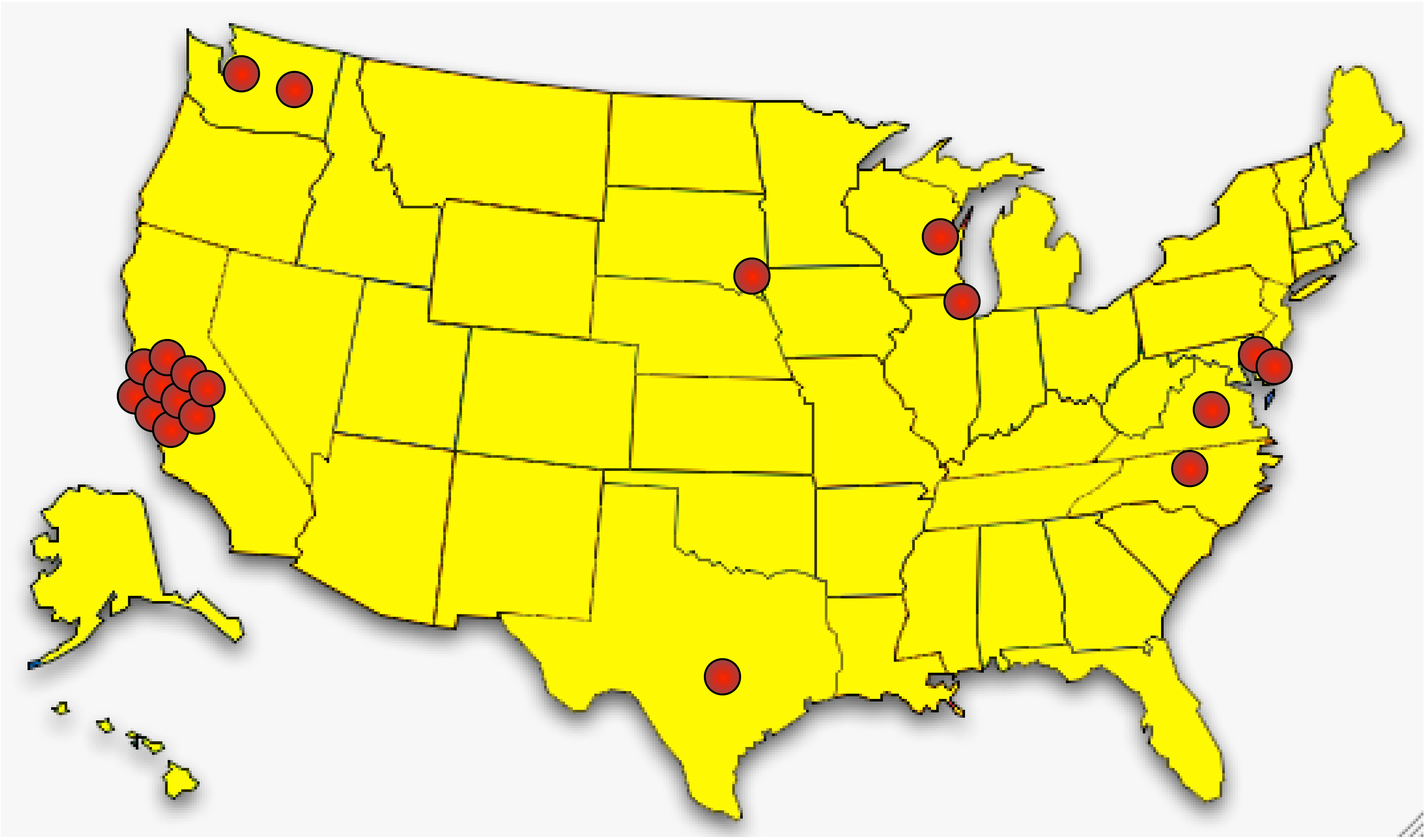
The *Remembrance of Data Passed Traceback Study*.

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. Ltr..doc
08/27/1999 /:dir270/Resume=Marymount U..doc
03/31/1999 /:dir270/NCR App. Ltr..doc
03/31/1999 /:dir270/Admissions counselor, NCR.doc
08/27/1999 /:dir270/Resume, Deb.doc
03/31/1999 /:dir270/UMUC App. Ltr..doc
03/31/1999 /:dir270/Ed. Coordinator Ltr..doc
03/31/1999 /:dir270/American College ...doc
04/01/1999 /:dir270/Am. U. Admin. Dir..doc
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 of compromised privacy was 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.

Poor training or supervision was the second leading cause.

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.

In two cases, the data custodians simply didn’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

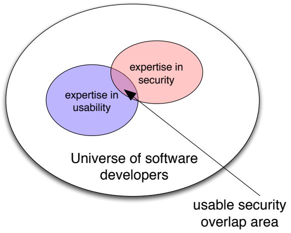
Unknown Reason: 7 cases

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

Regulation might have helped here, too.

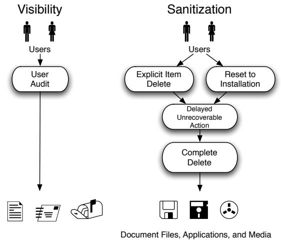
The Drives study establishes that data sanitization is a real problem.

1. Introduction to patterns. ✔

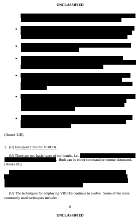


2. The Drives Study ✔

3. Patterns for sanitization.



4. Applying these patterns.



UNCLASSIFIED

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

(Annex 11E).

3. (U) Insurgent TTPs for VBIEDs

(U) There are two basic types of car bombs, i.e., [redacted]. Both can be either command or remote-detonated. (Annex 8E).

[redacted]

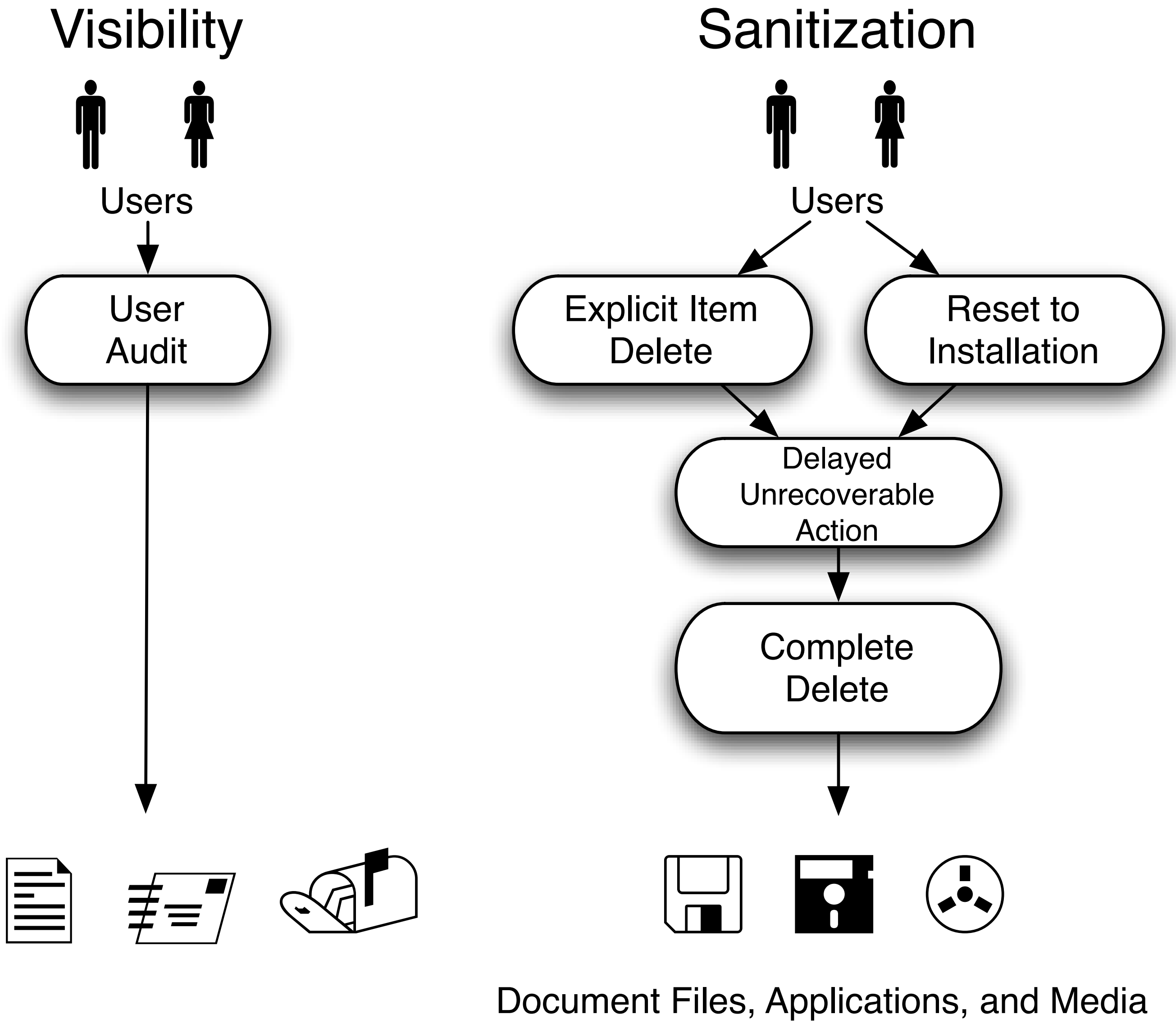
(U) The techniques for employing VBIEDs continue to evolve. Some of the more commonly used techniques include:

6

UNCLASSIFIED

But how can we solve it in a systematic fashion?

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



Visibility

Users

User Audit

Sanitization

Users

Explicit Item Delete

Reset to Installation

Delayed Unrecoverable Action

Complete Delete

Document Files, Applications, and Media

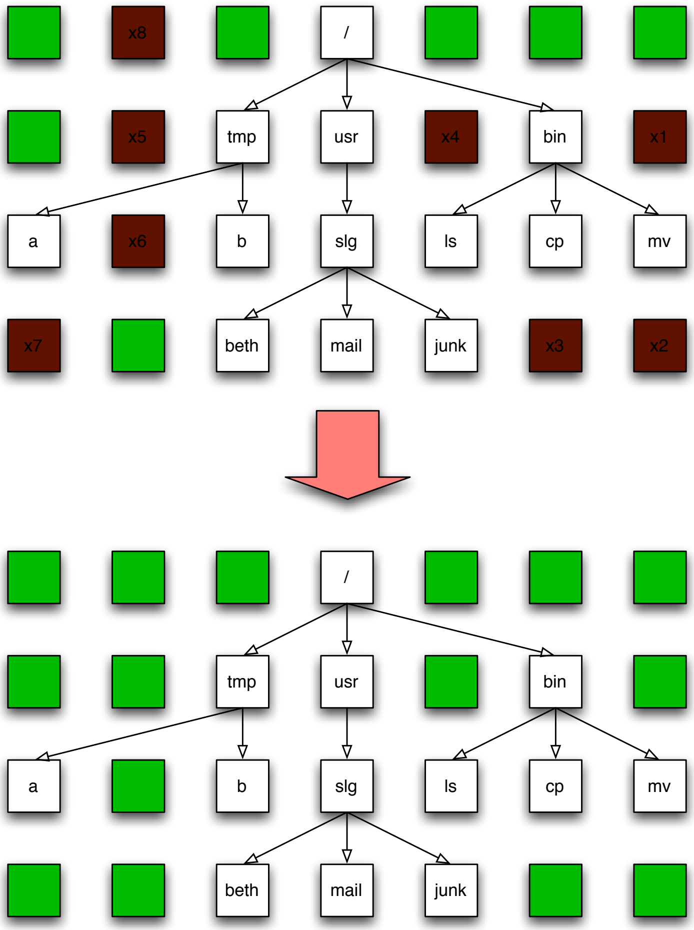
Complete Delete: assure that deleting the *visible* representation deletes the *hidden* data as well.

Sanitization

Users

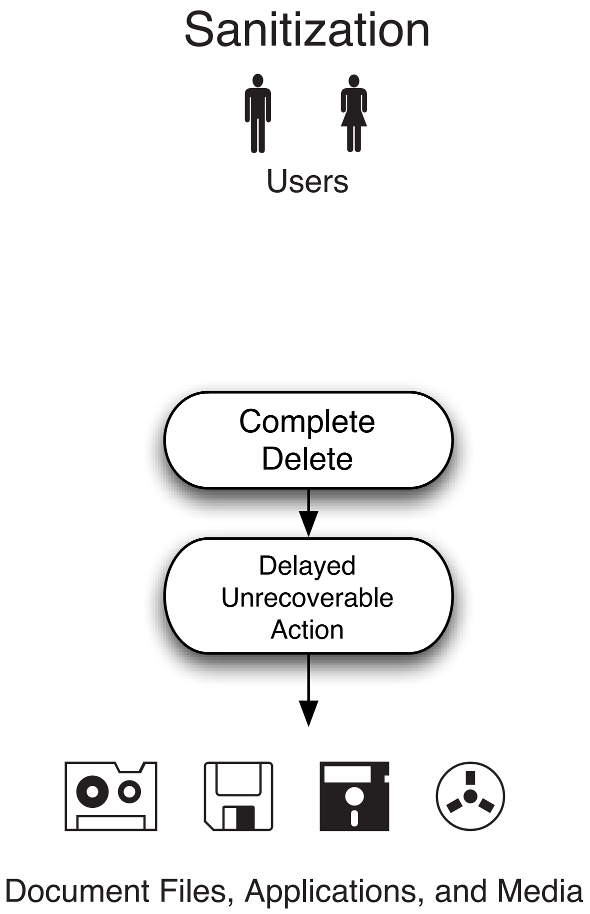
Complete Delete

Document Files, Applications, and Media



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

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



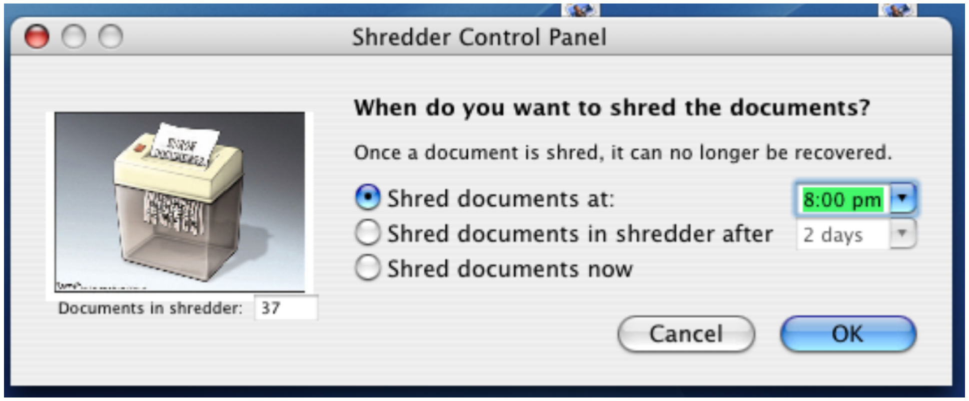
Sanitization

Users

Complete Delete

Delayed Unrecoverable Action

Document Files, Applications, and Media



Shredder Control Panel

When do you want to shred the documents?

Once a document is shred, it can no longer be recovered.

● Shred documents at: 8:00 pm

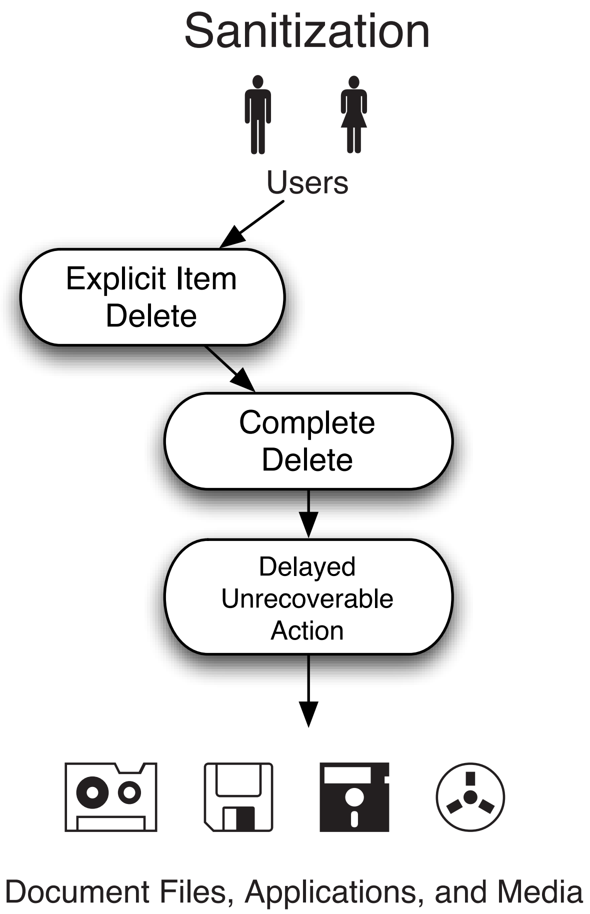
○ Shred documents in shredder after 2 days

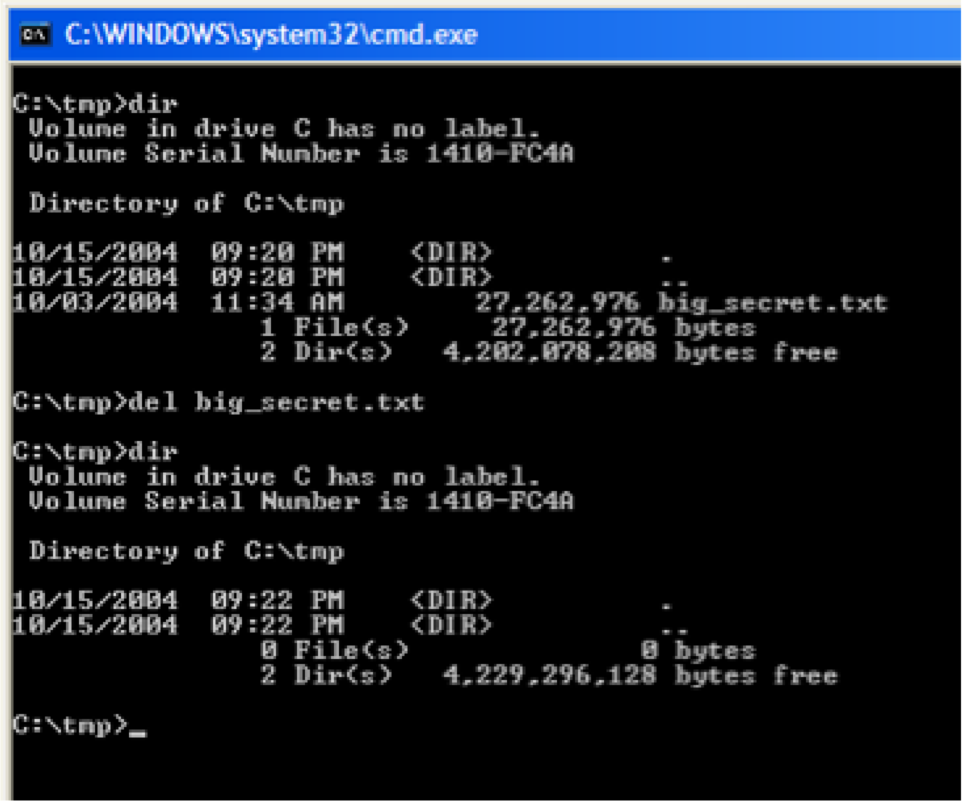
○ Shred documents now

Documents in shredder: 37

[Norman 83] and [Cooper 99] both suggest this functionality, but they do not give it a name.

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

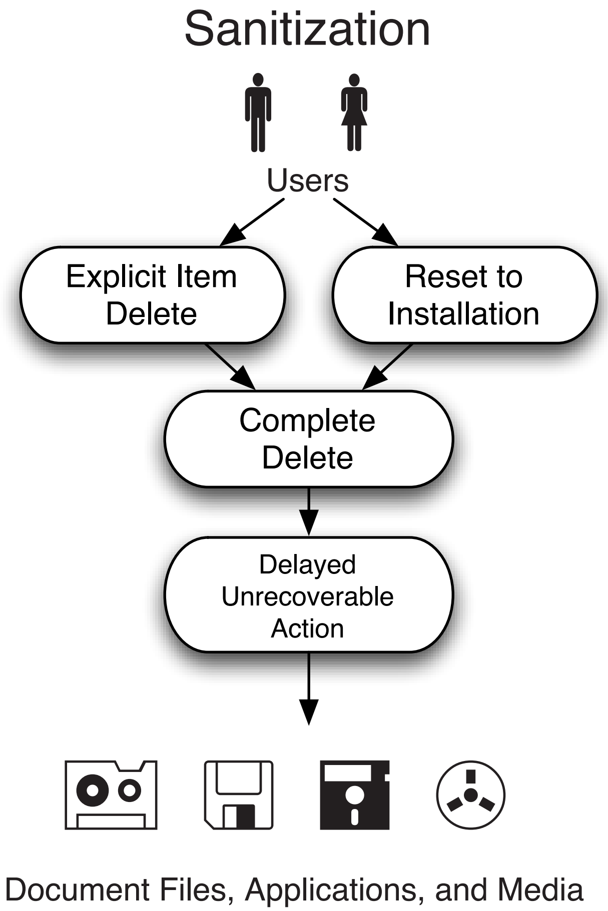

Sanitization
Users
Explicit Item Delete
Complete Delete
Delayed Unrecoverable Action
Document Files, Applications, and Media

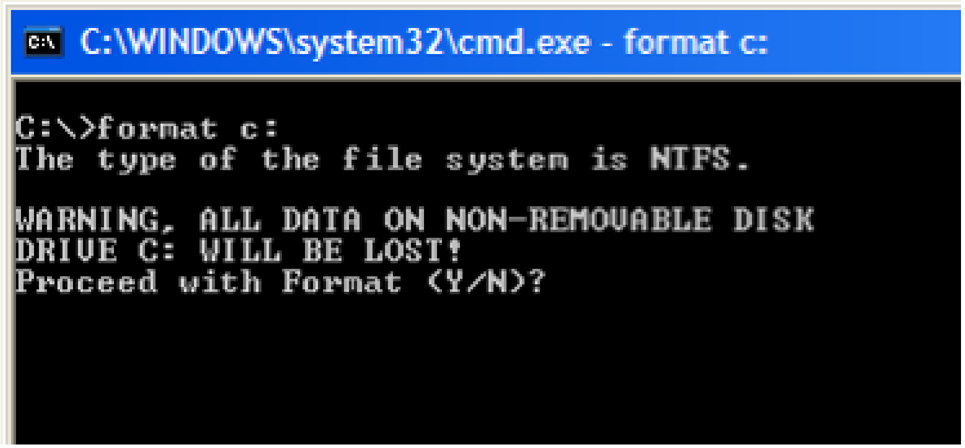


```
C:\tmp>dir
 Volume in drive C has no label.
 Volume Serial Number is 1410-FC4A

 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

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

C:\tmp>_
```

“Provide a means for deleting information where the information is displayed.”

Reset to Installation: Get rid of everything



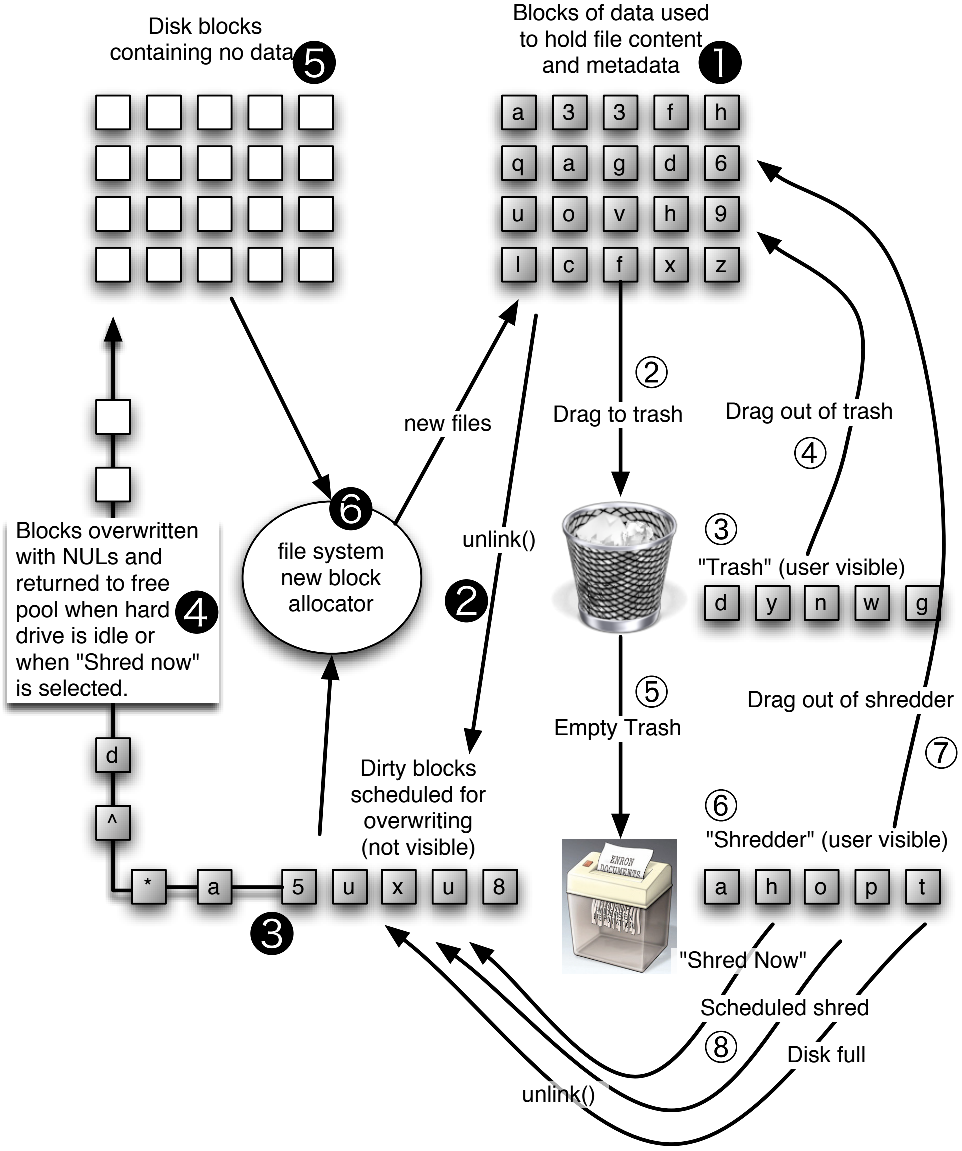


```
C:\>format c:
The type of the file system is NTFS.

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

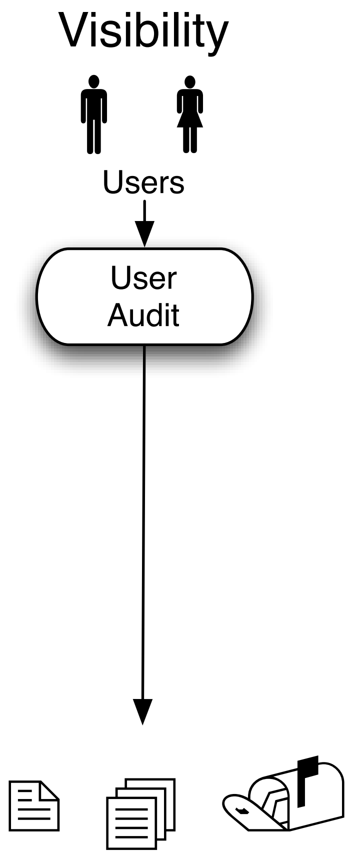
Reset/reinstall functionality is common (Windows; PalmOS; etc.).

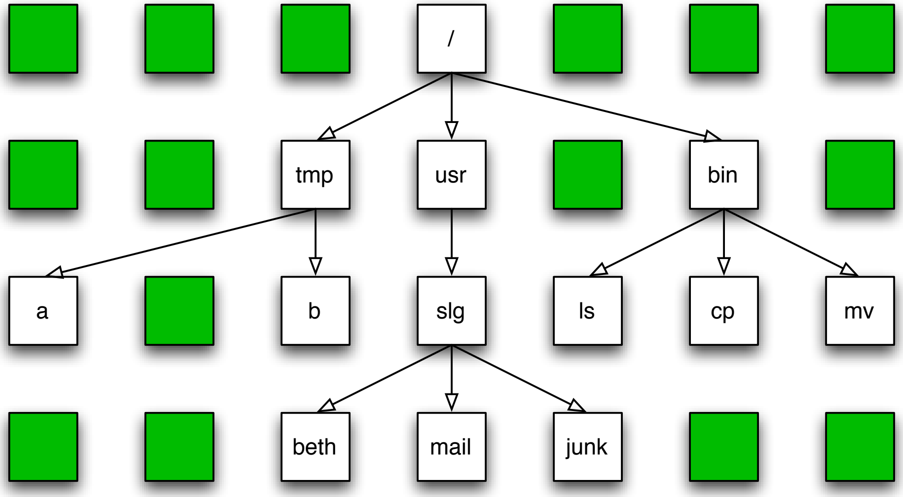
This pattern framework clarifies *Reset's* security property.

The shredder should be integrated into the file system.



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

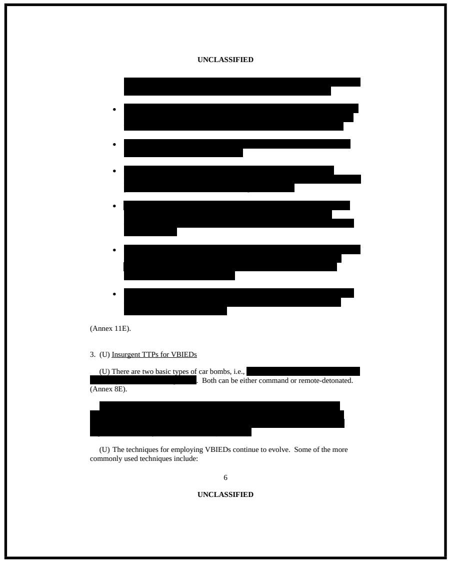




With files, this happens automatically when the *Complete Delete* pattern is implemented.

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

- Document Files



UNCLASSIFIED

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

(Annex 11E).

3. (U) Insurgent TTPs for VBIEDs

(U) There are two basic types of car bombs, i.e., [redacted]. Both can be either command or remote-detonated. (Annex 8E).

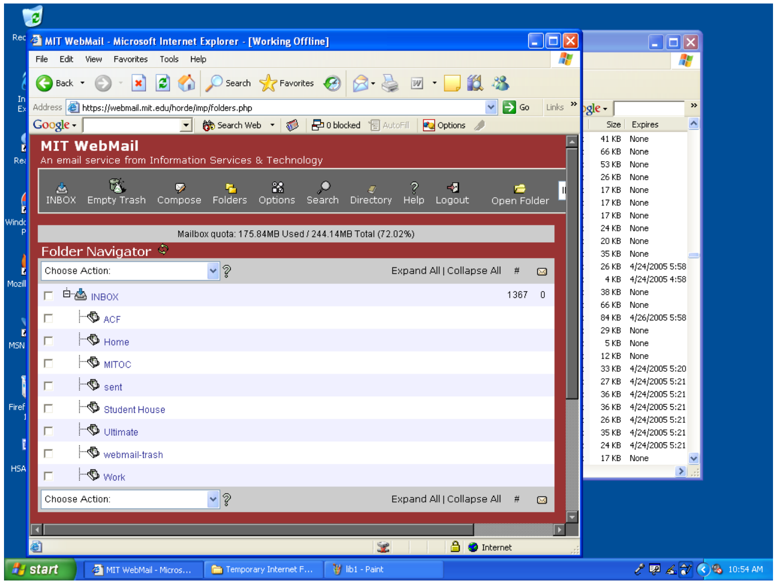
[redacted]

(U) The techniques for employing VBIEDs continue to evolve. Some of the more commonly used techniques include:

6

UNCLASSIFIED

- Web Browsers



https://webmail.mit.edu/horde/imp/folders.php

MIT WebMail

An email service from Information Services & Technology

Mailbox quota: 175.84MB Used / 244.14MB Total (72.02%)

Folder Navigator

Choose Action: — Expand All | Collapse All — #

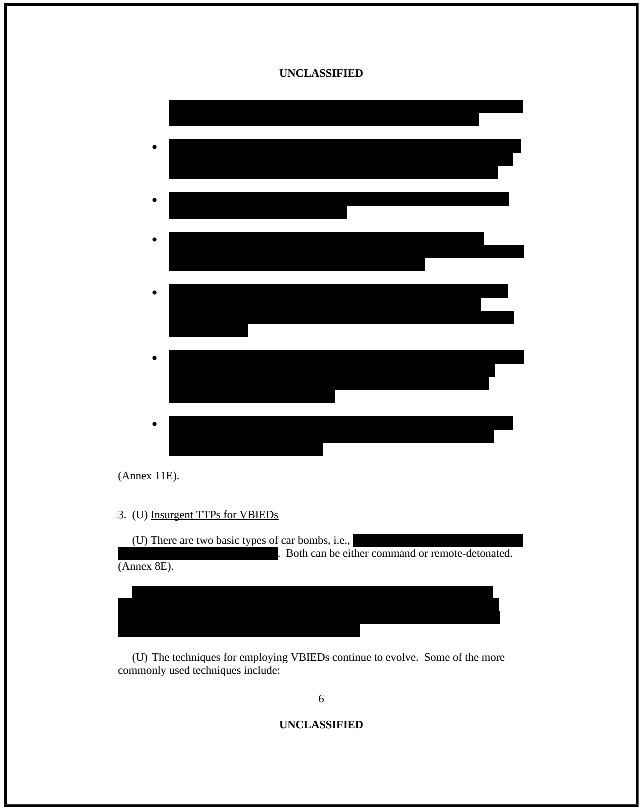
Folder	#	
☐ INBOX	1367	0
☐ ACF		
☐ Home		
☐ MITOC		
☐ sent		
☐ Student House		
☐ Ultimate		
☐ webmail-trash		
☐ Work		

Choose Action: — Expand All | Collapse All — #

Size	Expires
41 KB	None
66 KB	None
53 KB	None
26 KB	None
17 KB	None
17 KB	None
17 KB	None
24 KB	None
20 KB	None
35 KB	None
26 KB	4/24/2005 5:58
4 KB	4/24/2005 4:58
38 KB	None
66 KB	None
84 KB	4/26/2005 5:58
29 KB	None
5 KB	None
12 KB	None
33 KB	4/24/2005 5:20
27 KB	4/24/2005 5:21
36 KB	4/24/2005 5:21
36 KB	4/24/2005 5:21
26 KB	4/24/2005 5:21
35 KB	4/24/2005 5:21
24 KB	4/24/2005 5:21
17 KB	None

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 Forces-Iraq (MNF-I) report on the death of Nicola Calipari, March 4, 2005



UNCLASSIFIED

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

(Annex 11E).

3. (U) Insurgent TTPs for VBIEDs

(U) There are two basic types of car bombs, i.e., [redacted]. Both can be either command or remote-detonated. (Annex 8E).

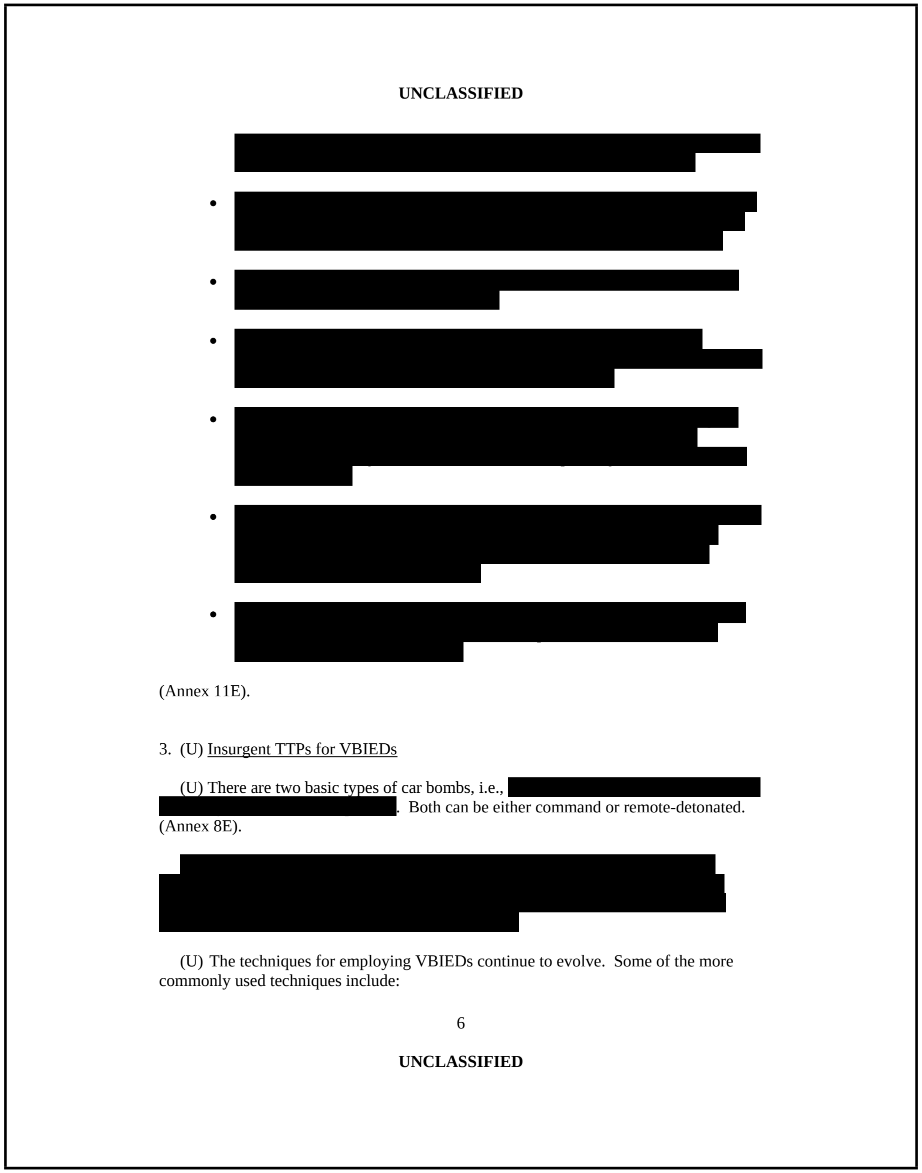
[redacted]

(U) The techniques for employing VBIEDs continue to evolve. Some of the more commonly used techniques include:

6

UNCLASSIFIED

Information was unintentionally hidden in the MNF-I report.



UNCLASSIFIED

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

(Annex 11E).

3. (U) Insurgent TTPs for VBIEDs

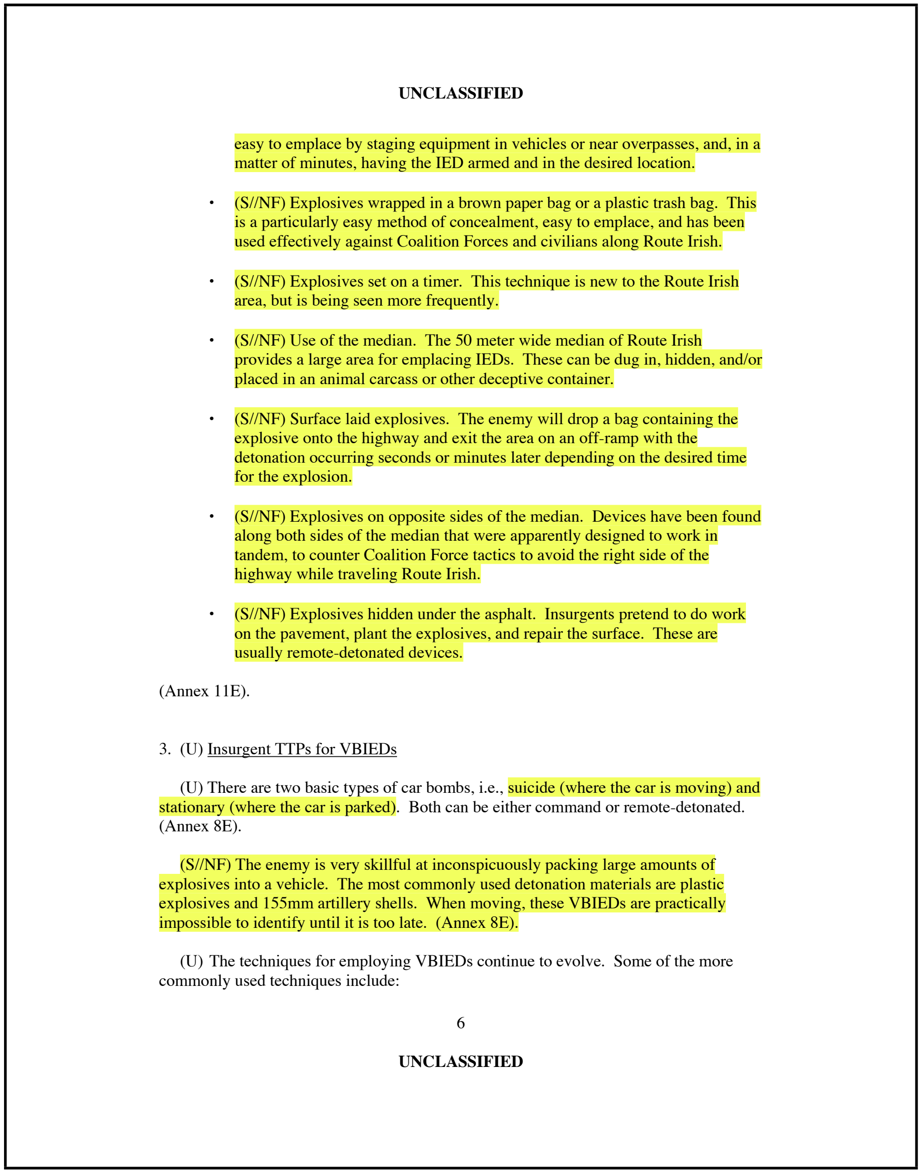
(U) There are two basic types of car bombs, i.e., [redacted]. Both can be either command or remote-detonated. (Annex 8E).

[redacted]

(U) The techniques for employing VBIEDs continue to evolve. Some of the more commonly used techniques include:

6

UNCLASSIFIED



UNCLASSIFIED

easy to emplace by staging equipment in vehicles or near overpasses, and, in a matter of minutes, having the IED armed and in the desired location.

- (S//NF) Explosives wrapped in a brown paper bag or a plastic trash bag. This is a particularly easy method of concealment, easy to emplace, and has been used effectively against Coalition Forces and civilians along Route Irish.
- (S//NF) Explosives set on a timer. This technique is new to the Route Irish area, but is being seen more frequently.
- (S//NF) Use of the median. The 50 meter wide median of Route Irish provides a large area for emplacing IEDs. These can be dug in, hidden, and/or placed in an animal carcass or other deceptive container.
- (S//NF) Surface laid explosives. The enemy will drop a bag containing the explosive onto the highway and exit the area on an off-ramp with the detonation occurring seconds or minutes later depending on the desired time for the explosion.
- (S//NF) Explosives on opposite sides of the median. Devices have been found along both sides of the median that were apparently designed to work in tandem, to counter Coalition Force tactics to avoid the right side of the highway while traveling Route Irish.
- (S//NF) Explosives hidden under the asphalt. Insurgents pretend to do work on the pavement, plant the explosives, and repair the surface. These are usually remote-detonated devices.

(Annex 11E).

3. (U) Insurgent TTPs for VBIEDs

(U) There are two basic types of car bombs, i.e., suicide (where the car is moving) and stationary (where the car is parked). Both can be either command or remote-detonated. (Annex 8E).

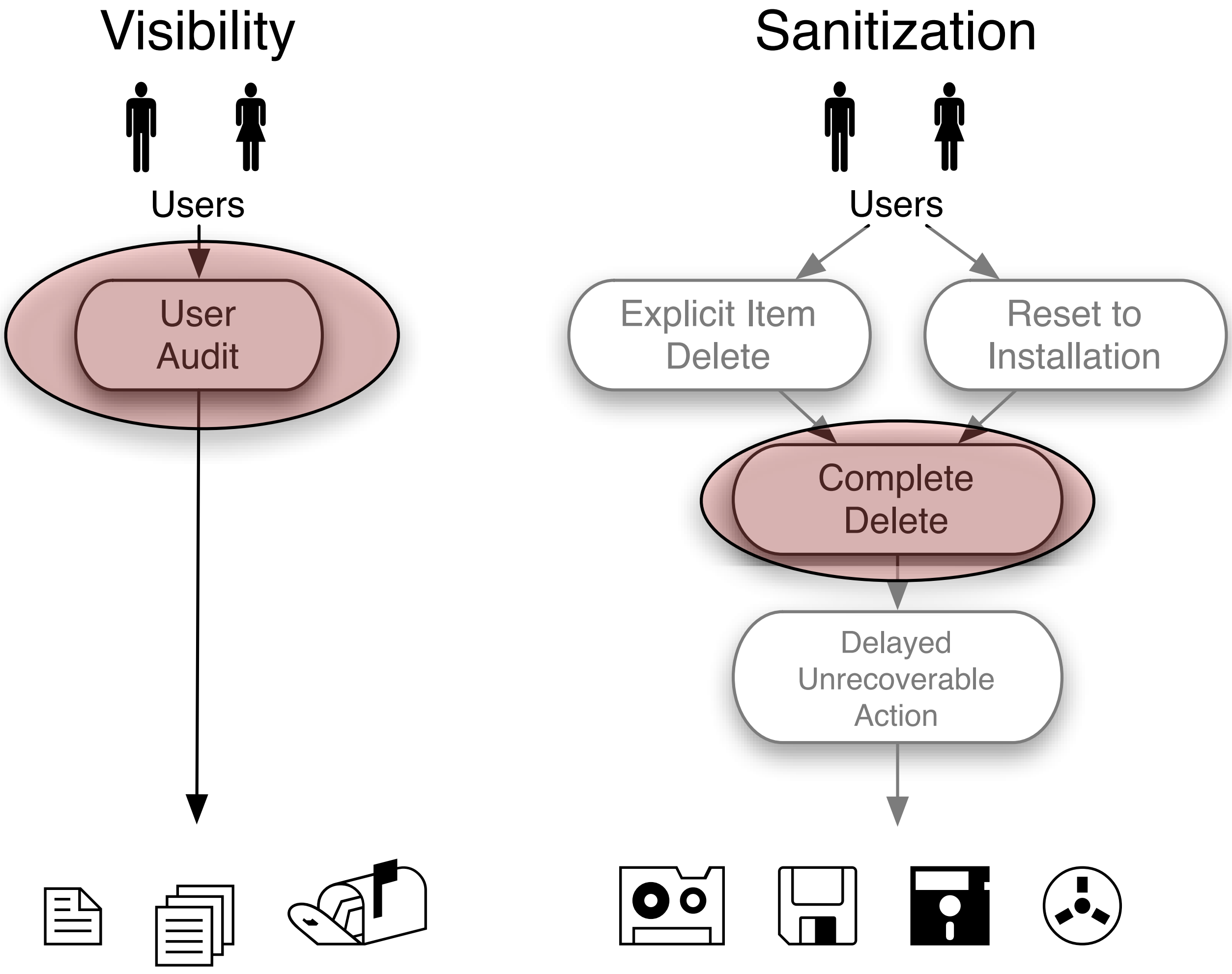
(S//NF) The enemy is very skillful at inconspicuously packing large amounts of explosives into a vehicle. The most commonly used detonation materials are plastic explosives and 155mm artillery shells. When moving, these VBIEDs are practically impossible to identify until it is too late. (Annex 8E).

(U) The techniques for employing VBIEDs continue to evolve. Some of the more commonly used techniques include:

6

UNCLASSIFIED

The information leaked because two patterns were not implemented.



Visibility

Users

User Audit

Sanitization

Users

Explicit Item Delete

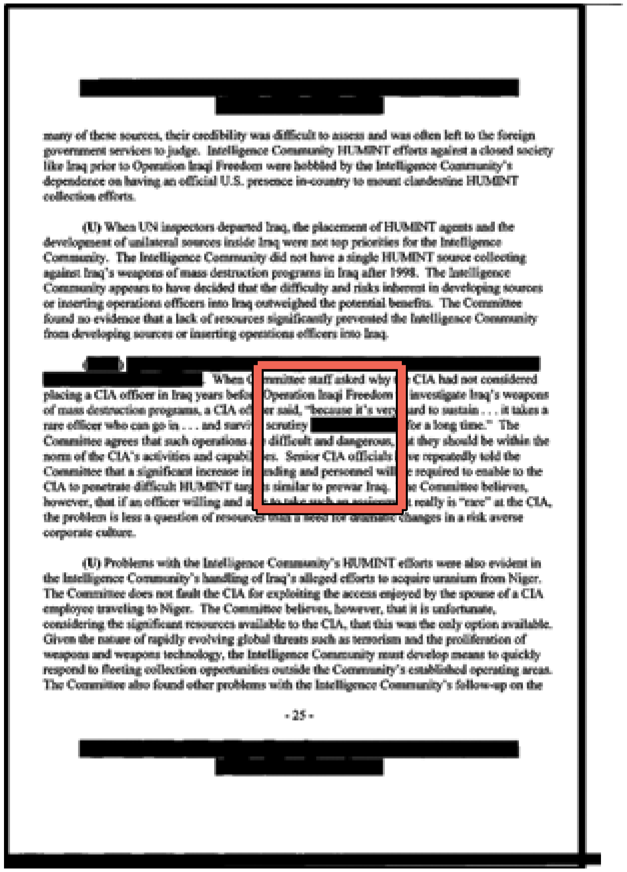
Reset to Installation

Complete Delete

Delayed Unrecoverable Action

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.



[redacted]

many of these sources, their credibility was difficult to assess and was often left to the foreign government services to judge. Intelligence Community HUMINT efforts against a closed society like Iraq prior to Operation Iraqi Freedom were hobbled by the Intelligence Community's dependence on having an official U.S. presence in-country to mount clandestine HUMINT collection efforts.

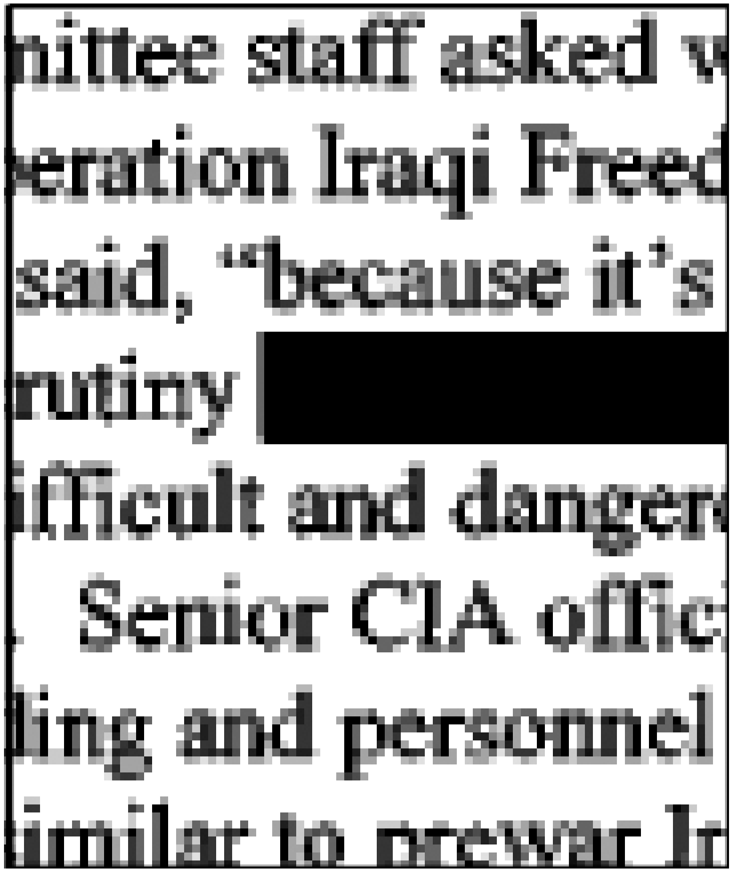
(U) When UN inspectors departed Iraq, the placement of HUMINT agents and the development of unilateral sources inside Iraq were not top priorities for the Intelligence Community. The Intelligence Community did not have a single HUMINT source collecting against Iraq's weapons of mass destruction programs in Iraq after 1998. The Intelligence Community appears to have decided that the difficulty and risks inherent in developing sources or inserting operations officers into Iraq outweighed the potential benefits. The Committee found no evidence that a lack of resources significantly prevented the Intelligence Community from developing sources or inserting operations officers into Iraq.

[redacted]. When Committee staff asked why the CIA had not considered placing a CIA officer in Iraq years before Operation Iraqi Freedom to investigate Iraq's weapons of mass destruction programs, a CIA officer said, "because it's very hard to sustain . . . it takes a rare officer who can go in . . . and survive scrutiny [redacted] for a long time." The Committee agrees that such operations are difficult and dangerous, but they should be within the norm of the CIA's activities and capabilities. Senior CIA officials have repeatedly told the Committee that a significant increase in funding and personnel will be required to enable to the CIA to penetrate difficult HUMINT targets similar to prewar Iraq. The Committee believes, however, that if an officer willing and able to take such an assignment really is "rare" at the CIA, the problem is less a question of resources than a need for dramatic changes in a risk averse corporate culture.

(U) Problems with the Intelligence Community's HUMINT efforts were also evident in the Intelligence Community's handling of Iraq's alleged efforts to acquire uranium from Niger. The Committee does not fault the CIA for exploiting the access enjoyed by the spouse of a CIA employee traveling to Niger. The Committee believes, however, that it is unfortunate, considering the significant resources available to the CIA, that this was the only option available. Given the nature of rapidly evolving global threats such as terrorism and the proliferation of weapons and weapons technology, the Intelligence Community must develop means to quickly respond to fleeting collection opportunities outside the Community's established operating areas. The Committee also found other problems with the Intelligence Community's follow-up on the

- 25 -

[redacted]



nittee staff asked w

eration Iraqi Freed

said, "because it's

rutiny [redacted]

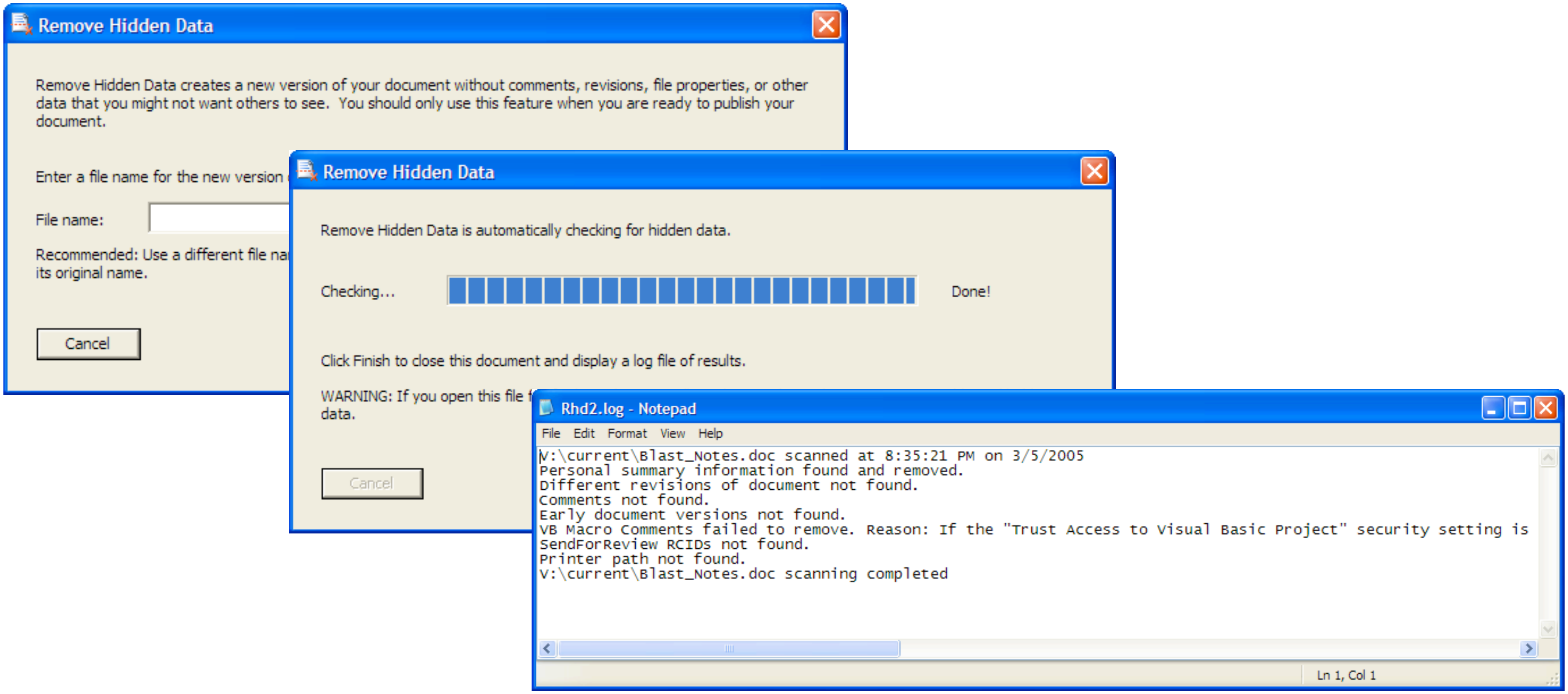
ifficult and danger

. 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 creates a new version of your document without comments, revisions, file properties, or other data that you might not want others to see. You should only use this feature when you are ready to publish your document.

Enter a file name for the new version

File name:

Recommended: Use a different file na
its original name.

Remove Hidden Data is automatically checking for hidden data.

Checking...

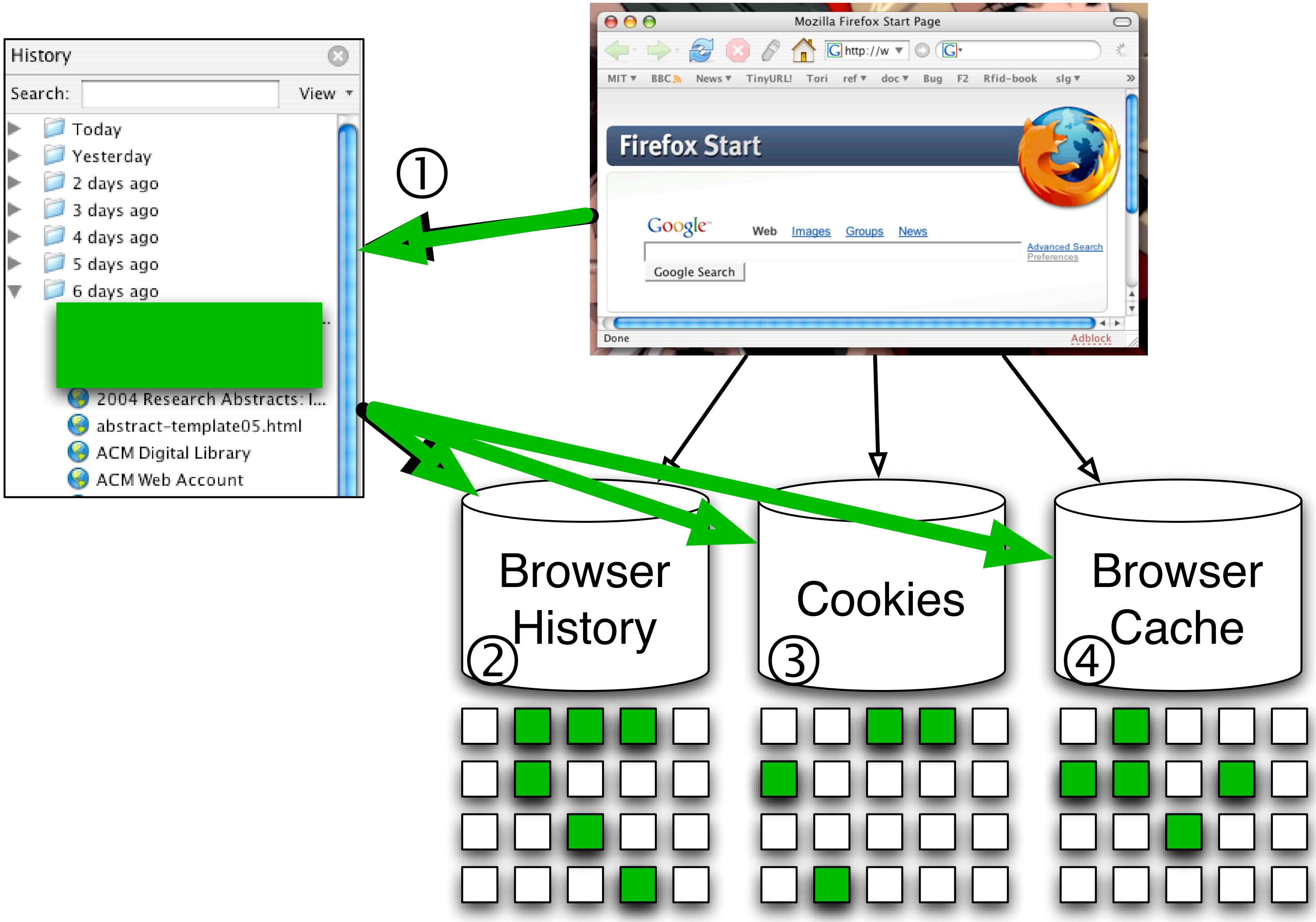
Click Finish to close this document and display a log file of results.

WARNING: If you open this file f
data.

```
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
```

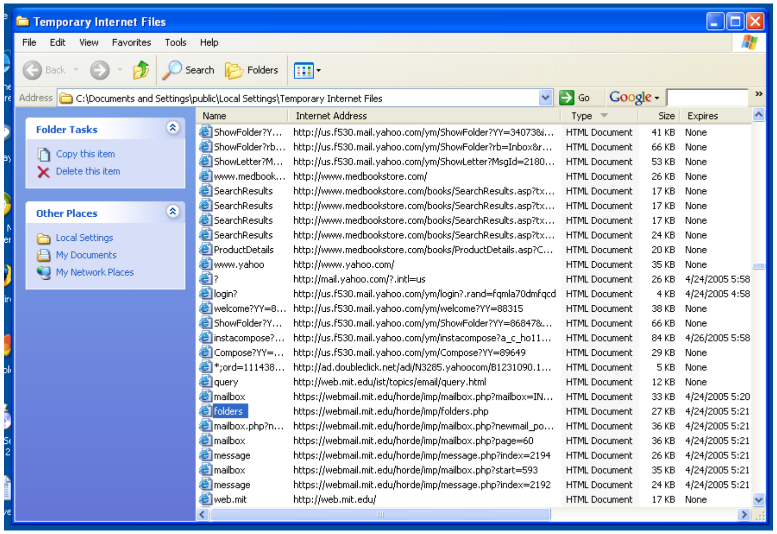
RHD doesn’t integrate into the flow of document preparation. The patterns-based analysis predicts that RHD will fail in many cases.

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.

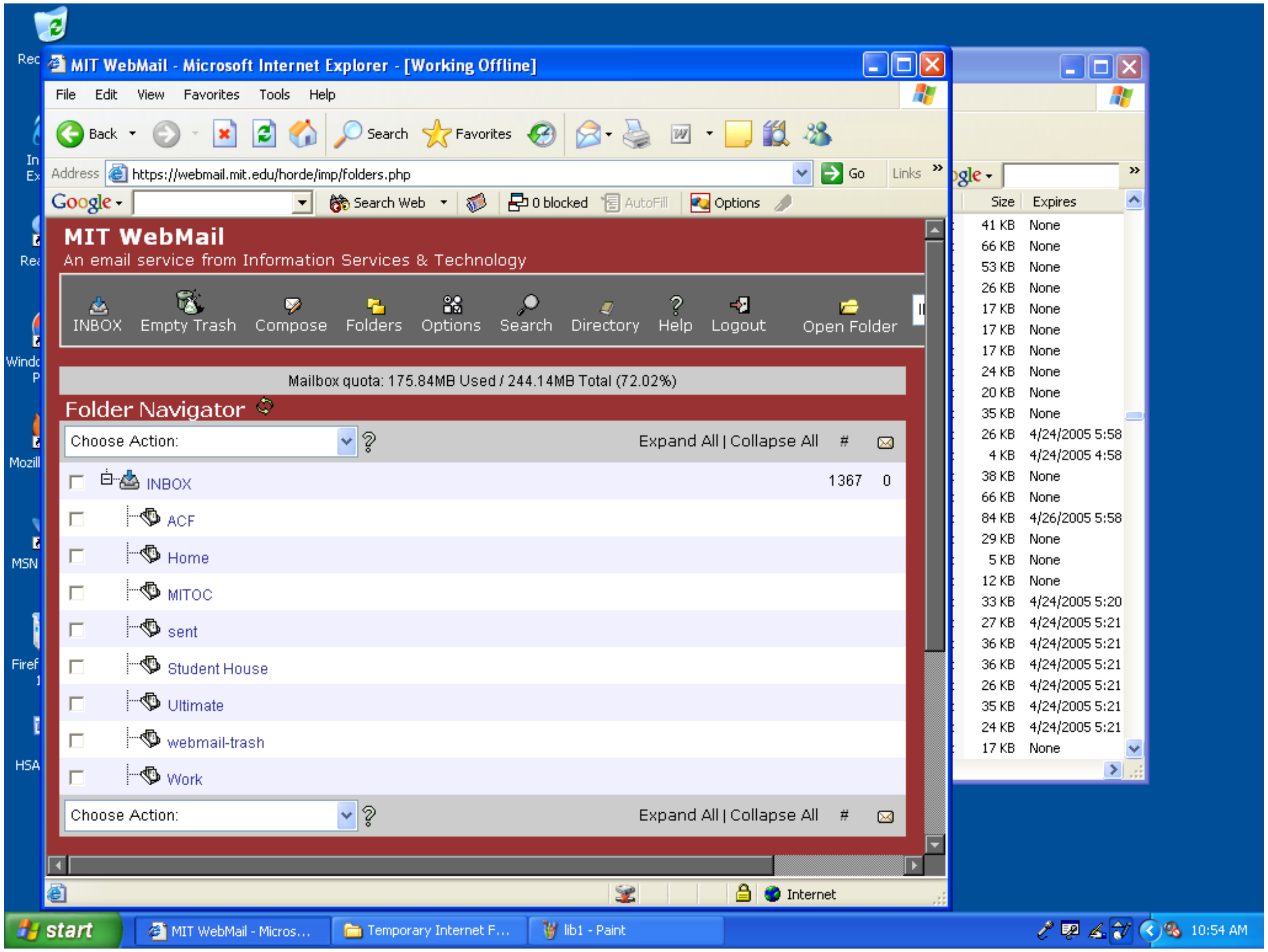


Address C:\Documents and Settings\public\Local Settings\Temporary Internet Files

Name	Internet Address	Type	Size	Expires
ShowFolder?Y...	http://us.f530.mail.yahoo.com/ym/ShowFolder?YY=34073&i...	HTML Document	41 KB	None
ShowFolder?rb...	http://us.f530.mail.yahoo.com/ym/ShowFolder?rb=Inbox&r...	HTML Document	66 KB	None
ShowLetter?M...	http://us.f530.mail.yahoo.com/ym/ShowLetter?MsgId=2180...	HTML Document	53 KB	None
www.medbook...	http://www.medbookstore.com/	HTML Document	26 KB	None
SearchResults	http://www.medbookstore.com/books/SearchResults.asp?tx...	HTML Document	17 KB	None
SearchResults	http://www.medbookstore.com/books/SearchResults.asp?tx...	HTML Document	17 KB	None
SearchResults	http://www.medbookstore.com/books/SearchResults.asp?tx...	HTML Document	17 KB	None
SearchResults	http://www.medbookstore.com/books/SearchResults.asp?tx...	HTML Document	24 KB	None
ProductDetails	http://www.medbookstore.com/books/ProductDetails.asp?C...	HTML Document	20 KB	None
www.yahoo	http://www.yahoo.com/	HTML Document	35 KB	None
?	http://mail.yahoo.com/?.intl=us	HTML Document	26 KB	4/24/2005 5:58
login?	http://us.f530.mail.yahoo.com/ym/login?.rand=fqmla70dmfqcd	HTML Document	4 KB	4/24/2005 4:58
welcome?YY=8...	http://us.f530.mail.yahoo.com/ym/welcome?YY=88315	HTML Document	38 KB	None
ShowFolder?Y...	http://us.f530.mail.yahoo.com/ym/ShowFolder?YY=86847&...	HTML Document	66 KB	None
instacompose?...	http://us.f530.mail.yahoo.com/ym/instacompose?a_c_ho11...	HTML Document	84 KB	4/26/2005 5:58
Compose?YY=...	http://us.f530.mail.yahoo.com/ym/Compose?YY=89649	HTML Document	29 KB	None
*;ord=111438...	http://ad.doubleclick.net/adi/N3285.yahoocom/B1231090.1...	HTML Document	5 KB	None
query	http://web.mit.edu/ist/topics/email/query.html	HTML Document	12 KB	None
mailbox	https://webmail.mit.edu/horde/imp/mailbox.php?mailbox=IN...	HTML Document	33 KB	4/24/2005 5:20
folders	https://webmail.mit.edu/horde/imp/folders.php	HTML Document	27 KB	4/24/2005 5:21
mailbox.php?n...	https://webmail.mit.edu/horde/imp/mailbox.php?newmail_po...	HTML Document	36 KB	4/24/2005 5:21
mailbox	https://webmail.mit.edu/horde/imp/mailbox.php?page=60	HTML Document	36 KB	4/24/2005 5:21
message	https://webmail.mit.edu/horde/imp/message.php?index=2194	HTML Document	26 KB	4/24/2005 5:21
mailbox	https://webmail.mit.edu/horde/imp/mailbox.php?start=593	HTML Document	35 KB	4/24/2005 5:21
message	https://webmail.mit.edu/horde/imp/message.php?index=2192	HTML Document	24 KB	4/24/2005 5:21
web.mit	http://web.mit.edu/	HTML Document	17 KB	None

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 Internet Explorer - [Working Offline]

https://webmail.mit.edu/horde/imp/folders.php

MIT WebMail

An email service from Information Services & Technology

Mailbox quota: 175.84MB Used / 244.14MB Total (72.02%)

Folder Navigator

Choose Action: ? Expand All | Collapse All #

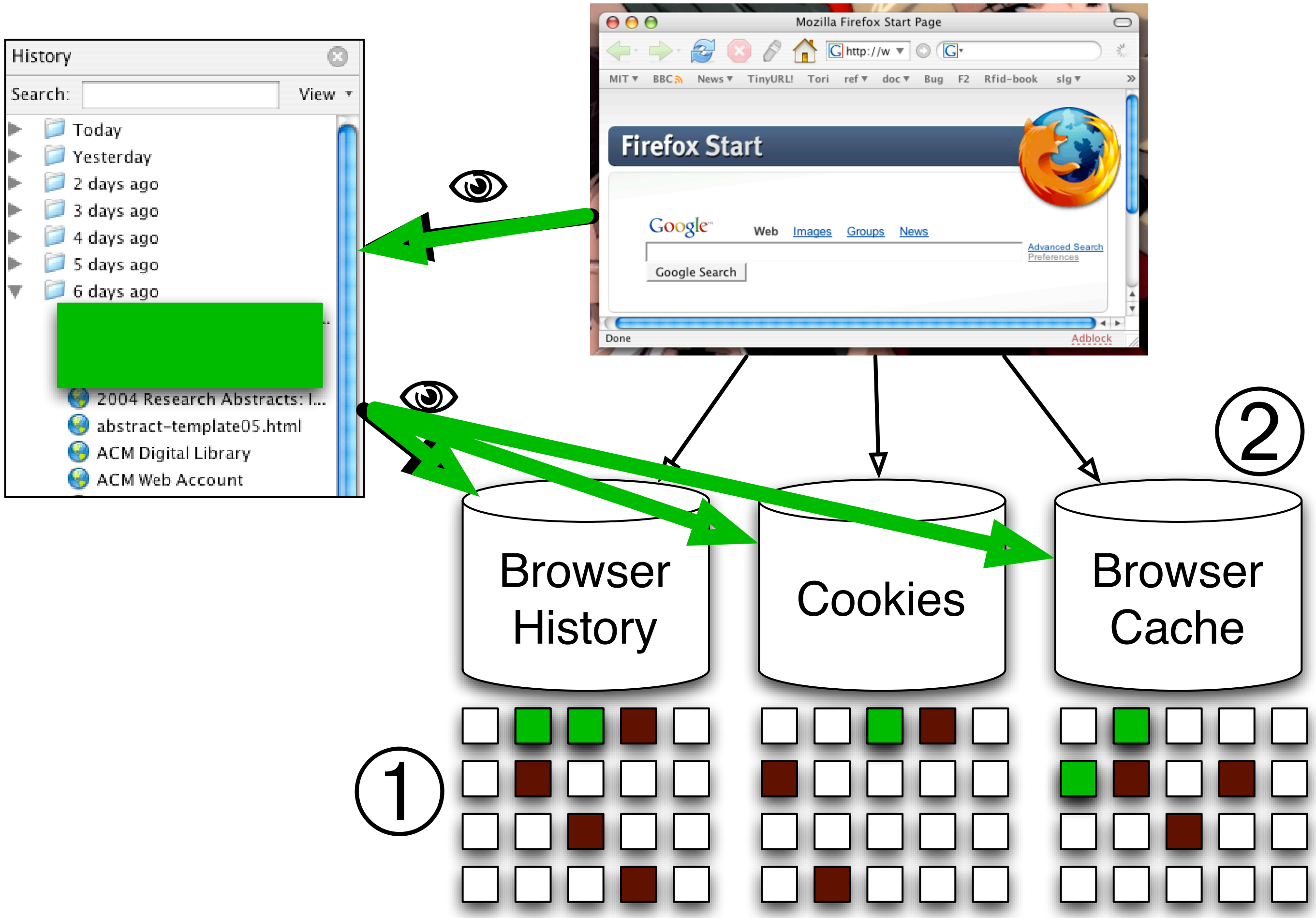
□	INBOX	1367	0
□	ACF		
□	Home		
□	MITOC		
□	sent		
□	Student House		
□	Ultimate		
□	webmail-trash		
□	Work		

Choose Action: ? Expand All | Collapse All #

Size	Expires
41 KB	None
66 KB	None
53 KB	None
26 KB	None
17 KB	None
17 KB	None
17 KB	None
24 KB	None
20 KB	None
35 KB	None
26 KB	4/24/2005 5:58
4 KB	4/24/2005 4:58
38 KB	None
66 KB	None
84 KB	4/26/2005 5:58
29 KB	None
5 KB	None
12 KB	None
33 KB	4/24/2005 5:20
27 KB	4/24/2005 5:21
36 KB	4/24/2005 5:21
36 KB	4/24/2005 5:21
26 KB	4/24/2005 5:21
35 KB	4/24/2005 5:21
24 KB	4/24/2005 5:21
17 KB	None

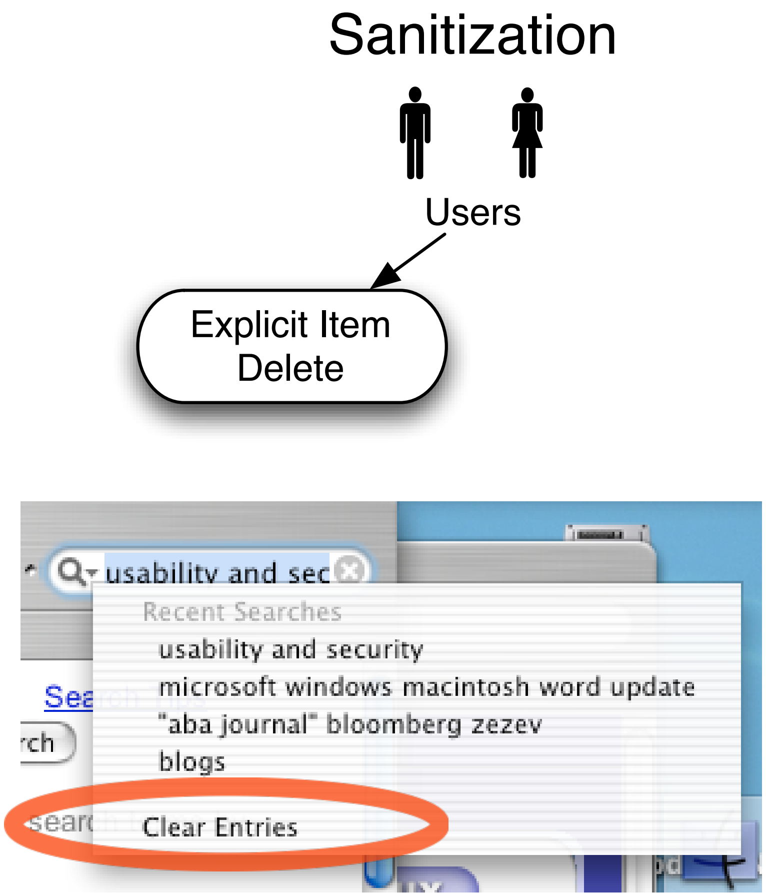
The American Library Association recommends software that automatically purges caches on a *daily* basis.[ALA 05] (It would be better to purge after each use.)

Applying the patterns, an obvious solution is to unify the history and cache:



The patterns make it easy to explain this concept to the browser developers and users.

The patterns also suggest opportunities for further promoting HCI-SEC within the browser.



usability and sec

Recent Searches

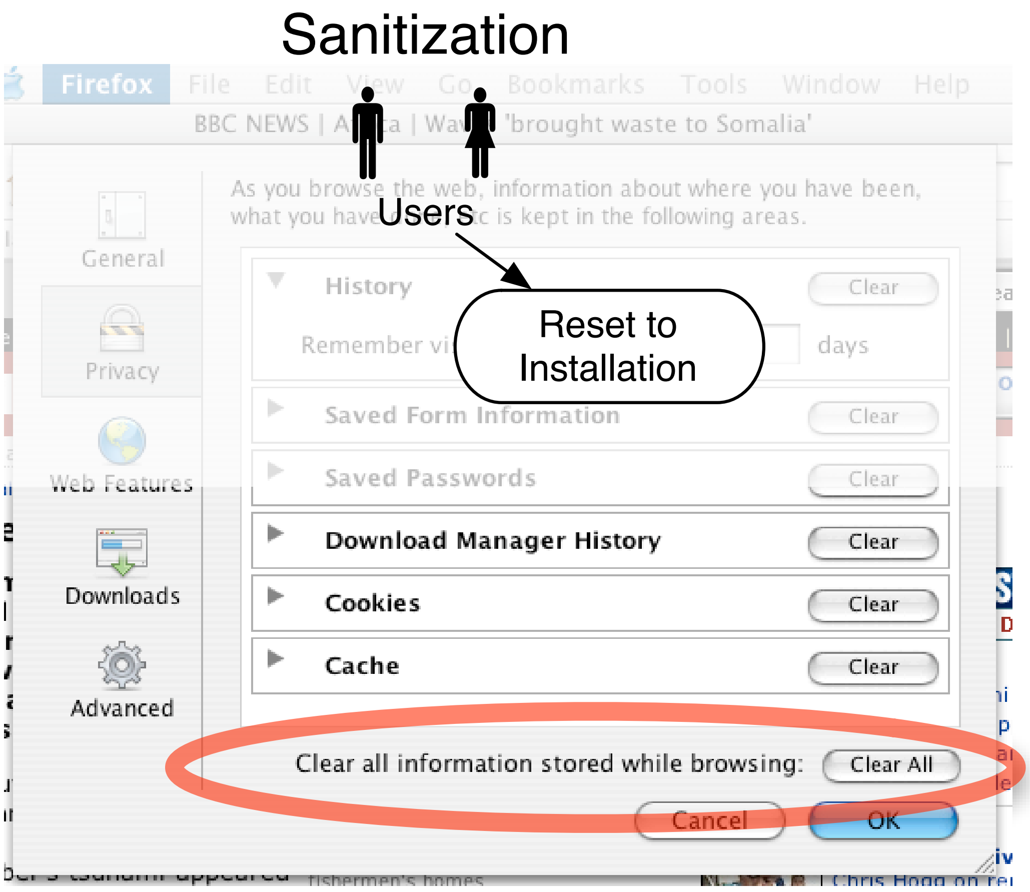
usability and security

microsoft windows macintosh word update

"aba journal" bloomberg zezev

blogs

Clear Entries



BBC NEWS | Africa | Waste 'brought waste to Somalia'

As you browse the web, information about where you have been, what you have done, etc is kept in the following areas.

History — Clear

Remember visited pages for the last days

Saved Form Information — Clear

Saved Passwords — Clear

Download Manager History — Clear

Cookies — Clear

Cache — Clear

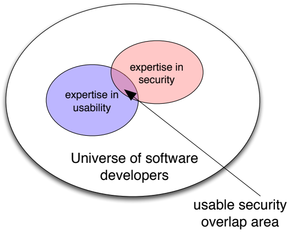
Clear all information stored while browsing: Clear All

Cancel OK

Without *Complete Delete* the data can still be recovered. This demonstrates the need for the complete pattern set.

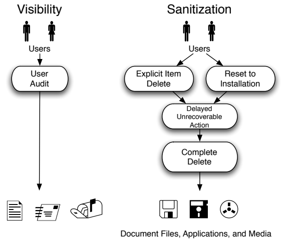
In Summary

1. Introduction to patterns. ✔

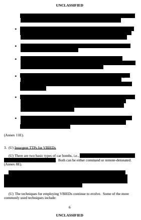


2. The Drives Study ✔

3. Patterns for sanitization. ✔



4. Applying these patterns. ✔



UNCLASSIFIED

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

(Annex 11E).

3. (U) Insurgent TTPs for VBIEDs

(U) There are two basic types of car bombs, i.e., [redacted]. Both can be either command or remote-detonated. (Annex 8E).

[redacted]

(U) The techniques for employing VBIEDs continue to evolve. Some of the more commonly used techniques include:

6

UNCLASSIFIED

Questions?